50 1190 0101

Утвержден

РУСБ.10015-01-УД

Подп. и дата	
Инв. № дубл.	
Взам. инв. №	
Подп. и дата	
Инв. № подл.	

ОПЕРАЦИОННАЯ СИСТЕМА СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ «ASTRA LINUX SPECIAL EDITION»

Руководство администратора. Часть 1

Бюллетень № 2025-0811SE18

РУСБ.10015-01 95 01-1

Листов 452

2025

Литера O_1

1.8.3

АННОТАЦИЯ

Настоящий документ является первой частью руководства администратора программного изделия РУСБ.10015-01 «Операционная система специального назначения «Astra Linux Special Edition» (далее по тексту — ОС).

Документ предназначен для администраторов системы и сети. Администраторы безопасности должны руководствоваться документом РУСБ.10015-01 97 01-1 «Операционная система специального назначения «Astra Linux Special Edition». Руководство по КСЗ. Часть 1».

Руководство администратора состоит из двух частей:

- РУСБ.10015-01 95 01-1 «Операционная система специального назначения «Astra Linux Special Edition». Руководство администратора. Часть 1»;
- РУСБ.10015-01 95 01-2 «Операционная система специального назначения «Astra Linux Special Edition». Руководство администратора. Часть 2. Установка и миграция».

Перед установкой и настройкой ОС необходимо провести ее контроль, предусмотренный формуляром при первичном закреплении экземпляра ОС за ответственным лицом.

В первой части руководства приведено назначение и настройка ОС. Рассмотрены системные компоненты, службы и команды, базовые сетевые службы, средства организации ЕПП, защищенная графическая подсистема, управление программными пакетами, резервное копирование и восстановление данных, система печати, защищенные комплексы программ гипертекстовой обработки данных и электронной почты, средства контроля целостности, централизованного протоколирования и разграничения доступа к подключаемым устройствам. Приведен список сообщений для администратора.

Во второй части руководства приведено описание установки ОС, а также порядок миграции на текущее очередное обновление ОС.

Требования к обеспечению безопасности среды функционирования, а также настройка параметров, необходимых для безопасной эксплуатации ОС, приведены в документе РУСБ.10015-01 97 01-1 и выполняются администратором безопасности.

Порядок работы с защищенной СУБД приведен в документе РУСБ.10015-01 97 01-3 «Операционная система специального назначения «Astra Linux Special Edition». Руководство по КСЗ. Часть 3. Защищенная СУБД».

Дополнительная информация о настройке компонентов и управлении программными пакетами, а также варианты реализации отдельных решений с использованием ОС приведены на официальном сайте `wiki.astralinux.ru`.

СОДЕРЖАНИЕ

РУСБ.10015-01 95 01-2 «Операционная система специального назначения «Astra Linux Special Edition». Руководство администратора. Часть 2. Установка и миграция»

1. АДМИНИСТРИРОВАНИЕ ОС

Административное управление в ОС отделено от общего доступа пользователей.

Большинство операций по настройке и администрированию ОС требуют прав суперпользователя (`root`), например:

- монтирование и размонтирование ФС;
- изменение корневого каталога процесса командой `chroot`;
- создание файлов устройств;
- установка системных часов;
- изменение принадлежности файлов;
- задание host-имени системы;
- конфигурирование сетевых интерфейсов.

ВНИМАНИЕ! После установки ОС интерактивный вход в систему суперпользователя по умолчанию заблокирован. Для администрирования системы при установке ОС создается пользователь, входящий в группу `astra-admin`. Пользователю, входящему в группу `astra-admin`, через механизм `sudo` предоставляются права для выполнения действий по настройке ОС, требующих привилегий `root`. Далее по тексту такой пользователь именуется администратором. Описание механизма `sudo` приведено в 1.1.2.

ВНИМАНИЕ! Действия по администрированию ОС при включенном мандатном контроле целостности (МКЦ) необходимо выполнять в привилегированном режиме с высокой меткой целостности. Пользователю, создаваемому при установке ОС, назначается максимальная метка целостности. Описание МКЦ приведено в документе РУСБ.10015-01 97 01-1.

1.1. Получение прав суперпользователя

Существует несколько способов получения прав суперпользователя:

- вход в систему от имени учетной записи `root` (по умолчанию заблокирован);
- использование команды `su` (по умолчанию заблокирован);
- использование команды `sudo` (рекомендуется).

1.1.1. su

Команда `su` используется пользователем для запуска команд от имени другого пользователя. В том числе могут быть запущены команды от имени учетной записи `root`.

При запуске команды `su` без параметров подразумевается, что пользователь хочет запустить командный интерпретатор `shell` от имени учетной записи `root`. При этом система просит

ввести пароль от учетной записи root. При вводе правильного пароля запускаемый интерпретатор команд получает права и привилегии суперпользователя, которые сохраняются до завершения его работы. Пользователю для получения прав суперпользователя не требуется завершать свою сессию и вновь входить в систему.

С помощью команды su, вводимой с параметром -c, пользователь может выполнять отдельные команды от имени учетной записи root без запуска командного интерпретатора shell. При этом пользователь получает права и привилегии суперпользователя на ограниченное время, а именно, на время исполнения заданной команды. Например, при необходимости поменять атрибуты файла ввести команду от имени учетной записи root:

```
su -c 'chmod 0777 /tmp/test.txt'
```

После ввода пароля учетной записи root команда chmod получит права и привилегии суперпользователя на выполнение заданного запроса, но при этом права и привилегии пользователя на выполнение других команд не изменятся.

Кроме выполнения команд от имени учетной записи root, команда su позволяет выполнять команды от имени любого другого пользователя, при этом для выполнения команды необходимо знать пароль этого пользователя. Если вход в систему выполнен от имени root, то при использовании su для выполнения команды от имени другого пользователя знание пароля данного пользователя не требуется — все команды от имени любого пользователя исполняются без запроса пароля.

При предоставлении прав на использование команды su следует учитывать, что для нее отсутствует механизм ограничения списка команд, разрешенных конкретному пользователю выполнять от имени учетной записи root. Таким образом, если у пользователя есть права на выполнение команды su, то он может выполнить от имени учетной записи root любые команды. Поэтому использование команды su должно быть разрешено только доверенным пользователям. Также рекомендуется при вводе команды использовать полное путевое имя /bin/su (вместо su).

Описание команды приведено в man su.

1.1.2. sudo

Команда sudo используется пользователем для запуска команд от имени учетной записи root.

В качестве параметров команда sudo принимает командную строку, которую следует выполнить с правами суперпользователя. При выполнении команды sudo просматривается конфигурационный файл /etc/sudoers, в котором приведен список пользователей, имеющих полномочия на запуск команды sudo, а также перечень команд, которые каждый

из пользователей имеет право выполнять от имени учетной записи `root`. Если данному пользователю разрешено выполнять указанную им команду, то при выполнении команды `sudo` у пользователя запрашивается его пароль. Таким образом, для каждого пользователя установлен набор команд, которые он может выполнять от имени учетной записи `root` без необходимости вводить пароль учетной записи `root`.

При использовании `sudo` подсистемой регистрации событий регистрируется следующая информация: выполненные команды, вызвавшие их пользователи, из какого каталога вызывались команды, время вызова команд.

Для изменения файла `/etc/sudoers` используется команда `visudo`, запущенная от имени администратора.

Описание команды приведено в `man sudo`.

1.2. Механизмы разделения полномочий

К механизмам разделения полномочий между системными администраторами ОС могут быть отнесены:

- механизм привилегий;
- механизм повышения полномочий на время выполнения команды (программы);
- механизм установки ACL на файлы.

Описание механизмов разделения полномочий приведено в документе РУСБ.10015-01 97 01-1.

1.2.1. Механизм привилегий

Механизм привилегий ОС предназначен для передачи отдельным пользователям прав выполнения определенных административных действий. Обычный пользователь системы не имеет дополнительных привилегий.

Привилегии наследуются процессами от своих «родителей» и не могут быть переданы сторонним процессам. Процессы, запущенные от имени суперпользователя, независимо от наличия у них привилегий, имеют возможность осуществлять все привилегированные действия.

Распределение (первоначальная настройка) привилегий выполняется администратором с максимальной меткой целостности, установленной в ОС.

1.2.2. Механизм повышения полномочий

Механизм повышения полномочий позволяет повысить полномочия пользователя на время выполнения определенной программы. Настройка механизма может быть выполнена администратором с максимальной меткой целостности, установленной в ОС.

1.2.3. Механизм установки ACL на файлы

Механизм установки ACL на файлы облегчает задачу распределения полномочий, позволяя предоставлять доступ только к тем файловым объектам, к которым он необходим в соответствии с ролью пользователя. Настройку механизмов ACL выполняет администратор с максимальной меткой целостности, установленной в ОС.

2. УСТАНОВКА, НАСТРОЙКА И ОБНОВЛЕНИЕ ОС

2.1. Установка ОС

Подробное описание последовательности действий при установке ОС или миграции с предыдущих очередных обновлений приведено в РУСБ.10015-01 95 01-2.

В программе установки необходимо выбрать уровень защищенности ОС в соответствии с лицензионным соглашением:

1) базовый («Орел»);
2) усиленный («Воронеж»);
3) максимальный («Смоленск»).

2.2. Первичная настройка ОС

В пунктах 2.2.1–2.2.3 приведены применяемые настройки ОС для соответствующего уровня защищенности в случае, если при установке ОС были выбраны предложенные по умолчанию значения.

2.2.1. Базовый уровень защищенности («Орел»)

После установки ОС готова к использованию без дополнительных настроек.

На данном уровне защищенности для разграничения доступа применяется механизм дискреционного управления доступом (в т.ч. в СУБД). По умолчанию выключены режим отладки `ptrace` и возможность использовать механизм `sudo` без ввода пароля.

Дополнительно для защиты информации могут использоваться доступные системные ограничения, а также функции безопасности, ограничивающие действия пользователей.

Настройка функций безопасности выполняется в соответствии с документом РУСБ.10015-01 97 01-1 и для защищенной СУБД в соответствии с документом РУСБ.10015-01 97 01-3.

2.2.2. Усиленный уровень защищенности («Воронеж»)

После установки ОС мандатный контроль целостности (МКЦ) ОС и файловой системы включаются автоматически. При включенном режиме МКЦ администрирование и настройка ОС должны выполняться только администратором с высокой меткой целостности.

На данном уровне защищенности для разграничения доступа применяется механизм дискреционного управления доступом (в т.ч. в защищенной СУБД). По умолчанию выключены режим отладки `ptrace` и возможность использовать механизм `sudo` без ввода пароля.

Дополнительно для защиты информации могут использоваться доступные системные ограничения, а также функции безопасности, ограничивающие действия пользователей.

Также на данном уровне защищенности для защиты информации доступны механизмы очистки памяти (в т.ч. в защищенной СУБД) и организация замкнутой программной среды.

Настройка функций безопасности выполняется в соответствии с документом РУСБ.10015-01 97 01-1 и для защищенной СУБД в соответствии с документом РУСБ.10015-01 97 01-3.

2.2.3. Максимальный уровень защищенности («Смоленск»)

После установки ОС режим МКЦ ОС и файловой системы включаются автоматически. При включенном режиме МКЦ администрирование и настройка ОС должны выполняться только администратором с высокой меткой целостности.

На данном уровне защищенности для разграничения доступа по умолчанию применяются механизмы мандатного управления доступом и дискреционного управления доступом (в т.ч. в защищенной СУБД). После установки ОС требуется определить режим работы КСЗ и выполнить генерацию КСЗ в соответствии с РУСБ.10015-01 97 01-1.

По умолчанию выключены режим отладки `ptrace` и возможность использовать механизм `sudo` без ввода пароля.

Дополнительно для защиты информации могут использоваться доступные системные ограничения, а также функции безопасности, ограничивающие действия пользователей.

Также на данном уровне защищенности для защиты информации доступны механизмы очистки памяти (в т.ч. в защищенной СУБД) и организация замкнутой программной среды.

Настройка средств защиты информации и функций безопасности выполняется в соответствии с документом РУСБ.10015-01 97 01-1 и для защищенной СУБД в соответствии с документом РУСБ.10015-01 97 01-3.

2.3. Смена локали в ОС

По умолчанию в ОС устанавливается и используется кодировка UTF-8 (локали `ru_RU.UTF-8` и `en_US.UTF-8`).

Смена кодировки по умолчанию не рекомендуется, так как это может вызвать ошибку загрузки графической сессии и некорректное отображение шрифтов.

Если необходимо использовать другую локаль для корректного отображения символов в определенной программе, то следует запускать эту программу с указанием локали в переменной окружения LC_ALL:

```
env LC_ALL=ru_RU.CP1251 <путь_к_исполняемому_файлу>
```

2.4. Создание LiveCD

2.4.1. Общие сведения

LiveCD — это ОС, загружаемая со съемного носителя (DVD-диска, USB-носителя), не требующая для своего функционирования установки на жесткий диск, при этом пользователю доступен весь функционал ОС.

В состав ОС входит инструмент командной строки live-build-astra для создания образа LiveCD (далее Live-образа).

Для установки live-build-astra выполнить команду:

```
sudo apt install live-build-astra
```

2.4.2. Сборка Live-образа

Для сборки Live-образа может быть использована одна из следующих команд:

```
live-build-astra [параметры]
live-build-astra -d <кодовое_имя_ОС> [параметры]
```

Команда может быть выполнена только от имени администратора.

Инструмент live-build-astra создает каталог сборки с конфигурационным файлом, скопированным из системного каталога /etc/astra-live/, другими необходимыми файлами для сборки Live-образа и запускает сборку.

При выполнении команды сборки без параметров будет открыто окно с запросом использовать для собираемого образа кодовое имя дистрибутива, на котором запущена команда сборки. При нажатии кнопки **[Нет]** выполнение команды сборки будет завершено с ошибкой отсутствия задания дистрибутива (значения параметра -d). Для согласия использовать для сборки кодовое имя дистрибутива, на котором запущена команда сборки, нажать кнопку **[Да]**. Окно с запросом будет закрыто.

В каталоге выполнения команды будет создан каталог сборки по умолчанию `./build/`, в котором:

1) в корень каталога `./build/` будет скопирован системный конфигурационный файл `/etc/astra-live/config`;

2) в `./build/sources` будет скопирован системный файл с источниками по умолчанию `/usr/share/astra-live/sources/<кодовое_имя_ОС>.list`;

3) в `./build/packages` будет скопирован системный файл с пакетами по умолчанию `/usr/share/astra-live/packages/<кодовое_имя_ОС>.list.chroot`;

4) в корень каталога `./build/` будут скопированы другие необходимые для сборки файлы и каталоги.

В `./build/` будет начата сборка Live-образа:

1) с кодовым именем дистрибутива, на котором запущена команда сборки;

2) из источника установки по умолчанию (из файла `<каталог_сборки>/sources/<кодовое_имя_ОС>.list`);

3) с установкой пакетов по умолчанию (из файла `<каталог_сборки>/packages/<кодовое_имя_ОС>.list.chroot`).

Live-образ будет создан в корне каталога `./build/`.

При выполнении команды `live-build-astra` с параметрами соответствующие значения параметров будут переопределены в конфигурационном файле `<каталог_сборки>/config` и будут перезаписаны файлы `<каталог_сборки>/sources/<кодовое_имя_ОС>.list` и `<каталог_сборки>/packages/<кодовое_имя_ОС>.list.chroot`.

ВНИМАНИЕ! В качестве репозиториев допустимо указывать только репозитории ОС. При использовании сторонних репозиториев полученный в результате сборки набор пакетов может оказаться неработоспособным.

Live-образ будет создан в каталоге сборки, заданном с помощью параметра `-b`.

Параметры инструмента `live-build-astra` приведены в таблице 1.

Таблица 1

Параметр	Описание
`-nal`, `--no-autologin`	Отключить автоматический вход в систему на собираемом образе. В LiveCD для входа в систему будет применен пустой пароль
`-hn <имя_хоста>`, `--host-name <имя_хоста>`	Указать имя хоста системы на собираемом Live-образе

Продолжение таблицы 1

Параметр	Описание
`-un <имя_пользователя>`, `--user-name <имя_пользователя>`	Указать имя пользователя системы на собираемом Live-образе
`-b <каталог>`, `--build-dir <каталог>`	Указать путь к каталогу сборки. Если путь к каталогу сборки не был указан в команде, то в качестве каталога сборки будет использован `./build/`
`-c <тип>`, `--compression <тип>`	Указать тип сжатия SquashFS. Если тип сжатия не был указан в команде, то будет применен тип сжатия `zstd`. Доступные типы сжатия `gzip`, `lzo`, `lz4`, `xz` и `zstd` (см. `man mksquashfs`)
`-d <кодовое_имя>`, `--distribution <кодовое_имя>`	Указать кодовое имя дистрибутива ОС. Если параметр не задан, то будет предложено использовать кодовое имя дистрибутива, на котором запущена команда сборки
`-rs`, `--remove-sources`	Удалить все содержимое каталога сборки перед началом сборки
`-kc`, `--keep-cache`	Не удалять кэш `apt` из каталога сборки. Используется совместно с `--remove-sources`
`-ki`, `--keep-images`	Не удалять ранее собранные ISO-образы из каталога сборки. Используется совместно с `--remove-sources`
`-kl`, `--keep-log`	Не удалять журналы сборки из каталога сборки. Используется совместно с `--remove-sources`
`-r <источник>`, `--repository <источник>`	Указать путь к одному или нескольким источникам. В качестве источника может быть указан путь к файлу образа, путь к каталогу монтирования, путь к каталогу локального репозитория, URL-адрес сетевого репозитория. По умолчанию используются источники из системного файла `/usr/share/astra-live/sources/<кодовое_имя_ОС>.list`. **ВНИМАНИЕ!** Если должно быть указано несколько источников, то первым должен быть указан установочный источник. Значения должны быть разделены пробелами или запятыми. Также данный параметр можно указывать в одной команде несколько раз
`-u`	То же, что и `-r`, используется для совместимости. Не рекомендуется к использованию. Данный параметр устарел и будет удален в будущих обновлениях
`-ap <пакеты>`, `--add-packages <пакеты>`	Добавить указанные пакеты. Если должно быть указано несколько пакетов, то имена пакетов должны быть разделены пробелами или запятыми
`-apl <файл>`, `--add-packages-list <файл>`	Добавить все пакеты из указанного файла. В файле каждое имя пакета должно располагаться на отдельной строке
`-dp <пакеты>`, `--delete-packages <пакеты>`	Исключить из файла с пакетами по умолчанию `<каталог_сборки>/packages/` все указанные пакеты. Если должно быть указано несколько пакетов, то имена пакетов должны быть разделены пробелами или запятыми

Продолжение таблицы 1

Параметр	Описание
-dpl <файл>, --delete-packages-list <файл>	Исключить из файла с пакетами по умолчанию <каталог_сборки>/packages/ все пакеты, содержащиеся в указанном файле. В файле каждое имя пакета должно располагаться на отдельной строке
-rp <пакеты>, --replace-packages <пакеты>	Заменить все пакеты, содержащиеся в файле пакетами по умолчанию <каталог_сборки>/packages/ <кодовое_имя_ОС>.list.chroot, на указанные пакеты. **ВНИМАНИЕ!** Данный параметр не может быть использован в одной команде совместно с параметрами --replace-packages-list и --tasks. Если должно быть указано несколько аргументов данного параметра, то имена пакетов должны быть разделены пробелами или запятыми
-rpl <файл>, --replace-packages-list <файл>	Заменить все пакеты, содержащиеся в файле со списком пакетов по умолчанию <каталог_сборки>/packages/ <кодовое_имя_ОС>.list.chroot, на все пакеты из указанного файла. В указанном файле каждое имя пакета должно располагаться на отдельной строке **ВНИМАНИЕ!** Данный параметр не может быть использован в одной команде совместно с параметрами --replace-packages и --tasks
-t <задачи>, --tasks <задачи>	Заменить все пакеты, содержащиеся в файле со списком пакетов по умолчанию <каталог_сборки>/packages/ <кодовое_имя_ОС>.list.chroot, на пакеты из указанных задач tasksel. **ВНИМАНИЕ!** Данный параметр не может быть использован в одной команде совместно с параметрами --replace-packages и --replace-packages-list. Если должно быть указано несколько аргументов данного параметра, то имена задач должны быть разделены пробелами или запятыми
-i <имя>, --iso <имя>	Создать ISO-образ с указанным именем. Если имя не задано, то у созданного ISO-образа будет имя типа livecd-DD.MM.YY_HH.MM.iso. Если в команде не указан ни один параметр, задающий расширение и имя выходного файла (-i, -D, -q, -R, -T, -V или -w), то параметр -i выполняется по умолчанию и генерируется ISO-образ
-D <имя>, --docker <имя>	Создать TAR-архив с DOCKER-контейнером с указанным именем. Если имя не указано, то у созданного архива будет имя типа docker-DD.MM.YY_HH.MM.tar
-q <имя>, --qcow2 <имя>	Создать QCOW2-образ с указанным именем. Если имя не указано, то у созданного QCOW2-образа будет имя типа qcow2-DD.MM.YY_HH.MM.qcow2
-R <имя>, --raw <имя>	Создать RAW-образ с указанным именем. Если имя не указано, то у созданного RAW-образа будет имя типа raw-DD.MM.YY_HH.MM.img

Окончание таблицы 1

Параметр	Описание
`-T <имя>`, `--tar <имя>`	Создать TAR-архив с указанным именем. Если имя не указано, то у созданного TAR-архива будет имя типа `tarball-DD.MM.YY_HH.MM.tar`
`-w <имя>`, `--wsl <имя>`	Создать TAR-архив дистрибутива WSL с указанным именем. Если имя не указано, то у созданного архива будет имя типа `wsl-DD.MM.YY_HH.MM.tar`
`-h`, `--help`	Вывод справки
`-v`, `--version`	Вывод версии

Пример

Создание Live-образа `astra-live.iso` с кодовым именем `1.8_x86-64`в каталоге сборки по умолчанию `./build`. В качестве источника установки использовать установочный ISO-образ и применить сжатие `zstd` для файловой системы LiveCD. Все пакеты по умолчанию заменить пакетами из задач `Base` и `Fly` и удалить пакет `mc`, входящий в задачу `Base`:

```
live-build-astra -d 1.8_x86-64 -r ~/iso-images/installation.iso -i astra-live.iso -
    zstd -t Base Fly -dp mc
```

Более подробное описание инструмента приведено в `man live-build-astra`.

Описание изменения набора пакетов в создаваемой LiveCD приведено в 2.4.3.

Описание записи на носитель информации собранного Live-образа приведено в 2.4.4.

2.4.3. Изменение набора пакетов в создаваемой LiveCD

Для изменения перечня пакетов, устанавливаемых в создаваемой LiveCD, используются следующие параметры инструмента `live-build-astra`: `--replace-packages`, `--replace-packages-list`, `--tasks`, `--add-packages`, `--delete-packages`, `--add-packages-list`, `--delete-packages-list`. Описание параметров приведено в таблице 1.

Параметры позволяют изменять список устанавливаемых пакетов, а также перечень пакетов из задач `tasksel`. Инструмент `tasksel` — это встроенная в ОС система управления пакетами, оперирующая предопределенными наборами пакетов, которые называются задачами `tasksel`.

Для просмотра перечня доступных задач в ОС выполнить команду:

```
tasksel --list-tasks
```

Для задания значений параметра `--tasks` необходимо использовать имена из второго столбца вывода команды.

Подробное описание инструмента `tasksel` см. в `man tasksel`.

Параметры, изменяющие список устанавливаемых в LiveCD пакетов и перечень пакетов в задачах `tasksel`, имеют разный приоритет применения.

Приоритет применения параметров для изменения списка устанавливаемых в LiveCD пакетов (в порядке уменьшения приоритета):

1) `--replace-packages` либо `--replace-packages-list`;

2) `--tasks`;

3) `--add-packages`, `--delete-packages`, `--add-packages-list`, `--delete-packages-list`.

Пакеты, от которых зависит работоспособность ОС, не указываются в файле `/usr/share/astra-live/packages/<кодовое_имя_ОС>.list.chroot` и не могут быть удалены.

Примечание. При задании в соответствующих параметрах путей с помощью переменных окружения или регулярных выражений необходимо учитывать, что все действия выполняются от пользователя `root`.

Описание записи на носитель информации собранного Live-образа приведено в 2.4.4.

2.4.4. Запись Live-образа

Созданный Live-образ можно использовать для загрузки ОС как с DVD-диска, так и с USB-носителя. Для этого необходимо записать ISO-образ на DVD-диск или USB-носитель.

Запись ISO-образа на USB-накопитель необходимо выполнять с помощью графической утилиты `fly-admin-iso` (описание утилиты приведено в электронной справке) либо с использованием команды `dd`.

Пример

Запись ISO-образа `livecd.iso` на подключенный USB-носитель, представленный в системе файлом устройства `/dev/sdb`:

```
dd if=livecd.iso of=/dev/sdb bs=1M
```

ВНИМАНИЕ! Команда `dd` записывает новое содержимое, удаляя имеющиеся записи. Указание некорректных параметров может привести к потере данных или невозможности загрузки ОС.

2.5. Обновление ОС

2.5.1. Ручное обновление

Для ручной установки обновлений ОС используется инструмент командной строки `astra-update`.

Общий синтаксис команды:

```
sudo astra-update [действие] [параметр] [источник][[источник]..]
```

В качестве источника может быть указан ISO-файл образа или сетевой репозиторий. Может быть указано несколько источников, разделенных пробелом.

При ручной установке обновлений проверяется наличие достаточного свободного пространства в корневом разделе диска. Если объем свободного пространства меньше 4 ГБ, то установка не будет выполнена.

При запуске команды может быть выбрано только одно действие. Список основных действий `astra-update` приведен в таблице 2.

Таблица 2

Действие	Описание
`-c`	Проверить, можно ли устанавливать обновление. Изменения в систему не вносятся. Является действием по умолчанию — выполняется, если в команде действие не указано
`-a`	Установить обновление автоматически в интерактивном режиме (с выводом запросов пользователю), выполняя автоматическое выключение и включение функций безопасности. Представляет собой последовательное выполнение действий `-d`, `-i` и `-e`
`-A`	Установить обновление полностью автоматически (без вывода сообщений и запросов пользователю), выполняя автоматическое выключение и включение функций безопасности. Представляет собой последовательное выполнение действий `-d`, `-I` и `-e`. Данный режим предназначен для массовой автоматической установки обновлений на удаленных компьютерах, в том числе для использования в сценариях ansible. Устройства чтения оптических дисков, добавленные с помощью команды `sudo apt-cdrom add`, не будут использованы в процессе неинтерактивной установки, т. к. могут потребовать действий пользователя
`-d`	Выключить функции безопасности, мешающие обновлению. Состояние функций безопасности при этом будет сохранено в файле `/etc/parsec/update-saveconf`
`-I`	Установить обновление в неинтерактивном режиме (без вывода сообщений и запросов пользователю) и не выполняя выключение и включение функций безопасности

Окончание таблицы 2

Действие	Описание
`-i`	Установить обновление в интерактивном режиме (с выводом запросов пользователю) и не выполняя выключение и включение функций безопасности
`-e`	Включить функции безопасности, которые были выключены перед обновлением действием `-d`. Состояние функций безопасности будет восстановлено из файла `/etc/parsec/update-saveconf`. Если файл не существует, то никакие изменения в систему внесены не будут
`-p <пакеты>`	Обновить инструменты обновления и пакеты, указанные в `<пакеты>`
`-bp`	Проверить возможность создания снимка состояния системы перед установкой обновления
`-bc`	Создать снимок состояния системы перед установкой обновления (доступно при использовании LVM)
`-be`	Проверка наличия выполненного снимка состояния системы
`-br`	Восстановить состояние системы из выполненного снимка
`-bd`	Удалить выполненный снимок состояния системы

Список параметров `astra-update` приведен в таблице 3.

Таблица 3

Параметр	Описание
`-k`	Сохранить источники для последующего использования (ISO-файлы образов будут скопированы на диск и указаны в `/etc/fstab`, сетевые репозитории будут добавлены в файл `/etc/apt/sources.list`)
`-K`	Установить последнее доступное ядро. Может использоваться только с действиями `-a`, `-A`, `-i` и `-I`
`-g`	Проверить контрольную сумму ISO-файла образа по алгоритму ГОСТ (файл с контрольной суммой должен располагаться в одном каталоге с образом)
`-m`	Проверить контрольную сумму ISO-файла образа по алгоритму MD5 (файл с контрольной суммой должен располагаться в одном каталоге с образом)
`-r`	Установка обновления из репозиториев, перечисленных в файле `/etc/apt/sources.list` (без внесения изменений в сам файл)
`-n`	Только имитировать установку обновления, без внесения изменений в систему
`-T`	Не искать репозиторий установочного диска, репозиторием обновления является технологический диск
`-o APT::Status-Fd=<1/2>`	Направлять сообщения о статусе обновления в файловый дескриптор 1 или 2

Окончание таблицы 3

Параметр	Описание
`-S`	Не проверять наличие 4 ГБ свободного места перед обновлением
`-N`	Не проверять доступность указанных в `/etc/apt/sources.list` сетевых репозиториев в процессе обновления. Позволяет успешно выполнить обновление при отсутствии сетевого подключения и наличии предварительно загруженных пакетов

ВНИМАНИЕ! При выполнении команды `astra-update` установочный диск всегда должен быть указан в `/etc/apt/sources.list` или указан в качестве источника при выполнении команды. Для указания технологического диска вместо установочного следует использовать параметр `-T`.

Информация по использованию инструмента `astra-update` доступна в терминале, для этого выполнить команду:

```
man astra-update
```

Для установки обновлений также может использоваться графическая утилита `fly-astra-update` («Установка обновлений»). Описание утилиты приведено в электронной справке.

2.5.2. Автоматическое обновление

Автоматическая проверка наличия обновлений ОС и установленного ПО в подключенных репозиториях, скачивание и установка данных обновлений осуществляются службой `astra-update-service`. Отображение уведомлений и подтверждение запуска процесса обновления осуществляется с помощью графической утилиты `fly-update-notifier` («Проверка обновлений»). Описание утилиты приведено в электронной справке.

Для включения автоматического обновления необходимо:

1) установить службу обновления и графическую утилиту отображения уведомлений:

```
sudo apt install astra-update-service fly-update-notifier
```

2) запустить службу обновления и добавить ее в автозапуск:

```
sudo astra-update-ctl enable
```

3) запустить графическую утилиту `fly-update-notifier`:

```
fly-update-notifier &
```

Утилита запустится в фоновом режиме и добавится в автозапуск. Проверка обновлений будет производиться в фоне.

По умолчанию наличие обновлений будет проверяться каждый час. При обнаружении обновлений будет показано уведомление с предложениями обновить систему при перезагрузке или отложить обновление. После подтверждения обновления необходимые пакеты будут скачаны в течение 240 минут (четырех часов). Обновление системы будет выполнено после перезагрузки. Если закрыть уведомление, не выбрав ни один из вариантов, то скачивание и установка обновлений будут выполнены принудительно в автоматическом режиме по истечении одной недели. Данные значения возможно изменить в конфигурационном файле службы.

Для управления службой `astra-update-service` используется инструмент `astra-update-ctl`. Пакет `astra-update-ctl` устанавливается автоматически вместе с пакетом `astra-update-service`.

Синтаксис команды:

```
astra-update-ctl [параметр]
```

Список параметров приведен в таблице 4.

Таблица 4

Параметр	Описание
`status`	Отобразить статус службы
`enable`	Запустить службу и добавить ее в автозапуск
`disable`	Остановить службу и убрать ее из автозапуска
`edit`	Открыть в консоли конфигурационный файл для редактирования
`parameters`	Вывести список доступных настроек конфигурационного файла
`set <статус>`	Принудительно установить один из возможных статусов: 1) `no-updates` — обновления отсутствуют; 2) `ready` — служба готова; 3) `activated` — служба запущена; 4) `stopped` — служба остановлена; 5) `force` — принудительная установка обновлений

Если доступно очередное обновление ОС, то будет установлен статус `stopped-for-major` и показано уведомление о возможности установки очередного обновления ОС. Результаты работы службы заносятся в журнал `/var/log/astra-update-service/service.log`.

Настройки службы хранятся в конфигурационном файле `/etc/astra-update-service/astra-update-daemon.conf`. Конфигурационный файл службы возможно изменить в текстовом редакторе, например выполнив команду:

```
sudo nano /etc/astra-update-service/astra-update-daemon.conf
```

Также конфигурационный файл возможно открыть для редактирования, выполнив команду:

```
sudo astra-update-ctl edit
```

После выполнения команды будет открыт редактор Vim. Для изменения содержимого файла необходимо перейти в режим редактирования, нажав клавишу **<i>**. После внесения нужных изменений следует вернуться в командный режим, нажав клавишу **<Esc>**. Для выхода с сохранением изменений ввести `:wq` и нажать клавишу **<Enter>**. Для выхода без сохранения изменений ввести `:q` и нажать клавишу **<Enter>**.

Список параметров конфигурационного файла приведен в таблице 5.

Таблица 5

Настройка	Описание
`T_check`	Интервал между проверками обновлений (в минутах), значение по умолчанию `60`
`T_download_min`	Минимальная задержка перед скачиванием обновлений (в минутах), значение по умолчанию `0`
`T_download_max`	Максимальная задержка перед скачиванием обновлений (в минутах), значение по умолчанию `240`
`T_delay`	Задержка перед принудительным переводом системы в режим обновления (в днях), значение по умолчанию `7`
`T_retry`	Задержка перед повторной попыткой перевода системы в режим обновления (в часах), значение по умолчанию `4`
`Action_on_error`	Действие после ошибки обновления. Возможные значения: 1) `Reset` — сбросить изменения; 2) `Stop` — остановить процесс обновления; 3) `Retry` — повторить попытку обновления

Окончание таблицы 5

Настройка	Описание
`Always_new_update`	Удаление скачанных обновлений перед скачиванием новых. Возможные значения: 1) `false` — не удалять скачанные обновления (значение по умолчанию); 2) `true` — удалять скачанные обновления
`Host_to_ping`	Адрес, опрашиваемый для проверки наличия интернет-соединения
`Free_space_policy`	Проверка наличия достаточного свободного пространства в корневом разделе для выполнения обновления. Если проверка не пройдена, то обновление не будет установлено. Возможные значения: 1) `0` — проверка наличия 4 ГБ свободного пространства (значение по умолчанию); 2) `1` — проверка наличия свободного пространства, рассчитанного исходя из размера устанавливаемых пакетов; 3) `2` — проверка наличия свободного пространства не выполняется
`Use_sources_list_d`	Проверка наличия обновлений в репозиториях, указанных в файлах в `/etc/apt/sources.list.d/`. Данная настройка позволяет использовать службу `astra-update-service` для обновления стороннего ПО, установленного в системе. Возможные значения: 1) `0` — используются только репозитории, указанные в `/etc/apt/sources.list` (обновления ОС, значение по умолчанию); 2) `1` — используются репозитории, указанные в `/etc/apt/sources.list` и репозитории, указанные в файлах в `/etc/apt/sources.list.d/` (обновления стороннего ПО). **ВНИМАНИЕ!** Данный параметр игнорируется, если в конфигурационном файле указан параметр `Extra_repos_policy` с любым из возможных значений
`Extra_repos_policy`	Проверка наличия обновлений в дополнительных репозиториях, указанных в значении параметра `Extra_repos`. Возможные значения: 1) `0` — используются только дополнительные репозитории без репозиториев, указанных в `/etc/apt/sources.list` (значение по умолчанию, если параметр указан без значения); 2) `1` — используются дополнительные репозитории и репозитории, указанные в `/etc/apt/sources.list`. **ВНИМАНИЕ!** При использовании данного параметра игнорируется значение параметра `Use_sources_list_d`. Чтобы дополнительно использовать репозитории из `/etc/apt/sources.list.d/`, нужно указать пути к их файлам в значении параметра `Extra_repos`
`Extra_repos`	Список путей к файлам с дополнительными репозиториями. Список указывается в виде строки в кавычках, пути в строке разделяются запятыми

Пример

Параметры кофигурационного файла службы, устанавливающие периодичность проверки обновлений каждые 15 минут, максимальную задержку перед их скачиванием 10 минут и задержку перед принудительным обновлением 2 дня:

```
T_check=15
T_download_max=10
T_delay=2
```

2.5.3. Пользовательские сценарии

В процессе обновления возможно выполнение пользовательских сценариев, например для проведения дополнительных проверок перед обновлением ОС или для обновления стороннего ПО, установленного вручную.

Процесс обновления ОС архитектурно поделен на следующие стадии:

1) блок проверок перед переводом ОС в режим обновления;
2) блок проверок перед обновлением ОС;
3) обновление ОС;
4) откат обновления (при наличии выполненного снимка состояния ОС).

На каждой из перечисленных стадий может выполняться одно или несколько действий, задаваемых пользовательским сценарием. Каждое действие может выполняться перед началом стадии или после ее окончания.

Пользовательские сценарии размещаются в каталоге `/usr/share/astra-update-service/scripts/`. Порядок запуска сценариев определяется алфавитным порядком имен их файлов.

Каждый сценарий должен иметь возможность запуска с параметром `config` для вывода основной информации о сценарии.

Результатом запуска сценария с указанным параметром должен быть вывод в `stdout` следующей основной информации о сценарии:

1) уникальный строковый идентификатор сценария;
2) список уникальных идентификаторов стадий обновления, на которых должен запускаться сценарий, перечисляемых через запятую:
   а) `ready` — стадия проверок перед переводом ОС в режим обновления;
   б) `activated` — стадия проверок перед обновлением ОС;
   в) `upgrade` — стадия обновления ОС;
   г) `rollback` — стадия отката обновления;

Если для сценария не задано ни одного идентификатора стадии или стадии с заданными идентификаторами не существуют, то сценарий не будет выполнен;

3) порядок выполнения на стадии:
   а) `pre` — перед выполнением стадии;
   б) `post` — после выполнения стадии.

Формат вывода конфигурации:

```
id: <уникальный_ID_сценария/плагина>
stage: <уникальный_ID_стадии_обновления>,...
substage: pre
```

Если в выводе отсутствует любой из вышеперечисленных параметров или какой-то из них некорректен, то сценарий не будет запущен.

Пример

Запуск сценария `verification_script`:

```
verification_script config
```

Вывод команды:

```
id: Condition verification script
stage: activated
substage: post
```

При запуске без параметров сценарий должен выполнять свой основной код. В процессе выполнения сценария может выводиться в `stdout` следующая информация:

1) произвольное сообщение, регистрируемое в системном журнале;
2) предупреждения;
3) ошибки.

Сценарий может иметь код возврата. Если он ненулевой, то считается, что действие из сценария вернуло ошибку.

Результаты выполнения сценария должны выводиться в следующем формате:

```
message: <произвольное сообщение>
warning: <предупреждение>
error: <ошибка>
```

Если вывод сценария пуст или не соответствует данному формату ни в одной выведенной строке, но код возврата при этом равен нулю, то действие считается полностью успешно выполненным.

Также в сценарий может быть передана информация о результатах выполнения предыдущей стадии обновления ОС. Данная возможность предусматривается для обработки возврата на предыдущие стадии. Для получения данной информации сценарий должен иметь возможность запуска с параметром `prev <идентификатор_стадии>`. Требования к выводу сценария при запуске с данными параметрами такие же, как при его запуске без параметров.

2.6. Установка и обновление ОС в режиме «Мобильный»

2.6.1. Подготовка к установке

Установка ОС в режиме «Мобильный» может быть выполнена на совместимое устройство (см. РУСБ.10015-01 31 01 «Операционная система специального назначения «Astra Linux Special Edition». Описание применения») со следующими характеристиками:

1) процессорная архитектура — x86-64 (AMD, Intel) с BIOS/UEFI;
2) оперативная память — не менее 1 ГБ;
3) внутренняя память — не менее 32 ГБ;
4) USB-порт.

Установка ОС на устройство выполняется с помощью установочного USB-носителя.

Для подготовки установочного USB-носителя требуется:

1) USB-носитель емкостью не менее 16 ГБ;
2) образ ОС для режима «Мобильный»;
3) инструментальный компьютер с установленной ОС или другой операционной системой семейства Linux.

Подготовка установочного USB-носителя:

1) загрузить инструментальный компьютер и войти в систему под учетной записью администратора;
2) в терминале выполнить команду:

```
sudo -s
```

3) записать на USB-носитель образ ОС, выполнив команду:

```
dd if=<путь_к_образу_ОС> of=/dev/<имя_устройства> bs=1M status=progress
```

где <имя_устройства> — имя USB-носителя в системе (данное имя будет отображаться в выводе команды dmesg после подключения USB-носителя, например sda).

После завершения процесса копирования установочный USB-носитель готов к использованию.

2.6.2. Установка

2.6.2.1. Настройка BIOS/UEFI

Перед установкой ОС в режиме «Мобильный» на устройство требуется настроить BIOS/UEFI устройства:

1) подключить установочный USB-носитель к устройству;
2) подключить внешнюю клавиатуру к устройству;
3) перезагрузить устройство и в процессе загрузки войти в меню настройки BIOS/UEFI, нажав соответствующую клавишу (на некоторых устройствах комбинация клавиш **<Fn+F2>**);
4) в меню настройки BIOS/UEFI установить корректную дату и время;
5) установить пароль на вход в BIOS/UEFI;
6) проверить настройку параметра Secure Boot — должен быть отключен («Disabled»);
7) сохранить изменения и перейти в следующее меню (на некоторых устройствах нажатием комбинации клавиш **<Fn+F10>**);
8) в меню настройки BIOS/UEFI выбрать вариант загрузки с USB-носителя и затем, в зависимости от модели устройства, нажать клавишу **<Enter>** или сохранить настройки и выйти из меню. На устройстве будет загружена ОС с установочного USB-носителя. По окончании загрузки будет отображено графическое меню установки ОС.

Доступны следующие способы установки ОС в режиме «Мобильный»:

1) графическая установка в соответствии с 2.6.2.2;
2) консольная установка в соответствии с 2.6.2.3.

2.6.2.2. Графическая установка

Для установки ОС в режиме «Мобильный» с использованием графического установщика необходимо:

1) в графическом меню установки ОС выбрать «Install» и нажать клавишу **<Enter>**;

2) выбрать устройство внутренней памяти, на которое будет установлена ОС, и нажать клавишу **<Enter>**;

3) выбрать модель устройства и нажать клавишу **<Enter>**. Начнется копирование файлов ОС во внутреннюю память устройства. По окончании копирования файлов отобразится соответствующее сообщение;

4) для завершения установки и выключения устройства нажать клавишу **<Enter>**.

Далее требуется отсоединить установочный USB-носитель, включить устройство и выполнить первоначальную настройку ОС в соответствии с 2.6.3.

2.6.2.3. Консольная установка

Для установки ОС в режиме «Мобильный» с использованием консольного установщика необходимо:

1) в графическом меню установки ОС выбрать «Exit» и нажать **<Enter>** — будет отображена командная строка и выполнен автоматический вход в систему с учетной записью суперпользователя `root`;

2) для установки ОС выполнить команду копирования:

```
/opt/astra-mobile-install -d /dev/<имя_устройства>
```

где `<имя_устройства>` — имя устройства внутренней памяти, на которое будет установлена ОС. Вывести список устройств внутренней памяти можно командой:

```
fdisk -l
```

Имя устройства отображается в строке `Диск /dev/...`

Пример

```
Диск /dev/mmcblk1
```

3) в ходе копирования файлов ОС во внутреннюю память устройства на запросы системы о выполнении разметки памяти или удалении имеющейся информации ответить `Y`;

4) выполнить в терминале команду перезагрузки устройства:

```
reboot
```

5) в момент перезагрузки устройства отсоединить установочный USB-носитель.

После перезагрузки устройства при первом запуске ОС требуется выполнить первоначальную настройку в соответствии с 2.6.3.

2.6.3. Настройка установленной ОС

2.6.3.1. Начальная настройка ОС

При установке ОС в режиме «Мобильный» на устройство автоматически создается учетная запись администратора `administrator`. При первом входе в систему будет отображено окно для установки пароля администратора.

При первом входе в систему необходимо:

1) ознакомиться с лицензионным соглашением, доступным по QR-коду, установить флаг **Я принимаю условия лицензионного соглашения** и нажать **[Начать]**;

2) задать пароль системного администратора и нажать **[>]**;

3) опционально включить Wi-Fi и подключиться к доступной беспроводной сети, затем нажать **[>]**;

4) настроить системную дату и время, затем нажать **[>]**;

5) в зависимости от приобретенной лицензии выбрать уровень защищенности системы и функции безопасности, доступные на данном уровне, затем нажать **[>]**;

6) опционально включить защитное преобразование пользовательских данных, задать пароль для доступа к данным, затем нажать **[>]**. Заданный пароль будет необходимо вводить при каждой загрузке системы;

7) опционально включить использование файла подкачки, затем нажать **[>]**;

8) нажать **[Сохранить]** и подтвердить сохранение настроек в отобразившемся диалоговом окне. После перезагрузки устройства выполнить вход в систему (см. электронную справку).

После установки ОС отображение меню загрузчика GRUB (и вход в него) по умолчанию заблокировано. Если будет разблокировано отображение меню загрузчика, то необходимо установить пароль на вход в меню загрузчика и на использование режима командной строки загрузчика (описание приведено на страницах руководства `info grub`).

Установленная на устройство ОС в режиме «Мобильный» предоставляет графический интерфейс ОС и набор программ, адаптированных для использования на устройствах с сенсорным экраном.

Описание графического интерфейса в режиме «Мобильный» приведено в электронной справке, для просмотра справки необходимо:

1) на экране приложений перейти в раздел «Десктопные» и запустить приложение «Помощь»;

2) в электронной справке перейти **Документация — Графический интерфейс — Режим «Мобильный»**.

Для использования в режиме «Мобильный» некоторых программ из состава ОС, в том числе не адаптированных для работы на устройствах с сенсорным экраном, может потребоваться установка соответствующих пакетов из репозитория ОС.

2.6.3.2. Настройка виртуальной клавиатуры

Для приложений в режиме «Мобильный» по умолчанию используется виртуальная клавиатура из состава рабочего стола KDE Plasma. При этом могут возникать ошибки в работе виртуальной клавиатуры с приложениями X11, функционирующими через Xwayland.

Если возникают ошибки в работе клавиатуры по умолчанию с тем или иным приложением, то можно использовать с данным приложением виртуальную клавиатуру `fly-vkbd`. Для использования клавиатуры `fly-vkbd` с определенным приложением требуется в файле `/etc/xdg/plasmamobilerc` в секции `[FlyVkbd]` для параметра `Applications` добавить название desktop-файла приложения.

Пример

```
[FlyVkbd]
Applications=chromium,yandex-browser
```

2.6.4. Обновление ОС

Обновление ОС в режиме «Мобильный» выполняется одним из следующих способов:

1) с загрузочного USB-носителя в соответствии с 2.6.4.1;
2) из источников (образов ISO и сетевых репозиториев) в соответствии с 2.6.4.2. Для указания источников рекомендуется использовать файл `/etc/apt/sources.list`.

ВНИМАНИЕ! При обновлении с загрузочного USB-носителя будут сохранены только каталоги `/opt` и `/home`, а остальные данные будут удалены. Настройки системы будут установлены по умолчанию, в том числе будет установлен уровень защищенности «Воронеж».

2.6.4.1. Обновление ОС с USB-носителя

Обновление ОС с загрузочного USB-носителя выполняется путем копирования на внутреннюю память устройства файлов с USB-носителя, при этом существующие на устройстве каталоги `/opt` и `/home` будут сохранены. Остальные данные будут удалены. Настройки системы будут установлены по умолчанию, в том числе будет установлен уровень защищенности «Воронеж».

Для обновления ОС с загрузочного USB-носителя требуется:

1) подготовить USB-носитель в соответствии с 2.6.1;

2) загрузиться с USB-носителя в соответствии с 2.6.2.1;

3) в графическом меню установки ОС выбрать «Exit» и нажать **<Enter>**. Будет отображена командная строка и выполнен автоматический вход в систему под учетной записью `root`;

4) для начала обновления ОС выполнить команду копирования:

```
/opt/astra-mobile-install -u -d /dev/<имя_устройства>
```

где `<имя_устройства>` — имя устройства внутренней памяти, на котором будет установлена ОС. Вывести список устройств внутренней памяти можно командой:

```
fdisk -l
```

Имя устройства отображается в строке `Диск /dev/...`.

Пример

```
Диск /dev/mmcblk1
```

5) в ходе копирования файлов ОС во внутреннюю память устройства на запросы системы о выполнении разметки памяти или удалении имеющейся информации ответить `Y`;

6) выполнить в терминале команду перезагрузки устройства:

```
reboot
```

7) в момент перезагрузки устройства отсоединить установочный USB-носитель.

После обновления ОС необходимо выполнить ее настройку в соответствии с 2.6.3.

2.6.4.2. Обновление ОС из источников

При обновлении ОС из источников выполняется обновление из сетевых репозиториев или из образов ISO, указанных в файле `/etc/apt/sources.list`.

Обновление может быть выполнено:

1) с помощью инструмента командной строки `astra-update`, описание инструмента приведено в `man astra-update`;

2) в графическом интерфейсе, порядок обновления приведен в электронной справке («Документация — Графический интерфейс — Режим «Мобильный»).

3. СИСТЕМНЫЕ КОМПОНЕНТЫ

3.1. Управление устройствами

3.1.1. Типы устройств

В ОС существует два типа устройств:

1) блочные устройства с произвольным доступом — данные, записанные в такие устройства, могут быть прочитаны (например, жесткие диски);

2) символьные устройства с последовательным или произвольным доступом — данные, записанные в такие устройства, не могут быть прочитаны (например, последовательные порты).

Каждое поддерживаемое устройство представляется в ФС файлом устройства. При выполнении операций чтения или записи с файлом устройства происходит обмен данными с устройством, на которое указывает этот файл. Данный способ доступа к устройствам позволяет не использовать специальные программы (а также специальные методы программирования, такие как работа с прерываниями).

Файлы устройств располагаются в каталоге `/dev`, для вывода списка файлов выполнить команду `ls`. При выполнении команды с параметром `-l` на экран монитора будет выведен список файлов с указанием в первой колонке типа файла и прав доступа к нему. Первый символ в первой колонке указывает на тип файла:

- `c` — символьное устройство;
- `b` — блочное устройство;
- `d` — каталог;
- `l` — символическая ссылка;
- «`-`» (дефис) — обычный файл.

Пример

Просмотр информации о файле, соответствующем звуковому устройству

```
ls -l /dev/dsp
```

Вывод команды:

```
crw-rw---- 1 root audio 14, 3 июл 1 13:05 /dev/dsp
```

Описание команды `ls` приведено в `man ls`.

Наличие файла устройства не означает, что данное устройство установлено в системе. Например, наличие файла `/dev/sda` не означает, что на компьютере установлен жесткий диск SCSI. Это предусмотрено для облегчения установки программ и нового оборудования, т. к. исключает необходимость поиска нужных параметров и создания файлов для новых устройств.

3.1.2. Жесткие диски

При администрировании дисков могут возникнуть задачи по разделению жесткого диска на разделы, созданию и монтированию ФС, форматированию диска и др.

Разделение жесткого диска может использоваться для хранения разных операционных систем на одном жестком диске, для хранения пользовательских и системных файлов в разных дисковых разделах. Разделение жесткого диска упрощает резервное копирование и восстановление, а также повышает защищенность системных файлов от повреждений.

Для использования диска или раздела необходимо создать на нем ФС.

Для штатного доступа к данным, находящимся в ФС, необходимо выполнить монтирование ФС. Монтирование выполняется с целью формирования единой структуры каталогов, обеспечения буферизации дисков и работы с виртуальной памятью.

Монтирование может выполняться как автоматически, так и вручную. Монтируемые вручную ФС должны быть размонтированы также вручную.

Центральный процессор и жесткий диск обмениваются информацией через дисковый контроллер. Это упрощает схему обращения и работы с диском, т. к. контроллеры для разных типов дисков могут быть построены с использованием единого интерфейса для связи с компьютером.

Каждый жесткий диск представлен отдельным файлом устройства в каталоге `/dev`:

- `/dev/hda` и `/dev/hdb` — для первого и второго диска, подключенного по IDE шине;
- `/dev/sda`, `/dev/sdb` и т. д. — для дисков, использующих SCSI или SATA-интерфейс.

3.1.3. Разделы жесткого диска

Весь жесткий диск может быть разделен на несколько дисковых разделов, при этом каждый раздел в системе представлен как отдельный диск. Разделение используется, например, при работе с двумя операционными системами на одном жестком диске. При этом каждая операционная система использует для работы отдельный дисковый раздел и не взаимодействует с другими. Таким образом, две различные системы могут быть установлены на одном жестком диске.

3.1.3.1. Разбиение жесткого диска

Главная загрузочная запись MBR (Master Boot Record) диска содержит место для четырех основных (первичных) разделов, пронумерованных от 1 до 4.

Если необходимо добавить еще разделы на диск, то следует преобразовать основной раздел в расширенный (extended). Далее расширенный раздел разделяется на один или несколько логических разделов с номерами от 5 до 15. Логические разделы функционируют так же, как и основные, различие состоит в схеме их создания.

При установке ОС разбиение жесткого диска (дисков) осуществляется средствами программы-установщика. При работе с ОС для разбиения жесткого диска на разделы используется инструмент командной строки `fdisk`.

Каждый раздел должен содержать четное количество секторов, т. к. в ОС используются блоки размером в 1 КБ, т. е. два сектора. Нечетное количество секторов приведет к тому, что последний из них будет не использован. Это ни на что не влияет, но при запуске `fdisk` будет выдано предупреждение.

При изменении размера раздела рекомендуется сначала сделать резервную копию раздела, затем удалить раздел, создать новый раздел и восстановить сохраненную информацию в новом разделе.

Описание инструмента `fdisk` приведено в `man fdisk`.

3.1.3.2. Файлы устройств и разделы

Каждому первичному и расширенному разделу соответствует отдельный файл устройства. Существует соглашение для имен подобных файлов, которое заключается в добавлении номера раздела к имени соответствующего файла устройства. Разделы с 1 по 4 являются первичными либо один из этих разделов является расширенным. Разделы с 5 по 15 являются логическими, на которые разбивается расширенный раздел. Например, `/dev/hda1` соответствует первому первичному разделу первого IDE-диска, а `/dev/sdb7` — третьему логическому разделу второго диска с интерфейсом SCSI или SATA.

3.1.4. Форматирование

Форматирование — это процесс записи специальных отметок на магнитную поверхность, которые используются для разделения дорожек и секторов. Новый диск не может использоваться без предварительного форматирования. Для IDE- и некоторых SCSI-дисков форматирование выполняется при их изготовлении и обычно не требуется повторение этой процедуры.

3.1.5. Программная организация дисковых разделов в RAID и тома LVM

В ядро ОС встроена программная реализация технологии RAID (уровни RAID 0, RAID 1, RAID 5 и их сочетания). Команда `mdadm` предоставляет административный интерфейс для создания и управления массивами RAID.

После создания массива RAID его устройство, например `/dev/md0`, используется также, как и `/dev/hda1` или `/dev/sdb7`.

Том LVM, с точки зрения ядра системы, использует унифицированные механизмы VFS и не нуждается в специальных конфигурациях ядра. В ОС обеспечивается полнофункциональное управление томами LVM, которое осуществляется стеком команд управления.

LVM обеспечивает более высокий уровень абстракции, чем традиционные диски и разделы Linux. Это позволяет добиться большей гибкости при выделении пространства для хранения данных. Логические тома можно перемещать с одного физического устройства на другое, а их размер изменять. Физические устройства можно добавлять и удалять. Томам, управляемым посредством LVM, можно назначать любые текстовые названия, например `database` или `home`, а не служебные `sda` или `hda`.

3.1.6. Разделы диска в режиме «Мобильный»

При установке ОС в режиме «Мобильный» разметка памяти устройства выполняется автоматически, при этом применяется таблица разделов GUID (GPT).

После установки ОС в режиме «Мобильный» на устройстве доступны следующие разделы:

1) `/boot/efi` — загрузочная область EFI. Размер раздела 100 МБ, тип ФС VFAT;

2) `/boot` — содержит необходимую информацию для загрузки системы: ядро, образ `initrd`, файлы загрузчика. Размер раздела 500 МБ, тип ФС ext4;

3) `recovery` — размещение образа для восстановления ОС, который используется при сбросе настроек ОС на значения по умолчанию. Размер раздела 8 ГБ, тип ФС ext4;

4) том LVM с разделами:

   а) корневой каталог (обозначается символом «/» — содержит файлы системы, точки монтирования ФС и др. Размер раздела 15 ГБ, тип ФС ext4;

   б) `/opt` — каталог для установки дополнительного ПО (например, текстовые и графические редакторы, средства антивирусной защиты, специальное программное обеспечение и т. п.). Каталоги дополнительного ПО должны иметь имя вида `/opt/<имя_вендора>/<название_ПО>`. Ярлыки дополнительного ПО должны быть установлены в `/opt/astra-mobile/menu`. При обновлении ОС каталог `/opt` не изменяется, соответственно, не требуется переустановка дополнительного ПО. Размер раздела 5 ГБ, тип ФС ext4;

в) /home — рабочие (домашние) каталоги пользователей, в т.ч. для размещения пользовательских данных приложений. При обновлении ОС каталог /home не изменяется, соответственно, пользовательские данные приложений будут сохранены. Размер раздела не менее 10 ГБ (при возможности расширяется после загрузки), тип ФС ext4.

3.2. Управление ФС

3.2.1. Общие сведения

Файловая система — это методы и структуры данных, которые используются ОС для хранения файлов на диске или его разделе.

Перед тем, как раздел или диск могут быть использованы для хранения информации (файлов), он должен быть инициализирован, а требуемые данные перенесены на этот диск. Этот процесс называется созданием ФС.

В ОС рекомендована к применению и используется по умолчанию ФС типа ext4, обеспечивающая поддержку длинных имен, символических связей, хранение мандатных атрибутов, возможность представления имен файлов русскими буквами. Дополнительно могут использоваться ФС ISO9660, FAT (MS-DOS), NTFS и др.

Все данные ОС состоят из множества файлов (программы, библиотеки, каталоги, системные и пользовательские файлы) и располагаются в ФС. Структура ФС имеет вид «перевернутого дерева», вершину которого называют корневым каталогом, в системе обозначается символом «/».

В зависимости от параметров, заданных в процессе установки ОС, каталоги могут относиться к различным ФС.

После установки ОС файловая система может состоять, например, из следующих каталогов:

- /bin (/usr/bin) — содержит исполняемые файлы, необходимые для работы системы. Многие команды ОС являются программами из этого каталога;
- /boot — содержит необходимую информацию для загрузки системы: ядро (ядра), образ initrd, файлы загрузчика;
- /dev — содержит файлы устройств (device files). С их помощью осуществляется доступ к физическим устройствам, установленным в системе;
- /root — рабочий (домашний) каталог суперпользователя;
- /tmp — используется для хранения временных файлов, создаваемых программами в процессе своей работы. При работе с программами, создающими много больших временных файлов, рекомендуется иметь отдельную ФС;

- /etc — содержит конфигурационные файлы ОС, в т. ч. файл паролей passwd и список ФС fstab, монтируемых при начальной загрузке. В этом же каталоге хранятся сценарии загрузки (startup scripts), список узлов (hosts) с их IP-адресами и другие данные о конфигурации;

- /lib (/usr/lib) — содержит разделяемые библиотеки, используемые программами во время своей работы. Применяя разделяемые библиотеки, хранящиеся в общедоступном месте, можно уменьшить размер программ за счет повторного использования одного и того же кода;

- /proc — является псевдофайловой системой и используется для чтения из памяти информации о системе;

- /sbin (/usr/sbin) — содержит исполняемые файлы, используется для системного администрирования и требующие для запуска права суперпользователя);

- /usr — содержит программы и данные, не подлежащие изменению. Каталог /usr и его подкаталоги необходимы для функционирования ОС, т. к. содержат наиболее важные программы. Данный каталог почти всегда является отдельной ФС;

- /var — содержит изменяемые файлы, например log-файлы и др.;

- /home — содержит рабочие (домашние) каталоги пользователей. Рекомендуется создавать в качестве отдельной ФС, чтобы обеспечить пользователям достаточное пространство для размещения своих файлов. Если пользователей в системе много, возможно разделить этот каталог на несколько ФС. Например, можно создать подкаталоги /home/staff и /home/admin соответственно для персонала и администраторов, установить каждый подкаталог как отдельную ФС и уже в них создавать рабочие каталоги пользователей.
В рабочих каталогах пользователей также содержатся некоторые конфигурационные файлы, которые являются скрытыми и изменяются редко. Файл становится скрытым, если поставить точку в начале имени файла. При выводе списка файлов командой ls для отображения в том числе скрытых файлов использовать параметр -a:

```
ls -a
```

Для обеспечения совместной работы пользователей в ОС создаются автоматически при установке совместно используемые каталоги, доступ к которым разрешен всем пользователям:

- /tmp — каталог временных файлов. Содержимое каталога не сохраняется после перезагрузки ОС;

- /var/tmp — каталог временных файлов. Содержимое каталога сохраняется после перезагрузки ОС;

- /dev/shm — каталог разделяемой памяти, используется для обмена временными рабочими данными через разделяемую оперативную память. Содержимое каталога не сохраняется после перезагрузки ОС;

- `/run/mount` — каталог временного монтирования пользовательских устройств, используется для автоматического монтирования с помощью сценариев подключаемых пользовательских устройств;
- `/var/cache` — каталог для кеширования данных.

Также при установке дополнительного ПО могут создаваться собственные совместно используемые каталоги данного ПО.

Совместно используемые каталоги предназначены для создания в них файловых объектов, доступных всем пользователям. Применяемый в ОС механизм дискреционного управления доступом позволяет всем пользователям выполнять создание файловых объектов в совместно используемые каталогах, а также поиск принадлежащих другим пользователям файловых объектов в совместно используемых каталогах. Чтение и изменение не принадлежащих пользователю файловых объектов ограничивается дискреционными правами доступа, заданным для данного объекта. Дополнительно применяется специальное ограничение дискреционного доступа sticky-бит, запрещающее удалять и переименовывать не принадлежащие пользователю файловые объекты.

3.2.2. Создание

ФС создается при помощи команды `mkfs`. Команда запускает требуемую программу в зависимости от типа создаваемой ФС. Тип ФС задается параметром `-t`.

Пример

```
mkfs -t ext2 /dev/hdb1
```

Описание команды приведено в `man mkfs`.

3.2.3. Монтирование

Перед началом работы с ФС она должна быть смонтирована. Так как все файлы в ОС принадлежат одной структуре каталогов, то монтирование обеспечивает работу с ФС как с каталогом, называемым точкой монтирования. При этом ОС выполняет действия, обеспечивающие функционирование монтируемой ФС.

Перед монтированием ФС к дереву каталогов ОС необходимо убедиться, что существует каталог (точка монтирования), в который будет осуществляться монтирование ФС, иначе монтирование завершится неудачно.

После успешного монтирования ФС в каталог в нем появятся все файлы и подкаталоги ФС. В противном случае каталог будет пустым.

Если использовать в качестве точки монтирования непустой каталог, то его содержимое станет недоступно до размонтирования ФС. Поэтому рекомендуется для монтирования разделов/устройств создавать отдельные каталоги. Обычно они располагаются в `/mnt` и `/media`.

Для получения информации об имеющихся в ОС файловых системах используется инструмент командной строки `df`. Описание инструмента приведено в `man df`.

3.2.3.1. mount

В ОС для монтирования ФС используется инструмент командной строки `mount`. По умолчанию в целях обеспечения безопасности информации использовать инструмент `mount` может только администратор.

Синтаксис:

```
mount [параметр[параметр]] [<устройство>] [<точка_монтирования>]
```

где `<устройство>` — устройство, которое необходимо примонтировать;
`<точка_монтирования>` — имя каталога, в который требуется примонтировать устройство.

Параметры, дополнительно используемые с инструментом `mount`, приведенные в таблице 6.

Таблица 6

Параметр	Описание
`-f`	Имитировать монтирование ФС. Выполняются все действия, кроме системного вызова для монтирования ФС
`-v`	Вывести подробный отчет о действиях, выполняемых командой
`-w`	Примонтировать ФС с доступом для чтения и записи
`-r`	Примонтировать ФС с доступом только для чтения
`-n`	Выполнить монтирование без записи в файл `/etc/mtab`
`-t <тип_ФС>`	Задать тип монтируемой ФС
`-a`	Подключить все ФС, перечисленные в `/etc/fstab`
`-o <параметр>`	Задать параметры монтирования ФС, параметры в списке разделяются запятыми. Список возможных параметров приведен в `man mount`

Если необходимый параметр не указан, `mount` попытается определить его по файлу `/etc/fstab`.

Примеры:

1. Монтирование раздела жесткого диска /dev/hdb3 в каталог /mnt:

```
mount /dev/hdb3 /mnt
```

2. Монтирование всех ФС типа NFS, перечисленных в файле /etc/fstab:

```
mount -vat nfs
```

Если правильно примонтировать ФС не удается, то для получения отчета о результатах выполнения команды mount выполнить команду:

```
mount -vf <устройство> <точка_монтирования>
```

В данном случае команда выполняет все действия, кроме монтирования, и выводится подробный отчет о каждом шаге выполнения команды.

Описание команды mount приведено в man mount.

3.2.3.2. fstab

В конфигурационном файле /etc/fstab указываются ФС для монтирования и перечисляются параметры их монтирования.

В файле /etc/fstab каждой ФС соответствует запись в одной строке. Поля в строках разделяются пробелами или символами табуляции. В таблице 7 приведено описание полей файла /etc/fstab.

Таблица 7

Поле	Описание
<file system> (файловая система)	Подключаемое блочное устройство или удаленная ФС
<mount point> (точка монтирования)	Каталог монтирования ФС. Чтобы сделать систему невидимой в дереве каталогов (например, для файлов подкачки), используется слово none
<type> (тип)	Указывает тип монтируемой ФС
<options> (параметры монтирования)	Список разделенных запятыми параметров для монтируемой ФС. Должен содержать, по крайней мере, тип монтирования. Более подробную информацию см. в руководстве man команды mount
<dump> (периодичность резервного копирования)	Указывает, как часто следует выполнять резервное копирование с помощью команды dump. Если в поле стоит значение 0, то резервное копирование ФС не выполняется

Окончание таблицы 7

Поле	Описание
<pass> (номер прохода)	Задает порядок проверки целостности ФС при загрузке с помощью команды fsck. Для корневой ФС следует указывать значение 1, для остальных — 2. Если значение не указано, целостность ФС при загрузке проверяться не будет

Рекомендуется монтировать ФС во время загрузки через /etc/fstab, без использования команды mount. Далее приведен пример файла fstab.

Пример

```
# /etc/fstab: static file system information.
#
# Use 'blkid' to print the universally unique identifier for a
# device; this may be used with UUID= as a more robust way to name devices
# that works even if disks are added and removed. See fstab(5).
#
# <file system> <mount point>   <type>  <options>       <dump>  <pass>
# / was on /dev/sda11 during installation
UUID=a50cefb7-a198-4240-b198-581200027898 / ext4 errors=remount-ro,
     secdel=2 0 1
# /home was on /dev/sda10 during installation
UUID=c94bba8d-95d4-467b-b3e0-2cd7f92c3355 /home  ext4  usrquota,secdelrnd
     0 2
# swap was on /dev/sda5 during installation
UUID=ce71b251-2405-4eed-8130-5f92a56b67ac none    swap    sw       0 0
/dev/sr0        /media/cdrom0   udf,iso9660 user,noauto     0       0
```

Комментарии в файле начинаются с символа #.

В файле fstab параметр defaults поля <options> указывает, что при монтировании ФС будет применен набор параметров по умолчанию, а именно — ФС будет примонтирована с разрешенным доступом для чтения и записи; она должна рассматриваться как отдельное блочное устройство; весь файловый ввод-вывод должен выполняться асинхронно; разрешено выполнение программных файлов; ФС может монтироваться с помощью команды mount -a; биты UID и GID файлов в ФС интерпретируются; обычным пользователям не разрешено подключать данную ФС.

Раздел подкачки (в примере /dev/sda5) используется ядром ОС для организации виртуальной памяти. Он должен присутствовать в файле /etc/fstab для информирования системы о его местонахождении. Чтобы он не отображался в дереве каталогов, точка монтирования в

файле fstab указывается none. Кроме того, разделы подкачки монтируются с параметром sw.

Псевдофайловая система /proc указывает на информационное пространство процессов в памяти. Соответствующий физический раздел для нее отсутствует.

ФС VFAT также можно монтировать автоматически. Раздел /dev/sdb1 — это первый раздел второго жесткого диска SCSI. Он монтируется как раздел VFAT, где vfat указывается в качестве типа ФС, /win — в качестве точки монтирования.

Для получения полной информации о допустимых в файле /etc/fstab параметрах см. руководство man fstab.

3.2.4. Размонтирование

Для размонтирования ФС используется инструмент командной строки umount. Размонтирование может понадобиться для проверки и восстановления ФС с помощью команды fsck. Удаленные ФС размонтируются в случае неполадок в сети.

Инструмент umount имеет следующий синтаксис:

```
umount <устройство>
umount <точка_монтирования>
umount -a
umount -t <тип_ФС>
```

где <устройство> — устройство, которое необходимо размонтировать;
<точка_монтирования> — имя каталога, от которого необходимо отмонтировать;
-a — размонтировать все ФС;
-t — размонтировать только ФС указанного типа <тип_ФС>.

Инструмент umount не размонтирует ФС, если она используется в текущий момент. Например, если ФС смонтировать в /mnt и выполнить команды:

```
cd /mnt
umount /mnt
```

то появится сообщение об ошибке, т. к. ФС занята. Перед размонтированием /mnt необходимо перейти в каталог другой ФС.

Для принудительного размонтирования устройства, независимо от его использования, можно воспользоваться параметром -f:

```
umount -f /cdrom
```

Для размонтирования и извлечения из устройств сменных носителей информации используется инструмент командной строки `eject`.

Инструмент командной строки `fuser` отображает сведения о процессах, использующих ФС:

```
fuser -v <точка_монтирования>
```

Для завершения всех процессов, использующих ФС, можно воспользоваться командой:

```
fuser -km <точка_монтирования>
```

Описание инструментов `umount`, `eject` и `fuser` приведено, соответственно, в `man umount`, `man eject` и `man fuser`.

3.3. Управление пользователями

3.3.1. Работа с пользователями

Управление пользователями заключается в добавлении и удалении пользователей, а также в определении их привилегий и предусматривает:

- добавление имен пользователей для возможности их работы в системе;
- создание или изменение паролей пользователей;
- определение их привилегий;
- создание и назначение рабочих каталогов;
- определение групп пользователей;
- удаление имен пользователей.

Каждый пользователь должен иметь уникальное регистрационное имя, дающее возможность идентифицировать пользователя и избежать ситуации, когда один пользователь может стереть файлы другого. Кроме того, каждый пользователь должен иметь свой пароль для входа в систему.

3.3.1.1. Добавление пользователя

Для добавления пользователя применяется инструмент командной строки `adduser` с указанием в качестве параметра имени добавляемого пользователя:

```
adduser <имя_пользователя>
```

Команда `adduser` добавляет пользователя, создает рабочий каталог пользователя, создает почтовый ящик, а также копирует файлы, имена которых начинаются с точки, из каталога `/etc/skel` в рабочий каталог пользователя. Каталог `/etc/skel` должен содержать все

файлы-шаблоны, которые необходимы каждому пользователю. Обычно это персональные конфигурационные файлы для настройки оболочки, например `.profile`, `.bashrc` и `.bash_logout`.

При добавлении пользователя в систему в файле `/etc/passwd` добавляется запись вида:

```
login_name:encrypted_password:user_ID:group_ID:user_information:
     login_directory:login_shell
```

Описание полей записи приведено в таблице 8.

Таблица 8

Поле	Описание
`login_name`	Регистрационное имя учетной записи пользователя (имя пользователя)
`encrypted_password`	Указатель на теневой файл паролей (`shadow`)
`user_ID`	Уникальный номер, используемый ОС для идентификации пользователя. Для локальных пользователей не должен превышать 2499
`group_ID`	Уникальный номер или имя, используемые для идентификации первичной группы пользователя. Если пользователь является членом нескольких групп, то он может в процессе работы менять группу (если это разрешено администратором)
`user_information`	Информация о пользователе, например его фамилия, имя и должность
`login_directory`	Рабочий каталог пользователя (в котором он оказывается после входа в систему)
`login_shell`	Оболочка, используемая пользователем после входа в систему (например, `/bin/bash`)

Описание файла `/etc/passwd` приведено в `man 5 passwd`.

Команда `adduser` представляет собой файл сценария `bash`, находящийся в каталоге `/usr/sbin`.

Для изменения информации о пользователе используется инструмент командой строки `chfn`.

Описание `adduser` и `chfn` приведено, соответственно, в `man adduser` и `man chfn`.

ВНИМАНИЕ! Для обеспечения штатной работы пользователя с сетевыми службами в системе должна быть явно задана его классификационная метка (диапазон уровней конфиденциальности и категорий конфиденциальности), даже если ему недоступны уровни и категории выше 0. Описание классификационной метки и порядок ее использования приведены в РУСБ.10015-01 97 01-1.

3.3.1.2. Установка пароля пользователя

Для установки пароля пользователя предназначена команда `passwd`. Задавать пароль необходимо для каждого пользователя. После входа в систему пользователь может изменить свой пароль. Для установки пароля пользователя выполнить следующее:

1) ввести команду и имя пользователя, например:

```
passwd ivanov
```

и нажать клавишу **<Enter>**;

2) после появления приглашения:

```
Новый пароль:
```

ввести пароль и нажать клавишу **<Enter>**;

3) ввести повторно пароль после появления соответствующего сообщения и нажать клавишу **<Enter>**.

Пароль будет преобразован и внесен в файл `/etc/shadow`.

ВНИМАНИЕ! Пароль рекомендуется создавать способом, максимально затрудняющем его подбор. Наиболее безопасный пароль состоит из случайной (псевдослучайной) последовательности букв, знаков препинания, специальных символов и цифр.

Описание команды приведено в `man passwd`.

Пример

Запись в файле `/etc/passwd`

```
ivanov:x:123:121:Petr Ivanov:/home/ivanov:/bin/bash
```

Второе поле записи содержит ссылку на пароль в преобразованном виде.

Примечание. Пароль пользователя не хранится в явном виде. Если пользователь забыл свой пароль, то администратор системы не может его восстановить. Для восстановления доступа пользователя в систему администратор может задать новый пароль для пользователя с помощью команды `passwd`.

3.3.1.3. Удаление пользователя

В ОС доступно несколько вариантов удалить пользователя:

- лишить пользователя возможности входа в систему;
- удалить учетную запись пользователя;

- удалить учетную запись пользователя и все его файлы и каталоги.

Лишение пользователя возможности входа в систему может быть использовано в случае его длительного перерыва в работе. На время отсутствия пользователя можно заблокировать его учетную запись с помощью команды:

```
usermod -L <имя_пользователя>
```

После выполнения команды вход в систему от имени указанного пользователя будет недоступен, при этом все пользовательские файлы и каталоги сохраняются.

Для разблокировки учетной записи необходимо выполнить команду:

```
usermod -U <имя_пользователя>
```

Одним из вариантов лишения пользователя возможности входа в систему может быть смена имени пользователя. При этом вход в систему под старым именем становится невозможным. Для этого необходимо выполнить команду:

```
usermod -l <новое_имя_пользователя> <имя_пользователя>
```

Примечание. Имена домашнего каталога и почтового ящика при изменении имени пользователя не меняются. Эти параметры должны быть изменены вручную.

Удаление учетной записи пользователя производится либо путем непосредственного редактирования файла `/etc/passwd`, либо с помощью команды:

```
deluser <имя_пользователя>
```

По умолчанию учетная запись удаляется без удаления домашнего каталога и файлов, принадлежащих удаляемому пользователю. Для удаления домашнего каталога может использоваться дополнительный параметр `--remove-home`, а для поиска и удаления всех файлов, принадлежащих удаляемому пользователю, — параметр `--remove-all-files`.

Также удаление пользователя, его домашнего каталога и файлов могут быть выполнены вручную путем последовательного выполнения следующих команд:

1) для полного удаления пользователя и всех его файлов из системы выполнить команду:

```
find / -user <имя_пользователя> -exec rm -r {} \;
```

2) удалить запись о пользователе из файла `/etc/passwd`;

3) для удаления файлов, не принадлежащих ни одному пользователю в системе, выполнить команду:

```
find / -nouser -exec rm -r {} \;
```

Описание команд приведено в `man usermod`, `man deluser` и `man find`.

3.3.1.4. Неуспешный вход в систему

При неуспешной аутентификации пользователя счетчик увеличивает число неуспешных попыток аутентификации данного пользователя на единицу. При исчерпании числа попыток учетная запись пользователя будет заблокирована. После успешной аутентификации пользователя счетчик сбрасывается.

В ОС существуют следующие политики блокировки учетной записи при исчерпании числа неуспешных попыток входа в систему:

- индивидуальная политика блокировки;
- общая политика блокировки.

Предельное число попыток входа в обоих политиках по умолчанию равно 8.

Блокировка учетных записей при неуспешных попытках входа не распространяется на учетные записи из группы `astra-admin`.

После установки ОС используется индивидуальная политика блокировки учетных записей — в файле `/etc/pam.d/common-auth` для модуля `pam_faillock.so` указан параметр `per_user`:

```
auth requisite pam_faillock.so preauth audit per_user deny=8 fail_interval=900
     unlock_time=600
...
auth requisite pam_faillock.so authfail audit per_user deny=8 fail_interval=900
     unlock_time=600
```

При индивидуальной политике блокировки можно настроить параметры блокировки для отдельных учетных записей (при этом для остальных учетных записей будут использоваться общие параметры блокировки).

Индивидуальная политика блокировки настраивается инструментом командной строки `faillog`. Описание инструмента `faillog` приведено в `man faillog`.

Установка для учетной записи индивидуального количества неуспешных попыток входа в систему выполняется командой:

```
sudo faillog -m <число_неуспешных_попыток> -u <имя_пользователя>
```

Выполнение команды без указания имени учетной записи установит максимальное число неуспешных попыток входа для всех учетных записей.

Команды установки максимального числа неуспешных попыток входа для конкретной учетной записи и для всех учетных записей равнозначны по приоритету — выполнение одной команды переопределяет действие другой. Например, если сначала задать число неуспешных попыток для всех учетных записей, а затем индивидуальное (для конкретной учетной записи), то для данной учетной записи будет установлено индивидуальное значение числа неуспешных попыток. Если после установки индивидуального значения задать число неуспешных попыток для всех учетных записей, то оно переопределит ранее установленное индивидуальное значение.

Чтобы просмотреть для всех учетных записей заданное количество неуспешных попыток входа, необходимо выполнить команду:

```
sudo faillog -a
```

Чтобы просмотреть для конкретной учетной записи заданное количество неуспешных попыток входа, необходимо выполнить команду:

```
sudo faillog -u <имя_пользователя>
```

Значение индивидуальной блокировки для пользователя указывается в файле `/var/log/faillog`. Если для пользователя на задано значение индивидуальной блокировки, то оно берется из файла `/etc/pam.d/common-auth` (значение параметра `deny`).

Для просмотра журнала неуспешных попыток входа в систему, а также для сброса счетчика попыток необходимо использовать инструмент `faillock`. Описание инструмента приведено в `man faillock`.

Запуск инструмента `faillock` без параметров позволяет просмотреть неуспешные попытки входа в систему всех учетных записей и время, в которое они произошли.

В графическом интерфейсе для настройки индивидуальной политики блокировки используется модуль «Пользователи» графической утилиты `astra-systemsettings` («Параметры

системы»), описание модуля приведено в электронной справке. Для вызова модуля можно использовать команду:

```
astra-systemsettings astra_kcm_users
```

Для включения общей политики блокировки необходимо в файле `/etc/pam.d/common-auth` для модуля `pam_faillock.so` удалить параметр `per_user`:

```
auth requisite pam_faillock.so preauth audit deny=8 fail_interval=900
     unlock_time=600
...
auth requisite pam_faillock.so authfail audit deny=8 fail_interval=900
     unlock_time=600
```

Количество неуспешных попыток входа в систему, после которых учетная запись пользователя будет заблокирована, задается параметром `deny`.

Подробное описание настройки приведено в `man pam.faillock`.

В случае если в ОС применяется общая политика блокировки учетных записей, то индивидуальные значения для каждой учетной записи не учитываются.

В графическом интерфейсе для настройки общей политики блокировки учетных записей используется модуль «Блокировка учетной записи» графической утилиты `astra-systemsettings` («Параметры системы»), описание модуля приведено в электронной справке. Для вызова модуля можно использовать команду:

```
astra-systemsettings astra_kcm_policy_lockout
```

Сброс счетчика неуспешных попыток входа (как при индивидуальной, так и при общей политике блокировки) выполняется:

- для отдельной учетной записи командой:

  ```
  sudo faillock --user <имя_пользователя> --reset
  ```

- для всех учетных записей командой:

  ```
  sudo faillock --reset
  ```

Также в графическом интерфейсе для сброса счетчика неуспешных попыток входа отдельной учетной записи используется модуль «Пользователи» графической утилиты

astra-systemsettings («Параметры системы»), описание модуля приведено в электронной справке.

3.3.2. Работа с группами

Каждый пользователь является членом группы. Разным группам можно назначить разные возможности и привилегии.

Пользователь может состоять в нескольких группах и переходить из одной в другую в процессе работы.

Информация о группах содержится в файле /etc/group. Описание файла /etc/group приведено в man 5 group.

3.3.2.1. Добавление

Информация о группах в файле /etc/group содержится в формате:

```
Admin:x:21:user1,user2,user3
```

где Admin — имя группы;
x — пароль в преобразованном виде. Если поле пустое, то пароль не требуется;
21 — уникальный идентификатор группы;
user1, user2, user3 — участники группы.

Добавление группы производится с помощью команды:

```
addgroup <имя_группы>
```

Также новую группу можно создать путем редактирования файла /etc/group, добавив в нем строку с необходимой информацией о группе.

ВНИМАНИЕ! Каждой группе присваивается уникальный идентификационный номер и ОС при работе учитывает номер группы, а не имя. Поэтому, если присвоить двум группам одинаковый номер, ОС будет воспринимать две группы как одну и ту же.

Описание инструмента addgroup и файла /etc/group приведено, соответственно, в man addgroup и man 5 group.

3.3.2.2. Удаление

Удаление группы производится с помощью команды:

```
delgroup <имя_группы>
```

Также удалить группу можно путем редактирования файла `/etc/group`, удалив записи о группе.

Описание команды `delgroup` приведено в `man delgroup`.

3.3.3. Рабочие каталоги пользователей

Рабочие каталоги пользователей на одном компьютере следует размещать в отдельном каталоге верхнего уровня (по умолчанию — `/home`). Если пользователей много, то оптимально разделить их домашние каталоги по группам (подразделениям), например, `/home/hr` (отдел персонала) `/home/admins`, `/home/buhg` и т. д.).

Таким образом, рабочие каталоги будут логически сгруппированы, что в дальнейшем облегчит администрирование системы.

3.4. Перезагрузка и выключение

Перезагрузка необходима в следующих случаях:

1) при подключении нового устройства или если работающее устройство «зависает» и его невозможно сбросить;

2) при модификации файла конфигурации, который используется только при начальной загрузке, т. к. для того чтобы изменения вступили в силу, необходимо загрузить систему заново;

3) если система «не отвечает» и невозможно зарегистрироваться и определить причину ошибки.

Перезагрузку можно выполнить одним из способов:

1) использовать команду `shutdown` с параметром `-r` в соответствии с 3.4.1;
2) использовать команду `reboot` в соответствии с 3.4.2;
3) использовать команду `init 6`.

Выключение компьютера предполагает корректное завершение работы системы (останов), позволяющее избежать потерь информации и сбоев ФС.

Выключение компьютера можно выполнить несколькими способами:

1) использовать команду `shutdown` (см. 3.4.1);
2) использовать команду `halt` (см. 3.4.2);
3) использовать команду `init 0`.

Работая с ОС, не рекомендуется выключать питание компьютера без предварительного завершения работы с использованием соответствующих инструментов ОС, т. к. ОС хранит

информацию ФС в оперативной памяти и при отключении питания информация может быть потеряна, а ФС повреждена.

Выключение питания также может повредить жесткий диск, если установленный в системе жесткий диск перед отключением питания требует установки в соответствующее положение защитный переключатель либо выполнения парковки головок.

3.4.1. shutdown

Команда `shutdown` позволяет безопасно и корректно инициировать завершение работы системы, выключение, перезагрузку или возврат в однопользовательский режим.

В качестве параметра команды `shutdown` возможно задать время ожидания перед завершением работы системы. Во время ожидания команда посылает зарегистрированным пользователям через постепенно укорачивающиеся промежутки времени предупреждения о завершении работы системы. По умолчанию сообщения содержат информацию о завершении работы и времени, оставшемся до завершения работы. При желании администратор может добавить собственное сообщение, например с информацией о причине останова и о времени, в течение которого вход в систему будет невозможен.

Параметры команды `shutdown` позволяют задать определенное действие для компьютера: остановиться, перейти в однопользовательский режим или перезагрузиться. Дополнительно возможно указать, следует ли перед перезагрузкой проверить диски с помощью команды `fsck`.

Синтаксис команды:

```
shutdown [<параметр>] [<время>] [<сообщение>]
```

где `<параметр>` — параметр, определяющий действие команды (без параметра команда выполняет выключение компьютера);
`<время>` — время завершения работы системы в формате `чч:мм`. Значение может быть также задано в формате `+m`, где `m` — количество минут ожидания до завершения работы. Значение `+0` может быть заменено словом `now`;
`<сообщение>` — сообщение, посылаемое всем пользователям, зарегистрированным в системе в момент запуска команды.

В таблице 9 перечислены основные параметры команды `shutdown`.

Таблица 9

Параметр	Описание
`-k`	Послать предупреждение без реального завершения работы системы
`-r`	Перезагрузить компьютер после завершения работы

Окончание таблицы 9

Параметр	Описание
`-h`	Выключить компьютер после завершения работы
`-n`	Не синхронизировать диски. Этот параметр следует использовать осторожно, т. к. могут быть потеряны или повреждены данные
`-f`	«Быстрая» перезагрузка. Создается файл `/etc/fastboot`, при наличии которого во время загрузки ОС не запускается программа `fsck`
`-c`	Отменить уже запущенный процесс завершения работы. Параметр `<время>` при этом не может быть использован

Описание команды приведено в `man shutdown`.

Команда `shutdown` посылает всем пользователям предупреждающее сообщение, затем ожидает заданное в командной строке время и посылает всем процессам сигнал `SIGTERM`. Далее вызывается команда `halt` или `reboot` — в зависимости от параметров командной строки.

3.4.2. halt и reboot

Команда `halt` выполняет все основные операции, необходимые для останова системы. Для вызова команды выполнить в командной строке:

```
halt
```

или

```
shutdown -H
```

Команда регистрирует останов, уничтожает несущественные процессы, осуществляет системный вызов `sync`, ожидает завершения операций записи ФС, а затем прекращает работу ядра.

При выполнении команды `halt` с параметром `-n`:

```
halt -n
```

вызов `sync` подавляется. Данная команда используется после исправления корневого раздела программой `fsck` для того, чтобы ядро не могло затереть исправления старыми версиями суперблока.

При выполнении команды `halt` с параметром `-q`:

```
halt -q
```

инициируется немедленный останов, без синхронизации, уничтожения процессов и записи в файлы регистрации.

Команда `reboot` выполняет все основные операции, необходимые для останова системы (аналогично команде `halt`), а затем перезагружает компьютер с нуля. Для вызова команды выполнить в командной строке:

```
reboot
```

или

```
shutdown -r
```

Описание команд `halt` и `reboot` приведено в `man halt` и `man reboot` соответственно.

4. ПАРАМЕТРЫ ЯДРА, СИСТЕМНЫЕ СЛУЖБЫ, СОСТОЯНИЯ И КОМАНДЫ

4.1. Профили ядра ОС

В ОС присутствует возможность изменять значения настраиваемых параметров ядра с помощью предустановленных профилей. Параметры ядра сгруппированы в шаблоны. Каждый профиль ядра содержит несколько шаблонов.

Выбор активного профиля ядра осуществляется с помощью инструмента командной строки `kernel-profiles-manager`.

Синтаксис команды:

```
kernel-profiles-manager [параметр]
```

Описание параметров инструмента приведено в таблице 10.

Таблица 10

Параметр	Описание
`-c, --current`	Вывести название активного профиля
`-d, --default-profile`	Сменить активный профиль ядра на профиль по умолчанию (`generic`)
`-l, --profiles-list`	Вывести список профилей, присутствующих в системе
`-m, --template <имя_шаблона>`	Вывести список параметров ядра, содержащихся в указанном шаблоне
`-n, --profile-name <имя_профиля>`	Вывести список параметров ядра, содержащихся в указанном профиля
`-p, --change-profile <имя_профиля>`	Сменить активный профиль ядра на указанный
`-t, --templates-list <имя_профиля>`	Вывести список шаблонов, содержащихся в указанном профиле
`-v, --verify <имя_профиля>`	Вывести состояние указанного профиля (`Активен`/`Неактивен`)
`-h, --help`	Вывести справку и выйти

Описание профилей и входящих в них шаблонов и параметров ядра приведено в 4.1.1 и 4.1.2.

Примеры:

1. Вывести список параметров ядра, входящих в шаблон `kexec-hardened`:

```
sudo kernel-profiles-manager -m kexec-hardened
```

2. Применить профиль `generic`:

```
sudo kernel-profiles-manager -p generic
```

3. Отобразить состояние профиля `hardened`:

```
sudo kernel-profiles-manager -v hardened
```

Вывод команды:

```
Неактивен
```

4.1.1. Профиль ядра generic

Профиль ядра `generic` обеспечивает непривилегированным пользователям доступ к средствам контейнеризации, инструментам отладки и трассировки.

Шаблоны, входящие в профиль `generic`, и содержащиеся в них параметры ядра приведены в таблице 11.

Таблица 11

Шаблон	Параметр ядра и его значение	Описание
`bpf-generic`	`kernel.net.core.bpf_jit_harden = 0`	Отключается усиленная JIT-компиляция BPF-программ
`namespaces-generic`	`user.max_user_namespaces = 15279`	Все пользователи могут создавать новые пространства имен (необходимо для работы средств контейнеризации)
`perf-generic`	`kernel.kptr_restrict = 0`	Разрешается использование инструментов отладки `perf` и BPF для сбора метрик и трассировки
	`kernel.perf_event_paranoid = 2`	Пользователи с Linux-привилегией `CAP_PERFMON` могут использовать точки трассировки ядра, инструмент `perf` и BPF-программы

Окончание таблицы 11

Шаблон	Параметр ядра и его значение	Описание
kexec-generic	kernel.kexec_load_disabled = 0	Возможна динамическая загрузка другого ядра с помощью механизма kexec и использование инструментов kexec-tools и kdump-tools

4.1.2. Профиль ядра hardened

Профиль ядра hardened позволяет повысить защищенность ОС от возможных атак. При использовании данного профиля непривилегированные пользователи не могут использовать средства контейнеризации, инструменты отладки и трассировки.

Шаблоны, входящие в профиль hardened, и содержащиеся в них параметры ядра приведены в таблице 12.

Таблица 12

Шаблон	Параметр ядра и его значение	Описание
bpf-hardened	net.core.bpf_jit_harden = 2	Для динамически скомпилированных программ используется случайное изменение адресов памяти для усложнения эксплуатации уязвимостей
namespaces-hardened	user.max_user_namespaces = 0	Запрещено создание новых пространств имен, работа средств контейнеризации невозможна
perf-hardened	kernel.kptr_restrict = 2	Адреса ядра полностью скрываются и блокируется загрузка символов ядра. Инструменты отладки не могут использоваться для анализа ядра и интерпретации данных
	kernel.perf_event_paranoid = 3	Запрещен сбор метрик производительности ядра непривилегированными пользователями
kexec-hardened	kernel.kexec_load_disabled = 1	Механизм kexec заблокирован на уровне ядра. Невозможна работа инструментов динамической загрузки ядра и восстановления системы

4.2. Системные службы

Службы — это специальные программы, выполняющие различные служебные функции. Обычно службы запускаются автоматически при наступлении определенного события (например, при загрузке ОС) и выполняются в фоновом режиме.

4.2.1. Управление службами

В среде ОС для управления службами, точками монтирования и т. п. применяется системный менеджер systemd. Менеджер systemd обеспечивает параллельный запуск служб в процессе загрузки ОС, использует сокеты и активацию D-Bus для запускаемых служб, предлагает запуск демонов по необходимости, отслеживает запуск служб, поддерживает мгновенные снимки и восстановление состояния системы, монтирование и точки монтирования, а также внедряет основанную на зависимостях логику контроля процессов сложных транзакций.

Отличительной особенностью systemd является использование контрольных групп Linux, обеспечивающих иерархическую структуризацию служб: любая запущенная служба помещается в отдельную контрольную группу с уникальным идентификатором. Служба, запуская другую зависимую службу, становится родительской службой, а зависимая служба — дочерней. Дочерняя служба автоматически включается в группу с тем же идентификатором, что и родительская. Непривилегированные службы не могут изменить свое положение в иерархии. При штатном завершении работы родительской службы будут завершены и все ее дочерние службы.

Информация о менеджере systemd также приведена в `man systemd`.

Описание использования менеджера systemd для управления доступом приведено в РУСБ.10015-01 97 01-1.

Менеджер systemd оперирует специально оформленными конфигурационными файлами — юнитами (unit). Каждый юнит отвечает за конкретную службу (`*.service`), точку монтирования (`*.mount`), устройство (`*.device`), файл подкачки (`*.swap`), сокет (`*.socket`) и т. д.

Юниты менеджера systemd располагаются в каталогах `/etc/systemd/system`, `/run/systemd/system`, `/usr/lib/systemd/system`, а также в пользовательских каталогах.

Приоритет выполнения юнитов зависит от их расположения:

1) `/usr/lib/systemd/system/` — юниты из установленных пакетов, имеют минимальный приоритет;

2) /run/systemd/system/ — юниты, созданные во время выполнения (в режиме runtime). Данные юниты имеют приоритет выше, чем юниты из установленных пакетов;

3) /etc/systemd/system/ — юниты, созданные и управляемые администратором. Данные юниты имеют приоритет выше, чем юниты, созданные во время выполнения.

Также в ОС доступен механизм управления службами systemV, сохраненный для обеспечения совместимости. Менеджер systemV управляет сценариями запуска в каталогах /etc/init.d, /etc/rc{0-6,S}.d.

Таким образом, администратор ОС может использовать два инструмента для управления службами:

1) /usr/sbin/service (service) — устаревший инструмент, работающий только со службами, сценарии управления которых находятся в каталогах /etc/init.d, /etc/rc{0-6,S}.d;

2) /bin/systemctl (systemctl) — инструмент для управления всеми службами.

Инструменты обеспечивают интерфейс пользователя с юнитами/сценариями. Юниты/сценарии, в свою очередь, обеспечивают интерфейс управления службами, предоставляя администратору задавать параметры для запуска, остановки, перезапуска, запроса состояния, а также для других действий со службой.

Сценарии systemV могут иметь произвольный набор параметров управления, поэтому предусмотрена возможность проверки доступных параметров с помощью инструмента service. Для этого выполнить команду с названием сценария в качестве параметра.

Пример

Команда запроса доступных параметров для службы cron:

```
sudo /usr/sbin/service cron
```

Результат выполнения команды:

```
[info] Usage: /etc/init.d/cron {start|stop|status|restart|reload|
     force-reload}
```

Инструмент service выводит информацию только о службах, сценарии которых находятся в каталоге /etc/init.d. Проверить текущее состояние служб можно указав параметр --status-all в команде:

```
sudo /usr/sbin/service --status-all
```

Пример

Вывод команды `/usr/sbin/service --status-all` проверки состояния служб:

```
[ + ]  acpi-support
[ + ]  acpid
[ - ]  anacron
...
```

Основные параметры инструмента `systemctl` приведены в таблице 13.

Таблица 13

Параметр	Описание
`start <юнит>`	Незамедлительно запустить юнит
`stop <юнит>`	Незамедлительно остановить юнит
`restart <юнит>`	Перезапустить юнит
`try-restart <юнит>`	Перезапустить (не запускать неработающие) юниты
`reload <юнит>`	Перезагрузить настройки юнита
`status`	Вывести общую информацию о состоянии системы и список юнитов, которым соответствуют запущенные процессы. При запуске команды с именем юнита будет выведена информация о статусе данного юнита
`cat <юнит>`	Показать содержимое юнита
`is-enabled <юнит>`	Проверить включение юнита в автозапуск при загрузке системы
`enable <юнит>`	Добавить юнит в автозапуск при загрузке системы
`disable <юнит>`	Удалить юнит из автозапуска при загрузке системы
`mask <юнит>`	Маскировать юнит для исключения возможности его запуска
`unmask <юнит>`	Снять маску юнита
`help <юнит>`	Показать справочную страницу по юниту (при наличии поддержки данной функции для указанного юнита)
`daemon-reload`	Перезагрузить systemd для поиска новых или измененных юнитов
`list-unit-files`	Показать список установленных юнитов
`-a`	Показать список юнитов, которые менеджер systemd загрузил и пробовал загрузить, не зависимо от их состояния в текущий момент
`list-units`	Показать список запущенных юнитов
`--failed`	Показать список юнитов, которые не были запущены из-за ошибки
`-t <тип_юнита>`	Показать только юниты указанного типа

Окончание таблицы 13

Параметр	Описание
`isolate <юнит_или_цель>`	Если указано имя юнита, то запускает этот юнит и все его зависимости, остановив все остальные службы. Если указано имя целевого состояния выполнения, то переводит систему в указанное состояние выполнения (имя состояния указывается без расширения `.target`)

Примеры:

1. Просмотр списка запущенных юнитов типа `socket`:

```
systemctl list-units -t socket
```

2. Получение списка юнитов типа `service`, которые загрузил и пробовал загрузить менеджер systemd:

```
systemctl -t service -a
```

Результат выполнения команды:

```
UNIT                    LOAD      ACTIVE    SUB     DESCRIPTION
acpi-support.service    loaded    active    exited  LSB: Start some power
? apache2.service       masked    inactive  dead    apache2.service
? apparmor.service      not-found inactive  dead    apparmor.service
assistant.service       loaded    active    running Assistant remote
control
```

Полное описание команды `systemctl` приведено в `man systemctl`.

4.2.2. Конфигурационные файлы systemd

При использовании менеджера systemd возможно как корректировать существующие юниты, так и создавать новые.

Юнит представляет собой `ini`-подобный файл, имя которого состоит из имени юнита и суффикса, определяющего тип юнита. В общем случае юнит-файл включает секции `[Unit]` и `[Install]`, а также секции, соответствующие конкретному типу юнита.

Секция `[Unit]` содержит описание юнита, а также информацию о зависимостях при запуске юнита. Основные параметры секции:

1) `Description=` — описание юнита;

2) `Wants=` — зависимость требования запуска. Требование исходного юнита запустить юнит, указанный в параметре. При этом результат запуска юнита, указанного в параметре, не влияет на запуск исходного юнита. При отсутствии параметров `After=` и `Before=` юниты будут запущены одновременно;

3) `Requires=` — зависимость требования запуска. Требование исходного юнита запустить юнит, указанный в параметре. При этом ошибка запуска юнита, приведенного в параметре, приведет к ошибке запуска исходного юнита. При отсутствии параметров `After=` и `Before=` юниты будут запущены одновременно;

4) `After=` — зависимость порядка запуска. Дополнительный, но не обязательный параметр к параметрам `Wants=` и `Requires=`, указывающий на необходимость запуска исходного юнита только после запуска юнита, указанного в параметре. При этом если данный параметр используется с параметром `Wants=`, то исходный юнит будет запущен вне зависимости от результата запуска юнита, указанного в параметре;

5) `Before=` — аналогичен параметру `After=`, только определяет запуск исходного юнита до запуска юнита, указанного в параметре.

Секция `[Install]` содержит информацию об установке юнита. Используется командами `systemctl enable <юнит>` и `systemctl disable <юнит>`. Может содержать следующие параметры:

1) `Alias=` — список альтернативных имен юнита, разделенных пробелом. Имена должны иметь тот же суффикс, что и имя файла юнита. При использовании команды `systemctl enable` будут созданы символические ссылки из перечисленных имен на данный юнит.
ВНИМАНИЕ! Не все типы юнитов могут иметь альтернативные имена. Для типов `*.mount`, `*.slice`, `*.swap` и `*.automount` данный параметр не поддерживается;

2) `WantedBy=` — указывает на целевое состояние (см. 4.3), при котором запускается данный юнит. При использовании команды `systemctl enable` будет добавлена символическая ссылка в `<имя_состояния>.target`;

3) `Also=` — определяет список юнитов, которые будут добавлены в автозапуск или удалены из автозапуска вместе с данным юнитом.

Секция `[Service]` присутствует в юнитах службы и может содержать следующие параметры, определяющие запуск службы:

1) `Type=` — определяет тип запуска службы:
   а) `simple` — служба считается запущенной, когда завершился основной процесс службы (процесс, определенный в `ExecStart=`, считается основным процессом). Не рекомендуется использовать данный тип, если другие службы зависят от очередности при запуске данной службы. Исключение — активация сокета;

б) forking — служба считается запущенной, когда основной (родительский) процесс службы создал дочерний процесс, при этом родительский процесс завершился. Дочерний процесс продолжает функционировать в качестве основного. Рекомендуется использовать данный тип для запуска классических демонов. Потребуется также задать значение параметра PIDFile= для отслеживания основного процесса;

в) oneshot — похож на тип simple, используется для сценариев, которые завершаются после выполнения одного задания;

г) notify — похож на тип simple, но служба запускается после отправки менеджеру systemd сигнала о своей готовности;

д) dbus — похож на тип simple, но ожидает появления в системной шине DBus шины, указанной в BusName=;

е) idle — менеджер systemd отложит выполнение службы и запустит ее после запуска остальных служб;

2) PIDFile= — расположение pid-файла службы;

3) ExecStart= — указывает на команду, которая должна быть выполнена при запуске службы;

4) ExecStop= — указывает на команды, которые должны быть выполнены для завершения службы, запущенной в ExecStart=;

5) ExecReload= — указывает на команду, которая должна быть выполнена для перезапуска службы;

6) Restart= — определяет перезапуск службы в случае самостоятельного или принудительного завершения основного процесса или при возникновении ошибки;

7) RemainAfterExit — позволяет считать службу активной даже в случае, если все ее процессы завершились. Значение по умолчанию no (нет).

Общие параметры, которые могут содержаться в секциях [Service], [Socket], [Mount], [Swap]:

1) WorkingDirectory= — рабочий каталог службы;

2) User= — пользователь, от имени которого будет запущена служба;

3) Group= — группа, от имени которой будет запущена служба;

4) OOMScoreAdjust= — корректирующее значение для Out-Of-Memory (OOM) Killer в ядре Linux для выполняемых процессов при нехватке памяти. Принимает целое число в диапазоне от -1000 (чтобы отключить OOM Killer и полностью запретить завершение процессов этого юнита) до 1000 (чтобы сделать очень вероятным завершение процессов этого юнита при нехватке памяти);

5) KillMode= — указывает на порядок завершения процессов данного юнита.

4.3. Системные (целевые) состояния

В systemd уровни запуска файлов реализованы в виде сгруппированных юнитов, представляющих целевое состояние (цель). Файлы, определяющие целевые состояния, хранятся в каталоге `/lib/systemd/system/` и имеют расширение имени `.target`. Для совместимости в ОС сохранено понятие «уровней выполнения». В стандартно установленной системе предусмотрено наличие шести системных уровней выполнения, каждому из которых соответствует целевое состояние.

Одна из целей назначается в качестве состояния по умолчанию, в которое переходит система после включения. В стандартно установленной ОС состоянием по умолчанию является `graphical.target` (уровень выполнения 5) — многопользовательский режим с графической оболочкой. Цель `multi-user.target` (с уровням выполнения 2, 3 и 4) — многопользовательский режим без графической оболочки. Целям `poweroff.target` (уровень выполнения 0) и `reboot.target` (уровень выполнения 6) соответствуют выключение и перезагрузка системы соответственно.

Проверить список соответствия состояний и уровней выполнения можно командой:

```
ls -la /lib/systemd/system/runlevel*
```

Пример вывода команды:

```
lrwxrwxrwx 1 ... /lib/systemd/system/runlevel0.target -> poweroff.target
lrwxrwxrwx 1 ... /lib/systemd/system/runlevel1.target -> rescue.target
lrwxrwxrwx 1 ... /lib/systemd/system/runlevel2.target -> multi-user.target
lrwxrwxrwx 1 ... /lib/systemd/system/runlevel3.target -> multi-user.target
lrwxrwxrwx 1 ... /lib/systemd/system/runlevel4.target -> multi-user.target
lrwxrwxrwx 1 ... /lib/systemd/system/runlevel5.target -> graphical.target
lrwxrwxrwx 1 ... /lib/systemd/system/runlevel6.target -> reboot.target
```

Каждая цель имеет собственное имя вида `<имя_состояния>.target` и предназначена для конкретных задач. Одновременно могут быть активны несколько целей. Цели могут наследовать все службы других целей, добавляя к ним свои. В systemd также имеются цели, имитирующие общие уровни выполнения SystemV, поэтому для переключения между целевыми юнитами можно использовать команду:

```
telinit RUNLEVEL
```

Для определения доступных целевых состояний используется команда:

```
systemctl list-unit-files --type=target
```

Для определения активных целевых состояний используется команда:

```
systemctl list-units --type=target
```

Для перехода в целевое состояние используется команда:

```
systemctl isolate <имя_состояния>.target
```

или команда:

```
sudo init <уровень_выполнения>
```

Данные команды изменят только текущий уровень выполнения и их действие не повлияет на последующие загрузки системы.

Пример

Для перехода в целевое состояние командой `systemctl` выполнить:

```
systemctl isolate multi-user.target
```

Для перехода в целевое состояние командой `init` выполнить:

```
sudo init 3
```

Обе команды переведут систему в состояние `multi-user` (многопользовательский режим без графической оболочки), что соответствует третьему уровню выполнения. При этом будут запущены/остановлены все службы, указанные в соответствующем описании состояния.

Для просмотра целевого состояния по умолчанию, которое systemd использует сразу после загрузки системы, используется команда:

```
systemctl get-default
```

Для просмотра дерева зависимостей юнитов от цели выполнить команду:

```
systemctl list-dependencies <имя_состояния>.target
```

Для проверки текущего уровня выполнения выполнить команду:

```
sudo runlevel
```

Для изменения состояния системы, заданного по умолчанию, выполнить команду:

```
sudo systemctl set-default <имя_состояния>.target
```

В новое состояние по умолчанию система будет переведена после перезагрузки. Для принудительного перевода системы в нужное состояние без перезагрузки используется команда `systemctl` с параметром `isolate` и именем целевого состояния (имя состояния может быть указано без расширения `.target`). или команда `init` с указанием уровня выполнения.

Для обеспечения совместимости с более ранними реализациями помимо запуска/остановки юнитов, определенных в файлах `.target`, при переводе системы в другое целевое состояние systemd проверяет все файлы управления службами, имеющиеся в соответствующем целевому уровню выполнения каталоге `/etc/rc{0-6}.d/`, и запускает/останавливает соответствующие этим файлам собственные юниты или, если соответствующий юнит не обнаружен, автоматически генерирует юнит из файла управления и выполняет его.

Подробное описание данных команд и служб приведено на страницах руководства `man systemctl`, `man init`.

4.4. Системные команды

Основные системные команды ОС приведены в таблице 14.

Таблица 14

Команда	Назначение
`addgroup`	Создание новой учетной записи группы
`adduser`	Создание новой учетной записи пользователя
`ar`	Создание и работа с библиотечными архивами
`at`	Формирование или удаление отложенного задания
`awk`	Язык обработки строковых шаблонов
`bc`	Строковый калькулятор
`chfn`	Управление информацией учетной записи пользователя (имя, описание)
`chsh`	Управление выбором командного интерпретатора (по умолчанию — для учетной записи)
`cut`	Разбивка файла на секции, задаваемые контекстными разделителями
`delgroup`	Удаление учетной записи группы
`deluser`	Удаление учетной записи пользователя и соответствующих файлов окружения
`df`	Вывод отчета об использовании дискового пространства
`dmesg`	Вывод содержимого системного буфера сообщений

Продолжение таблицы 14

Команда	Назначение
du	Вычисление количества использованного пространства элементов ФС
echo	Вывод содержимого аргументов на стандартный вывод
egrep	Поиск строки (в т. ч. в файлах), содержащей заданное регулярное выражение
fgrep	Поиск строки (в т. ч. в файлах), содержащей заданный фиксированный шаблон
file	Определение типа файла
find	Поиск файла по различным признакам в иерархии каталогов
gettext	Получение строки интернационализации из каталогов перевода
grep	Поиск строки (в т. ч. в файлах), содержащей шаблон поиска
groupadd	Создание новой учетной записи группы
groupdel	Удаление учетной записи группы
groupmod	Изменение учетной записи группы
groups	Вывод списка групп
gunzip	Распаковка файла
gzip	Упаковка файла
hostname	Вывод и задание имени хоста
install	Копирование файла с установкой атрибутов
ipcrm	Удаление средства IPC
ipcs	Вывод информации о средствах IPC
kill	Отправка процессу сигнала прекращения выполнения
killall	Отправка всем процессам с указанным именем сигнала прекращения выполнения
lpr	Система печати
ls	Вывод содержимого каталога
lsb_release	Вывод информации о дистрибутиве
mknod	Создание файла специального типа
mktemp	Генерация уникального имени файла
more	Постраничный вывод содержимого файла
mount	Монтирование ФС
msgfmt	Создание объектного файла сообщений из файла сообщений
newgrp	Смена идентификатора группы
nice	Изменение приоритета процесса перед его запуском
nohup	Работа процесса после выхода из системы
od	Вывод содержимого файла в восьмеричном и других видах
passwd	Смена пароля учетной записи
patch	Применение файла описания изменений к оригинальному файлу
pidof	Вывод идентификатора процесса по его имени

Окончание таблицы 14

Команда	Назначение
ps	Вывод информации о процессах
renice	Изменение уровня приоритета процесса
sed	Строковый редактор
sendmail	Транспорт системы электронных сообщений
sh	Командный интерпретатор
shutdown	Команда останова системы
su	Изменение идентификатора запускаемого процесса
sync	Сброс системных буферов на носители
tar	Файловый архиватор
umount	Размонтирование ФС
useradd	Создание новой учетной записи пользователя или обновление существующей
userdel	Удаление учетной записи пользователя и соответствующих файлов окружения
usermod	Модификация информации об учетной записи пользователя
w	Список пользователей, работающих в настоящий момент в системе, и ресурсов, с которым осуществляется работа
who	Вывод списка пользователей системы

Описание команд приведено на страницах руководства man.

4.4.1. Планирование запуска команд

4.4.1.1. at

Для запуска одной или более команд в заранее определенное время используется команда at. В ней можно определить время и/или дату запуска той или иной команды. Команда at требует двух (или большего числа) параметров. Как минимум, следует указать время запуска и какая команда должна быть запущена.

Команды для запуска с помощью команды at вводятся как список в строках, следующих за ней. Ввод каждой строки завершается нажатием клавиши **<Enter>**. По окончании ввода всей команды нажать клавиши **<Ctrl+D>** для ее завершения.

Примеры:

1. Запустить команды lpr /usr/sales/reports/. и echo "Files printed" в 8:00

```
at 8:00
lpr /usr/sales/reports/.
```

```
echo "Files printed"
```

После ввода всей команды отобразится следующая запись:

```
job 756603300.a at Tue Jul 8 08:00:00 2014
```

означающая, что указанные команды будут запущены в 8:00, идентификатор задания `756603300.a` (может понадобится, если необходимо отменить задание командой `at -d`)

В результате выполнения команды в 8:00 будут распечатаны все файлы каталога `/usr/sales/reports`, и пользователю будет выведено сообщение на экран монитора.

2. Для запуска всех команд, перечисленных в файле `getdone`, в 17:30 следует воспользоваться одной из двух форм команды `at`:

```
at 17:30 < getdone
```

или

```
at 10:30 -f getdone
```

Обе приведенные команды эквивалентны. Разница заключается в том, что в первой команде используется механизм перенаправления потоков ввода-вывода, во второй команде — дисковый файл.

Кроме времени в команде `at` может быть определена дата.

Пример

```
at 10:00 Jul 14
lp /usr/sales/reports/
echo "Files printed"
```

Задания, определяемые администратором системы, помещаются в очередь, которую ОС периодически просматривает. Администратору необязательно находиться в системе для того, чтобы `at` отработала задания. В данном случае команда работает в фоновом режиме.

Для просмотра очереди заданий ввести:

```
at -l
```

Если предыдущие примеры были запущены, то будет выведено:

```
job 756603300.a at Sat Jul 8 08:00:00 2014 job 756604200.a at Sat Jul 14
  17:00:00 2014
```

Администратор системы видит только свои задания по команде `at`.

Для удаления задания из очереди следует запустить `at` с параметром `-d` и номером удаляемого задания:

```
at -d 756604200.a
```

В таблице 15 показаны варианты использования команды `at`.

Таблица 15

Формат команды	Назначение
`at hh:mm`	Выполнить задание во время `hh:mm` в 24-часовом формате
`at hh:mm месяц день год`	Выполнить задание во время `hh:mm` в 24-часовом формате в соответствующий день
`at -l`	Вывести список заданий в очереди; псевдоним команды — `atq`
`at now+count time-units`	Выполнить задание через определенное время, которое задано параметром `count` в соответствующих единицах — неделях, днях, часах или минутах
`at -d job_ID`	Удалить задание с идентификатором `job_ID` из очереди; псевдоним команды — `atrm`

Администратор системы может применять все эти команды. Для других пользователей права доступа к команде `at` определяются файлами `/etc/at.allow` и `/etc/at.deny`. Если существует файл `/etc/at.allow`, то применять команду `at` могут только перечисленные в нем пользователи. Если же такого файла нет, проверяется наличие файла `/etc/at.deny`, в котором отражено, кому запрещено пользоваться командой `at`. Если ни одного файла нет, значит, команда `at` доступна только суперпользователю.

Подробное описание команды приведено в `man at`.

4.4.1.2. cron

Для регулярного запуска команд в ОС существует команда `cron`. Администратор системы определяет для каждой программы время и дату запуска в минутах, часах, днях месяца, месяцах года и днях недели.

Команда `cron` запускается один раз при загрузке системы. Отдельные пользователи не должны иметь к ней непосредственного доступа. Кроме того, запуск `cron` никогда не осу-

ществляется вручную путем ввода имени программы в командной строке, а только из сценария загрузки ОС.

При запуске `cron` проверяет очередь заданий команды `at` и задания пользователей в файлах `crontab`. Если команд для запуска нет, `cron` «засыпает» на одну минуту и затем вновь приступает к поискам команды, которую следует запустить в этот момент. Большую часть времени команда `cron` проводит в «спящем» состоянии, и для ее работы используется минимум системных ресурсов.

Чтобы определить список заданий для `cron` используется команда `crontab`. Для каждого пользователя с помощью данной команды создается файл `crontab` со списком заданий, находящийся в каталоге `/var/spool/cron/crontabs` и имеющий то же имя, что и имя пользователя.

Примечание. Пользователи, которым разрешено устанавливать задания командой `cron`, перечислены в файле `/etc/cron.allow`. Файл заданий для команды `cron` можно создать с помощью обычного текстового редактора, но при этом нельзя просто заменить им существующий файл задания в каталоге `/var/spool/cron/crontabs`. Для передачи `cron` сведений о новых заданиях обязательно должна использоваться команда `crontab`.

Каждая строка в файле `crontab` содержит шаблон времени и команду. Можно создать любое количество команд для `cron`. Команда выполняется тогда, когда текущее время соответствует приведенному шаблону. Шаблон состоит из пяти частей, разделенных пробелами или символами табуляции.

Синтаксис команд в файле `crontab`:

```
<минуты> <часы> <день_месяца> <месяц> <день_недели> <задание>
```

Первые пять полей представляют шаблон времени и должны присутствовать в файле. Для того чтобы `cron` игнорировала то или иное поле шаблона времени, следует поставить в поле символ * (звездочка).

Примечание. Символ * означает соответствие любому корректному значение.

Пример

Шаблон:

```
02 00 01 * *
```

определяет, что команда должна быть запущена в 00 часов 2 минуты каждого первого числа любого месяца (символ * в четвертом поле) независимо от дня недели (символ * в пятом поле).

В таблице 16 приведены допустимые значения полей записей crontab.

Таблица 16

Поле	Диапазон
<минуты>	00–59
<часы>	00–23 (полночь — 00)
<день_месяца>	01–31
<месяц>	01–12
<день_недели>	01–07 (понедельник — 01, воскресенье — 07)

Пример

Запись команды в файле crontab, выполняющая сортировку и отправку пользователю pav файла /usr/sales/weekly каждый понедельник в 7:30

```
30 07 * * 01 sort /usr/sales/weekly | mail -s"Weekly Sales" pav
```

Поле команд может содержать все, что может быть в команде, вводимой в командной строке оболочки. В нужное время cron для выполнения команд запустит стандартную оболочку (bash) и передаст ей команду для выполнения.

Для того чтобы определить несколько значений в поле используется запятая в качестве разделяющего символа. Например, если программа chkquotes должна выполняться в 9, 11, 14 и 16 часов по понедельникам, вторникам и четвергам 10 марта и 10 сентября, то запись выглядит так:

```
. 09,11,14,16 10 03,09 01,02,04 chkquotes
```

Параметры команды crontab приведены в таблице 17.

Таблица 17

Параметр	Описание
-e	Позволяет редактировать компоненты файла (при этом вызывается редактор, определенный в переменной EDITOR оболочки)
-r	Удаляет текущий файл crontab из каталога
-l	Используется для вывода списка текущих заданий cron

Команда crontab работает с файлом согласно регистрационному имени.

За корректное использование команды `cron` ответственность несут как администратор системы, так и пользователи, например, использование программы не должно вызвать перегрузку системы.

Подробное описание команд и файла `crontab` приведено в `man cron`, `man crontab` и `man 5 crontab`.

4.4.2. Администрирование многопользовательской и многозадачной среды

4.4.2.1. who

Для получения списка пользователей, работающих в ОС, используется инструмент командной строки `who`. Результатом выполнения команды является список, содержащий идентификаторы активных пользователей, терминалы и время входа в систему.

Пример

Результат выполнения команды `who`:

```
root console May 19 07:00
```

Основные параметры команды `who`:

1) `-u` — вывести список пользователей с указанием времени бездействия (символ «`.`» (точка) означает, что пользователь активно работал в последнюю минуту, `old` — что последний раз нажатие клавиш было более суток назад);

2) `-H` — вывести подробную информацию о пользователях. При этом выводится строка заголовка таблицы пользователей, описание столбцов приведено в таблице 18.

Таблица 18

Поле	Описание
ИМЯ	Имя пользователя
ЛИНИЯ	Использованные линии и терминалы
ВРЕМЯ	Время, прошедшее после регистрации пользователя в системе
IDLE	Время, прошедшее со времени последней активной работы пользователя
PID	Идентификатор процесса входной оболочки пользователя
КОММЕНТАРИЙ	Комментарий

Пример

Выполнение команды who с параметрами -u и -H:

```
who -uH
```

Результат выполнения команды:

```
ИМЯ    ЛИНИЯ     ВРЕМЯ           IDLE    PID     КОММЕНТАРИЙ
root console Dec 12 08:00    .       10340
```

Подробное описание команды приведено в man who.

4.4.2.2. ps

Для получения информации о состоянии запущенных процессов используется команда ps. Команда выводит следующую информацию о процессах:

- выполненные процессы;
- процессы, вызвавшие проблемы в системе;
- как долго выполняется процесс;
- какие системные ресурсы затребовал процесс;
- идентификатор процесса (который будет необходим, например, для прекращения работы процесса с помощью команды kill) и т. д.

Данная информация полезна как для пользователя, так и для системного администратора. Запущенная без параметров командной строки ps выдает список процессов, порожденных администратором.

Наиболее распространенное применение команды ps — отслеживание работы фоновых и других процессов в системе. Поскольку в большинстве случаев фоновые процессы не взаимодействуют с экраном и с клавиатурой, команда ps остается основным средством наблюдения за ними.

В таблице 19 приведены четыре основных поля информации для каждого процесса, выводимые командой ps.

Таблица 19

Поле	Описание
PID	Идентификатор процесса
TTY	Терминал, с которого был запущен процесс
TIME	Время работы процесса
CMD	Имя выполненной команды

Подробное описание команды приведено в `man ps`.

4.4.2.3. nohup

Обычно дочерний процесс завершается после завершения родительского. Таким образом, если запущен фоновый процесс, он будет завершен при выходе из системы. Для того чтобы процесс продолжал выполняться после выхода из системы, применяется команда `nohup`, указанная в начале командной строки:

```
nohup sort sales.dat &
```

Команда `nohup` заставляет ОС игнорировать выход из нее и продолжать выполнение процесса в фоновом режиме, пока он не закончится. Таким образом, будет запущен процесс, который будет выполняться длительное время, не требуя контроля со стороны администратора системы.

Подробное описание команды приведено в `man nohup`.

4.4.2.4. nice

Команда `nice` позволяет предопределять приоритет выполнения процесса (фонового или переднего плана) во время его запуска.

При запуске все процессы имеют одинаковый приоритет и ОС равномерно распределяет между ними процессорное время. С помощью команды `nice` можно понизить приоритет выбранного процесса, предоставив другим процессам больше процессорного времени.

Приоритет выполнения процесса может изменяться от -20 (наивысший приоритет) до 19 (наименьший приоритет). По умолчанию приоритет каждого процесса равен 10.

Повышение приоритета процесса осуществляется от имени администратора.

Синтаксис команды:

```
nice -<число> <команда>
```

Параметр `<число>` определяет на какое значение должен быть изменен приоритет выбранного процесса. Чем больше значение параметра `<число>`, тем меньше будет приоритет выбранного процесса.

Пример

Для процесса сортировки, запущенного командой:

```
sort sales.dat > sales.srt &
```

необходимо повысить приоритет над процессом печати.

Для этого необходимо запустить процесс печати с уменьшенным приоритетом, выполнив команду:

```
nice -5 lp mail_list &
```

Или назначить процессу печати самый низкий приоритет, выполнив команду:

```
nice -10 lp mail_list &
```

Для назначения процессу максимального приоритета -20 необходимо от имени администратора выполнить команду:

```
nice --30 <команда> &
```

Подробное описание команды приведено в `man nice`.

4.4.2.5. renice

Команда `renice` позволяет изменить приоритет запущенного процесса. Повышение приоритета процесса осуществляется от имени администратора.

Синтаксис команды:

```
renice -<число> <PID>
```

где `PID` — идентификатор процесса.

Определить PID можно с помощью команды `ps`:

```
ps -e | grep <имя_процесса>
```

Команда `grep` отфильтрует записи по имени нужного процесса.

Возможно изменить приоритет всех процессов пользователя или группы пользователей, для этого в команде `renice` используется идентификатор пользователя или группы.

Пример

Для изменения приоритета процесса текущего пользователя (`pav`) необходимо:

1) отобразить идентификаторы всех процессов, запущенных текущим пользователем, выполнив команду:

```
ps -ef | grep $LOGNAME
```

Результат выполнения команды:

```
pav 11805 11804 0 Dec 22 ttysb 0:01 sort sales.dat > sales srt
pav 19955 19938 4 16:13:02 ttypo 0:00 grep pav
pav 19938
1 0 16:11:04 ttypo 0-00 bash
pav 19940 19938 42 16:13:02 ttypo 0:33 find . -name core -exec
     nn {};
```

2) уменьшить приоритет процесса `find` с идентификатором 19940, выполнив команду:

```
renice -5 19940
```

Подробное описание команды приведено в `man renice`.

4.4.2.6. kill

Команда `kill` отправляет сигнал указанному процессу или процессам. Каждый сигнал имеет номер и название. Для просмотра всех сигналов необходимо выполнить команду:

```
kill -l
```

Синтаксис команды:

```
kill [-<сигнал>] <PID_1> [<PID_2> [...]]
```

где `<сигнал>` — номер сигнала или его название. Если параметр не задан, то по умолчанию будет применен сигнал с номером 15 (`SIGTERM`) на завершение выполнения процесса;
`<PID_n>` — идентификатор процесса.

С помощью параметра `<сигнал>` можно, например, дать указание процессу перечитать конфигурационные файлы без прекращения работы.

Если процесс работает не в фоновом режиме, нажатие комбинации клавиш **<Ctrl+C>** должно прервать его выполнение. Фоновый процесс прервать возможно только с помощью команды `kill`, посылающей процессу сигнал завершения.

Примеры:

1. Завершить процесс с идентификатором 127:

```
kill -SIGTERM 127
```

или:

```
kill -15 127
```

2. Завершить процессы с идентификаторами 127 и 240:

```
kill 127 240
```

Для завершения процесса, только что запущенного в фоновом режиме, необходимо выполнить команду:

```
kill $!
```

Для завершения всех фоновых процессов необходимо выполнить команду:

```
kill 0
```

При успешном завершении процесса сообщение не выводится. Сообщение появится при попытке завершения процесса без наличия соответствующих прав доступа или при попытке завершить несуществующий процесс.

Завершение родительского процесса приводит к завершению дочерних (кроме запущенных с помощью `nohup`). Однако для полной уверенности в завершении всех процессов, связанных с данным, следует указывать их в команде `kill`.

Некоторые процессы могут игнорировать посылаемые им сигналы, включая сигнал 15 (`SIGTERM`). Сигнал с номером 9 (`SIGKILL`) не может быть проигнорирован процессом, и процесс будет принудительно завершен. Например, если процесс не завершился после выполнения команды:

```
kill <PID_процесса>
```

то необходимо выполнить команду:

```
kill -9 <PID_процесса>
```

После выполнения команды процесс завершится без возможности корректно закрыть файлы, что может привести к потере данных.

Преимущественное право контроля над процессом принадлежит владельцу. Права владельца могут отменяться только суперпользователем.

Ядро назначает каждому процессу четыре идентификатора: реальный и эффективный UID, реальный и эффективный GID. Реальные ID используются для учета использования системных ресурсов, а эффективные — для определения прав доступа. Как правило, реальные и эффективные ID совпадают. Владелец процесса может посылать в процесс сигналы, а также понижать приоритет процесса.

Процесс, приступающий к выполнению другого программного файла, осуществляет один из системных вызовов семейства `exec`. Когда такое случается, эффективные UID и GID процесса могут быть установлены равными UID и GID файла, содержащего образ новой программы, если у этого файла установлены биты смены идентификатора пользователя и идентификатора группы. Системный вызов `exec` — это механизм, с помощью которого такие команды, как `passwd`, временно получают права суперпользователя (команде `passwd` они нужны для того, чтобы изменить `/etc/passwd`).

Подробное описание команды приведено в `man kill`.

5. УПРАВЛЕНИЕ ПРОГРАММНЫМИ ПАКЕТАМИ

В ОС используются программные пакеты (далее по тексту — пакеты) в формате DEB (файлы с расширением `.deb`). Для управления пакетами в режиме командной строки или в эмуляторе терминала в графическом режиме предназначены набор команд нижнего уровня `dpkg` и комплекс программ высокого уровня `apt`, `apt-get`, `apt-cache` и `aptitude`.

В графическом режиме управлять пакетами можно с помощью программы Synaptic (универсальная графическая оболочка для `apt`).

По умолчанию обычный пользователь не имеет права использовать эти инструменты. Для всех операций с пакетами (за исключением некоторых случаев получения информации о пакетах) необходимы права администратора.

Примечание. Права доступа к исполняемым файлам позволяют непривилегированным пользователям запускать их на выполнение, но удалять или модифицировать такие файлы может только администратор. В общем случае приложения устанавливаются в каталог с правами чтения для непривилегированных пользователей.

Средства управления пакетами обеспечивают возможность автоматизированной установки обновлений ОС.

5.1. dpkg

Инструмент командной строки `dpkg` предназначен для операций с пакетами на локальном уровне. С помощью `dpkg` можно устанавливать и удалять пакеты, собирать пакеты из исходных текстов, получать информацию о конкретном пакете и об установленных в системе пакетах.

Для установки пакета выполнить команду:

```
dpkg -i <полное_имя_пакета>
```

Пример

Для установки пакета `nftables_1.0.6-2+deb12u2_amd64.deb`, находящегося в домашнем каталоге пользователя `/home/user1`, выполнить команду:

```
dpkg -i /home/user1/nftables_1.0.6-2+deb12u2_amd64.deb
```

В случае нарушения зависимостей будет выведено сообщение об ошибке, в котором будут перечислены все необходимые пакеты, которые следует установить для разрешения обязательных зависимостей.

Для удаления пакета с сохранением его конфигурационных, пользовательских и других файлов (в случае, если данный пакет не связан зависимостями с другими установленными пакетами) выполнить команду:

```
dpkg -r <имя_пакета>
```

Пример

Для удаления пакета `nftables_1.0.6-2+deb12u2_amd64.deb` выполнить команду:

```
dpkg -r iptables
```

Для удаления пакета и его конфигурационных, пользовательских и других файлов (в случае, если данный пакет не связан зависимостями с другими установленными пакетами) выполнить команду:

```
dpkg -P <имя_пакета>
```

Пример

Для удаления пакета `nftables_1.0.6-2+deb12u2_amd64.deb` и его конфигурационных файлов выполнить команду:

```
dpkg -P iptables
```

При удалении пакета с зависимостями с другими пакетами будет отображено сообщение об ошибке с перечнем зависимостей.

Подробное описание команды приведено в `man dpkg`.

5.2. apt

Инструмент командной строки `apt` предназначен для выполнения операций с пакетами при наличии доступа к настроенным источникам (например, к установочному диску или сетевому репозиторию). Инструмент позволяет устанавливать и удалять пакеты, разрешать зависимости. А также искать пакеты по заданным критериям и просматривать подробную информацию о пакете.

5.2.1. Настройка списка источников (репозиториев)

Информация об источниках пакетов (установочных дисках, сетевых и локальных репозиториях) содержится в файле `/etc/apt/sources.list`. В файле могут быть указаны как активные источники, так и неактивные. Активные источники используются для установки и обновления пакетов. Неактивные источники закомментированы (в начале строки стоит символ «#»). В файле источников могут быть указаны различные виды активных источников и любое их количество. Источники перечисляются по одному на строке в порядке убывания их приоритета.

Пример

```
# deb cdrom:[OS Astra Linux 1.8_x86-64 DVD]/ 4.8_arm contrib main
non-free non-free-firmware
deb https://dl.astralinux.ru/astra/stable/4.8_arm/repository-main/
1.8_x86-64 main contrib non-free non-free-firmware
deb https://dl.astralinux.ru/astra/stable/4.8_arm/repository-update/
1.8_x86-64 main contrib non-free non-free-firmware
```

Описание файла `/etc/apt/sources.list` приведено в `man sources.list`.

После установки ОС в файле `/etc/apt/sources.list` по умолчанию в качестве активного источника указан источник, из которого выполнялась установка ОС. Если при установке ОС были добавлены другие источники, то они также будут присутствовать в файле как активные источники.

При установке ОС с DVD-диска или из ISO-образа в качестве активного источника в файле `/etc/apt/sources.list` будет указан установочный диск:

```
deb cdrom:[OS Astra Linux 4.8_arm DVD]/ 4.8_arm contrib main non-free
     non-free-firmware
```

Добавить данную строку в список источников также можно при помощи следующей команды (при этом DVD-диск с дистрибутивом ОС должен находиться в устройстве чтения CD/DVD-дисков, монтировать его не обязательно):

```
sudo apt-cdrom add
```

Добавление и удаление источников, а также настройка их использования (сделать активными или неактивными, изменить приоритет) выполняется путем редактирования файла `/etc/apt/sources.list` в любом текстовом редакторе. Сохранение изменений файла доступно только администратору.

После установки ОС создается локальная БД с информацией об установленных пакетах и обо всех пакетах из источников, которые использовались при установке и были указаны при установке. При внесении изменений в файл источников `/etc/apt/sources.list`, а также при изменении содержимого этих источников должна быть обновлена локальная БД. Обновление локальной БД выполняется командой:

```
sudo apt update
```

5.2.2. Установка и удаление пакетов

Для управления пакетами используется инструмент командной строки `apt`.

Перед установкой пакета или получением информации о пакете рекомендуется обновить содержимое локальной БД (см. 5.2.1). Для этого необходимо выполнить команду:

```
sudo apt update
```

Для получения информации о пакете выполнить команду:

```
apt show <имя_пакета>
```

Пример

Для просмотра информации о пакете `iptables` выполнить команду:

```
apt show iptables
```

Установка отдельного пакета выполняется командой:

```
sudo apt install <имя_пакета>
```

При этом будут проверены и разрешены все обязательные зависимости и, при необходимости, установлены необходимые дополнительные пакеты.

Удаление пакета (с сохранением его конфигурационных файлов) выполняется командой:

```
sudo apt remove <имя_пакета>
```

Для удаления пакета вместе с его конфигурационными файлами (кроме конфигурационных файлов из домашних каталогов пользователей) применяется команда:

```
sudo apt remove --purge <имя_пакета>
```

Полное описание инструмента `apt` приведено в `man apt`.

Описание обновления установленных в ОС пакетов приведено в 2.5.

6. БАЗОВЫЕ СЕТЕВЫЕ СЛУЖБЫ

6.1. Протокол TCP/IP

6.1.1. Пакеты и сегментация

Данные передаются по сети в форме сетевых пакетов, каждый из которых состоит из заголовка и полезной нагрузки. Заголовок содержит сведения о том, откуда прибыл пакет и куда он направляется. Заголовок, кроме того, может включать контрольную сумму, информацию, характерную для конкретного протокола, и другие инструкции по обработке. Полезная нагрузка — это данные, подлежащие пересылке.

6.1.2. Адресация пакетов

Сетевые пакеты могут достичь пункта назначения только при наличии правильного сетевого адреса. Протокол TCP/IP использует сочетание нескольких схем сетевой адресации.

Самый нижний уровень адресации задается сетевыми аппаратными средствами.

На следующем, более высоком, уровне используется адресация Интернет (которую чаще называют «IP-адресацией»). Каждому включенному в сеть устройству присваивается один четырехбайтовый IP-адрес (в соответствии с протоколом IPv4). IP-адреса глобально уникальны и не зависят от аппаратных средств.

IP-адреса идентифицируют компьютер, но не обеспечивают адресацию отдельных процессов и служб. Протоколы TCP и UDP расширяют IP-адреса, используя порты. Порт в данном случае представляет собой двухбайтовое число, добавляемое к IP-адресу и указывающее конкретного адресата той или иной сетевой службы. Все стандартные UNIX-службы связываются с известными портами, которые определены в файле `/etc/services`. Для того чтобы предотвратить попытки нежелательных процессов замаскироваться под эти службы, установлено, что порты с номерами до 1024 могут использоваться только суперпользователем. Описание файла `/etc/services` приведено в `man services`.

6.1.3. Маршрутизация

6.1.3.1. Таблица

Маршрутизация — это процесс направления пакета по ряду сетей, находящихся между источником и адресатом.

Данные маршрутизации хранятся в таблице маршрутизации. Каждый элемент этой таблицы содержит несколько параметров, включая поле метрики, в котором указано значение приоритета маршрута на определенном сетевом интерфейсе (если таблица содержит противоречивую информацию). Для направления пакета по конкретному адресу подбирается

наиболее подходящий маршрут. Если нет такого маршрута и нет маршрута по умолчанию, то отправителю возвращается ошибка «network unreachable» (сеть недоступна).

Таблицу маршрутизации компьютера можно вывести на экран монитора с помощью команды `route`.

6.1.3.2. Организация подсетей

Организация подсетей задается маской подсети, в которой биты сети включены, а биты компьютера выключены. Маска подсети задается во время начальной загрузки, когда конфигурируется сетевой интерфейс командой `ifconfig`. Ядро, как правило, использует сам класс IP-адресов для того, чтобы выяснить, какие биты относятся к сетевой части адреса; если задать маску явно, то эта функция просто отменяется.

При организации подсетей необходимо учесть, что если вычислительная сеть имеет более одного соединения с сетью Интернет, то другие сети должны уметь отличать подсети сети пользователя, чтобы определить в какой маршрутизатор следует послать пакет.

6.1.4. Создание сети TCP/IP

Процесс создания сети TCP/IP состоит из следующих этапов:

- планирование сети;
- назначение IP-адресов;
- настройка сетевых интерфейсов;
- настройка статических маршрутов.

6.1.4.1. Планирование сети

Планирование сети включает:

- определение сегментов сети;
- определение технических и программных средств, с помощью которых сегменты объединяются в сеть;
- определение серверов и рабочих станций, которые будут установлены в каждом сегменте;
- определение типа среды (витая пара и др.).

6.1.4.2. Назначение IP-адресов

Адреса назначают сетевым интерфейсам, а не компьютерам. Если у компьютера есть несколько физических интерфейсов, то у него будет несколько сетевых адресов.

Существует возможность создания виртуального сетевого интерфейса (loopback), который реализован программно и не связан с оборудованием, но при этом полностью интегрирован во внутреннюю сетевую инфраструктуру компьютерной системы.

Для того, чтобы можно было обращаться к компьютерам по их именам рекомендуется использовать службу DNS, также соответствие между именем и IP-адресом может быть задано в файле `/etc/hosts` на компьютере, с которого выполняется обращение.

6.1.4.3. Настройка сетевых интерфейсов

Инструмент `ifconfig` используется для включения и выключения сетевого интерфейса, задания IP-адреса, широковещательного адреса и связанной с ним маски подсети, а также для установки других параметров. Он обычно используется при первоначальной настройки, но может применяться и для внесения изменений в дальнейшем.

Если в конфигурационном файле `/etc/default/grub` для параметра `GRUB_CMDLINE_LINUX` отсутствует значение или установлено значение `net.ifnames=1`, то для сетевых интерфейсов используется схема назначения предсказуемых имен (`enp0s3`, `wlp2s0` и т.д.).

Если в конфигурационном файле `/etc/default/grub` для параметра `GRUB_CMDLINE_LINUX` установлено значение `net.ifnames=0`, то используются имена интерфейсов вида `eth*` (`eth0`, `eth1` и т.д.), номера интерфейсам будут присвоены в порядке их обнаружения при загрузке. По умолчанию в ОС для сетевых интерфейсов используется схема назначения предсказуемых имен. Подробное описание именования интерфейсов приведено в `man systemd.net-naming-scheme` и в `man systemd.link`.

В большинстве случаев команда имеет следующий формат:

```
ifconfig интерфейс [семейство] <адрес> up <параметр> ...
```

Пример

```
ifconfig enp0s3 128.138.240.1 up netmask 255.255.255.0 \
     broadcast 128.138.240.255
```

Здесь интерфейс обозначает аппаратный интерфейс, к которому применяется команда. Примеры распространенных имен `enp0s3`, `eth1`, `lo0`, `ppp0` образуются из имени драйвера устройства, используемого для управления им. Для того чтобы выяснить, какие интерфейсы имеются в системе, можно воспользоваться командой:

```
netstat-i
```

Параметр `up` включает интерфейс, а параметр `down` выключает его.

Описание инструмента приведено в `man ifconfig`.

6.1.4.4. Настройка статических маршрутов

Инструмент `route` определяет статические маршруты — явно заданные элементы таблицы маршрутизации, которые обычно не меняются даже в тех случаях, когда запускается серверный процесс маршрутизации.

Маршрутизация выполняется на уровне IP. Когда поступает пакет, предназначенный для другого компьютера, IP-адрес пункта назначения пакета сравнивается с маршрутами, указанными в таблице маршрутизации ядра. Если номер сети пункта назначения совпадает с номером сети какого-либо маршрута, то пакет направляется по IP-адресу следующего шлюза, связанного с данным маршрутом.

Существующие маршруты можно вывести на экран.

Описание инструмента приведено в `man route`.

6.1.5. Проверка и отладка сети

6.1.5.1. ping

Инструмент `ping` служит для проверки соединений в сетях на основе TCP/IP.

После команды запуска он работает в бесконечном цикле, если не задан параметр `-c`, определяющий количество пакетов, после передачи которого команда завершает свое выполнение. Чтобы прекратить работу `ping`, необходимо нажать **<Ctrl+C>**.

Описание инструмента приведено в `man ping`.

6.1.5.2. netstat

Инструмент `netstat` выдает информацию о состоянии, относящуюся к сетям:

- проверка состояния сетевых соединений;
- анализ информации о конфигурации интерфейсов;
- изучение таблицы маршрутизации;
- получение статистических данных о различных сетевых протоколах.

Команда запуска `netstat` без параметров выдает информацию о состоянии активных портов TCP и UDP. Неактивные серверы, ожидающие установления соединения, как правило, не показываются (их можно просмотреть командой `netstat -a`).

Основные параметры `netstat`:

1) `-i` — показывает состояние сетевых интерфейсов;
2) `-r` — выдает таблицу маршрутизации ядра;
3) `-s` — выдает содержимое счетчиков, разбросанных по сетевым программам.

Описание инструмента приведено в `man netstat`.

6.1.5.3. arp

Инструмент `arp` обращается к таблице ядра, в которой задано соответствие IP-адресов аппаратным адресам. В среде Ethernet таблицы ведутся с помощью протокола ARP и не требуют администрирования.

Команда:

```
arp -a
```

выводит содержимое таблицы соответствий.

Описание инструмента приведено в `man arp`.

6.2. Протокол FTP

В ОС передача файлов обеспечивается с помощью интерактивного инструмента `lftp`, запускаемого на клиентской стороне, и серверной службы `vsftpd`, которая запускается на компьютере, выполняющем функцию сервера FTP. Инструмент и служба реализуют протокол передачи файлов FTP. Для копирования файлов клиенту обычно необходимо знание имени и пароля пользователя (хотя существует и вариант анонимного доступа), которому принадлежат файлы на сервере FTP.

6.2.1. Клиентская часть

Клиентская часть может быть установлена командой:

```
apt install lftp
```

Запуск инструмента `lftp` осуществляется командой:

```
lftp <имя_сервера>
```

Интерактивный доступ к серверу службы FTP обеспечивается следующими основными внутренними командами `lftp`:

1) `open`, `user`, `close` — связь с удаленным компьютером;
2) `lcd`, `dir`, `mkdir`, `lpwd` — работа с каталогами в FTP-сервере;
3) `get`, `put`, `ftpcopy` — получение и передача файлов;
4) `ascii`, `binary`, `status` — установка параметров передачи.

Выход из инструмента `lftp` осуществляется по команде `exit`.

Описание инструмента приведено в `man lftp`.

6.2.2. Служба vsftpd сервера FTP

В ОС служба `vsftpd` устанавливается командой:

```
apt install vsftpd
```

После установки службы `vsftpd` по умолчанию в конфигурационном файле `/etc/vsftpd.conf` указаны параметры для работы с включенной IPv4- и IPv6-адресацией — для параметров `listen` и `listen_ipv6` установлены следующие значения:

```
listen=NO
listen_ipv6=YES
```

Для приема соединения как от клиентов IPv4, так и от клиентов IPv6 достаточно, чтобы для параметра `listen_ipv6` было установлено значение `YES`, при этом значение параметра `listen` всегда будет интерпретироваться как `YES`.

Если в системе включена IPv6-адресация, то служба `vsftpd` запускается автоматически без дополнительных настроек.

Если в системе отключена IPv6-адресация или необходимо использовать только IPv4-адресацию, то для запуска службы `vsftpd` требуется отредактировать файл `/etc/vsftpd.conf` — для параметров `listen` и `listen_ipv6` должны быть установлены следующие значения:

```
listen=YES
listen_ipv6=NO
```

Для настройки `vsftpd` не требуется указывать все доступные параметры, а достаточно указать только те, значения которых следует переопределить. Параметры, не указанные

явным образом в файле /etc/vsftpd.conf, будут принимать значения по умолчанию. Значения, принимаемые по умолчанию, приведены в man vsftpd.conf.

В конфигурационном файле /etc/vsftpd.conf присутствуют параметры, которые зависят от других параметров. Если один параметр, от которого зависит другой, отключен, то и зависимый параметр также будет отключен. Например, если параметр local_enable, позволяющий авторизоваться локальным пользователям, будет отключен, то зависящий от него параметр local_umask также будет отключен.

Для запуска службы vsftpd с параметрами, отличными от указанных в файле /etc/vsftpd.conf, необходимо использовать инструмент командной строки vsftpd. Таким образом, если значение параметра, переданное в командной строке, не совпадает с указанным в конфигурационном файле, то будет применено значение параметра, указанное в командной строке, так как оно имеет приоритет над указанным в конфигурационном файле. Значения параметров, указанных в командной строке, применяются последовательно.

После установки службы vsftpd создается каталог с документацией службы /usr/share/doc/vsftpd, где каталог examples содержит примеры конфигурационного файла vsftpd.conf.

Описание службы vsftpd и файла /etc/vsftpd.conf приведено в man vsftpd и man vsftpd.conf соответственно.

6.3. Протокол DHCP

На компьютере, выполняющем роль сервера динамической конфигурации сетевых подключений компьютеров, должна быть установлена служба DHCP-сервера. Данная служба также может использоваться для предоставления адресов серверов сетевой загрузки. Описание сетевой загрузки приведено в документе РУСБ.10015-01 95 01-2 «Операционная система специального назначения «Astra Linux Special Edition». Руководство администратора. Часть 2. Установка и миграция».

В состав ОС входит DHCP-сервер Kea, который представлен пакетом kea и дополнительными пакетами, необходимыми для настройки и работы службы DHCP. Перечень пакетов и их описание приведены в таблице 20.

Таблица 20

Пакет	Описание
kea	Метапакет, включающий в себя основные компоненты DHCP-сервера Kea, такие как сервер DHCP (позволяющий назначать IP-адреса IPv4 или IPv6), агент управления и другие компоненты

Окончание таблицы 20

Пакет	Описание
`kea-admin`	Инструмент для управления базой данных DHCP-сервера Kea. Позволяет выполнять миграции базы данных пользователей, управлять пользователями и паролями, а также настраивать резервное копирование данных
`kea-common`	Общие библиотеки и конфигурационные файлы, которые используются всеми компонентами DHCP-сервера Kea. Этот пакет необходим для работы всех других модулей Kea
`kea-ctrl-agent`	Агент управления, который предоставляет интерфейс для управления DHCP-сервером Kea через HTTP-запросы. Позволяет изменять конфигурации, получать статистику и выполнять иные действия
`kea-dhcp-ddns-server`	Сервер динамических обновлений DNS (DHCP-DDNS), который отвечает за отправку обновлений на DNS-серверы при изменении состояния аренды IP-адресов клиентами (например, при аренде нового адреса)
`kea-dhcp4-server`	DHCP-сервер Kea для предоставления IP-адресов IPv4 и других сетевых параметров клиентам
`kea-dhcp6-server`	DHCP-сервер Kea для предоставления IP-адресов IPv6 и других сетевых параметров клиентам
`python3-kea-connector`	Инструмент для интеграции DHCP-сервера Kea с приложениями на языке Python. Предоставляет возможности управления компонентами DHCP-сервера Kea для автоматизации процессов

Для установки DHCP-сервера выполнить команду от имени администратора с использованием механизма `sudo`:

```
sudo apt install kea
```

При установке пакета `kea` также автоматически будут установлены необходимые дополнительные пакеты.

После установки служба DHCP-сервера запускается автоматически и настроена на автоматический запуск после перезагрузки ОС. Чтобы убедиться, что служба добавлена в автоматический запуск, возможно выполнить следующую команду:

```
systemctl is-enabled kea-dhcp4-server
```

Будет выведено сообщение:

```
enabled
```

Настройки службы DHCP-сервера задаются в файлах:

- `/etc/kea/kea-dhcp4.conf` — конфигурационный файл, который определяет параметры работы DHCP-сервера Kea, предоставляющего IP-адреса IPv4;
- `/etc/kea/kea-dhcp6.conf` — конфигурационный файл, который определяет параметры работы DHCP-сервера Kea, предоставляющего IP-адреса IPv6;
- `/etc/kea/kea-ctrl-agent.conf` — конфигурационный файл, который позволяет настроить работу агента управления DHCP-сервера Kea;
- `/etc/kea/kea-dhcp-ddns.conf` — конфигурационный файл, который позволяет настроить динамическое обновление DNS-записей на основе предоставленных DHCP-сервером Kea IP-адресов.

Для базовой настройки DHCP-сервера с назначением IP-адресов IPv4 достаточно задать следующие параметры в конфигурационном файле `/etc/kea/kea-dhcp4.conf`:

- интерфейс для работы DHCP-сервера;
- диапазон выдаваемых IP-адресов и параметры подсети;
- период аренды IP-адреса.

Интерфейс для работы DHCP-сервера, период аренды IP-адреса (`valid-lifetime`), запрос на продление аренды (`renew-timer`), а также время до попытки повторного получения IP-адреса после неуспешных попыток запроса на продление аренды (`rebind-timer`), необходимо указать в конфигурационном файле `/etc/kea/kea-dhcp4.conf` в секции `Dhcp4`:

```
"Dhcp4": {

"interfaces-config": {

        "interfaces": [ "<наименование_интерфейса>" ]
    },

    ...

    },

    "renew-timer": <секунды>,
    "rebind-timer": <секунды>,
    "valid-lifetime": <секунды>,
    ...
```

Параметры подсети, диапазон выдаваемых IP-адресов, шлюз по умолчанию и IP-адреса DNS-серверов необходимо указать в конфигурационном файле `/etc/kea/kea-dhcp4.conf` в секции `subnet4`:

```
"subnet4": [
    {
    "subnet": "<IP-адрес_подсети/маска_подсети>",
    "pools": [ { "pool": "<начальный_IP-адрес> - <конечный_IP-адрес>" } ],
    "option-data": [
          {
              "name": "routers",
              "data": "<IP-адрес_шлюза_по_умолчанию>"
          }
    ],

    ...

          {

              "option-data": [ {
                  "name": "domain-name-servers",
                  "data": "<IP-адрес_основного_DNS-сервера>,
                  <IP-адрес_дополнительного_DNS-сервера>"
              } ]
              ...
    }
```

После задания параметров в конфигурационном файле `/etc/kea/kea-dhcp4.conf` необходимо перезапустить службу DHCP-сервера:

```
sudo systemctl restart kea-dhcp4-server
```

Для проверки статуса DHCP-сервера выполнить команду:

```
systemctl status kea-dhcp4-server
```

Описание основных параметров настройки DHCP-сервера, содержащихся в файле `/etc/kea/kea-dhcp4.conf`, приведено в таблице 21.

Таблица 21

Параметр	Описание
interfaces-config.interfaces	Указывает сетевые интерфейсы, через которые сервер будет обрабатывать DHCP-запросы
subnet4.subnet	Определяет адрес подсети и маску подсети в формате CIDR (например, 192.168.1.0/24)
subnet4.pools.pool	Указывает диапазон IP-адресов, которые могут быть выданы клиентам (например, 192.168.1.100 – 192.168.1.150)
subnet4.option-data.name	Указывает наименование параметра DHCP (например, шлюз по умолчанию или широковещательный адрес)
subnet4.option-data.data	Определяет значение для параметра DHCP (например, IP-адрес шлюза по умолчанию)
lease-database.type	Задает тип базы данных для хранения информации о выданных IP-адресах (например, memfile или mysql)
lease-database.lfc-interval	Задает интервал для выполнения процесса очистки устаревших данных в БД при использовании типа memfile в параметре lease-database.type (в секундах)
reservations.hw-adress	Определяет MAC-адрес устройства, для которого будет зарезервирован IP-адрес
reservations.ip-adress	Определяет IP-адрес, который будет выделен устройству с указанным MAC-адресом
loggers.name	Задает имя файла для регистрации системных событий
loggers.output_options.syslog	Задает параметры выходного файла для регистрации системных событий (например, stdout или syslog)
loggers.severity	Задает уровень регистрации системных событий (например, ERROR или INFO)
valid-lifetime	Задает максимально допустимое время аренды IP-адреса (в секундах)
renew-timer	Задает время до первой попытки запроса на продление аренды IP-адреса (в секундах)
rebind-timer	Задает время до попытки заново привязать аренду IP-адреса после неудачных попыток запроса на продление аренды (в секундах)

Описание основных параметров настройки агента управления DHCP-сервера, содержащихся в файле /etc/kea/kea-ctrl-agent.conf, приведено в таблице 22.

Таблица 22

Параметр	Описание
`http-host`	Определяет IP-адрес, на котором будет работать HTTP-сервер агента управления (например, `127.0.0.1` — доступ с локального узла, `0.0.0.0` — доступ с любого узла)
`http-port`	Определяет порт, на котором будет работать HTTP-сервер агента управления
`control-sockets.dhcp4`	Указывает путь к Unix-сокету, который используется для передачи команд и получения ответов от DHCP-сервера, предоставляющего IP-адреса IPv4
`control-sockets.dhcp6`	Указывает путь к Unix-сокету, который используется для передачи команд и получения ответов от DHCP-сервера, предоставляющего IP-адреса IPv6
`control-sockets.d2`	Указывает путь к Unix-сокету, который используется для передачи команд и получения ответов от сервера Dynamic DNS (D2)
`hooks-libraries`	Указывает пути к библиотекам расширений (`hooks`), которые могут быть загружены агентом управления. Библиотеки позволяют расширить функциональность DHCP-сервера
`loggers.name`	Задает имя файла для регистрации системных событий
`loggers.output_options.output`	Указывает, куда будут выводится регистрируемые события (например, в файл или консоль)
`loggers.output_options.pattern`	Определяет шаблон для регистрируемых событий
`loggers.severity`	Задает уровень регистрации событий (например, `ERROR` или `INFO`)
`loggers.debuglevel`	Определяет уровень детализации для сообщений отладки (от `0` до `99`) в случае, если для параметра `loggers.severity` установлено значение `DEBUG`. Чем больше число, тем больше будет уровень детализации

Описание основных параметров настройки сервера динамических обновлений DNS (DHCP-DDNS), содержащихся в файле `/etc/kea/kea-dhcp-ddns.conf`, приведено в таблице 23.

Таблица 23

Параметр	Описание
`ip-address`	Определяет IP-адрес, на котором будет работать DDNS-сервер
`port`	Определяет порт, на котором будет работать DDNS-сервер
`control-socket.socket-type`	Определяет тип сокета для связи с контроллером Kea

Окончание таблицы 23

Параметр	Описание
`control-socket.socket-name`	Определяет имя или путь к сокету для взаимодействия с Kea через контроллер
`tsig-keys`	Указывает ключи TSIG (Transaction SIGnature), которые необходимы для защищенных обновлений DNS
`forward-ddns`	Определяет параметры для обновления прямых DNS-записей (`forward lookup`)
`reverse-ddns`	Определяет параметры для обновления обратных DNS-записей (`reverse lookup`)
`loggers.name`	Определяет имя компонента, для которого настраивается регистрация событий
`loggers.output_options.output`	Указывает, куда будут выводится регистрируемые события (например, в файл или консоль)
`loggers.output_options.pattern`	Определяет шаблон для регистрируемых событий
`loggers.severity`	Задает уровень регистрации событий (например, `ERROR` или `INFO`)
`loggers.debuglevel`	Определяет уровень детализации для сообщений отладки (от `0` до `99`) в случае, если для параметра `loggers.severity` установлено значение `DEBUG`. Чем больше число, тем больше будет уровень детализации

6.4. Протокол NFS

Протокол NFS обеспечивает общий доступ к файлам и каталогам *nix-систем (в т. ч. Linux), что позволяет использовать ФС удаленных компьютеров.

В ОС используется реализация службы NFS, работающая на уровне ядра и представленная пакетом `nfs-kernel-server`.

Доступ к ФС удаленных компьютеров обеспечивается с помощью программ на сторонах сервера и клиента.

При работе с сетевой ФС любые операции над файлами, производимые на локальном компьютере, передаются через сеть на удаленный компьютер.

В протоколе NFSv4.x реализована поддержка списков контроля доступа (ACL), которые концептуально похожи на списки контроля доступа, используемые в ОС. При этом ACL в NFSv4.x могут содержать отрицательные права (отказ в доступе), имеют больше типов разрешений и менее строгую структуру наследования прав.

Особенности применения ACL в NFSv4.x представлены в документе РУСБ.10015-01 97 01-1.

6.4.1. Установка и настройка сервера

Для установки сервера выполнить от имени администратора команды:

```
apt update
apt install nfs-kernel-server
```

Для нормального запуска и возобновления работы службы сервера NFS требуется после установки пакета и перезагрузки компьютера внести изменения в UNIT-файл `/etc/systemd/system/multi-user.target.wants/nfs-server.service`, добавив следующие строки в секцию `unit`:

```
[Unit]
Requires=rpcbind.service
After=rpcbind.service
```

Затем перезапустить службу, выполнив команды:

```
systemctl daemon-reload
systemctl restart nfs-kernel-server
```

На стороне сервера существуют следующие программы, используемые для обеспечения службы NFS:

- `rpc.idmapd` — перенаправляет обращения, сделанные с других компьютеров к службам NFS;
- `rpc.nfsd` — переводит запросы к службе NFS в действительные запросы к локальной ФС;
- `rpc.svcgssd` — поддерживает создание защищенного соединения;
- `rpc.statd` — поддерживает восстановление соединения при перезагрузке сервера;
- `rpc.mountd` — запрашивается для монтирования и размонтирования ФС.

Описание программ приведено на страницах руководства `man`.

Запросы монтирования поступают от клиентских компьютеров к серверу монтирования `mountd`, который проверяет правильность клиентского запроса на монтирование и разрешает серверу службы NFS (`nfsd`) обслуживать запросы клиента, выполнившего монтирование. Клиенту разрешается выполнять различные операции с экспортированной ФС в пределах своих полномочий. Для получения хорошего качества обслуживания клиентов рекомендуется на сервере службы NFS одновременно запускать несколько копий процесса `nfsd`.

На стороне сервера выполняется экспортирование ФС. Это означает, что определенные поддеревья, задаваемые каталогами, объявляются доступными для клиентских компьютеров. Информация об экспортированных ФС заносится в файл `/etc/exports`, в котором указывается, какие каталоги доступны для определенных клиентских компьютеров, а также какими правами доступа обладают клиентские компьютеры при выполнении операций на сервере. В конфигурационный файл `/etc/exports` информация заносится строкой вида:

```
<общий_каталог> <IP-адрес_клиента>(<параметр>)
```

Параметр определяет правила монтирования общего ресурса для клиента. Если параметров несколько, то они указываются через запятую. Перечень параметров и их описание приведены в таблице 24.

Таблица 24

Параметр	Описание
`rw`	Предоставляет права на чтение и запись
`ro`	Предоставляет права только на чтение
`no_root_squash`	По умолчанию в общих ресурсах NFS пользователь `root` становится обычным пользователем (`nfsnobody`). Таким образом, владельцем всех файлов, созданных `root`, становится `nfsnobody`, что предотвращает загрузку на сервер программ с установленным битом `setuid`. Если указан параметр `no_root_squash`, то удаленные пользователи `root` могут изменить любой файл в разделяемой файловой системе и внести вредоносный код для других пользователей. В целях безопасности рекомендуется этот параметр не использовать
`nohide`	Служба NFS автоматически не показывает нелокальные ресурсы (например, примонтированные с помощью `mount --bind`). Данный параметр включает отображение таких ресурсов
`sync`	Синхронный режим доступа. Указывает, что сервер должен отвечать на запросы только после записи на диск изменений, выполненных этими запросами
`async`	Асинхронный режим доступа. Указывает серверу не ждать записи информации на диск и давать ответ на запрос сразу. Использование этого режима повышает производительность, но понижает надежность, т.к. в случае обрыва соединения или отказа оборудования возможна потеря данных
`noaccess`	Запрещает доступ к указанному каталогу. Применяется, если доступ к определенному каталогу выдан всем пользователям сети, но при этом необходимо ограничить доступ для отдельных пользователей
`all_squash`	Подразумевает, что все подключения будут выполняться от анонимного пользователя

Окончание таблицы 24

Параметр	Описание
subtree_check	Выполняет контроль поддерева — позволяет экспортировать не весь раздел, а лишь его часть. При этом сервер NFS выполняет дополнительную проверку обращений клиентов для проверки, что они предпринимают попытку доступа к файлам, находящимся в соответствующих подкаталогах. Параметр subtree_check включен по умолчанию
no_subtree_check	Отменяет контроль поддерева. Не рекомендуется использовать данный параметр, т. к. может быть нарушена безопасность системы. Параметр может применяться в том случае, если экспортируемый каталог совпадает с разделом диска
anonuid=1000	Привязывает анонимного пользователя к локальному UID
anongid=1000	Привязывает анонимную группу пользователя к локальной группе GID

Пример

Описание в конфигурационном файле /etc/exports экспорта совместно используемого каталога /nfsshare

```
/srv/nfsshare 192.168.1.20/255.255.255.0(rw,nohide,all_squash,
     anonuid=1000,anongid=1000,no_subtree_check)
```

ВНИМАНИЕ! Использование пробелов между IP-адресом/именем клиента и правами его доступа в файле /etc/exports влечет изменение трактовки прав доступа. Например, строка:

```
/tmp/nfs/ master.astralinux.ru(rw)
```

предоставляет ресурсу master.astralinux.ru права на доступ и чтение, в то время как строка:

```
/tmp/nfs/ master.astralinux.ru (rw)
```

предоставляет ресурсу master.astralinux.ru права только на чтение, а всем остальным — на чтение и запись.

После внесения изменений в файл /etc/exports необходимо выполнить команду:

```
exportfs -ra
```

6.4.2. Установка и настройка клиента

Для установки клиента выполнить на компьютере от имени администратора команды:

```
apt update
apt install nfs-common
```

После установки пакета `nfs-common` на клиенте возможно примонтировать совместно используемые ресурсы. Список доступных ресурсов можно проверить, выполнив команду:

```
showmount -e <IP-адрес_сервера>
```

Для монтирования совместно используемого ресурса на клиенте выполнить команду:

```
mount <IP-адрес_сервера>:<общий_каталог> <каталог_монтирования>
```

где `<IP-адрес_сервера>` — имя сервера NFS;
`<общий_каталог>` — экспортированный каталог сервера NFS;
`<каталог_монтирования>` — каталог монтирования на клиенте.

На стороне клиента для поддержки службы NFS используется модифицированная команда `mount` (если указывается ФС NFS4, то автоматически вызывается команда `mount.nfs4`). Команда модифицирована таким образом, чтобы она могла понимать запись:

```
<IP-адрес_сервера>:<общий_каталог>
```

Для удаленных ФС, которые являются частью постоянной конфигурации клиента и должны автоматически монтироваться во время начальной загрузки клиента, должны присутствовать соответствующие строки в файле `/etc/fstab` клиента, например:

```
192.168.1.10:/srv/nfsshare/    /mnt/share nfs rw,sync,hard,intr 0 0
```

Кроме того, для поддержки защищенных соединений на клиентской стороне должна запускаться команда `rpc.gssd`.

6.5. DNS

Система доменных имен DNS (Domain Name System) представляет собой иерархическую распределенную систему для получения информации о компьютерах, службах и ресурсах, входящих в глобальную или приватную компьютерную сеть. Чаще всего используется

для получения IP-адреса по имени компьютера или устройства, получения информации о маршрутизации почты и т. п.

Основой DNS является представление об иерархической структуре доменного имени и зонах. Распределенная база данных DNS поддерживается с помощью иерархии DNS-серверов, взаимодействующих по определенному протоколу. Каждый сервер, отвечающий за имя, может делегировать ответственность за дальнейшую часть домена другому серверу, что позволяет возложить ответственность за актуальность информации на серверы различных организаций (людей), отвечающих только за «свою» часть доменного имени.

Основными важными понятиями DNS являются:

- домен (область) — именованная ветвь или поддерево в дереве имен. Структура доменного имени отражает порядок следования узлов в иерархии; доменное имя читается справа налево от младших доменов к доменам высшего уровня (в порядке повышения значимости);
- полное имя домена (FQDN) — полностью определенное имя домена. Включает в себя имена всех родительских доменов иерархии DNS;
- зона — часть дерева доменных имен (включая ресурсные записи), размещаемая как единое целое на некотором сервере доменных имен;
- DNS-запрос — запрос от клиента (или сервера) серверу для получения информации.

Служба доменных имен `named` предназначена для генерации ответов на DNS-запросы. Существуют два типа DNS-запросов:

- прямой — запрос на преобразование имени компьютера в IP-адрес;
- обратный — запрос на преобразование IP-адреса в имя компьютера.

6.5.1. Установка DNS-сервера

В ОС используется DNS-сервер BIND9. Для установки службы DNS-сервера выполнить в терминале команду:

```
apt install bind9
```

При установке пакета `bind9` будет автоматически уставновлен пакет инструментов командной строки `bind9utils`, включающий:

- `named-checkconf` — инструмент проверки синтаксиса файлов конфигурации;
- `named-checkzone` — инструмент проверки файлов зон DNS;
- `rndc` — инструмент управления службой DNS.

Дополнительно также рекомендуется установить пакет инструментов командной строки для работы с DNS `dnsutils`, выполнив команду:

```
apt install dnsutils
```

В составе пакета `dnsutils` будут установлены следующие инструменты:

- `dig` — инструмент для опроса DNS-серверов и проверки их ответа;
- `nslookup` — инструмент для проверки преобразования имен в IP-адреса (разрешение имен);
- `nsupdate` — инструмент для динамического обновления записей DNS.

ВНИМАНИЕ! При установке службы DNS-сервера будут автоматически созданы учетная запись пользователя `bind` и группа `bind`. Соответственно, служба будет работать от имени `bind:bind`.

6.5.2. Настройка сервера службы доменных имен `named`

Конфигурационные параметры службы `named` хранятся в файлах каталога `/etc/bind/`, перечень конфигурационных файлов приведен в таблице 25.

Таблица 25 – Конфигурационные файлы службы доменных имен `named`

Файл	Описание
`/etc/bind/named.conf`	Основной конфигурационный файл. Содержит значения конфигурационных параметров для всего сервера и ссылки на другие конфигурационные файлы
`/etc/bind/named.conf.options`	Конфигурационный файл основных параметров сервера, основным из которых является параметр `directory`, содержащий каталог конфигурационных файлов зон. Значение по умолчанию `/var/cache/bind`
`/etc/bind/named.conf.local`	Конфигурационный файл описания локальных зон сервера. Для каждой зоны указываются пути к конфигурационным файлам для прямого и обратного разыменования (как правило, в указанном ранее каталоге `/var/cache/bind`)
`/etc/bind/named.conf.default-zones`	Конфигурационный файл зон по умолчанию. В частности, в этом файле содержатся ссылки на автоматически созданные файлы конфигурации `/etc/bind/db.local` и `/etc/bind/127.db` зоны `localhost`. В большинстве случаев не требует правки

Настройка сервера доменных имен является сложной задачей. Перед использованием DNS следует ознакомиться с существующей документацией, файлами помощи и страницами

руководства man службы named, конфигурационного файла named.conf и сопутствующих утилит.

Далее приведен типовой пример настройки службы доменных имен named, обслуживающей одну доменную зону. Пример достаточен для демонстрации функционирующего домена ЕПП ОС.

Примечание. Обновление конфигурации сервера может выполняться без перезапуска самой службы доменных имен named вызовом:

```
rndc reload
```

Пример

Настройка сервера DNS домена my.dom подсети 192.168.1.

В конфигурационный файл /etc/bind/named.conf.local необходимо добавить следующие строки:

```
zone "my.dom" {
        type master;
        file "/var/cache/bind/db.my.dom";
};

zone "1.168.192.in-addr.arpa" {
        type master;
        file "/var/cache/bind/db.192.168.1";
};
```

Примечание. Имена конфигурационных файлов следует выбирать так, чтобы было понятно для какой конфигурации они используются. В приведенном примере имя конфигурационного файла для зоны обратного просмотра может быть, например, /var/cache/bind/1.168.192.in-addr.arpa.zone или /var/cache/bind/db.my.dom.inv.

Конфигурационный файл /var/cache/bind/db.my.dom содержит информацию зоны прямого просмотра:

```
;
; BIND data file for my.dom zone
;
$TTL    604800
@       IN      SOA     my.dom. root.my.dom. (
                         2014031301     ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
```

```
                          604800 )       ; Negative Cache TTL
;
@       IN      NS      server.my.dom.
@       IN      A       192.168.1.100
@       IN      MX      1       server.my.dom.

server          IN      A       192.168.1.100
client1         IN      A       192.168.1.101
client2         IN      A       192.168.1.102
client3         IN      A       192.168.1.103

ns      IN      CNAME   server
;gw CNAMEs
ftp     IN      CNAME   server
repo    IN      CNAME   server
ntp     IN      CNAME   server

_https._tcp  IN SRV     10 10 443 server.my.com.

client1      IN TXT    "MAKS"
```

Конфигурационный файл `/var/cache/bind/db.192.168.1` содержит информацию зоны обратного просмотра:

```
;
; BIND reverse data file for my.dom zone
;
$TTL    86400
@       IN      SOA my.dom. root.my.dom. (
                         2014031301     ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                         2419200        ; Expire
                          86400 )       ; Negative Cache TTL
;
@       IN      NS      server.my.dom.

100     IN      PTR     server.my.dom.
101     IN      PTR     client1.my.dom.
102     IN      PTR     client2.my.dom.
103     IN      PTR     client3.my.dom.
```

Описание зон может содержать следующие основные типы записей:

- NS — имя DNS сервера;
- A — связь имени с IP-адресом;
- CNAME — связь псевдонима с другим именем (возможно псевдонимом);
- PTR — обратная связь IP-адреса с именем;
- SRV — запись о сетевой службе;
- TXT — текстовая запись.

ВНИМАНИЕ! Перевод строки в конце конфигурационных файлов зон обязателен. В большинстве применений необходимо указание точки в конце имен компьютеров для предотвращения вывода корневого суффикса имени вида «1.168.192.in-addr.arpa».

6.5.3. Настройка клиентов для работы со службой доменных имен

Для работы со службой доменных имен на компьютерах необходимо наличие конфигурационного файла /etc/resolv.conf, содержащего информацию о доменах и именах серверов DNS, например:

```
domain my.dom
search my.dom
nameserver 192.168.1.100
```

Также может быть рассмотрена установка системы поддержки работы со службой доменных имен, содержащейся в пакете resolvconf.

ВНИМАНИЕ! Для взаимодействия DNS-сервера с клиентами, функционирующими в разных мандатных контекстах, требуется дополнительная настройка механизма privsock. Описание настройки сетевых служб для работы с использованием механизма privsock приведено в документе РУСБ.10015-01 97 01-1.

6.6. Настройка SSH

SSH — это клиент-серверная система для организации защищенных туннелей между двумя и более компьютерами. В туннелях защищаются все передаваемые данные, в т. ч. пароли.

6.6.1. Служба ssh

Служба ssh (синоним sshd) может быть установлена при установке ОС. При этом служба будет запущена автоматически после завершения установки и перезагрузки, что обеспечит удаленный доступ к установленной ОС для выполнения дальнейших настроек.

При необходимости служба может быть установлена отдельно:

```
apt install ssh
```

Проверить состояние службы:

```
systemctl status ssh
```

Служба берет свои конфигурации сначала из командной строки, затем из файла `/etc/ssh/sshd_config`. Синтаксис:

```
sshd [-deiqtD46] [-b bits] [-f config_file] [-g login_grace_time]
[-h host_key_file] [-k key_gen_time] [-o option] [-p port] [-u len]
```

Параметры, которые могут присутствовать в файле `/etc/ssh/sshd_config`, описаны в таблице 26. Пустые строки, а также строки, начинающиеся с `#`, игнорируются. Названия параметров не чувствительны к регистру символов.

Таблица 26

Параметр	Описание
`AllowGroups`	Задает список групп, разделенный пробелами, которые будут допущены в систему
`DenyGroups`	Действие, противоположное действию параметра `AllowGroups`: записанные в данный параметр группы не будут допущены в систему
`AllowUsers`	Задает разделенный пробелами список пользователей, которые получат доступ в систему. По умолчанию доступ разрешен всем пользователям
`DenyUsers`	Действие, противоположное действию параметра `AllowUsers`: записанные в данный параметр пользователи не получат доступ в систему
`AFSTokenPassing`	Указывает на то, может ли маркер `AFS` пересылаться на сервер. Значение по умолчанию `yes`
`AllowTCPForwarding`	Указывает на то, разрешены ли запросы на переадресацию портов. Значение по умолчанию `yes`
`Banner`	Отображает полный путь к файлу сообщения, выводимого перед аутентификацией пользователя
`ChallengeResponseAuthentication`	Указывает на то, разрешена ли аутентификация по методу «оклик — ответ». Значение по умолчанию `yes`
`Ciphers`	Задает разделенный запятыми список методов защиты соединения, разрешенных для использования

Продолжение таблицы 26

Параметр	Описание
CheckMail	Указывает на то, должна ли служба sshd проверять почту в интерактивных сеансах регистрации. Значение по умолчанию no
ClientAliveInterval	Задает интервал ожидания в секундах, по истечении которого клиенту посылается запрос на ввод данных
ClientAliveCountMax	Задает число напоминающих запросов, посылаемых клиенту. Если по достижении указанного предела от клиента не поступит данных, сеанс завершается и сервер прекращает работу. Значение по умолчанию 3
HostKey	Полный путь к файлу, содержащему личный ключ компьютера. Значение по умолчанию /etc/ssh/ssh_host_key
GatewayPorts	Указывает на то, могут ли удаленные компьютеры подключаться к портам, для которых клиент запросил переадресацию. Значение по умолчанию no
HostbasedAuthentication	Указывает на то, разрешена ли аутентификация пользователей с проверкой файлов .rhosts и /etc/hosts.equiv и открытого ключа компьютера. Значение по умолчанию no
IgnoreRhosts	Указывает на то, игнорируются ли файлы $HOME/.rhosts и $HOME/.shosts. Значение по умолчанию yes
IgnoreUserKnownHosts	Указывает на то, игнорируется ли файл $HOME/.ssh/known_hosts в режимах аутентификации RhostsRSAAuthentication и HostbasedAuthentication. Значение по умолчанию no
KeepAlive	Если установлено значение yes (по умолчанию), демон sshd будет периодически проверять наличие связи с клиентом. В случае неуспешного завершения проверки соединение разрывается. Для выключения данного механизма задать значение параметра no в файле конфигурации сервера и клиента
KerberosAuthentication	Указывает на то, разрешена ли аутентификация с использованием Kerberos. Значение по умолчанию no
KerberosOrLocalPasswd	Указывает на то, должна ли использоваться локальная парольная аутентификация в случае неуспешной аутентификации на основе Kerberos
KerberosTgtPassing	Указывает на то, может ли структура TGT системы Kerberos пересылаться на сервер. Значение по умолчанию no
KerberosTicketCleanup	Указывает на то, должен ли при выходе пользователя удаляться кэш-файл его пропуска Kerberos

Продолжение таблицы 26

Параметр	Описание
ListenAddress	Задает интерфейс, к которому подключается служба sshd. Значение по умолчанию 0.0.0.0, т. е. любой интерфейс
LoginGraceTime	Задает интервал времени в секундах, в течение которого должна произойти аутентификация пользователя. Если процесс аутентификации не успевает завершиться вовремя, сервер разрывает соединение и завершает работу. Значение по умолчанию 600 с
LogLevel	Задает степень подробности журнальных сообщений. Возможные значения: QUIET, FATAL, ERROR, INFO (по умолчанию), VERBOSE, DEBUG (не рекомендуется)
MACs	Задает разделенный запятыми список доступных алгоритмов MAC (код аутентификации сообщений), используемых для обеспечения целостности данных
MaxStartups	Задает максимальное число одновременных неаутентифицированных соединений с демоном sshd
PAMAuthenticationViaKbdInt	Указывает на то, разрешена ли парольная аутентификация с использованием PAM. Значение по умолчанию no
PasswordAuthentication	Если установлено значение yes (по умолчанию) и ни один механизм беспарольной аутентификации не приносит положительного результата, тогда пользователю выдается приглашение на ввод пароля, который проверяется самим демоном sshd. Если значение параметра no, парольная аутентификация запрещена
PermitEmptyPasswords	Если установлено значение yes, пользователи, не имеющие пароля, могут быть аутентифицированы службой sshd. Если установлено значение no (по умолчанию), пустые пароли запрещены
PermitRootLogin	Указывает на то, может ли пользователь root войти в систему с помощью команды ssh. Возможные значения: no (по умолчанию), without-password, forced-command-only и yes
PidFile	Задает путь к файлу, содержащему идентификатор главного процесса. Значение по умолчанию /var/run/sshd.pid
Port	Задает номер порта, к которому подключается sshd. Значение по умолчанию 22
PrintLastLog	Указывает на то, должна ли служба sshd отображать сообщение о времени последнего доступа. Значение по умолчанию yes
PrintMotd	Указывает на то, следует ли после регистрации в системе отображать содержимое файла /etc/motd. Значение по умолчанию yes

Окончание таблицы 26

Параметр	Описание
Protocol	Задает разделенный запятыми список версий протокола, поддерживаемых службой sshd
PubKeyAuthentication	Указывает на то, разрешена ли аутентификация с использованием открытого ключа. Значение по умолчанию yes
ReverseMappingCheck	Указывает на то, должен ли выполняться обратный поиск имен. Значение по умолчанию no
StrictModes	Если равен yes (по умолчанию), sshd будет запрещать доступ любому пользователю, чей начальный каталог и/или файл .rhosts принадлежат другому пользователю либо открыты для записи
Subsystem	Предназначается для конфигурирования внешней подсистемы. Аргументами является имя подсистемы и команда, выполняемая при поступлении запроса к подсистеме
SyslogFacility	Задает название средства, от имени которого регистрируются события в системе Syslog. Возможны значения: DAEMON, USER, AUTH (по умолчанию), LOCAL0-7
UseLogin	Указывает на то, должна ли применяться команда login для организации интерактивных сеансов регистрации. Значение по умолчанию no
X11Forwarding	Указывает на то, разрешена ли переадресация запросов к системе X Window. Значение по умолчанию no
X11DisplayOffset	Задает номер первого дисплея (сервера) системы X Window, доступного демону sshd для переадресации запросов. Значение по умолчанию 10
XAuthLocation	Задает путь к команде xauth. Значение по умолчанию /usr/X11R6/bin/xauth

6.6.2. Клиент ssh

В роли клиента выступает инструмент командной строки ssh. Синтаксис команды:

```
ssh [-afgknqstvxACNTX1246] [-b bind_address] [-c cipher_spec] [-e escape_char]
[-i identity_file] [-login_name] [-m mac_spec] [-o option] [-p port]
[-F configfile] [-L port:host:hostport] [-R port:host:hostport]
[-D port] hostname | user@hostname [command]
```

Подробное описание параметров инструмента приведено man ssh. В простом варианте инициировать соединение с сервером sshd можно командой:

```
ssh 10.1.1.170
```

где 10.1.1.170 — IP-адрес компьютера с запущенной службой sshd. При этом sshd будет считать, что пользователь, запрашивающий соединение, имеет такое же имя, под каким он аутентифицирован на компьютере-клиенте.

Клиент ssh может заходить на сервер sshd под любым именем, используя параметр:

```
-l <имя_клиента>
```

Однако сервер будет согласовывать ключ сеанса (например, при беспарольной аутентификации по открытому ключу пользователя), проверяя открытые ключи в домашнем каталоге пользователя именно с этим именем на компьютере-клиенте. Если же используется парольная аутентификация, на компьютере-сервере должна существовать учетная запись с таким именем. Использовать беспарольную аутентификацию по открытым ключам компьютера настоятельно не рекомендуется, т. к. при этом способе в системе должны существовать потенциально опасные файлы: /etc/hosts.equiv, /etc/shosts.equiv, $HOME/.rhosts, $HOME/.shosts.

Инструментssh берет свои конфигурационные установки сначала из командной строки, затем из пользовательского файла $HOME/.ssh/config и из общесистемного файла /etc/ssh/ssh_config. Если идентичные параметры заданы по-разному, выбирается самое первое значение.

В таблице 27 описаны параметры, которые могут присутствовать в файле $HOME/.ssh/config или /etc/ssh/ssh_config. Пустые строки и комментарии игнорируются.

Таблица 27

Параметр	Описание
CheckHostIP	Указывает на то, должна ли команда ssh проверять IP-адреса в файле known_hosts. Значение по умолчанию yes
Ciphers	Задает разделенный запятыми список методов защиты сеанса, разрешенных для использования. По умолчанию aes122b-cbc, 3des-cbc, blowfish-cbc, cast128-cbc, arcfour, aes192-cbc, aes256-cbc
Compression	Указывает на то, должны ли данные сжиматься с помощью команды gzip. Значение по умолчанию no. Эта установка может быть переопределена с помощью параметра командной строки -C
ConnectionAttempts	Задает число неудачных попыток подключения (одна в секунду), после чего произойдет завершение работы. Значение по умолчанию 4

Продолжение таблицы 27

Параметр	Описание
EscapeChar	Задает escape-символ, используемый для отмены специального назначения следующего символа в сеансах с псевдотерминалом. Значение по умолчанию ~. Значение none запрещает использование escape-символа
ForwardAgent	Указывает на то, будет ли запрос к команде ssh-agent переадресован на удаленный сервер. Значение по умолчанию no
ForwardX11	Указывает на то, будут ли запросы к системе X Window автоматически переадресовываться через SSH-туннель с одновременной установкой переменной среды DISPLAY. Значение по умолчанию no
GatewayPorts	Указывает на то, могут ли удаленные компьютеры подключаться к локальным портам, для которых включен режим переадресации. Значение по умолчанию no
GlobalKnownHostsFile	Задает файл, в котором хранится глобальная база ключей компьютера. По умолчанию глобальная база ключей компьютера хранится в файле /etc/ssh/ssh_known_hosts
HostbasedAuthentication	Указывает на то, разрешена ли аутентификация пользователей с проверкой файлов .rhosts, /etc/hosts.equiv и открытого ключа компьютера. Этот параметр рекомендуется установить в значение no
HostKeyAlgorithm	Задает алгоритмы получения ключей компьютеров в порядке приоритета. Значение по умолчанию ssh-rsa, ssh-dss
HostKeyAlias	Задает псевдоним, который должен использоваться при поиске и сохранении ключей компьютера
HostName	Задает имя или IP-адрес компьютера, на котором следует регистрироваться. По умолчанию выбирается имя, указанное в командной строке
IdentityFile	Задает файл, содержащей личный ключ пользователя. Значение по умолчанию $HOME/.ssh/identity. Вместо имени начального каталога пользователя может стоять символ ~. Разрешается иметь несколько таких файлов. Все они будут проверены в указанном порядке
KeepAlive	Если равен yes (по умолчанию), команда ssh будет периодически проверять наличие связи с сервером. В случае неуспешного завершения проверки (в т. ч. из-за временных проблем с маршрутизацией) соединение разрывается. Чтобы выключить этот механизм, следует задать данный параметр, равным no, в файлах /etc/ssh/sshd_config и /etc/ssh/ssh_config либо в файле $HOME/.ssh/config
KerberosAuthentication	Указывает на то, разрешена ли аутентификация с применением Kerberos
KerberosTgtPassing	Указывает на то, будет ли структура TGT системы Kerberos пересылаться на сервер

Продолжение таблицы 27

Параметр	Описание
LocalForward	Требует значения в формате порт:узел:удаленный_порт. Указывает на то, что запросы к соответствующему локальному порту перенаправляются на заданный порт удаленного узла
LogLevel	Задает степень подробности журнальных сообщений команды ssh. Возможные значения: QUIET, FATAL, ERROR, INFO (по умолчанию), VERBOSE, DEBUG
MACs	Задает разделенный запятыми список доступных алгоритмов аутентификации сообщений для обеспечения целостности данных. Стандартный выбор: hmac-md5, hmac-sha1, hmac-ripemd160@openssh.com, hmac-sha1-96, hmac-md5-96
NumberOfPasswordPrompts	Задает число допустимых попыток ввода пароля. Значение по умолчанию 3
PasswordAuthentication	Если равен yes (по умолчанию), то в случае необходимости команда ssh пытается провести парольную аутентификацию
Port	Задает номер порта сервера. Значение по умолчанию 22
PreferredAuthentications	Задает порядок применения методов аутентификации. Значение по умолчанию: publickey, password, keyboard-interactive
Protocol	Задает в порядке приоритета версии протокола SSH
ProxyCommand	Задает команду, которую следует использовать вместо ssh для подключения к серверу. Эта команда выполняется интерпретатором /bin/sh. Спецификация %p соответствует номеру порта, а %h — имени удаленного узла
PubkeyAuthentication	Указывает на то, разрешена ли аутентификация с использованием открытого ключа. Значение по умолчанию yes
RemoteForward	Требует значения в формате удаленный_порт:узел:порт. Указывает на то, что запросы к соответствующему удаленному порту перенаправляются на заданный порт заданного узла. Переадресация запросов к привилегированным портам разрешена только после получения прав суперпользователя на удаленной системе. Эта установка может быть переопределена с помощью параметра командной строки -R
StrictHostKeyCheking	Если равен yes, команда не будет автоматически добавлять ключи компьютера в файл $HOME/.ssh/known_hosts и откажется устанавливать соединение с компьютерами, ключи которых изменились. Если равен no, команда будет добавлять непроверенные ключи сервера в указанные файлы. Если равен ask (по умолчанию), команда будет спрашивать пользователя о том, следует ли добавлять открытый ключ сервера в указанные файлы
UsePrivilegedPort	Указывает на то, можно ли использовать привилегированный порт для установления исходящих соединений. Значение по умолчанию no

Окончание таблицы 27

Параметр	Описание
User	Задает пользователя, от имени которого следует регистрироваться в удаленной системе. Эта установка может быть переопределена с помощью параметра командной строки -l
UserKnownHostsFile	Задает файл, который используется для автоматического обновления открытых ключей
XAuthLocation	Задает путь к команде xauth. Значение по умолчанию /usr/X11R6/bin/xauth

Клиентские конфигурационные файлы бывают глобальными, на уровне системы (/etc/ssh/ssh_config), и локальными, на уровне пользователя ($HOME/.ssh/config). Следовательно, пользователь может полностью контролировать конфигурацию клиентской части SSH.

Конфигурационные файлы разбиты на разделы, установки которых относятся к отдельному компьютеру, группе компьютеров или ко всем компьютерам. Установки разных разделов могут перекрывать друг друга.

6.6.3. Настройки безопасности

В поставляемую в составе дистрибутива версию пакета ssh встроены алгоритмы защитного преобразования по ГОСТ Р 34.12-2015 («Кузнечик») в режиме гаммирования (Counter, CTR) по ГОСТ Р 34.13-2015 и имитовставки с длиной хеш-кода 256 бит на основе ГОСТ Р 34.11-2012. Эти алгоритмы используются по умолчанию, их использование не требует специальной настройки.

Для вывода полного списка поддерживаемых алгоритмов выполнить следующие команды:

- вывести список поддерживаемых алгоритмов защитного преобразования:

```
ssh -Q cipher
```

- вывести список поддерживаемых алгоритмов выработки имитовставки:

```
ssh -Q mac
```

Наборы используемых алгоритмов защитного преобразования и выработки имитовставки указываются в конфигурационном файле клиента /etc/ssh/ssh_config в качестве значений параметров Ciphers и MACs соответственно. Если значения данных параметров не указаны или их строки закомментированы, то используются следующие алгоритмы в порядке уменьшения их приоритета:

1) защитное преобразование: grasshopper-ctr128 («Кузнечик» по ГОСТ Р 34.12-2015), chacha20-poly1305@openssh.com,

aes128-ctr, aes192-ctr, aes256-ctr, aes128-gcm@openssh.com, aes256-gcm@openssh.com, grasshopper-cbc;

2) имитовставка: hmac-gost2012-256-etm (по ГОСТ Р 34.11-2012), umac-64-etm@openssh.com, umac-128-etm@openssh.com, hmac-sha2-256-etm@openssh.com, hmac-sha2-512-etm@openssh.com, hmac-sha1-etm@openssh.com, umac-64@openssh.com, umac-128@openssh.com, hmac-sha2-256, hmac-sha2-512, hmac-sha1.

Для вывода списка текущих используемых алгоритмов в порядке уменьшения их приоритета выполнить следующие команды:

- вывести список используемых алгоритмов защитного преобразования:

```
sudo sshd -T | grep ciphers
```

- вывести список используемых алгоритмов выработки имитовставки:

```
sudo sshd -T | grep macs
```

Для указания других алгоритмов следует в конфигурационном файле сервера /etc/ssh/sshd_config раскомментировать строки с параметрами Ciphers и MACs и в качестве значений параметров указать через запятую нужные алгоритмы защитного преобразования и имитовставки соответственно в порядке уменьшения приоритета их выполнения.

Пример

```
Ciphers grasshopper-ctr128,chacha20-poly1305@openssh.com,aes128-ctr,\
   aes192-ctr,aes256-ctr,aes128-gcm@openssh.com,aes256-gcm@openssh.com
MACs hmac-gost2012-256-etm,umac-128-etm@openssh.com,hmac-sha2-256-\
   etm@openssh.com,hmac-sha2-512-etm@openssh.com,hmac-sha1-etm@openssh.\
   com,umac-128@openssh.com,hmac-sha2-256,hmac-sha2-512,hmac-sha1
```

ВНИМАНИЕ! В целях безопасности не рекомендуется использовать слабые и устаревшие алгоритмы, такие как алгоритмы на основе CBC, RC4, MD5 и алгоритмы с длиной ключа менее 128 бит.

Если компьютер, выступающий в роли сервера SSH, не предполагается использовать для обеспечения работы каких-либо сетевых приложений, то рекомендуется дополнительно отключить передачу меток времени по протоколу TCP (TCP Timestamps). Данные служебные метки используются для расчета времени приема-передачи, максимального времени ожидания и других нужд сетевого протокола. Также с их помощью возможно узнать принадлежность сетевой службы конкретному серверу и время работы сервера с момента последнего запуска. Подобная информация может быть использована для определения набора

обновлений безопасности, установленных на сервере, и поиска уязвимостей. Для отключения TCP Timestamps необходимо добавить в конфигурационный файл `/etc/sysctl.conf` следующую строку:

```
net.ipv4.tcp_timestamps = 0
```

Дополнительная информация по применению `ssh` доступна на официальном сайте разработчика `wiki.astralinux.ru`.

6.7. Службы точного времени

В состав ОС входят следующие службы точного времени:

1) службы, использующие протокол синхронизации времени NTP:
   а) `systemd-timesyncd` — клиентская служба синхронизации времени, используется в ОС по умолчанию. Описание службы приведено в 6.7.1;
   б) `chronyd` — клиент и сервер протокола точного времени NTP. Описание службы приведено в 6.7.2;
2) служба времени высокой точности PTP (Precision Time Protocol) — описание службы приведено в 6.7.3.

При настройке служб времени используются термины для обозначения времени, приведенные в таблице 28.

Таблица 28

Термин	Описание	Пример
Universal time, UTC	UTC (Coordinated Universal Time) — всемирное координированное время. Не зависит от местоположения компьютера, используется в качестве системного времени: времени в ядре ОС, для отметок времени записи журналов и для синхронизации времени службами времени	Universal time: Ср 2019-02-20 07:51:49 UTC
Time Zone	Временная зона. Определяет временное смещение и параметры сезонного (зимнего/летнего) времени.	Time zone: Europe/Moscow (MSK, +0300)
Local time	Локальное время (местное время). Получается из всемирного координированного времени добавлением временного смещения. Используется в основном для взаимодействия с пользователями системы	Local time: Ср 2019-02-20 10:51:49 MSK

Окончание таблицы 28

Термин	Описание	Пример
RTC time	Аппаратное время, установленное в аппаратных часах компьютера (Real Time Clock, RTC, также CMOS или BIOS time). Используется для первоначальной установки времени при загрузке ОС. Аппаратные часы могут быть настроены как на всемирное координированное, так и на местное время. При установке системного времени на основании показаний аппаратных часов ОС принимает решение о том, какое именно время (UTC или местное) показывают аппаратные часы, на основании собственных внутренних настроек (см. `man timedatectl`)	RTC time: Ср 2019-02-20 07:51:49

6.7.1. Служба systemd-timesyncd

Служба `systemd-timesyncd` предназначена для использования в роли клиента и не может выполнять функции сервера точного времени. Подходит для синхронизации времени с доверенным сервером времени в локальной сети. Может применяться в системах, где не требуется высокая точность синхронизации времени. Поддерживает только упрощенный протокол передачи времени.

6.7.1.1. Установка и настройка

Служба `systemd-timesyncd` устанавливается автоматически, если при установке ОС был выбран для установки компонент «Консольные утилиты».

Служба синхронизации запускается автоматически, если при установке ОС для настройки времени была выбрана синхронизация времени по сети.

Для запуска службы синхронизации времени вручную и для ее добавления в автозапуск выполнить команду:

```
systemctl enable systemd-timesyncd
```

Служба не может работать одновременно со службами `ntpd` или `chronyd` (не будет выполняться синхронизация времени). Служба завершает свою работу без сообщений об ошибке, если обнаружит на компьютере:

- установленную службу `ntpd` (даже незапущенную);
- для виртуальных машин — установленные гостевые дополнения Oracle Virtual Box;
- установленную службу `chronyd` (даже незапущенную).

Запись о завершении работы `systemd-timesyncd` будет внесена в системный журнал `/var/log/syslog`.

Состояние службы systemd-timesyncd можно проверить командой:

```
systemctl status systemd-timesyncd
```

Также для проверки статуса службы синхронизации времени можно использовать команду:

```
timedatectl status
```

Примечание. Необходимо учитывать, что timedatectl может использоваться и с другими службами синхронизации времени. Таким образом, если просматривать статус службы времени, то отображается статус запущенной в данной момент службы. А при использовании timedatectl, например, для запуска службы времени будет запущена установленная в системе служба.

Пример

Вывод команды timedatectl status

```
Local time: Ср 2018-12-26 11:08:12 MSK
Universal time: Ср 2018-12-26 08:08:12 UTC
RTC time: Ср 2018-12-26 08:08:12
Time zone: Europe/Moscow (MSK, +0300)
System clock synchronized: yes
NTP service: active
RTC in local TZ: no
```

Автоматический запуск службы отключается командой:

```
systemctl disable systemd-timesyncd
```

или

```
timedatectl set-ntp false
```

6.7.1.2. Выбор серверов времени

Основные и резервные серверы времени указываются в конфигурационных файлах службы systemd-timesyncd:

1) /etc/systemd/timesyncd.conf
2) /etc/systemd/timesyncd.conf.d/*.conf;

3) /run/systemd/timesyncd.conf.d/*.conf;

4) /usr/lib/systemd/timesyncd.conf.d/*.conf.

Основные параметры в конфигурационном файле:

1) NTP= — список имен основных серверов единого времени, разделенный пробелами. Объединяется со списком имен, полученных от службы systemd-networkd. По умолчанию список пустой и используются резервные серверы времени, указанные в параметре FallbackNTP=;

2) FallbackNTP= — список имен резервных серверов единого времени, разделенный пробелами.

Служба systemd-timesyncd перебирает по очереди серверы из основного списка и, если не удалось связаться ни с одним из серверов, обращается к серверам из резервного списка.

По умолчанию для службы systemd-timesyncd указаны российские серверы точного времени ВНИИФТРИ.

Дополнительно служба systemd-timesyncd может получать имена серверов времени от службы systemd-networkd, если в конфигурационных файлах этой службы (каталоги /lib/systemd/network/, /run/systemd/network/, /etc/systemd/network/ или файл /lib/) указаны серверы единого времени, привязанные к сетевым интерфейсам.

Более подробная информация о службе systemd-networkd приведена в man systemd.network.

6.7.2. Служба chronyd

Служба точного времени chronyd рекомендована к применению вместо службы ntpd. Служба chronyd может выступать в роли клиента и сервера протокола сетевого времени NTP и позволяет:

- быстрее синхронизировать системные часы;
- использовать аппаратные метки времени, что обеспечивает более точную синхронизацию времени;
- не прекращать работу службы синхронизации, обнаружив слишком большое отклонение времени, а попытаться выполнить коррекцию времени;
- работать, если порт 123 закрыт для исходящих запросов.

Службы chronyd обеспечивает надежную работу синхронизации при нестабильных сетевых соединениях, частичной доступности или перегрузки сети.

6.7.2.1. Установка

При установке ОС служба `chronyd` автоматически не устанавливается. Для установки службы требуется установить пакет `chrony` (при этом будет удален пакет установленной ранее службы `systemd-timesyncd`):

```
apt install chrony
```

ВНИМАНИЕ! При установке контроллера домена FreeIPA пакет `chrony` будет установлен автоматически, при этом будет удален пакет `systemd-timesyncd`.

6.7.2.2. Настройка

В режиме клиента служба `chronyd` может запускаться с настройками по умолчанию без конфигурационного файла.

По умолчанию для службы `chronyd` указаны российские серверы точного времени ВНИИФТРИ.

Для настройки работы службы `chronyd` в режиме сервера времени (т. е. чтобы служба отвечала клиентам на запросы) необходимо отредактировать (или при его отсутствии — создать) конфигурационный файл `/etc/chrony/chrony.conf`. В конфигурационном файле требуется добавить строку с разрешениями клиентам подключаться к серверу NTP.

Пример

Настройка разрешений подключаться к NTP-серверу:

1) разрешить всем клиентам:

```
allow
```

2) разрешить только клиенту с определенным IP-адресом:

```
allow 10.10.12.5
```

3) разрешить клиентам определенной сети:

```
allow 10.10.12
```

Более подробная информация о настройке конфигурационного файла `/etc/chrony/chrony.conf` приведена в `man chrony.conf`.

После редактирования конфигурационного файла перезапустить службу `chronyd`:

```
systemctl restart chronyd
```

6.7.3. Служба времени высокой точности PTP

Служба времени высокой точности PTP включает следующие службы:

- `ptp4l` — служба протокола времени высокой точности, реализующая работу по протоколу времени высокой точности PTP в соответствии со стандартом IEEE 1588. Точность протокола зависит от способа установки отметок времени (`time stamping`) в пакетах IEEE 1588. При программном методе установки отметок времени обеспечивается точность 1-100 микросекунд, на точность влияют прерывания, загрузка процессора и иные факторы. Аппаратная поддержка обеспечивает точность до единиц микросекунд;
- `phc2sys` — служба синхронизации часов;
- `timemaster` — служба координации, обеспечивающая совместную работу службы времени NTP (`chronyd`) и службы времени высокой точности PTP.

6.7.3.1. Проверка оборудования

Служба времени высокой точности ориентирована на использование аппаратных средств точного времени, в частности, аппаратных возможностей сетевых карт (аппаратные отметки времени).

Проверить, поддерживает ли сетевая карта аппаратные отметки времени, можно из командной строки с помощью инструмента `ethtool`. Для этого необходимо:

1) установить пакет `ethtool`, если он не был установлен ранее, выполнив команду:

```
apt install ethtool
```

2) проверить оборудование, выполнив команду:

```
ethtool -T <имя_интерфейса>
```

Если сетевая карта не поддерживает аппаратные отметки времени, возможно настроить и использовать службу времени высокой точности на основе программных отметок времени, но это повлечет снижение точности. Настройка использования сетевых карт без аппаратной поддержки отметок времени приведена в 6.7.3.3.

6.7.3.2. Установка службы PTP

Служба времени высокой точности PTP устанавливается из пакета `linuxptp` командой:

```
apt install linuxptp
```

6.7.3.3. Настройка службы ptp4l

Для включения службы `ptp4l` необходимо раскомментировать в конфигурационном файле `/etc/linuxptp/timemaster.conf` секцию домена точного времени `[ptp_domain 0]` и указать данные сетевой карты.

Пример

Настройки домена точного времени, использующего интерфейс `enp0s3`:

```
[ptp_domain 0]
interfaces enp0s3
delay 10e-6
```

Домен точного времени обслуживается службой `ptp4l`.

Настройка службы `tp4l` осуществляется с помощью конфигурационного файла `/etc/linuxptp/ptp4l.conf`.

При использовании сетевых карт без аппаратной поддержки отметок времени необходимо в конфигурационном файле `/etc/linuxptp/ptp4l.conf` в параметре `time_stamping` заменить аппаратную поддержку (`hardware`) на программную (`software`):

```
time_stamping software
```

Подробное описание настроек конфигурационного файла приведено в `man pdp4l`.

6.7.3.4. Настройка службы timemaster

Настройка службы `timemaster` осуществляется с помощью конфигурационного файла `/etc/linuxptp/timemaster.conf`.

Необходимо разрешить автоматический запуск службы `timemaster` при старте ОС, выполнив команду:

```
systemctl enable timemaster
```

Подробно параметры настройки описаны в `man timemaster`.

6.7.3.5. Настройка службы phc2sys

Служба `phc2sys` не требует настройки. Если в системе установлена сетевая карта, поддерживающая аппаратные отметки времени, которую необходимо синхронизировать с системными часами RTC, служба `phc2sys` запускается автоматически с нужными параметрами.

При работе с сетевыми картами, не поддерживающими аппаратные отметки времени, служба `phc2sys` не запускается.

6.7.3.6. Запуск службы PTP

После завершения настройки запуск всех служб осуществляется командой:

```
systemctl start timemaster
```

Служба `timemaster` запустит все остальные службы.

Пример

Проверка состояния службы `timemaster`:

```
systemctl status timemaster
```

Результат выполнения команды при штатном функционировании и наличии аппаратной поддержки:

```
timemaster.service - Synchronize system clock to NTP and PTP time sources
Loaded: loaded (/lib/systemd/system/timemaster.service; enabled; preset:
      enabled)
Active: active (running) since Thu 2024-02-22 12:33:42 MSK; 2s ago
Docs: man:timemaster
Main PID: 32390 (timemaster)
Tasks: 3 (limit: 4001)
Memory: 1.1M
CPU: 12ms
CGroup: /system.slice/timemaster.service
   32390 /usr/sbin/timemaster -f /etc/linuxptp/timemaster.conf
   32391 /usr/sbin/chronyd -n -f /var/run/timemaster/chrony.conf
   32392 /usr/sbin/ptp4l -l 5 -f /var/run/timemaster/ptp4l.0.conf -H -i
        enp0s3
   32393 /usr/sbin/phc2sys -l 5 -a -r -R 1.00 -z /var/run/timemaster/
         ptp4l.0.socket -n 0 -E ntpshm -M 0
```

6.7.3.7. Настройка режима интерпретации показаний аппаратных часов

По умолчанию ОС настроена на интерпретацию показаний аппаратных часов как всемирного координированного времени (UTC) без поправки на часовой пояс. Это позволяет исключить проблемы, связанные с коррекцией времени и сменой сезонного локального времени.

При необходимости можно настроить ОС на интерпретацию показаний аппаратных часов как локального времени. Это может быть нужно, например, если на компьютере параллельно

установлена Windows или иная операционная система, которая по умолчанию интерпретирует показания аппаратных часов как локальное время. Разная интерпретация показаний аппаратных часов может приводить к тому, что операционные системы будут показывать разное системное время.

Настройку интерпретации показаний аппаратных часов можно выполнить при установке ОС. После установки ОС настройку интерпретации показаний аппаратных часов можно выполнить с помощью инструмента командной строки `timedatectl`.

Настройка ОС на интерпретацию показаний аппаратных часов как локального времени выполняется командой:

```
timedatectl set-local-rtc 1
```

Настройка ОС на интерпретацию показаний аппаратных часов как UTC выполняется командой:

```
timedatectl set-local-rtc 0
```

При выполнении команды настройки будет произведена синхронизация аппаратных часов с системным временем. Если нужно при настройке выполнить синхронизацию системного времени с аппаратными часами, то следует использовать параметр `--adjust-system-clock`:

```
timedatectl set-local-rtc 1 --adjust-system-clock
```

Настройку интерпретации показаний аппаратных часов также можно выполнить с помощью модуля «Дата и время» графической утилиты `astra-systemsettings` («Параметры системы»). Описание модуля приведено в электронной справке.

Проверка показаний системного, локального и аппаратного времени выполняется командой:

```
timedatectl
```

Если ОС настроена на интерпретацию показаний аппаратных часов как локального времени, то в выводе команды будет отображено соответствующее предупреждение.

6.7.4. Ручная синхронизация времени ntpdate

Инструмент `ntpdate` применяется для проверки работы сервера времени и/или синхронизации с ним системного времени.

Ручная синхронизация времени может применяться для:

1) проверки, независимой от запущенных служб времени, степени рассинхронизации времени;
2) проверки доступности серверов через порт 123.

Инструмент устанавливается в ОС по умолчанию.

Запускать необходимо с правами `root`. Возможен запуск как из командной строки (вручную), так и из стартового сценария, выполняемого при загрузке ОС. Возможно выполнение `ntpdate` по расписанию из сценария `cron` для периодической коррекции времени.

Для установки инструмента выполнить команду:

```
sudo apt install ntpdate
```

Синтаксис команды:

```
ntpdate [-параметры] <NTP-сервер>
```

Основные параметры инструмента приведены в таблице 29.

Таблица 29

Параметр	Описание
`-a <ключ>`	Разрешение аутентификации и указание ключа для использования. По умолчанию аутентификация отключена
`-d`	Проверка доступности сервера времени запросом времени с подробной диагностикой без коррекции показаний локальных часов
`-q`	Проверка доступности сервера времени запросом времени без коррекции показаний локальных часов
`-u`	Предписывает использовать для запроса времени IP-порт, отличный от 123. По умолчанию `ntpdate` использует тот же IP-порт (123) что и служба `ntpd`, и, если служба `ntpd` запущена, то `ntpdate` при запуске выдаст ошибку, что порт занят. Также IP-порт 123 может быть закрыт для обеспечения безопасности
`-b`	Принудительное пошаговая коррекция времени с помощью вызова функции `settimeofday()`. Параметр следует использовать при вызове из файла запуска во время начальной загрузки

Например, для осуществление периодической коррекции времени выполнить команду:

```
ntpdate -ubv 0.ru.pool.ntp.org
```

Более подробная информация приведена в `man ntpdate`.

6.8. Программный коммутатор Open vSwitch

Open vSwitch (OVS) — это многоуровневый программный коммутатор, который поддерживает стандартные интерфейсы управления. Open vSwitch используется для работы в качестве виртуального коммутатора в средах виртуальных машин. В дополнение к стандартным интерфейсам управления и видимости на уровне виртуальной сети, Open vSwitch поддерживает распределение между несколькими физическими серверами.

Коммутатор Open vSwitch поддерживает несколько технологий виртуализации на базе Linux, включая KVM и VirtualBox.

В коммутаторе OVS реализованы следующие функции:

- стандартная модель VLAN 802.1Q с магистральными портами доступа;
- NIC teaming (bonding) — объединение интерфейсов сетевых карт (как поддерживающих LACP, так и не поддерживающих) на порте вышестоящего коммутатора;
- протоколы NetFlow, sFlow(R) для мониторинга и анализа состояния сети;
- зеркалирование для повышения видимости;
- конфигурация QoS (качество обслуживания) и его контроль;
- туннелирование Geneve, GRE, VXLAN, STT и LISP;
- управление сбоями подключения 802.1ag;
- OpenFlow 1.0.

Коммутатор OVS может полностью работать как на уровне ядра, так и в пользовательском пространстве без модуля ядра. OVS в пользовательском пространстве может получить доступ к устройствам Linux или DPDK.

Коммутатор OVS поддерживает фильтрацию сетевого потока на основе классификационных меток при включенном в ОС мандатном управлении доступом. Порядок настройки параметров фильтрации описан в РУСБ.10015-01 97 01-1.

6.8.1. Основные модули

Основными компонентами OVS являются:

1) `ovs-vswitchd` — демон, обеспечивающий работу OVS;
2) `ovsdb-server` — сервер баз данных для хранения конфигурации `ovs-vswitchd`;
3) `ovs-dpctl` — инструмент командной строки для настройки коммутатора;
4) сценарии и спецификации для создания пакетов `deb`;
5) `ovs-vsctl` — инструмент командной строки для запроса и обновления конфигурации `ovs-vswitchd`;

6) `ovs-appctl` — инструмент командной строки для отправки команд запущенным демонам OVS;

7) `ovs-ofctl` — инструмент командной строки для управления коммутаторами и контроллерами OpenFlow;

8) `ovs-pki` — инструмент командной строки для создания и управления инфраструктурой открытых ключей для коммутаторов OpenFlow;

9) `ovs-testcontroller` — контроллер OpenFlow, может использоваться для тестирования;

10) модуль для `tcpdump`, который позволяет анализировать сообщения OpenFlow.

6.8.2. Установка и настройка Open vSwitch

Для установки OVS выполнить команду:

```
sudo apt install openvswitch-switch openvswitch-common
```

Пакеты `openvswitch-switch` и `openvswitch-common` содержат основные компоненты пользовательского пространства коммутатора. Также доступны дополнительные пакеты с документацией на OVS, поддержкой IPsec, PKI, VTEP и Python.

Для переключения пользовательского пространства требуется установить пакет `openvswitch-switch-dpdk`, предоставляющий Open vSwitch с поддержкой DPDK.

6.8.3. Добавление сетевого моста и портов

Добавление сетевого моста осуществляется командой:

```
sudo ovs-vsctl add-br <имя_сетевого_моста>
```

Добавление порта осуществляется командой:

```
sudo ovs-vsctl add-port <имя_сетевого_моста> <порт> [<параметры>]
```

Указываемый в команде сетевой мост должен присутствовать в системе.

Пример

Для создания сетевого моста в OVS требуется:

1) запустить OVS для создания БД:

```
sudo /usr/share/openvswitch/scripts/ovs-ctl start
```

2) сконфигурировать порты, выполнив команды:

```
sudo ip tuntap add mode tap tap0
sudo ifconfig tap0 up
sudo ip tuntap add mode tap tap1
sudo ifconfig tap1 up
```

3) создать сетевой мост и добавить на него порты, выполнив команды:

```
sudo ovs-vsctl add-br br0
sudo ovs-vsctl add-port br0 tap0
sudo ovs-vsctl add-port br0 tap1
```

4) запустить сетевой мост:

```
sudo ifconfig br0 up
```

5) добавить физический интерфейс, выполнив команды:

```
sudo ovs-vsctl add-port br0 enp0s3
sudo ifconfig enp0s3 0
sudo dhclient br0
```

Проверить добавление портов возможно командой:

```
sudo ovs-vsctl show
```

Результат выполнения команды:

```
517c8376-7b07-45e9-9f6f-d0844efd0207
    Bridge br0
        Port enp0s3
            Interface enp0s3
        Port tap1
            Interface tap1
        Port br0
            Interface br0
                type: internal
        Port tap0
            Interface tap0
    ovs_version: "3.1.0"
```

6.8.4. Конфигурирование правил обработки пакетов

Правила обработки пакетов реализуются через OpenFlow — протокол управления процессом обработки данных, передающихся по сети маршрутизаторами и коммутаторами, реализующий технологию программно-конфигурируемой сети.

Примеры:

1. Правило, блокирующее пакеты, которые в своем уровне IP имеют ip_dst=87.250.250.242:

```
ovs-ofctl add-flow br0 ip,nw_dst=87.250.250.242,actions=drop
```

2. Правило, отбрасывающее все IP-пакеты:

```
ovs-ofctl add-flow br0 ip,actions=drop
```

3. Правило, отправляющее пакеты обратно на порт с индексом 2:

```
ovs-ofctl add-flow br0 in_port=2,actions=in_port
```

4. Правило, устанавливающее новые MAC-адреса в пакете и возвращающее этот пакет обратно на тот же порт:

```
ovs-ofctl add-flow br0 in_port=vport1,
actions=mod_dl_dst=08:00:27:8e:fc:42,
mod_dl_src=08:00:27:03:6a:e3,in_port
```

Правила OpenFlow, помимо блокировки и пропуска пакетов, также могут менять поля в пакете.

Пример

Правило, устанавливающее новые MAC-адреса в пакете и возвращающее этот пакет обратно на тот же порт:

```
ovs-ofctl add-flow br0 in_port=vport1,
actions=mod_dl_dst=08:00:27:8e:fc:42,
mod_dl_src=08:00:27:03:6a:e3,in_port
```

Возможно задание правил, учитывающих порт, VLAN и протоколы, также правилу можно задать приоритет.

6.8.5. Регистрация событий

В программном коммутаторе OVS присутствуют встроенные средства регистрации событий. Также коммутатор OVS из состава ОС доработан для реализации возможности регистрации событий безопасности и аудита IP-пакетов.

6.8.5.1. Встроенные средства регистрации

Настройка встроенных средств регистрации событий осуществляется с помощью инструмента командной строки `ovs-vswitchd`.

Для управления регистрацией событий используется команда:

```
sudo ovs-vswitchd -v <модуль>:<способ>:<уровень>
     [-v <модуль>:<способ>:<уровень> ...]
```

где `<модуль>` — модуль из состава OVS, для которого настраивается регистрация событий;
`<способ>` — способ регистрации событий;
`<уровень>` — уровень регистрируемых событий.

Коммутатор OVS состоит из модулей и настройка регистрации событий выполняется для каждого из модулей отдельно.

Список модулей OVS с настроенными для них уровнями регистрации можно вывести командой:

```
sudo ovs-appctl vlog/list
```

Встроенные средства регистрации событий коммутатора OVS обеспечивают регистрацию следующими способами: запись в системный журнал `/var/log/syslog`, запись в заданный файл, вывод в терминал, а также отправка информации о событиях на удаленный компьютер.

Если настраивается регистрация событий в файл, то должна быть включена возможность регистрации событий в файл командой:

```
sudo ovs-vswitchd --log-file[=<имя_файла>]
```

Если файл не указан, то по умолчанию события будут регистрироваться в файл `/var/log/openvswitch/ovs-vswitchd.log`.

Для настройки отправки информации о событиях на удаленный компьютер выполнить команду:

```
sudo ovs-vswitchd --syslog-target=<IP-адрес>:<порт>
```

Вывод информации о событиях в терминал по умолчанию отключен.

Также регистрируемые события разделены на уровни, определяющие серьезность события. При указании уровня выполняется регистрация событий заданного уровня и более высоких уровней. Наивысший уровень `off`, при котором регистрация событий не выполняется. Информация об уровнях регистрации приведена в `man ovs-appctl`.

Регистрация событий в системном журнале `/var/log/syslog` по умолчанию выполняется автоматически для уровней `emer` и `err`.

Дополнительная информация по использованию инструмента командной строки `ovs-vswitchd` для настройки регистрации событий приведена в `man ovs-vswitchd`.

Настройка регистрации событий после запуска службы `ovs-vswitchd` также может осуществляться с помощью инструмента командной строки `ovs-appctl`:

```
sudo ovs-appctl vlog/set <модуль>:<способ>:<уровень>
     [<модуль>:<способ>:<уровень> ...]
```

Дополнительная информация по использованию инструмента командной строки `ovs-appctl` приведена в `man ovs-appctl`.

Для просмотра системного журнала `/var/log/syslog` может использоваться графическая утилита `ksystemlog`, описание утилиты приведено в электронной справке.

6.8.5.2. Регистрация событий безопасности

В коммутаторе OVS из состава ОС реализована регистрация следующих событий безопасности:

- запуск и остановка OVS;
- изменение конфигурации OVS;
- изменение классификационных меток;
- действия с правилами OpenFlow.

Регистрация событий безопасности выполняется подсистемой регистрации событий, описание которой приведено в 17.2.

Также регистрация событий безопасности выполняется автоматически в системном журнале `/var/log/syslog`, запись о событии имеет метку `ovs_audit`. Для просмотра системного журнала `/var/log/syslog` может использоваться графическая утилита `ksystemlog`, описание утилиты приведено в электронной справке.

6.8.5.3. Аудит IP-пакетов

В коммутаторе OVS из состава ОС реализован аудит IP-пакетов, к которым была применена фильтрация на основе классификационных меток (см. РУСБ.10015-01 97 01-1). Регистрируется информация о пропуске или блокировке IP-пакетов на основе правил OpenFlow.

Для настройки аудита с выводом информации о событиях в журнал `/var/log/syslog` выполнить команду:

```
sudo ovs-appctl vlog/set syslog:ovs_mac:dbg
```

Для настройки аудита с выводом информации о событиях в терминал выполнить команду:

```
sudo ovs-appctl vlog/set console:ovs_mac:dbg
```

Сообщения аудита IP-пакетов имеют метку `ovs_mac`. Для просмотра системного журнала `/var/log/syslog` может использоваться графическая утилита `ksystemlog`, описание утилиты приведено в электронной справке.

6.9. Сетевая защищенная файловая система

6.9.1. Назначение и возможности

Для организации защищенных файловых серверов предназначена сетевая защищенная ФС (СЗФС), в основу которой положена CIFS, работающая по протоколу SMB/CIFS. Протокол СЗФС содержит в себе сообщения, которые передают информацию о мандатном контексте (метке безопасности и дополнительных мандатных атрибутах управления доступом) субъекта доступа. Подробное описание мандатого контекста приведено в документе РУСБ.10015-01 97 01-1.

Условием корректного функционирования СЗФС является использование механизма ЕПП, обеспечивающее в рамках данной ЛВС однозначное соответствие между логическим именем пользователя и его идентификатором (а также именем группы и ее идентификатором) на всех компьютерах (рабочих станциях и серверах), на которых данный пользователь может работать. Для корректной работы СЗФС необходима синхронизация UID/GID в системах клиента и сервера, т. к. информация о пользователях и группах передается в сеть в численных значениях.

СЗФС предоставляет следующие базовые возможности:

- разделение операционной системой типа Windows файловой системы ОС и наоборот;

- совместное использование принтеров, подключенных к ОС, операционной системой типа Windows и наоборот.

6.9.2. Состав

Основой СЗФС является клиент-серверная архитектура.

Сервер представляет собой расширенный сервер Samba и выполняет следующие задачи:

1) управление совместно используемые ресурсами;

2) контроль доступа к совместно используемым ресурсам. При подключении клиента сервер устанавливает метку безопасности процесса, обслуживающего запросы клиента, в соответствии с меткой безопасности этого клиента. Этим обеспечивается мандатный контроль доступа к совместно используемым файлам на стороне сервера.

Клиент представляет собой сетевую ФС в составе системы управления файлами ядра ОС и реализует интерфейс между виртуальной ФС ядра и сервером СЗФС. Клиент СЗФС выполняет следующие задачи:

1) отображение каталогов и файлов смонтированного сетевого ресурса;

2) передача на сервер дополнительной информации о классификационной метке пользователя (процесса), работающего с совместно используемым ресурсом.

С точки зрения пользователя, СЗФС выглядит как стандартная ФС, поддерживающая все механизмы защиты ОС и позволяющая работать с удаленной ФС с помощью стандартных команд.

В состав СЗФС входят следующие компоненты:

- `smbd` — служба сервера, которая обеспечивает работу службы печати и разделения файлов для клиентов операционной системы типа Windows. Конфигурационные параметры службы `smbd` описываются в файле `smb.conf`;

- `nmbd` — служба сервера, которая обеспечивает работу службы имен NetBIOS, а также может использоваться для запроса других служб имен;

- `smbclient` — служба, которую реализует клиент, используемый для доступа к другим серверам и для печати на принтерах, подключенных к серверам;

- `testparm` — команда, позволяющая протестировать конфигурационный файл `smb.conf`;

- `smbstatus` — команда, выводящая информацию о том, кто в настоящее время пользуется сервером Samba.

6.9.3. Настройка

СЗФС устанавливается в процессе установки ОС.

Основная настройка СЗФС в ОС осуществляется путем редактирования конфигурационного файла `/etc/samba/smb.conf`.

Файл `/etc/samba/smb.conf` состоит из основных именованных разделов `[global]`, `[homes]` и `[printers]`, возможно добавление пользовательских разделов. Внутри каждого раздела находится ряд параметров вида `<имя_параметра> = <значение>`.

В разделе `[global]` описаны параметры, управляющие сервером Samba в целом, а также находятся значения параметров по умолчанию для других разделов.

Примеры:

1. Фрагмент конфигурационного файла, определяющий рабочую группу `WORKGR1`, к которой относится компьютер, а также описывающий саму систему:

```
[global];
;workgroup = NT-Domain-Name или Workgroup-Name
workgroup = WORKGR1
;comment эквивалентен полю описания NT (Description field)
comment = Сервер СЗФС
```

2. Фрагмент конфигурационного файла, описывающий тип системы печати, доступной на сервере администратора, а также местонахождение конфигурационного файла принтера. Последняя строка говорит о том, что все принтеры, определенные в файле `printcap`, должны быть доступны в сети:

```
;printing = BSD или SYSV или A1X (и т.д.)
printing = bsd
printcap name = /etc/printcap
load printers = yes
```

3. Фрагмент конфигурационного файла, определяющий поддержку сервером гостевого входа. Следующие два параметра определяют работу с журнальными файлами. Параметр `m` сообщает службе Samba, что для каждого клиента ведется свой файл, а последняя строка говорит о том, что максимальный размер создаваемого журнального файла — 50 КБ:

```
;Раскомментируйте это поле, если вам нужен гостевой вход
;guest = pcguest
log file = /var/log/samba-log.%m
max log size = 50
```

Раздел [homes] позволяет подключаться к рабочим каталогам пользователей без их явного описания. При запросе клиентом определенной службы ищется соответствующее ей описание в файле и, если такового нет, просматривается раздел [homes]. Если этот раздел существует, просматривается файл паролей для поиска рабочего каталога пользователя, сделавшего запрос, и, найдя его, он становится доступным по сети. Основные параметры раздела [homes]:

1) comment — значение параметра выводится для клиента при запросе о доступных ресурсах;

2) browseable — определяет, как выводить ресурс в списке просмотра;

3) read only — определяет, может ли пользователь создавать и изменять файлы в своем рабочем каталоге при подключении по сети;

4) create mask — определяет права доступа для вновь создаваемых файлов в рабочем каталоге пользователя.

Пример

```
[homes]
comment = Home Directories
browseable = no
case sensitive = yes
read only = yes
create mask = 0700
directory mask = 0700
ea support = yes
```

Раздел [printers] используется для предоставления доступа к принтерам, определенным в файле /etc/printcap. В разделе [printers] описываются параметры управления печатью при отсутствии иного явного описания. Параметры comment, browseable, read only, create mask аналогичны параметрам раздела [homes], остальные параметры:

1) path — определяет местонахождение файла спулера при печати через SMB;

2) printable — определяет, может ли использоваться данный ресурс для печати;

3) guest ok — определяет, может ли воспользоваться принтером гостевой пользователь.

Пример

```
[printers]
comment = All Printers
```

```
browseable = no
path = /var/spool/samba
printable = no
guest ok = no
read only = yes
create mask = 0700
```

После настройки параметров сервера по умолчанию можно создать совместно используемые каталоги, доступ к которым могут получать определенные пользователи, группы пользователей или все пользователи.

Пример

Создание совместно используемого каталога с доступом только для одного пользователя. Для этого необходимо создать отдельный раздел файла `smb.conf` и заполнить его необходимой информацией (обычно это пользователь, каталог и конфигурационная информация)

```
[User1]
comment = User1' s remote source code directory
path = /usr/locaI/src
valid users = victor
browseable = yes
public = no
writeable = yes
create mode = 0700
```

В данном разделе создается совместно используемый каталог с именем `User1`. На локальном сервере его путь — `/usr/local/src`, `browseable = yes`, поэтому ресурс будет виден в списках ресурсов сети, но т. к. `public = no`, получить доступ к нему сможет только пользователь `victor`. Предоставить доступ другим пользователям можно, поместив их в запись `valid users`.

По умолчанию сервер Samba поддерживает подключение по протоколу SMB всех версий, а клиент при подключении начинает процедуру согласования протокола подключения со старшей версии. Для принудительного определения диапазона возможных протоколов используются параметры конфигурационного файла `/etc/samba/smb.conf`, приведенные в таблице 30.

Таблица 30

Имя параметра	Синоним параметра	Значение по умолчанию	Описание
`server min protocol`	`min protocol`	`NT1`	Минимальная версия протокола сервера
`server max protocol`	`max protocol`, `protocol`	`SMB3_11`	Максимальная версия протокола сервера
`client min protocol`		`NT1`	Минимальная версия протокола клиента
`client max protocol`		`SMB3_11`	Максимальная версия протокола клиента
`client ipc min protocol`		`NT1` (значение параметра `client min protocol`)	Минимальная версия протокола клиента для межпроцессного взаимодействия
`client ipc max protocol`		`SMB3_11`	Максимальная версия протокола клиента для межпроцессного взаимодействия

Допустимые значения параметров, указанных в таблице 30, для каждой версии протокола приведены в таблице 31.

Таблица 31

Версия протокола	Значение	Примечание
SMB v1	`NT1`	

SMB v2	`SMB2`
	`SMB2_02`
	`SMB2_10`
	`SMB2_22`
	`SMB2_24`
		`SMB2 = SMB2_10`

SMB v3	`SMB3`
	`SMB3_00`
	`SMB3_02`
	`SMB3_10`
	`SMB3_11`
		`SMB3 = SMB3_11`

В зависимости от реализации клиент Samba может принудительно требовать от сервера версию протокола. Обычно версия протокола задается одним из параметров подключения и имеет собственную нотацию. Способы конфигурирования протокола в зависимости от типа клиента, а также допустимые значения приведены в таблице 32.

Таблица 32

Утилита	Конфигурирование	Допустимые значения	Значение по умолчанию
mount.cifs	Применение параметра монтирования vers=	1.0 2.0 2.1 3.0 3.02 3.1.1 3.11	3.11
smbclient	Использование параметра -m, --max-protocol с инструментом командной строки	NT1 SMB2 SMB3	Определяется параметрами в /etc/samba/smb.conf

После редактирования конфигурационного файла /etc/smb.conf необходимо протестировать его корректность при помощи команды testparm, которая проверяет наличие в файле внутренних противоречий и несоответствий.

Примечание. Выполнение testparm не подтверждает, что все службы и ресурсы, описанные в конфигурационном файле, доступны и будут корректно работать.

Команда testparm имеет следующий синтаксис:

```
testparm [configfile [hostname hostip]]
```

Параметр configfile определяет местоположение конфигурационного файла (если это не файл /etc/smb.conf). Параметр hostname hostip указывает команде testparm проверить доступ к службам со стороны узла, определяемого параметром.

Если ошибки не будут обнаружены, на экране появится сообщение вида:

```
it testparm
Load smb config files from /etc/smb.conf
Processing section "[homes]"
Processing section "[printers]"
Loaded services file OK.
Press enter to see a dump of your service definitions
```

При нажатии клавиши **<Enter>** testparm протестирует каждый раздел, определенный в конфигурационном файле.

В случае обнаружения ошибок о них будет предоставлена полная информация.

6.9.4. Графическая утилита настройки СЗФС

В состав ОС входит графическая утилита `fly-admin-samba`, которая позволяет настроить пользовательский доступ к ресурсам СЗФС. Установка утилиты выполняется командой:

```
apt install fly-admin-samba
```

Описание использования утилиты приведено в электронной справке.

6.9.5. Запуск сервера

Сервер запускается либо из инициализирующих сценариев, либо из `inetd` в качестве системной службы.

Если сервер запускается из сценариев инициализации, то можно воспользоваться для запуска и остановки работы сервера следующей командой:

```
systemctl {start|stop} smbd
```

Монтирование ресурсов сервера может выполняться из командной сроки с помощью `mount`, автоматически при входе в пользовательскую сессию или по запросу (`pam_mount`, `automount`). Также возможно использование графической утилиты `fly-fm` (см. электронную справку).

Инструмент командной строки `smbclient` позволяет получить информацию о совместно используемых ресурсах или перенести файлы. Например, для запроса списка доступных ресурсов на удаленном сервере `win.netwhart.com` используется команда:

```
smbclient -L -I win.netwhart.com
```

где `-L` — указывает, что требуется вывести список совместно используемых ресурсов;
`-I` — указывает, что указанное далее имя следует рассматривать как имя DNS, а не NetBIOS.

Для пересылки файла необходимо сначала подключиться к серверу путем выполнения команды:

```
smbclient '\\WORKGR1\PUBLIC' -I win.netwhart.com -U tackett
```

где `\\WORKGR1\PUBLIC` — определяет удаленную службу на другом компьютере (обычно это каталог ФС или принтер);

`-U` — позволяет определить имя пользователя для подключения к ресурсу (при этом, если необходимо, СЗФС запросит соответствующий пароль).

После подключения появится приглашение:

```
Smb:\
```

где `\` — текущий рабочий каталог.

Используя инструмент командной строки `smbclient` можно указать команды для передачи файлов и работы с ними. Дополнительно описание параметров инструмента приведено в руководстве `man smbclient`.

6.9.6. Правила конвертации меток целостности

В ОС используется метка целостности, которая может принимать значение 256 и более.

Для штатной работы СЗФС Samba из состава ОС с СЗФС Samba других систем, в которых максимальное значение метки целостности составляет 255, реализована совместимость меток целостности. При передаче из ОС файла с меткой целостности, значение которой составляет 256 или более, в систему с максимальным значением метки целостности равным 255, метка целостности передаваемого файла будет преобразована в максимальное значение 255, т.е. будет выполнено понижение целостности при передаче файла.

Подробное описание метки целостности ОС приведено в документе РУСБ.10015-01 97 01-1.

6.10. Средство создания защищенных каналов

Для создания между компьютерами сети защищенных каналов типа точка-точка или сервер-клиент используется свободная реализация технологии виртуальной частной сети (VPN) с открытым исходным кодом OpenVPN. Данная технология позволяет устанавливать соединения между компьютерами, находящимися за NAT и сетевым экраном, без необходимости изменения их настроек.

ВНИМАНИЕ! OpenVPN не является сертифицированным криптографическим средством защиты информации и не может применяться в целях криптографической защиты информации. Основное назначение OpenVPN в составе ОС — обеспечение целостности заголовка IP-пакетов, содержащего классификационную метку, при передаче по сетям связи.

Для обеспечения безопасности управляющего канала и потока данных OpenVPN использует библиотеку `OpenSSL` (устанавливается автоматически при установке ОС). При этом

OpenVPN использует алгоритмы защитного преобразования OpenSSL в соответствии с требованиями ГОСТ (пакет библиотеки алгоритмов ГОСТ libgost-astra).

Дополнительная информация по применению OpenVPN и библиотеки алгоритмов ГОСТ libgost-astra доступна на сайте wiki.astralinux.ru.

6.10.1. Установка

Установка программного продукта OpenVPN выполняется либо из графического менеджера пакетов Synaptic, либо из терминала.

Для установки OpenVPN из терминала необходимо:

1) на компьютере, предназначенном на роль сервера OpenVPN, и на клиентских компьютерах установить пакет openvpn:

```
sudo apt install openvpn
```

2) на компьютере, предназначенном на роль сервера OpenVPN, для управления службой openvpn установить инструмент командной строки astra-openvpn-server или графическую утилиту fly-admin-openvpn-server:

```
sudo apt install astra-openvpn-server
sudo apt install fly-admin-openvpn-server
```

При установке инструмента командной строки astra-openvpn-server автоматически устанавливается и настраивается пакет libgost-astra с алгоритмами защитного преобразования ГОСТ.
При установке графической утилиты автоматически будет установлен инструмент командной строки astra-openvpn-server.

6.10.2. Управление с помощью инструмента командной строки

6.10.2.1. Параметры инструмента командной строки

Команды, используемые с инструментом командной строки astra-openvpn-server, приведены в таблице 33.

Таблица 33

Параметр	Описание
Информационные команды	
-h, --help	Вывод справки
-v, --version	Вывод версии
--show-ciphers	Вывод списка поддерживаемых ключей

Продолжение таблицы 33

Параметр	Описание
Управление выводом	
`-s`	Не выводить сообщения и предупреждения. Может быть указана в любом месте. Отменяет вывод комментариев о ходе выполнения, предупреждений, сообщений об ошибках
Управление сервером	
`start`	Запустить службу `openvpn`. При выполнении этой команды без указания дополнительных параметров служба будет запущена со стандартной конфигурацией из файла `/etc/openvpn/server.conf`. Если файл конфигурации, ключи и сертификаты сервера не существуют, то они будут созданы с параметрами по умолчанию. С данной командой дополнительно могут быть заданы параметры сервера, указаны файлы для аутентификации и параметры аутентификации
`stop`	Остановить службу. После выполнения данной команды другие команды не выполняются
`status`	Проверить службу. После выполнения данной команды другие команды не выполняются
`rebuild-server-certs`	Остановить службу, удалить все сертификаты сервера и клиентов, повторно сгенерировать все сертификаты сервера и запустить сервер. Имена файлов сертификатов сервера берутся из файла конфигурации сервера. Если файл конфигурации отсутствует, то остальные действия не выполняются. После выполнения данной команды другие команды не выполняются
Параметры сервера	
`server <IP-адрес> <маска>`	IP-адрес и маска создаваемой сети VPN (по умолчанию IP-адрес `10.8.0.0` и маска `255.255.255.0`), например: `astra-openvpn-server server "10.8.0.0 255.255.255.0"`
`port <порт>`	Порт (по умолчанию 1194)
`cipher <метод>`	Метод защитного преобразования данных. Поддерживаются следующие методы защитного преобразования: - `kuznyechik-cbc` — алгоритм «Кузнечик», используется по умолчанию; - `AES-256-GCM` — рекомендован для применения в системах общего назначения; - `AES-256-CBC` — допустим для применения в системах общего назначения; - `AES-128-CBC` — используется для совместимости со старыми системами, к применению не рекомендуется
Указание файлов для аутентификации	
`cert <имя_файла>.crt`	Файл сертификата пользователя

Окончание таблицы 33

Параметр	Описание
`ca <имя_файла>.crt`	Файл сертификата центра аутентификации
`key <имя_файла>.key`	Личный ключ
`dh <имя_файла>.pem`	Файл Диффи-Хеллмана
`tls-auth <имя_файла>.key`	Файл аутентификации TLS
Параметры аутентификации	
`EASYRSA_REQ_COUNTRY`	Название страны
`EASYRSA_REQ_PROVINCE`	Название области
`EASYRSA_REQ_CITY`	Название города
`EASYRSA_REQ_ORG`	Название организации
`EASYRSA_REQ_EMAIL`	Адрес электронной почты
`EASYRSA_REQ_OU`	Название подразделения организации
`EASYRSA_REQ_CN`	Имя пользователя
Генерация и отзыв ключей клиентов	
`client <имя_клиента>`	Создать ключи и сертификаты для указанного клиента
`revoke <имя_клиента>`	Отозвать сертификат указанного клиента
Параметры индивидуальной настройки сервера	
`get <параметр>`	Прочитать значение параметра из файла конфигурации `/etc/openvpn/server.conf`. Если файл конфигурации не существует, то он будет создан с параметрами по умолчанию
`del <параметр>`	Удалить значение параметра из файла конфигурации `/etc/openvpn/server.conf`. Если файл конфигурации не существует, то он будет создан с параметрами по умолчанию, после чего указанный параметра будет удалн
`set <параметр> <значение>`	Записать значение параметра в файл конфигурации `/etc/openvpn/server.conf`. Если файл конфигурации не существует, то он будет создан с параметрами по умолчанию, после чего в файл будет записано указанное значение

Примечания:

1. Если в командной строке заданы информационные команды, то будет выполнена первая из них. Дальнейшее выполнение сценария будет прекращено.
2. Команды управления сервером несовместимы с командами генерации и отзыва ключей для клиентов.
3. Полный список параметров индивидуальной настройки сервера доступен в документации на OpenVPN.

6.10.2.2. Запуск службы

Для запуска службы openvpn из терминала ввести команду:

```
astra-openvpn-server start
```

При запуске службы будут созданы следующие стандартные файлы и каталоги:

- файл конфигурации службы openvpn:

/etc/openvpn/server.conf

- локальный центр аутентификации, размещается в каталоге:

/etc/openvpn/openvpn-certificates

- сертификат открытого ключа центра аутентификации:

/etc/openvpn/keys/ca.crt

- сертификат открытого ключа:

/etc/openvpn/keys/server.crt

- закрытый ключ сервера:

/etc/openvpn/keys/server.key

- файл параметров Диффи-Хеллмана для аутентификации пользователей:

/etc/openvpn/keys/dh2048.pem

- файл дополнительной аутентификации TLS:

/etc/openvpn/keys/ta.key

- дополнительно, при выполнении отзыва сертификатов, будет создан стандартный файл списка отзыва сертификатов:

/etc/openvpn/keys/crl.pem

Также при первом запуске службы будут выполнены настройки межсетевого экрана и другие настройки ОС для работы openvpn как стандартной системной службы с автоматическим запуском при включении компьютера.

Запуск команды astra-openvpn-server start с указанием файлов для аутентификации (см. таблицу 33) позволяет при создании файла конфигурации и запуске службы openvpn задать расположение ранее установленных файлов ключей и сертификатов.

ВНИМАНИЕ! Чтобы избежать запроса пароля при автоматическом запуске службы openvpn необходимо файлы создавать без применения защитного преобразования.

Пример

Запуск сервера с указанием ранее установленных файлов ключей и сертификатов

```
astra-openvpn-server start cert /root/secrets/server.crt \
    ca /root/secrets/ca.crt key /root/secrets/server.key \
    dh /root/secrets/dh2048.pem tls-auth /root/secrets/ta.key
```

Указание файлов для аутентификации несовместимо с указанием параметров идентификации (см. таблицу 33).

ВНИМАНИЕ! В случае если указан хотя бы один файл для аутентификации, то все файлы будут проверены на существование. При отсутствии одного из файлов сценарий будет завершен с ошибкой без выполнения каких-либо действий. Проверка файлов на корректность не выполняется.

ВНИМАНИЕ! Если заданы файлы для аутентификации, то создание собственного центра аутентификации не выполняется.

6.10.2.3. Генерация сертификатов и ключей

При использовании собственного центра аутентификации создание ключей и сертификатов для клиентов осуществляется на сервере OpenVPN с помощью инструмента командной строки `astra-openvpn-server`. Для создания клиентского комплекта файлов используется команда `client`:

```
astra-openvpn-server client <имя_клиента>
```

При генерации могут быть заданы параметры аутентификации (см. таблицу 33).

Команда генерации ключей клиента несовместима с параметрами сервера и командами управления сервером (см. таблицу 33).

При выполнении данной команды для указанного клиента будет создан новый файл закрытого ключа `<имя_клиента>.key` и файл сертификата открытого ключа `<имя_клиента>.crt`, подписанный центром аутентификации.

Для удобства последующей передачи файлов ключей клиенту, созданные файлы будут скопированы в каталог `/etc/openvpn/clients-keys/<имя_клиента>`. Дополнительно в каталог будут скопированы и другие, необходимые для работы клиента, файлы: файл сертификата центра аутентификации (по умолчанию `ca.crt`) и файл дополнительной аутентификации TLS (`ta.key`).

Дополнительно при создании пользовательских ключей могут быть указаны такие параметры аутентификации, как страна, город, организация и др. (см. таблицу 33). В таблице 33 приве-

дены значения параметров аутентификации, используемые по умолчанию при генерации сертификатов.

ВНИМАНИЕ! Если задан любой из параметров аутентификации, то будет произведена автоматическая генерация сертификатов.

Пример

Задание дополнительных параметров аутентификации при выполнении команды создания сертификатов для клиента:

```
astra-openvpn-server client ivanov \
EASYRSA_REQ_COUNTRY RU \
EASYRSA_REQ_PROVINCE MO \
EASYRSA_REQ_CITY MOSCOW \
EASYRSA_REQ_ORG COMPANY \
EASYRSA_REQ_EMAIL ivanov@company.ru
```

ВНИМАНИЕ! Клиентские ключи генерируются без применения защитных преобразований, чтобы избежать ввода пароля при подключении клиента к серверу.

Параметры аутентификации несовместимы с указанием файлов для аутентификации (см. таблицу 33).

6.10.2.4. Отзыв сертификатов

Отзыв сертификатов применяется для запрета подключений клиента даже в тех случаях, когда в распоряжении клиента имеются копии всех сертификатов и ключей.

Для отзыва сертификата используется команда `revoke` инструмента командной строки `astra-openvpn-server`:

```
astra-openvpn-server revoke <имя_клиента>
```

Команда отзыва ключей клиента несовместима с параметрами сервера и командами управления сервером (см. таблицу 33).

При выполнении данной команды:

- сертификат клиента в базе данных центра аутентификации будет помечен как «отозванный»;
- будет создан (или обновлен ранее созданный) список отозванных сертификатов;
- новый список отозванных сертификатов будет скопирован в каталог `/etc/openvpn/keys`, сервер OpenVPN будет автоматически перезапущен для применения обновлений.

6.10.2.5. Замена сертификатов

Полная замена сертификатов сервера выполняется с помощью инструмента командной строки `astra-openvpn-server`:

```
astra-openvpn-server rebuild-server-certs
```

При выполнении данной команды:

- останавливается служба `openvpn`;
- удаляются все файлы центра аутентификации;
- удаляются все копии сертификатов сервера и клиентов;
- создается новый центр аутентификации;
- создаются новые сертификаты сервера;
- повторно запускается сервер.

Имена файлов сертификатов сервера берутся из файла конфигурации сервера. Если файл конфигурации отсутствует, то никакие действия не выполняются. После выполнения данной команды другие команды не выполняются.

6.10.2.6. Настройка клиента

На компьютер клиента должны быть перенесены файлы ключей и сертификатов, созданные на сервере, либо с помощью отчуждаемого носителя информации, либо путем передачи по защищенному соединению (например, `ssh`).

Для настройки компьютера клиента следует установить программное обеспечение OpenVPN. Установка выполняется либо из графического менеджера пакетов Synaptic, либо из терминала командой:

```
apt install openvpn
```

После установки программного обеспечения OpenVPN следует выполнить следующие действия:

1) создать файл конфигурации клиента. В качестве исходного файла возможно использовать входящий в комплект установки OpenVPN стандартный шаблон файла конфигурации, предоставляемый разработчиками OpenVPN. Шаблон файла конфигурации расположен в `/usr/share/doc/openvpn/examples/sample-config-files/client.conf`. Шаблон файла следует скопировать в каталог `/etc/openvpn/client`, выполнив команду:

```
cp /usr/share/doc/openvpn/examples/sample-config-files/client.conf \
```

```
/etc/openvpn/client
```

2) в скопированном файле конфигурации внести следующие исправления:

а) для параметра `remote` указать в качестве его значения IP-адрес сервера OpenVPN. Если был изменен порт, то также указать данное значение вместо стандартного;

б) в строках:

```
;user nobody
;group nogroup
```

удалить начальные символы «`;`»:

```
user nobody
group nogroup
```

в) для параметров `ca`, `cert` и `key` указать расположение соответствующих файлов сертификатов и ключа для аутентификации, например:

```
ca /etc/openvpn/keys/ca.crt
cert /etc/openvpn/keys/home-pc.crt
key /etc/openvpn/keys/home-pc.key
```

г) для параметра `tls-auth` указать расположение файла дополнительной аутентификации TLS, например:

```
tls-auth /etc/openvpn/keys/ta.key
```

д) для параметра `cipher` указать метод защитного преобразования данных, используемый службой. Используемый метод защитного преобразования можно узнать на сервере OpenVPN с помощью инструмента командной строки `astra-openvpn-server`:

```
sudo astra-openvpn-server get cipher
```

Защитному преобразованию по алгоритму «Кузнечик» в режиме простой замены с зацеплением соответствует значение `kuznyechik-cbc`;

е) сохранить исправленный файл.

Для проверки работы клиента OpenVPN из командной строки использовать команду:

```
/usr/sbin/openvpn --config /etc/openvpn/client/client.conf
```

где `client.conf` — конфигурационный файл клиента.

Для запуска клиента OpenVPN в качестве службы выполнить команду:

```
systemctl start openvpn-client@<имя_файла_конфигурации>
```

где <имя_файла_конфигурации> — имя файла конфигурации без расширения, расположенного в каталоге /etc/openvpn/client.

6.10.3. Управление службой с помощью графической утилиты

В графической утилите fly-admin-openvpn-server («Настройка OpenVPN сервера Fly») доступны:

- вкладка «Настройки» — в ней располагаются элементы управления для настройки сервера OpenVPN. По умолчанию доступны базовые настройки, расширенные настройки становятся доступны после нажатия кнопки **[Показать расширенные настройки]**. Описание настроек приведено в 6.10.3.2;
- вкладка «Клиентские сертификаты» — в ней располагаются элементы управления клиентскими сертификатами. Описание управления сертификатами приведено в 6.10.3.3;
- кнопки **[Запустить]** и **[Остановить]** — служат для управления службой openvpn.

6.10.3.1. Управление службой

Для запуска службы openvpn с помощью графической утилиты необходимо:

1) запустить fly-admin-openvpn-server. При первом запуске будет создан файл конфигурации службы openvpn по умолчанию и будут выпущены сертификаты сервера;
2) при необходимости отредактировать файл конфигурации и сертификаты;
3) нажать кнопку **[Запустить]**.

ВНИМАНИЕ! Графическая утилита при ее запуске не производит автоматический запуск службы openvpn.

При запуске службы будут созданы следующие стандартные файлы и каталоги:

- файл конфигурации службы openvpn:

/etc/openvpn/server.conf

- локальный центр аутентификации, размещается в каталоге:

/etc/openvpn/openvpn-certificates

- сертификат открытого ключа центра аутентификации:

/etc/openvpn/keys/ca.crt

- сертификат открытого ключа:

/etc/openvpn/keys/server.crt

- закрытый ключ сервера:

`/etc/openvpn/keys/server.key`

- файл параметров Диффи-Хеллмана для аутентификации пользователей:

`/etc/openvpn/keys/dh2048.pem`

- файл дополнительной аутентификации TLS:

`/etc/openvpn/keys/ta.key`

- дополнительно, при выполнении отзыва сертификатов, будет создан стандартный файл списка отзыва сертификатов:

`/etc/openvpn/keys/crl.pem`

Если на компьютере установлены и настроены библиотеки, поддерживающие метод защитного преобразования по алгоритму ГОСТ Р 34.12-2015 («Кузнечик») в режиме простой замены с зацеплением (Cipher Block Chaining, CBC) по ГОСТ Р 34.13-2015, то для защиты канала данных будет выбран данный метод `kuznyechik-cbc`. В противном случае будет выбран метод защитного преобразования `AES-256-GCM`.

Также при первом запуске службы будут выполнены настройки межсетевого экрана и другие настройки ОС для работы `openvpn` как стандартной системной службы с автоматическим запуском при включении компьютера.

Для остановки службы `openvpn` используя графическую утилиту необходимо нажать кнопку **[Остановить]**.

6.10.3.2. Настройка службы

Настройка службы выполняется во вкладке «Настройки» графической утилиты.

Базовые настройки включают:

1) «IP-адрес» — IP-адрес создаваемой сети VPN. По умолчанию установлено значение `10.8.0.0`;

2) «Маска» — маска создаваемой сети VPN. По умолчанию установлено значение `255.255.255.0`;

3) «Порт» — сетевой порт сервера, который будут использовать клиенты для подключения. По умолчанию установлено значение `1194`. Поддерживаются номера свободных портов от 1 до 65535;

4) «Метод защитного преобразования» — выбор метода защитного преобразования:
   а) `kuznyechik-cbc` — алгоритм «Кузнечик», выбран по умолчанию;
   б) `AES-256-GCM` — рекомендован для применения в системах общего назначения;
   в) `AES-256-CBC` — допустим для применения в системах общего назначения;

г) `AES-128-CBC` — используется для совместимости со старыми системами, к применению не рекомендуется.

Расширенные настройки позволяют задать расположение ранее предустановленных файлов ключей и сертификатов внешнего центра аутентификации, а также заново выпустить сертификаты локального центра аутентификации.

Для указания расположения ранее предустановленных файлов ключей и сертификатов внешнего центра аутентификации используются следующие поля:

- «Сертификат пользователя» — сертификат открытого ключа;
- «Сертификат ЦС» — сертификат открытого ключа центра аутентификации;
- «Личный ключ» — закрытый ключ сервера;
- «Файл Диффи-Хеллмана» — файл параметров Диффи-Хеллмана;
- «Файл аутентификации TLS» — файл дополнительной аутентификации TLS.

Проверка файлов на корректность не проводится.

Кнопка **[Сбросить сертификаты]** предназначена для удаления всех сертификатов локального центра аутентификации и повторного выпуска сертификатов сервера. После выполнения этого действия сертификаты клиентов станут недействительными, и клиенты потеряют возможность подключения к серверу OpenVPN. При выполнении данного действия:

- останавливается служба `openvpn`;
- удаляются все файлы центра аутентификации;
- удаляются все копии сертификатов сервера и клиентов;
- создается новый центр аутентификации;
- создаются новые сертификаты сервера;
- повторно запускается сервер.

6.10.3.3. Управление сертификатами

Управление сертификатами выполняется во вкладке «Клиентские сертификаты» графической утилиты.

В данной вкладке расположены таблица с данными о клиентских сертификатах и кнопки управления:

1) **[Создать сертификат]** — создание ключа и сертификата пользователя. При нажатии на кнопку будет открыто диалоговое окно с полями:

а) «Имя пользователя» — имя сертификата. Имя сертификата должно быть уникальным, не может быть пустым и не может содержать пробелы;

б) «Страна» — двухбуквенный код страны. Если поле пустое, то по умолчанию будет установлено значение «RU»;

в) «Область» — название области. Если поле пустое, то по умолчанию будет установлено значение «MO»;

г) «Город» — название города. Если поле пустое, то по умолчанию будет установлено значение «Moscow»;

д) «Организация» — название организации. Если поле пустое, то по умолчанию будет установлено значение «none»;

е) «Email» — адрес электронной почты. Если поле пустое, то по умолчанию будет установлено значение «none»;

ж) «Отдел» — название подразделения организации. Если поле пустое, то по умолчанию будет установлено значение «none»;

з) «Имя» — имя пользователя. Если поле пустое, то по умолчанию будет установлено значение «noname»;

При нажатии на кнопку **[Да]** будет создан новый файл закрытого ключа `<имя_клиента>.key` и файл сертификата открытого ключа `<имя_клиента>.crt`, подписанный центром аутентификации.

Для удобства последующей передачи файлов ключей клиенту, созданные файлы будут скопированы в каталог `/etc/openvpn/clients-keys/<имя_клиента>`. Дополнительно в каталог будут скопированы и другие, необходимые для работы клиента, файлы: файл сертификата центра аутентификации (по умолчанию `ca.crt`) и файл дополнительной аутентификации TLS (`ta.key`).

ВНИМАНИЕ! Клиентские ключи генерируются без применения защитных преобразований, чтобы избежать ввода пароля при подключении клиента к серверу;

2) **[Отозвать сертификат]** — отзыв клиентских сертификатов. Отзыв сертификатов применяется для запрета подключений клиента даже в тех случаях, когда в распоряжении клиента имеются копии всех сертификатов и ключей. Для отзыва сертификата выбрать в таблице клиентов строку с отзываемым сертификатом и нажать данную кнопку. При нажатии на данную кнопку будут выполнены следующие действия:

а) сертификат клиента в базе данных центра аутентификации будет помечен как «отозванный»;

б) будет создан (или обновлен ранее созданный) список отозванных сертификатов;

в) новый список отозванных сертификатов будет скопирован в каталог `/etc/openvpn/keys`;

3) **[Открыть папку сертификатов]** — открытие каталога `/etc/openvpn/clients_keys` в файловом менеджере.

6.10.3.4. Настройка клиента

Настройка сетевых подключений клиентских компьютеров осуществляется с помощью графической утилиты `network-manager-openvpn`. Установка утилиты выполняется командой:

```
apt install network-manager-openvpn network-manager-openvpn-gnome
```

Для настройки клиентского подключения следует в области уведомлений панели задач нажать левой кнопкой мыши на значок сетевых соединений и в раскрывшемся меню выбрать «Соединения VPN — Добавить VPN соединение» (или «Соединения VPN — Настроить VPN», если создается не первое соединение). В открывшемся окне из выпадающего списка выбрать «OpenVPN» и нажать **[Создать]**.

В открывшемся окне необходимо:

1) в поле «Шлюз» указать IP-адрес ранее запущенного сервера OpenVPN;

2) в поле «Тип» оставить значение по умолчанию «Сертификат TLS»;

3) в поле «Сертификат CA» указать путь к скопированному файлу сертификата центра аутентификации `ca.crt` (6.10.2.3);

4) в поле «Сертификат пользователя» указать путь к скопированному файлу сертификата открытого ключа пользователя `<имя_клиента>.crt` (6.10.2.3);

5) в поле «Приватный ключ Пользователя» указать путь к файлу закрытого ключа `<имя_клиента>.key` (6.10.2.3);

6) нажать кнопку **[Дополнительно]**, в открывшемся окне перейти во вкладку «Аутентификация TLS» и в секции «Дополнительная аутентификация или шифрование TLS» выполнить настройки:

   а) из выпадающего списка «Режим» выбрать «TLS-Auth» (режим «TLS-Crypt» следует выбирать, если необходимо использовать защитное преобразование для соединения);

   б) в поле «Файл ключа» указать путь к ранее скопированному на компьютер пользователя файлу дополнительной аутентификации TLS (см. 6.10.3.3);

   в) из выпадающего списка «Направление ключа» выбрать «1».

Все остальные настройки можно оставить заданными по умолчанию. После нажатия кнопки **[ОК]** созданное VPN-соединение будет сохранено.

Для включения сохранного соединения нужно повторно нажать левой кнопкой мыши на значок сетевых подключений в области уведомлений панели задач, в раскрывшемся меню выбрать «Соединения VPN» и отметить включаемое соединение.

Для экспорта параметров созданного клиентского соединения с целью их повторного использования на других клиентах выполнить следующие действия:

1) нажать левой кнопкой мыши на значок сетевых соединений в области уведомлений панели задач и в раскрывшемся меню выбрать «Соединения VPN — Настроить VPN»;

2) из появившегося списка соединений выбрать нужное соединение, нажать кнопку **[Изменить]**, затем нажать **[Экспортировать]**;

3) указать файл, в который сохранить параметры соединения.

При создании соединения VPN используя ранее сохраненные параметры соединения необходимо:

1) нажать левой кнопкой мыши на значок сетевых соединений в области уведомлений панели задач и в раскрывшемся меню выбрать «Соединения VPN — Добавить VPN соединение»;

2) в открывшемся окне из выпадающего списка выбрать «Импортировать сохраненную конфигурацию VPN» и нажать **[Создать]**;

3) указать путь к файлу с параметрами соединения.

6.10.4. Диагностика работы службы и клиента

В процессе работы службы и клиента OpenVPN информация о событиях записывается в системный журнал сервера или клиента, соответственно.

Для просмотра системного журнала полностью используется команда:

```
journalctl
```

Для просмотра последних событий и вывода новых событий по мере их появления используется команда:

```
journalctl -f
```

Для вывода только новых сообщений от службы `openvpn` по мере их добавления в журнал используется команда:

```
tail -f /var/log/syslog | grep ovpn-server
```

При каждом подключении клиента в журнал сервера записывается информация о параметрах подключения, в том числе о выбранном методе защитного преобразования передаваемых данных для входящего и исходящего каналов.

Для проверки установленного метода защитного преобразования используется команда:

```
grep  "Data Channel: Cipher" /var/log/syslog
```

6.10.5. Использование инструмента XCA для создания собственного центра аутентификации

6.10.5.1. Установка инструмента XCA

Для безопасного и эффективного управления файлами ключей и сертификатов рекомендуется использовать графический инструмент создания и управления центром аутентификации XCA.

Инструмент XCA применяется для создания центра аутентификации (Certification Authority, CA) и инфраструктуры открытых ключей (Public Key Infrastructure, PKI).

Инструмент XCA входит в состав ОС. Установка выполняется либо из графического менеджера пакетов Synaptic, либо из терминала командой:

```
apt install xca
```

После установки инструмент XCA доступен для запуска из меню «Пуск — Утилиты — Цифровые сертификаты XCA» (при использовании классического меню «Пуск»). По умолчанию инструмент XCA запускается на языке операционной системы. Выбор языка возможно изменить вручную через меню «Файл — Язык».

После первого запуска инструмента XCA необходимо создать новую БД. Для этого:

1) выбрать в меню пункт «Файл — Новая база данных»;
2) указать название и путь размещения БД;
3) нажать **[Сохранить]**.

Перед созданием БД будет запрошена установка пароля для доступа к БД. При нажатии **[Да]** без установки пароля БД будет создана без пароля.

ВНИМАНИЕ! Утеря БД может привести к компрометации или полной неработоспособности систем, использующих выданные центром сертификаты. Рекомендуется разворачивать центр аутентификации на отдельном физическом компьютере, не подключенном к сети, передачу сертификатов осуществлять с помощью съемных носителей информации и принять все возможные меры для ограничения доступа к БД.

6.10.5.2. Подготовка шаблонов

Перед созданием сертификатов для упрощения дальнейшей работы рекомендуется заполнить и сохранить типовые значения полей, которые будут применяться в дальнейшем при создании сертификатов. Для этой цели в инструменте XCA предусмотрен механизм шаблонов.

Для создания нового шаблона перейти во вкладку «Шаблоны» и нажать кнопку **[Новый шаблон]**. Из появившегося списка выбрать типовой шаблон. Новый шаблон будет создан как копия выбранного предустановленного шаблона. В инструменте XCA предусмотрено три предустановленных шаблона:

- [default] CA — предустановленный шаблон сертификата центра аутентификации (ЦА);
- [default] HTTPS_client — предустановленный шаблон сертификата клиента;
- [default] HTTPS_server — предустановленный шаблон сертификата сервера.

Предустановленные шаблоны ориентированы на службу HTTPS, поэтому рекомендуется создать на их основе свои шаблоны, полностью настроенные на службу OpenVPN. Для всех шаблонов во вкладке «Субъект» следует заполнить следующие поля:

- «Внутреннее имя» — любое имя;
- «countryName» — двухбуквенный код страны;
- «stateOrProvinceName» — двухбуквенный код региона;
- «localityName» — название города;
- «organizationName» — название организации;
- «organizationalUnitName» — название структурной единицы внутри организации;
- «commonName» — общедоступное имя;
- «emailAddress» — адрес электронной почты.

При заполнении информационных полей шаблона не рекомендуется использовать кириллицу. Все поля являются необязательными, однако, в шаблоне, как минимум, обязательно должно быть заполнено либо поле «Внутреннее имя», либо поле «commonName».

Дополнительно необходимо внести следующие изменения в предустановленные шаблоны:

1) для шаблона сертификата ЦА — во вкладке «Расширения» проверить корректность данных:
   а) тип сертификата «Центр сертификации»;
   б) наличие флага «Critical»;
   в) наличие флага «Subject Key Identifier». При необходимости уточнить даты и срок действия сертификата.

   После корректировки шаблона сохранить его, нажав кнопку **[Да]**;

2) для шаблона сертификата сервера — во вкладке «Расширения» проверить корректность данных:

а) тип сертификата «Конечный субъект»;

б) наличие флага «Critical»;

в) наличие флага «Subject Key Identifier». При необходимости уточнить даты и срок действия сертификата.

Во вкладке «Область применения ключа»:

а) в левом поле «X509v3 Key Usage» должны быть выбраны пункты «Digital Signature» и «Key Encipherment»;

б) в левом поле «X509v3 Key Usage» снять выбор с пункта «Non Repudiation»;

в) в правом поле «X509v3 Extended Key Usage» должен быть выбран пункт «TLS Web Server Authentication».

Во вкладке «Netscape» в поле «Netscape Cert Type» снять выбор с пункта «SSL Server».

После корректировки шаблона сохранить его, нажав кнопку **[Да]**;

3) для шаблона сертификата клиента — во вкладке «Расширения» проверить корректность данных:

а) тип сертификата «Конечный субъект»;

б) наличие флага «Critical»;

в) наличие флага «Subject Key Identifier». При необходимости уточнить даты и срок действия сертификата.

Во вкладке «Область применения ключа»:

а) в левом поле «X509v3 Key Usage» снять выбор с пунктов «Data Encipherment» и «Key Encipherment»;

б) в левом поле «X509v3 Key Usage» должен быть выбран пункт «Key Agreement»;

в) в правом поле «X509v3 Extended Key Usage» должен быть выбран пункт «TLS Web Client Authentication».

Во вкладке «Netscape» в поле «Netscape Cert Type» снять выбор с пунктов «SSL Client» и «S/MIME».

После корректировки шаблона сохранить его, нажав кнопку **[Да]**.

6.10.5.3. Типовая схема применения инструмента XCA

Типовая упрощенная схема применения инструмента XCA включает в себя следующие действия:

1) создание корневого сертификата ЦА;

2) создание закрытого ключа и сертификата открытого ключа сервера;

3) экспорт для использования сервером:

а) сертификата ЦА в соответствии с 6.10.5.7;

б) закрытого ключа сервера в соответствии с 6.10.5.8;

в) сертификата открытого ключа сервера в соответствии с 6.10.5.8;

г) файла параметров Диффи-Хеллмана в соответствии с 6.10.5.8;

д) файла параметров дополнительной аутентификации протокола TLS в соответствии с 6.10.5.8;

4) создание закрытого ключа и сертификата открытого ключа клиента;

5) экспорт для использования клиентом:

а) сертификата ЦА в соответствии с 6.10.5.7;

б) закрытого ключа клиента в соответствии с 6.10.5.9;

в) сертификата открытого ключа клиента в соответствии с 6.10.5.9;

г) файла параметров дополнительной аутентификации протокола TLS в соответствии с 6.10.5.9;

6) повторная генерация сертификатов по мере истечения их срока действия.

Пункты 4) и 5) перечисления выполняются для каждого нового подключаемого клиента. Пункт 6) повторяется для центра аутентификации, сервера и клиентов по мере истечения срока действия их сертификатов.

Процедура экспорта подразумевает копирование необходимых данных в файлы и перенос соответствующих файлов на компьютеры сервера и клиентов с использованием процедур, предотвращающих несанкционированный доступ к передаваемой информации (сменные носители, защищенные каналы связи и др.).

6.10.5.4. Создание корневого сертификата центра аутентификации

Корневой сертификат может быть получен из внешнего ЦА или создан как самозаверенный собственный корневой сертификат.

Для создания самоподписанного корневого сертификата необходимо запустить инструмент XCA и выполнить следующие действия:

1) перейти во вкладку «Сертификаты», нажать **[Новый сертификат]**;

2) в открывшемся окне будет установлен флаг «Создать самозаверенный сертификат» и в поле «Шаблон для нового сертификата» выбрать предустановленный шаблон «[default] CA». Если был создан собственный шаблон, то выбрать его, затем нажать кнопку **[Применить всё]**;

3) перейти во вкладку «Субъект». Если был применен собственный шаблон, то поля формы будут автоматически заполнены данными из выбранного шаблона (кроме поля «Внутреннее имя», которое должно быть указано индивидуально для каждого сертификата). Заполнить следующие незаполненные поля:

а) «Внутреннее имя» — указать имя сертификата, например, «rootCA»;

б) «commonName» — указать то же имя — «rootCA»;

в) нажать кнопку **[Сгенерировать новый ключ]**.

Будет предложено создать новый закрытый ключ с заданным именем. Проверить параметры ключа: «Тип Ключа: RSA», «Длинна ключа: 2048 bit». Нажать кнопку **[Создать]**, затем нажать **[Да]**;

4) перейти во вкладку «Расширения»:

а) убедиться, что в поле «Тип» выбран «Центр Сертификации»;

б) проверить установку флагов «Critical» и «Subject Key Identifier»;

в) определить период действия сертификата, заполнив поля «Период действия» и «Срок действия»;

5) перейти во вкладку «Область применения ключа», убедиться, что в левом поле «X509v3 Key Usage» выбраны пункты:

а) «Certificate Sign»;

б) «CRL Sign»;

6) перейти во вкладку «Netscape», убедиться, что в поле «Netscape Cert Type» выбраны пункты:

а) «SSL CA»;

б) «S/MIME CA»;

в) «Object signing CA»;

7) после проверок нажать **[Да]** для создания сертификата.

После выполнения данных действий в списке сертификатов появится корневой сертификат, который в дальнейшем будет использовать для подписания других сертификатов.

6.10.5.5. Создание сертификата сервера

Для создания сертификата сервера выполнить следующие действия:

1) перейти во вкладку «Сертификаты», нажать **[Новый сертификат]**;

2) в открывшемся окне во вкладке «Первоисточник»:

а) установить флаг «Использовать этот сертификат для подписи» (флаг «Создать самозаверенный сертификат» будет снят автоматически) и в соответствующем выпадающем списке выбрать созданный согласно 6.10.5.4 корневой сертификат;

б) в поле «Шаблон для нового сертификата» выбрать предустановленный шаблон «[default] HTTPS_server». Если был создан собственный шаблон, то выбрать его, затем нажать кнопку **[Применить всё]**;

3) перейти во вкладку «Субъект». Если был применен собственный шаблон, то поля формы будут автоматически заполнены данными из выбранного шаблона (кроме поля «Внутреннее имя», которое должно быть указано индивидуально для каждого сертификата). Заполнить следующие незаполненные поля:

а) «Внутреннее имя» — указать имя сертификата;

б) «commonName» — указать то же имя;

в) нажать кнопку **[Сгенерировать новый ключ]**.

Будет предложено создать новый закрытый ключ с заданным именем. Проверить параметры ключа: «Тип Ключа: RSA», «Длинна ключа: 2048 bit». Нажать кнопку **[Создать]**, затем нажать **[Да]**;

4) перейти во вкладку «Расширения»:

а) убедиться, что в поле «Тип» выбран «Конечный субъект»;

б) проверить установку флагов «Critical» и «Subject Key Identifier»;

в) определить период действия сертификата, заполнив поля «Период действия» и «Срок действия»;

5) перейти во вкладку «Область применения ключа», убедиться, что:

а) в левом поле «X509v3 Key Usage» выбраны пункты «Digital Signature» и «Key Encipherment»;

б) в правом поле «X509v3 Extended Key Usage» выбран пункт «TLS Web Server Authentication»;

6) нажать **[Да]** для создания сертификата.

После создания сертификата сервера он отобразится в общем списке сертификатов. Инструмент XCA представляет список сертификатов в виде дерева, корнем которого является корневой сертификат центра аутентификации.

6.10.5.6. Создание сертификата клиента

Для создания сертификата клиента выполнить следующие действия:

1) перейти во вкладку «Сертификаты», нажать **[Новый сертификат]**;

2) в открывшемся окне во вкладке «Первоисточник»:

а) установить флаг «Использовать этот сертификат для подписи» (флаг «Создать самозаверенный сертификат» будет снят автоматически) и в соответствующем выпадающем списке выбрать созданный согласно 6.10.5.4 корневой сертификат;

б) в поле «Шаблон для нового сертификата» выбрать предустановленный шаблон «[default] HTTPS_client». Если был создан собственный шаблон, то выбрать его, затем нажать кнопку **[Применить всё]**;

3) перейти во вкладку «Субъект». Если был применен собственный шаблон, то поля формы будут автоматически заполнены данными из выбранного шаблона (кроме поля «Внутреннее имя», которое должно быть указано индивидуально для каждого сертификата). Заполнить следующие незаполненные поля:

а) «Внутреннее имя» — указать имя сертификата;

б) «commonName» — указать то же имя;

в) нажать кнопку **[Сгенерировать новый ключ]**.

Будет предложено создать новый закрытый ключ с заданным именем. Проверить параметры ключа: «Тип Ключа: RSA», «Длинна ключа: 2048 bit». Нажать кнопку **[Создать]**, затем нажать **[Да]**;

4) перейти во вкладку «Расширения»:
   а) убедиться, что в поле «Тип» выбран «Конечный субъект»;
   б) проверить установку флагов «Critical» и «Subject Key Identifier»;
   в) определить период действия сертификата, заполнив поля «Период действия» и «Срок действия»;
5) перейти во вкладку «Область применения ключа», убедиться, что:
   а) в левом поле «X509v3 Key Usage» выбран пункт «Key Agreement»;
   б) в правом поле «X509v3 Extended Key Usage» выбран пункт «TLS Web Client Authentication»;
6) нажать **[Да]** для создания сертификата.

После создания сертификата клиента он отобразится в общем списке сертификатов.

6.10.5.7. Экспорт корневого сертификата центра аутентификации

Для работы серверов и клиентов нужен только сертификат ЦА. Закрытый корневой сертификат ЦА не должен передаваться в другие системы, однако, его копии следует хранить в системах резервного копирования и восстановления.

Для экспорта корневого сертификата:

- в основном окне программы перейти во вкладку «Сертификаты»;
- в списке выбрать корневой сертификат и нажать кнопку **[Экспорт]**;
- в открывшейся окне указать имя файла контейнера сертификата, место сохранения и выбрать формат экспорта «PEM (`*.crt`)»;
- нажать кнопку **[Да]**.

6.10.5.8. Экспорт файлов сертификатов и ключей сервера

Для экспорта сертификата сервера необходимо:

1) в основном окне программы перейти во вкладку «Сертификаты»;
2) в списке выбрать сертификат сервера и нажать кнопку **[Экспорт]**;
3) в открывшейся окне указать место сохранения и выбрать формат экспорта «PEM (`*.crt`)»;
4) нажать кнопку **[Да]**.

Для экспорта закрытого ключа сервера необходимо:

1) в основном окне программы перейти во вкладку «Закрытые ключи»;

2) в списке выбрать закрытый ключ сервера и нажать кнопку **[Экспорт]**;
3) в открывшейся окне выбрать формат экспорта «Закрытый ключ PEM (*.pem)»;
4) нажать кнопку **[Да]**.

Закрытый ключ сервера экспортируется в открытом виде без применения защитного преобразования данных.

Закрытый ключ сервера должен находиться на сервере и не должен передаваться клиентам.

Для создания файла с параметрами Диффи-Хеллмана необходимо:

1) в основном окне программы выбрать в меню «Дополнительно — Сгенерировать параметры Диффи-Хэллмана»;
2) в открывшейся окне указать значение «2048 (2048 бит)»;
3) нажать кнопку **[Да]**.
Примечание. Генерация занимает много времени, об активности программы свидетельствует индикатор в правом нижнем углу окна программы;
4) в открывшейся окне указать место для сохранения полученного файла;
5) нажать кнопку **[Да]** для сохранения.

Создание файл дополнительной аутентификации протокола TLS в инструменте XCA не предусмотрено. Данный файл должен быть создан отдельно средствами OpenVPN при помощи команды:

```
openvpn --genkey --secret <имя_файла>
```

6.10.5.9. Экспорт файлов сертификатов и ключей клиента

Для экспорта сертификата клиента необходимо:

1) в основном окне программы перейти во вкладку «Сертификаты»;
2) в списке выбрать сертификат клиента и нажать кнопку **[Экспорт]**;
3) в открывшейся окне указать место сохранения и выбрать формат экспорта «PEM (*.crt)»;
4) нажать кнопку **[Да]**.

Для экспорта закрытого ключа клиента необходимо:

1) в основном окне программы перейти во вкладку «Закрытые ключи»;
2) в списке выбрать закрытый ключ клиента и нажать кнопку **[Экспорт]**;
3) в открывшейся окне выбрать формат экспорта «Закрытый ключ PEM (*.pem)»;
4) нажать кнопку **[Да]**.

Закрытый ключ клиента экспортируется в открытом виде без применения защитного преобразования данных.

6.10.5.10. Отзыв сертификатов. Списки отзыва сертификатов

Для отзыва сертификата необходимо:

1) в основном окне программы перейти во вкладку «Сертификаты»;
2) найти в списке отзываемый сертификат, нажать правой кнопкой мыши и в раскрывшемся меню выбрать «Отозвать».

Аналогичным способом можно отменить отзыв сертификата, выбрав пункт «Вернуть».

Списки отозванных сертификатов привязываются к корневому сертификату ЦА, подписавшего эти сертификаты.

Для просмотра списка отозванных сертификатов, относящихся к корневому сертификату, необходимо:

1) в основном окне программы перейти во вкладку «Сертификаты»;
2) в списке выбрать корневой сертификат, нажать правой кнопкой мыши и в раскрывшемся меню выбрать «ЦС — Управление отзывами».

Откроется список отозванных сертификатов.

Для создания списка отозванных сертификатов в формате, пригодном для экспорта в другие системы, необходимо:

1) в основном окне программы перейти во вкладку «Сертификаты»;
2) в списке выбрать корневой сертификат, нажать правой кнопкой мыши и в раскрывшемся меню выбрать «ЦС — Сгенерировать CRL»;
3) в открывшемся окне, при необходимости, уточнить параметры списка;
4) нажать кнопку **[Да]**.

Созданные списки отзыва можно просмотреть во вкладке «Списки отзыва сертификатов». Из этой же вкладки списки отозванных сертификатов можно экспортировать, нажав кнопку **[Экспорт]**, формат экспорта «PEM (`*.pem`)».

6.11. Средство удаленного администрирования Ansible

Ansible является программным решением для настройки и централизованного управления конфигурациями удаленных машин, в том числе одновременно группой машин. Для работы Ansible используется существующая инфраструктура SSH.

В Ansible для применения конфигурации на удаленной машине используется режим push mode, который заключается в распространении конфигурации с управляющей машины на удаленную.

6.11.1. Состав

В состав Ansible входят модули, обеспечивающие развертывание, контроль и управление компонентами удаленных машин. Перечень основных модулей приведен в таблице 34.

Таблица 34

Модуль	Описание
shell	Позволяет запускать shell-команды на удаленном узле, например: `ansible -i step-02/hosts -m shell -a 'uname -a' host0.example.org`
copy	Позволяет копировать файл из управляющей машины на удаленный узел: `ansible -i step-02/hosts -m copy -a 'src=<исходный_каталог> dest=<каталог_назначения>' host0.example.org`
setup	Предназначен для сбора фактических данных с узлов: `ansible -i step-02/hosts -m setup host0.example.org`

6.11.2. Установка и настройка Ansible

На управляющей и управляемых машинах должен быть установлен Python.

Дополнительно для работы Ansible необходимы следующие Python-модули на управляющей машине:

- `python-yaml`;
- `paramiko`;
- `python-jinja2`.

Установка модулей осуществляется путем выполнения команды:

```
apt install python-yaml python-jinja2 python-paramiko python-crypto
```

Для установки Ansible выполнить команду:

```
apt install ansible
```

Перечень машин, которыми нужно управлять, задается двумя способами:

- в текстовом файле (по умолчанию используется `ini`-файл) в каталоге `/etc/ansible/hosts`;

- с помощью сценария, получающего перечень машин из сторонних программных продуктов, например, от Zabbix.

Кроме списка управляемых машин в `ini`-файле может указываться дополнительная информация: номера портов для подключения по SSH, способ подключения, пароль для подключения, имя пользователя, объединения групп и т. п.

Примеры:

1. Конфигурационный `ini`-файл, в квадратных скобках указаны имена групп управляемых машин

```
[dbservers]
nude1.example.ru
nude2.example.ru

[webservers]
srv1.example.ru ansible_ssh_port=8877 ansible_ssh_host=192.168.1.1
srv2.example.ru
srv[3:20].example.ru
```

2. Конфигурационный YAML-файл

```
all:
hosts:
mail.example.ru:
children:
webservers:
hosts:
srv1.example.ru:
jumper:
ansible_port: 8877
ansible_host: 192.168.1.1
srv2.example.ru:
dbservers:
hosts:
nude1.example.ru:
nude2.example.ru:
```

В дополнение к конфигурационному файлу при определении и управлении группами удаленных машин используется переменные параметры. Переменные параметры могут быть

объединены в группы. Данные о переменных предпочтительно хранить в отдельных YAML-файлах в соответствующих каталогах:

- `/etc/ansible/group_vars/<имя_группы>` — для переменных группы машин ;
- `/etc/ansible/host_vars/<имя_машины>` — для переменных отдельных машин.

6.11.3. Сценарии Ansible

Ansible позволяет использовать сценарии, предназначенные для выполнения на управляемых машинах. Сценарии пишутся на языке YAML.

Для выполнения сценария используется команда `ansible-playbook` со следующим синтаксисом:

```
ansible-playbook <имя_файла_сценария.yml> ... [другие параметры]
```

Описание основных параметров сценариев приведено в таблице 35.

Таблица 35

Параметр	Описание
`hosts`	Указываются управляемые узлы или группы узлов, к которым нужно применить изменения
`tasks`	Описывается состояние, в которое необходимо привести управляемый узел, альтернативой могут быть роли
`gather_facts`	Указывает собирать или нет информацию об узлах перед выполнением задач. Значение по умолчанию — «Да»
`vars`	Указываются переменные, которые будут использованы при выполнении сценария
`connection`	Используется для указания метода соединения с узлами: pure ssh, paramiko, fireball, chroot, jail, local, accelerate
`sudo`	После установления соединения выполнять задачу с привилегиями другого пользователя. Значение по умолчанию — `root`
`sudo_user`	В сочетании с параметром `sudo` можно указать пользователя, с привилегиями которого будет выполнена задача
`vars_prompt`	Перед выполнением сценария Ansible в интерактивном режиме может уточнить указанные в этом разделе параметры
`remote_user` (`user`)	Имя пользователя для авторизации на удаленном узле

7. СРЕДСТВА ОБЕСПЕЧЕНИЯ ОТКАЗОУСТОЙЧИВОСТИ И ВЫСОКОЙ ДОСТУПНОСТИ

7.1. Pacemaker и Corosync

В состав ОС входит набор программного обеспечения Pacemaker и Corosync, используемого для построения кластерных систем высокой доступности. Основные особенности Pacemaker и Corosync:

- обнаружение и восстановление после сбоев узлов и служб;
- независимость от подсистемы хранения — не требуется общее хранилище;
- независимость от типов ресурсов — все что может быть выполнено путем запуска сценария, может быть кластеризовано;
- поддержка кластеров любого размера;
- поддержка кворумных и ресурсозависимых кластеров;
- поддержка избыточной конфигурации;
- автоматическая репликация конфигурации, может быть обновлена с любого узла кластера;
- возможность задания порядка запуска ресурсов независимо от того, на каком узле они находятся;
- поддержка ресурсов, запускаемых на множестве узлов, — клонов;
- поддержка ресурсов с мульти-режимами работы (master/slave, primary/secondary).

С точки зрения кластера все используемые сущности: службы, точки монтирования, тома и разделы — это ресурсы, поэтому в данном руководстве под словом «ресурс» понимается все, что находится под управлением кластера.

7.1.1. Установка

Для установки Pacemaker и Corosync необходимо выполнить следующее:

1) на каждом сервере отказоустойчивого кластера установить пакеты `pacemaker` и `pcs`:

```
sudo apt install pacemaker pcs
```

2) на каждом сервере разрешить автозапуск Corosync. Для этого в конфигурационном файле `/etc/default/corosync` указать параметр:

```
START=yes
```

3) на каждом сервере следует произвести запуск необходимых служб `hacluster`:

```
sudo systemctl start corosync
sudo systemctl start pacemaker
sudo systemctl restart pacemaker
```

7.1.2. Пример настройки кластера

Настройка Pacemaker и Corosync на примере двух серверов с ОС: `server-1` и `server-2`. Оба сервера должны видеть друг друга по имени, для этого должен быть настроен DNS или в файле `/etc/hosts` содержаться соответствующие записи.

Для настройки необходимо выполнить следующие действия:

1) на каждом сервере настроить службу синхронизации времени в соответствии с 6.7;

2) на каждом сервере удалить возможно сохранившуюся предыдущую конфигурацию кластера:

```
sudo pcs cluster destroy
```

3) на каждом сервере установить одинаковый пароль (например, 12345678) для учетной записи администратора кластера `hacluster`, выполнив команду и введя пароль при соответствующих запросах:

```
sudo passwd hacluster
```

4) на первом (главном) сервере настроить авторизацию для обоих серверов, выполнив команду:

```
sudo pcs host auth server-1 server-2 -u hacluster -p 12345678
```

Результат выполнения команды:

```
server-2: Authorized
server-1: Authorized
```

5) создать и запустить кластер, последовательно выполнив на первом сервере команды:

```
sudo pcs cluster setup mycluster server-1 server-2 --force
sudo pcs cluster start --all
```

где `mycluster` — имя создаваемого кластера.
Результат выполнения команд:

```
No addresses specified for host 'server-1', using 'server-1'
No addresses specified for host 'server-2', using 'server-2'
Destroying cluster on hosts: 'server-1', 'server-2'...
server-1: Successfully destroyed cluster
server-2: Successfully destroyed cluster
Requesting remove 'pcsd settings' from 'server-1', 'server-2'
server-1: successful removal of the file 'pcsd settings'
server-2: successful removal of the file 'pcsd settings'
Sending 'corosync authkey', 'pacemaker authkey' to 'server-1', 'server-2'
server-1: successful distribution of the file 'corosync authkey'
```

```
server-1: successful distribution of the file 'pacemaker authkey'
server-2: successful distribution of the file 'corosync authkey'
server-2: successful distribution of the file 'pacemaker authkey'
Synchronizing pcsd SSL certificates on nodes 'server-1', 'server-2'...
server-1: Success
server-2: Success
Sending 'corosync.conf' to 'server-1', 'server-2'
server-1: successful distribution of the file 'corosync.conf'
server-2: successful distribution of the file 'corosync.conf'
Cluster has been successfully set up.

server-1: Starting Cluster...
server-2: Starting Cluster...
```

6) на обоих серверах перезапустить службу `pcsd`:

```
sudo systemctl restart pcsd
```

7) на первом сервере включить автозапуск кластера:

```
sudo pcs cluster enable --all
```

Результат выполнения команды:

```
server-1: Cluster Enabled
server-2: Cluster Enabled
```

8) для текущего кластера, состоящего из двух серверов, задать базовые настройки:

   а) отключить использование механизма `stonith`, отвечающего за изоляцию некорректно работающих серверов от основного кластера, выполнив команду:

   ```
   sudo pcs property set stonith-enabled=false
   ```

   ВНИМАНИЕ! Отключать использование `stonith` рекомендуется только при выполнении тестирования, в эксплуатируемых кластерах для предотвращения потери данных `stonith` должен быть включен. Включить механизм `stonith` можно будет после его настройки;

   б) отключить действия при потере кворума (т. к. кворум возможен в кластере из трех и более серверов), выполнив команду:

   ```
   sudo pcs property set no-quorum-policy=ignore
   ```

   в) для возможности запуска ресурсов на любом из серверов кластера включить симметричный кластер командой:

   ```
   sudo pcs property set symmetric-cluster=true
   ```

Если в кластере требуется ограничить запуск ресурсов на определенном сервере, то необходимо отключить использование симметричного кластера командой:

```
sudo pcs property set symmetric-cluster=false
```

При использовании несимметричного кластера необходимо для каждого ресурса указывать правила и приоритет запуска на серверах. Ресурсы, для которых не определены правила и серверы, не будут запускаться.

Для проверки статуса кластера выполнить команду:

```
sudo pcs status
```

Результат выполнения команды:

```
Cluster name: mycluster
Stack: corosync
Current DC: server-1 (version 2.0.1-9e909a5bdd) - partition with quorum
Last updated: Wed Jul 27 16:08:22 2022
Last change: Wed Jul 27 16:07:41 2022 by root via cibadmin on server-1

2 nodes configured
0 resources configured

Online: [ server-1 server-2 ]

No resources

Daemon Status:
corosync: active/enabled
pacemaker: active/enabled
pcsd: active/enabled
```

Если вывод команды показывает, что второй сервер недоступен:

```
Online: [ server-1 ]
OFFLINE: [ server-2 ]
```

следует отредактировать конфигурационный файл `/etc/corosync/corosync.conf` на обоих серверах, заменив имена серверов в строках:

```
ring0_addr: server-1
ring0_addr: server-2
```

на их IP-адреса:

```
ring0_addr: <IP-адрес_server-1>
ring0_addr: <IP-адрес_server-2>
```

После редактирования конфигурационного файла следует перезапустить службу `corosync` на обоих серверах, выполнив команду:

```
sudo systemctl restart corosync
```

Для управления кластером Pacemaker используются инструменты командной строки `pcs` и `crm_mon`.

Управление кластером может также осуществляться через веб-интерфейс:

```
https://server-1:2224/
```

7.2. Keepalived

Keepalived используется в качестве управляющего ПО для организации мониторинга и обеспечения высокой доступности узлов и служб.

Демон Keepalived обеспечивает автоматический переход на резервный ресурс в режиме ожидания в случае возникновения ошибки или сбоя основного ресурса.

Для обеспечения автоматического перехода используется протокол VRRP (Virtual Redundancy Routing Protocol). Данный протокол позволяет использовать виртуальный IP-адрес VIP (virtual IP), который является плавающим (расшаренным) между узлами.

7.2.1. Установка

Пакет Keepalived необходимо установить на каждом узле, доступность которых требуется обеспечить, и на каждом резервном узле. Для установки выполнить следующую команду:

```
apt install keepalived
```

7.2.2. Пример настройки

Настройка Keepalived на примере двух серверов с ОС: `server-1` (основной) и `server-2` (резервный). На серверах должен быть настроен режим репликации для обеспечения

горячего резервирования. Также на обоих серверах должно быть два сетевых интерфейса. Одному из сетевых интерфейсов основного сервера присвоить VIP.

На каждом сервере в конфигурационный файл `/etc/sysctl.conf` добавить строку:

```
net.ipv4.ip_forward = 1
net.ipv4.ip_nonlocal_bind = 1
```

и выполнить для проверки команду:

```
sysctl -p
```

На основном сервере откорректировать конфигурационный файл Keepalived `/etc/keepalived/keepalived.conf`, указав необходимые значения для основных параметров:

- `interface` — интерфейс подключения;
- `state` — статус сервера, для основного указывается значение `MASTER`;
- `virtual_router_id` — идентификатор виртуального маршрутизатора (должен быть одинаковым для обоих серверов);
- `priority` — приоритет основного сервера. Должен быть больше, чем резервного;
- `auth_type` — значение `PASS` задает парольную аутентификацию для серверов;
- `auth_pass` — общий пароль для всех узлов кластера;
- `virtual_ipaddress` — виртуальный IP-адрес.

Пример

Конфигурационный файл `/etc/keepalived/keepalived.conf` основного сервера

```
global_defs {
   notification_email {
       username@domain.ru
   }
   notification_email_from servers@domain.ru
       smtp_server 1.1.1.1
       smtp_connect_timeout 30
       router_id main
}

vrrp_instance server-1 {
   interface enp0s3
```

```
    state MASTER
    virtual_router_id 200
    priority 100
    advert_int 1
    authentication {
        auth_type PASS
        auth_pass password
         }

    virtual_ipaddress {
        10.1.9.190/32 dev enp0s3
         }

}
```

Для применения настроек и запуска демона Keepalived выполнить команду:

```
systemctl start keepalived
```

Далее необходимо откорректировать конфигурационный файл Keepalived `/etc/keepalived/keepalived.conf` резервного сервера, указав необходимые значения для основных параметров:

- `interface` — интерфейс подключения;
- `state` — статус сервера, для резервного указывается значение `BACKUP`;
- `virtual_router_id` — идентификатор виртуального маршрутизатора (должен быть одинаковым для обоих серверов);
- `priority` — приоритет резервного сервера. Должен быть меньше, чем основного;
- `auth_type` — значение `PASS` задает парольную аутентификацию для серверов;
- `auth_pass` — общий пароль для всех узлов кластера;
- `virtual_ipaddress` — виртуальный IP-адрес.

Пример

Конфигурационный файл `/etc/keepalived/keepalived.conf` резервного сервера

```
global_defs {
    notification_email {
        username@domain.ru
    }
    notification_email_from servers@domain.ru
```

```
        smtp_server 1.1.1.1
        smtp_connect_timeout 30
        router_id reserve
}

vrrp_instance server-2 {
   interface enp0s3
   state BACKUP
   virtual_router_id 200
   priority 50
   advert_int 1
   authentication {
       auth_type PASS
       auth_pass password
 }

   virtual_ipaddress {
       10.4.1.190/32 dev enp0s3
 }
}
```

Для применения настроек и запуска демона Keepalived выполнить команду:

```
systemctl start keepalived
```

7.3. Распределенная файловая система Ceph

Распределенные файловые системы используются в высокоскоростных вычислениях и фокусируются на высокой доступности, производительности и масштабируемости. ОС поддерживает распределенную файловую систему Ceph.

Ceph — распределенная объектная система хранения, предоставляющая файловый и блочный интерфейсы доступа. Ceph представляет собой кластер узлов, выполняющих различные функции, обеспечивая хранение и репликацию данных, а также распределение нагрузки, что гарантирует высокую доступность и надежность. При добавлении или удалении новых узлов кластера массив хранимых данных автоматически балансируется с учетом внесенных изменений.

Схема программных компонентов Ceph представлена на рис. 1.

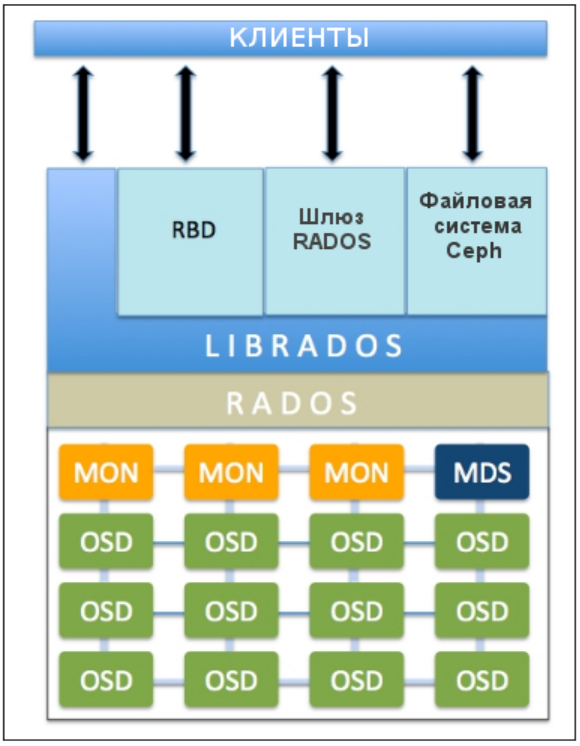

Рис. 1

Основой Ceph является служба RADOS (безотказное автономное распределенное хранилище объектов, Reliable Autonomic Distributed Object Store). В кластере Ceph данные хранятся в виде объектов, а служба RADOS обеспечивает хранение этих объектов независимо от их типа данных. Чтобы обеспечить высокую доступность и надежность системы хранения, служба RADOS осуществляет репликацию данных, обнаружение отказов и восстановление данных, а также миграцию данных и балансировку кластера при добавлении дополнительного устройства хранения или его извлечении.

Служба OSD (служба хранения объектов, Object Storage Daemon) обеспечивает хранение данных и обрабатывает запросы клиентов, обмениваясь данными с другими экземплярами службы OSD. Как правило, один экземпляр службы OSD связан с одним физическим устройством хранения.

Служба MON (монитор, monitor) отслеживает состояние всего кластера путем хранения карты состояния кластера, которая включает в себя карты состояния других программных компонентов Ceph. Для обеспечения высокой доступности и надежности кластера рекомендуется разворачивать три или пять экземпляров службы MON на различных узлах кластера. Главное, чтобы количество экземпляров было нечетным для обеспечения кворума. Если больше половины экземпляров службы MON будут недоступны, операция записи данных в кластер заблокируется для предотвращения рассогласованности данных.

Служба MGR (администратор, manager) отслеживает метрики времени выполнения различных команд и параметры состояния кластера Ceph, включая использование хранилища, текущие метрики производительности и нагрузку на систему. Служба MGR предоставляет

интерфейс взаимодействия для внешних систем управления и мониторинга. Для обеспечения высокой доступности и надежности кластера рекомендуется развернуть несколько экземпляров службы MGR на различных узлах кластера. Как правило, служба MGR разворачивается на тех же узлах кластера, на которых развернуты экземпляры службы MON. При этом в активном режиме функционирует только один экземпляр службы MGR, остальные экземпляры находятся в режиме ожидания.

Библиотека `librados` предоставляет интерфейс доступа к службе RADOS с поддержкой языков программирования PHP, Ruby, Python, C и C++.

Служба RBD (блочное устройство RADOS, RADOS block device) предоставляет пользователю возможность создавать и использовать виртуальные блочные устройства произвольного размера. Программный интерфейс RBD позволяет работать с этими устройствами в режиме чтения/записи и выполнять служебные операции — изменение размера, клонирование, создание и возврат к снимку состояния и т. д.

Шлюз RADOS позволяет использовать Ceph для хранения пользовательских объектов и предоставляет API, совместимый с Amazon S3 RESTful и OpenStack Swift.

Файловая система Ceph (CephFS) — POSIX-совместимая файловая система, использующая Ceph в качестве хранилища. Для того чтобы клиенты могли подключать Ceph как файловую систему, в кластере необходимо развернуть хотя бы один экземпляр службы MDS.

Служба MDS (сервер метаданных, MetaData Server) обеспечивает синхронное состояние файлов в точках монтирования CephFS. Служба MDS отслеживает метаданные файловой иерархии и сохраняет их только для CephFS. Использует активную копию и резервные, причем активная копия в пределах кластера только одна.

7.3.1. Развертывание Ceph

Пример развертывания распределенного хранилища на базе кластера Ceph из трех узлов `node1`, `node2` и `node3`. На узлах кластера будут развернуты службы MON и OSD. Кроме того, на узле `node1` будет запущена служба MGR.

ВНИМАНИЕ! Данная конфигурация предназначена только для ознакомления и тестирования Ceph. При развертывании кластера Ceph на объекте эксплуатации не рекомендуется размещать службы MON и OSD на одном узле.

В описываемой конфигурации в составе каждого из узлов кластера имеются два жестких диска: на дисках `sda` установлена ОС, диски `sdb` будут задействованы для хранения данных.

Как правило, в кластере Ceph используются две сети: одна используется для организации взаимодействия пользователей и служб Ceph, вторая — для репликации данных. В описы-

ваемой конфигурации для этих целей будет использоваться один сегмент сети. Сетевым интерфейсам узлов назначен фиксированный IP-адрес:

- 10.0.0.171 для узла `node1`;
- 10.0.0.172 для узла `node2`;
- 10.0.0.173 для узла `node3`.

В описываемой конфигурации на узлах кластера настроена служба синхронизации времени в соответствии с 6.7.

Для развертывания кластера Ceph необходимо выполнить следующие действия:

1) развернуть первый экземпляр службы MON (см. 7.3.1.1);
2) добавить необходимое количество экземпляров службы MON (см. 7.3.1.2);
3) развернуть необходимое количество экземпляров службы MGR (см. 7.3.1.3);
4) развернуть необходимое количество экземпляров службы OSD (см. 7.3.1.4).

7.3.1.1. Инициализация первого экземпляра службы MON

Для инициализации первого экземпляра службы MON на одном из узлов кластера необходимо выполнить следующие действия:

1) установить пакет ceph:

```
sudo apt install ceph
```

2) сгенерировать идентификатор кластера в формате UUID командой:

```
uuidgen
```

Пример вывода после выполнения команды:

```
f98c5e15-6736-41e9-966d-e38798029719
```

3) создать конфигурационный файл `/etc/ceph/<кластер>.conf` со следующими строками:

```
[global]
fsid = <идентификатор_кластера>
mon initial members = <узел_MON>
mon host = <адрес_узла_MON>
public network = <сеть_управления>
cluster network = <сеть_данных>
auth_allow_insecure_global_id_reclaim = false
osd_pool_default_pg_autoscale_mode = off
```

где <кластер> — условное наименование кластера. По умолчанию используется наименование ceph;

<идентификатор_кластера> — идентификатор в формате UUID;

<узел_MON> — сетевое имя узла, на котором будет развернут первый экземпляр службы MON;

<адрес_узла_MON> — IP-адрес узла, на котором будет развернут первый экземпляр службы MON;

<сеть_управления> — параметры сети, которая используется для взаимодействия пользователей и служб Ceph;

<сеть_данных> — параметры сети, которая используется для репликации данных. В описываемой конфигурации будет использоваться тот же сегмент, что и для сети управления.

В параметре auth_allow_insecure_global_id_reclaim заданное значение false устанавливает запрет на подключение к кластеру тех клиентов, которые не могут безопасным образом восстановить свой идентификатор.

В параметре osd_pool_default_pg_autoscale_mode заданное значение false устанавливает запрет на автоматическое изменение количества групп размещения в пуле.

В описываемой конфигурации файл /etc/ceph/ceph.conf имеет следующие строки:

```
[global]
fsid = f98c5e15-6736-41e9-966d-e38798029719
mon initial members = node1
mon host = 10.0.0.171
public network = 10.0.0.1/24
cluster network = 10.0.0.1/24
auth_allow_insecure_global_id_reclaim = false
osd_pool_default_pg_autoscale_mode = off
```

4) сгенерировать ключ для службы MON:

```
sudo ceph-authtool --create-keyring /tmp/ceph.mon.keyring --gen-key \
     -n mon. --cap mon 'allow *'
```

5) сгенерировать ключ администратора кластера:

```
sudo ceph-authtool --create-keyring /etc/ceph/ceph.client.admin.keyring \
     --gen-key -n client.admin --cap mon 'allow *' --cap osd 'allow *' \
     --cap mds 'allow *' --cap mgr 'allow *'
```

6) добавить ключ администратора кластера в файл с ключом службы MON:

```
sudo ceph-authtool /tmp/ceph.mon.keyring --import-keyring \
     /etc/ceph/ceph.client.admin.keyring
```

7) сгенерировать ключ для службы OSD:

```
sudo ceph-authtool --create-keyring \
     /var/lib/ceph/bootstrap-osd/ceph.keyring --gen-key -n \
     client.bootstrap-osd --cap mon 'profile bootstrap-osd' \
     --cap mgr 'allow r'
```

8) добавить ключ службы OSD в файл с ключом службы MON:

```
sudo ceph-authtool /tmp/ceph.mon.keyring --import-keyring \
     /var/lib/ceph/bootstrap-osd/ceph.keyring
```

9) сформировать карту состояния кластера командой:

```
monmaptool --create --add <узел_MON> <адрес_узла_MON> \
     --fsid <идентификатор_кластера> /tmp/monmap
```

В описываемой конфигурации команда имеет вид:

```
monmaptool --create --add node1 10.0.0.171 \
     --fsid f98c5e15-6736-41e9-966d-e38798029719 /tmp/monmap
```

10) создать рабочий каталог для первого экземпляра службы MON командой:

```
sudo mkdir /var/lib/ceph/mon/<кластер>-<узел_MON>
```

В описываемой конфигурации команда имеет вид:

```
sudo mkdir /var/lib/ceph/mon/ceph-node1
```

11) инициализировать рабочий каталог службы MON, указав карту состояния кластера и ключевой файл:

```
sudo ceph-mon --mkfs -i <узел_MON> ----monmap /tmp/monmap \
     --keyring /tmp/ceph.mon.keyring
```

В описываемой конфигурации команда имеет вид:

```
sudo ceph-mon --mkfs -i node1 --monmap /tmp/monmap --keyring \
     /tmp/ceph.mon.keyring
```

12) системного пользователя ceph установить владельцем рабочего каталога службы MON:

```
sudo chown -R ceph:ceph /var/lib/ceph/mon
```

13) запустить службу MON в качестве системной службы, для этого последовательно выполнить следующие команды:

```
sudo systemctl enable ceph-mon.target
sudo systemctl enable ceph-mon@<узел>
sudo systemctl start ceph-mon@<узел>
```

Пример команд для описываемой конфигурации:

```
sudo systemctl enable ceph-mon.target
sudo systemctl enable ceph-mon@node1
sudo systemctl start ceph-mon@node1
```

14) включить использование второй версии протокола сетевого обмена между экземплярами службы MON:

```
sudo ceph mon enable-msgr2
```

15) вывести информацию о кластере Ceph:

```
sudo ceph -s
```

Пример вывода после выполнения команды:

```
cluster:
id:     f98c5e15-6736-41e9-966d-e38798029719
health: HEALTH_OK

services:
mon: 1 daemons, quorum node1 (age 39s)
mgr: no daemons active
osd: 0 osds: 0 up, 0 in

data:
pools:   0 pools, 0 pgs
objects: 0 objects, 0 B
usage:   0 B used, 0 B / 0 B avail
pgs:
```

Сообщение вида:

```
health: HEALTH_OK
```

указывает на корректность выполненных настроек.

7.3.1.2. Добавление нового экземпляра службы MON

Дополнительные экземпляры службы MON разворачиваются на отдельных узлах кластера Ceph. В описываемой конфигурации экземпляры службы MON будут развернуты на узлах `node2` и `node3`.

Для развертывания нового экземпляра службы MON необходимо выполнить следующие действия:

1) на узле, на котором развернут первый экземпляр службы MON, в конфигурационный файл /etc/ceph/ceph.conf добавить информацию об узлах, на которых будут развернуты дополнительные экземпляры службы MON:

```
mon initial members = <узел_1>, <узел_2> ...  <узел_N>
mon host = <IP-адрес_узла_1>, <IP-адрес_узла_2> ... <IP-адрес_узла_N>
```

Для описываемой конфигурации в файле /etc/ceph/ceph.conf необходимо указать следующую информацию об узлах:

```
...
mon initial members = node1,node2,node3
mon host = 10.0.0.171,10.0.0.172,10.0.0.173
...
```

2) на дополнительных узлах установить пакет ceph-mon:

```
sudo apt install ceph-mon
```

3) на дополнительных узлах получить копии конфигурационного файла /etc/ceph/ceph.conf и ключа администратора кластера /etc/ceph/ceph.client.admin.keyring. Для этого можно воспользоваться следующими командами:

```
ssh <администратор>@<первый_MON> "cat /etc/ceph/ceph.conf" \
    | sudo tee /etc/ceph/ceph.conf
ssh <администратор>@<первый_MON> "sudo -S cat \
     /etc/ceph/ceph.client.admin.keyring" \ | sudo tee \
     /etc/ceph/ceph.client.admin.keyring
```

где <администратор> — локальный администратор узла, на котором развернут первый экземпляр службы MON;

<первый_MON> — IP-адрес узла, на котором развернут первый экземпляр службы MON.

Пример команд для описываемой конфигурации:

```
ssh astra@10.0.0.171 "cat /etc/ceph/ceph.conf" \
    | sudo tee /etc/ceph/ceph.conf
ssh astra@10.0.0.171 "sudo -S cat /etc/ceph/ceph.client.admin.keyring" \
    | sudo tee /etc/ceph/ceph.client.admin.keyring
```

4) на дополнительных узлах получить карту состояния кластера:

```
sudo ceph mon getmap -o /tmp/ceph.map
```

5) на дополнительных узлах получить ключ службы MON:

```
sudo ceph auth get mon. -o /tmp/ceph.mon.keyring
```

6) на дополнительных узлах инициализировать рабочий каталог службы MON, указав карту состояния кластера и ключевой файл:

```
sudo ceph-mon -i <узел> --mkfs --monmap /tmp/ceph.map \
     --keyring /tmp/ceph.mon.keyring
```

Пример команд для описываемой конфигурации:

а) на узле node2:

```
sudo ceph-mon -i node2 --mkfs --monmap /tmp/ceph.map \
     --keyring /tmp/ceph.mon.keyring
```

б) на узле node3:

```
sudo ceph-mon -i node3 --mkfs --monmap /tmp/ceph.map \
     --keyring /tmp/ceph.mon.keyring
```

7) на дополнительных узлах для каталога /var/lib/ceph/mon/ceph-<узел> установить владельцем системного пользователя ceph. Пример команд для описываемой конфигурации:

а) на узле node2:

```
sudo chown -R ceph:ceph /var/lib/ceph/mon/ceph-node2
```

б) на узле node3:

```
sudo chown -R ceph:ceph /var/lib/ceph/mon/ceph-node3
```

8)) на дополнительных узлах запустить службу MON в качестве системной службы, для этого последовательно выполнить следующие команды:

```
sudo systemctl enable ceph-mon.target
sudo systemctl enable ceph-mon@<узел>
sudo systemctl start ceph-mon@<узел>
```

Пример команд для описываемой конфигурации:

а) на узле node2:

```
sudo systemctl enable ceph-mon.target
sudo systemctl enable ceph-mon@node2
sudo systemctl start ceph-mon@node2
```

на узле node3:

```
sudo systemctl enable ceph-mon.target
sudo systemctl enable ceph-mon@node3
sudo systemctl start ceph-mon@node3
```

9) на одном из узлов вывести информацию о кластере Ceph:

```
sudo ceph -s
```

В случае успешного развертывания дополнительных экземпляров службы MON в терминале отобразится информация о количестве функционирующих экземпляров. Пример вывода после выполнения команды для описываемой конфигурации:

```
...
services:
mon: 3 daemons, quorum node1,node3,node2 (age 44s)
...
```

7.3.1.3. Добавление экземпляра службы MGR

Как правило, служба MGR разворачивается на тех же узлах кластера, на которых развернуты экземпляры службы MON. В описываемой конфигурации экземпляр службы MGR будет развернут на узле `node1`.

Для развертывания экземпляра службы MGR на узле кластера необходимо выполнить следующие действия:

1) установить пакет `ceph-mgr`:

```
sudo apt install ceph-mgr
```

Для описываемой конфигурации указанная команда не выполняется, так как пакет `ceph-mgr` устанавливается автоматически при установке пакета `ceph`;

2) создать рабочий каталог для экземпляра службы MGR командой:

```
sudo mkdir /var/lib/ceph/mgr/<кластер>-<узел>
```

В описываемой конфигурации команда имеет вид:

```
sudo mkdir /var/lib/ceph/mgr/ceph-node1
```

3) сгенерировать ключ для службы MGR:

```
sudo ceph auth get-or-create mgr.`hostname -s` mon 'allow profile mgr' \
     osd 'allow *' mds 'allow *' \
     -o /var/lib/ceph/mgr/<кластер>-<узел>/keyring
```

В описываемой конфигурации команда имеет вид:

```
sudo ceph auth get-or-create mgr.`hostname -s` mon 'allow profile mgr' \
     osd 'allow *' mds 'allow *' \
     -o /var/lib/ceph/mgr/ceph-node1/keyring
```

4) для рабочего каталога службы MGR установить владельцем системного пользователя ceph:

```
sudo chown -R ceph:ceph /var/lib/ceph/mgr
```

5) запустить экземпляр службы MGR в качестве системной службы, для этого последовательно выполнить следующие команды:

```
sudo systemctl enable ceph-mgr.target
sudo systemctl enable ceph-mgr@<узел>
sudo systemctl start ceph-mgr@<узел>
```

Пример команд для описываемой конфигурации:

```
sudo systemctl enable ceph-mgr.target
sudo systemctl enable ceph-mgr@node1
sudo systemctl start ceph-mgr@node1
```

Запуск экземпляра службы MGR может занять длительное время. Для просмотра текущего статуса службы можно воспользоваться командой:

```
sudo systemctl status ceph-mgr@<узел>
```

6) вывести информацию о кластере Ceph:

```
sudo ceph -s
```

В случае успешного развертывания экземпляра службы MGR в терминале отобразится информация о количестве функционирующих экземпляров. Пример вывода после выполнения команды для описываемой конфигурации:

```
...
services:
...
mgr: node1(active, since 7s)
...
```

7.3.1.4. Добавление экземпляра службы OSD

Экземпляры службы OSD разворачиваются на отдельных узлах кластера Ceph. Как правило, один экземпляр службы OSD связан с одним физическим диском кластера. В описываемой конфигурации экземпляры службы OSD будут развернуты на узлах `node1`, `node2` и `node3`.

ВНИМАНИЕ! Данная конфигурация предназначена только для ознакомления и тестирования Ceph. При развертывании кластера Ceph на объекте эксплуатации не рекомендуется размещать службы MON и OSD на одном узле.

Для развертывания экземпляра службы OSD необходимо выполнить следующие действия:

1) на дополнительных узлах (в описываемой конфигурации это `node2` и `node3` установить пакет `ceph-osd`:

```
sudo apt install ceph-osd
```

2) на дополнительных узлах получить минимально необходимую конфигурацию кластера:

```
ssh <администратор>@<первый_MON> \
   "sudo -S ceph config generate-minimal-conf" \
   | sudo tee /etc/ceph/ceph.conf
```

где <администратор> — локальный администратор узла, на котором развернут первый экземпляр службы MON;

<первый_MON> — IP-адрес узла, на котором развернут первый экземпляр службы MON.

В описываемой конфигурации этот шаг не выполняется, так как на узлах node2 и node3 уже имеется конфигурационный файл /etc/ceph/ceph.conf;

3) на дополнительных узлах получить копию ключа службы OSD:

```
ssh <администратор>@<первый_MON> "sudo -S cat \
     /var/lib/ceph/bootstrap-osd/ceph.keyring" \
     | sudo tee /var/lib/ceph/bootstrap-osd/ceph.keyring
```

где <администратор> — локальный администратор узла, на котором развернут первый экземпляр службы MON;

<первый_MON> — IP-адрес узла, на котором развернут первый экземпляр службы MON.

В описываемой конфигурации команда имеет вид:

```
ssh astra@10.0.0.171 "sudo -S cat \
     /var/lib/ceph/bootstrap-osd/ceph.keyring" \
     | sudo tee /var/lib/ceph/bootstrap-osd/ceph.keyring
```

4) на всех узлах инициализировать экземпляр службы OSD командой:

```
sudo ceph-volume lvm create --data <диск>
```

В описываемой конфигурации команда имеет вид:

```
sudo ceph-volume lvm create --data /dev/sdb
```

Пример вывода после успешного выполнения команды:

```
...
--> ceph-volume lvm activate successful for osd ID: 0
--> ceph-volume lvm create successful for: /dev/sdb
```

5) на одном из узлов с развернутой службой MON вывести информацию о кластере Ceph:

```
sudo ceph -s
```

В случае успешного развертывания экземпляров службы OSD в терминале отобразится информация о количестве функционирующих экземпляров. Пример вывода после выполнения команды для описываемой конфигурации:

```
...
services:
...
osd: 3 osds: 3 up (since 43s), 3 in (since 57s)
...
```

7.3.2. Использование кластера Ceph

Ceph представляет для клиента различные варианты доступа к данным:

1) файловая система Ceph (CephFS);
2) программный интерфейс RBD;
3) шлюз RADOS.

CephFS предоставляет возможность монтировать один и тот же каталог с данными на чтение и запись множеству клиентов.

Для того чтобы клиенты могли использовать кластер Ceph как файловую систему, необходимо выполнить следующие действия:

1) инициализировать файловую систему (см. 7.3.2.1);
2) развернуть хотя бы один экземпляр службы MDS (см. 7.3.2.2);
3) настроить разделяемый ресурс (см. 7.3.2.3);
4) настроить подключение клиента к разделяемому ресурсу (см. 7.3.2.4).

7.3.2.1. Инициализация CephFS

Чтобы инициализировать файловую систему, на узле с развернутой службой MON необходимо выполнить команду:

```
sudo ceph fs volume create <наименование_фс>
```

В описываемой конфигурации команда имеет вид:

```
sudo ceph fs volume create testcephfs
```

Примечание. В процессе выполнения команды будут автоматически созданы два пула ресурсов хранения: один для размещения метаданных и второй для размещения пользовательских данных.

Чтобы вывести информацию о файловых системах, имеющихся в кластере, на узле с развернутой службой MON необходимо выполнить команду:

```
sudo ceph fs ls
```

Пример вывода после выполнения команды:

```
name: testcephfs, metadata pool: cephfs.testcephfs.meta, data pools:
[cephfs.testcephfs.data]
```

7.3.2.2. Добавление экземпляра службы MDS

В описываемой конфигурации экземпляр службы MDS будет развернут на узле `node1`.

Для развертывания экземпляра службы MDS на узле кластера необходимо выполнить следующие действия:

1) создать рабочий каталог для экземпляра службы MDS командой:

```
sudo mkdir -p /var/lib/ceph/mds/<кластер>-<узел>
```

В описываемой конфигурации команда имеет вид:

```
sudo mkdir -p /var/lib/ceph/mds/ceph-node1
```

2) сгенерировать ключ для службы MDS и разместить его в рабочем каталоге экземпляра службы MDS:

```
sudo ceph auth get-or-create mds.<узел> mon 'profile mds' \
     mgr 'profile mds' mds 'allow *' osd 'allow *' \
     -o /var/lib/ceph/mds/<кластер>-<узел>/keyring
```

В описываемой конфигурации команда имеет вид:

```
sudo ceph auth get-or-create mds.node1 mon 'profile mds' \
     mgr 'profile mds' mds 'allow *' osd 'allow *' \
     -o /var/lib/ceph/mds/ceph-node1/keyring
```

3) для рабочего каталога службы MDS установить владельцем системного пользователя `ceph`:

```
sudo chown -R ceph:ceph /var/lib/ceph/mds
```

4) запустить экземпляр службы MDS в качестве системной службы, для этого последовательно выполнить следующие команды:

```
sudo systemctl enable ceph-mds.target
sudo systemctl enable ceph-mds@<узел>
sudo systemctl start ceph-mds@<узел>
```

Пример команд для описываемой конфигурации:

```
sudo systemctl enable ceph-mds.target
sudo systemctl enable ceph-mds@node1
sudo systemctl start ceph-mds@node1
```

5) вывести информацию о кластере Ceph:

```
sudo ceph -s
```

В случае успешного развертывания экземпляра службы MDS в терминале отобразится информация о количестве функционирующих экземпляров.
Пример вывода после выполнения команды для описываемой конфигурации:

```
...
services:
...
mds: 1/1 daemons up
...
```

Примечание. Пока в кластере Ceph не будет создана файловая система служба MDS находится в неактивном режиме. В связи с этим информация об экземплярах службы MDS не отображается в выводе после выполнения команды:

```
sudo ceph -s
```

7.3.2.3. Подготовка разделяемого ресурса

Чтобы создать разделяемый ресурс, к которому будут подключаться клиенты, на узле с развернутой службой MON необходимо выполнить команду:

```
sudo ceph fs subvolume create <наименование_фс> <ресурс>
```

В описываемой конфигурации команда имеет вид:

```
sudo ceph fs subvolume create testcephfs data1
```

Чтобы настроить доступ к разделяемому ресурсу, на узле с развернутой службой MON необходимо выполнить команду:

```
sudo ceph fs subvolume authorize <наименование_фс> <ресурс> \
     <имя_пользователя> --access-level=<права_доступа>
```

В описываемой конфигурации команда имеет вид:

```
sudo ceph fs subvolume authorize testcephfs data1 user1 --access-level=rw
```

Примечание. Создавать учетные записи предварительно не требуется. В процессе выполнения команды будет автоматически создана учетная запись пользователя, которой будут присвоены указанные права доступа к разделяемому ресурсу.

7.3.2.4. Настройка подключения клиента к разделяемому ресурсу

Для подключения к разделяемому ресурсу необходимы следующие сведения:

- полный путь к разделяемому ресурсу;
- ключ пользователя, которому предоставлен доступ к разделяемому ресурсу.

Чтобы получить указанные сведения, на узле с развернутой службой MON необходимо выполнить команду:

```
sudo ceph auth ls | grep <имя_пользователя> -A2
```

Для описываемой конфигурации команда имеет вид:

```
sudo ceph auth ls | grep user1 -A2
```

Пример вывода после выполнения команды:

```
client.user1
key: AQD9D2hm+0psJxAArn5iVMhDewigF/E6r+dlCg==
caps: [mds] allow rw
path=/volumes/_nogroup/data1/1de2e9d3-fed9-47bc-824a-c6e5ab5512e3
```

Настройка подключения разделяемого ресурса на узле кластера

Для подключения разделяемого ресурса на узле кластера Ceph необходимо выполнить следующие действия:

1) получить ключ пользователя, которому предоставлен доступ к разделяемому ресурсу командой:

```
ssh <администратор>@<первый_MON> "sudo -S ceph auth get-or-create \
    client.user1" | sudo tee /etc/ceph/ceph.client.user1.keyring
```

где <администратор> — локальный администратор узла, на котором развернут первый экземпляр службы MON;

<первый_MON> — IP-адрес узла, на котором развернут первый экземпляр службы MON.

Для описываемой конфигурации команда имеет вид:

```
ssh astra@10.0.0.171 "sudo -S ceph auth get-or-create client.user1" \
    | sudo tee /etc/ceph/ceph.client.user1.keyring
```

2) подключить разделяемый ресурс командой:

```
sudo mount.ceph <имя_пользователя>@.<наименование_фс>=<ресурс> \
    <локальный_каталог>
```

где <наименование_фс> — наименование инициализированной файловой системы (см. 7.3.2.1);

ВНИМАНИЕ! Обязательно должен присутствовать символ точки (« . ») перед наименованием файловой системы;

<имя_пользователя> — имя пользователя, которому предоставлен доступ к разделяемому ресурсу;

<ресурс> — полный путь к разделяемому ресурсу;

<локальный_каталог> — локальный каталог, в который необходимо смонтировать разделяемый ресурс.

Для описываемой конфигурации команда имеет вид:

```
sudo mount.ceph user1@.testcephfs=\
    /volumes/_nogroup/data1/4025b53e-8df1-49b1-adee-365e0eeafc6d /mnt/
```

Настройка подключения разделяемого ресурса на внешнем компьютере с использованием инструментов Ceph

Для подключения разделяемого ресурса на компьютере, не входящем в кластер Ceph, необходимо выполнить следующие действия:

1) установить пакет ceph-common:

```
sudo apt install ceph-common
```

2) получить минимально необходимую конфигурацию кластера:

```
ssh <администратор>@<первый_MON> "sudo -S ceph config \
     generate-minimal-conf" | sudo tee /etc/ceph/ceph.conf
```

где <администратор> — локальный администратор узла, на котором развернут первый экземпляр службы MON;

<первый_MON> — IP-адрес узла, на котором развернут первый экземпляр службы MON.

Для описываемой конфигурации команда имеет вид:

```
ssh astra@10.0.0.171 "sudo -S ceph config generate-minimal-conf" \
     | sudo tee /etc/ceph/ceph.conf
```

3) получить ключ пользователя, которому предоставлен доступ к разделяемому ресурсу командой:

```
ssh <администратор>@<первый_MON> "sudo -S ceph auth get-or-create \
     client.user1" | sudo tee /etc/ceph/ceph.client.user1.keyring
```

где <администратор> — локальный администратор узла, на котором развернут первый экземпляр службы MON;

<первый_MON> — IP-адрес узла, на котором развернут первый экземпляр службы MON.

Для описываемой конфигурации команда имеет вид:

```
ssh astra@10.0.0.171 "sudo -S ceph auth get-or-create client.user1" \
     | sudo tee /etc/ceph/ceph.client.user1.keyring
```

4) подключить разделяемый ресурс командой:

```
sudo mount.ceph <имя_пользователя>@.<наименование_фс>=<ресурс> \
     <локальный_каталог>
```

где <наименование_фс> — наименование инициализированной файловой системы (см. 7.3.2.1);

ВНИМАНИЕ! Обязательно должен присутствовать символ точки (« . ») перед наименованием файловой системы;

<имя_пользователя> — имя пользователя, которому предоставлен доступ к разделяемому ресурсу;

<ресурс> — полный путь к разделяемому ресурсу;

<локальный_каталог> — локальный каталог, в который необходимо смонтировать разделяемый ресурс.

Для описываемой конфигурации команда имеет вид:

```
sudo mount.ceph user1@.testcephfs=\
    /volumes/_nogroup/data1/4025b53e-8df1-49b1-adee-365e0eeafc6d /mnt/
```

Настройка подключения разделяемого ресурса на внешнем компьютере без использования инструментов Ceph

Если на компьютере, не входящем в кластер Ceph, нет возможности установить пакет ceph-common, то подключить разделяемый ресурс можно следующей командой:

```
sudo mount -t ceph <узлы_MON>:<ресурс> <локальный_каталог> \
     -o name=<имя_пользователя>,secret=<ключ>
```

где <узлы_MON> — IP-адреса узлов кластера, на которых развернуты экземпляры службы MON;

<ресурс> — полный путь к разделяемому ресурсу;

<локальный_каталог> — локальный каталог, в который необходимо смонтировать разделяемый ресурс;

<имя_пользователя> — имя пользователя, которому предоставлен доступ к разделяемому ресурсу;

<ключ> — ключ пользователя, которому предоставлен доступ к разделяемому ресурсу.

Для описываемой конфигурации команда имеет вид:

```
sudo mount -t ceph 10.0.0.171,10.0.0.172,10.0.0.173:\
     /volumes/_nogroup/data1/1de2e9d3-fed9-47bc-824a-c6e5ab5512e3 \
     /mnt/ -o name=user1,secret='AQD9D2hm+0psJxAArn5iVMhDewigF/E6r+dlCg=='
```

Сообщение об ошибке вида:

```
2024-06-25T08:21:48.660+0300 76ae9321bfc0 -1 auth: unable to find a keyring on
/etc/ceph/ceph.client.user1.keyring, /etc/ceph/ceph.keyring,/etc/ceph/keyring,
/etc/ceph/keyring.bin: (2) No such file or directory
```

можно игнорировать, такое сообщение появляется в случае, если в ОС установлено программное обеспечение Ceph. В таком случае производится попытка подключить разделяемый ресурс в первую очередь с использованием инструментов Ceph. Затем, в случае неудачи, производится попытка подключить разделяемый ресурс с использованием аутентификационных параметров, указанных в команде в качестве аргументов.

7.4. Средство эффективного масштабирования HAProxy

Для эффективного масштабирования используется программное средство HAProxy. HAProxy обеспечивает высокую доступность, отказоустойчивость и распределение нагрузки для TCP- и HTTP-приложений посредством распределения входящих запросов на несколько обслуживающих серверов.

HAProxy предоставляет следующие возможности:

- периодическая проверка доступности обслуживающих серверов, на которые перенаправляются запросы пользователей;
- несколько алгоритмов определения доступности сервера: tcp-check, http-check, mysql-check;
- распределение HTTP/HTTPS/TCP-запросов между доступными серверами;

- возможность закрепления определенных клиентов за конкретными обслуживающими серверам (stick-tables);
- поддержка IPv6 и UNIX sockets, HTTP/1.1 сжатия (deflate, gzip, libslz), SSL, полная поддержка постоянного HTTP-соединения;
- поддержка переменных блоков и Lua-сценариев в конфигурации сервера;
- веб-интерфейс с актуальным состоянием и статистикой работы программы.

7.4.1. Установка

На основном сервере, который будет принимать запросы и распределять их, необходимо установить пакет HAProxy:

```
apt install haproxy
```

7.4.2. Настройка

Настройка выполняется в конфигурационном файле `/etc/haproxy/haproxy.cfg`, включающем следующие разделы:

- `global` — определяет общую конфигурацию для всего HAProxy;
- `defaults` — является обязательным и определяет настройки по умолчанию для остальных разделов;
- `frontend` — используется для описания набора интерфейсов для принятия соединений от клиентов, а также правил распределения нагрузки;
- `backend` — используется для описания набора серверов, к которым будет выполняться подключение переадресованных входящих соединений, а также определения алгоритма распределения нагрузки;
- `listen` — объединенный раздел для описания `frontend` и `backend`. Используется для описания прокси-сервера в одном разделе, как правило, только для TCP-трафика.

В таблице 36 представлены основные примеры значений параметров конфигурационного файла и их описание.

Таблица 36

Раздел	Параметр	Описание
`global`	`log <address> <facility> [max level [min level]]` Например, `log 127.0.0.1 local0 notice`	Добавляет сервер системного журнала. `<facility>` — должен быть одним из 24 стандартных типов регистрации событий: `kern user mail daemon auth syslog lpr news uucp cron auth2 ftp ntp audit alert cron2 local0 local1 local2 local3 local4 local5 local6 local7`

Продолжение таблицы 36

Раздел	Параметр	Описание
	`maxconn <number>` Например, `maxconn 10000`	Устанавливает максимальное число одновременных подключений для каждого процесса `haproxy`
	`nbproc <number>` Например, `nbproc 2`	Задает количество процессов `haproxy`. По умолчанию создается только один процесс `haproxy`
	`daemon`	Устанавливает процессу `haproxy` режим работы «daemon»
	`user`	Пользователь, от имени которого работает процесс `haproxy`
	`group`	Группа, от имени которой работает процесс `haproxy`
	`chroot /var/lib/haproxy`	Устанавливает окружение процесса `haproxy`
`defaults`	`log global`	Включает в регистрацию событий информацию о трафике
	`mode http`	Режим работы HAProxy. Возможны два режима: - `http` — выполняется анализ Layer 7, подходит для распределения http-трафика; - `tcp` — распределение любого трафика
	`option dontlognull`	Отключает регистрацию пустых подключений
	`retries 3`	Количество попыток определить состояние обслуживающего сервера после сбоя подключения
	`option redispatch`	Распределяет запросы после сбоя подключения к одному из обслуживающих серверов
	`option httpclose`	Закрывает пассивные соединения
	`option forwardfor`	Включает X-Forwarded-For для передачи IP-адреса клиента обслуживающему серверу
`frontend`	`frontend http`	Задает имя `frontend`
	`bind *:80`	Задает IP-адрес и порт для прослушивания запросов
`backend`	`backend sitecluster`	Задает имя обслуживающего сервера

Продолжение таблицы 36

Раздел	Параметр	Описание
	`balance (roundrobin/leastconn/ static-rr/uri/source)`	Настройка алгоритма распределения. Поддерживаются следующие алгоритмы: - `Round Robin` — направляет новые подключения к следующему серверу в циклическом списке, который видоизменяется при помощи веса сервера, на основании которого идет распределение запросов. Вес сервера можно изменить «на лету». Параметр включается при помощи команды `balance roundrobin`; - `Least Connected` — направляет новые подключения к серверу с наименьшим числом соединений. Параметр включается при помощи команды `balance leastconn`; - `Static Round Robin` — направляет новые подключения к следующему серверу в циклическом списке, который видоизменяется при помощи веса сервера, на основании которого идет распределение запросов. В отличие от стандартной реализации `Round Robin`, в данном алгоритме нельзя изменить вес сервера «на лету». Изменение веса сервера требует перезагрузки HAProxy. Параметр включается при помощи команды `balance static-rr`; - `Source` — выбирает сервер исходя из хеша, построенного на основе IP-адреса пользователя. Таким образом, пользователь всегда обращается к одному и тому же серверу
	`server srv-1.3.my.com 21.86.21.20:80 cookie site113ha check inter 2000 fall 3 minconn 30 maxconn 70 weight 100`	Описание обслуживающего сервера, где: - `srv-1.3.my.com` — имя сервера; - `21.86.21.20:80` — IP-адрес: порт; - `cookie site113ha` — задание cookie, необходимого для правильного распределения сессий клиентов; - `check inter 2000 fall 3` — проверка доступности сервера каждые 2 с, при наличии трех ошибок считать сервер недоступным; - `minconn 30 maxconn 70` — организация очереди запросов, ограничение не более 70 одновременно обрабатывающихся запросов; - `weight 100` — вес сервера, возможные значения от 1 до 100
	`stats enable`	Включает статистику

Окончание таблицы 36

Раздел	Параметр	Описание
	`fullconn 200`	Задает максимальное значение одновременных подключений
`listen`	`listen stats-srv-3.my.com *:8180`	Описывает IP-адрес и порт доступа к статистике
	`stats uri /stats`	URL доступа к статистике
	`stats realm Haproxy Statistics`	Заголовок (title) страницы статистики
	`stats show-legends`	Отображает в статистике дополнительную информацию о параметрах
	`stats refresh 5s`	Указывает интервал автоматического обновления страницы статистики
	`stats auth test:test`	Устанавливает логин и пароль доступа к странице статистики

Пример

Конфигурационный файл для распределения нагрузки сервера Apache

```
global
log /dev/log local0
log /dev/log local1 notice
maxconn 40000
chroot /var/lib/haproxy
stats socket /run/haproxy/admin.sock mode 660 level admin
stats timeout 30s
user haproxy
group haproxy
daemon        # Размещение сертификатов SSL
ca-base /etc/ssl/certs
crt-base /etc/ssl/private    # Алгоритмы защитного преобразования,
# применяемые для SSL-подключений
# Подробнее см. по ссылке:
# https://hynek.me/articles/hardening-your-web-servers-ssl-ciphers/
ssl-default-bind-ciphers ECDH+AESGCM:DH+AESGCM:ECDH+AES256:DH+AES256:
ECDH+AES128:DH+AES:ECDH+3DES:DH+3DES:RSA+AESGCM:RSA+AES:RSA+
3DES:!aNULL:!MD5:!DSS
ssl-default-bind-options no-sslv3

defaults
log global
mode http
```

```
option httplog
option dontlognull
retries 3
option redispatch
maxconn 2000
timeout connect 5000
timeout client 50000
timeout server 50000
errorfile 400 /etc/haproxy/errors/400.http
errorfile 403 /etc/haproxy/errors/403.http
errorfile 408 /etc/haproxy/errors/408.http
errorfile 500 /etc/haproxy/errors/500.http
errorfile 502 /etc/haproxy/errors/502.http
errorfile 503 /etc/haproxy/errors/503.http
errorfile 504 /etc/haproxy/errors/504.http

frontend localnodes
bind *:80
mode http
default_backend nodes

backend nodes
mode http
balance roundrobin
server webserver1 192.168.13.150:80 cookie serv1 check
server webserver2 192.168.13.151:80 cookie serv2 check
```

8. СРЕДСТВА ОРГАНИЗАЦИИ ЕПП

8.1. Архитектура ЕПП

Единое пространство пользователей представляет собой средства организации работы пользователя в сети компьютеров, работающих под управлением ОС. В основу положен доменный принцип построения сети, подразумевающий объединение в одну сеть логически связанных компьютеров, например, принадлежащих одной организации. При этом пользователь получает возможность работы с сетевыми ресурсами сети и взаимодействия с другими пользователями.

Организация ЕПП обеспечивает:

- сквозную аутентификацию в сети;
- централизацию хранения информации об окружении пользователей;
- централизацию хранения настроек системы защиты информации на сервере.

Сетевая аутентификация и централизация хранения информации об окружении пользователя основана на использовании двух основных механизмов: NSS, описание которого приведено в 8.1.1, и PAM, описание которого приведено в 8.1.2.

В качестве источника данных для базовых системных служб на базе механизмов NSS и PAM используется служба каталогов LDAP в соответствии с 8.1.3.

Сквозная доверенная аутентификация реализуется технологией Kerberos в соответствии с 8.1.4.

Централизация хранения информации об окружении пользователей подразумевает и централизованное хранение домашних каталогов пользователей. Для этого используется СЗФС CIFS в соответствии с 6.9.

При создании ЕПП в качестве основной службы рекомендуется использовать службу FreeIPA, описанную в 8.2.

8.1.1. Механизм NSS

Механизм NSS предоставляет всем программам и службам, функционирующим на локальном компьютере, системную информацию через соответствующие программные вызовы. Он обращается к конфигурационному файлу `/etc/nsswitch.conf`, в котором указаны источники данных для каждой из системных служб. Краткое описание системных служб приведено в таблице 37.

Таблица 37

Служба	Источник данных по умолчанию	Описание
passwd	/etc/passwd	Окружение пользователя (домашний каталог, идентификатор пользователя и пр.)
shadow	/etc/shadow	Пароли пользователей
group	/etc/group	Принадлежность пользователей группам
hosts	/etc/hosts	Соответствие имен хостов адресам
services	/etc/services	Характеристики сетевых служб (порт, тип транспортного протокола)

Каждая из базовых системных служб поддерживает ряд библиотечных программных вызовов, таких как getpwent, getspent, getgrent, getservent. При выполнении данных программных вызовов производится поиск в конфигурационном файле /etc/nsswitch.conf источника данных соответствующей службы (например, passwd для получения домашнего каталога пользователя). По умолчанию в качестве источника данных системных служб используются соответствующие конфигурационные файлы в каталоге /etc (источник files). NSS при получении имени источника данных из конфигурационного файла /etc/nsswitch.conf осуществляет поиск программной разделяемой библиотеки в каталоге /lib с именем libnss_<имя_источника_данных>-<версия_библиотеки>.so, где в качестве имени источника данных выступает строка, полученная из /etc/nsswitch.conf. Например, при вызове getpwent, при условии, что в /etc/nsswitch.conf находится строка:

```
passwd : files
```

будет вызвана соответствующая функция из библиотеки /lib/libnss_files.so.

8.1.2. Механизм PAM

Механизм PAM (Pluggable Authentication Modules — подключаемые модули аутентификации) позволяет интегрировать различные низкоуровневые методы аутентификации и предоставить единые механизмы для использования прикладных программ в процессе аутентификации. Механизм состоит из набора разделяемых библиотек и конфигурационных файлов — сценариев процедур аутентификации.

В каталоге /etc/pam.d расположены конфигурационные файлы PAM для соответствующих служб, в т. ч. файл службы login в котором дана информация по проведению аутентификации.

Модули PAM вызываются при выполнении следующих функций:

1) auth — аутентификация;

2) account — получение привилегий доступа;

3) password — управление паролями;

4) session — сопровождение сессий.

Для выполнения каждой функции может быть перечислено несколько модулей PAM, которые будут вызываться последовательно, образуя стек PAM для данной задачи. Каждый вызываемый модуль возвращает в стек результат своей работы: успешный (PAM_SUCCESS), неуспешный (PAM_AUTH_ERR), игнорирующий (PAM_IGNORE) или иной. Для каждого вызова может быть указан набор управляющих флагов в виде соответствия кода возврата и того, как результат работы модуля скажется на обработке всей служебной задачи, например, ignore, ok, die. Для управления аутентификацией используются следующие флаги:

- requisite — немедленное прекращение дальнейшего выполнения служебной задачи с общим неуспешным результатом в случае неуспешного результата выполнения данного модуля;

- required — требование удачного выполнения этого модуля одновременно с выполнением всех остальных, перечисленных в данной служебной задаче;

- sufficient — в случае позитивных результатов выполнения данного модуля и всех предыдущих с флагом required в стеке задачи немедленно прекращается дальнейшее выполнение служебной задачи в целом с общим позитивным результатом. Если же модуль вернул негативный результат, то его значение игнорируется;

- optional — выполнение данного модуля никак не сказывается на результате всей задачи, но играет дополнительную информационную роль.

8.1.3. Служба каталогов LDAP

Служба каталогов LDAP — общее название клиент-серверной технологии доступа к службе каталогов X.500 с помощью протокола LDAP. Служба каталогов X.500 является средством иерархического представления информационных ресурсов, принадлежащих организации, и информации об этих ресурсах. При этом служба каталогов обеспечивает централизованное управление ресурсами и информацией о них, а также позволяет контролировать их использование третьими лицами. Каждый ресурс может принадлежать одному или более классам. Каждый класс показывает, что ресурс является определенным типом сущности и имеет определенный набор свойств. Совокупности классов могут объединяться в схемы, которые описывают типы ресурсов, применяемые в отдельно взятой предметной области.

Информация, хранящаяся в каталоге, называется «информационной базой каталога» (DIB). Пользователь каталога, который может быть как человеком, так и компьютером, получает доступ к каталогу посредством клиента. Клиент от имени пользователя каталога взаимодействует с одним или более серверами. Сервер хранит фрагмент DIB.

DIB содержит два типа информации:

- пользовательская — информация, предоставляемая пользователям и, возможно, изменяемая ими;
- административная и функциональная — информация, используемая для администрирования и/или функционирования каталога.

Множество записей, представленных в DIB, организовано иерархически в структуру дерева, известную как «информационное дерево каталога» (DIT). При этом запись в каталоге LDAP состоит из одного или нескольких атрибутов, обладает уникальным именем (DN — Distinguished Name) и может состоять только из тех атрибутов, которые определены в описании класса записи. В схеме определено, какие атрибуты являются для данного класса обязательными, а какие — необязательными. Каждый атрибут, хранящийся в каталоге LDAP (например, тип данных), имеет определенный синтаксис, который накладывает ограничения на структуру и формат его значений. Сравнение значений не является частью определения синтаксиса, а задается отдельно определяемыми правилами соответствия. Правила соответствия специфицируют аргумент, значение утверждения, которое также имеет определенный синтаксис.

Предполагается, что информация каталога достаточно статична, т.е. чаще читается, чем модифицируется. Примером подобного каталога является специализированная БД, например, телефонная книга, база данных службы DNS.

Службы каталогов LDAP могут быть использованы в качестве источника данных для базовых системных служб на базе механизмов NSS и PAM.

В результате вся служебная информация пользователей сети может располагаться на выделенном сервере в распределенной гетерогенной сетевой среде. Добавление новых сетевых пользователей в этом случае производится централизованно на сервере службы каталогов.

Благодаря предоставлению информации LDAP в иерархической древовидной форме разграничение доступа в рамках службы каталогов LDAP может быть основано на введении доменов. В качестве домена в данном случае будет выступать поддерево службы каталогов LDAP.

8.1.4. Доверенная аутентификация Kerberos

Kerberos является протоколом, обеспечивающим централизованную аутентификацию пользователей и применяющим техническое маскирование данных для противодействия различным видам атак.

Основным компонентом системы Kerberos является центр распределения ключей (KDC). Программы, настроенные на взаимодействие с Kerberos, называются «керберизованны-

ми приложениями». KDC отвечает за аутентификацию в некоторой области Kerberos. В процессе работы система Kerberos выдает билеты (tickets) на использование различных служб.

Сервером Kerberos называется компьютер, на котором выполняется серверная программа Kerberos, или сама программа KDC. Клиент Kerberos — это компьютер или программа, которые получают билет от сервера Kerberos. Обычно действия системы Kerberos инициирует пользователь, отправляющий запрос на получение услуг от некоторого сервера приложения (например, сервера почты). Kerberos предоставляет билеты принципалам, в роли которых выступают пользователи или серверные программы. Для описания принципала применяется идентификатор, состоящий из трех компонентов: основы (`primary`), экземпляра (`instance`) и области (`realm`). Данный идентификатор имеет вид:

```
основа/экземпляр@область
```

Система Kerberos выполняет следующие задачи:

1) обеспечение аутентификации в сети. Для предотвращения НСД к службам сервер должен иметь возможность идентифицировать пользователей. Кроме того, в некоторых средах важно, чтобы клиент мог идентифицировать серверы. Это исключит работу пользователей с фальшивыми серверами, созданными для незаконного сбора конфиденциальной информации;

2) защиту паролей. Открытость паролей, используемых в ряде сетевых служб, создает угрозу безопасности системы, т. к. они могут быть перехвачены и использованы для незаконного доступа к системе. Для решения данной проблемы используется техническое маскирование билетов Kerberos.
Технология Kerberos представляет собой механизм аутентификации пользователей и служб, основным достоинством которой является повышенная защищенность при использовании в сети, которая достигается механизмом защищенного обмена билетами между пользователями, службами и сервером учетных записей Kerberos. При данном механизме пароли пользователей по сети не передаются, что обеспечивает повышенную защищенность от сетевых атак. С помощью механизма открытых и закрытых ключей, а также синхронизации часов клиентских компьютеров с сервером Kerberos обеспечивается уникальность билетов и их защищенность от подделки.
В ОС используется реализация MIT Kerberos;

3) обеспечение однократной регистрации в сети. Система Kerberos дает возможность пользователю работать с сетевыми службами, пройдя лишь единожды аутентификацию на своем компьютере. При этом для обмена с приложениями дополнительно вводить пароль не требуется.
Локальные системы учетных записей пользователей и система ЕПП существуют в ОС параллельно. Различие между ними проводится с помощью разграничения

диапазонов UID (значения UID меньшие, чем 2500, относятся к локальным пользователям, а большие или равные 2500 — к пользователям ЕПП).

ВНИМАНИЕ! Обязательным требованием для функционирования аутентификации по Kerberos является синхронизация времени на клиенте и сервере. Синхронизация может быть обеспечена использованием сервера NTP (см. 6.7).

8.1.5. Централизация хранения атрибутов СЗИ в распределенной сетевой среде

В среде ОС работа пользователя осуществляется с учетом назначенных ему атрибутов, связанных с механизмами СЗИ ОС, например:

- привилегии администрирования, вхождение в группы;
- разрешенные параметры входа (список разрешенных компьютеров домена);
- политики паролей и учетных записей;
- мандатные атрибуты (диапазон доступных уровней и категорий конфиденциальности, разрешенные метки целостности, привилегии);
- параметры регистрации событий (маски регистрируемых успешных и неуспешных событий).

Одни атрибуты предназначены только для использовании в ЕПП, другие являются общими атрибутами СЗИ ОС. Доступ к мандатным атрибутам пользователей осуществляется с использованием программной библиотеки `parsec`. Данная библиотека получает из соответствующего конфигурационного файла информацию об источнике данных для СЗИ, функционирующих в условиях применения мандатного управления доступом и мандатного контроля целостности. По умолчанию используются локальные текстовые файлы.

Концепция ЕПП подразумевает централизованное хранение системной информации о пользователе (в т. ч. и его мандатные атрибуты). В этом случае вся информация хранится в службе каталогов LDAP.

8.2. Служба FreeIPA

Служба FreeIPA предназначена для реализации централизованного управления сетевыми службами, идентификацией и аутентификацией, а также для установки доверительных отношений и обеспечения взаимодействия Linux-систем с доменом Active Directory (AD).

В FreeIPA используется системный демон SSSD (System Security Services Daemon), управляющий доступом к удаленным каталогам и механизмам аутентификации, входящим в состав FreeIPA.

FreeIPA основывается на технологиях LDAP и Kerberos и поддерживает миграцию учетных записей из LDAP и NIS. FreeIPA предоставляет следующий функционал:

- DNS-сервер;
- сервер времени;
- управление доступом на основе политик.

FreeIPA позволяет создавать централизованные системы по управлению идентификацией пользователей, заданию политик доступа и аудита для сетей на основе ОС. В состав FreeIPA входят следующие компоненты:

- сервер 389 Directory Server — используется в качестве сервера LDAP;
- MIT Kerberos 5 — используется для аутентификации и единой точки входа;
- Apache и Python — используются для управления ПО, входящим в состав FreeIPA;
- BIND и DHCP — используются для управления службой DNS в сети.

В соответствии с моделью мандатного доступа служба FreeIPA реализует для зарегистрированных с помощью службы пользователей:

- задание уровней конфиденциальности;
- задание метки целостности;
- задание PARSEC-привилегий.

Управление FreeIPA доступно как через терминал, так и через веб-интерфейс.

8.2.1. Структура

Основу доменной структуры FreeIPA составляет домен IPA, в который может входить множество доменов DNS. Домен IPA воспринимается внешним доменом AD как отдельный лес доменов AD, при этом домен Primary DNS домена IPA выступает в роли корневого домена леса доменов FreeIPA.

Интеграция домена IPA с доменом AD возможна двумя способами:

- синхронизация учетных записей пользователей и их паролей (не рекомендуется);
- создание доверительных отношений между лесами доменов (рекомендуется).

В документе приводится описание только рекомендованного способа интеграции на основе доверительных отношений между доменом AD и доменом IPA.

Для обеспечения отказоустойчивости FreeIPA применяется репликация — создание реплики FreeIPA, при этом рекомендуется использовать две или три (но не более четырех) реплики. Реплики поддерживают работу в режиме «ведущий–ведомый».

8.2.2. Состав

Все необходимые компоненты службы FreeIPA входят в состав пакетов, приведенных в таблице 38.

Таблица 38

Наименование	Описание
`freeipa-admintools`	Пакет администрирования FreeIPA, содержит набор утилит по управлению сервером FreeIPA
`freeipa-client`	Клиентская часть FreeIPA. Пакет должен устанавливаться на все клиентские компьютеры, входящие в домен
`freeipa-server`	Серверная часть FreeIPA. Пакет должен устанавливаться на контроллере домена. При установке данного пакета также устанавливается средство администрирования `ipa` и клиентская часть
`freeipa-server-dns`	Пакет, предназначенный для установки или интеграции с DNS сервером
`freeipa-server-trust-ad`	Пакет для интеграции с Active Directory от Microsoft путем установки доверительных отношений
`astra-freeipa-server`	Инструмент командной строки управления FreeIPA
`astra-freeipa-client`	Инструмент командной строки управления клиентом FreeIPA
`fly-admin-freeipa-server`	Графическая утилита управления FreeIPA
`fly-admin-freeipa-client`	Графическая утилита управления клиентом FreeIPA

Служба FreeIPA состоит из ядра, отвечающего за основной функционал системы, ряда интерфейсов (LDAP, Kerberos, Config, RPC) и модулей расширения, предназначенных для расширения командного интерфейса утилит и настройки необходимых служб и подсистем, что позволяет повышать функциональность FreeIPA.

В FreeIPA возможно использование следующих группы модулей расширения:

- `freeipa-client-*` — расширение, необходимое клиентской части FreeIPA;
- `freeipa-admintools-*` — расширение утилиты администрирования FreeIPA;
- `freeipa-server-*` — расширение, необходимое для организации хранения атрибутов на сервере FreeIPA.

Описание пакетов приведено на справочных страницах `man`, список которых приведен в таблице 39.

Таблица 39

Наименование	Описание
`ipa`	Администрирование домена IPA

Продолжение таблицы 39

Наименование	Описание
default.conf	Образец конфигурационного файла default.conf
ipa-client-install	Настройка клиентской части FreeIPA
ipa-server-install	Настройка серверной части FreeIPA
ipa-server-upgrade	Обновление сервера FreeIPA
ipa-dns-install	Утилита добавления DNS как службы на серверной части FreeIPA
ipa-backup	Резервное копирования мастер-сервера FreeIPA
ipactl	Интерфейс управления серверной частью FreeIPA
ipa-advise	Предоставляет рекомендации по конфигурациям для различных вариантов использования
ipa-cacert-manage	Управление сертификатами CA на FreeIPA
ipa-certupdate	Обновление локальных БД сертификатов FreeIPA вместе с сертификатами от сервера
ipa-client-automount	Настройка автомонтирования и ФС NFS для FreeIPA
ipa-compat-manage	Включение и выключение модуля совместимости схемы
ipa-csreplica-manage	Управление репликой FreeIPA CS
ipa-getcert	Инструмент ipa-getcert выдает запросы службе certmonger от имени вызывающего пользователя
ipa-getkeytab	Получение keytab-файла. Keytab — это файл с одним или несколькими закрытыми ключами для принципала Kerberos. Keytab-файлы используются службами, например, sshd, при аутентификации Kerberos
ipa-join	Подключение хоста к области FreeIPA и получение keytab-файла для размещения службы хоста принципала Kerberos
ipa-kra-install	Установка KRA на серверной части FreeIPA
ipa-ldap-updater	Обновление настроек FreeIPA LDAP
ipa-managed-entries	Включения и выключение модулей схемы управляемых модулей ввода
ipa-nis-manage	Включение и выключение модуля прослушивателя NIS
ipa-otptoken-import	Импорт OTP-токенов из RFC 6030 XML файлов
ipa-replica-conncheck	Проверка сетевого подключения реплики и мастер-сервера перед установкой
ipa-replica-install	Создание реплики FreeIPA
ipa-replica-manage	Управление репликой FreeIPA
ipa-replica-prepare	Создание файла реплики FreeIPA
ipa-restore	Восстановление мастер-сервера FreeIPA
ipa-rmkeytab	Удаление принципала Kerberos из keytab-файла
ipa-server-certinstall	Установка новых SSL-сертификатов сервера

Окончание таблицы 39

Наименование	Описание
`ipa-winsync-migrate`	Полный переход от пользователей AD, созданных `winsync`, к обычным пользователям AD
`ipa-upgradeconfig`	Обновление конфигурации Apache FreeIPA

8.2.3. Предварительная настройка контроллера домена

При развертывании FreeIPA в качестве контроллера домена следует использовать отдельный компьютер с фиксированным IP-адресом, который в дальнейшем не должен изменяться.

ВНИМАНИЕ! При развертывании домена FreeIPA на контроллере домена создается веб-сервер Apache2 для размещения веб-интерфейса FreeIPA. Работа домена FreeIPA осуществляется только при отключенном режиме `AstraMode` данного веб-сервера (описание режима приведено в 11.2). Данный режим автоматически отключается инструментом установки сервера FreeIPA `astra-freeipa-server` и графической утилитой `fly-admin-freeipa-server`. Описание настройки веб-сервера Apache2 в разделе 11 не относится к веб-серверу на контроллере домена.

Для штатного функционирования FreeIPA необходимо выполнение следующих условий:

1) в настройках сетевого интерфейса в качестве первичного DNS должен быть указан IP-адрес компьютера;

2) компьютеру должно быть присвоено полное имя, при этом использовать доменное имя второго уровня или ниже (например, `domain.net`, `domain.test.net`). Имя компьютера можно задать с помощью команды:

```
hostnamectl set-hostname <полное_имя_сервера>
```

Пример

```
hostnamectl set-hostname server.domain.net
```

Инструмент `hostname` должен возвращать полное имя компьютера (например, `server.domain.net`);

3) разрешение имен должно быть настроено таким образом, чтобы имя компьютера разрешалось, в первую очередь, как полное имя (разрешение имен для сервера FreeIPA добавляется автоматически при установке, см. 8.2.4).

Пример

Записи в файле `/etc/hosts` для сервера FreeIPA:

```
127.0.0.1       localhost
192.168.1.1     server.domain.net server
```

4) должна быть выполнена синхронизация времени в ОС для аутентификации по Kerberos. Синхронизация может быть настроена с помощью протокола синхронизации времени (см. 8.2.10).

Настройка всех компонентов сервера FreeIPA осуществляется автоматически при установке сервера с помощью `fly-admin-freeipa-server` или `astra-freeipa-server`.

8.2.4. Установка компонентов FreeIPA

Программные компоненты FreeIPA входят в состав ОС и могут быть установлены с помощью графической утилиты для работы с пакетами Synaptic либо из терминала.

ВНИМАНИЕ! Без установки пакетов расширения совместно с соответствующими основными пакетами невозможно централизованное хранение атрибутов СЗИ в распределенной сетевой среде, что может привести к невозможности входа пользователей в систему.

Для развертывания FreeIPA необходимо:

1) на компьютере, предназначенном на роль контроллера домена, установить следующие программные компоненты:
   а) серверную часть FreeIPA `astra-freeipa-server`, для установки из терминала ввести команду:

   ```
   apt install astra-freeipa-server
   ```

   б) графическую утилиту управления серверной частью FreeIPA `fly-admin-freeipa-server`, для установки из терминала ввести команду:

   ```
   apt install fly-admin-freeipa-server
   ```

   При установке графической утилиты `fly-admin-freeipa-server` автоматически будет установлен инструмент командной строки `astra-freeipa-server`;
2) на клиентских компьютерах установить следующие программные компоненты:
   а) `astra-freeipa-client`, для установки из терминала ввести команду:

   ```
   apt install astra-freeipa-client
   ```

   б) `fly-admin-freeipa-client`, для установки из терминала ввести команду:

   ```
   apt install fly-admin-freeipa-client
   ```

   При установке графической утилиты `fly-admin-freeipa-client` автоматически будет установлен инструмент командной строки `astra-freeipa-client`.

При установке данных компонентов FreeIPA автоматически устанавливается служба синхронизации времени `chrony` (при этом удаляется служба `systemd-timesyncd`), а также все необходимые пакеты в зависимости от назначения компьютера.

ВНИМАНИЕ! Для создания ЕПП FreeIPA, в которое должны быть введены клиенты, поддерживающие МКЦ и мандатное управление доступом, в роли сервера FreeIPA необходимо использовать компьютер с включенным МКЦ и мандатным управлением доступом. После установки сервера FreeIPA изменение работы МКЦ и мандатного управления доступом не поддерживается.

8.2.5. Создание контроллера домена и запуск служб FreeIPA

Создание контроллера домена и запуск служб сервера FreeIPA может быть выполнено с помощью графической утилиты или из командной строки.

8.2.5.1. С использованием графической утилиты

Для создания контроллера домена и запуска служб FreeIPA с помощью графической утилиты `fly-admin-freeipa-server` (описание утилиты см. в электронной справке) необходимо запустить графическую утилиту командой:

```
fly-admin-freeipa-server
```

В окне программы, при необходимости, указать следующие данные:

- в поле «Домен» — имя домена, определяется автоматически на основе полного имени компьютера;
- в поле «Имя компьютера» — имя компьютера, определяется автоматически;
- в поле «Пароль» — задать пароль администратора домена. Указанный пароль будет использоваться для входа в веб-интерфейс FreeIPA и при работе с инструментом командной строки.

Далее нажать кнопку **[Создать]**.

После успешного конфигурирования необходимых служб и инициализации домена появится ссылка для перехода в веб-интерфейс FreeIPA, в котором можно продолжить настройку. Порядок работы с FreeIPA используя веб-интерфейс приведен в 8.2.15.

8.2.5.2. С использованием инструмента командной строки

Для создания контроллера домена и запуска служб FreeIPA с помощью инструмента командной строки `astra-freeipa-server` выполнить команду:

```
astra-freeipa-server -d <имя_домена> -n <имя_компьютера> -o
```

После выполнения команды будет определен адрес компьютера и будут выведены на экран все исходные данные.

Пример

```
compname= server
domain= domain.net
будет использован ip address = 192.168.32.97 или укажите ip адрес ключем
     -ip
продолжать ? (y\n)
```

Для подтверждения данных ввести y и нажать **<Enter>**. После подтверждения появится запрос на установку пароля администратора домена. Указанный пароль будет использоваться для входа в веб-интерфейс FreeIPA и при работе с инструментом командной строки.

После ввода пароля будет выполнено конфигурирование необходимых служб и инициализации домена, ход выполнения будет отображаться на экране. После успешного завершения инициализации на экран будут выведены сообщения о перезапуске системных служб, а также данные контроллера домена и ссылка для веб-интерфейса FreeIPA, в котором можно продолжить настройку. Порядок работы с FreeIPA используя веб-интерфейс приведен в 8.2.15.

Пример

```
Restarting Directory Service
Restarting krb5kdc Service
Restarting kadmin Service
Restarting named Service
Restarting ipa_memcached Service
Restarting httpd Service
Restarting ipa-custodia Service
Restarting ipa-otpd Service
Restarting ipa-dnskeysyncd Service
Starting chronyd Service
ipa: INFO: The ipactl command was successful
Существует настроенный домен
host = server.domain.net
basedn = dc=domain,dc=net
domain = domain.net
xmlrpc_uri = https://server.domain.net/ipa/xml
WEB: https://server.domain.net
```

После завершения работы мастера требуется убедиться в наличии открытых портов на сервере:

1) TCP Ports:
   - 80, 443: HTTP/HTTPS;

- 389, 636: LDAP/LDAPS;
- 88, 464: kerberos;
- 53: bind;

2) UDP Ports:
   - 88, 464: kerberos;
   - 53: bind;
   - 123: ntp.

Параметры инструмента командной строки `astra-freeipa-server` приведены в таблице 40.

Таблица 40

Параметр	Описание
`-h, --help`	Вывести справку по командам
`-d`	Задать имя домена
`-n`	Задать имя компьютера
`-ip`	Задать IP-адрес веб-интерфейса. Если адрес не задан, то инструмент пытается определить его автоматически
`-y`	Отключить запрос подтверждения после вывода заданных параметров запуска
`-i`	Вывести информацию о существующем домене
`-px`	Получить пароль администратора домена из `stdin`
`-p`	Получить пароль администратора домена из командной строки (небезопасно)
`-s`	Включить установку и запуск поддержки AD SMB
`-c`	Запретить изменять файл `/etc/hosts`
`-o`	Запретить проверку регистрации домена. Применяется при установке в изолированной сети
`-e`	Отключить установку и запуск собственной службы DNS
`-U`	Удалить все настройки
`-l`	Указать сертификат (имя компьютера и домена должны совпадать)
`-lp`	Указать пароль сертификата

8.2.6. Конфигурационный файл сервера FreeIPA

Настройки сервера FreeIPA содержатся в конфигурационном файле `/etc/ipa/default.conf`. Формат файла:

```
имя_параметра=значение # Комментарий
```

Описание параметров конфигурационного файла приведено в таблице 41.

Таблица 41

Параметр	Описание
basedn <запись_DN>	Задает базовую запись DN, используемую при выполнении операций LDAP. Запись должна быть в формате DN (например, dc=example,dc=com)
context <контекст>	Задает контекст, в котором выполняется IPA. Работа IPA определяется в зависимости от контекста. Текущие определенные контексты — cli и server (клиент и сервер). Кроме того, значение используется для загрузки файла /etc/ipa/<контекст>.conf для применения контекстной конфигурации. Например, если необходимо всегда выполнять клиентские запросы в подробном режиме, но при этом не использовать подробный режим на сервере, то следует добавить параметр verbose в /etc/ipa/cli.conf
debug <boolean>	При значении True предоставляет подробную информацию. В частности, значение debug устанавливается для глобального уровня log-журнала. Значение по умолчанию False
domain <имя_домена>	Домен сервера FreeIPA, например, example.com
enable_ra <boolean>	Значение True определяет, что будет использоваться удаленная служба центра аутентификации, например, когда служба Dogtag используется в качестве центра аутентификации. Эта настройка применяется исключительно в конфигурации сервера IPA
fallback <boolean>	Значение True определяет, что клиент IPA должен выполнять возврат и обращаться к другим службам в случае сбоя первого подключения
host <имя_хоста>	Задает имя хоста локальной системы
in_server <boolean>	Определяет, будут ли запросы направляться на сервер IPA (True) или обрабатываться локально (False). Внутри IPA они используются подобно контексту. Та же самая IPA-конструкция используется IPA-инструментами командной строки и сервера. Этот параметр указывает конструкции, выполнить ли команду так, как если бы она была на сервере или переслать ее через XML-RPC на удаленный сервер
in_tree <boolean>	Используется при разработке. Параметр указывается при необходимости выполнить код в исходном дереве
interactive <boolean>	Определяет, следует ли запрашивать значения. Значение по умолчанию True
ldap_uri <URI>	Указывает URI сервера IPA LDAP для подключения. Схема URI может быть ldap или ldapi. По умолчанию используется ldapi, например, ldapi://%2fvar%2frun%2fslapd-EXAMPLE-COM.socket

Продолжение таблицы 41

Параметр	Описание

`log_logger_<уровень> <регулярное_выражение, ...>`	Перечень регулярных выражений `regexp`, разделенных запятыми. Логированиям (loggers), соответствующим регулярным выражениям, будет присвоен уровень `<уровень>`.
	Уровни логирования (logger levels) могут быть явно заданы для конкретных логирований в отличие от глобального уровня журналирования (global logging level). Если имя логирования соответствует регулярному выражению, то ему присваивается соответствующий уровень. Этот элемент конфигурации должен начинаться с `log_logger_level_`, а затем должен следовать символический или числовой уровень журнала (log level). Этот элемент конфигурации полезен, если требуется просмотреть вывод журнала только для одного или нескольких выбранных логирований. Обычно логирования привязаны к классам и модулям.
	Пример
	Настроить логирование модуля `ipalib.dn` на уровень для отладки:
	`log_logger_level_debug = ipalib\.dn\..*`
	Настроить логирование `ipa.plugins.dogtag` на уровень 35:
	`log_logger_level_35 = ipalib\.plugins\.dogtag`
	Примечание. Имена логирований (logger names) — список с разделяющей точкой, образующий путь в данном дереве логирования (logger tree). Символ точки также является метасимволом регулярного выражения (соответствует любому символу), поэтому, чтобы избежать точек в именах логирования, обычно требуется перед ними ставить обратную косую черту «\.».

`mode <режим_работы>`	Определяет режим работы сервера. В настоящее время поддерживаемыми значениями являются эксплуатация (`production`) и разработка (`development`). При работе в режиме `production` некоторые самопроверки пропускаются для повышения производительности
`mount_ipa <URI>`	Задает точку монтирования для регистрации сервера разработки. По умолчанию `/ipa/`
`prompt_all <boolean>`	Определяет, должны ли для клиента IPA запрашиваться все параметры, в т. ч. необязательные значения. По умолчанию устанавливается `False`
`ra_plugin <имя>`	Задает имя назначенного для использования CA. Текущими параметрами являются `dogtag` и `selfsign`. Настройка на стороне сервера. Изменять значение не рекомендуется, т.к. назначенный CA настраивается только во время первоначальной установки
`realm <realm>`	Указывает область Kerberos

Продолжение таблицы 41

Параметр	Описание
session_auth_duration <интервал_времени>	Задает допустимый интервал для времени кэширования учетных данных проверки подлинности в сеансе. По истечении срока действия учетные данные будут автоматически переопределены. Например, 2 hours, 1h:30m, 10 minutes, 5min, 30sec
session_duration_type <тип_вычисления>	Определяет способ вычисления срока действия сеанса. Возможные значения: - inactivity_timeout — срок действия увеличивается на значение session_auth_duration каждый раз, когда пользователь обращается к службе; - from_start сроком действия сеанса является начало сеанса пользователя плюс значение session_auth_duration
server <имя_сервера>	Задает имя сервера IPA
skip_version_check <boolean>	Пропустить проверки версии API клиента и сервера. Может привести к ошибкам/сбоям, когда новые клиенты обращаются к прежним серверам. Использовать с осторожностью
startup_timeout <время_ожидания>	Определяет время ожидания в секундах до начала запуска сервера. Значение по умолчанию 120 секунд
startup_traceback <boolean>	Если сервер IPA не запускается при заданном значении True, то сервер будет пытаться сгенерировать обратное python-отслеживание, чтобы облегчить определение причины сбоя
validate_api <boolean>	Используется внутри исходного пакета IPA для проверки неизменности API. Применяется для предотвращения регрессии. Если установлено значение True, то некоторые ошибки игнорируются, чтобы обеспечить загрузку инфраструктуры IPA, достаточной для проверки API, даже если дополнительные компоненты не установлены. Значение по умолчанию False
verbose <boolean>	При установке значения True предоставляет дополнительные сведения — устанавливает глобальный уровень журнала (global log level) на событие info

Окончание таблицы 41

Параметр	Описание
wait_for_dns <boolean>	Контролирует синхронность работы IPA команд dnsrecord-{add,mod,del}. Команды DNS будут повторять DNS-запросы указанное количество попыток до тех пор, пока DNS-сервер возвращает ответ up-to-date на запрос об измененных записях. Задержка между повторными попытками одна секунда. Команды DNS будут порождать исключение DNSDataMismatch, если ответ не совпадает с ожидаемым значением, даже после указанного числа попыток. DNS-запросы будут отправлены в очередь для разрешения решателем, который сконфигурирован в файле /etc/resolv.conf на сервере IPA. **ВНИМАНИЕ!** Не включать параметр в режиме production! Это может вызвать проблемы, если решатель (resolver) на сервере IPA использует кэширование сервера, а не локального сервера авторизации или, например, если DNS-ответы будут изменены шлюзом DNS64. Значение по умолчанию disable (выключено), параметр отсутствует
xmlrpc_uri <URI>	Задает URI сервера XML-RPC для клиента. Может использоваться IPA и используется некоторыми внешними средствами, такими как ipa-getcert. Например, https://ipa.example.com/ipa/xml
jsonrpc_uri <URI>	Задает URI сервера JSON для клиента. Используется IPA. Если параметр не задан, он наследуется от xmlrpc_uri. Например, https://ipa.example.com/ipa/json
rpc_protocol <URI>	Задает тип RPC-вызовов IPA makes: jsonrpc или xmlrpc. По умолчанию используется jsonrpc

Более подробное описание конфигурационного файла приведено в руководстве man.

Пример

Конфигурационный файл /etc/ipa/default.conf

```
[global]
host = server.domain.net
basedn = dc=domain,dc=net
realm = DOMAIN.NET
domain = domain.net
xmlrpc_uri = https://server.domain.net/ipa/xml
ldap_uri = ldapi://%2fvar%2frun%2fslapd-DOMAIN-NET.socket
enable_ra = False
ra_plugin = none
mode = production
```

8.2.7. Управление службами FreeIPA

Для проверки работы и управления службами FreeIPA используется команда `ipactl`:

1) запуск служб FreeIPA:

```
ipactl start
```

2) отображение текущего состояния всех служб FreeIPA:

```
ipactl status
```

3) перезапуск служб FreeIPA:

```
ipactl restart
```

4) остановка служб FreeIPA:

```
ipactl stop
```

Дополнительно с командой `ipactl` можно использовать параметр `-d` для выполнения команды в режиме отладки:

```
ipactl start -d
```

8.2.8. Ввод компьютера в домен

8.2.8.1. Настройка клиентского компьютера

Для ввода нового компьютера в домен необходимо выполнение условий:

1) клиентский компьютер не должен входить в другой домен;

2) разрешение имен должно быть настроено таким образом, чтобы имя системы разрешалось, в первую очередь, как полное имя.

Пример

Файл `/etc/hosts`:

```
127.0.0.1 localhost
192.168.1.2 client.domain.net client
192.168.1.1 server.domain.net server
```

Инструмент `hostname` должен возвращать полное имя компьютера, например `client.domain.net`.

Разрешение имен также может быть настроено с помощью сервера DNS в соответствии с 6.5;

3) клиентский компьютер и сервер FreeIPA должны видеть друг друга в сети. Для проверки можно использовать команду:

```
ping <ip-адрес>
```

4) должна быть выполнена синхронизация времени в ОС для аутентификации по Kerberos. Синхронизация может быть настроена с помощью протокола синхронизации времени (см. 8.2.10);

5) наличие установленного пакета `astra-freeipa-client`.

Далее необходимо настроить DNS-адрес сервера FreeIPA на клиентском компьютере одним из способов:

1) отредактировав конфигурационный файл `resolv.conf`;

2) отредактировав файл `interfaces`;

3) с помощью утилиты NetworkManager.

ВНИМАНИЕ! В некоторых случаях, если адрес сервера FreeIPA стоит в DNS не первым, клиентский компьютер может не находить домен.

Ввод компьютера в домен можно выполнить с помощью инструмента командной строки или графической утилиты.

8.2.8.2. Ввод компьютера в домен с использованием инструмента командной строки

Для ввода компьютера в домен с использованием инструмента командной строки `astra-freeipa-client` необходимо выполнить команду:

```
sudo astra-freeipa-client -d <контроллер_домена> -u admin -px
```

Для просмотра перечня дополнительных параметров для запуска с командой `astra-freeipa-client` выполнить:

```
astra-freeipa-client --help
```

После ввода компьютера в домен необходимо выполнить перезагрузку.

8.2.8.3. Ввод компьютера в домен с использованием графической утилиты

Для ввода компьютера в домен с использованием графической утилиты `fly-admin-freeipa-client` («Настройка FreeIPA клиент Fly», описание утилиты см. в электронной справке) необходимо запустить графическую утилиту командой:

```
fly-admin-freeipa-client
```

В открывшемся окне, приведенном на рис. 2, следует ввести:

1) в поле «Домен» — имя домена;
2) в поле «Логин» — имя администратора домена;
3) в поле «Пароль» — пароль администратора домена.

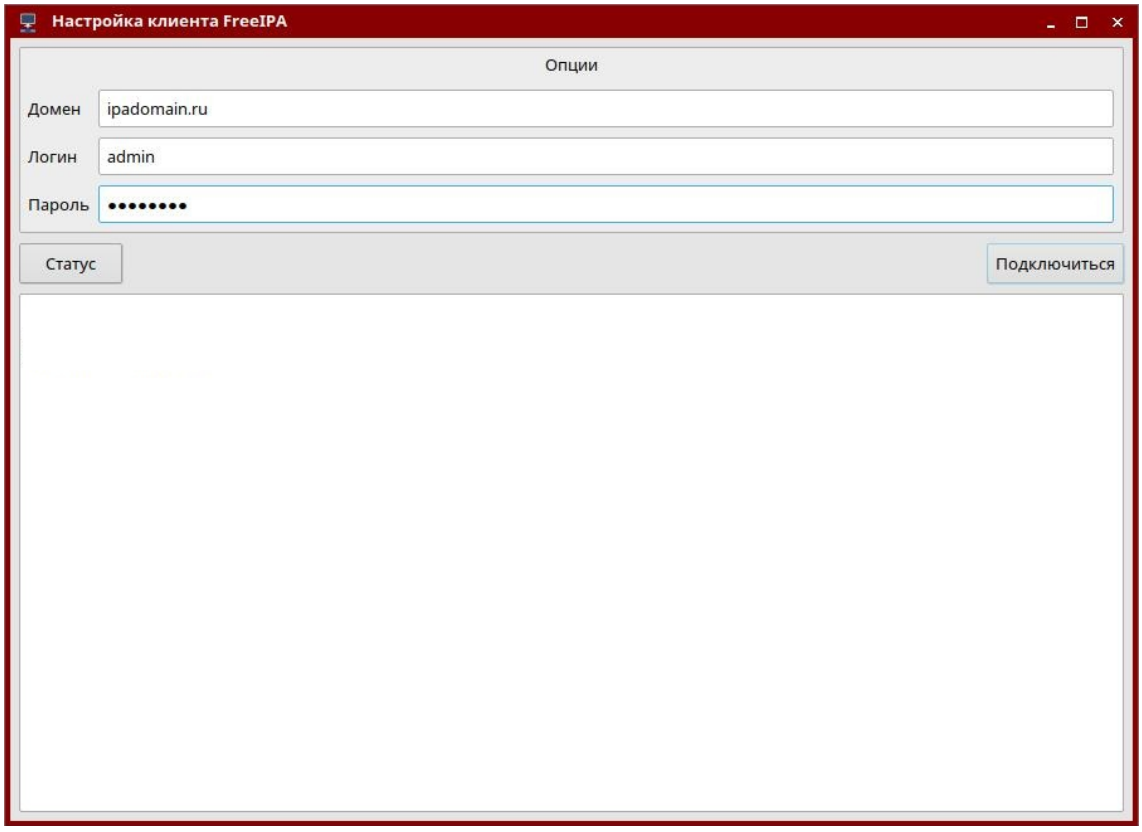

Рис. 2

После ввода данных следует нажать кнопку **[Подключиться]**.

8.2.8.4. Отображение списка доменных учетных записей в окне входа в ОС

По умолчанию список доменных учетных записей не отображается в окне входа в ОС, в том числе если в графической утилите `fly-admin-dm` включено отображение списка пользователей и настроен диапазон отображения, содержащий системные идентификаторы пользователей (`uid`) домена FreeIPA. Описание графической утилиты `fly-admin-dm` см. в электронной справке.

Для включения отображения списка доменных пользователей, дополнительно к настройкам с помощью графической утилиты `fly-admin-dm`, необходимо откорректировать конфигурационный файл `/etc/sssd/sssd.conf`, изменив в секции `[domain]` значение параметра `enumerate` на `TRUE` или добавив параметр, если он отсутствует:

```
[domain]
enumerate = True
```

При включении отображения списка доменных пользователей в окне входа в ОС рекомендуется ограничивать выводимый список путем задания соответствующего диапазона в графической утилите `fly-admin-dm`, т. к. вывод большого списка пользователей может снизить производительность.

8.2.9. Шаблоны конфигурационных файлов

Служба FreeIPA в процессе работы осуществляет конфигурирование сетевых служб (Samba, Kerberos, LDAP и т. п.) с помощью их конфигурационных файлов. Для удобства существуют шаблоны конфигурационных файлов, модифицируемых службой FreeIPA. Шаблоны расположены в каталогах `/usr/share/ipa` и `/usr/share/ipa/advise/legacy/`.

Перечень шаблонов конфигурационных файлов приведен в таблице 42.

Таблица 42

Имя шаблона	Служба	Описание, размещение конфигурационного файла
`*.ldif`	389-BASE	LDAP схемы
`default.conf`	IPA	`/etc/ipa/default.conf`
`ipa-httpd.conf.template`	IPA	`/etc/systemd/system/apache2.service.d/ipa.conf`
`ipa-kdc-proxy.conf.template`	IPA	`/etc/ipa/kdcproxy/ipa-kdc-proxy.conf`
`sssd.conf.template`	SSSD	`/etc/sssd/sssd.conf`
`ldap.conf`	LDAP клиенты	`/etc/ldap/ldap.conf`
`krb5.conf.template`	Kerberos клиенты	`/etc/krb5.conf`
`kdc.conf.template`	Kerberos KDC	`/etc/krb5kdc/kdc.conf`
`certmap.conf.template`	389-BASE	`/etc/dirsrv/config/certmap.conf`
`bind.named.conf.template`	BIND9	`/etc/bind/named.conf`
`custodia.conf.template`	IPA	`/etc/ipa/custodia/custodia.conf`
`smb.conf.template`	Samba	`/etc/samba/smb.conf`
`opendnssec_conf.template`	Opendnssec	`/etc/opendnssec/conf.xml`
`pam.conf.sssd.template`	SSSD	`/etc/pam.d/`

Окончание таблицы 42

Имя шаблона	Служба	Описание, размещение конфигурационного файла
mldap.conf	PARSEC	/etc/parsec/mldap.conf
mswitch.conf	PARSEC	/etc/parsec/mswitch.conf
krb.con.template	IPA	/usr/share/ipa/html
krbrealm.con.template	IPA	/usr/share/ipa/html
krb5.ini.template	IPA	/usr/share/ipa/html

8.2.10. Настройка синхронизация времени

При установке и инициализации FreeIPA конфигурация службы синхронизации времени chronyd настраивается автоматически для использования российских серверов точного времени ВНИИФТРИ.

При развертывании FreeIPA в сети без доступа к общедоступным серверам точного времени необходимо в конфигурационном файле /etc/chrony/chrony.conf указать IP-адрес локального сервера времени.

Затем перезапустить службу синхронизации времени:

```
systemctl restart chronyd
```

ВНИМАНИЕ! При использовании виртуальных машин процедура перезапуска автоматической синхронизации обязательно должна быть выполнена после каждого перезапуска и/или отката виртуальных машин.

8.2.11. Создание резервной копии и восстановление

Поддерживается создание резервных копий двух типов: полная резервная копия всей системы и резервная копия только данных. Установка пароля на резервные копии не поддерживается.

Резервные копии хранятся в каталоге /var/lib/ipa/backup. Для полного резервного копирования и резервного копирования данных используются, соответственно, обозначения ipa-full-YEAR-MM-DD-HH-MM-SS и ipa-data-YEAR-MM-DD-HH-MM-SS, где YEAR-MM-DD-HH-MM-SS — год, месяц, день, час, минуты и секунды в часовом поясе GMT создания резервной копии, например, 2018-03-05-10-30-22.

В каталоге /var/lib/ipa/backup размещается файл, в котором приведена информация о резервных копиях: тип, система, даты резервного копирования, версия FreeIPA, версия резервного копирования и др.

ВНИМАНИЕ! Резервную копию невозможно восстановить на другом компьютере или на другой версии FreeIPA.

Резервное копирование выполняется с помощью команды `ipa-backup`. Дополнительно с командой возможно использовать параметры, приведенные в таблице 43.

Таблица 43

Параметр	Описание
`--data`	Выполнить резервное копирование только данных. По умолчанию выполняется резервное копирование всех файлов FreeIPA и данных
`--logs`	Включить в резервную копию файлы журнала службы FreeIPA
`--online`	Выполнить резервное копирование без остановки сервера. Используется с параметром `--data`
`-v`, `--verbose`	Вывести сведения об отладке
`-d`, `--debug`	Вывести детальные сведения об отладке. Используется с параметром `--verbose`
`-q`, `--quiet`	Вывести только сведения о ошибках
`--log-file=FILE`	Выполнять регистрацию событий в файл `FILE`

8.2.12. Создание резервного сервера FreeIPA (настройка репликации)

Новый сервер FreeIPA возможно настроить на выполнение роли резервного сервера (реплики). Созданный резервный сервер будет являться точной копией исходного сервера FreeIPA и приравниваться к мастер-серверу. Изменения, внесенные в любой мастер-сервер, автоматически реплицируются на другие мастер-сервера.

Для добавления резервного сервера в домен FreeIPA необходимо выполнить следующие действия:

1) резервному серверу назначить фиксированный IP-адрес, который впоследствии не должен изменяться, и зарегистрировать резервный сервер в качестве клиента в домене FreeIPA в соответствии с 8.2.8;

2) на резервном сервере установить программный компонент `astra-freeipa-server` в соответствии с 8.2.4;

3) на резервном сервере запустить службу SSH, выполнив команду: `sudo systemctl enable --now ssh`

4) на основном сервере домена с использованием инструмента `astra-freeipa-server-crt` выпустить сертификат для резервного сервера с последующим переносом сертификата в домашний каталог администратора резервного сервера:

```
astra-freeipa-server-crt --host <реплика> --export --push \
```

```
<администратор>@<IP-адрес> --pin <пароль> --48
```

где <реплика> — полное доменное имя резервного сервера;
<администратор> — имя администратора резервного сервера;
<IP-адрес> — IP-адрес резервного сервера;
<пароль> — пароль к создаваемому контейнеру закрытого ключа и сертификата;
--48 — указание создать сертификат для FreeIPA версии 4.8.x (по умолчанию будут создаваться сертификаты для FreeIPA версии 4.6.x) .

Во время выпуска сертификата на все вопросы ответить «y» («Да»), и затем вести пароль администратора резервного сервера;

5) на резервном сервере из домашнего каталога администратора, в который ранее был скопирован контейнер закрытого ключа и сертификата, выполнить команду:

```
astra-freeipa-replica -a <реплика>.p12 --pin <пароль>
```

где <реплика> — полное доменное имя резервного сервера (в таком формате задается имя файла контейнера закрытого ключа и сертификата);
<пароль> — пароль к созданному контейнеру закрытого ключа и сертификата.

В ходе выполнения команды необходимо вести пароль администратора домена, а затем на все вопросы ответить «y» («Да»).

В случае успешной активации резервный сервер должен появиться на топологической схеме в веб-интерфейсе FreeIPA («IPA-сервер — Топология — Topology Graph», см. рис. 3).

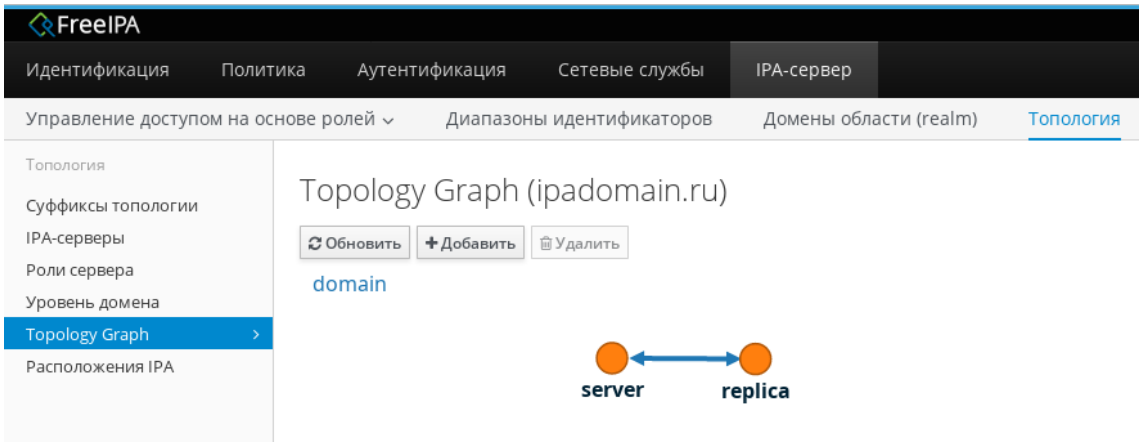

Рис. 3

8.2.13. Доверительные отношения между доменами

8.2.13.1. Общие сведения

Перед настройкой доверительных отношений контроллер домена AD должен быть настроен и работоспособен, а службы FreeIPA запущены в соответствии с 8.2.5.

ВНИМАНИЕ! Не удастся установить доверительные отношения с доменом AD, если имя области сервера FreeIPA не совпадает с его доменным именем.

Для создания доверительных отношений сервера FreeIPA с доменом AD служит пакет `freeipa-server-trust-ad`. Установка службы доверительных отношений выполняется с помощью инструмента командной строки `ipa-adtrust-install`.

В случае необходимости переустановки ранее удаленных объектов или поврежденных файлов конфигурации команду `ipa-adtrust-install` можно запустить несколько раз. Таким образом могут быть созданы новая конфигурация Samba (файл `smb.conf`) и конфигурация, на которой базируется регистрация. Некоторые элементы, например конфигурация локального диапазона, не могут быть изменены в результате повторного запуска команды `ipa-adtrust-install`, т. к. в данном случае изменения могут затронуть и другие объекты.

При выполнении команды `ipa-adtrust-install` для разрешения обмена информацией между доменами FreeIPA и AD необходимо удостовериться, что открыты следующие порты:

- 135/tcp EPMAP
- 138/tcp NetBIOS-DGM
- 139/tcp NetBIOS-SSN
- 445/tcp Microsoft-DS
- 1024/tcp
- 3268/tcp Microsoft-GC
- 138/udp NetBIOS-DGM
- 139/udp NetBIOS-SSN
- 389/udp LDAP

Дополнительно с командой `ipa-adtrust-install` возможно использовать параметры, приведенные в таблице 44.

Таблица 44

Параметр	Описание
`-d, --debug`	Вывести детальные сведения об отладке
`--netbios-name=NETBIOS_NAME`	Задать имя NetBIOS для домена FreeIPA. Если не указано, то оно определяется на основе ведущего компонента DNS-имени домена. Если запустить команду `ipa-adtrust-install` во второй раз с другим именем NetBIOS, то это имя изменится. **ВНИМАНИЕ!** Изменение имени NetBIOS может нарушить существующие доверительные отношения с другими доменами

Продолжение таблицы 44

Параметр	Описание
`--add-sids`	Добавить SID для существующих пользователей и групп в качестве активных на заключительных шагах запуска команды `ipa-adtrust-install`. Если в среде существует множество действующих пользователей и групп и несколько резервных серверов, то выполнение данного действия может привести к высокой скорости репликации трафика и снижению производительности всех серверов FreeIPA в среде. Чтобы избежать этого рекомендуется генерацию SID запускать после выполнения команды `ipa-adtrust-install`, для этого загрузить отредактированную версию `ipa-sidgen-task-run.ldif` с помощью команды `ldapmodify` на сервере домена AD
`--add-agents`	Добавить мастер-сервер FreeIPA в список для предоставления информации о пользователях доверенных лесов. Мастер-сервер FreeIPA может предоставлять эту информацию клиентам SSSD. Мастер-серверы FreeIPA не добавляются в список автоматически, т. к. для этого требуется перезапуск службы LDAP на каждом из них. Компьютер, на котором выполнена команда `ipa-adtrust-install`, добавляется автоматически. **ВНИМАНИЕ!** Мастер-серверы FreeIPA, на которых команда `ipa-adtrust-install` не была запущена, могут работать с информацией о пользователях доверенных лесов только если они активированы путем выполнения команды `ipa-adtrust-install` на любом другом мастер-сервере FreeIPA
`-U`, `--unattended`	Удалить без подтверждения. Ввод данных пользователем не будет запрашиваться
`--rid-base=RID_BASE`	Задать первое значение RID локального домена. Первый Posix ID локального домена будет присвоен данному RID, второй будет присвоен RID+1 и т. д.
`--secondary-rid-base=SECONDARY_RID_BASE`	Задать начальное значение вторичного RID диапазона, которое используется только в том случае, если пользователь и группа используют один и тот же Posix ID
`-A`, `--admin-name=ADMIN_NAME`	Задать имя пользователя с правами администратора для данного сервера FreeIPA. По умолчанию `admin`

Окончание таблицы 44

Параметр	Описание
`-a, --admin-password=password`	Задать пароль для пользователя с правами администратора для данного сервера FreeIPA. Будет запрашиваться в интерактивном режиме если параметр `-U` не указан. Учетные данные администратора будут использованы для получения билета Kerberos перед настройкой поддержки доверительных отношений перекрестной области, а также в дальнейшем, чтобы убедиться, что билет содержит MS-PAC сведения, необходимые для фактического добавления доверительных отношений с доменом AD при помощи команды `ipa trust-add -type=ad`

8.2.13.2. Предварительная настройка

Серверы домена AD и домена FreeIPA должны находиться в одной сети и на обоих серверах должна успешно выполняться команда:

```
ping <IP-адрес>
```

где `<IP-адрес>` — IP-адрес сервера домена AD при выполнении команды на сервере домена FreeIPA или IP-адрес сервера домена FreeIPA при выполнении команды на сервере домена AD.

8.2.13.3. Инициализация доверительных отношений

Для инициализации доверительных отношений необходимо на сервере домена FreeIPA выполнить следующие действия:

1) получить полномочия администратора домена и проверить работоспособность служб FreeIPA, выполнив команды:

```
kinit <администратор_домена_FreeIPA>
id <администратор_домена_FreeIPA>
getent passwd <администратор_домена_FreeIPA>
```

В результате выполнения команд не должны быть выявлены ошибки;

2) запустить службу доверительных отношений FreeIPA командой:

```
sudo ipa-adtrust-install
```

На все вопросы ответить «Да» («y») и затем вести пароль администратора домена FreeIPA. Проверить правильность автоматического определения имени домена и ответить «Да» («y»);

3) настроить и проверить перенаправление DNS. Добавление зоны перенаправления осуществляется командой:

```
ipa dnsforwardzone-add <домен_AD> --forwarder=WIN_IP ?forward-policy=only
```

Проверка успешного выполнения команды выполняется путем:

а) проверки доступности сервер домена AD:

```
ping -c 3 <сервер_домена_AD>.<домен_AD>
```

б) проверки доступности службы FreeIPA:

```
dig SRV _ldap._tcp.<домен_FreeIPA>
```

в) проверки доступности службы домена AD:

```
dig SRV _ldap._tcp.<домен_AD>
```

4) сохранить конфигурацию Samba, выполнив команду:

```
cp /etc/samba/smb.conf /etc/samba/smb.conf && sudo testparm \
    | sudo tee /etc/samba/smb.conf > /dev/null
```

5) проверить работоспособность службы Samba командой:

```
smbclient -k -L <сервер_домена_FreeIPA>.<домен_FreeIPA>
```

6) установить доверительные отношения между доменами:

а) одностороннее доверительное отношение — одностороннее доверие к домену AD, при котором область FreeIPA доверяет лесу доменов AD, используя механизм доверительных отношений между деревьями доменов AD, но дерево доменов AD не доверяет области FreeIPA. Пользователи дерева доменов AD получают доступ к ресурсам области FreeIPA. Устанавливается командой:

```
ipa trust-add --type=ad <домен_AD> --admin \
     <администратор_домена_AD> --password
```

б) двустороннее доверительное отношение устанавливается командой:

```
ipa trust-add --type=ad <домен_AD> --admin \
     <администратор_домена_AD> --password --two-way=true
```

в) внешнее доверительное отношение — отношение доверия между доменами AD, находящимися в разных лесах доменов AD. Установление доверительных отношений между лесами доменов всегда требует установления доверительных отношений между корневыми доменами этих лесов, однако, внешнее доверительное отношение может быть установлено между любыми доменами в лесу. Применяется для установления доверительных отношений с конкретными доменами и не переходит границы доверенного домена. Устанавливается командой:

```
ipa trust-add --type=ad <домен_AD> --admin \
     <администратор_домена_AD> --password --two-way=true --external
```

7) после установления доверительных отношений следует выполнить команду для получения списка доверенных доменов:

```
ipa trust-fetch-domains <домен_AD>
```

Домен должен быть найден при выполнении команды:

```
ipa trustdomain-find <домен_AD>
```

8) для работы пользователей домена AD в домене FreeIPA следует зарегистрировать данных пользователей, добавив соответствующие группы и пользователей в них:

```
ipa group-add --desc='ad domain external map' ad_admins_external \
     --external
ipa group-add --desc='ad domain users' ad_admins
ipa group-add-member ad_admins_external --external \
     '<домен_AD>\Domain Admins'
ipa group-add-member ad_admins --groups ad_admins_external
```

На запросы «member_user» и «member_group» нажать клавишу **<Enter>**;

9) для предоставления пользователям прав доступа к разделяемым ресурсам требуется указать их идентификаторы безопасности. Для получение идентификатора безопасности пользователей домена AD на сервере AD из оболочки CMD (но не из оболочки PowerShell) выполнить команду:

```
c:\> wmic useraccount get name,sid
```

Для получение идентификатора безопасности пользователей домена FreeIPA на сервере FreeIPA выполнить команду:

```
ipa group-show ad_admins_external --raw
```

Для добавления разделяемого каталога `/share_dir`, который будет доступен для пользователей домена AD под именем `share_name` выполнить:

```
sudo mkdir /share_dir
sudo net conf setparm 'share_name' 'comment' 'Trust test share'
sudo net conf setparm 'share_name' 'read only' 'no'
sudo net conf setparm 'share_name' 'valid users' "$d_admins_sid"
sudo net conf setparm 'share_name' 'path' '/share_dir'
```

Проверить, что ресурс добавлен, выполнив команду:

```
smbclient -k -L <сервер_домена_FreeIPA>.<домен_FreeIPA>
```

После добавления каталога проверить доступность ресурса с сервера AD через веб-браузер.

8.2.13.4. Проверка установки доверительных отношений

При успешной установке доверительных отношений пользователи домена AD должны получить возможность входа в систему с использованием своего имени и пароля:

- через терминал;
- через графический интерфейс;
- через SSH (если установлена соответствующая сетевая служба).

Также пользователям AD предоставляется возможность доступа к разделяемым ресурсам.

ВНИМАНИЕ! Для входа необходимо использовать полное имя пользователя с указанием домена, к которому пользователь относится, например, `Administrator@windomain.ad`, при этом имя домена пишется строчными буквами, а имя пользователя с сохранением строчных и заглавных букв.

Проверка настройки DNS на сервере домена AD выполняется из командной строки. Для просмотра записей выполнить команду:

```
c:\>nslookup.exe
```

В выводе выполнения команды будут приведены записи о работе служб и служб домена:

1) записи, отвечающие за работу служб Kerberos через UDP и LDAP через TCP:

```
> set type=SRV
> _kerberos._udp.<домен_FreeIPA>.
_kerberos._udp.<домен_FreeIPA>.       SRV service location:
priority                = 0
weight                  = 100
port                    = 88
svr hostname   = <сервер_домена_FreeIPA>.<домен_FreeIPA>.
> _ldap._tcp.<домен_FreeIPA>.
_ldap._tcp.<домен_FreeIPA>       SRV service location:
priority                = 0
weight                  = 100
port                    = 389
svr hostname   = <сервер_домена_FreeIPA>.<домен_FreeIPA>.
```

2) записи, отвечающие за имя Kerberos realm домена FreeIPA:

```
> set type=TXT
_kerberos.<домен_FreeIPA>.
_kerberos.<домен_FreeIPA>.        Text =
        "<домен_FreeIPA>"
```

3) после выполнения команды `ipa-adtrust-install` должны появиться записи, отвечающие за работу служб MS DC Kerberos через UDP и LDAP через TCP:

```
> set type=SRV
> _kerberos._udp.dc._msdcs.<домен_FreeIPA>.
_kerberos._udp.dc._msdcs.<домен_FreeIPA>.        SRV service location:
priority                = 0
weight                  = 100
port                    = 88
svr hostname = <сервер_домена_FreeIPA>.<домен_FreeIPA>.
> _ldap._tcp.dc._msdcs.<домен_FreeIPA>.
_ldap._tcp.dc._msdcs.<домен_FreeIPA>.        SRV service location:
priority                = 0
weight                  = 100
port                    = 389
svr hostname = <сервер_домена_FreeIPA>.<домен_FreeIPA>.
```

Проверка наличия записей для работы служб AD на DNS-сервере AD выполняется из командной строки. Для просмотра записей выполнить команду:

```
c:\>nslookup.exe
```

Записи, отвечающие за работу служб Kerberos через UDP и LDAP через TCP:

```
> set type=SRV
> _kerberos._udp.dc._msdcs.<домен_AD>.
_kerberos._udp.dc._msdcs.<домен_AD>.  SRV service location:
priority = 0
weight = 100
port = 88
svr hostname = <сервер_домена_AD>.<домен_AD>.
> _ldap._tcp.dc._msdcs.<домен_AD>.
_ldap._tcp.dc._msdcs.<домен_AD>.  SRV service location:
priority = 0
weight = 100
port = 389
svr hostname = <сервер_домена_AD>.<домен_AD>.
```

Проверка настройки DNS на сервере домена FreeIPA и наличия записей для работы служб FreeIPA на DNS-сервере FreeIPA выполняется из командной строки.

Для просмотра записи, отвечающей за работу службы Kerberos через UDP, выполнить команду:

```
dig +short -t SRV _kerberos._udp.<домен_FreeIPA>.
```

Запись выводится в следующем виде:

```
0 100 88 <сервер_домена_FreeIPA>.<домен_FreeIPA>.
```

Для просмотра записи, отвечающей за работу службы LDAP через TCP, выполнить команду:

```
dig +short -t SRV _ldap._tcp.<домен_FreeIPA>.
```

Запись выводится в следующем виде:

```
0 100 389 <сервер_домена_FreeIPA>.<домен_FreeIPA>.
```

Для просмотра записи, отвечающей за имя Kerberos realm домена FreeIPA, выполнить команду:

```
dig +short -t TXT _kerberos.<домен_FreeIPA>.
```

Запись выводится в следующем виде:

```
"<домен_FreeIPA>"
```

После выполнения команды `ipa-adtrust-install` должны появиться записи, отвечающие за работу служб MS DC Kerberos через UDP и LDAP через TCP:

```
# dig +short -t SRV _kerberos._udp.dc._msdcs.<домен_FreeIPA>.
0 100 88 <сервер_домена_FreeIPA>.<домен_FreeIPA>.

# dig +short -t SRV _ldap._tcp.dc._msdcs.<домен_FreeIPA>.
0 100 389 <сервер_домена_FreeIPA>.<домен_FreeIPA>.
```

Проверка наличия записей для работы служб AD на DNS-сервере FreeIPA выполняется из командной строки.

Записи, отвечающие за работу служб Kerberos через UDP и LDAP через TCP:

```
# dig +short -t SRV _kerberos._udp.dc._msdcs.<домен_AD>.
0 100 88 <сервер_домена_AD>.<домен_AD>.
```

```
# dig +short -t SRV _ldap._tcp.dc._msdcs.<домен_AD>.
0 100 389 <сервер_домена_AD>.<домен_AD>.
```

Если запись `_kerberos._udp.dc._msdcs.source-<домен_AD>.` недоступна, то необходимо проверить `_kerberos._tcp.dc._msdcs.source-<домен_AD>.`

8.2.14. Создание самоподписанного сертификата

8.2.14.1. Создание сертификата с помощью инструмента XCA

Установка и настройка инструмента XCA выполняется в соответствии с 6.10.5.1.

Для создания цепочки сертификатов необходимо запустить инструмент XCA и выполнить следующие действия:

1) создать корневой сертификат:

   а) во вкладке «Закрытые ключи» нажать кнопку **[Новый ключ]**. В открывшемся окне в поле «Внутреннее имя» указать имя «rootKey» и нажать **[Создать]**;

   б) перейти во вкладку «Сертификаты», нажать **[Новый сертификат]**;

   в) в открывшемся окне «Создать сертификат x509» перейти во вкладку «Субъект»:

   - в поле «Внутреннее имя» указать имя сертификата «rootCA»;
   - в поле «commonName» указать то же имя — «rootCA»;
   - в блоке «Закрытый ключ» выбрать ранее созданный ключ «rootKey»;

   г) в окне «Создать сертификат x509» перейти во вкладку «Расширения»:

   - в поле «Тип» выбрать «Центр Сертификации»;
   - определить период действия сертификата, указав в блоке «Выбор периода» значение «10»;
   - нажать кнопку **[Применить]**, затем нажать **[Да]**.

2) создать сертификат для сервера:

   а) в основном окне программы перейти во вкладку «Закрытые ключи» и нажать кнопку «Новый ключ»;

   б) в открывшемся окне в поле «Внутреннее имя» указать имя «serverKey» и нажать **[Создать]**;

   в) перейти во вкладку «Сертификаты», нажать **[Новый сертификат]**;

   г) в открывшемся окне «Создать сертификат x509» во вкладке «Первоисточник»:

   - в блоке «Подписание» установить флаг «Использовать этот сертификат для подписи» и выбрать значение «rootCA» (имя корневого сертификата);
   - в поле «Алгоритм подписи» указать «SHA 256»;

д) в окне «Создать сертификат x509» перейти во вкладку «Субъект»:

- в поле «Внутреннее имя» указать FQDN сервера, для которого формируется сертификат, например, `dc01.example.ru`;

- в поле «commonName» также указать FQDN сервера, для которого формируется сертификат;

- в блоке «Закрытый ключ» выбрать ранее созданный ключ «serverKey»;

е) в окне «Создать сертификат x509» перейти во вкладку «Расширения»:

- в поле «Тип» выбрать «Конечный субъект»;

- определить период действия сертификата, указав в блоке «Выбор периода» значение «10»;

- нажать кнопку **[Применить]**, затем нажать **[Да]**.

3) экспортировать сертификат сервера:

а) в основном окне программы перейти во вкладку «Сертификаты»;

б) выбрать требуемый сертификат сервера и нажать кнопку **[Экспорт]**;

в) в открывшемся окне указать имя файла контейнера сертификата и его расположение;

г) в блоке «Формат для экспорта» выбрать формат «PKCS12» и нажать кнопку **[Да]**;

д) задать пароль на экспортируемый контейнер и нажать кнопку **[Да]**.

На контроллере домена FreeIPA для указания контейнера с сертификатом выполнить команду `astra-freeipa-server` с параметрами `-l` и `-lp`:

```
astra-freeipa-server -l <путь_к_контейнеру> -lp <пароль_к_контейнеру>
```

Просмотреть перечень дополнительных параметров для запуска с командой `astra-freeipa-server` можно выполнив:

```
astra-freeipa-server --help
```

8.2.14.2. Создание сертификата с помощью инструмента командной строки

Инструмент командной строки `astra-freeipa-server-crt` автоматизирует выпуск сертификатов для серверов (реплик) FreeIPA и предназначен для автоматизации работы в системах, в которых не применяется DogTag, являющийся штатной системой управления сертификатами FreeIPA.

Установка инструмента командной строки `astra-freeipa-server-crt` выполняется автоматически при установке графической утилиты `fly-admin-freeipa-server` или инструмента командной строки `astra-freeipa-server` в соответствии с 8.2.4.

При инициализации домена FreeIPA в соответствии с 8.2.5 в каталоге `/etc/ssl/freeipa` первого контроллера домена автоматически создаются файлы, перечень которых приведен в таблице 45.

Таблица 45

Наименование, размещение файла	Описание
`/etc/ssl/freeipa/ca.key`	Закрытый ключ центра аутентификации
`/etc/ssl/freeipa/ca.crt`	Сертификат закрытого ключа центра аутентификации
`/etc/ssl/freeipa/server.key`	Закрытый ключ сервера
`/etc/ssl/freeipa/server.crt`	Сертификат закрытого ключа сервера

При первом запуске инструмента командной строки `astra-freeipa-server-crt` будет создан новый закрытый ключ сервера, который будет размещен в файле `/etc/ssl/freeipa/<имя_компьютера>.<имя_домена>.key`. Созданный закрытый ключ будет использоваться для выпуска и перевыпуска всех сертификатов.

ВНИМАНИЕ! Замена закрытых ключей посредством инструмента командной строки `astra-freeipa-server-crt` не поддерживается.

Кроме того, при запуске инструмента командной строки `astra-freeipa-server-crt` без указания параметров будет создан новый сертификат сервера. Выпущенный сертификат будет размещен в файле `/etc/ssl/freeipa/<имя_компьютера>.<имя_домена>-<дата_время>.crt`.

ВНИМАНИЕ! По умолчанию будут создаваться сертификаты для FreeIPA версии 4.6.x. Поэтому при запуске инструмента командной строки `astra-freeipa-server-crt` всегда необходимо указывать параметр `--48` (создавать сертификаты для FreeIPA версии 4.8.x).

Параметры инструмента командной строки `astra-freeipa-server` приведены в таблице 46.

Таблица 46

Параметр	Описание
`-h, --help`	Вывести справку по инструменту командной строки
`--certdir DIR`	Задать имя каталога (`DIR`) для поиска ключа и сертификата центра аутентификации и для размещения создаваемых сертификатов. Если каталог не существует — он будет создан. Значение по умолчанию `/etc/ssl/freeipa`
`--host FQDN`	Указать полное доменное имя (`FQDN`) сервера, для которого выпускается сертификат. Если имя не задано — используется `hostname` текущего сервера
`--cacrt FILE`	Указать имя файла (`FILE`) с существующим сертификатом центра аутентификации. Значение по умолчанию `/etc/ssl/freeipa/ca.crt`

Окончание таблицы 46

Параметр	Описание
`--cakey FILE`	Указать имя файла (`FILE`) с существующим закрытым ключом центра аутентификации. Значение по умолчанию `/etc/ssl/freeipa/ca.key`
`--sekey FILE`	Указать имя файла (`FILE`) с закрытым ключом сервера. Если файл не существует — будет создан новый закрытый ключ. Если имя не задано — ключ будет размещен в файле с именем `FQDN.key` в каталоге для размещения сертификатов
`--sekey_parm ALG`	Указать через двоеточие алгоритм и длину закрытого ключа сервера (`ALG`). Значение по умолчанию `rsa:2048`
`--secrt_days NUM`	Указать в днях срок действия (`NUM`) выпускаемого сертификата. Значение по умолчанию `365 дней`
`--export`	Экспортировать сертификат в контейнер формата `pkcs12` для установки нового сервера (новой реплики) FreeIPA. Экспорт будет выполнен в файл с именем `FQDN-<дата_время>.p12` в каталоге для размещения сертификатов. Не требуется для обновления сертификата уже установленного сервера
`--pin PIN`	Пароль (`PIN`) для экспорта сертификата. Чтобы задать пустой пароль, указать пробел в кавычках `--pin " "`. Если пароль не задан — он будет запрошен в процессе выполнения команды
`--push ADMIN`	Скопировать через `ssh/scp` созданные файлы на сервер, указанный в параметре `--host`, и зарегистрировать их. В параметре `ADMIN` можно задать не только имя пользователя, но и адрес целевого сервера, например `admin@192.168.32.11`. Все действия будут выполняться от имени `ADMIN`. Все файлы будут копироваться в домашний каталог этого пользователя. Если выполнялся экспорт сертификата для нового сервера (новой реплики), то сертификат будет скопирован в файл с именем `FQDN.p12`. Если создавался новый сертификат для существующего сервера, то: - копия этого сертификата будет скопирована в файл с именем `FQDN.crt`; - будет сделана попытка зарегистрировать его в БД сертификатов `/etc/apache2/nssdb`. **ВНИМАНИЕ!** После регистрации в БД сертификатов нового сертификата службы FreeIPA должны быть перезапущены вручную
`--46`	Создать сертификаты для FreeIPA версии 4.6.x. Данный параметр используется по умолчанию
`--48`	Создать сертификаты для FreeIPA версии 4.8.x
`-y`	Выполнить действия без запроса подтверждения

Пример использования инструмента командной строки `astra-freeipa-server-crt` для создания реплики в домене FreeIPA представлен в 8.2.12.

В случае необходимости выпуска новых сертификатов, например при истечении срока действия, можно воспользоваться следующей командой:

```
astra-freeipa-server-ctr --host <имя_компьютера>.<имя_домена> \
     --push <имя_локального_администратора>
```

8.2.15. Веб-интерфейс FreeIPA

Использование веб-интерфейса возможно после запуска FreeIPA согласно 8.2.5. Для входа в веб-интерфейс ввести в адресной строке браузера ссылку, предоставленную при запуске FreeIPA. В случае если при первом входе в веб-интерфейс появится сообщение о том, что соединение не защищено, следует добавить данный адрес в исключения.

Для входа в веб-интерфейс используется имя учетной записи `admin` и пароль, заданный при запуске FreeIPA (см. 8.2.5).

8.2.15.1. Установка мандатных атрибутов (user mac)

Для установки мандатных атрибутов пользователя необходимо:

1) выбрать пользователя и перейти во вкладку «Параметры»;
2) используя раскрывающиеся списки «Min MAC», «Max MAC» и «Уровень целостности» задать мандатные атрибуты;
3) для установки мандатных атрибутов нажать **[Сохранить]**.

Поле «Мандатный атрибут» должно принять заданное значение в соответствии с рис. 4.

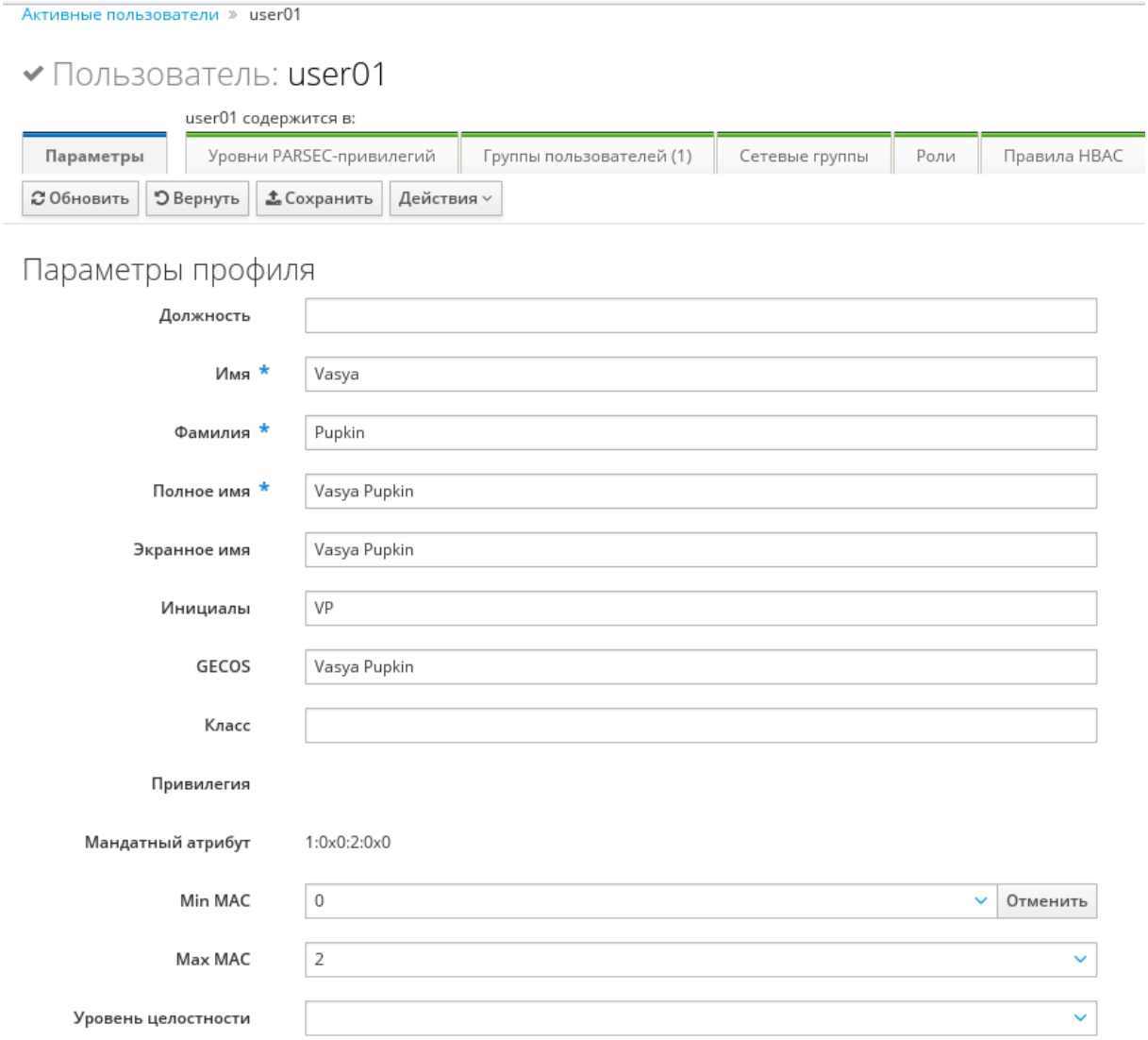

Рис. 4

8.2.15.2. Установка привилегий PARSEC

Для установки привилегий PARSEC необходимо:

1) выбрать пользователя и перейти во вкладку «Уровни PARSEC-привилегий»;
2) нажать **[Добавить]**;
3) в открывшемся окне в блоке «Доступен» отметить требуемые привилегии;
4) переместить отмеченные привилегии в блок «Ожидаемый», нажав кнопку **[>]**, затем нажать **[Добавить]** (см. рис. 5).

Поле «Мандатный атрибут» должно принять заданное значение.

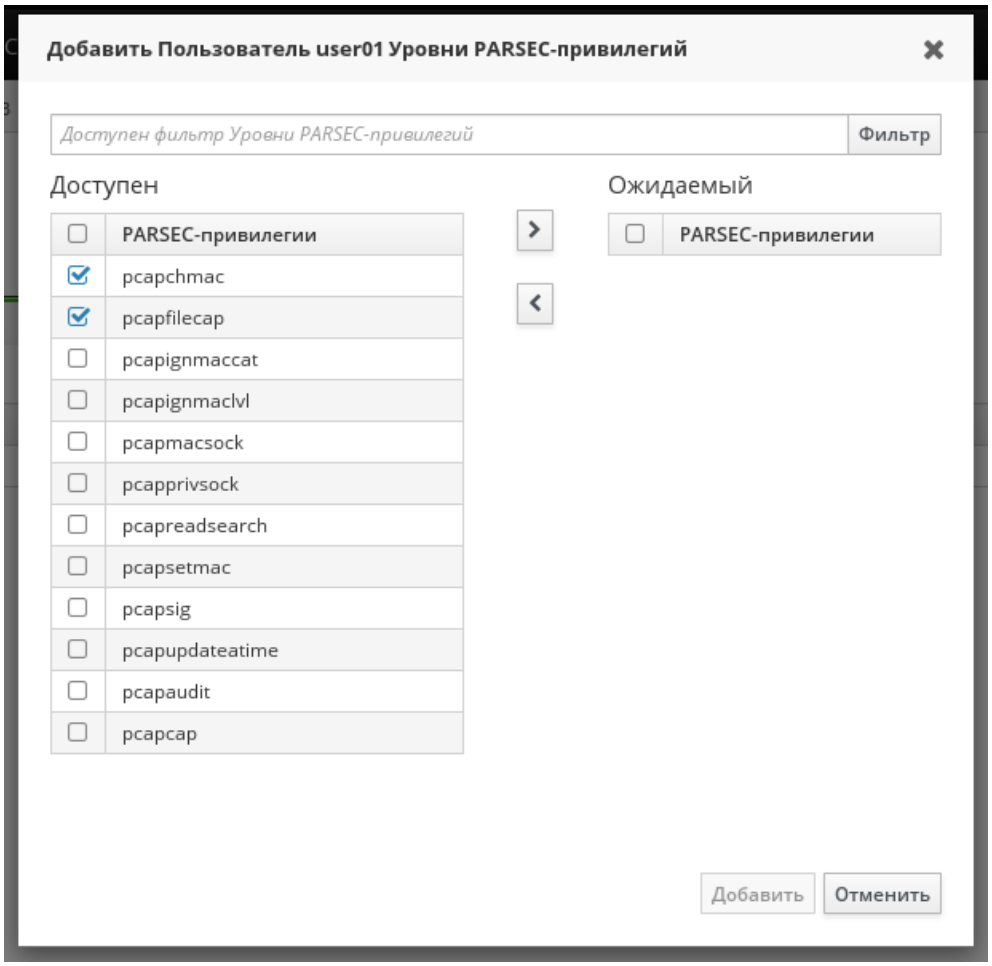

Рис. 5

Описание PARSEC-привилегий приведено в документе РУСБ.10015-01 97 01-1.

8.2.15.3. Добавление доменной службы

Для добавления новой доменной службы необходимо:

1) в разделе «Идентификация» перейти во вкладку «Службы»;

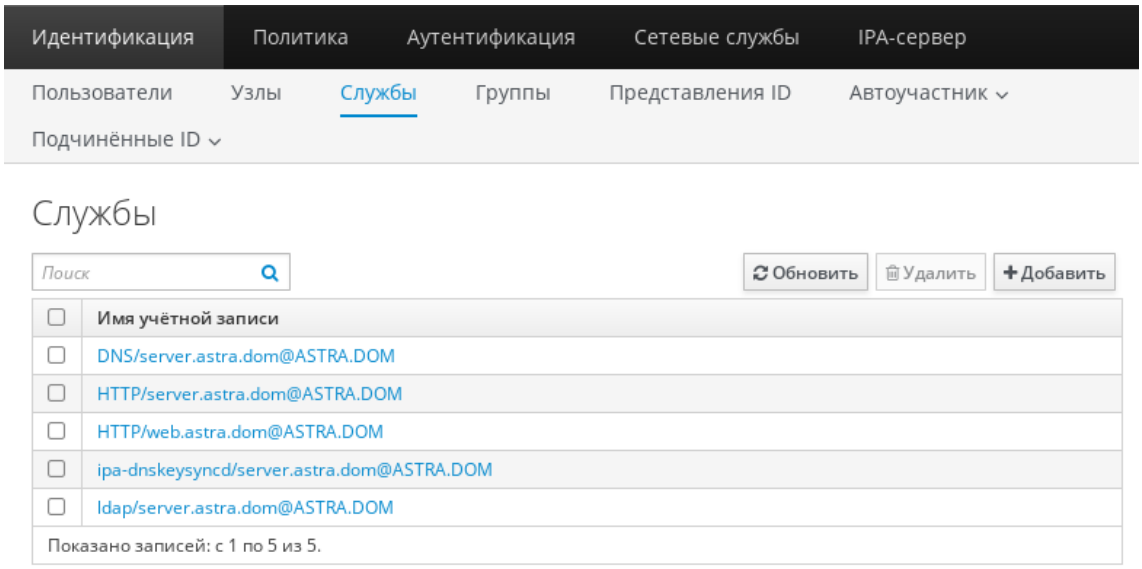

Рис. 6

2) нажать **[Добавить]**;

3) в открывшемся окне «Добавить службу» выбрать из выпадающих списков «Служба» и «Имя узла» тип службы и компьютер, на котором она будет работать;

4) для принудительной установки имени учетной записи службы, если для ее узла отсутствует запись в DNS, установить флаг «Принудительно»;

5) если узел для размещения службы недоступен или ещё не создан, то установить флаг «Пропустить проверку узла»;

6) для завершения добавления службы нажать **[Добавить]**. Для добавления службы и открытия окна для добавления еще одной службы нажать **[Добавить и добавить еще]**. Для добавления службы и последующего изменения ее параметров нажать **[Добавить и изменить]**. Для отмены изменений и закрытия окна нажать **[Отменить]**.

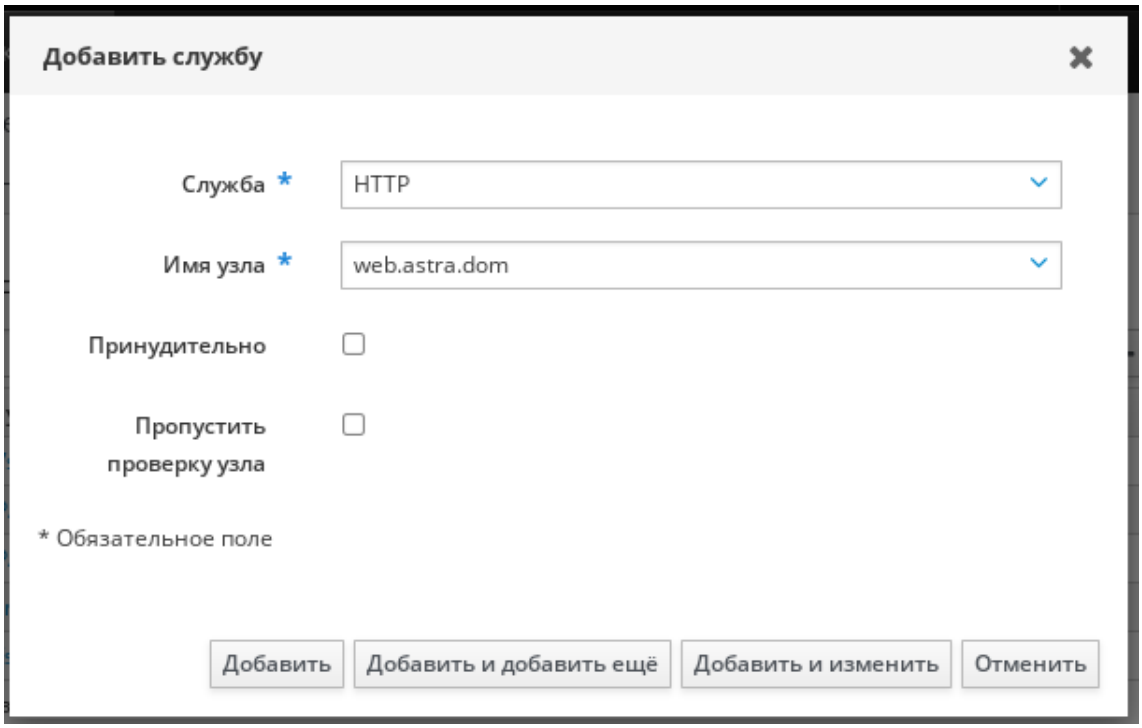

Рис. 7

8.2.16. Удаление контроллера домена

Для удаления контроллера домена с помощью инструмента командной строки `astra-freeipa-server` выполнить команду:

```
astra-freeipa-server -U
```

8.3. Samba

В состав ОС входит пакет программ Samba, предназначенный для решения задач совместимости со средой Microsoft Active Directory.

Samba позволяет ОС выступать как в роли контроллера домена AD, так и в роли клиента домена.

Возможности Samba:

- служба аутентификации на базе Kerberos;
- LDAP-совместимая служба каталогов с поддержкой репликации;
- поддержка групповых политик;
- поддержка доверительных отношений;
- DNS-сервер на базе BIND или собственной реализации.

В состав ОС входят консольные и графические средства, позволяющие инициализировать AD домен или подключиться к уже существующему.

Актуальные инструкции для разных сценариев применения приведены на официальном сайте wiki.astralinux.ru.

8.3.1. Настройка контроллера домена

В состав ОС входит инструмент командной строки astra-sambadc, включающий сценарии автоматизированной настройки и построения нового контроллера домена или включения в существующий домен в роли контроллера домена.

Для установки инструмента выполнить команду:

```
apt install astra-sambadc
```

При выполнении команды также будут установлены необходимые для работы домена AD пакеты samba, winbind и ntp.

Для создания нового домена в дополнение к инструменту astra-sambadc и автоматически устанавливаемым пакетам следует установить пакет krb5-kdc:

```
apt install krb5-kdc
```

Для создания нового домена используется команда:

```
astra-sambadc -d <имя_домена> -px
```

Данные, необходимые для создания домена и не указанные при выполнении команды, будут запрошены в интерактивном режиме.

Дополнительная информация по использованию команды доступна при выполнении команды с параметром -h:

```
astra-sambadc -h
```

Для настройки и построения нового контроллера домена или включения в существующий домен в роли контроллера домена в графическом режиме используется утилита fly-admin-ad-server.

Для установки графической утилиты выполнить команду:

```
apt install fly-admin-ad-server
```

Описание графической утилиты приведено в электронной справке.

8.3.2. Настройка участников домена

В состав ОС входит инструмент командной строки `astra-winbind`, включающий сценарии автоматизированной настройки компьютера для ввода в существующий домен.

ВНИМАНИЕ! Перед вводом компьютера в домен необходимо настроить на этом компьютере службу разрешения имен (DNS) так, чтобы в качестве сервера DNS использовался сервер DNS домена. Если этого не сделать, то контроллер домена не будет обнаружен.

Для ввода компьютера в домен используется команда:

```
astra-winbind -dc <имя_домена> -u <имя_администратора_домена> -px
```

Данные, необходимые для ввода в домен и не указанные при выполнении команды, будут запрошены в интерактивном режиме.

Дополнительная информация по использованию команды доступна при выполнении команды с параметром `-h`:

```
astra-winbind -h
```

Для ввода компьютера в существующий домен в графическом режиме используется утилита `fly-admin-ad-client`. Описание графической утилиты приведено в электронной справке.

Для проверки успешности присоединения к домену можно использовать команду:

```
net ads testjoin -k
```

8.4. Настройка сетевых служб

Ряд сетевых служб, таких как СУБД, электронная почта, обработка гипертекстовых документов (веб-сервер), система печати и др. должны быть настроены для работы в ЕПП. Как правило, настройка заключается в обеспечении возможности использования этими службами сквозной аутентификации по Kerberos и получения необходимой информации из БД LDAP.

Примечание. При выполнении настройки сетевых служб потребуется использование учетной записи привилегированного пользователя через механизм `sudo`. При снятии блокировки на интерактивный вход в систему для суперпользователя `root` не рекомендуется осуществлять переключение в режим суперпользователя командой `su`. Необходимо исполь-

зовать команду:

```
# su -
```

ВНИМАНИЕ! Для обеспечения нормальной работы пользователя с сетевыми службами в ЕПП должна быть явно задана его классификационная метка (диапазон уровней конфиденциальности и категорий конфиденциальности) с помощью соответствующих утилит, даже если ему не доступны уровни и категории выше 0.

Описание настройки следующих сетевых служб приведены в соответствующих подразделах:

- система обмена сообщениями электронной почты описана в 16.4;
- защищенный комплекс программ гипертекстовой обработки данных описан в разделе 11;
- защищенный комплекс программ печати и маркировки документов описан в 14.

Описание настройки СУБД приведено в документе РУСБ.10015-01 97 01-3.

9. ВИРТУАЛИЗАЦИЯ СРЕДЫ ИСПОЛНЕНИЯ

ОС поддерживает технологию виртуализации[1)] . Данная технология позволяет запускать множество виртуальных машин (ВМ), называемых гостевыми, на одной физической машине, называемой хостовой машиной. При этом гостевые операционные системы, установленные на каждой из гостевых машин, могут отличаться друг от друга и от операционной системы хостовой машины и являются полностью изолированными. Монитор виртуальных машин (гипервизор) обеспечивает параллельную работу гостевых операционных систем, их изоляцию, защиту, управление ресурсами и другие необходимые функции. Основными средствами, необходимыми для создания среды виртуализации, являются:

- сервер виртуализации libvirt;
- программа эмуляции аппаратного обеспечения QEMU.

Описание защиты среды виртуализации приведено в РУСБ.10015-01 97 01-1.

9.1. Сервер виртуализации libvirt

Сервер виртуализации состоит из службы сервера виртуализации `libvirtd`, предоставляющей возможность удаленного управления по сети с использованием различных протоколов и способов аутентификации, клиентской библиотеки `libvirt0`, командной оболочки `virsh` и ряда других утилит командной строки. В графическом интерфейсе управление сервером виртуализации и виртуальными машинами выполняется в утилите `virt-manager`.

ВНИМАНИЕ! Все конфигурационные файлы или файлы сервера виртуализации libvirt, содержащие ключевую информацию Kerberos или PKI, не должны быть доступны пользователям.

Сервер виртуализации использует следующие каталоги хостовой файловой системы (ФС):

1) `/etc/libvirt/` — каталог конфигурации сервера виртуализации libvirt:
   а) `qemu/` — каталог конфигурационных XML-файлов виртуальных машин QEMU:
      - `network/` — каталог конфигурационных XML-файлов виртуальных сетей;
      - `.xml` — конфигурационные XML-файлы виртуальных машин QEMU;
   б) `storage/` — каталог конфигурационных файлов пулов файлов-образов;
   в) `libvirt.conf` — клиентский конфигурационный файл сервера виртуализации libvirt;
   г) `libvirtd.conf` — конфигурационный файл службы сервера виртуализации `libvirtd` (см. 9.2);
   д) `qemu.conf` — конфигурационный файл QEMU (см. 9.6);

[1)] Для процессоров, поддерживающих технологию виртуализации.

2) /var/lib/libvirt/ — рабочий каталог сервера виртуализации libvirt:

а) images/ — каталог файлов-образов (используется по умолчанию);

б) network/ — рабочий каталог виртуальных сетей;

в) qemu/ — рабочий каталог запущенных виртуальных машин QEMU:

- save/ — каталог сохраненных состояний виртуальных машин;

- snapshot — каталог снимков виртуальных машин;

г) runimages/ — каталог расположения копий файлов-образов виртуальных машин, запущенных в режиме запрета модификации файлов-образов («только чтение»);

3) /var/run/libvirt/ — каталог текущего состояния сервера виртуализации libvirt:

а) network/ — рабочий каталог запущенных виртуальных сетей;

б) qemu/ — каталог текущих XML-файлов запущенных виртуальных машин QEMU;

в) libvirt-sock — unix-сокет для локальных соединений со службой сервера виртуализации libvirtd;

г) libvirt-sock-ro — unix-сокет, доступный только для чтения, для локальных соединений со службой сервера виртуализации libvirtd.

9.2. Служба сервера виртуализации libvirtd

Служба сервера виртуализации libvirtd предоставляет возможность удаленного управления сервером виртуализации по сети с использованием различных протоколов и способов аутентификации. При этом поддерживается возможность решения всех задач по созданию и учету виртуальных машин, настройке их конфигурации и непосредственно запуска.

Доступ к службе сервера виртуализации возможен как с помощью локальных Unix-сокетов, так и по сети с помощью консольных или графических инструментов управления виртуальными машинами.

Основным конфигурационным файлом службы сервера виртуализации является /etc/libvirt/libvirtd.conf. Он содержит описание необходимых для работы службы настроек и параметров. Файл разбит на секции, описывающие параметры функционирования службы сервера виртуализации: интерфейсы взаимодействия и права доступа к ним, способы и параметры аутентификации, политику разграничения доступа, состав выводимой в журнал информации и т. п. Основные параметры, указываемые в файле, приведены в таблице 47.

Таблица 47 – Параметры конфигурационного файла /etc/libvirt/libvirtd.conf

Параметр	Описание
listen_tls	Принимать TLS-соединения с использованием сертификатов
listen_tcp	Принимать TCP-соединения **ВНИМАНИЕ!** Для применения данной настройки дополнительно необходимо указать значение -l для параметра libvirtd_opts в конфигурационном файле /etc/default/libvirtd
listen_addr	Адрес сетевого интерфейса для приема соединений
tls_port	Порт для сетевых соединений TLS
tcp_port	Порт для сетевых соединений TCP
auth_tcp	Используемая для TCP-соединений аутентификация. Параметр должен содержать значение "sasl" (см. 9.3).
admin_group	Группа администраторов сервера виртуализации (значение по умолчанию "libvirt-admin"). Участие в данной группе позволяет администрировать ВМ. Если параметр закомментирован, то доступ к ВМ, в т.ч. для администрирования, будут иметь все пользователи
admvm_group	Группа администраторов виртуальных машин (значение по умолчанию "libvirt-admvm"). Участие в данной группе позволяет получать доступ к ВМ или выполнять ее администрирование в соответствии с ACL. При применении драйвера доступа "polkit" не рекомендуется изменение значения данного параметра
devel_group	Группа разработчиков виртуальных машин (значение по умолчанию "libvirt-dev"). При применении драйвера доступа "polkit" не рекомендуется изменять значение данного параметра
access_drivers	Применяемый драйвер ролевого доступа к серверу виртуализации. Параметр принимает значения: 1) ["polkit", "parsec"] — реализация ролевого управления доступом на основе драйвера доступа polkit; 2) ["parsec"] — реализация ролевого управления доступом на основе драйвера доступа parsec

Продолжение таблицы 47

Параметр	Описание
integrity_control	Применение механизма контроля целостности на основании подсчета контрольных сумм файлов конфигураций («отпечатка конфигурации»). Для включения механизма необходимо установить значение 1. Включение рекомендуется осуществлять после завершения всех настроек системы виртуализации
integrity_image_control	Применение механизма контроля целостности к файлам образов ВМ. Для включения механизма необходимо задать значение 1. Применяется только при включенном механизме контроля целостности на основании подсчета контрольных сумм файлов конфигураций (integrity_control = 1)
hash_type	Алгоритм вычисления контрольной суммы (хеша) образов ВМ
ilev_vm	Категория целостности, присваиваемая ВМ. Значение по умолчанию 63
memory_integrity_check_period_s	Применение механизма контроля целостности областей памяти ВМ. Для включения механизма необходимо задать значение периода проверки (в секундах). При выявлении нарушения целостности областей памяти ВМ выполняется регистрация фактов нарушения целостности объектов контроля
memory_integrity_check_shutdown_domain	Принудительное выключение ВМ в случае нарушения целостности установленных на контроль областей памяти ВМ. Для включения режима необходимо задать значение 1. При выявлении нарушения целостности областей памяти ВМ помимо регистрации фактов нарушения будет выполняться принудительное выключение ВМ
file_integrity_check_period_s	Применение механизма контроля целостности к установленным на контроль файлам гостевой операционной системы в процессе ее функционирования. Для включения механизма необходимо задать значение периода проверки (в секундах). При выявлении нарушения целостности файлов гостевой операционной системы выполняется регистрация фактов нарушения целостности объектов контроля
file_integrity_check_shutdown_domain	Применение режима принудительного выключения ВМ в случае нарушения целостности установленных на контроль файлов гостевой операционной системы. Для включения режима необходимо задать значение 1. При выявлении нарушения целостности файлов гостевой операционной системы помимо регистрации фактов нарушения будет выполняться принудительное выключение ВМ

Окончание таблицы 47

Параметр	Описание
file_integrity_on_startup_VM	Применение механизма контроля целостности файлов гостевой операционной системы при запуске ВМ. Для включения механизма необходимо задать значение 1. При выявлении нарушения целостности файлов гостевой операционной системы обеспечивается блокировка запуска ВМ и регистрация фактов нарушения целостности объектов контроля. Использование механизма возможно при условии применения ОС в качестве гостевой операционной системы
set_levels_in_VM	Ограничить максимальную классификационную метку, с которой можно войти в сессию операционной системы ВМ. Для ограничения необходимо задать значение 1. При включенном ограничении невозможно выполнить вход в сессию операционной системы ВМ с классификационной меткой выше, чем классификационная метка запустившего данную ВМ пользователя (классификационная метка данной ВМ)
keep_security_label_on_disks	Сохранить метку безопасности, присвоенную образу диска при запуске ВМ, после выключения этой ВМ. Для сохранения метки безопасности необходимо задать значение 1

Примечание. Конфигурационные параметры TLS для доступа к серверу виртуализации libvirt рассматриваются в 9.7.

9.3. Конфигурационные файлы сервера виртуализации

При использовании механизмов SALS для доступа к серверу виртуализации libvirt или к рабочим столам виртуальных машин через систему VNC или по протоколу SPICE необходимо наличие соответствующих конфигурационных файлов с параметрами SASL в каталоге /etc/sasl2. Для сервера виртуализации требуется файл libvirt.conf, для QEMU (VNC и SPICE) — qemu.conf.

Описание основных параметров конфигурационного файла SASL /etc/sasl2/libvirt.conf приведено в таблице 48.

Таблица 48

Параметр	Описание
mech_list	Список механизмов SASL

Окончание таблицы 48

Параметр	Описание
`keytab`	Путь к файлу ключевой информации Kerberos. Параметр необходим при использовании в ЕПП. Должен содержать корректные значения для файлов, содержащих ключевую информацию для VNC и SPICE
`sasldb_path`	Путь к базе данных SASL. При использовании в ЕПП не применяется и должен быть закомментирован.

ВНИМАНИЕ! Файлы ключевой информации Kerberos для VNC и SPICE должны быть доступны на чтение пользователям, запускающим виртуальные машины, и группе `libvirt-qemu`.

Для VNC и SPICE могут быть заданы другие пути расположения конфигурационного файла SASL. Описание конфигурационного файла `qemu.conf` приведено в 9.6.

9.4. Консольный интерфейс virsh

В состав пакетов сервера виртуализации libvirt входит консольный интерфейс управления виртуальными машинами `virsh`, позволяющий в консоли с помощью командной оболочки производить действия по управлению конфигурацией виртуальных машин.

Командная оболочка содержит набор команд по управлению виртуальными машинами, файлами-образами носителей, виртуальными интерфейсами и сетями и позволяет править конфигурационные файлы виртуальных машин.

Более подробно возможности консольного интерфейса управления виртуальными машинами `virsh` описаны в соответствующем руководстве `man`.

9.5. Графическая утилита virt-manager

Графическая утилита управления виртуальными машинами `virt-manager` предоставляет доступ к возможностям сервера виртуализации libvirt из графического интерфейса пользователя. Внешний вид окна утилиты приведен на рис. 8.

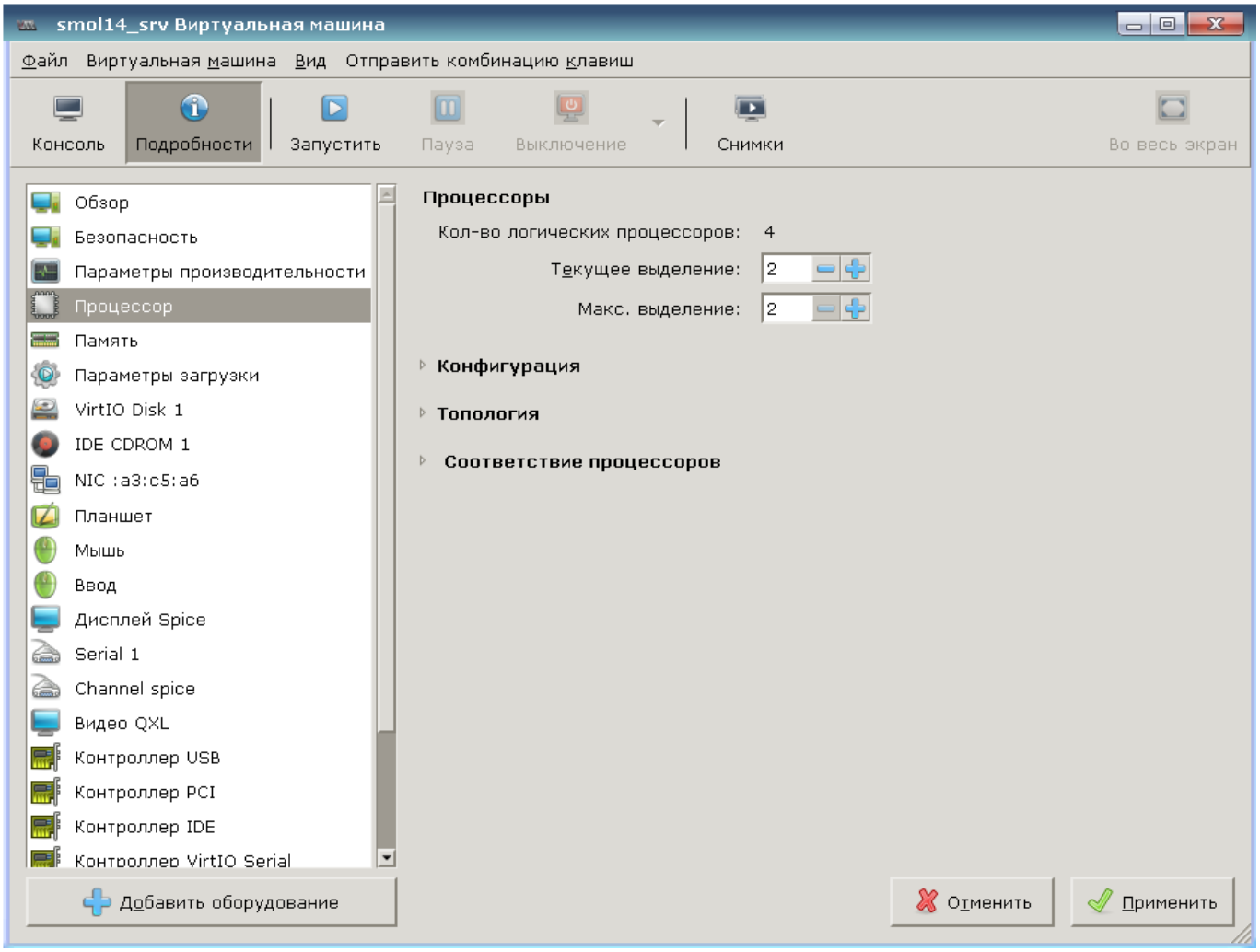

Рис. 8

Утилита позволяет выполнять действия по созданию виртуальных машин, управлению их конфигурацией и файлами-образов дисковых носителей. Также обеспечивает удаленный доступ к рабочему столу выбранной виртуальной машины по протоколам VNC и SPICE.

9.6. Средства эмуляции аппаратного обеспечения на основе QEMU

Средства эмуляции аппаратного обеспечения на основе QEMU реализуют программно-аппаратное окружение запускаемой виртуальной машины, включая заданную конфигурацию аппаратной платформы и набор эмулируемых устройств, доступных гостевой операционной системе. В случае совпадения гостевой аппаратной платформы и аппаратной платформы хостовой машины используются возможности аппаратной поддержки виртуализации средствами KVM (Kernel-based Virtual Machine) для хостовых операционных систем семейства Linux.

Компонент состоит из пакетов, представляющих программу эмуляции аппаратного обеспечения QEMU для различных аппаратных платформ и необходимый набор утилит командной строки.

QEMU Guest Agent (гостевой агент QEMU) обеспечивает возможность взаимодействия с гостевой ОС. Для отправки и получения команд гостевой агент использует последовательное соединение virtio. Он позволяет зафиксировать файловую систему до выполнения снимка, при этом в снимке не будет большой части записанных данных. Фиксация файловой системы возможна только с драйверами хранилищ Ceph и qcow2. Для использования агента необходимо установить пакет `qemu-guest-agent` на гостевой ОС.

ВНИМАНИЕ! Применение гостевого агента QEMU доступно только для виртуальных машин, запущенных из нулевого мандатного контекста.

Запущенная средствами QEMU/KVM виртуальная машина представляет собой отдельный процесс хостовой операционной системы.

Основным конфигурационным файлом QEMU является `/etc/libvirt/qemu.conf`. Он содержит описание параметров, необходимых для запуска и функционирования виртуальных машин (например, интерфейсов взаимодействия с рабочим столом виртуальных машин, способов и параметров аутентификации, политики управления безопасностью и изоляцией виртуальных машин), а также значения по умолчанию некоторых параметров конфигурации виртуальных машин. Описание основных параметров конфигурационного файла `/etc/libvirt/qemu.conf` приведено в таблице 49.

Таблица 49

Параметр	Описание
`vnc_listen`	Адрес сетевого интерфейса для приема соединений VNC
`vnc_tls`	Использовать TLS для приема соединений VNC
`vnc_tls_x509_cert_dir`	Путь к сертификатам TLS при работе VNC
`vnc_password`	Пароль для соединений VNC
`vnc_sasl`	Использовать SASL для приема соединений VNC
`vnc_sasl_dir`	Каталог конфигурационного файла `qemu.conf`, содержащий SASL-параметры для приема соединений VNC (см. 9.3)
`spice_listen`	Адрес сетевого интерфейса для приема соединений по протоколу SPICE
`spice_tls`	Использовать TLS для приема соединений по протоколу SPICE
`spice_tls_x509_cert_dir`	Путь к сертификатам TLS при работе по протоколу SPICE
`spice_password`	Пароль для соединений по протоколу SPICE
`spice_sasl`	Использовать SASL для приема соединений по протоколу SPICE
`spice_sasl_dir`	Каталог конфигурационного файла `qemu.conf`, содержащий SASL-параметры для приема соединений по протоколу SPICE
`security_driver`	Применяемый драйвер безопасности. Параметр должен содержать значение `"parsec"`

Окончание таблицы 49

Параметр	Описание
`run_images_dir`	Каталог расположения копий файлов-образов виртуальных машин, запущенных в режиме запрета модификации файлов-образов

Примечание. Конфигурационные параметры TLS для доступа к рабочим столам виртуальных машин посредством VNC рассматриваются в 9.8.

ВНИМАНИЕ! При использовании в виртуальной машине SPICE-графики, в гостевой ОС должен быть установлен QXL-драйвер. В ОС драйвер устанавливается с пакетом `xserver-xorg-video-qxl`.

9.7. Идентификация и аутентификация при доступе к серверу виртуализации libvirt

Сервер виртуализации может использовать для идентификации и аутентификации клиентов следующие механизмы:

- локальная peer-cred аутентификация;
- удаленная SSH-аутентификация (строка соединения `qemu+ssh://...`);
- удаленная SASL-аутентификация, в том числе с поддержкой Kerberos (строка соединения `qemu+tcp://...`);
- удаленная TLS-аутентификация с использованием сертификатов (строка соединения `qemu+tls://...`).

ВНИМАНИЕ! В целях обеспечения удаленного доступа пользователей с использованием сетей связи общего пользования к средствам виртуализации из состава ОС должны применяться средства криптографической защиты информации, прошедшие процедуру оценки соответствия согласно законодательству Российской Федерации.

Параметры для различных способов аутентификации задаются в конфигурационном файле `/etc/libvirt/libvirtd.conf`: параметры локальных UNIX сокетов (секция «UNIX socket access control»), разрешение приема сетевых соединений tcp и tls (параметры `listen_tls` и `listen_tcp`) и порты для их приема (параметры `tls_port` и `tcp_port`), расположение необходимых файлов при использовании сертификатов x509 (секция «TSL x509 certificate configuration»), варианты аутентификации (параметры `auth_unix_ro`, `auth_unix_rw`, `auth_tcp`, `auth_tls`).

По умолчанию используется следующее расположение файлов сертификатов на сервере для аутентификации к серверу виртуализации libvirt:

- `/etc/pki/CA/cacert.pem` — корневой сертификат;
- `/etc/pki/CA/crl.pem` — файл отозванных сертификатов;

- /etc/pki/libvirt/servercert.pem — сертификат открытого ключа сервера виртуализации libvirt;
- /etc/pki/libvirt/private/serverkey.pem — закрытый ключ сервера виртуализации libvirt.

Примечание. Файлы ключей сервера виртуализации libvirt должны быть доступны на чтение группе libvirt-qemu.

По умолчанию используется следующее расположение файлов сертификатов на клиенте для аутентификации к серверу виртуализации libvirt («~» — домашний каталог пользователя):

- /etc/pki/CA/cacert.pem — корневой сертификат;
- ~/.pki/libvirt/clientcert.pem — сертификат открытого ключа клиента;
- ~/.pki/libvirt/clientkey.pem — закрытый ключ клиента.

В случае SASL-аутентификации используется конфигурационный файл /etc/sasl2/libvirt.conf, в котором задаются параметры аутентификации SASL (например, применяемые механизмы). Имя службы сервера виртуализации libvirt при использовании SASL-аутентификации регистрируется как libvirt/<имя сервера>@<домен>.

ВНИМАНИЕ! При указании механизма SASL gssapi следует в конфигурационном файле /etc/default/libvirtd указать с помощью соответствующей переменной окружения расположение файла ключей Kerberos сервера виртуализации, например:

```
export KRB5_KTNAME=/etc/libvirt/libvirt.keytab.
```

Для организации двусторонней аутентификации пользователя по ключам при удаленном подключении к серверу виртуализации необходимо на узле, с которого будет производиться подключение, сгенерировать SSH-ключ и скопировать его публичную часть на сервер. Для этого с правами пользователя, от имени которого будет создаваться подключение, требуется выполнить следующие действия:

1) создать ключ командой:

```
ssh-keygen -t rsa
```

2) скопировать созданный ключ на хост командой (при соответствующем запросе ввести пароль для аутентификации):

```
ssh-copy-id user@host
```

где host — IP-адрес сервера с libvirt;
user — пользователь, заведенный на сервере. В результате появится возможность работы с домашними каталогами пользователя user на сервере с libvirt.

Для защиты закрытого ключа (аутентифицирующего пользователя) от утечки, он может быть преобразован на парольной фразе (passphrase), которая задается при создании ключа. Пользователю необходимо вводить пароль для преобразования ключа один раз в начале сессии.

При следующем подключении запрос о подлинности сервера не задается, если сервер не был подменен (ключ сервера не изменился). Если сервер оказывается подменен (изменен адрес, на который разрешается имя `host`), выдается предупреждение и соединение не устанавливается.

При подключения по SSH из графической утилиты `virt-manager` в меню выбрать «Файл — Добавить соединение», отметить флаг «Connect to remote host over SSH» в соответствии с рис. 9.

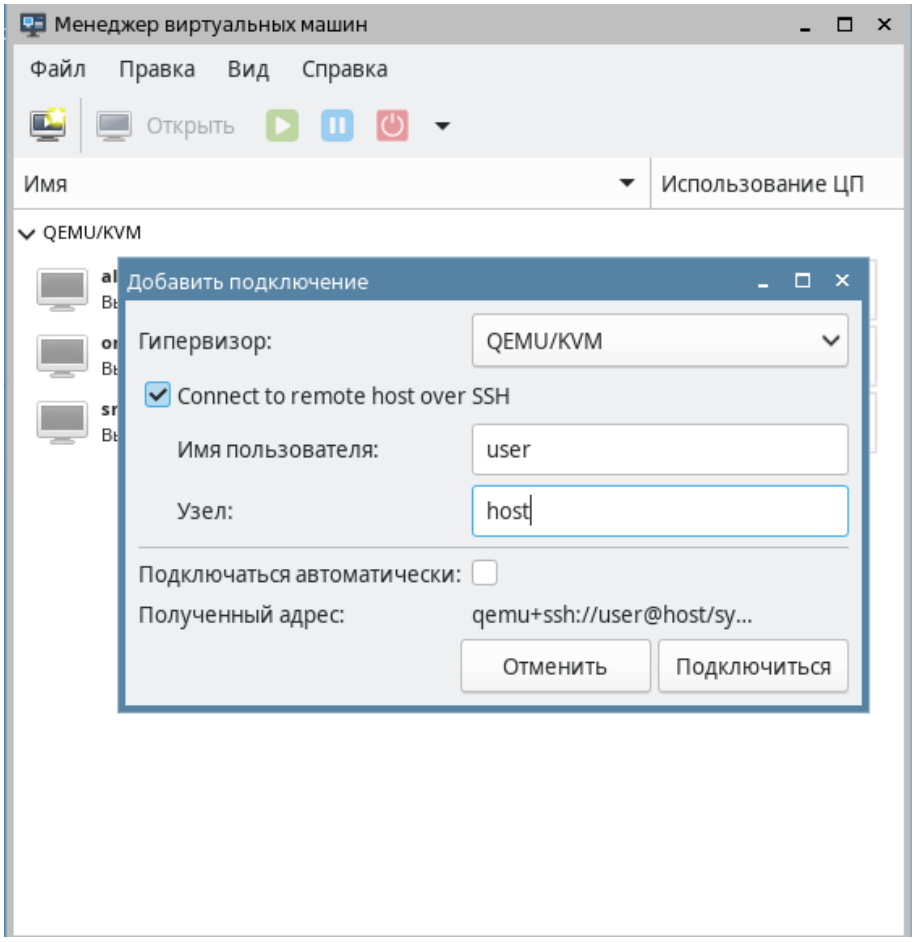

Рис. 9

При подключении из терминала к серверу виртуализации libvirt по SSH указать унифицированный идентификатор ресурса (URI) следующего вида:

```
qemu+ssh://user@host/system
```

где host — IP-адрес сервера с libvirt;

user — пользователь, заведенный на сервере.

9.8. Идентификация и аутентификация при доступе к рабочему столу виртуальных машин

Параметры аутентификации при доступе к рабочему столу виртуальной машины задаются в конфигурационном файле /etc/libvirt/qemu.conf раздельно для VNC и SPICE. В данном конфигурационном файле указываются необходимые параметры аутентификации и пути к конфигурационным файлам SASL, например /etc/sasl2/qemu.conf. Имя служб VNC и SPICE при использовании SASL-аутентификации регистрируется как vnc/<имя сервера>@<домен> и spice/<имя сервера>@<домен>, соответственно.

По умолчанию используется следующее расположение файлов сертификатов на сервере для аутентификации к виртуальной машине посредством VNC:

- /etc/pki/libvirt-vnc/ca-cert.pem — корневой сертификат;
- /etc/pki/libvirt-vnc/server-cert.pem — сертификат открытого ключа сервера VNC QEMU;
- /etc/pki/libvirt-vnc/server-key.pem — закрытый ключ сервера VNC QEMU.

Примечание. Файлы ключей сервера VNC QEMU должны быть доступны на чтение группе libvirt-qemu.

По умолчанию используется следующее расположение файлов сертификатов на клиенте для аутентификации к серверу VNC QEMU («~» — домашний каталог пользователя):

- /etc/pki/CA/cacert.pem — корневой сертификат;
- ~/.pki/libvirt-vnc/clientcert.pem — сертификат открытого ключа клиента;
- ~/.pki/libvirt-vnc/private/clientkey.pem — закрытый ключ клиента.

10. КОНТЕЙНЕРИЗАЦИЯ

В ОС реализован механизм контейнеризации, обеспечивающий режим виртуализации и изоляции ресурсов на уровне ядра ОС. Использование данного механизма позволяет запускать приложение и необходимый ему минимум системных библиотек в полностью стандартизованном контейнере, соединяющемся с хостовой ОС при помощи определенных интерфейсов.

Контейнеры используют ядро хостовой ОС и, в отличие от полной виртуализации, не требуют эмуляции аппаратного обеспечения. Приложения, запущенные внутри разных контейнеров, изолированы и не могут влиять друг на друга.

10.1. Контейнеризация с использованием Docker

В состав ОС входит программное обеспечение Docker для автоматизации развертывания и управления приложениями в средах с поддержкой контейнеризации.

10.1.1. Установка Docker

Установка Docker возможна либо через графический менеджер пакетов Synaptic, либо через терминал с помощью команды:

```
sudo apt install docker.io
```

После установки возможно добавить пользователя в группу `docker`, что позволит работать с Docker без использования `sudo`.

Для включения пользователя в группу `docker` выполнить команду:

```
sudo usermod -aG docker <имя_пользователя>
```

Текущего пользователя можно включить в группу командой:

```
sudo usermod -aG docker $USER
```

Для применения действия необходимо выйти из текущей сессии пользователя и зайти повторно.

10.1.2. Работа с Docker

Полный список команд для работы с Docker доступен на странице помощи:

```
docker help
```

Информацию о параметрах конкретной команды можно получить на странице помощи или в справочной странице `man`.

Пример

```
docker attach --help
man docker-attach
```

ВНИМАНИЕ! Описание работы с образами и контейнерами Docker приведено для привилегированного режима. Данный режим не рекомендуется к применению в связи с потенциальной небезопасностью использования контейнеров в привилегированном режиме. Рекомендуется работать с Docker в непривилегированном (rootless) режиме в соответствии с описанием 10.1.3.

10.1.2.1. Создание образа Docker

Образ — это шаблон контейнера, включающий в себя:

1) базовую файловую систему;
2) слои — изменения в файловой системе, расположенные друг над другом в том порядке, в котором эти изменения были произведены;
3) параметры выполнения, используемые при запуске контейнера из данного образа.

Примечание. Из одного образа возможно запускать несколько контейнеров.

Каждый слой образа представляет собой инструкцию, выполняемую в базовой файловой системе при создании образа. В процессе работы контейнера изменения файловой системы образуют новый слой контейнера, а слои образа остаются неизменными.

Слои могут быть последовательно записаны в текстовом документе, который называется докерфайлом (Dockerfile).

Образ возможно создать тремя способами:

- из `chroot`-окружения;
- с помощью докерфайла;
- на основе контейнера.

Создание образа из chroot-окружения

Для создания собственных образов Docker из `chroot`-окружения необходимо установить пакет `debootstrap`. Это можно сделать либо с помощью графического менеджера пакетов Synaptic, либо из терминала, выполнив команду:

```
sudo apt install debootstrap
```

Для создания образа Docker необходимо:

1) собрать `chroot`-окружение;
2) настроить `chroot`-окружение;
3) конвертировать `chroot`-окружение в образ Docker.

Сборка `chroot`-окружения выполняется инструментом командной строки `debootstrap` от имени администратора.

Загрузка пакетов для сборки `chroot`-окружения может быть выполнена из репозитория, доступного по сети.

Пример

```
sudo debootstrap --verbose \
     --components=main,contrib,non-free,non-free-firmware 1.8_x86-64 /var/do
     http://dl.astralinux.ru/astra/stable/1.8_x86-64/repository-main
```

где `1.8_x86-64` — код дистрибутива;
`/var/docker-chroot` — каталог сборки окружения;
`http://dl.astralinux.ru/...` — расположение репозитория в сети.

Загрузка пакетов для сборки `chroot`-окружения также может быть выполнена из репозитория в локальной ФС.

При сборке `chroot`-окружения для удобства дальнейшей работы можно сразу установить пакеты `ncurses-term`, `mc`, `locales`, `nano`, `gawk`, `lsb-release`, `acl`, `perl-modules`.

Пример

```
sudo debootstrap --verbose --include \
     ncurses-term,mc,locales,nano,gawk,lsb-release,acl,perl-modules-5.28 \
     1.8_x86-64 /var/docker-chroot file:///srv/repo
```

где `1.8_x86-64` — код дистрибутива;
`/var/docker-chroot` — каталог сборки окружения;
`file:///srv/repo` — каталог локального репозитория.

Примечание. При включенном МРД и/или МКЦ рекомендуется размещать каталог сборки `chroot`-окружения в `/var`. Данный каталог имеет метку безопасности `3:63:-1:ccnr`, что позволяет создавать в нем файловые объекты с любыми метками безопасности. Для работы пользователей в непривилегированном режиме администратором системы должен быть создан доступный пользователю каталог с необходимой меткой безопасности.

Настройка `chroot`-окружения выполняется от имени администратора в следующей последовательности:

1) при необходимости настроить для `chroot`-окружения разрешение имен в файле `/etc/resolv.conf` и список репозиториев в `/etc/apt/sources.list` (например, скопировать одноименные файлы из корневой ФС в каталог для `chroot`-окружения);

2) перейти в `chroot`-окружение командой `sudo chroot` и обновить пакеты окружения:

```
sudo chroot /var/docker-chroot
apt update
apt dist-upgrade
exit
```

Для создания образа Docker следует добавить настроенное `chroot`-окружение в архив с помощью инструмента командной строки `tar`, запущенного от имени администратора, и конвертировать полученный архив в образ командой:

```
docker import <параметры>
```

Пример

Создать образ `wiki/astralinux:se` из `chroot`-окружения:

```
sudo tar -C /var/docker-chroot -cpf - . | sudo docker import \
- wiki/astralinux:se --change "ENV PATH \
/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin" \
--change 'CMD ["/bin/bash"]'
```

где `-C /var/docker-chroot` — задать каталог в качестве рабочего каталога для архивирования;

`-cpf - .` — создать новый архив из рабочего каталога с сохранением разрешений, установленных на входящие в него каталоги и файлы, и передать архив в `stdin`;

`docker import -` — импортировать данные для создания образа из `stdout`;

`--change "ENV PATH ..."` — задать переменную окружения `PATH`;

`--change 'CMD ["/bin/bash"]'` — задать команду, которая будет автоматически выполнена в контейнере при запуске контейнера из данного образа.

Если все операции выполнены успешно, то созданный образ будет отображаться в списке образов, доступном по команде:

```
sudo docker images
```

Для запуска контейнера из созданного образа используется команда:

```
sudo docker run -it --rm <имя_образа>
```

где `-i` — запустить контейнер в интерактивном режиме;

`-t` — выделить терминал для контейнера;

`--rm` — удалить контейнер после выхода из него.

Создание образа с использованием докерфайла

Докерфайл представляет собой инструкции для создания образа Docker. Используя докерфайл и контекст (совокупность каталогов и файлов в указанном месте) возможно создавать новые образы на основе существующих с помощью команды:

```
docker build
```

При этом полное содержимое контекста рекурсивно пересылается службе `dockerd` и может быть скопировано в создаваемый образ командами, указанными в докерфайле. Поэтому не рекомендуется использовать в качестве контекста корневой каталог файловой системы ОС. Местоположение контекста может быть задано как путь к каталогу в файловой системе либо как ссылка на репозиторий в сети.

По умолчанию используется докерфайл с именем `Dockerfile`, расположенный в каталоге контекста сборки. Произвольное расположение докерфайла задается параметром `-f`:

```
docker build -f <путь_к_докерфайлу> .
```

Перед выполнением инструкций в докерфайле проводится их проверка на корректность. Если в инструкциях содержится ошибка (например, неправильный синтаксис), при попытке собрать образ будет выведено сообщение об ошибке.

Пример

Создать образ с использованием докерфайла, содержащего несуществующую инструкцию `RUNCMD`:

```
docker build -t test/myimg .
```

В терминале будет выведено сообщение об ошибке:

```
Sending build context to Docker daemon 2.048 kB
Error response from daemon: Unknown instruction: RUNCMD
```

При создании нового образа инструкции выполняются последовательно и результат выполнения каждой инструкции записывается в отдельный слой образа.

Пример

Для сборки нового образ на основе существующего образа `wiki/astralinux:se` следует:

1) создать корневой каталог контекста сборки:

```
mkdir build-smolensk
```

2) создать в контексте сборки файл `data-to-import` содержащий произвольный текст:

```
echo "Это импортированные данные" > build-smolensk/data-to-import
```

3) в файл `build-smolensk/Dockerfile` внести следующий текст:

```
# указание из какого образа выполнять сборку
FROM wiki/astralinux:se
# скопировать файл data-to-import из контекста сборки в образ
COPY /data-to-import /srv
# создать в образе пустой файл /srv/created-file
RUN touch /srv/created-file
# вывести на печать содержимое скопированного файла
RUN cat /srv/data-to-import
# вывести на печать рабочий каталог
RUN echo Current work directory is $(pwd)
```

4) выполнить сборку образа с именем `test`:

```
docker build -t test build-smolensk/
```

Вывод в терминале будет иметь следующий вид:

```
Sending build context to Docker daemon   5.12kB
Step 1/5 : FROM wiki/astralinux:se
---> 60d0611fe56a
Step 2/5 : COPY /data-to-import /srv
---> 7a75a002d29f
Step 3/5 : RUN touch /srv/created-file
---> Running in 709bb54af8c3
Removing intermediate container 709bb54af8c3
---> b5fd28178901
Step 4/5 : RUN cat /srv/data-to-import
---> Running in 4c69f455cf2f
Это импортированные данные
Removing intermediate container 4c69f455cf2f
---> c8f8c7c3797a
Step 5/5 : RUN echo Current work directory is $(pwd)
---> Running in 27db5fcaaba5
Current work directory is /
Removing intermediate container 27db5fcaaba5
---> 14446097a09e
Successfully built 14446097a09e
Successfully tagged test:latest
```

5) проверить, что образ `test` присутствует в списке образов:

```
docker images
```

6) если образ был успешно создан, запустить контейнер из образа:

```
docker run --rm -it test
```

7) проверить содержимое контейнера, выполнив в контейнере команду:

```
ls -l /srv
```

Результат выполнения команды должен быть следующего вида:

```
total 4
-rw-r--r-- 1 root root  0 Jan 20 10:12 created-file
-rw-r--r-- 1 root root 51 Jan 20 10:11 data-to-import
```

затем выполнить команду:

```
cat /srv/data-to-import
```

Результат выполнения команды должен быть следующего вида:

```
Это импортированные данные
```

Из вывода в терминале видно, что в контейнере присутствует файл `data-to-import`, скопированный из контекста сборки в образ, и пустой файл `created-file`, созданный в образе при сборке.

Подробное описание команды `docker build` и работы с докерфайлами приведено в `man docker-build` и `man dockerfile`, соответственно.

Создание образа из контейнера

При наличии сохраненного или активного контейнера (описание работы с контейнерами приведено в 10.1.2.3) данный контейнер возможно конвертировать в образ Docker следующей командой:

```
docker container commit <параметры> <имя_контейнера> <имя_образа>
```

Пример

Создать образ `test-image` из контейнера `test`:

```
docker container commit test test-image
```

Все изменения в контейнере относительно образа, из которого тот был запущен, а также команды, переданные в качестве параметров при создании нового образа, сформируют новый слой создаваемого образа.

Параметры данной команды описаны в `man docker-container-commit`.

10.1.2.2. Копирование образа

Образ, хранящийся на локальной машине, может быть скопирован (например на другую машину).

Пример

Для того чтобы скопировать образ `wiki/astralinux:se` на другую машину, необходимо:

1) выгрузить образ в архив:

```
docker save -o astralinux-se.bz2 wiki/astralinux:se
```

где `-o` — задает имя файла, в который будет выведен образ. Если этот параметр не указан, образ будет выведен в `stdout`;

2) скопировать полученный файл `astralinux-se.bz2` на целевую машину;

3) на целевой машине загрузить файл в локальный реестр образов:

```
docker load -i astralinux-se.bz2
```

где `-i` — указывает имя файла, из которого будет загружен образ. Если этот параметр не указан, образ будет загружен из `stdin`.

Эту процедуру возможно выполнить одной командой с копированием созданного архива через SSH (для этого на целевой машине должен быть настроен SSH):

```
docker save wiki/astralinux:se | bzip2 | ssh user@host \
'bunzip2 | docker load'
```

где `docker save wiki/astralinux:se` — выгрузить образ `wiki/astralinux:se` в `stdout`;
`bzip2` — программа сжатия данных;
`ssh user@host 'bunzip2 | docker load'` — подключиться через SSH к машине с именем `host` от имени пользователя `user` и запустить команды загрузки образа из стандартного ввода (`stdin`). Пользователь `user` на целевой машине должен иметь право работать с Docker без использования `sudo`.

10.1.2.3. Создание и работа с контейнерами

Для того, чтобы создать новый контейнер с заданным именем из образа, используется следующая команда:

```
docker run <параметры> <имя_образа>
```

Примеры:

1. Создать контейнер с именем `run-smolensk` из образа `smolensk`:

```
docker run --name run-smolensk --rm -it smolensk
```

где `run-smolensk` — имя контейнера. Если параметр не указан, присваивается случайное имя;

`--rm` — уничтожить контейнер после завершения его работы. Если параметр не указан, контейнер будет локально сохранен;

`-i` — запустить контейнер в интерактивном режиме. Если параметр не указан, контейнер запустится в фоновом режиме;

`-t` — создать терминал;

`smolensk` — имя образа, из которого создается контейнер.

2. Для создания нескольких контейнеров с произвольными именами из образа `smolensk` следует:

1) запустить контейнер из образа `smolensk`:

```
docker run smolensk
```

2) выполнить команду повторно;

3) вывести список контейнеров:

```
docker container ls -a
```

В выводе будут отображены два контейнера со случайными именами, созданные из образа `smolensk`:

```
CONTAINER ID IMAGE ... NAMES
b894e0b0b22d smolensk ... admiring_murdock
825a33f9c18c smolensk ... amazing_morse
```

Для запуска сохраненного контейнера следует использовать команду:

```
docker start <имя_контейнера>
```

Пример

Запустить контейнер `amazing_morse` в интерактивном режиме:

```
docker start -ai amazing_morse
```

К контейнеру, работающему в фоновом режиме, можно подключиться командой:

```
docker attach <имя_контейнера>
```

Пример

Подключиться к контейнеру `amazing_morse`, работающему в фоновом режиме:

```
docker attach amazing_morse
```

Для просмотра списков контейнеров выполнить команду:

```
sudo docker container list
```

10.1.2.4. Запуск контейнеров на выделенном уровне МКЦ

С целью изоляции и ограничения среды исполнения потенциально опасного или вредоносного кода в ОС реализована возможность запуска контейнеров на низком уровне МКЦ. Описание функции приведено в документе РУСБ.10015-01 97 01-1.

10.1.2.5. Монтирование файловых ресурсов хостовой машины в контейнер

Docker поддерживает следующие типы монтирования файловых ресурсов хостовой машины в контейнер:

1) `bind` — монтирование файла или каталога, расположенного на хостовой машине, в контейнер;

2) `mount` — монтирование управляемых Docker изолированных томов для хранения данных;

3) `tmpfs` — монтирование временного файлового хранилища (`tmpfs`) в контейнер. Это позволяет контейнеру размещать временные ресурсы в памяти хостовой машины.

Параметры монтирования задаются при создании контейнеров и сохраняются в течение их работы.

ВНИМАНИЕ! Чтобы предотвратить нежелательные изменения в конфигурации хостовой машины, следует исключить монтирование файловых ресурсов, влияющих на конфигурацию хостовой машины, либо ограничить права доступа контейнера к файловым ресурсам правом на чтение.

Параметры монтирования могут быть заданы с использованием одного из двух флагов, определяющих формат, в котором будут заданы параметры и их значения:

1) с использованием флага `-v` — параметры монтирования задаются набором значений, разделенных двоеточием. Набор параметров зависит от типа монтирования. Например, тип монтирования `bind` будет иметь следующий вид:

```
docker run -v <монтируемый_ресурс>:<точка_монтирования>:
<дополнительные_параметры> <имя_образа>
```

2) с использованием флага `--mount` — параметры монтирования задаются в виде `<параметр>=<значение>` и отделяются друг от друга запятыми:

```
docker run --mount type=<тип_монтирования>,source=<монтируемый_ресурс>,
target=<точка_монтирования>,<дополнительные_параметры> <имя_образа>
```

bind

Тип монтирования `bind` монтирует каталог, расположенный на хостовой машине, в ФС контейнера. Содержимое каталога на хостовой машине и в точке монтирования в контейнере полностью идентично, а изменения в одном каталоге повторяются в другом.

ВНИМАНИЕ! Данный метод монтирования является устаревшим.

С использованием флага `-v` параметры типа монтирования `bind` задаются следующим образом:

```
docker run -v <монтируемый_ресурс>:<точка_монтирования>:
<дополнительные_параметры> <имя_образа>
```

С использованием флага `--mount` параметры типа монтирования `bind` задаются следующим образом:

```
docker run --rm -it --mount type=<тип_монтирования>,
source=<монтируемый_ресурс>,target=<точка_монтирования>,
<дополнительные_параметры> <имя_образа>
```

Примеры:

1. Смонтировать рабочий каталог хостовой машины в каталог `/app` контейнера с параметром `readonly`, используя флаг `--mount`:

```
docker run --rm -it --mount \
type=bind,source="$(pwd)",target=/app,readonly smolensk
```

2. Смонтировать рабочий каталог хостовой машины в каталог `/app` контейнера с параметром `read-only`, используя флаг `-v`:

```
docker run --rm -it -v $(pwd):/app:ro smolensk
```

Тип монтирования `bind` позволяет настраивать распространение монтирования (bind propagation). В контексте контейнеризации распространение монтирования определяет, как события монтирования (монтирование и размонтирование ресурсов) в контейнере могут повлиять на ресурсы хостовой машины и/или других контейнеров, а события монтирования на хостовой машине — на ресурсы одного или нескольких контейнеров.

Для настройки распространения монтирования используется параметр `bind-propagation`. Параметр принимает следующие значения:

- `shared` — если при создании контейнера в него был смонтирован каталог с этим параметром, например каталог `/myfiles` на хостовой машине в `/contfiles` в контейнере, то другие ресурсы, смонтированные внутри `/contfiles`, также будут доступны в `/myfiles`. Аналогично ресурсы, смонтированные внутри `/myfiles`, будут доступны в `/contfiles`. Если при создании нескольких контейнеров в каждый из них был смонтирован с этим параметром один и тот же каталог, то смонтированные внутри него ресурсы также будут доступны в каждом из данных контейнеров;
ВНИМАНИЕ! В режиме `shared` изменения в одной точке монтирования распространяются на все остальные точки монтирования, что может привести к нежелательным изменениям файловых объектов других контейнеров, и, как следствие, нарушению их работы;
- `rshared` — то же, что `shared`, но применяется рекурсивно;
- `slave` — если при создании контейнера в него был смонтирован каталог с этим параметром, например каталог `/myfiles` на хостовой машине в `/contfiles` в контейнере, то другие ресурсы, смонтированные внутри `/myfiles`, также будут доступны в каталоге `/contfiles`, но при этом ресурсы, смонтированные внутри `/contfiles`, не будут доступны на хостовой машине;
- `rslave` — то же, что `slave`, но применяется рекурсивно;
- `private` — если при создании контейнера в него был смонтирован каталог с этим параметром, например каталог `/myfiles` на хостовой машине в `/contfiles` в контейнере, то другие ресурсы, смонтированные внутри `/contfiles`, не будут доступны на хостовой машине, а ресурсы, смонтированные внутри `/myfiles`, не будут доступны в контейнере;
- `rprivate` — то же, что `private`, но применяется рекурсивно. Используется по умолчанию.

Примеры:

1. Смонтировать подкаталог `/target` рабочего каталога хостовой машины в каталог `/app` контейнера с типом распространения монтирования `rslave`, используя флаг `--mount`:

```
docker run -d -it --mount \
type=bind,source="$(pwd)"/target,target=/app,readonly,\
bind-propagation=rslave smolensk
```

2. Смонтировать подкаталог `/target` рабочего каталога хостовой машины в каталог `/app` контейнера с типом распространения монтирования `shared`, используя флаг `-v`:

```
docker run -d -it -v "$(pwd)"/target:/app:ro,shared smolensk
```

mount

Том Docker представляет собой файловую систему, расположенную на хостовой машине вне контейнера и находящуюся под управлением Docker. Тома хранятся в каталоге Docker на хостовой машине, например `/var/lib/docker/volumes/`. Тома существуют независимо от жизненного цикла контейнера и могут быть многократно использованы разными контейнерами. Управление томами описано в `man docker-volume`.

Для создания тома используется следующая команда:

```
docker volume create <имя_тома>
```

Пример

Создать том с именем `my-vol`:

```
docker volume create my-vol
```

С флагом `-v` параметры монтирования `mount` задаются следующим образом:

```
docker run -v <имя_тома>:<точка_монтирования> <имя_образа>
```

С использованием флага `--mount` команда будет иметь следующий вид:

```
docker run --mount src=<имя_тома>,dst=<точка_монтирования> <имя_образа>
```

Примеры:

1. Смонтировать том `my-vol` в каталог `/app` контейнера с использованием флага `-v`:

```
docker run --rm -it -v my-vol:/app smolensk
```

2. Смонтировать том `my-vol` в каталог `/app` контейнера с использованием флага `--mount`:

```
docker run --rm -it --mount src=my-vol,dst=/app smolensk
```

tmpfs

Тип монтирования `tmpfs` монтирует временное файловое хранилище (`tmpfs`) в ФС контейнера, что позволяет контейнеру хранить временные файловые ресурсы в памяти хостовой машины. Доступ к этим файловым ресурсам имеет только тот контейнер, в котором они были созданы. При остановке контейнера временные файловые ресурсы будут полностью удалены из ФС контейнера и памяти хостовой машины.

С использованием флага `--mount` параметры монтирования `tmpfs` задаются следующим образом:

```
docker run --mount type=tmpfs,destination=<точка_монтирования> <имя_образа>
```

С использованием флага `--tmpfs` команда будет иметь следующий вид:

```
docker run --tmpfs <точка_монтирования> <имя_образа>
```

Примеры:

1. Запустить контейнер из образа `smolensk` с монтированием `tmpfs` в каталог контейнера `/app`, используя флаг `--mount`:

```
docker run --rm -it --mount type=tmpfs,destination=/app smolensk
```

2. Запустить контейнер из образа `smolensk` с монтированием `tmpfs` в каталог контейнера `/app`, используя флаг `--tmpfs`:

```
docker run --rm -it --tmpfs /app smolensk
```

Примечания:

1. Синтаксис `--tmpfs` не поддерживает использование параметров монтирования.
2. Монтирование `tmpfs` не поддерживает флаг `-v`.

10.1.3. Работа с Docker в непривилегированном режиме

Работа с образами и контейнерами Docker в непривилегированном (rootless) режиме подразумевает работу от имени пользователя без использования механизма `sudo`. В непривилегированном режиме служба контейнеризации и контейнеры не получают прав суперпользователя в хостовой ОС, при этом для приложения в контейнере служба контейнеризации работает как суперпользователь.

Для работы с Docker в непривилегированном режиме используется инструмент командной строки `rootlessenv`, который настраивает окружение для работы в данном режиме. При работе в непривилегированном режиме инструмент `rootlessenv` должен использоваться вместо механизма `sudo` в командах при настройке и работе с образами и контейнерами Docker (см. 10.1.2).

Для настройки работы в режиме rootless необходимо выполнить следующие шаги:

1) установить Docker в соответствии с 10.1.1;

2) установить пакет `rootless-helper-astra` для использования непривилегированного режима :

```
sudo apt install rootless-helper-astra
```

3) запустить службы rootless Docker для пользователя, который будет использовать образы и контейнеры Docker в непривилегированном режиме:

```
sudo systemctl start rootless-docker@<имя_пользователя>
```

4) при необходимости настроить автозапуск служб rootless Docker выполнить:

```
sudo systemctl enable rootless-docker@<имя_пользователя>
```

Запуск и настройка автозапуска служб могут быть выполнены для нескольких пользователей, для этого необходимо выполнить соответствующие команды отдельно для каждого пользователя.

Чтобы запустить контейнер от имени текущего пользователя с использованием `rootlessenv`, следует выполнить:

```
rootlessenv docker run --rm -ti <имя_образа>
```

Для запуска контейнера от имени произвольного пользователя с `rootlessenv` выполнить:

```
sudo -u <имя_пользователя> rootlessenv docker run --rm -ti <имя_образа>
```

Работа с образами и контейнерами, созданными в режиме rootless, возможна только в режиме rootless.

Для просмотра списка контейнеров, созданных в режиме rootless, выполнить команду:

```
rootlessenv docker container list
```

Работа с `rootless-helper-astra` и `rootlessenv` более подробно описана в `man rootless-helper-astra` и `man rootlessenv`, соответственно.

Описание работы с образами и контейнерами Docker в непривилегированном режиме с ненулевыми метками безопасности приведено в документе РУСБ.10015-01 97 01-1.

10.1.4. Docker swarm

Docker позволяет выполнять некоторые функции оркестратора контейнеров и создавать простые кластеры, состоящие из узлов, на которых запускаются контейнеры. При этом Docker не является полноценной системой оркестрации, так как не обеспечивает контроль доступа по сети, не позволяет планировать выполнение служебных задач и работать с группами контейнеров. Для управления кластерами используется механизм `docker swarm`.

Синтаксис команды:

```
docker swarm <действие> [параметры]
```

Список основных действий команды `docker swarm` приведен в таблице 50.

Таблица 50

Действие	Описание
`init`	Инициализировать кластер
`join`	Присоединить узел к кластеру в качестве рабочего или управляющего
`join-token`	Получить токен безопасности для присоединения узла к кластеру
`leave`	Вывести рабочий узел из кластера
`update`	Применить параметры кластера после их изменения

Полный список действий и параметров команды `docker swarm` приведен в официальной документации Docker.

Для разграничения доступа к кластерам и их ресурсам используются роли. Назначение ролей осуществляется добавлением пользователей в группы, приведенные в таблице 51. Группы создаются автоматически при установке Docker.

Таблица 51

Роль	Группа	Описание
Администратор кластера	`swarm-cluster-admin`	Управляет всем кластером с возможностью создания кластера и подключения нового узла к управляющему узлу кластера. Пользователям из группы доступны все возможности `docker swarm`
Администратор сервиса	`swarm-service-admin`	Управление сервисами кластера
Администратор рабочего узла	`swarm-cluster-node-admin`	Управление рабочим узлом, просмотр состояния узла, подключение узла к существующему кластеру
Наблюдатель	`swarm-observer`	Просмотр состояния кластера без внесения изменений

Управление доступа к кластерам по умолчанию включено. Для его отключения следует в файле `/etc/docker/daemon.json` изменить значение параметра `swarm-rules-enabled` на `false` (см. 10.3.2.4 и 10.3.3).

10.2. Контейнеризация с использованием Podman

Программное обеспечение Podman для автоматизации развертывания и управления приложениями в средах с поддержкой контейнеризации аналогично программному обеспечению Docker, но предоставляет дополнительные возможности по управлению группами контейнеров и может работать без использования учетной записи `root`. Podman использует контейнеры стандарта Open Container Initiative (OCI), что обеспечивает совместимость с образами Docker.

10.2.1. Установка Podman

Podman представлен одноименным пакетом `podman`. Пакет может быть установлен с помощью графического менеджера пакетов Synaptic или из командной строки с помощью команды:

```
sudo apt install podman
```

При работе с включенным мандатным управлением доступом после установки пакета необходимо перезапустить пользовательскую сессию или перезагрузить ОС.

10.2.2. Стандартные команды

Podman поддерживает все команды Docker, кроме `docker swarm`, а также имеет ряд собственных команд. Полный список команд для работы с Podman доступен на странице помощи:

```
podman --help
```

Информация о параметрах конкретной команды доступна на странице помощи или на справочной странице `man`.

Пример

```
podman pod create --help
man podman-pod-create
```

ВНИМАНИЕ! По умолчанию Podman использует среду выполнения контейнеров `crun`. В ОС работа контейнеров поддерживается только при использовании среды `runc`. В связи с этим для запуска контейнеров следует использовать команды Podman с параметрами `--runtime=runc` и `--cgroup-manager=cgroupfs`.

10.2.3. Работа с Podman

10.2.3.1. Включение отладки

Для включения отладки используется параметр `--log-level` с указанием требуемого уровня отладки. Отладочная информация выводится в стандартный поток сообщений об ошибках `stderr`.

Пример

Выполнение команды с включенным уровнем отладки `debug`:

```
podman --log-level debug ps -a
```

10.2.3.2. Запуск контейнера из образа

Для запуска контейнера из загруженного образа используется команда:

```
podman run <параметры> <имя_образа>
```

Пример

Запустить контейнер из образа `astralinux` в интерактивном режиме с терминалом и уничтожить его после завершения работы:

```
podman run -it --rm astralinux /bin/bash
```

Для запуска контейнера в фоновом режиме используется команда:

```
podman run -d <имя_образа>
```

При запуске контейнера к его файловой системе может быть примонтирован каталог из файловой системы хостовой машины. Для этого следует выполнить команду:

```
podman run --mount
type=bind,source=<монтируемый_каталог>,target=<точка_монтирования>
<имя_образа>
```

10.2.3.3. Вывод списка контейнеров

Для вывода списка запущенных (работающих) контейнеров используется команда:

```
podman ps
```

Для вывода списка всех контейнеров (в том числе завершивших работу) используется команда:

Пример

```
podman ps -a
```

Пример вывода команды:

```
CONTAINER ID  IMAGE       COMMAND     CREATED
0468d9f62e2d  astralinux  /bin/bash   12 seconds ago

STATUS                     PORTS       NAMES
Exited (0) 5 seconds ago               priceless_hertz
```

10.2.3.4. Действия с сохраненными контейнерами

Возможно выполнение следующих действий с контейнерами (при этом в командах в качестве идентификатора контейнера используется его числовой идентификатор `CONTAINER ID` или имя `NAMES`, см. 10.2.3.3):

1) запуск сохраненного контейнера выполняется командой:

```
podman start <идентификатор_контейнера>
```

2) остановка контейнера выполняется командой:

```
podman stop <идентификатор_контейнера>
```

3) удаление контейнера выполняется командой:

```
podman rm <идентификатор_контейнера>
```

Перед удалением контейнер должен быть остановлен;

4) получение полной информации о контейнере выполняется командой:

```
podman inspect <идентификатор_контейнера>
```

Эта команда выводит большой объем информации, отфильтровать вывод информации можно применением параметра `--format`:

```
podman inspect <идентификатор_контейнера> --format '<параметр_фильтрации>'
```

5) вывод журналов контейнера выполняется командой:

```
podman logs <идентификатор_контейнера>
```

6) вывод статистики работы контейнеров выполняется командой:

```
podman stats
```

Эта команда после запуска не завершает свою работу, а продолжает выводить статистику с заданным интервалом (по умолчанию каждые 5 секунд). Для однократного вывода статистики с последующим завершением выполнения команды работы следует использовать параметр `--no-stream`:

```
podman stats --no-stream
```

10.2.3.5. Удаление образа

Для удаления образа предварительно необходимо остановить и удалить все созданные из него контейнеры. После этого использовать команду:

```
podman rmi <идентификатор_образа>
```

10.2.4. Создание собственного контейнера из существующего образа

Для создания собственного контейнера на основе имеющегося образа следует выполнить следующее:

1) создать докерфайл с указанием образа, из которого будет создаваться контейнер, и команд для его создания:

```
echo -e "FROM smolensk\nRUN
mkdir /testdir\nRUN echo test > /testdir/testfile" > Dockerfile
```

2) создать контейнер:

```
podman --runtime=runc --cgroup-manager=cgroupfs build -t testbuild .
```

10.2.5. Создание собственного образа

Создание собственного образа производится аналогично описанному в 10.1.2.1. При этом в командах следует заменять `docker` на `podman`.

10.2.6. Управление группами контейнеров

Podman позволяет оркестрировать контейнеры — объединять контейнеры в группы («поды») и управлять ими как единым целым. Контейнеры в поде используют общие ресурсы и пространство имен. Это полезно в ситуациях, когда для выполнения одной задачи требуется одновременная работа нескольких контейнеров, например, база данных в одном контейнере и веб-сервер для доступа к ней в другом контейнере.

10.2.6.1. Создание нового пода

Для создания нового пода необходимо выполнить команду:

```
podman --cgroup-manager cgroupfs pod create <имя_пода>
```

Создание пода происходит следующим образом:

- если имя пода не задано, то используется случайно созданное имя;
- создается полный идентификатор (выводится на экран при успешном создании пода);
- в поде создается служебный контейнер (так называемый infra-контейнер), для чего загружается специальный образ `podman-pause`. Этот контейнер нужен для резервирования места для пода в пространстве имен. Это позволяет в дальнейшем подключать к поду другие (функциональные) контейнеры, а также останавливать все контейнеры пода, оставляя сам под запущенным.

В дальнейшем поды идентифицируются именами или идентификаторами — полным идентификатором, или кратким (первые символы полного идентификатора).

10.2.6.2. Список существующих подов

Для вывода списка подов следует использовать команду:

```
podman pod ps
```

Пример вывода команды:

```
POD ID        NAME       STATUS    CREATED         INFRA ID      # OF CONTAINERS
312fb1c5553f testpod   Created   22 minutes ago 76972a488dbb  1
```

Команда выводит краткий идентификатор пода (`POD ID`), имя пода (`NAME`), количество контейнеров (`# OF CONTAINERS`), а также идентификатор infra-контейнера (`INFRA ID`). Для отображения полных идентификаторов следует использовать параметр `--no-trunc`. Статус пода (`STATUS`) может иметь следующие значения:

- `Created` — в поде нет исполняющихся или остановленных контейнеров;
- `Running` — хотя бы один контейнер исполняется;
- `Stopped` — исполняющихся контейнеров нет, есть хотя бы один остановленный;
- `Exited` — все контейнеры остановлены.
- `Dead` — ошибка получения статуса.

Получить имена контейнеров в подах можно следующей командой:

```
podman pod ps --ctr-names
```

Пример вывода команды:

```
POD ID        NAME        STATUS      CREATED
312fb1c5553f  testpod     Created     56 minutes ago

INFRA ID      NAMES
76972a488dbb  friendly_rhodes,312fb1c5553f-infra,brave_turing
```

Имена контейнеров в поде перечислены в столбце `NAMES` через запятую.

10.2.6.3. Добавление контейнера в под

Для добавления контейнеров в под используются команды создания и запуска контейнеров с параметром `--pod=<идентификатор_пода>`.

Примеры:

1. Создание контейнера `nginx` и добавление его в под `testpod`:

```
podman create --pod=testpod nginx
```

2. Запуск одного контейнера в поде без запуска остальных:

```
podman run -it --pod=testpod mongodb
```

10.3. Сканирование образов контейнеров на уязвимости

Программное обеспечение Docker и Podman обеспечивает сканирование образов контейнеров на уязвимости. Сканирование может выполняться:

- при создании образов;
- при запуске контейнеров на основе образов;
- периодически с заданным периодом выполнения.

Система сканирования представлена пакетами `openscap-scanner` и `oval-db`, устанавливаемыми автоматически при установке Docker или Podman. При необходимости пакеты могут быть установлены отдельно.

Информация об уязвимостях, подверженных им объектах и методах выявления уязвимостей содержится в файлах oval-описаний в формате XML. Актуальные версии описаний устанавливаются автоматически вместе с пакетом `oval-db` и могут автоматически обновляться (см. 10.3.2.2).

Oval-описания содержатся в отдельных файлах для каждого уровня угрозы (критический, высокий, средний, низкий, отсутствует) и группируются по имени и версии операционной системы образа в каталогах `/usr/share/oval/db/<имя>/<версия>`.

Имя и идентификатор версии (код релиза ОС) операционной системы образа содержатся внутри образа в файле `/etc/os-release` в значениях параметров `ID` и `VERSION_ID` соответственно.

Пример

```
PRETTY_NAME="Astra Linux"
```

```
NAME="Astra Linux"
ID=astra
ID_LIKE=debian
ANSI_COLOR="1;31"
HOME_URL="https://astralinux.ru"
SUPPORT_URL="https://astralinux.ru/support"
LOGO=astra
VERSION_ID=1.8_x86-64
VERSION_CODENAME=1.8_x86-64
VARIANT_ID=se
```

10.3.1. Базовое использование

После установки пакетов система сканирования уязвимостей готова к работе со следующими настройками по умолчанию:

1) включено сканирование при создании образов;
2) включено сканирование при запуске контейнеров на основе образов;
3) включено периодическое сканирование образов с периодом 168 часов (7 суток);
4) для Docker дополнительно включено применение swarm-правил: проверка пользователя, работающего с Docker, на членство в группах в соответствии с ролями (см. 10.1.4).

Сканирование контейнеров при запуске выполняется в следующих случаях:

- образ контейнера ранее не сканировался;
- образ контейнера был изменен;
- с момента предыдущего сканирования прошло более 48 часов.

10.3.2. Инструмент oval-db

Для работы с oval-описаниями и изменения параметров сканирования используется инструмент командной строки `oval-db`.

Синтаксис команды:

```
sudo oval-db <действие> [параметры]
```

Действия инструмента приведены в таблице 52.

Таблица 52

Действие	Описание
`auto-update`	Включить или отключить автоматическое обновление oval-описаний
`config`	Запустить графический конфигуратор `oval-db`
`history`	Вывести историю сканирований на уязвимости
`list`	Вывести список загруженных файлов oval-описаний
`load`	Загрузить файл oval-описания из XML-файла
`restore`	Восстановить файл oval-описания из резервной копии
`remove`	Удалить загруженный файл oval-описания
`status`	Вывести состояние службы `oval-dbd`
`update`	Принудительно обновить oval-описания
`vul-info`	Вывести информацию о конкретной уязвимости
`help [действие]`	Вывести справку по указанному действию. Если действие не указано, то вывести общую справку по инструменту

10.3.2.1. Действия с файлами oval-описаний

Для вывода списка загруженных файлов oval-описаний используется действие `list`.

Синтаксис команды:

```
sudo oval-db list [параметры]
```

Параметры команды приведены в таблице 53.

Таблица 53

Параметр	Описание
`-b, --backup-include`	Включить в список каталоги с резервными копиями предыдущих версий файлов oval-описаний
`-c, --check`	Включить в список результаты проверки контрольных сумм загруженных файлов oval-описаний
`-h, --help`	Вывести справку и выйти

Пример

```
sudo oval-db list-b
```

Вывод команды:

```
astra:1.7_x86-64; Critical: 239, High: 312, Low: 2221, Medium: 16574
```

```
astra:1.7_x86-64 (Backup); High: 306, Low: 128, Medium: 2393, None: 548
astra:1.8_x86-64; Critical: 4, High: 206, Low: 8, Medium: 97, None: 7
astra:1.8_x86-64 (Backup); Critical: 11, High: 206, Low: 8, Medium: 97
ubuntu:24.04; Medium: 16574, Critical: 239, High: 312, Low: 2221
```

Для ручного добавления файлов oval-описаний используется действие `load`.

Синтаксис команды:

```
sudo oval-db load [параметры]
```

Параметры команды приведены в таблице 54.

Таблица 54

Параметр	Описание
`-f, --filepath <путь>`	Путь к загружаемому файлу oval-описания. Обязательный параметр
`-o, --os <имя>`	Имя операционной системы, для которой загружается oval-описание. Обязательный параметр
`-v, --version <идентификатор>`	Идентификатор версии операционной системы (код релиза ОС), для которой загружается oval-описание. Обязательный параметр
`-h, --help`	Вывести справку и выйти

Пример

```
sudo oval-db load -f /tmp/oval.xml -o astra -v 1.7_x86-64
```

При добавлении новой версии ранее добавленных файлов старые файлы перемещаются в подкаталог `backup`.

Для восстановления старой версии файлов из резервной копии в подкаталоге `backup` используется действие `restore`.

Синтаксис команды:

```
sudo oval-db restore [параметры]
```

Параметры команды приведены в таблице 55.

Таблица 55

Параметр	Описание
-o, --os <имя>	Имя операционной системы, для которой восстанавливается oval-описание. Обязательный параметр
-v, --version <идентификатор>	Идентификатор версии операционной системы (код релиза ОС), для которой восстанавливается oval-описание. Обязательный параметр
-h, --help	Вывести справку и выйти

Для удаления добавленных oval-описаний используется действие `remove`.

Синтаксис команды:

```
sudo oval-db remove [параметры]
```

Параметры команды приведены в таблице 56.

Таблица 56

Параметр	Описание
-o, --os <имя>	Имя операционной системы, для которой удаляется oval-описание. Обязательный параметр
-v, --version <идентификатор>	Идентификатор версии операционной системы (код релиза ОС), для которой удаляется oval-описание. Обязательный параметр
-h, --help	Вывести справку и выйти

10.3.2.2. Обновление oval-описаний

Инструмент `oval-db` поддерживает автоматическое и ручное обновление oval-описаний для образов на основе ОС. Oval-описания для других операционных систем обновляются путем ручного добавления новых версий файлов (см. 10.3.2.1).

Автоматическое обновление oval-описаний по умолчанию отключено. Для управления автоматическим обновлением используется действие `auto-update`.

Синтаксис команды:

```
sudo oval-db auto-update [параметры]
```

Параметры команды приведены в таблице 57.

Таблица 57

Параметр	Описание
`-e, --enable`	Включить автоматическое обновление oval-описаний
`-e=false`	Отключить автоматическое обновление oval-описаний
`-h, --help`	Вывести справку и выйти

Для ручного обновления oval-описаний используется действие `update`.

Синтаксис команды:

```
sudo oval-db update [параметры]
```

Параметры команды приведены в таблице 58.

Таблица 58

Параметр	Описание
`-v, --version <код_релиза_ОС>`	Очередное обновление ОС, для которого будут обновлены oval-описания. Обязательный параметр. Чтобы обновить oval-описания для всех очередных обновлений ОС, следует указать значение `all`
`-h, --help`	Вывести справку и выйти

10.3.2.3. Вывод описаний уязвимостей

Инструмент `oval-db` позволяет выводить справочную информацию по конкретным уязвимостям с помощью действия `vul-info`.

Синтаксис команды:

```
sudo oval-db vul-info [параметры]
```

Параметры команды приведены в таблице 59.

Таблица 59

Параметр	Описание
`-i <идентификатор>`	Идентификатор уязвимости. Обязательный параметр
`-o, --os <имя>`	Имя операционной системы, к которой относится уязвимость. Обязательный параметр
`-v, --version <идентификатор>`	Идентификатор версии операционной системы (код релиза ОС), к которой относится уязвимость. Обязательный параметр

Окончание таблицы 59

Параметр	Описание
`-x, --xml`	Вывести информацию в XML-формате
`-h, --help`	Вывести справку и выйти

Пример

Вывести описание уязвимости в ОС очередного обновления 1.8:

```
sudo oval-db vul-info -i \
     oval:astra:def:101849418303406667215420926023021 1 \
     -o astra -v 1.8_x86-64
```

10.3.2.4. Графический конфигуратор системы сканирования уязвимостей

Графический конфигуратор позволяет настроить параметры сканирования и обнаружения уязвимостей для систем контейнеризации Docker и Podman.

Для запуска графического конфигуратора выполнить команду:

```
sudo oval-db config
```

Навигация в графическом интерфейсе производится с помощью мыши или клавиатуры. Используемые клавиши и их действия приведены в таблице 60.

Таблица 60

Клавиша	Описание
<←> или **<→>**	Переход между вкладками
<Enter>	Подтверждение действия
<Tab>	Переход к следующему параметру
<↑>	Переход к выбору шаблона настроек
<Q>	Выход без сохранения изменений

Интерфейс графического конфигуратора приведен на рис. 10.

Рис. 10

В графическом конфигураторе возможно выбрать один из предустановленных шаблонов настроек. Доступны шаблоны шести уровней безопасности, шаблон отключения всех функций сканирования и поиска уязвимостей, а также пользовательский шаблон. Пользовательский шаблон выбирается автоматически при изменении любых параметров.

Шаблоны настроек и их состав приведены в таблице 61.

Таблица 61

Имя шаблона	Сканирование на уязвимости при создании образа	Сканирование на уязвимости при запуске контейнера	Периодическое сканирование на уязвимости	Использование swarm-правил	Запуск контейнеров без oval-описаний	Сканирование контейнера на уязвимости / Запрет запуска при обнаружении уязвимостей				
						Уровень критичности				
						нет	низкий	средний	высокий	критический
Level 1	Да	Да	Да 7 дней	Да	Нет	Да / Да	Да / Да	Да / Да	Да / Да	Да / Да

Окончание таблицы 61

Имя шаблона	Сканирование на уязвимости при создании образа	Сканирование на уязвимости при запуске контейнера	Периодическое сканирование на уязвимости	Использование swarm-правил	Запуск контейнеров без oval-описаний	Сканирование контейнера на уязвимости / Запрет запуска при обнаружении уязвимостей				
						Уровень критичности				
						нет	низкий	средний	высокий	критический
Level 2	Да	Да	Да 7 дней	Да	Да	Да / Да	Да / Да	Да / Да	Да / Да	Да / Да
Level 3	Да	Да	Да 7 дней	Да	Да	Да / Нет	Да / Нет	Да / Да	Да / Да	Да / Да
Level 4	Да	Да	Да 7 дней	Да	Да	Нет / Нет	Да / Нет	Да / Нет	Да / Да	Да / Да
Level 5	Да	Да	Да 7 дней	Да	Да	Нет / Нет	Нет / Нет	Да / Нет	Да / Да	Да / Да
Level 6	Да	Да	Да 14 дней	Да	Да	Нет / Нет	Нет / Нет	Нет / Нет	Да / Нет	Да / Нет
None	Нет	Нет	Нет	Нет	Да	Нет / Нет	Нет / Нет	Нет / Нет	Нет / Нет	Нет / Нет

10.3.3. Конфигурационные файлы системы сканирования уязвимостей

Настройки системы сканирования уязвимостей хранятся в формате JSON в следующих конфигурационных файлах:

- `/etc/podman.json` — параметры сканирования для системы контейнеризации Podman;
- `/etc/docker/daemon.json` — параметры сканирования для системы контейнеризации Docker;
- `/usr/share/oval/conf/podman.json` — параметры поиска уязвимостей при использовании Podman;
- `/usr/share/oval/conf/docker.json` — параметры поиска уязвимостей при использовании Docker;
- `/usr/share/oval/conf/daemon.json` — параметры службы `oval-dbd`.

При отсутствии какого-либо файла применяются настройки по умолчанию.

Параметры сканирования образов и контейнеров содержатся в конфигурационных файлах Docker и Podman — `/etc/docker/daemon.json` и `/etc/podman.json` соответственно. Для обоих систем контейнеризации используются одинаковые параметры, за исключением параметра `swarm-rules-enabled`. После установки системы сканирования уязвимостей в

файлы добавляются следующие настройки по умолчанию. Комментарии в файле начинаются с символа «#».

```
{
   # Включение или отключение сканирования при создании образов
   "scan-on-image-create": true,

   # Включение или отключение сканирования при запуске контейнеров из образов
   "scan-on-container-start": true,

   # Включение или отключение swarm-правил (только для /etc/docker/daemon.json)
   "swarm-rules-enabled": true,

   # Период сканирования образов в часах
   "periodic-scan-time-in-hours": 168
}
```

Параметры поиска уязвимостей при использовании Docker и Podman содержатся в конфигурационных файлах `oval-db — /usr/share/oval/conf/docker.json` и `/usr/share/oval/conf/podman.json` соответственно. Для обоих систем контейнеризации используются одинаковые параметры. После установки системы сканирования уязвимостей файлы имеют следующее содержимое, соответствующее настройкам по умолчанию. Комментарии в файле начинаются с символа «#».

```
{

   # система контейнеризации (docker или podman)
   "engine": "docker",

   # управление запуском контейнеров без oval-описаний (true - разрешено, false - \
      запрещено)
   "allow-run-wo-oval-file": true,

   # параметры для различных уровней критичности уязвимостей
   "levels": {
      "critical": {

         # обнаружение уязвимостей данного уровня критичности (true - включено, \
            false - отключено)
         "enabled": true,

         # запрет запуска контейнеров с обнаруженными уязвимостями (true - запуск \
            запрещен, false - запуск разрешен)
         "drop": true
      },
      "high": {
         "enabled": true,
         "drop": true
```

```
      },
      "medium": {
         "enabled": true,
         "drop": true
      },
      "low": {
         "enabled": true,
         "drop": true
      },
      "none": {
         "enabled": true,
         "drop": true
      }
   }
}
```

Параметры службы `oval-dbd` содержатся в файле `/usr/share/oval/conf/daemon.json`. После установки системы сканирования уязвимостей файл имеет следующее содержимое, соответствующее настройкам по умолчанию. Комментарии в файле начинаются с символа «#».

```
{
  # Параметры базы данных уязвимостей
  "Database": {

    # Путь к базе данных с результатами сканирования
    "Path": "/usr/share/oval/history/scan_results.db",

    # Срок устаревания результатов сканирования (в часах)
    "ExpireTime": 48
  },

  # Параметры автоматического обновления oval-описаний для образов на основе Astra \
     Linux
  "Update": {

    # Автоматическая проверка наличия обновлений oval-описаний
    "Auto": true,

    # URL сервера, с которого будет выполняться обновление
    "ManifestUrl": "https://dl.astralinux.ru/artifactory/al-oval/oval_meta.json",

    # Временный каталог для размещения загружаемых файлов
    "TmpDir": "/tmp/oval_temp/",

    # Интервал проверки обновлений oval-описаний (в часах)
    "Interval": 24,

    # URL каталога с файлами oval-описаний на сервере
```

```
   "FoldersForVersionsUrl": "https://dl.astralinux.ru/astra/oval/"
  }
}
```

10.3.4. Обновление oval-описаний в закрытом контуре

10.3.4.1. Настройка сервера обновления oval-описаний

При необходимости возможно создать локальный сервер для обновления oval-описаний уязвимостей ОС с доступом по протоколам HTTP/HTTPS или FTP. На сервере должен присутствовать каталог с oval-описаниями, все элементы которого должны быть доступны для загрузки.

Пример

Вариант структуры каталога с oval-описаниями на сервере.

```
oval/
| 1.7_x86-64/
|    |--- oval-definitions-alse-1.7.xml
|    |--- oval-definitions-alse-1.7.xml.md5
|    |--- oval-definitions-alse-1.7.xml.sha1
|    |--- oval-definitions-alse-1.7.xml.sha256
| 1.8_x86-64/
|    |---...
| 4.7_arm/
|    |---...
|--- oval_meta.json
|--- oval_meta.json.md5
|--- oval_meta.json.sha1
|--- oval_meta.json.sha256
...
```

Oval-описания хранятся в файлах формата XML и размещаются для удобства в отдельных каталогах для каждого очередного обновления и архитектуры ОС. Файлы форматов MD5, SHA1 и SHA256 размещаются в тех же каталогах и содержат контрольные суммы одноименных файлов. Файл `oval_meta.json` содержит ссылки на все доступные oval-описания и значения их контрольных сумм.

Пример

Файл `oval_meta.json`. Комментарии в файле начинаются с символа «#».

```
{
# Массив процессорных архитектур ОС
"platforms": [
   {
      # Процессорная ахитектура ОС
      "platform": "x86-64",

      # Массив очередных обновлений ОС в рамках процессорной архитектуры
      "targets": [

         {
            # Очередное обновление ОС (обязательный элемент)
            "target": "1.8_x86-64",

            # URL файла oval-описания (обязательный элемент)
            "url": "http://server.astra.dom/oval/1.8_x86-64/oval-definitions-\
               alse-1.8.xml",

            # Контрольная сумма файла oval-описания по MD5 (обязательный \
               элемент)
            "md5": "ccf88d2c64764db8fdd3ded3f5cfd54f",

            # Контрольные суммы файла oval-описания по SHA256 и ГОСТ
            "sha256sum": "58\
               f8075bbf40fb822de9a2cacc91067c8055ed8e05449f58997e3c50cf93371b\
               ",
            "gost": "\
               ad35297e12241c12574d6abc9edae6004bd7e9eb97a8daba2b93fdd2ed76bc27\
               ",

            # Дата добавления файла oval-описания на сервер
            "uploaded": "21-05-2025 14:54:10.513"
         },
         {
            "target": "1.7_x86-64",
            "url": "http://server.astra.dom/oval/1.7_x86-64/oval-definitions-\
               alse-1.7.xml",
            "md5": "b1d7fbd7de8d4b5554d18cf4168224a0",
            "sha256sum": "783709\
               c6a0ad9b8f610c05be2e86e45e69538b0c573f3e654279ce2379640e37",
            "gost": "\
               af9f17dfcffa95b5a3ac85f9da834dde07ef8434b7a6d9ac59de581eab990c45\
               ",
            "uploaded": "19-05-2025 14:38:41.976"
         }
      ]
   }
   {
      "platform": "arm",
      "targets": [
```

```
            {
               "target": "4.7_arm",
               "url": "https://dl.astralinux.ru/astra/oval/4.7_arm/oval-\
                  definitions-alse-4.7.xml",
               "md5": "1534df4ecb76014aec8da1d090948e3b",
               "sha256sum": "\
                  bed2619a835e6afc31171f29c1a0b659d7124604fa03e8cc5a9c3dadd3c474f5\
                  ",
               "gost": "7\
                  ee2703817bfbf13ff242b5bb55daccf554dfc7c30a0bc4cdc20854e70bd6423\
                  ",
               "uploaded": "02-06-2025 16:28:37.169"
            }
         ]
      }
]
}
```


Обновление файлов oval-описаний на сервере в закрытом контуре выполняется вручную:

1) получить актуальные версии oval-описаний на компьютере с установленным пакетом `oval-db` и доступом в Интернет:

а) для получения актуальных версий всех oval-описаний для ОС выполнить команду:

```
sudo oval-db update -v all
```

б) для получения актуальных версий oval-описаний для определенного очередного обновления ОС выполнить команду:

```
sudo oval-db update -v <кодовое_имя_ОС>
```

где кодовое имя ОС — это значение параметра `VERSION_ID` в файле `/etc/os-release`;

Пример

```
sudo oval-db update -v 1.8_x86-64
```

2) после завершения обновления перенести содержимое каталога `/usr/share/oval/db/astra/` в такой же каталог на сервере обновления и убедиться, что права доступа к файлам и подкаталогам такие же, как на исходном компьютере.

10.3.4.2. Настройка клиента для обновления oval-описаний

Настройки обновления oval-описаний на клиентском компьютере содержатся в файле `/usr/share/oval/conf/daemon.json` (см. 10.3.3). Данный файл по умолчанию отсут-

ствует и создается при включении автоматического обновления oval-описаний (см. 10.3.2.2). Для указания сервера обновлений следует изменить значения следующих параметров:

1) `ManifestUrl` — указать URL или путь к файлу `oval_meta.json` на сервере обновлений;

2) `FoldersForVersionsUrl` — указать URL каталога с oval-описаниями на сервере обновлений.

Пример

Файл `/usr/share/oval/conf/daemon.json`.

```
{
  "Database": {
    "Path": "/usr/share/oval/history/scan_results.db",
    "ExpireTime": 48
  },
  "Update": {
    "Auto": true,
    "ManifestUrl": "http://server.astra.dom/oval/oval_meta.json",
    "TmpDir": "/tmp/oval_temp/",
    "Interval": 24,
    "FoldersForVersionsUrl": "http://server.astra.dom/oval/"
  }
}
```

11. ЗАЩИЩЕННЫЙ КОМПЛЕКС ПРОГРАММ ГИПЕРТЕКСТОВОЙ ОБРАБОТКИ ДАННЫХ

Защищенный комплекс программ гипертекстовой обработки данных — это ПО, обеспечивающее взаимодействие по HTTP-протоколу между сервером и веб-браузерами: прием запросов, поиск указанных файлов и передача их содержимого, выполнение приложений на сервере и передача клиенту результатов их выполнения. В комплексе программ гипертекстовой обработки данных в качестве веб-севера используется ПО Apache2. Для доступа к веб-серверу используются браузеры, например Firefox, Chromium.

ВНИМАНИЕ! Для обеспечения корректной работы пользователя с сетевыми службами должна быть явно задана его классификационная метка (диапазон уровней конфиденциальности и категорий конфиденциальности) с помощью соответствующих утилит, даже если ему не доступны уровни и категории выше 0. Дополнительная информация приведена в документе РУСБ.10015-01 97 01-1.

11.1. Установка и настройка веб-сервера Apache2

Для развертывания веб-сервера Apache2 требуется установить пакет `apache2` на компьютер, который будет использовать в качестве веб-сервера. Установка выполняется командой:

```
sudo apt install apache2
```

После установки веб-сервер Apache2 будет готов к приему запросов на всех сетевых интерфейсах на 80 порту.

Если по каким-то причинам он не работоспособен, следует проверить минимально необходимые настройки сервера:

1) в файле `/etc/apache2/ports.conf` должен быть указан параметр:

```
Listen 80
```

2) в каталоге `/etc/apache2/sites-available` должны находиться файлы с настройками виртуальных хостов и как минимум один из них должен быть разрешен к использованию командой:

```
sudo a2ensite <имя_файла>
```

ВНИМАНИЕ! В команде необходимо использовать только имя файла (без указания полного пути).
Для разрешенного к использованию виртуального хоста будет добавлена в каталог `/etc/apache2/sites-enabled` символьная ссылка на его конфигурационный файл.

Пример

Конфигурация виртуального хоста с минимальным набором параметров:

```
<VirtualHost *:80>
        ServerAdmin webmaster@localhost
        ServerName server.domain.name
        DocumentRoot /var/www/html
        <Directory /var/www/html>
                Options Indexes FollowSymLinks MultiViews
                AllowOverride None
        </Directory>
        ErrorLog /var/log/apache2/error.log
        LogLevel warn
        CustomLog /var/log/apache2/access.log combined
</VirtualHost>
```

Дополнительные настройки веб-сервера для предоставления пользователям доступа к страницам и другому содержимому веб-сайтов с ненулевыми классификационными метками приведены в 11.6.

После окончания правки конфигурационных файлов необходимо перезапустить сервер командой:

```
sudo systemctl restart apache2
```

11.2. Режим работы AstraMode

Сервер гипертекстовой обработки данных Apache2, входящий в состав ОС, поддерживает работу с ненулевыми классификационными метками при включенном мандатном управлении доступом (см. РУСБ.10015-01 97 01-1). Для обеспечения работы средств разграничения доступа должна выполняться аутентификация и авторизация пользователей.

Для управления авторизацией пользователей в сервере Apache2 используется параметр `AstraMode`, который указывается в конфигурационном файле `/etc/apache2/apache2.conf`:

- для включения обязательной авторизации задать для параметра значение `on`:

  ```
  AstraMode on
  ```

  При этом отсутствие в конфигурационном файле параметра `AstraMode` (или закомментированная строка с параметром) соответствует значению `AstraMode on`;

- для отключения обязательной авторизации задать для параметра значение `off`:

```
AstraMode off
```

По умолчанию режим обязательной авторизации включен.

Отключение обязательной авторизации снижает защищенность ресурсов, но может быть необходимо для обеспечения совместимости с программами, не поддерживающими работу с классифицированными метками и не использующими авторизацию.

ВНИМАНИЕ! Для доступа к данным, имеющим ненулевые классификационные метки, должна выполняться авторизация пользователей. Анонимный доступ к данным, имеющим ненулевую классификационную метку, недопустим.

ВНИМАНИЕ! При выключенной авторизации сервер Apache2 осуществляет все запросы к своим ресурсам от имени одной системной учетной записи (по умолчанию `www-data`), которая в случае применения мандатного контроля целостности имеет категорию целостности `1`.

В конфигурационном файле `/etc/apache2/apache2.conf` задается глобальное значение параметра `AstraMode`, которое по умолчанию применяется для всех добавляемых файлов конфигурации и для всех активных веб-сайтов, запускаемых службой.

Глобальное значение параметра `AstraMode` может быть переопределено для добавляемого конфигурационного файла, при этом необходимость авторизации будет учитываться на основе последнего обнаруженного значения. Переопределение значения `AstraMode` для файла, добавляемого в конфигурацию с помощью `IncludeOption` и `Include`, выполняется путем добавления строки со значением параметра `AstraMode` в начале добавляемого файла или перед инструкцией добавления файла.

Пример

```
AstraMode off
IncludeOption conf-new/*.conf
```

Использовать множественные определения параметра не рекомендуется, так как неверное определение или изменение порядка их обработки может вызвать ошибки.

Глобальное значение параметра `AstraMode` может быть переопределено для конкретного виртуального веб-сайта путем указания нового значения в списке параметров для данного веб-сайта.

Пример

```
<VirtualHost *:443>
```

```
AstraMode off
...
</VirtualHost>
```

11.3. Настройка аутентификации через PAM

Для ресурсов веб-сервера должна использоваться аутентификация и авторизация через PAM, если не настроена сквозная аутентификация и авторизация через Kerberos для сервера и клиента, работающих в ЕПП (см. 11.4). При PAM-аутентификации используется пользовательская БД, прописанная в настройках ОС.

Для настройки аутентификации и авторизации через PAM установить пакет `libapache2-mod-authnz-pam` и выполнить следующую команду:

```
sudo a2enmod authnz_pam
```

В конфигурационных файлах виртуальных хостов веб-сервера Apache2 задать базовую аутентификацию с использованием PAM-модуля и разрешить доступ только тем пользователям, которые успешно прошли аутентификацию:

```
AuthType Basic
AuthName "PAM authentication"
AuthBasicProvider PAM
AuthPAMService apache2
Require valid-user
```

Логин и пароль пользователя будут передаваться от пользователя к серверу в открытом виде с использованием метода аутентификации Basic. Для корректного функционирования авторизации через PAM пользователю, от которого работает веб-сервер (по умолчанию `www-data`), необходимо выдать права на чтение информации из БД пользователей и сведений о метках безопасности:

```
sudo usermod -a -G shadow www-data
sudo setfacl -d -m u:www-data:r /etc/parsec/macdb
sudo setfacl -R -m u:www-data:r /etc/parsec/macdb
sudo setfacl -m u:www-data:rx /etc/parsec/macdb
```

Если установлен модуль веб-сервера Apache2 `auth-gssapi` из пакета `libapache2-mod-auth-gssapi` для аутентификации через Kerberos в соответствии с 11.4, то выключить его использование при помощи команды:

```
sudo a2dismod auth_gssapi
```

Для передачи в http-заголовке текущего иерархического уровня конфиденциальности и текущих неиерархических категорий конфиденциальности пользователя может быть сконфигурирован модуль Apache2 `mod_headers`. Для этого необходимо:

1) в конфигурационном файле `/etc/apache2/apache2.conf` добавить строку:

```
Header set MyHeader "%m %c"
```

где `%m` — место подстановки текущего иерархического уровня конфиденциальности;
`%c` — текущих неиерархических категорий конфиденциальности;

2) включить модуль, выполнив команду:

```
sudo a2enmod headers
```

3) перезапустить сервер Apache2:

```
sudo systemctl restart apache2
```

Сервер для PAM-аутентификации использует сценарий PAM, содержащийся в конфигурационном файле `/etc/pam.d/apache2`. PAM-сценарий включает `common-auth` и `common-account`. По умолчанию в ОС для фиксации числа неверных попыток входа пользователей применяется PAM-модуль `pam_faillock.so`. Использование `pam_faillock.so` в секции `auth` в файле `/etc/pam.d/common-auth` обеспечивает увеличение счетчика неверных попыток входа пользователя при начале процесса аутентификации. Для корректной работы данного механизма необходимо разрешить пользователю `www-data` запись в `/var/log/faillog`, выполнив команду:

```
sudo setfacl -m u:www-data:rw /var/log/faillog
```

Выполнить перезапуск сервера:

```
sudo systemctl restart apache2
```

11.4. Настройка веб-сервера Apache2 для работы в домене FreeIPA

При работе в составе домена FreeIPA веб-сервер Apache2 может использоваться для аутентификации пользователей с использованием Kerberos, в том числе для сквозной аутентификации в приложениях.

Для обеспечения работы веб-сервера Apache2 в составе домена FreeIPA требуется:

1) развернутый домен FreeIPA, например `astra.dom` (см. 8.2.3, 8.2.4 и 8.2.5);

2) отдельный компьютер для размещения веб-сервера Apache2, удовлетворяющий следующим требованиям:

а) компьютер с веб-сервером должен быть введен в домен FreeIPA в соответствии с 8.2.8;

б) разрешение имен должно быть настроено таким образом, чтобы имя компьютера с веб-сервером разрешалось как полное доменное имя (FQDN), например `web.astra.dom`;

в) компьютеру с веб-сервером должен быть назначен статический IP-адрес.

В качестве дополнительной меры безопасности возможно настроить использование защищенных SSL-соединений между веб-сервером и его клиентами (см. 11.5).

Для настройки аутентификации Kerberos требуется дополнительно установить на веб-сервере модуль аутентификации `auth-gssapi`. Установка выполняется командой:

```
sudo apt install libapache2-mod-auth-gssapi
```

Активация модуля происходит автоматически при установке.

Если в ОС установлен в соответствии с 11.3 модуль веб-сервера Apache2 `authnz_pam` для аутентификации через PAM, то его следует отключить при помощи команды:

```
sudo a2dismod authnz_pam
```

Если модуль `auth_gssapi` был ранее отключен, то для его активации выполнить команду:

```
sudo a2enmod auth_gssapi
```

ВНИМАНИЕ! При установке на компьютер веб-сервера Apache2 по умолчанию включается режим `AstraMode` для работы с ненулевыми классификационными метками (см. 11.2). Для работы аутентификации Kerberos в данном режиме следует в конфигурационном файле `/etc/apache2/apache2.conf` добавить (раскомментировать) параметр `IncludeRealm` со значением `on`.

ВНИМАНИЕ! При включенном режиме `AstraMode` доменным пользователям, проходящим аутентификацию, должны быть явно заданы классификационные метки (диапазоны уровней конфиденциальности и категорий конфиденциальности) с помощью соответствующих утилит, даже если этим пользователям недоступны уровни и категории выше 0. Дополнительная информация приведена в документе РУСБ.10015-01 97 01-1.

Развернутый веб-сервер необходимо зарегистрировать в качестве доменной службы одним из следующих способов:

1) в веб-интерфейсе администратора FreeIPA (см. 8.2.15.3);

2) с помощью инструмента командной строки `ipa`. Для этого необходимо на контроллере домена или компьютере веб-сервера выполнить следующее:

а) получить билет Kerberos администратора домена:

```
kinit admin
```

б) зарегистрировать доменную службу:

```
ipa service-add HTTP/<полное_доменное_имя_хоста_веб-сервера>
```

Пример

```
ipa service-add HTTP/web.astra.dom
```

Для аутентификации пользователей на веб-сервере необходимо загрузить с контроллера домена на компьютер веб-сервера таблицу ключей для зарегистрированной службы, выполнив на компьютере веб-сервера следующее:

1) получить билет Kerberos администратора домена для пользователя `root` (необходимо для последующего использования билета с механизмом `sudo`):

```
sudo kinit admin
```

2) получить с контроллера домена таблицу ключей Kerberos и сохранить ее в файл:

```
sudo ipa-getkeytab -p HTTP/<полное_доменное_имя_хоста_веб-сервера> -k \
     <путь_к_сохраняемому_файлу_таблицы>
```

Пример

```
sudo ipa-getkeytab -p HTTP/web.astra.dom -k /etc/apache2/keytab
```

Примечание. Получить таблицу ключей с помощью `ipa-getkeytab` можно на контроллере домена. В этом случае полученную таблицу необходимо скопировать на компьютер веб-сервера;

3) изменить владельца полученной таблицы ключей на служебную учетную запись `www-data` и установить права доступа:

```
sudo chown www-data <путь_к_таблице_ключей>
sudo chmod 600 <путь_к_таблице_ключей>
```

На компьютере веб-сервера создать конфигурационный файл с параметрами аутентификации Kerberos, например /etc/apache2/conf-available/kerberos-auth.conf, в котором указать путь к сохраненной таблице ключей. Файл должен содержать следующие строки:

```
<Directory /var/www>
# тип аутентификации
AuthType GSSAPI
# Подсказка с информацией о ресурсе (выводится при запросе пароля)
AuthName "Astra Kerberos protected area"
GssapiCredStore keytab:<путь_к_таблице_ключей>
# Включить 3 нижних параметра, если нужно кешировать сессии
#GssapiUseSessions On
#Session On
#SessionCookieName myapp_web_gssapi_session path=/my_url;httponly;secure;
Require valid-user
</Directory>
```

Созданный конфигурационный файл необходимо указать с помощью директивы Include в конфигурационных файлах веб-сайтов, размещаемых в каталоге /etc/apache2/sites-available/. Путь к файлу аутентификации указывается относительно каталога /etc/apache2/.

Пример

```
Include conf-available/kerberos-auth.conf
```

Чтобы использовать аутентификацию на веб-сайте, созданном по умолчанию при установке Apache2 (http://<полное_доменное_имя_хоста_веб-сервера>/), следует указать файл аутентификации в его конфигурационном файле /etc/apache2/sites-available/000-default.conf.

Для создания веб-сайта, например http://web.astra.dom/authorized/, требующего аутентификацию Kerberos, необходимо выполнить следующее:

1) создать конфигурационный файл веб-сайта /etc/apache2/sites-available/authorized.conf и указать в нем ранее созданный файл аутентификации /etc/apache2/conf-available/kerberos-auth.conf:

```
<VirtualHost *:80>
ServerAdmin webmaster@localhost
DocumentRoot /var/www/html
ErrorLog ${APACHE_LOG_DIR}/error.log
```

```
CustomLog ${APACHE_LOG_DIR}/access.log combined
Include conf-available/kerberos-auth.conf
</VirtualHost>
```

2) активировать созданный конфигурационный файл веб-сайта:

```
sudo a2ensite authorized
```

3) создать каталог `/var/www/html/authorized` для файлов веб-сайта;

4) создать файл `/var/www/html/authorized/index.html` с заглавной страницей.

Пример

```
<html>
<body>
<div style="width: 100%; font-size: 40px; font-weight: bold; text-\
   align: center;">
Тестовая страница для проверки аутентификации Kerberos.
Если вы видите этот текст, то аутентификация выполнена успешно.
</div>
</body>
</html>
```

5) для корректного отображения кириллицы в тексте страниц веб-сайта добавить в конфигурационный файл `/etc/apache2/apache2.conf` строку:

```
AddDefaultCharset UTF-8
```

6) обновить конфигурацию веб-сервера:

```
sudo systemctl reload apache2
```

Для аутентификации на веб-сервере необходимо на компьютере, с которого осуществляется доступ к веб-серверу, получить билет Kerberos:

1) если используемый компьютер входит в домен:

   а) при работе от имени доменного пользователя билет выдается автоматически при входе в сессию. Для просмотра выданных билетов выполнить команду:

   ```
   klist
   ```

   б) при работе от имени локального пользователя получить билет Kerberos на имя доменного пользователя:

   ```
   kinit <имя_пользователя_домена>
   ```

2) если используемый компьютер не входит в домен:

а) установить клиент Kerberos:

```
sudo apt install krb5-user
```

б) указать в качестве DNS-сервера адрес контроллера домена FreeIPA (см. 8.2.8);

в) получить билет Kerberos на имя доменного пользователя:

```
kinit <имя_пользователя_домена>
```

Для проверки аутентификации через консоль следует загрузить заглавную страницу веб-сайта:

```
curl --negotiate -u : http://<полное_доменное_имя_хоста_веб-сервера>/authorized/
```

В случае успешной аутентификации доменного пользователя по билету Kerberos будет получен доступ к заглавной странице сайта и команда выведет содержимое созданного файла `/var/www/html/authorized/index.html`.

Для работы аутентификации Kerberos при использовании веб-браузера данный браузер должен поддерживать метод аутентификации `negotiate`. Для включения метода `negotiate` и проверки аутентификации в веб-браузере Mozilla Firefox выполнить следующее:

1) в адресной строке веб-браузера ввести:

```
about:config
```

2) ввести в строке поиска параметр `network.negotiate-auth.trusted-uris` и нажать «Изменить»;

3) задать маски доменов, для которых будет использоваться аутентификация `negotiate`. В общем случае в качестве значения можно указать `http://`, `https://`;

4) нажать «Сохранить»;

5) ввести в адресной строке:

```
http://<полное_доменное_имя_хоста_веб-сервера>/authorized/
```

В случае успешной аутентификации пользователя по билету Kerberos будет отображена заглавная страница сайта `/var/www/html/authorized/index.html`.

Если необходимо обеспечить сквозную аутентификацию из сценариев при работе с другими службами, например с сервером СУБД, то в веб-браузере Mozilla Firefox для параметра `network.negotiate-auth.delegation-uris` следует задать маски доменов, которым

можно передавать данные для сквозной аутентификации. При этом в запускаемых сценариях следует выставить переменную окружения KRB5CCNAME.

Пример

Установка переменной для сценариев на языке PHP:

```
putenv("KRB5CCNAME=" . $_SERVER['KRB5CCNAME']);
```

11.5. Настройка защищенных соединений SSL с использованием сертификатов

При установке веб-сервера Apache2 для защищенных соединений SSL по умолчанию используется предустановленный закрытый ключ /etc/ssl/private/ssl-cert-snakeoil.key и соответствующий ему сертификат /etc/ssl/certs/ssl-cert-snakeoil.pem. Данные ключ и сертификат следует заменить на ключ и сертификат, выданные центром аутентификации согласно 8.2.14 .

Созданные центром аутентификации сертификат и ключ, например apache.crt и apache.key, следует сохранить в каталоге /etc/ipa/.

Расположение сертификатов необходимо указать в конфигурационных файлах веб-сайтов, поддерживающих соединения SSL. Например, в конфигурационном файле etc/apache2/sites-enabled/default-ssl.conf веб-сайта, устанавливаемого по умолчанию:

```
SSLCertificateFile /etc/ipa/apache.crt
SSLCertificateKeyFile /etc/ipa/apache.key
```

Для начала работы с использованием SSL необходимо:

1) загрузить модуль работы по протоколу SSL, выполнив команду:

```
sudo a2enmod ssl
```

2) включить веб-сайт, для которого настраивается работа по протоколу SSL. Например, для включения устанавливаемого по умолчанию веб-сайта default-ssl выполнить команду:

```
sudo a2ensite default-ssl
```

3) обновить конфигурацию веб-сервера, выполнив команду:

```
sudo systemctl reload apache2
```

11.6. Настройка веб-сервера Apache2 для работы с данными ограниченного доступа

Разграничение доступа к содержимому веб-сайтов на веб-сервере Apache2 осуществляется за счет мандатного управления доступом при включенном параметре `AstraMode` (см. 11.2).

Доступ пользователя к содержимому веб-сайта определяется сопоставлением классификационных меток файлов веб-сервера с классификационной меткой пользователя. Файлы с ненулевыми классификационными метками доступны только из сессии пользователя с соответствующей классификационной меткой. Если классификационная метка пользователя ниже метки файла или несравнима с ней, то файл будет недоступен и веб-сервер вернет ошибку «404».

Перед назначением классификационных меток каталогу и файлам веб-сайта необходимо назначить каталогам веб-сервера `/var/www/` и `/var/www/html/` максимальные классификационные метки, с которыми планируется работать, а также дополнительный атрибут `ccnr`:

```
sudo pdpl-file -u 3::\
     <категории_конфиденциальности>:ccnr /var/www
sudo pdpl-file -u <уровень_конфиденциальности>::
     <категории_конфиденциальности>:ccnr /var/www/html
```

Если каталогу веб-сайта назначается классификационная метка с дополнительным атрибутом `ccnr`, то файлы и подкаталоги в нем могут иметь различные классификационные метки (в том числе нулевые), но не выше метки каталога. Это позволяет создать заглавную страницу с нулевой классификационной меткой, видимую всем пользователям, и ограничить доступ к другому содержимому.

Пример

Назначить каталогу веб-сайта `/restricted` второй уровень конфиденциальности, все возможные категории конфиденциальности и атрибут `ccnr`, а файлу `secret.html` — первый уровень и категорию `Категория_1` (категория должна быть определена в системе):

```
sudo pdpl-file -u 2::-1:ccnr /var/www/html/restricted
sudo pdpl-file -u 1::Категория_1 /var/www/html/restricted/secret.html
```

Если каталогу веб-сайта назначается классификационная метка без атрибута `ccnr`, то все файлы и подкаталоги в нем могут иметь только такую же классификационную метку. Доступ ко всему содержимому веб-сайта будет возможен только из сессии пользователя с классификационной меткой не ниже назначенной.

Примечание. Если назначить классификационную метку без атрибута `ccnr` каталогу веб-сайта по умолчанию `/var/www/html/`, то на веб-сервере будет возможно создавать другие веб-сайты только с такой же классификационной меткой.

Для ограничения доступа к создаваемому новому веб-сайту с использованием единой классификационной метки для всего его содержимого необходимо создать каталог веб-сайта и назначить ему требуемую классификационную метку:

```
sudo pdpl-file -u <уровень_конфиденциальности>::\
     <категории_конфиденциальности> /var/www/html/<каталог_веб-сайта>
```

Пример

Создать каталог веб-сайта `/secret` и назначить ему третий уровень конфиденциальности:

```
sudo mkdir /var/www/html/secret
sudo pdpl-file -u 3 /var/www/html/secret
```

Если требуется ограничить доступ с использованием единой классификационной метки к веб-сайту с уже имеющимся содержимым, то необходимо:

1) назначить каталогу веб-сайта и всему его содержимому требуемую классификационную метку и атрибут `ccnr` (нужен для рекурсивного изменения меток):

```
sudo pdpl-file -R -u <уровень_конфиденциальности>::\
     <категории_конфиденциальности>:ccnr /var/www/html/<каталог_веб-сайта>
```

2) снять атрибут `ccnr` с каталогов и подкаталогов веб-сайта:

```
sudo pdpl-file -R -s <уровень_конфиденциальности>:::ccnr \
     /var/www/html/<каталог_веб-сайта>
```

Пример

Назначить веб-сайту `/secret` второй уровень конфиденциальности и категорию `Категория_2` (категория должна быть определена в системе) без атрибута `ccnr`:

```
sudo pdpl-file -R -u 2::Категория_2:ccnr /var/www/html/secret
sudo pdpl-file -R -s 2:::ccnr /var/www/html/secret
```

Для применения изменений необходимо перезапустить веб-сервер:

```
sudo systemctl restart apache2
```

Дополнительная информация по мандатному управлению доступом приведена в документе РУСБ.10015-01 97 01-1.

11.7. Установка PARSEC-привилегий на дочерние процессы

При работе веб-сервера в условиях мандатного управления доступом и при включенной сквозной аутентификации или авторизации пользователей на сервере Apache2 (см. 11.3 и 11.4) возможно настроить присвоение PARSEC-привилегий дочерним процессам веб-сервера, которые выполняют запросы пользователя. Подробное описание PARSEC-привилегий приведено в документе РУСБ.10015-01 97 01-1.

Установку PARSEC-привилегий на дочерние процессы возможно выполнить:

- глобально — путем редактирования конфигурационного файла `/etc/apache2/apache2.conf`;
- для конкретного виртуального хоста — путем редактирования конфигурационного файла данного хоста `/etc/apache2/sites-available/<имя_хоста>.conf`.

Назначаемые PARSEC-привилегии указываются в качестве значения параметра `ChildCapabilitiesParsec`:

```
ChildCapabilitiesParsec <PARSEC-привилегия>
```

Возможно установить несколько привилегий через пробел.

Если не нужно устанавливать привилегии для дочерних процессов всех хостов, то необходимо в конфигурационном файле `/etc/apache2/apache2.conf` установить для параметра `ChildCapabilitiesParsec` значение `none`:

```
ChildCapabilitiesParsec none
```

PARSEC-привилегии для виртуальных хостов применяются следующим образом:

- если в файле `/etc/apache2/sites-available/<имя_хоста>.conf` заданы привилегии, то они применяются для конкретных виртуальных хостов;
- если в файле `/etc/apache2/sites-available/<имя_хоста>.conf` не заданы привилегии, то применяются глобальные привилегии из файла `/etc/apache2/apache2.conf`;
- если в файле `/etc/apache2/sites-available/<имя_хоста>.conf` для параметра `ChildCapabilitiesParsec` установлено значение `none`, то никакие привилегии не применяются.

Пример

Имеется три виртуальных хоста со следующими именами: `client_1`, `client_2` и `client_3`. Для хостов `client_1` и `client_2` требуется применять глобальную PARSEC-привилегию на дочерние процессы — разрешение на запуск процесса с другой классификационной меткой, а для хоста `client_3` — разрешение на действия в каталоге с меткой `ccnr` над вложенными файлами и каталогами с уровнями конфиденциальности не выше уровня конфиденциальности данного каталога.

Чтобы применить глобальную PARSEC-привилегию на запуск процесса с другой классификационной меткой для хостов `client_1` и `client_2`, необходимо в конфигурационном файле `/etc/apache2/apache2.conf` для параметра `ChildCapabilitiesParsec` установить значение `PARSEC_CAP_SUMAC`.

Чтобы применить для хоста `client_3` PARSEC-привилегию на действия в каталоге с меткой `ccnr` над вложенными файлами и каталогами, необходимо в конфигурационном файле `/etc/apache2/sites-available/client_3.conf` для параметра `ChildCapabilitiesParsec` установить значение `PARSEC_CAP_CCNR_RELAX`.

12. ЗАЩИЩЕННАЯ ГРАФИЧЕСКАЯ ПОДСИСТЕМА

В ОС используется защищенная графическая подсистема, основанная на использовании оконной системы X Window System[1)] (реализация X.Org) со встроенной мандатной защитой.

Для установки пакетов графической подсистемы следует в процессе работы программы установки ОС отметить в окне «Выбор программного обеспечения» строку «Рабочий стол Fly».

Графический вход в систему осуществляется при помощи утилит `fly-dm` (запуск серверной части системы) и `fly-qdm` (поддержка графического интерфейса), переход к которым происходит после окончания работы загрузчика. Утилиты обеспечивают загрузку графической среды для работы в системе, соединение с удаленным XDMCP-сервером, а также завершение работы системы.

После установки ОС значения параметров графического входа устанавливаются по умолчанию. Изменение установленных значений осуществляется с помощью утилиты `fly-admin-dm` («Вход в систему»), запущенной от имени администратора. Описание утилиты приведено в электронной справке.

12.1. Конфигурирование менеджера окон и рабочего стола в зависимости от типа сессии

Выбор режима рабочего стола Fly выполняется в меню «Тип сессии» в окне графического входа в систему (утилита `fly-dm`). По умолчанию предусмотрено несколько режимов, но администратор системы может добавить новые режимы, например, для систем с низкими характеристиками производительности или удаленных терминалов можно создавать режим `fly-light` и т. д.

Для создания нового режима необходимо добавить файл (файлы) сессии с расширением `desktop` в `/usr/share/fly-dm/sessions` и создать соответствующие конфигурационные файлы для `fly-wm`.

При входе через `fly-dm` выставляется переменная `DESKTOP_SESSION=имя_режима`, например `fly`, `fly-desktop`, `fly-tablet`). Данная переменная является именем ярлыка сессии из `/usr/share/fly-dm/sessions` (но без расширения `.desktop`), которая указывает на тип сессии. Например:

`DESKTOP_SESSION=fly` — десктопный

`DESKTOP_SESSION=fly-tablet` — планшетный

[1)] Недоступно в режиме «Мобильный».

Данное имя сессии добавляется как суффикс «.$DESKTOP_SESSION» к базовому имени конфигурационного файла и используется для выбора конфигурационных файлов менеджера окон fly-wm в соответствии с типом сессии.

Если тип сессии десктопный, т. е. DESKTOP_SESSION=fly, то конфигурационные файлы остаются без суффикса для обратной совместимости.

Существуют следующие конфигурационные файлы в /usr/share/fly-wm/:

```
apprc
apprc.fly-mini
apprc.fly-tablet
en.fly-wmrc
en.fly-wmrc.fly-mini
en.fly-wmrc.fly-tablet
en.miscrc
en.miscrc.fly-mini
en.miscrc.fly-tablet
keyshortcutrc
keyshortcutrc.fly-mini
keyshortcutrc.fly-tablet
ru_RU.UTF-8.fly-wmrc
ru_RU.UTF-8.fly-wmrc.fly-mini
ru_RU.UTF-8.fly-wmrc.fly-tablet
ru_RU.UTF-8.miscrc
ru_RU.UTF-8.miscrc.fly-mini
ru_RU.UTF-8.miscrc.fly-tablet
sessrc
sessrc.fly-mini
sessrc.fly-tablet
theme/default.themerc
theme/default.themerc.fly-mini
theme/default.themerc.fly-tablet
```

Также есть конфигурационный файл fly-wmrc.mini, который служит для совместимости и включает все файлы с расширением *.fly-mini. Названия этих файлов определяют их назначение, а в комментариях в файлах приведены особенности использования.

При использовании файлов типа:

```
~/.fly/*rc
~/.fly/theme/*rc
/usr/share/fly-wm/*rc
/usr/share/fly-wm/theme/*rc
```

необходимо переделать формирование имени конфигурационного файла. Например, это сделано в утилитах `fly-admin-theme`, `fly-admin-hotkeys`, `fly-admin-winprops` и др.

В ярлыках в полях `NotShowIn` и `OnlyShowIn` можно использовать имена типов сессий (`fly`, `fly-tablet`). Функция `FlyDesktopEntry::isDisplayable()` из `libflycore` изменена с учетом нахождения в сессии какого-либо типа (`$DESKTOP_SESSION`), также в `libflycore` добавлены:

```
const char * flySessionName()
const char * flySessionConfigSuffix()
```

Используя имена типов сессий в `NotShowIn` и `OnlyShowIn`, можно скрывать/показывать определенные ярлыки из меню «Пуск», панели задач или автозапуска (в зависимости от текущего режима).

Если у какой-либо Qt-программы есть сохраняемые/восстанавливаемые параметры, «чувствительные» к типу сессии (планшет, десктоп и т. д.), то программа будет иметь такие параметры в отдельных экземплярах для каждого типа сессии, добавляя, например, суффиксы `$DESKTOP_SESSION` к именам параметров.

12.2. Рабочий стол как часть экрана

В файлах `*themerc` (прежде всего в `~/.fly/theme/current.themerc`) можно задавать параметры `FlyDesktopWidth` и `FlyDesktopHeight`, которые определяют размер (в пикселях) рабочего стола на экране. Это может быть полезно, например, для:

- деления широкоформатного монитора на две части: с рабочим столом и свободной областью, куда можно перетаскивать окна;
- для задания области рабочего стола только на левом мониторе в двухмониторной конфигурации с Xinerama.

12.3. Удаленный вход по протоколу XDMCP

По умолчанию в системе удаленный вход по протоколу XDMCP запрещен. Чтобы его разрешить необходимо:

1) в файле `/etc/X11/fly-dm/Xaccess` заменить `localhost` на символ `*`;
2) в файле `/etc/X11/fly-dm/fly-dmrc` убедиться, что `Enable=true`:

```
...
[Xdmcp]
Enable=true
...
```

12.4. Решение возможных проблем с видеодрайвером Intel

Видеодрайвер для систем на базе процессоров Intel может в некоторых случаях устранять возможные проблемы в работе графической подсистемы, например искажения на экране или отказ X-сервера. В ряде случаев это может быть вызвано типом используемого ускорения графики. По умолчанию в драйвере включен тип ускорения SNA. Для использования более старого, но более стабильного UXA можно в `/usr/share/X11/xorg.conf.d` разместить файл `10-intel.conf`:

```
Section "Device"
Identifier "intel"
Driver "intel"
Option "AccelMethod" "uxa"
EndSection
```

12.5. Автоматизация входа в систему

Для включения автоматизации входа пользователя в систему на разных разрешенных ему уровнях конфиденциальности с последующим переключением между такими входами необходимо в секции `[Service]` файла `/lib/systemd/system/fly-dm.service` задать переменную:

```
...
Environment=DM_LOGIN_AUTOMATION=value
...
```

Затем на рабочих столах пользователя создать, например, следующие ярлыки:

- ярлык для запуска или перехода в сессию с меткой `0:0:0x0:0x0`:

```
[Desktop Entry]
Name = session 0
Name[ru] = Сессия 0
Type = Application
NoDisplay = false
Exec = fly-dmctl maclogin user password 0:0:0x0:0x0
Icon = ledgreen
X-FLY-IconContext = Actions
Hidden = false
Terminal = false
StartupNotify = false
```

- ярлык для запуска или перехода в сессию с меткой `1:0:0x0:0x0`:

```
[Desktop Entry]
Name = session 1
Name[ru] = Сессия 1
Type = Application
NoDisplay = false
Exec = /usr/bin/fly-dmctl maclogin user password 1:0:0x0:0x0
Icon = ledyellow
X-FLY-IconContext = Actions
Hidden = false
Terminal = false
StartupNotify = false
```

- ярлык для запуска или перехода в сессию с меткой `2:0:0x0:0x0`:

```
[Desktop Entry]
Name = session 2
Name[ru] = Сессия 2
Type = Application
NoDisplay = false
Exec = fly-dmctl maclogin user password  2:0:0x0:0x0
Icon = ledred
X-FLY-IconContext = Actions
Hidden = false
Terminal = false
StartupNotify = false
```

С помощью ярлыков данного типа пользователь сможет максимально переключаться между сессиями с разными метками безопасности.

12.6. Рабочий стол Fly

В состав рабочего стола Fly входит оконный менеджер и графические утилиты, которые могут быть использованы для администрирования ОС. Большинство утилит представляет собой графические оболочки соответствующих утилит командной строки.

Основные графические утилиты для настройки и администрирования системы приведены в таблице 62.

Таблица 62

Утилита	Описание
`systemdgenie` «Инициализация системы»	Управление службой инициализации системы Systemd

Продолжение таблицы 62

Утилита	Описание
`synaptic` «Менеджер пакетов Synaptic»	Графическая утилита управления пакетами
`gufw` «Настройка межсетевого экрана»	Настройка межсетевого экрана UFW (Uncomplicated Firewall)
`fly-admin-reflex` «Обработка «горячего» подключения»	Настройка действий, выполняемых при подключении устройств
`fly-admin-env` «Переменные окружения»	Добавление, изменение и удаление переменных окружения
`astra-systemsettings` «Параметры системы»	Управление системой и локальной политикой безопасности. Программа состоит из модулей, которые позволяют настраивать пользовательское окружение, оборудование, загрузчик, управлять пользователями и группами и др. Также в программе возможно настраивать функции безопасности: мандатное управление доступом, мандатный контроль целостности, ограничение программной среды, правила подключения устройств, права доступа, привилегии, политики, регистрацию событий и др.
`fly-mimeapps` «Приложения для типов файлов»	Просмотр доступных приложений и установка приложения по умолчанию для типов файлов
`fly-admin-printer` «Принтеры»	Управление принтерами, настройка печати и управление заданиями на печать
`fly-admin-policykit-1` «Санкции PolicyKit-1»	Просмотр, предоставление и аннулирование санкций на выполнение привилегированных действий, управляемых с использованием PolicyKit-1
`fly-admin-session` «Сессии Fly»	Настройки параметров входа и выхода из сессий пользователя
`nm-connection-editor` «Сетевые соединения»	Настройка сетевых соединений
`fly-admin-network` «Параметры сети»	Управление автозапуском сетевых служб
`fly-admin-alternatives` «Системные альтернативы»	Управление системой альтернатив дистрибутивов, основанных на Debian
`hp-setup` «Установка принтеров, факсов и сканеров HP»	Установка новых устройств HP
`hp-plugin` «Установка дополнительного плагина HP»	Установка драйверов HP
`ksystemlog` «Просмотр системных журналов Ksystemlog»	Просмотр журнала расширенной системы протоколирования

Продолжение таблицы 62

Утилита	Описание
`system-config-audit` «Конфигурация аудита»	Настройки аудита системы
`fly-sosreport` «Центр системных отчетов»	Сбор данных о конфигурации системы и работе подсистем для последующей диагностики
`fly-run` «Запуск приложения»	Запуск программы или осуществление доступа к ресурсу из командной строки, в том числе от имени другого пользователя и/или с другими мандатными атрибутами
«Контроль целостности файлов»	Графическая утилита программы afick монитора изменений файлов системы
`fly-admin-device-manager` «Менеджер устройств»	Просмотр доступных устройств, настройка их драйверов и параметров
`fly-admin-usbip` «Сервис удаленных USB-накопителей»	Предоставление удаленного доступа к USB-носителям и токенам с помощью USB-over-IP.
`fly-admin-format` «Форматирование внешнего носителя»	Удаление данных и форматирование внешнего носителя и его разделов
`fly-admin-iso` «Запись ISO образа на USB носитель»	Программа записи iso-образа на USB-носитель
`fly-admin-int-check` «Проверка целостности системы»	Проверка целостности системы для рабочего стола Fly
`fly-admin-marker` «Редактор маркеров»	Просмотр и изменение настроек маркировки печати, редактирование шаблонов маркера
`fly-print-station` «Управление печатью документов»	Печать и маркировка документов ограниченного доступа с возможностью перемещений заданий на другой принтер
`gparted` «Редактор разделов Gparted»	Создание, перераспределение или удаление системных разделов ОС
`ksysguard` «Системный монитор»	Просмотр информации о процессах и общей загрузке системы: ЦПУ, памяти, раздела подкачки и сети
`konsole` «Терминал»	Эмулятор терминала, позволяющий взаимодействовать с консолью
`mc` «Менеджер файлов MC»	Просмотр папок и элементов ФС, выполнение основных функций управления файлами, обращение к сетевым ресурсам, работа с архивами
`kgpg` «Управление ключами KGpg»	Управление ключами GPG
`fly-admin-ad-client` «Настройка клиента Active Directory Fly»	Ввод клиентского компьютера в существующий домен AD Windows

Окончание таблицы 62

Утилита	Описание
`fly-admin-ad-server` «Настройка сервера Active Directory Fly»	Запуск службы контроллера домена AD
`fly-admin-ad-sssd-client` «Настройка клиента SSSD Fly»	Ввод клиентского компьютера в существующий домен AD Windows, при этом будет задействована служба управления аутентификацией и авторизацией (System Security Services Daemon (SSSD))
`fly-admin-freeipa-server` «Настройка FreeIPA server Fly»	Установка и настройка сервера FreeIPA
`fly-admin-freeipa-client` «Настройка FreeIPA client Fly»	Ввод клиентского компьютера в существующий домен FreeIPA
`fly-admin-multiseat` «Мультитерминальный режим»	Подготовка компьютера для одновременной работы нескольких пользователей
`fly-admin-openvpn-server` «Настройка OpenVPN сервера Fly»	Настройка сервера VPN
`fly-admin-ftp` «FTP-сервер»	Настройка сервера FTP
`fly-admin-samba` «Общие папки (Samba)»	Управление общими папками Samba
`fly-passwd` «Изменить пароль»	Смена пароля
`fly-su` «Подмена пользователя»	Выполнение команды от имени другого пользователя
`fly-astra-update` «Установка обновлений»	Программа установки обновлений
`fly-admin-repo` «Редактор репозиториев»	Создание и управление репозиториями

Не все из приведенных в таблице 62 утилит устанавливаются по умолчанию при установке ОС. Описание утилит доступно в электронной справке. Вызов электронной справки осуществляется с помощью ярлыка «Помощь», размещенного на рабочем столе, а также путем нажатия комбинации клавиш **<Alt+F1>** или путем нажатия клавиши **<F1>** в активном окне графической утилиты.

12.7. 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 недоступна возможность переопределить параметры, заданные в `/usr/share/fly-wm/theme.master/themerc`.

12.8. Мандатное управление доступом

Мандатная защита, встроенная в рабочий стол Fly и устанавливаемая по умолчанию вместе с ОС, позволяет администратору задавать отдельно для каждого пользователя разрешенный диапазон иерархических уровней конфиденциальности и неиерархических категорий конфиденциальности. Для этой цели следует использовать модуль «Пользователи» в разделе «Пользователи и группы» графической утилиты `astra-systemsettings` («Параметры системы», см. электронную справку). Для вызова модуля можно использовать команду:

```
astra-systemsettings astra_kcm_users
```

После того как пользователь, для которого установлены возможные иерархические уровни конфиденциальности и неиерархические категории конфиденциальности, отличные от нуля, войдет в систему, ему будет предложено установить конкретный иерархический уровень конфиденциальности и конкретную неиерархическую категорию конфиденциальности для данной сессии в пределах разрешенных диапазонов. Выбранные значения этих параметров отображаются на цветном индикаторе с числом внутри, расположенном в области уведомлений на панели задач. Для получения информационного сообщения следует навести курсор на индикатор (рис. 11).

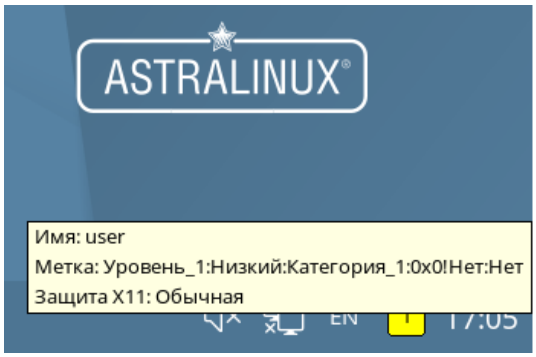

Рис. 11

13. ГРАФИЧЕСКАЯ ПОДСИСТЕМА РЕЖИМА «МОБИЛЬНЫЙ»

Графическая подсистема режима «Мобильный» реализована на основе протокола Wayland, в качестве оконного менеджера используется KWin.

В графическом интерфейсе пользователя для создания окружения рабочего стола используется KDE Plasma Mobile (для мобильного вида) и KDE Plasma (для десктопного вида).

13.1. Отображение графического интерфейса

В режиме «Мобильный» графический интерфейс адаптирован для использования на устройствах, оснащенных сенсорным устройством указания на чувствительной области экрана дисплея при помощи прикосновения (типа «touch-screen»).

Данный режим поддерживает отображение графического интерфейса в мобильном виде и в десктопном виде. Мобильный вид используется по умолчанию при использовании ОС в режиме «Мобильный». Из мобильного вида возможно выполнить переход в десктопный вид. При подключении к устройству монитора, клавиатуры и мыши десктопный вид может быть использован в роли ПЭВМ для администрирования и настройки ОС на устройстве.

13.2. Автоматизация входа в систему

Для включения автоматического входа пользователя в систему используется конфигурационный файл `~/.config/kscreenlockerrc`, в котором задан параметр:

```
[<имя_пользователя>]
PermitEmptyPasswords=true
```

Параметр позволяет входить пользователю с пустым паролем.

Шаблон конфигурационного файла, который будет использоваться при создании конфигурационного файла для каждого пользователя, можно создать в `/etc/xdg/kscreenlockerrc` с необходимыми параметрами (доступные параметры приведены в `kscreenlocker/settings/kscreenlockersettings.kcfg`).

Пример

```
[Version]
update_info=kscreenlocker.upd:0.1-autolock

[User]
PermitEmptyPasswords=true
```

Настройка автоматического входа в систему также может быть настроена через панель быстрого доступа, кнопка **[Безопасность]**, пункт «Общие» (см. электронную справку «Документация — Графический интерфейс — Режим «Мобильный»).

13.3. Рабочий стол

В состав рабочего стола KDE Plasma входит оконный менеджер и приложения (в т. ч. адаптированные для работы на устройствах с сенсорным экраном), которые могут быть использованы для администрирования ОС. Перечень основных приложений приведен в таблице 63.

Таблица 63

Приложение	Описание
`plasma-settings` «Настройки»	Настройка и администрирование системы
`fly-admin-cron` «Планировщик задач»	Установка расписания задач для выполнения в фоновом режиме, настройка среды выполнения задачи (переменных окружения), разрешение или запрет на выполнение уже установленной задачи
`mc` «Менеджер файлов MC»	Просмотр папок и элементов ФС, выполнение основных функций управления файлами, обращение к сетевым ресурсам, работа с архивами
`gufw` «gufw»	Программа настройки межсетевого экрана UFW (Uncomplicated Firewall)
`fly-admin-autostart` «Автозапуск»	Управление автозапуском приложений, автоматическим открытием файлов и каталогов при загрузке рабочего стола
`fly-admin-device-manager` «Менеджер устройств»	Просмотр доступных устройств, настройка их драйверов и параметров
`fly-admin-policykit-1` «Санкции PolicyKit-1»	Просмотр, предоставление и аннулирование санкций на выполнение привилегированных действий, управляемых с использованием PolicyKit-1
`nm-connection-editor` «Сетевые соединения»	Настройки сетевых соединений (по умолчанию при загрузке системы выполняется автозапуск программы)
`fly-event-viewer` «Журнал системных событий»	Просмотр записей в журнале системных событий, печать и экспорт записей
`ksysguard` «Системный монитор»	Отслеживание системных параметров
`fly-term` «Терминал Fly»	Эмулятор терминала, позволяющий взаимодействовать с консолью
`ksystemlog` «Журнал аудита»	Просмотр журнала расширенной системы протоколирования

Окончание таблицы 63

Приложение	Описание
`hp-setup` «Установка принтеров, факсов и сканеров HP»	Установка новых устройств HP
`fly-admin-printer` «Принтеры»	Добавление, настройка, удаление и просмотр информации о принтерах, настройка печати и управление заданиями на печать
`fly-admin-format` «Форматирование внешнего носителя»	Удаление данных и форматирование внешнего носителя и его разделов
`hp-plugin` «Установка дополнительного плагина HP»	Установка драйверов HP
`fly-admin-env` «Переменные окружения»	Добавление, изменение и удаление переменных окружения
`systemdgenie` «Инициализация системы»	Управление службой инициализации системы Systemd
`fly-run` «Запуск приложения»	Запуск программы или осуществление доступа к ресурсу из командной строки, в т.ч. от имени другого пользователя и/или с другими мандатными атрибутами
`system-config-audit` «Конфигурация аудита»	Проверка и изменение статуса и настроек системы аудита

Описание приложений доступно в справке, вызываемой из приложения, или в электронной справке, вызываемой с помощью ярлыка «Помощь», размещенного на экране приложений.

14. ЗАЩИЩЕННЫЙ КОМПЛЕКС ПРОГРАММ ПЕЧАТИ И МАРКИРОВКИ ДОКУМЕНТОВ

Одной из основных служб, предоставляемых ОС, является служба печати, доработанная для маркировки документов и позволяющая осуществлять печать документовв соответствии с требованиями, предъявляемыми к защищенным ОС.

Защищенный комплекс программ печати и маркировки документов обеспечивает:

- управление заданиями на печать;
- выполнение команд администратора печати;
- предоставление информации о состоянии принтеров локальным и удаленным программам;
- маркировку выводимых на печать документов;
- выдачу информационных сообщений пользователям.

14.1. Устройство системы печати

Состав защищенного комплекса программ печати и маркировки приведен в таблице 64.

Таблица 64

Название	Пакет	Описание
CUPS	`cups-daemon`	Сервер печати. Обрабатывает запросы от пользователя и выполняет запуск служебных программ
`fly-admin-printer`	`fly-admin-printer`	Графическая утилита для настройки принтеров и сервера печати CUPS, а также управления очередью печати. При установленном пакете `fly-admin-printer-mac` позволяет маркировать документы и настраивать метки безопасности принтера
`fly-print-monitor`	`fly-print-monitor`	Графическая утилита для отслеживания состояния принтеров и сервера печати
`fly-jobviewer`	`fly-jobviewer`	Графическая утилита для управления очередью печати. При установленном пакете `fly-admin-printer-mac` позволяет также маркировать документы

Окончание таблицы 64

Название	Пакет	Описание
fly-print-station	fly-print-station	Графическая утилита для управления печатью и маркировки документов
psmarker	parsec-cups	Программа для маркировки документов в формате PostScript. Модифицирует исходный файл задания, добавляя в него маркеры. Запускается с помощью CUPS
fonarik	parsec-cups	Программа для создания файла маркировки на обратной стороне последнего листа. Запускается с помощью CUPS
markerdb	parsec-cups	Программа для записи журнала маркировки. Вызывается из CUPS после завершения задания маркировки. В процессе маркировки не участвует
pdfhelper	parsec-cups	Программа для определения размера и ориентации PDF-документов. Запускается с помощью CUPS перед маркировкой
markjob	parsec-cups-client	Инструмент для маркировки документов в консольном режиме
libfly-admin-printer-mac	libfly-admin-printer-mac3	Библиотека с функциями маркировки и просмотра журнала для графических клиентов. Упрощает взаимодействие с сервером CUPS при выполнении задач маркировки
fly-admin-printer-mac	fly-admin-printer-mac	Утилита, добавляющая функции маркировки в графические утилиты fly-admin-printer и fly-jobviewer
fly-admin-marker	fly-admin-marker	Графическая утилита для редактирования шаблонов маркировки. Работает только локально вместе с сервером печати CUPS

Планировщик — это сервер, который управляет списком доступных принтеров и направляет задания на печать, используя подходящие фильтры и выходные буферы (backends).

Файлами конфигурации являются:

- файл конфигурации сервера;
- файлы определения принтеров и классов;
- типы MIME и файлы правил преобразования;
- файлы описания PostScript-принтеров (PPD).

Конфигурационный файл сервера похож на файл конфигурации веб-сервера и определяет все свойства управления доступом.

Файлы описания принтеров и классов перечисляют доступные очереди печати и классы. Классы принтеров — наборы принтеров. Задания, посланные классу принтеров, направляются к первому доступному принтеру данного класса.

Очередь печати — механизм, который позволяет буферизовать и организовать задания, посылаемые на принтер. Необходимость организации такого механизма обуславливается тем, что принтер является медленно действующим устройством, и задания не могут быть распечатаны мгновенно. Очевидно, что в многопользовательской среде возникает конкуренция со стороны пользователей при доступе к принтерам, поэтому задания необходимо располагать в очереди. Для этого используется буферный каталог `/var/spool/cups/`.

Файлы типов MIME перечисляют поддерживаемые MIME-типы (`text/plain`, `application/postscript` и т. д.) и правила для автоматического обнаружения формата файла. Они используются сервером для определения поля `Content-Type` для GET- и HEAD-запросов и обработчиком запросов IPP, чтобы определить тип файла.

Правила преобразования MIME перечисляют доступные фильтры. Фильтры используются, когда задание направляется на печать, таким образом, приложение может послать файл удобного (для него) формата системе печати, которая затем преобразует документ в требуемый печатный формат. Каждый фильтр имеет относительную «стоимость», связанную с ним, и алгоритм фильтрования выбирает набор фильтров, который преобразует файл в требуемый формат с наименьшей общей «стоимостью».

Файлы PPD описывают возможности всех типов принтеров. Для каждого принтера имеется один PPD-файл. Файлы PPD для не-PostScript-принтеров определяют дополнительные фильтры посредством атрибута `cupsFilter` для поддержки драйверов принтеров.

В ОС стандартным языком описания страниц является язык PostScript. Большинство прикладных программ (редакторы, браузеры) генерируют программы печати на этом языке. Когда необходимо напечатать ASCII-текст, программа печати может быть ASCII-текстом. Имеется возможность управления размером шрифтов при печати ASCII-текста. Управляющая информация используется для контроля доступа пользователя к принтеру и аудита печати. Также имеется возможность печати изображений в форматах GIF, JPEG, PNG, TIFF и документов в формате PDF.

Фильтр — программа, которая читает из стандартного входного потока или из файла, если указано его имя. Все фильтры поддерживают общий набор параметров, включающий имя принтера, идентификатор задания, имя пользователя, имя задания, число копий и параметры задания. Весь вывод направляется в стандартный выходной поток.

Фильтры предоставлены для многих форматов файлов и включают, в частности, фильтры файлов изображения и растровые фильтры PostScript, которые поддерживают принтеры, не относящиеся к типу PostScript. Иногда несколько фильтров запускаются параллельно для получения требуемого формата на выходе.

Программа `backend` — это специальный фильтр, который отправляет печатаемые данные устройству, в т. ч. через сетевое соединение. В состав системы печати включены фильтры для поддержки устройств, подключаемых с помощью параллельного и последовательного интерфейсов, а также шины USB.

Клиентские программы используются для управления заданиями и сервером печати.

Управление заданиями включает:

- формирование;
- передачу серверу печати;
- мониторинг и управление заданиями в очереди на печать.

Управление сервером включает:

- запуск/остановку сервера печати;
- разрешение/запрет постановки заданий в очередь;
- разрешение/запрет вывода заданий на принтер.

В общем случае вывод данных на принтер происходит следующим образом:

1) программа формирует запрос на печать задания к серверу печати;

2) сервер печати принимает подлежащие печати данные, формирует в буферном каталоге файлы с содержимым задания и файлы описания задания, при этом задание попадает в соответствующую очередь печати;

3) сервер печати просматривает очереди печати для незанятых принтеров, находит в них задания и запускает конвейер процессов, состоящий из фильтров и заканчивающийся выходным буфером, информация из которого поступает в принтер посредством драйверов ОС;

4) контроль и мониторинг процесса печати выполняется с помощью программ `lpq`, `lpc`, `lprm`, `lpstat`, `lpmove`, `cancel`, а также с помощью графической утилиты `fly-admin-printer`.

Система печати ОС решает следующие задачи:

1) монопольная постановка задания в очередь на печать. Данная функция предполагает невозможность вывода документа на печать в обход системы печати;
2) маркировка каждого напечатанного листа. Каждый лист сопровождается автоматической маркировкой (учетными атрибутами документа).

ВНИМАНИЕ! Для обеспечения штатной работы пользователя с сетевыми службами должна быть явно задана его метка безопасности (диапазон уровней конфиденциальности, категорий конфиденциальности и меток целостности) с помощью соответствующих утилит, даже если ему не доступны уровни и категории выше 0. Дополнительная информация приведена в документе РУСБ.10015-01 97 01-1.

14.2. Установка комплекса программ печати

Основные компоненты защищенного комплекса программ печати и маркировки документов устанавливаются автоматически при установке ОС.

В случае необходимости возможно вручную установить защищенный комплекс программ печати и маркировки документов, выполнив команду:

```
sudo apt install parsec-cups fly-admin-printer-mac fly-admin-marker fly-print-station
```

14.3. Настройка комплекса программ печати

Настройка защищенного комплекса программ печати и маркировки документов (сервер печати CUPS) выполняется редактированием конфигурационных файлов `/etc/cups/cupsd.conf` и `/etc/cups/cups-files.conf`. Копии конфигурационных файлов, устанавливаемые вместе с пакетом, размещаются в `/usr/share/cups` (файлы `cupsd.conf.default` и `cups-files.conf.default`), данные файлы могут использоваться при необходимости восстановить комплекс программ печати и маркировки документов в исходное состояние.

Настройка сервера печати CUPS также может выполняться следующими способами:

1) графической утилитой `fly-admin-printer`;
2) через веб-интерфейс по адресу:

```
localhost:631/admin
```

3) инструментом командной строки `cupsctl`. Запуск инструмента возможен:
   а) от имени пользователя `root` с использованием механизма `sudo`:

```
sudo cupsctl [параметры]
```

б) от имени пользователя, входящего в группы с правами администрирования сервера печати CUPS, командой:

```
/usr/sbin/cupsctl [параметры]
```

Группы пользователей с правами администрирования сервера печати CUPS указаны в качестве значения параметра `SystemGroup` в файле `/etc/cups/cups-files.conf`. По умолчанию в этот список включены группы `root` и `lpadmin`. Если удалить группу `root` из значения параметра `SystemGroup`, то инструмент командной строки `cupsctl`, запущенный на компьютере сервера печати с использованием механизма `sudo`, будет возвращать ошибку доступа.

Основные пользовательские настройки содержатся в конфигурационных файлах `/etc/cups/client.conf` и `/home/<имя_пользователя>/.cups/lpoptions`.

14.3.1. Настройка сервера печати с локальной аутентификацией

Чтобы сервер печати мог удаленно принимать задания и команды, необходимо разрешить совместный доступ к принтерам, выполнив команду:

```
sudo cupsctl --share-printers
```

При необходимости принимать задания печати с любых адресов, а не только из подсети сервера печати, следует выполнить команду:

```
sudo cupsctl --remote-any
```

Администрирование сервера печати CUPS по умолчанию разрешено только локально. Для включения удаленного администрирования выполнить команду:

```
sudo cupsctl --remote-admin
```

По умолчанию сервер печати использует политику доступа, которая позволяет не прошедшим аутентификацию пользователям добавлять принтеры и отправлять задания на печать. Для разрешения доступа к серверу печати и принтерам только аутентифицированным пользователям необходимо применить встроенную политику доступа `authenticated`:

```
sudo cupsctl DefaultPolicy=authenticated
```

Для применения изменений перезагрузить сервер печати:

```
sudo systemctl restart cups
```

14.3.2. Настройка сервера печати для работы в ЕПП

Для работы системы печати в ЕПП компьютер сервера печати CUPS должен быть введен в домен в соответствии с 8.2.8.

Для авторизации на сервере печати и выполнения действий по управлению принтерами и очередями печати следует создать в FreeIPA учетную запись администратора печати и предоставить ей права на сервере печати одним из следующих способов:

- добавить учетную запись администратора печати в локальную группу администраторов печати `lpadmin`:

```
sudo gpasswd –a <доменное_имя_учетной_записи> lpadmin
```

Пример

```
sudo gpasswd –a print_admin@ASTRA.DOM lpadmin
```

- указать в значении параметра `SystemGroup` в файле `/etc/cups/cups-files.conf` первичную группу администратора печати, совпадающую с его доменным именем:

```
SystemGroup root lpadmin <полное_имя_первичной_группы>
```

Пример

```
SystemGroup root lpadmin print_admin@ASTRA.DOM
```

- добавить учетную запись администратора печати в доменную группу и указать эту группу в значении параметра `SystemGroup` в файле `/etc/cups/cups-files.conf`:

```
SystemGroup root lpadmin <полное_имя_доменной_группы>
```

Пример

```
SystemGroup root lpadmin printer_admins@ASTRA.DOM
```

Все члены указанной доменной группы получат права на управление сервером печати.

Для доступа пользователей к серверу печати через веб-интерфейс необходима HTTP-служба, зарегистрированная для компьютера сервера печати в домене FreeIPA. Если сервер печати развернут на контроллере домена, то данная служба уже была создана автоматически при создании домена. Если сервер печати развернут на отдельном компьютере в составе домена, то для регистрации службы необходимо на сервере печати выполнить следующее:

1) получить билет Kerberos администратора домена для пользователя `root` (необходимо для последующего использования билета с механизмом `sudo`):

```
sudo kinit admin
```

2) зарегистрировать доменную службу HTTP:

```
sudo ipa service-add HTTP/<полное_имя_хоста_сервера_печати>
```

Пример

```
sudo ipa service-add HTTP/cups.astra.dom
```

3) получить с контроллера домена таблицу ключей Kerberos и сохранить ее в файл:

```
sudo ipa-getkeytab -p HTTP/<полное_имя_хоста_сервера_печати> -k \
     /etc/krb5.keytab
```

Пример

```
sudo ipa-getkeytab -p HTTP/cups.astra.dom -k /etc/krb5.keytab
```

Если сервер печати развернут на контроллере домена, то доменную службу создавать и регистрировать не нужно. Для получения копии существующих ключей доменной службы HTTP выполнить следующее:

1) получить билет Kerberos администратора домена для пользователя `root` (необходимо для последующего использования билета с механизмом `sudo`):

```
sudo kinit admin
```

2) разрешить группе администраторов домена получение таблицы ключей:

```
sudo ipa service-allow-retrieve-keytab \
     HTTP/<полное_имя_контроллера_домена> --groups=admins
```

3) получить копию таблицы ключей:

```
sudo ipa-getkeytab -p \
     HTTP/<полное_имя_контроллера_домена> -k /etc/krb5.keytab -r
```

4) вернуть изначальное состояние доступа к таблице ключей:

```
sudo ipa service-disallow-retrieve-keytab \
     HTTP/<полное_имя_контроллера_домена> --groups=admins
```

Для проверки добавления ключей выполнить команду:

```
sudo klist -kte /etc/krb5.keytab
```

Корректный вывод команды:

```
Keytab name: FILE:/etc/krb5.keytab
KVNO Timestamp Principal
---- ------------------ ------------------------------------------------------
  1 26.06.2025 14:22:30 host/cups.astra.dom@ASTRA.DOM (aes256-cts-hmac-sha384-192)
  1 26.06.2025 14:22:30 host/cups.astra.dom@ASTRA.DOM (aes128-cts-hmac-sha256-128)
  1 26.06.2025 14:22:30 host/cups.astra.dom@ASTRA.DOM (aes256-cts-hmac-sha1-96)
  1 26.06.2025 14:22:30 host/cups.astra.dom@ASTRA.DOM (aes128-cts-hmac-sha1-96)
  1 26.06.2025 14:39:01 HTTP/cups.astra.dom@ASTRA.DOM (aes256-cts-hmac-sha384-192)
  1 26.06.2025 14:39:01 HTTP/cups.astra.dom@ASTRA.DOM (aes128-cts-hmac-sha256-128)
  1 26.06.2025 14:39:01 HTTP/cups.astra.dom@ASTRA.DOM (aes256-cts-hmac-sha1-96)
  1 26.06.2025 14:39:01 HTTP/cups.astra.dom@ASTRA.DOM (aes128-cts-hmac-sha1-96)
```

Для дальнейшей настройки сервера печати выполнить следующее:

1) выбрать метод `Negotiate` в качестве способа аутентификации по умолчанию:

```
sudo cupsctl DefaultAuthType=Negotiate
```

2) указать имя хоста сервера печати:

```
sudo cupsctl ServerName=<полное_имя_хоста_сервера_печати>
```

3) включить поддержку мандатного управления доступом:

```
sudo cupsctl MacEnable=On
```

4) перезапустить службу сервера печати, выполнив команду:

```
sudo systemctl restart cups
```

ВНИМАНИЕ! В конфигурационном файле защищенного сервера печати `/etc/cups/cupsd.conf` не допускается установка значения `None` параметра `DefaultAuthType` (отключение аутентификации) и внесение изменений в параметры политики PARSEC, не соответствующих эксплуатационной документации.

По умолчанию локальные пользователи сервера печати, входящие в группу `lpadmin`, не проходят аутентификацию Kerberos при доступе к серверу печати, так как локальное соединение с сервером выполняется через сокет (механизм `SO_PEERCRED`). Для переключения локальных пользователей на сетевое соединение с аутентификацией Kerberos необходимо:

1) создать на сервере печати файл `/etc/cups/client.conf`, содержащий строку:

```
ServerName <полное_имя_хоста_сервера_печати>
```

2) сделать данный файл доступным на чтение всем пользователям:

```
sudo chmod +r /etc/cups/client.conf
```

При настроенном удаленном администрировании (см. 14.3.1) сервер печати по умолчанию принимает только обращения, содержащие в HTTP-заголовке полное сетевое имя его хоста. При необходимости возможно настроить доступ к серверу печати с помощью одного или нескольких сетевых псевдонимов (псевдоним должен разрешаться в IP-адрес службой DNS). Для указания псевдонима выполнить команду:

```
sudo cupsctl ServerAlias=<псевдоним_сервера_печати>
```

Пример

Указать псевдоним `printserver` для доступа к серверу печати по адресу `http://printserver:631`:

```
sudo cupsctl ServerAlias=printserver
```

Указать несколько псевдонимов возможно через пробел в значении параметра `ServerAlias` в конфигурационном файле `/etc/cups/cupsd.conf`. Если в качестве псевдонима указать символ «*», то будут разрешены обращения по любым псевдонимам.

Если удаленное администрирование отключено, то единственным разрешенным псевдонимом является `localhost`.

Настройка браузера Mozilla Firefox для использования аутентификации Kerberos описана в 11.4.

Настройка принтеров может быть выполнена с использованием графической утилиты `fly-admin-printer` (см. электронную справку).

14.3.3. Настройка клиентов сервера печати

Основные компоненты клиентской части защищенного комплекса программ печати и маркировки документов устанавливаются автоматически при установке ОС.

В случае необходимости возможно вручную установить клиентскую часть комплекса, выполнив команду:

```
sudo apt install parsec-cups-client fly-admin-printer-mac
```

На компьютеры, с которых будет выполняться маркировка документов (см. 14.5), дополнительно установить следующие пакеты:

```
fly-print-station fly-admin-marker
```

Для работы клиента с сервером печати необходимо:

1) создать на компьютере клиента файл `/etc/cups/client.conf`, содержащий строку:

```
ServerName <полное_имя_хоста_сервера_печати>
```

Пример

```
ServerName cups.astra.dom
```

2) сделать данный файл доступным на чтение всем пользователям:

```
sudo chmod +r /etc/cups/client.conf
```

Если сервер печати настроен для работы в ЕПП (см. 14.3.2), то компьютер клиента должен быть введен в домен в соответствии с 8.2.8.

14.3.4. Регистрация событий

Регистрация событий защищенного комплекса печати и маркировки документов выполняется в следующих журналах:

1) `/var/log/cups/error_log` — сообщения об ошибках сервера печати, принтеров или других программ печати защищенного комплекса;

2) `/var/log/cups/access_log` — запросы к серверу печати;

3) `/var/log/cups/page_log` — сообщения успешной обработки страниц задания на печать;

4) в журнале подсистемы регистрации событий из состава ОС (см. 17.2) — события заданий на печать (создано, завершено, отменено и т. д.), события маркировки и события изменения принтеров (добавлен, удален, изменен).

Регистрация в журналы /var/log/cups/error_log, /var/log/cups/access_log и /var/log/cups/page_log выполняется автоматически.

Включение и отключение регистрации событий в журнал подсистемы регистрации событий осуществляется в графической утилите fly-admin-printer (см. электронную справку) или в конфигурационном файле /etc/cups/cupsd.conf путем задания значения параметру MacAudit (on — регистрация включена, задано по умолчанию после установки пакета; off — регистрация отключена):

```
MacAudit on
```

14.4. Настройка принтера и управление печатью

14.4.1. Общие положения

Установку и настройку принтера следует производить после завершения установки и первоначальной настройки ОС.

При печати через локальный сервер печати данные сначала формируются на локальном сервере, как для любой другой задачи печати, после чего посылаются на принтер, подключенный к данному компьютеру.

Системные каталоги, определяющие работу системы печати ОС, содержат файлы, которые не являются исполняемыми и содержат необходимую для драйвера принтера информацию (используемое физическое устройство, удаленный компьютер и принтер для удаленной печати), а также файлы журнала:

- /etc/cups/printers.conf — описание принтеров в ОС;
- /etc/cups/ppd/<имя_очереди>.ppd — описание возможностей принтера, которые используются при печати заданий и при настройке принтеров;
- /var/log/cups/error_log — файл журнала, содержащий сообщения об ошибках сервера печати, принтера или других программ системы печати;
- /var/log/cups/access_log — файл журнала, содержащий все запросы к серверу печати;
- /var/log/cups/page_log — файл журнала, содержащий сообщения успешной обработки страниц задания фильтрами и принтером.

Далее термин «принтер» в настоящем подразделе используется для обозначения принтера, соответствующего одной записи в файле /etc/cups/printers.conf. Под термином «физический принтер» подразумевается устройство, с помощью которого производится вывод информации на бумажный носитель. В файле /etc/cups/printers.conf может быть несколько записей, описывающих один физический принтер различными способами.

14.4.2. Команды управления печатью

В систему печати ОС включены файлы, предоставляющие командный интерфейс пользователя в стиле BSD и System V. Перечень файлов приведен в таблице 65.

Таблица 65

Файл	Описание
/usr/bin/lpr	Постановка заданий в очередь. Совместима с командой lpr системы печати BSD UNIX
/usr/bin/lp	Постановка заданий в очередь. Совместима с командой lp системы печати System V UNIX
/usr/bin/lpq	Просмотр очередей печати
/usr/sbin/lpc	Управление принтером. Является частичной реализацией команды lpc системы печати BSD UNIX
/usr/bin/lprm	Отмена заданий, поставленных в очередь на печать
/usr/sbin/cupsd	Сервер печати
/usr/sbin/lpadmin	Настройка принтеров и классов принтеров
/usr/sbin/lpmove	Перемещение задания в другую очередь
/usr/bin/fly-admin-printer	Настройка системы печати, установка и настройка принтеров, управление заданиями

Описание данных команд приведено на страницах руководства man.

CUPS предоставляет утилиты командной строки для отправления заданий и проверки состояния принтера. Команды lpstat и lpc status также показывают сетевые принтеры (принтер@сервер), когда разрешен обзор принтеров.

Команды администрирования System V предназначены для управления принтерами и классами. Средство администрирования lpc поддерживается только в режиме чтения для проверки текущего состояния очередей печати и планировщика.

Остановить работу службы печати можно с помощью команды:

```
systemctl stop cups
```

Запустить службу печати можно с помощью команды:

```
systemctl start cups
```

14.4.2.1. lp

С помощью команды `lp` выполняется передача задачи принтеру, т. е. задача ставится в очередь на печать. В результате выполнения этой команды файл передается серверу печати, который помещает его в каталог `/var/spool/cups/`.

14.4.2.2. lpq

Команда `lpq` предназначена для проверки очереди печати, используемой LPD, и вывода состояния заданий на печать, указанных при помощи номера задания либо системного идентификатора пользователя, которому принадлежит задание (владельца задания). Команда выводит для каждого задания имя его владельца, текущий приоритет задания, номер задания и размер задания в байтах, без параметров выводит состояние всех заданий в очереди.

14.4.2.3. lprm

Команда `lprm` предназначена для удаления задания из очереди печати. Для определения номера задания необходимо использовать команду `lpq`. Удалить задание может только его владелец или администратор печати.

14.4.2.4. lpadmin

Команда `lpadmin` также используется для настройки принтера в ОС.

Ее запуск с параметром `-p` используется для добавления или модификации принтера:

```
/usr/sbin/lpadmin -p printer [параметры]
```

Основные параметры команды `lpadmin` приведены в таблице 66.

Таблица 66

Параметр	Описание
`-c class`	Добавляет названный принтер к классу принтеров `class`. Если класс не существует, то он создается
`-m model`	Задает стандартный драйвер принтера, обычно файл `PPD`. Файлы `PPD` обычно хранятся в каталоге `/usr/share/cups/model/`. Список всех доступных моделей можно вывести командой `lpinfo` с параметром `-m`
`-r class`	Удаляет указанный принтер из класса `class`. Если в результате класс становится пустым, он удаляется
`-v device-uri`	Указывает адрес устройства для связи с принтером
`-D info`	Выдает текстовое описание принтера
`-E`	Разрешает использование принтера и включает прием заданий
`-L location`	Выводит расположение принтера

Окончание таблицы 66

Параметр	Описание
`-P ppd-file`	Указывает локальный файл `PPD` для драйвера принтера

Для данной команды существуют также параметры по регулированию политики лимитов и ограничений по использованию принтеров и политики доступа к принтерам.

Запуск команды `lpadmin` с параметром `-x` используется для удаления принтера:

```
/usr/sbin/lpadmin -x printer
```

14.4.3. Графическая утилита настройки сервера печати

Утилита `fly-admin-printer` предназначена для настройки печати в графическом режиме.

Позволяет администратору печати устанавливать, настраивать и удалять принтеры и классы принтеров, а также настраивать сервер печати и управлять заданиями на печать.

Непривилегированному пользователя позволяет настраивать печать и параметры принтера, а также управлять заданиями на печать (удалять, приостанавливать, возобновлять печать и устанавливать отложенную печать). Для вызова привилегированных действий запрашивается авторизация.

Подробную информацию по использованию утилиты `fly-admin-printer` см. в электронной справке.

Для установки драйверов принтеров производства Hewlett Packard рекомендуется использовать утилиту `hp-setup`.

14.5. Маркировка документа

14.5.1. Общие сведения

При поступлении задания на печать считывается метка безопасности сетевого соединения и копируется в атрибут задания `mac-job-mac-label`.

При печати задания с нулевой меткой безопасности (нулевой уровень конфиденциальности, без категорий конфиденциальности и нулевая метка целостности) маркировка листов не выполняется и печать осуществляется в штатном режиме. При этом атрибут принтера `mac-printer-mac-min` должен быть нулевым, иначе задание на печать будет завершено с ошибкой.

При печати задания с ненулевой меткой безопасности оно принудительно переводится сервером печати в состояние «отложено» до проведения привилегированным пользователем маркировки выводимых на печать листов. Файлы заданий (в каталоге `/var/spool/cups`) маркируются согласно мандатному контексту документа.

ВНИМАНИЕ! Задания печати администратора печати (учетная запись, входящая в группу `lpadmin`), отправляются сразу на печать без задержки на маркировку.

Для печати заданий с ненулевой меткой безопасности необходимо соответствующим образом настроить принтер, а также маркеры печати (при необходимости). Описание настройки принтеров, маркеров печати и порядка маркировки приведено в РУСБ.10015-01 97 01-1.

ВНИМАНИЕ! Мандатный контекст задания должен находиться в диапазоне между минимальным и максимальным мандатным контекстом принтера, на который отправлено задание. Если метка безопасности задания ненулевая, но не попадает в множество разрешенных меток для данного принтера, заданных атрибутами `mac-printer-mac-min` и `mac-printer-mac-max`, то задание на печать будет завершено с ошибкой.

ВНИМАНИЕ! Контроль метки целостности работает только для локальных соединений (через Unix Domain Socket). Любому соединению по TCP/IP будет присваиваться нулевая метка целостности. Поэтому для возможности печати с удаленного компьютера необходимо разрешить принтеру печать с нулевой меткой целостности.

Маркировка осуществляется «наложением» маркеров с учетными атрибутами документа, включающими:

- уровень конфиденциальности документа;
- номер экземпляра;
- количество листов в экземпляре;
- дату вывода документа на печать;
- номер каждого входящего документа;
- имя исполнителя;
- имя пользователя, производившего печать.

Система печати является инвариантной по отношению к приложениям, которые обращаются к службе печати. Это означает, что приложения, выводящие на печать, должны учитывать маркировку листов и оставлять для этого свободное место. В противном случае маркеры могут наложиться на фрагменты печатаемой информации.

Маркировка задания выполняется в пять этапов:

1) блокировка задания. Если задание в процессе маркировки другим пользователем или соединением, то выдается ошибка;

2) проверка наличия и установка атрибутов задания;
3) с помощью переменных маркировки запрос у пользователя атрибутов задания;
4) выставление атрибутов задания, полученных на предыдущем этапе;
5) непосредственно маркировка задания.

Маркировка документов при использовании локальной базы осуществляется от имени пользователя, входящего в группу `lpmac`. Если группа отсутствует в системе, она должна быть создана.

Маркировка документов в ЕПП осуществляется от имени доменного пользователя, входящего в локальную группу `lpmac` на сервере печати. Для добавления пользователя в локальную группу `lpmac` необходимо на сервере печати выполнить команду:

```
sudo gpasswd -a ipa_marker_user lpmac
```

Маркировка документа выполняется с помощью инструмента командной строки `markjob`, описанного в 14.5.2, или с помощью графической утилиты `fly-print-station`. Описание использования утилиты `fly-print-station` приведено в электронной справке.

14.5.2. Маркировка документа в командной строке

Маркировка документа в командной строке выполняется с помощью инструмента `markjob`. Инструмент `markjob` требует наличия утилиты `lpq`, входящей в состав пакета `cups-bsd`.

Для маркировки с помощью `markjob` выполнить команду:

```
markjob -m
```

или

```
markjob
```

Подробное описание инструмента `markjob` приведено в `man markjob`.

В процессе работы инструмента `markjob` у пользователя запрашиваются настроенные атрибуты для маркера печати, например:

- `mac-inv-num` — инвентарный номер;
- `mac-owner-phone` — телефон исполнителя;
- `mac-workplace-id` — идентификатор рабочего места;
- `mac-distribution` — список рассылки.

При вводе списка рассылки адреса разделяются символом «^». Если в значении списка рассылки используется пробел, то значение атрибута необходимо взять в кавычки целиком.

Пример

Выдается запрос на ввод списка рассылки:

```
Enter mac-distribution - Distribution list, addresses separated by '^':
```

Ввести список рассылки:

```
"В дело^В адрес"
```

После выполнения маркировки в очереди формируются два дополнительных задания в состояние «отложено»: первое (с меньшим номером) представляет собой промаркированный документ, а второе (с большим номером) — размещаемую на обороте последнего листа документа маркировку.

Для печати промаркированного документа необходимо возобновить печать первого отложенного задания. Затем на обороте последнего листа документа печатается маркировка путем возобновления выполнения второго дополнительного задания.

При выполнении маркировки от имени пользователя, входящего в группу `lpmac`, возможно получение сообщения:

```
Невозможно выполнить запрос: запрещено
```

В данном случае необходимо выполнить команду `id` от имени пользователя, выполняющего маркировку, и повторно запустить инструмент `markjob`.

Если ведение журнала маркировки включено, то после завершения задания данные маркировки будут записаны в него. Описание журнала маркировки приведено в 14.5.4.

14.5.3. Маркировка нескольких экземпляров документа

Для печати нескольких экземпляров документа с ненулевой меткой безопасности пользователь должен отправить на печать только одну копию документа.

Пользователь, осуществляющий маркировку, должен выполнить следующую последовательность действий:

1) получить номер задания для маркировки, выполнив команду:

```
lpq -a
```

2) задать число копий для печати, выполнив команду:

```
lpattr -j <номер_задания> -s copies=<число_копий>
```

3) произвести маркировку с помощью инструмента `markjob` или графической утилиты `fly-print-station`.

После выполнения маркировки в очереди формируются по два дополнительных задания для каждого экземпляра документа, располагаемых в очереди последовательно. Первое (с меньшим номером) представляет собой промаркированный экземпляр документа, а второе (с большим номером) — маркировку, размещаемую на обороте последнего листа экземпляра документа. Для печати экземпляра документа необходимо возобновить выполнение первого соответствующего ему задания, что приведет к печати промаркированного экземпляра документа. Затем на обороте последнего листа экземпляра документа печатается маркировка посредством возобновления выполнения второго соответствующего экземпляру документа дополнительного задания.

14.5.4. Журнал маркировки

Журнал маркировки ведется при установке в конфигурационном файле `/etc/cups/cupsd.conf` для параметра `MacJournal` значения `on`. По умолчанию журнал записывается в базу данных SQLITE `/var/spool/cups/parsec/marking-journal.sqlite`.

Включить журнал маркировки возможно путем редактирования конфигурационного файла или выполнив команду от имени администратора:

```
cupsctl MacJournal=On
```

Просмотр журнала возможен с использованием графической утилиты `fly-print-station` и графической утилиты `fly-admin-printer` с установленным плагином `fly-admin-printer-mac`.

15. ЗАЩИЩЕННАЯ СИСТЕМА УПРАВЛЕНИЯ БАЗАМИ ДАННЫХ

В качестве защищенной СУБД в составе ОС используется СУБД Tantor (в исполнении Basic), доработанной в соответствии с требованием интеграции с ОС в части защиты информации, в том числе мандатного управления доступом.

СУБД предназначена для создания и управления реляционными БД и предоставляет многопользовательский доступ к расположенным в них данным. Данные в реляционной БД хранятся в отношениях (таблицах), состоящих из строк и столбцов. При этом единицей хранения и доступа к данным является строка, состоящая из полей. Каждое поле строки идентифицируется именами столбцов. Кроме таблиц существуют другие объекты БД (виды, процедуры и т. п.), которые предоставляют доступ к данным, хранящимся в таблицах.

Подробное описание настройки и управления защищенной СУБД приведено в документе РУСБ.10015-01 97 01-3. Описание работы пользователя с СУБД приведено в документе РУСБ.10015-01 93 01 «Операционная система специального назначения «Astra Linux Special Edition». Руководство пользователя».

16. ЗАЩИЩЕННЫЙ КОМПЛЕКС ПРОГРАММ ЭЛЕКТРОННОЙ ПОЧТЫ

В качестве защищенного комплекса программ электронной почты используется сервер электронной почты, состоящий из агента передачи электронной почты (Mail Transfer Agent, MTA) Exim4, агента доставки электронной почты (Mail Delivery Agent, MDA) Dovecot и клиента электронной почты (Mail User Agent, MUA) Mozilla Thunderbird.

Защищенный комплекс программ электронной почты доработан для реализации дополнительных функциональных возможностей:

- интеграции с ядром ОС и базовыми библиотеками для обеспечения разграничения доступа;
- реализации мандатного управления доступом к почтовым сообщениям;
- автоматической маркировки создаваемых почтовых сообщений, отражающих уровень их конфиденциальности;
- регистрации попыток доступа к почтовым сообщениям.

Агент передачи электронной почты Exim4 использует протокол SMTP и обеспечивает решение следующих задач:

- доставку исходящей почты от авторизованных клиентов до сервера, который является целевым для обработки почтового домена получателя;
- прием и обработку почтовых сообщений доменов, для которых он является целевым;
- передачу входящих почтовых сообщений для обработки агентом доставки электронной почты.

Агент доставки электронной почты предназначен для обслуживания почтового каталога и предоставления удаленного доступа к почтовому ящику по протоколу IMAP.

Клиент электронной почты — это прикладное ПО, устанавливаемое на рабочем месте пользователя и предназначенное для получения, создания, отправки и хранения сообщений электронной почты пользователя.

16.1. Состав

Защищенный комплекс программ электронной почты состоит из следующих пакетов:

- `exim4-daemon-heavy` — агент передачи сообщений Exim4. Пакет `exim4-daemon-light` не поддерживает работу с классификационными метками, отличными от `0:0`;
- `dovecot-imapd` — агент доставки сообщений Dovecot. Работает только по протоколу IMAP, протокол POP3 отключен. Серверная часть защищенного комплекса

программ электронной почты использует в качестве почтового хранилища MailDir (mailbox не поддерживает работу с классификационными метками, отличными от 0:0);

- thunderbird — клиент электронной почты Mozilla Thunderbird.

16.2. Настройка серверной части

Настройки по умолчанию:

1) прием почтовых сообщений по протоколу SMTP только от MUA из доменов relay-domens и из подсети;

2) отправка почтовых сообщений по протоколу SMTP в соответствии с DNS;

3) хранение локальной почты в MailDir в /var/mail/%u, где %u — локальная часть адресата;

4) выдача локальных почтовых сообщений по протоколу IMAP.

ВНИМАНИЕ! Для обеспечения нормальной работы пользователя с сетевыми службами должна быть явно задана его классификационная метка (диапазон уровней конфиденциальности и категорий конфиденциальности) с помощью соответствующих утилит, даже если ему не доступны уровни и категории выше 0. Дополнительная информация приведена в документе РУСБ.10015-01 97 01-1.

Редактирование конфигурационных файлов и выполнение команд по настройке необходимо выполнять от имени учетной записи администратора с использованием механизма sudo.

16.2.1. Настройка агента доставки сообщений

Настройка агента доставки сообщений Dovecot осуществляется путем правки конфигурационного файла /etc/dovecot/dovecot.conf и конфигурационных файлов в каталоге /etc/dovecot/conf.d.

В файле /etc/dovecot/dovecot.conf необходимо задать список интерфейсов, с которых будут приниматься соединения, и установить протокол IMAP, например:

```
protocols = imap
listen =  192.168.2.55
```

Для настройки аутентификации с использованием PAM в конфигурационном файле /etc/dovecot/conf.d/10-auth.conf необходимо установить:

```
disable_plaintext_auth = no
auth_mechanisms = plain
```

Агент доставки сообщений Dovecot для PAM-аутентификации использует сценарий PAM, содержащийся в конфигурационном файле `/etc/pam.d/dovecot`. PAM-сценарий для Dovecot включает `common-auth` и `common-account`. По умолчанию в ОС для фиксации числа неуспешных попыток входа пользователей применяется PAM-модуль `pam_faillock`. Увеличение счетчика неуспешных попыток входа пользователя при начале процесса аутентификации обеспечивает использование `pam_faillock` в секции `auth` в файле `/etc/pam.d/common-auth`. Для сброса счетчика неуспешных попыток входа пользователя после успешной аутентификации в Dovecot необходимо в конфигурационном файле `/etc/pam.d/dovecot` в сценарий PAM для секции `account` добавить использование `pam_faillock`. PAM-сценарий для Dovecot будет иметь следующий вид:

```
@include common-auth
@include common-account
@include common-session
account required pam_faillock.so
```

Для вывода информации о неуспешных попытках входа следует выполнить команду:

```
sudo faillock
```

В случае когда SSL не будет использоваться в конфигурационном файле `/etc/dovecot/conf.d/10-ssl.conf`, необходимо установить:

```
ssl = no
```

Для настройки встроенного в MDA Dovecot сервера SASL, к которому будет обращаться MTA Exim4 для аутентификации пользователей, в конфигурационном файле `/etc/dovecot/conf.d/10-master.conf` в секцию `service auth` необходимо добавить:

```
unix_listener auth-client {
mode = 0600
user = Debian-exim
}
```

Перезапустить MDA Dovecot, выполнив команду:

```
sudo systemctl restart dovecot
```

16.2.2. Настройка агента передачи сообщений

Для настройки агента передачи сообщений Exim4 требуется инициировать переконфигурирование пакета `exim4-config`, для этого выполнить в эмуляторе терминала команду:

```
sudo dpkg-reconfigure exim4-config
```

В появившемся окне настройки для указанных ниже параметров необходимо установить следующие значения:

1) «Общий тип почтовой конфигурации» — выбрать пункт «интернет-сайт; прием и отправка почты напрямую, используя SMTP»;

2) «Почтовое имя системы» — ввести имя домена;

3) «IP-адреса, с которых следует ожидать входящие соединения» — ввести IP-адрес сервера;

4) «Другие места назначения, для которых должна приниматься почта» — ввести имя домена;

5) «Домены, для которых доступна релейная передача почты» — оставить пустым;

6) «Машины, для которых доступна релейная передача почты» — оставить пустым;

7) «Сокращать количество DNS-запросов до минимума» — выбрать пункт «Нет»;

8) «Метод доставки локальной почты» — выбрать пункт «Maildir формат в /var/mail/»;

9) «Разделить конфигурацию на маленькие файлы» — выбрать пункт «Да»;

10) «Получатель почты, адресованной root и postmaster» — ввести имя учетной записи, которая будет получать сообщения, адресованные указанным пользователям.

При необходимости изменить каталог хранения временных файлов почты `/var/spool/exim4/` на другой каталог (например, `/newspool/`) можно следующим образом:

1) открыть терминал и запустить консоль от имени пользователя `root`, выполнив команду:

```
sudo -i
```

2) создать новый каталог, выполнив команду:

```
mkdir /newspool
```

3) скопировать содержимое каталога `/var/spool/exim4/` в новое расположение с сохранением прав доступа, выполнив команду:

```
cp -a /var/spool/exim4/* /newspool/
```

4) перейти в созданный каталог, выполнив команду:

```
cd /newspool
```

5) установить на каталог /newspool/ и его содержимое такую же метку безопасности, как и у исходного каталога, выполнив команду:

```
pdpl-file $(pdpl-file /var/spool/exim4) . db input msglog db/\
   retry db/retry.lockfile
```

6) закрыть консоль пользователя root, выполнив команду:

```
exit
```

7) в файле /etc/exim4/conf.d/main/02_exim4-config_options в качестве значения параметра SPOOLDIR указать путь к новому каталогу хранения временных файлов почты:

```
SPOOLDIR = /newspool
```

8) перезапустить службу exim4, выполнив команду:

```
sudo systemctl restart exim4
```

При необходимости изменить каталог хранения почтовых сообщений /var/mail/ на другой каталог (например, /newmail/) можно следующим образом:

1) создать новый каталог, выполнив команду:

```
sudo mkdir /newmail
```

2) установить на созданный каталог права 1777, выполнив команду:

```
sudo chmod 1777 /newmail
```

3) установить на созданный каталог такую же метку безопасности, как и у исходного каталога, выполнив команду:

```
sudo pdpl-file $(sudo pdpl-file /var/mail) /newmail
```

4) в файле /etc/exim4/conf.d/transport/30_exim4-config_mail_spool изменить значение параметра file, указав путь к созданному каталогу перед переменной $local_part или $local_part_data:

```
file = /newmail/$local_part_data
```

5) в файле /etc/exim4/conf.d/transport/30_exim4-config_maildir_home изменить значения параметров directory и current_directory, указав путь к созданному каталогу перед переменной $local_part или $local_part_data:

```
directory = /newmail/$local_part_data
current_directory = /newmail/$local_part_data
```

6) в конфигурационном файле `/etc/exim4/conf.d/router/mmm_mail4root` для параметра `data` установить следующее значение:

```
data = /newmail/mail
```

7) в конфигурационном файле `/etc/dovecot/conf.d/10-mail.conf` для параметра `mail_location` установить следующее значение:

```
mail_location = maildir:/newmail/%u
```

8) перезапустить службы `exim4` и `dovecot`:

```
sudo systemctl restart dovecot
sudo systemctl restart exim4
```

ВНИМАНИЕ! После изменения каталога хранения почтовых сообщений будет потеряна вся существующая переписка. Для пользователей с ранее настроенной учетной записью сервера электронной почты при подключении к почтовому серверу будут автоматически созданы новые пустые почтовые ящики, а почтовые ящики на компьютерах пользователей будут очищены.

Для штатной работы `exim4-daemon-heavy` необходимо удалить файлы, созданные в каталоге `/var/mail` при установке пакета.

В каталоге `/etc/exim4/conf.d/auth` необходимо создать файл с именем `05_dovecot_login` и следующим содержимым:

```
dovecot_plain:
driver = dovecot
public_name = plain
server_socket = /var/run/dovecot/auth-client
server_set_id = $auth1
```

Для запрета отправки писем без аутентификации необходимо в конфигурационном файле `/etc/exim4/conf.d/acl/30_exim4-config_check_rcpt` в начало секции `acl_check_rcpt` добавить строки:

```
deny
message = "Auth required"
hosts = *:+relay_from_hosts
!authenticated = *
```

Настройку сквозной аутентификации для сервера и клиента, работающих в рамках ЕПП, см. в 16.4.

Настроить автоматический запуск службы MTA Exim4, выполнив команду:

```
sudo systemctl enable exim4
```

Перезапустить MTA Exim4, выполнив команду:

```
sudo systemctl restart exim4
```

16.3. Настройка клиентской части

Первичное создание для пользователя учетной записи сервера электронной почты в MUA Mozilla Thunderbird должно производиться с нулевой классификационной меткой (значение уровня конфиденциальности `0`, категорий конфиденциальности нет). Далее для каждой конкретной классификационной метки (значение уровня и набор категорий) создание учетной записи необходимо повторить.

При создании учетной записи пользователя в MUA Mozilla Thunderbird необходимо выбрать тип используемого сервера входящей почты IMAP.

При настройке учетной записи установить в параметрах сервера и параметрах сервера исходящей почты:

- «Защита соединения» — из выпадающего списка выбрать «Нет»;
- «Метода аутентификации» — выбрать «Обычный пароль».

16.4. Настройка для работы со службой FreeIPA

Для обеспечения совместной работы сервера электронной почты с FreeIPA должны быть установлены:

- агент передачи сообщений Exim4 — из пакета `exim4-daemon-heavy`;
- агент доставки сообщений Dovecot — из пакета `dovecot-imapd`;
- пакет `dovecot-gssapi` поддержки GSSAPI-аутентификации для MDA Dovecot;
- клиент Mozilla Thunderbird — из пакета `thunderbird`.

Для настройки совместной работы сервера электронной почты с FreeIPA должно быть предварительно выполнено:

- установлен сервер контроллера домена FreeIPA (например, домен `astra.mta`);
- на отдельном компьютере установлен почтовый сервер, введенный в домен FreeIPA (например, сервер `exim1.astra.mta` с IP-адресом `192.168.32.3`).

ВНИМАНИЕ! Имена доменных пользователей, для которых будут настраиваться почтовые клиенты, не должны совпадать с именами локальных пользователей компьютеров, входящих в домен.

16.4.1. Настройка почтового сервера

Установить на почтовом сервере необходимые пакеты следующей командой:

```
sudo apt install exim4-daemon-heavy dovecot-imapd dovecot-gssapi
```

При установке пакетов `dovecot-imapd` и `dovecot-gssapi` создается файл `/etc/dovecot/conf.d/10-master.conf`. В секции `service auth` этого файла необходимо добавить следующие строки:

```
unix_listener auth-client {
mode = 0600
user = Debian-exim
}
```

После внесения изменений следует выполнить команду для реконфигурации Exim:

```
sudo dpkg-reconfigure exim4-config
```

В появившемся окне настройки для указанных ниже параметров необходимо установить следующие значения:

1) «Общий тип почтовой конфигурации» — выбрать пункт «доставка только локальной почты; доступа к сети нет»;
2) «Почтовое имя системы» — ввести имя домена, например «astra.mta»;
3) «IP-адреса, с которых следует ожидать входящие соединения» — указать IP-адрес сервера или оставить поле пустым;
4) «Другие места назначения, для которых должна приниматься почта» — ввести имя домена, например «astra.mta»;
5) «Машины, для которых доступна релейная передача почты» — указать IP-адреса, например «192.168.32.0/24»;
6) «Сокращать количество DNS-запросов до минимума» — выбрать пункт «Нет»;
7) «Метод доставки локальной почты» — выбрать пункт «Maildir формат в /var/mail/»;
8) «Разделить конфигурацию на маленькие файлы» — выбрать пункт «Да».

В журнале Exim (файл /var/log/exim4/paniclog) могут появляться сообщения об ошибках вида:

```
Failed to create spool file /var/spool/exim4//input//1jb2ok-00031u-5R-D:
Operation not permitted
```

В этом случае следует исправить права доступа к каталогу /var/spool/exim4:

```
sudo chown -R Debian-exim:Debian-exim /var/spool/exim4/
```

Для указания корректного почтового имени сервера выполнить команду:

```
sudo hostname -f | sudo tee /etc/mailname
```

Если в конфигурационном файле /etc/sssd/sssd.conf параметр use_fully_qualified_names имеет значение True, то выполнить следующее:

1) в файле /etc/sssd/sssd.conf в разделе [sssd] после строки с параметром domains добавить строку с указанием домена:

```
default_domain_suffix = astra.mta
```

2) остановить службу sssd, выполнив команду:

```
sudo systemctl stop sssd
```

3) удалить содержимое каталога /var/lib/sss/db/;

4) запустить службу sssd, выполнив команду:

```
sudo systemctl start sssd
```

5) в файле /etc/exim4/conf.d/transport/30_exim4-config_maildir_home в параметрах directory и current_directory изменить переменные в конце значений с $local_part_data на $local_part_data@$domain_data:

```
directory = /var/mail/$local_part_data@$domain_data
current_directory = /var/mail/$local_part_data@$domain_data
```

6) перезапустить MTA Exim4, выполнив команду:

```
sudo systemctl restart exim4
```

16.4.2. Регистрация почтовых служб на контроллере домена

На контроллере домена необходимо добавить принципалов служб:

- `imap/exim1.astra.mta@ASTRA.MTA`
- `smtp/exim1.astra.mta@ASTRA.MTA`

Это можно сделать через веб-интерфейс FreeIPA, перейдя «Идентификация — Службы» и нажав кнопку **[Добавить]** (см. рис. 12).

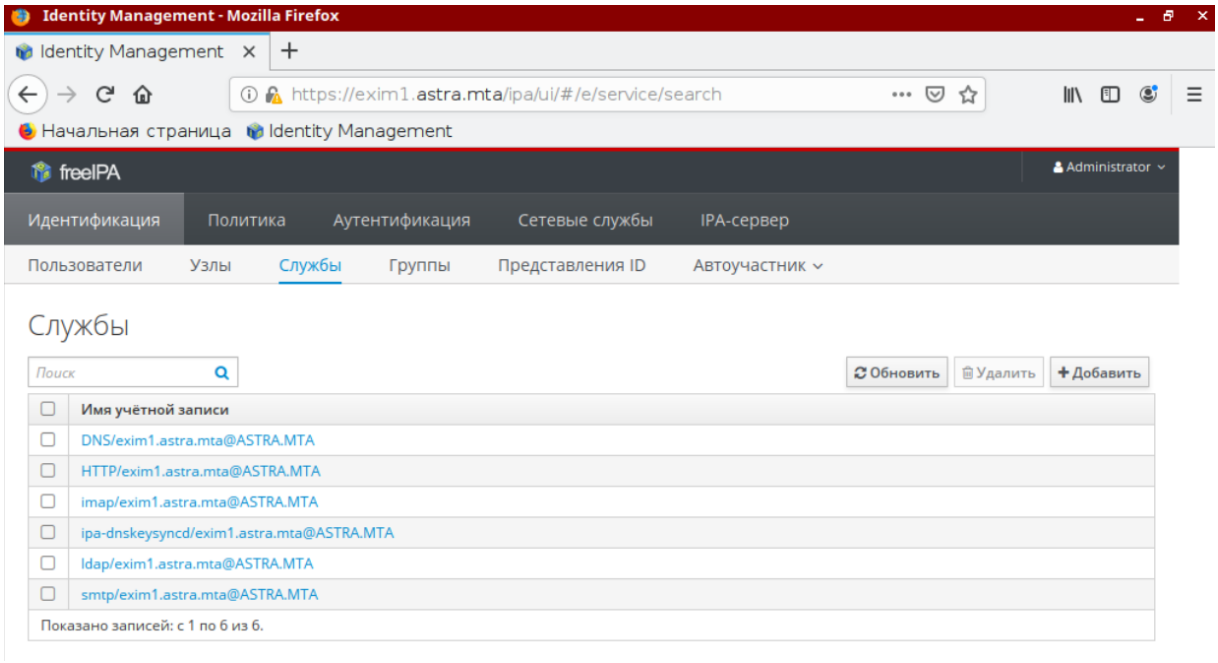

Рис. 12

Также данное действие возможно выполнить из командной строки, предварительно получив полномочия администратора домена:

```
sudo kinit admin
sudo ipa service-add imap/exim1.astra.mta@ASTRA.MTA
sudo ipa service-add smtp/exim1.astra.mta@ASTRA.MTA
```

16.4.3. Получение таблицы ключей на почтовом сервере

На почтовом сервере следует получить таблицу ключей для службы `imap`, затем добавить таблицу ключей для службы `smtp`:

```
sudo kinit admin
sudo ipa-getkeytab --principal=imap/exim1.astra.mta@ASTRA.MTA \
     --keytab=/var/lib/dovecot/dovecot.keytab
sudo ipa-getkeytab --principal=smtp/exim1.astra.mta@ASTRA.MTA \
```

```
--keytab=/var/lib/dovecot/dovecot.keytab
```

Проверить полученную таблицу ключей:

```
sudo klist -k /var/lib/dovecot/dovecot.keytab
```

Вывод в терминале будет иметь следующий вид:

```
Keytab name: FILE:/var/lib/dovecot/dovecot.keytab
KVNO Principal
----------------------------------------------------------------------------
1 imap/exim1.astra.mta@ASTRA.MTA
1 imap/exim1.astra.mta@ASTRA.MTA
1 smtp/exim1.astra.mta@ASTRA.MTA
1 smtp/exim1.astra.mta@ASTRA.MTA
```

После этого следует выдать пользователю `dovecot` права на чтение файла ключа Kerberos:

```
sudo setfacl -m u:dovecot:x /var/lib/dovecot
sudo setfacl -m u:dovecot:r /var/lib/dovecot/dovecot.keytab
```

Далее убедиться, что в конфигурационном файле `/etc/dovecot/dovecot.conf` отключено использование протоколов POP3, и отключить неиспользуемые протоколы, оставив только IMAP:

```
protocols = imap
```

После этого следует выполнить настройки в конфигурационном файле `/etc/dovecot/conf.d/10-auth.conf`:

- для отключения передачи при аутентификации пароля открытым текстом установить:

```
disable_plaintext_auth = yes
```

- для настройки аутентификации посредством Kerberos с использованием метода GSSAPI установить:

```
auth_gssapi_hostname = exim1.astra.mta
auth_krb5_keytab = /var/lib/dovecot/dovecot.keytab
auth_mechanisms = gssapi
```

Затем перезапустить Dovecot:

```
sudo systemctl restart dovecot
```

16.4.4. Настройка аутентификации через Kerberos

Для настройки аутентификации в Exim следует создать конфигурационный файл `/etc/exim4/conf.d/auth/33_exim4-dovecot-kerberos-ipa` со следующим содержимым:

```
dovecot_gssapi:
driver = dovecot
public_name = GSSAPI
server_socket = /var/run/dovecot/auth-client
server_set_id = $auth1
```

Далее запустить сервер Exim и разрешить его автоматический запуск после перезагрузки:

```
sudo systemctl start exim4
sudo systemctl enable exim4
```

После настройки аутентификации через Kerberos в домене FreeIPA требуется настройка параметров почтового сервера (параметров пересылки почты) и настройка клиентской части на клиентах.

17. СРЕДСТВА АУДИТА И ЦЕНТРАЛИЗОВАННОГО ПРОТОКОЛИРОВАНИЯ

17.1. Аудит

В ОС отправка и регистрация информации о событиях в системе осуществляется в соответствии со стандартом Syslog. Стандарт определяет формат сообщений о событиях и правила их передачи и регистрации в журналах. Основное расположение файлов журналов — системный каталог `/var/log`.

Аудит основных системных событий с момента запуска ОС ведется в системном журнале `/var/log/syslog`.

Аудит событий постановки/снятия с контроля целостности исполняемых модулей и файлов данных, а также событий неудачного запуска неподписанных файлов осуществляется в журнале ядра `/var/log/kern.log`.

Аудит событий создания/удаления/изменения настроек учетных записей пользователей и начала/окончания сеансов работы учетных записей пользователей осуществляется в журнале `/var/log/auth.log`.

Аудит событий изменения для учетных записей полномочий по доступу к информации осуществляется в журнале `/var/log/auth.log`.

Аудит событий смены аутентифицирующей информации учетных записей осуществляется в журнале `/var/log/auth.log`.

Аудит событий вывода текстовых (графических) документов на бумажный носитель осуществляется в журнале `/var/log/cups/page_log`.

Для аудита ОС также могут использоваться журналы различных служб и программ.

Для регистрации событий безопасности в ОС используется служба аудита `auditd`, описание которой приведено в РУСБ.10015-01 97 01-1, и подсистема регистрации событий (см. 17.2).

17.2. Подсистема регистрации событий

В ОС реализована подсистема регистрации событий, которая собирает информацию о событиях, выполняет ее регистрацию и предоставляет инструменты для просмотра собранных данных и реагирования на события. Регистрация событий безопасности выполняется с учетом требований ГОСТ Р 59548-2022.

Сбор и регистрацию событий осуществляет служба `syslog-ng`. Служба `syslog-ng` принимает информацию о событиях из различных источников (события от `auditd`, собственные подключаемые модули, файлы, прикладное ПО и др.), выполняет фильтрацию и обработ-

ку полученных данных, регистрирует события в журнал `/parsec/log/astra/events`, а также, в зависимости от конфигурации, может сохранять в файл, отправлять по сети и т. д.

Для управления подсистемой регистрации событий из терминала используются инструменты командной строки `astra-admin-events` и `astra-event-viewer`. Порядок использования инструментов приведен на соответствующих страницах помощи:

```
astra-admin-events -h
astra-event-viewer -h
```

Для управления подсистемой регистрацией событий в графическом интерфейсе используются графические утилиты `fly-admin-events` («Настройка регистрации системных событий») и `fly-event-viewer` («Журнал системных событий»). Описание использования утилит приведено в электронной справке.

Информирование (оповещение) о событиях осуществляется с помощью утилиты `fly-notifications` («Центр уведомлений»). Описание утилиты приведено в электронной справке.

Подробное описание подсистемы регистрации событий приведено в РУСБ.10015-01 97 01-1.

17.3. Средство распределенного мониторинга Zabbix

Для решения задач централизованного протоколирования и анализа журналов аудита, а также организации распределенного мониторинга сети, жизнеспособности и целостности серверов используется программное решение Zabbix, реализованное на веб-сервере Apache, СУБД (MySQL, Oracle, PostgreSQL, SQLite) и языке сценариев PHP.

Zabbix предоставляет гибкий механизм сбора данных. Все отчеты и статистика Zabbix, а также параметры настройки компонентов Zabbix доступны через веб-интерфейс. В веб-интерфейсе реализован следующий функционал:

- вывод отчетности и визуализация собранных данных;
- создание правил и шаблонов мониторинга состояния сети и узлов;
- определение допустимых границ значений заданных параметров;
- настройка оповещений;
- настройка автоматического реагирования на события безопасности.

17.3.1. Архитектура

Zabbix состоит из следующих основных программных компонентов:

1) сервер — является основным компонентом, который выполняет мониторинг, взаимодействует с прокси и агентами, вычисляет триггеры, отправляет оповещения. Является главным хранилищем данных конфигурации, статистики, а также оперативных данных;

2) агенты — разворачиваются на наблюдаемых системах для активного мониторинга за локальными ресурсами и приложениями и для отправки собранных данных серверу или прокси;

3) прокси — может собирать данные о производительности и доступности от имени сервера. Прокси является опциональной частью Zabbix и может использоваться для снижения нагрузки на сервер;

4) база данных — вся информация о конфигурации, а также собранные Zabbix данные, хранятся в базе данных;

5) веб-интерфейс — используется для доступа к Zabbix из любого места и с любой платформы.

17.3.2. Сервер

Сервер Zabbix обеспечивает мониторинг различных метрик серверного и сетевого оборудования, рабочих станций, системных служб и приложений.

В общем случае сбор данных и отправку их на сервер осуществляет агент, установленный на узле, мониторинг которого осуществляется. Также для сбора данных могут использоваться интерфейсы SNMP, JMX, IPMI.

Сервер Zabbix обеспечивает выполнение действий при определенных событиях мониторинга в виде отправки оповещений пользователям и/или выполнения заданных команд (сценариев) на контролируемых узлах.

17.3.2.1. Установка сервера

Для развертывания сервера Zabbix в конфигурации с СУБД и веб-сервером Apache на одном узле требуется установить следующие пакеты (перед установкой проверить настройку доступа к репозиториям в соответствии с 5.2.1):

```
sudo apt install zabbix-server-pgsql zabbix-frontend-php php-pgsql
```

17.3.2.2. Настройка сервера для работы в условиях мандатного управления доступом и МКЦ

Для обеспечения возможности функционирования сервера Zabbix в условиях мандатного управления доступом и МКЦ требуется:

1) назначить метки безопасности служебным пользователям `postgres` (нулевую классификационную метку и максимальную категорию целостности) и `zabbix` (нулевую классификационную метку, категорию целостности не назначать):

```
sudo pdpl-user -l 0:0 -i 63 postgres
sudo pdpl-user -l 0:0 zabbix
```

2) предоставить служебному пользователю `postgres` право чтения БД меток безопасности локальных пользователей:

```
sudo setfacl -d -m u:postgres:r /etc/parsec/{macdb,capdb}
sudo setfacl -R -m u:postgres:r /etc/parsec/{macdb,capdb}
sudo setfacl -m u:postgres:rx /etc/parsec/{macdb,capdb}
```

17.3.2.3. Настройка сервера

В общем случае для настройки Zabbix со значениями параметров по умолчанию требуется настроить СУБД, веб-сервер Apache и веб-интерфейс Zabbix.

Настроить СУБД для хранения данных Zabbix:

1) в файле `/etc/postgresql/<версия_СУБД>/main/pg_hba.conf` добавить строки с именем БД для хранения данные Zabbix (например, `zabbix`) и СУБД-пользователя для обращения к данной БД (например, `zabbix`):

```
# TYPE   DATABASE   USER         ADDRESS          METHOD

local    zabbix     zabbix                        trust

# IPv4 local connections:

host     zabbix     zabbix      127.0.0.1/32      trust
```

2) перезапустить службу СУБД:

```
sudo systemctl restart postgresql
```

3) запустить интерактивный терминал `psql` от имени пользователя `postgres`:

```
sudo -u postgres psql
```

и выполнить следующие команды:

а) создать БД zabbix и СУБД-пользователя zabbix, которые были указаны в конфигурационном файле, см. пункт 1) перечисления:

```
CREATE DATABASE zabbix;
CREATE USER zabbix WITH ENCRYPTED PASSWORD '<пароль_СУБД-пользователя_zabbix>';
```

б) предоставить СУБД-пользователю zabbix полные права доступа к БД zabbix и назначить его владельцем БД zabbix:

```
GRANT ALL ON DATABASE zabbix TO zabbix;
ALTER DATABASE zabbix OWNER TO zabbix;
```

в) выйти из терминала psql:

```
\q
```

4) заполнить БД zabbix на основе шаблонов Zabbix, выполнив команду:

```
zcat /usr/share/zabbix-server-pgsql/{schema,images,data}.sql.gz | psql -h \
    localhost zabbix zabbix
```

на запрос системы ввести пароль СУБД-пользователя zabbix;

5) в конфигурационном файле /etc/zabbix/zabbix_server.conf раскомментировать параметр DBPassword и указать в качестве значения пароль СУБД-пользователя zabbix:

```
DBPassword=<пароль_СУБД-пользователя_zabbix>
```

Если при настройке СУБД были заданы другие имя БД и пользователь СУБД, а также при необходимости изменить настройки сервера по умолчанию, то следует отредактировать и другие параметры (описание параметров конфигурационного файла приведено в 17.3.2.4).

Настроить веб-сервер Apache:

1) отключить режим работы AstraMode (см. 11.2) веб-сервера Apache, для этого в конфигурационном файле /etc/apache2/apache2.conf раскомментировать строку параметра AstraMode и указать значение off:

```
AstraMode off
```

2) настроить часовой пояс, с учетом которого будут отображаться данные в веб-интерфейсе, для этого в конфигурационном файле /etc/php/<версия>/apache2/php.ini раскомментировать строку date.timezone и в качестве значения указать временную зону:

```
[Date]
date.timezone = Europe/Moscow
```

Примечание. По умолчанию Zabbix работает с временными метками в формате UTC;

3) перезапустить службу веб-сервера Apache:

```
sudo systemctl restart apache2
```

Инициализировать конфигурацию веб-интерфейса сервера Zabbix, для этого:

1) создать конфигурационный файл /etc/zabbix/zabbix.conf.php из шаблона:

```
sudo cp /usr/share/zabbix/conf/zabbix.conf.php.example \
    /etc/zabbix/zabbix.conf.php
```

2) служебному пользователю www-data веб-сервера Apache предоставить права доступа к файлу /etc/zabbix/zabbix.conf.php:

```
sudo chown www-data:www-data /etc/zabbix/zabbix.conf.php
```

3) в файле /etc/zabbix/zabbix.conf.php указать значения для переменных TYPE (тип СУБД) и PASSWORD (пароль СУБД-пользователя zabbix):

```
$DB['TYPE'] = 'POSTGRESQL';
...
$DB['PASSWORD'] = '<пароль_СУБД-пользователя_zabbix>';
```

4) применить конфигурацию веб-интерфейса Zabbix в веб-сервере Apache:

```
sudo a2enconf zabbix-frontend-php
```

5) перезапустить службы сервера Zabbix и веб-сервера Apache:

```
sudo systemctl restart zabbix-server
sudo systemctl restart apache2
```

Порядок доступа к веб-интерфейсу Zabbix приведен в 17.3.5.

Сервер Zabbix функционирует в ОС как служба zabbix-server. Управление службой осуществляется в соответствии с 4.2.1.

17.3.2.4. Конфигурационные параметры сервера

Параметры работы сервера Zabbix настраиваются в конфигурационном файле /etc/zabbix/zabbix_server.conf.

После изменения конфигурационного файла перезапустить службу сервера.

Основные параметры конфигурационного файла сервера приведены в таблице 67.

Таблица 67

Параметр	Описание
AllowRoot	Разрешение запускать службу сервера от имени пользователя root (значение 0 — запрещено, значение 1 — разрешено). Если задано значение 0 (запрещено), но выполняется попытка запуска службы сервера от имени root, тогда сервер автоматически попробует запустить службу от имени пользователя, указанного в параметре User. Значение по умолчанию 0. Если настроен запуск службы сервера от имени пользователя, отличного от root, то параметр не применяется
CacheSize	Размер кеша для хранения данных мониторинга. Указывается в байтах (B), килобайтах (K), мегабайтах (M) или гигабайтах (G), возможные значения от 128 КБ до 64 ГБ. Значение по умолчанию 32 МБ
CacheUpdateFrequency	Частота обновления кеша с данными мониторинга. Указывается в секундах, возможные значения от 1 до 3600 сек. Значение по умолчанию 60 сек.
DBHost	Имя узла, на котором размещена БД Zabbix. Значение по умолчанию localhost (используется локальное подключение) — сервер Zabbix и БД располагаются на одном узле. В случае отсутствия значения также будет использоваться локальное подключение
DBName	Имя БД Zabbix. Обязательный параметр. Значение по умолчанию zabbix
DBUser	Пользователь для подключения к БД Zabbix. Значение по умолчанию zabbix
DBPassword	Пароль пользователя для доступа к БД Zabbix
DBPort	Порт для подключения к БД Zabbix, если не используется localhost (см. параметр DBHost)
DBSchema	Указывает имя схемы базы данных, которая будет использоваться Zabbix для доступа к своим таблицам и данным
HousekeepingFrequency	Частота выполнения автоматической очистки базы данных от устаревшей информации. Задается в часах, возможные значения от 0 до 24 ч. Значение по умолчанию 1 ч.
LogFile	Имя файла журнала. Обязательный параметр, если способ ведения журнала file (параметр LogType=file). Значение по умолчанию /var/log/zabbix-server/zabbix_server.log
LogType	Способ ведения журнала: - file — запись журнала в файл, указанный в параметре LogFile; - system — запись журнала в syslog; - console — запись журнала в стандартный вывод
User	Указанный служебный пользователь будет использоваться для запуска службы сервера при попытке запустить службу сервера от имени пользователя root при установленном запрете на запуск от имени root (параметр AllowRoot=0). Значение по умолчанию zabbix

17.3.3. Агенты

17.3.3.1. Установка агента

Для установки и настройки агента Zabbix выполнить следующие действия:

1) установить пакет (перед установкой проверить настройку доступа к репозиториям в соответствии с 5.2.1):

```
sudo apt install zabbix-agent
```

2) в конфигурационном файле `/etc/zabbix/zabbix_agentd.conf` для параметра `Server` указать IP-адрес или доменное имя сервера Zabbix (для выполнения пассивных проверок):

```
Server=<IP-адрес_или_имя_сервера_Zabbix>
```

Примечание. Более подробное описание настройки серверов Zabbix для агента приведено в 17.3.3.2.

3) перезапустить службу агента Zabbix:

```
sudo systemctl restart zabbix-agent
```

После запуска службы агента на узле требуется зарегистрировать данный узел на сервере Zabbix, для этого перейти в веб-интерфейс Zabbix и выполнить настройки:

1) на боковой панели перейти «Мониторинг — Узлы сети»;
2) на открывшейся странице нажать **[Создать узел сети]**;
3) в открывшемся окне:
   а) в поле «Имя узла сети» указать краткое имя добавляемого узла (оно должно быть уникальным в веб-интерфейсе Zabbix);
   б) в поле «Группы» выбрать группы, в которые будет включен узел (в дальнейшем их возможно будет изменить);
   в) активировать строку «Интерфейсы» — нажать на ссылку «Добавить» и в раскрывшемся списке выбрав «Агент»;
   г) в поле «IP-адрес» ввести IP-адрес узла с установленным агентом;
   д) в поле «Порт» указать порт в случае, если на узле с агентом в конфигурационном файле `/etc/zabbix/zabbix_agentd.conf` было изменено значение параметра `ListenPort`;
   е) остальные поля заполнить при необходимости (например, если в конфигурационном файле агента задано для параметров `Server` и/или `ServerActive` указаны прокси, то необходимо из выпадающего списка «Наблюдение через прокси» выбрать соответствующий прокси);
4) нажать **[Добавить]**.

17.3.3.2. Настройка агента

Агент выполняет мониторинг и передает данные серверу в соответствии с заданными шаблонами с элементами данных. Для начала сбора данных агентом требуется в веб-интерфейсе Zabbix в настройках соответствующего узла выбрать шаблоны с элементами данными для мониторинга.

Агенты могут выполнять пассивные и активные проверки. При пассивной проверке сервер (или прокси) Zabbix отправляет запрос с элементами данных, агент передает состояние по запрашиваемым данным. При активной проверке агент получает от сервера перечень элементов данных для мониторинга, затем осуществляет сбор данных согласно полученному перечню и периодически отправляет собранные данные серверу (или прокси) Zabbix.

Какие проверки должен выполнять агент (пассивные или активные) — определяется параметром «Тип» у элемента данных: тип «Zabbix агент» для пассивных проверок, тип «Zabbix агент (активный)» для активных проверок. Тип элемента данных настраивается в веб-интерфейсе Zabbix.

Для выполнения активной или пассивной проверки следует соответственно настроить агент. Пассивные проверки были настроены при установке агента согласно 17.3.3.1 (указан сервер для пассивных проверок). Для настройки активных проверок следует в конфигурационном файле `/etc/zabbix/zabbix_agentd.conf` указать значения соответствующих параметров.

Описание параметров конфигурационного файла агента для настройки активных проверок, а также для других настроек, приведено в таблице 68.

Таблица 68

Параметр	Описание
`AllowRoot`	Разрешение запускать службу агента от имени пользователя `root` (значение 0 — запрещено, значение 1 — разрешено). Если задано значение 0 (запрещено), но выполняется попытка запуска службы агента от имени `root`, тогда агент автоматически попробует запустить службу от имени пользователя, указанного в параметре `User`. Значение по умолчанию 0. Если настроен запуск службы агента от имени пользователя, отличного от `root`, то параметр не применяется
`Hostname`	Уникальное регистрозависимое имя агента. Обязательный параметр для активных проверок. Значение должно совпадать с именем узла сети, указанным в веб-интерфейсе Zabbix
`ListenIP`	Список IP-адресов, разделенных запятой, которые агент должен слушать
`ListenPort`	Порт, который необходимо слушать для подключений с сервера (прокси). Значение по умолчанию 10050

Окончание таблицы 68

Параметр	Описание
LogFile	Имя файла журнала. Обязательный параметр, если способ ведения журнала file (LogType=file). Значение по умолчанию /var/log/zabbix-agent/zabbix_agentd.log
LogType	Способ ведения журнала: - file — запись журнала в файл, указанный в параметре LogFile; - system — запись журнала в syslog; - console — запись журнала в стандартный вывод
StartAgents	Количество запущенных экземпляров агента Zabbix, которые агент может использовать для обработки входящих запросов от сервера (прокси) Zabbix (для пассивных проверок). Если установить значение 0, то пассивные проверки выполняться не будут. Значение по умолчанию 3. Если параметр Server не задан (пассивные проверки не выполняются), то данный параметр необходимо раскомментировать и задать значение 0
Server	Список IP-адресов или имен серверов (прокси) Zabbix, разделенных запятой, для пассивных проверок. Пассивные проверки инициируются сервером (прокси) Zabbix путем отправки запроса агенту. Агент будет принимать входящие соединения только с серверов (прокси), указанных в параметре. Обязательный параметр, если параметр StartAgents закомментирован или имеет значение отличное от 0
ServerActive	Список IP-адресов или имен серверов (прокси) Zabbix, разделенных запятой, для активных проверок. Активные проверки инициируются агентом. Агент будет передавать данные и запрашивать задания только от серверов (прокси), указанных в параметре
User	Указанный служебный пользователь будет использоваться для запуска службы агента при попытке запустить службу агента от имени пользователя root при установленном запрете на запуск от имени root (параметр AllowRoot=0). Значение по умолчанию zabbix

После изменения конфигурационного файла перезапустить службу агента:

```
sudo systemctl restart zabbix-agent
```

Агент Zabbix функционирует в ОС как служба zabbix-agent. Управление агентом осуществляется в соответствии с 4.2.1.

17.3.4. Прокси

Прокси является опциональным компонентом Zabbix и может использоваться для снижения нагрузки на сервер Zabbix. Прокси требуется только одно TCP-соединение к серверу Zabbix

для передачи собранных данных. Каждый прокси использует собственную БД для сбора и хранения данных.

Прокси только собирает данные от агентов и (в отличие от сервера Zabbix) не вычисляет триггеры, не обрабатывает события и не отправляет оповещения.

17.3.4.1. Установка прокси

Для развертывания прокси Zabbix в конфигурации с СУБД и веб-сервером Apache на одном узле требуется установить следующий пакет (перед установкой проверить настройку доступа к репозиториям в соответствии с 5.2.1):

```
sudo apt install zabbix-proxy-pgsql
```

17.3.4.2. Настройка прокси для работы в условиях мандатного управления доступом и МКЦ

Для обеспечения возможности функционирования прокси Zabbix в условиях мандатного управления доступом и МКЦ требуется:

1) назначить метки безопасности служебным пользователям `postgres` (нулевую классификационную метку и максимальную категорию целостности) и `zabbix` (нулевую классификационную метку, категорию целостности не назначать):

```
sudo pdpl-user -l 0:0 -i 63 postgres
sudo pdpl-user -l 0:0 zabbix
```

2) предоставить служебному пользователю `postgres` право чтения БД меток безопасности локальных пользователей:

```
sudo setfacl -d -m u:postgres:r /etc/parsec/{macdb,capdb}
sudo setfacl -R -m u:postgres:r /etc/parsec/{macdb,capdb}
sudo setfacl -m u:postgres:rx /etc/parsec/{macdb,capdb}
```

17.3.4.3. Настройка прокси

В общем случае для настройки прокси Zabbix со значениями параметров по умолчанию требуется настроить СУБД и веб-сервер Apache.

Настроить СУБД для хранения данных:

1) в файле `/etc/postgresql/<версия_СУБД>/main/pg_hba.conf` добавить строки с именем БД для хранения данные Zabbix (например, `zabbix_proxy`) и СУБД-пользователя для обращения к данной БД (например, `zabbix`):

```
# TYPE   DATABASE            USER         ADDRESS                 METHOD
```

```
local zabbix_proxy   zabbix                trust

# IPv4 local connections:

host zabbix_proxy    zabbix 127.0.0.1/32 trust
```

ВНИМАНИЕ! Имя БД прокси должно отличаться от имени БД сервера Zabbix;

2) перезапустить службу СУБД:

```
sudo systemctl restart postgresql
```

3) запустить интерактивный терминал `psql` от имени пользователя `postgres`:

```
sudo -u postgres psql
```

и выполнить следующие команды:

а) создать БД `zabbix_proxy` и СУБД-пользователя `zabbix`, которые были указаны в конфигурационном файле, см. пункт 1) перечисления:

```
CREATE DATABASE zabbix_proxy;
CREATE USER zabbix WITH ENCRYPTED PASSWORD '<пароль_СУБД-пользователя_zabbix>';
```

б) предоставить СУБД-пользователю `zabbix` полные права доступа к БД `zabbix_proxy` и назначить его владельцем БД `zabbix_proxy`:

```
GRANT ALL ON DATABASE zabbix_proxy TO zabbix;
ALTER DATABASE zabbix_proxy OWNER TO zabbix;
```

в) выйти из терминала `psql`:

```
\q
```

4) заполнить БД `zabbix_proxy` на основе шаблонов Zabbix, выполнив команду:

```
zcat /usr/share/zabbix-proxy-pgsql/schema.sql.gz | psql -h localhost \
     zabbix_proxy zabbix
```

на запрос системы ввести пароль СУБД-пользователя `zabbix`;

5) в конфигурационном файле `/etc/zabbix/zabbix_proxy.conf`:

а) для параметра `Server` в качестве значения указать IP-адрес или доменное имя сервера Zabbix:

```
Server=<IP-адрес_или_имя_сервера_Zabbix>
```

б) для параметра `Hostname` в качестве значения указать имя прокси:

```
Hostname=<имя_прокси>
```

в) раскомментировать параметр DBPassword и указать в качестве значения пароль СУБД-пользователя zabbix:

```
DBPassword=<пароль_СУБД-пользователя_zabbix>
```

Если при настройке СУБД были заданы другие имя БД и пользователь СУБД, а также при необходимости изменить настройки прокси по умолчанию, то следует отредактировать и другие параметры (описание параметров конфигурационного файла приведено в 17.3.4.4);

6) перезапустить системную службу прокси Zabbix:

```
sudo systemctl restart zabbix-proxy
```

Прокси Zabbix функционирует в ОС как служба zabbix-proxy, управление прокси осуществляется в соответствии с 4.2.1.

После запуска службы прокси на узле требуется зарегистрировать данный узел на сервере Zabbix, для этого перейти в веб-интерфейс Zabbix и выполнить настройки:

1) на боковой панели перейти «Администрирование — Прокси»;
2) на открывшейся странице нажать **[Создать прокси]**;
3) в открывшемся окне в поле «Имя прокси» указать имя прокси (в конфигурационном файле /etc/zabbix/zabbix_proxy.conf значение параметра Hostname), остальные поля заполнить при необходимости;
4) нажать **[Добавить]**.

17.3.4.4. Конфигурационные параметры прокси

Конфигурация прокси Zabbix определяется администратором через значения параметров в конфигурационном файле /etc/zabbix/zabbix_proxy.conf.

Основные параметры конфигурационного файла прокси приведены в таблице 69.

Таблица 69

Параметр	Описание
AllowRoot	Разрешение запускать службу прокси от имени пользователя root (значение 0 — запрещено, значение 1 — разрешено). Если задано значение 0 (запрещено), но выполняется попытка запуска службы прокси от имени root, тогда прокси автоматически попробует запустить службу от имени пользователя, указанного в параметре User. Значение по умолчанию 0. Если настроен запуск службы прокси от имени пользователя, отличного от root, то параметр не применяется

Продолжение таблицы 69

Параметр	Описание
CacheSize	Размер кеша для хранения данных мониторинга. Указывается в байтах (B), килобайтах (K), мегабайтах (M) или гигабайтах (G), возможные значения от 128 КБ до 64 ГБ. Значение по умолчанию 32 МБ
ConfigFrequency	Частота получения конфигурационных данных от сервера, в секундах. Параметр активного прокси. Игнорируется пассивными прокси (см. параметр ProxyMode). Возможные значения от 1 до 604800 сек., значение по умолчанию 3600 сек.
DBHost	Имя узла, на котором размещена БД Zabbix. Значение по умолчанию localhost (используется локальное подключение) — сервер Zabbix и БД располагаются на одном узле. В случае отсутствия значения также будет использоваться локальное подключение
DBName	Имя БД Zabbix. Обязательный параметр. Значение по умолчанию zabbix_proxy
DBPassword	Пароль пользователя для доступа к БД Zabbix
DBPort	Порт для подключения к БД Zabbix, если не используется localhost (см. параметр DBHost)
DBSchema	Указывает имя схемы базы данных, которая будет использоваться Zabbix для доступа к своим таблицам и данным
DBUser	Пользователь для подключения к БД Zabbix. Значение по умолчанию zabbix
DataSenderFrequency	Частота отправки собранных данных серверу, в секундах. Параметр активного прокси. Игнорируется пассивными прокси (см. параметр ProxyMode). Возможные значения от 1 до 3600 сек., значение по умолчанию 1 сек.
Hostname	Уникальное регистрозависимое имя прокси. Значение должно совпадать с именем прокси, указанным в веб-интерфейсе Zabbix
HousekeepingFrequency	Частота выполнения автоматической очистки базы данных от устаревшей информации. Задается в часах, возможные значения от 0 до 24 ч. Значение по умолчанию 1 ч.
LogFile	Имя файла журнала. Обязательный параметр, если способ ведения журнала file (параметр LogType=file). Значение по умолчанию /var/log/zabbix-server/zabbix_server.log
LogType	Способ ведения журнала: - file — запись журнала в файл, указанный в параметре LogFile; - system — запись журнала в syslog; - console — запись журнала в стандартный вывод
ProxyMode	Режим работы прокси: - 0 — активный режим, прокси инициирует соединение с сервером Zabbix для передачи данных и получения инструкций, является значением по умолчанию; - 1 — пассивный режим, сервер Zabbix инициирует соединение с прокси для получения собранных данных

Окончание таблицы 69

Параметр	Описание
`Server`	Список IP-адресов или имен серверов Zabbix, разделенных запятой. Обязательный параметр
`User`	Указанный служебный пользователь будет использоваться для запуска службы сервера при попытке запустить службу сервера от имени пользователя `root` при установленном запрете на запуск от имени `root` (параметр AllowRoot=0). Значение по умолчанию `zabbix`

После изменения конфигурации перезапустить системную службу прокси.

17.3.5. Веб-интерфейс

Веб-интерфейс обеспечивает визуальный обзор собранных данных мониторинга, а также настройку и управление взаимодействием между компонентами и объектами Zabbix.

Доступ к веб-интерфейсу осуществляется пользователем через браузер:

1) с компьютера, на котором установлен сервер Zabbix — в адресной строке браузера ввести:

```
localhost/zabbix
```

2) с другого компьютера — в адресной строке браузера ввести IP-адрес или имя узла, на котором развернут сервер Zabbix:

```
<IP-адрес_или_имя_сервера_Zabbix>/zabbix
```

Для входа в веб-интерфейс использовать данные технологической учетной записи администратора — имя пользователя `Admin`, пароль `zabbix`. После входа для смена данных в веб-интерфейсе перейти «Администрирование — Пользователи», затем на странице выбрать учетную запись `Admin` и в открывшемся окне изменить имя пользователя и/или пароль.

В случае успешной авторизации откроется обзорная панель меню «Мониторинг» веб-интерфейса Zabbix.

Для установки русского языка в веб-интерфейсе следует:

1) на боковой панели навигации перейти «User settings — Profile»;
2) во вкладке User в поле «Language» выбрать значение «Russian (ru_RU)»;
3) нажать **[Update]**.

Для навигации используется боковая панель:

- раздел «Мониторинг» содержит подразделы, предоставляющие обзор собранных данных с контролируемых узлов сети;
- раздел «Услуги» содержит подразделы, необходимые для создания иерархии данных в качестве услуги и мониторинга доступности услуг IT-инфраструктуры;
- раздел «Инвентаризация» содержит подразделы, предоставляющие обзор инвентарных данных узлов сети;
- раздел «Отчеты» содержит подразделы, предоставляющие обзор различных отчетов о собранных данных мониторинга;
- раздел «Настройка» содержит подразделы, необходимые для настройки объектов Zabbix — узлов сети, элементов данных и шаблонов, триггеров и действий, средств визуализации данных;
- раздел «Администрирование» содержит подразделы, необходимые для управления прокси, пользователями, режимами аутентификации и способами оповещений;
- раздел «Помощь» предназначен для доступа к официальной документации Zabbix на сайте `www.zabbix.com`;
- раздел «Настройки пользователя» содержит подразделы, необходимые для настройки профиля текущего пользователя, в том числе языка интерфейса;
- раздел «Выход» предназначен для выхода из веб-интерфейса Zabbix.

17.3.6. Мониторинг событий аудита ОС

Мониторинг событий аудита ОС средствами Zabbix осуществляется с использованием шаблонов Astra Linux из состава сервера Zabbix.

17.3.6.1. Шаблоны Astra Linux

Шаблоны Template Astra Linux CE и Template Astra Linux SE представляют собой файлы `zabbix_astra_template.xml` и `zabbix_astra_parsec_template.xml` соответственно в каталоге `/usr/share/zabbix/conf/` на сервере Zabbix. Шаблоны копируется в каталог при установке пакета сервера Zabbix.

Шаблоны содержат элементы данных, которые по заданным критериям собирают записи из журнала аудита `/var/log/audit/audit.log`. Для сбора данных средствами Zabbix необходимо, чтобы аудит соответствующих событий был включен локально на компьютерах.

Элементы данных шаблона Template Astra Linux CE отслеживают появление в журнале аудита записей аудита.

Элементы данных шаблона Template Astra Linux SE отслеживают появление в журнале аудита записей PARSEC-аудита следующих типов (см. документ РУСБ.10015-01 97 01-1):

- события AVC (связанные с мандатным управлением доступом) и USER_AVC (события пользователя);
- PARSEC-аудит файлов;
- PARSEC-аудит процессов.

17.3.6.2. Применение шаблона Astra Linux

Для применения шаблонов Astra Linux необходимо выполнить локальную настройку каждого из агентов, а средствами веб-интерфейса импортировать файлы шаблона в Zabbix и присоединить шаблоны к узлам сети.

Узлы с установленными агентами должны быть предварительно настроены в веб-интерфейсе Zabbix (см. 17.3.3.1).

Шаблоны Astra Linux содержат элементы данных для активных проверок, поэтому агенты должны быть настроены для выполнения активных проверок (см. 17.3.3.2).

Для локальной настройки агента Zabbix выполнить следующие действия:

1) для выполнения агентом активных проверок требуется в конфигурационном файле `/etc/zabbix/zabbix_agentd.conf` указать значения параметров `ServerActive` и `Hostname`:

```
ServerActive=<IP-адрес_или_имя_сервера_Zabbix>
Hostname=<имя_агента>
```

2) добавить пользователя `zabbix` в группу `adm`:

```
sudo usermod -aG adm zabbix
```

3) перезапустить системную службу агента:

```
sudo systemctl restart zabbix-agent
```

На сервере Zabbix открыть веб-интерфейс и выполнить следующие действия:

1) импортировать поочередно каждый файл шаблона Astra Linux (`zabbix_astra_template.xml`, `zabbix_astra_parsec_template.xml`):
   а) на боковой панели навигации перейти «Настройка — Шаблоны»;
   б) на странице нажать **[Импорт]**;
   в) в открывшемся окне нажать **[Выберите файл]**;
   г) в окне навигации перейти в каталог `/usr/share/zabbix/conf/` и выбрать файл шаблона, затем нажать **[Импорт]** и еще раз нажать **[Импорт]**;

2) присоединить шаблоны к каждому из узлов сети:
   а) на боковой панели навигации перейти «Настройка — Узлы сети»;
   б) выбрать узел сети;
   в) в поле «Шаблоны» ввести часть имени шаблона «astra» и выбрать из списка шаблоны Template Astra Linux CE и Template Astra Linux SE;
   г) нажать **[Обновить]**.

В результате полученная информация о контролируемых событиях аудита ОС будет представлена в меню «Мониторинг — Последние данные».

Шаблоны Astra Linux обеспечивают только сбор информации от агентов. Для автоматического анализа собранных данных и реагирования на них требуется дополнительно настроить триггеры и действия в веб-интерфейсе.

18. РЕЗЕРВНОЕ КОПИРОВАНИЕ И ВОССТАНОВЛЕНИЕ ДАННЫХ

Система резервного копирования является составной частью плана восстановления системы.

Резервное копирование выполняется с целью обеспечения возможности восстановления отдельных файлов или ФС в целом с минимальными затратами труда и времени в случае утери рабочей копии информации. Резервные копии должны создаваться периодически, в соответствии с заранее установленным графиком (см. 18.2).

Процесс резервного копирования должен быть максимально автоматизирован и требовать наименьшего участия со стороны администратора системы.

Резервное копирование — это процесс, влияющий на работоспособность системы. Резервное копирование и восстановление увеличивает текущую нагрузку на систему, что может вызывать замедление работы системы. Кроме того, в зависимости от вида резервного копирования и восстановления, может потребоваться монопольный доступ к системе или полная остановка ее работы.

Основная идея резервного копирования — создание копий критической части содержания резервируемой системы. Основными исключениями, как правило, не входящими в процедуру резервного копирования функционирующей ОС, являются каталоги, содержащие служебные данные, меняющиеся в процессе функционирования (`/dev`, `/media`, `/mnt`, `/parsecfs`, `/proc`, `/run`, `/sys`, `/tmp`), а также сетевые каталоги (смонтированная NFS, Samba и прочие виды сетевых данных).

Элементы системы резервного копирования должны включать необходимое оборудование, носители резервных копий и ПО. Для хранения резервных копий могут быть использованы различные носители информации: дисковые накопители, отчуждаемые носители информации или специально выделенные разделы жесткого диска. Тип и количество носителей определяются используемым оборудованием, объемами обрабатываемых данных и выбранной схемой резервирования данных. ПО резервного копирования и восстановления из состава ОС включает утилиты командной строки и распределенные системы управления хранилищами данных:

1) комплекс программ Bacula (18.3);
2) утилита копирования `rsync` (18.4);
3) утилиты архивирования `tar`, `cpio`, `gzip` (18.5).

ВНИМАНИЕ! Для восстановления мандатных атрибутов файлов из резервных копий процесс должен иметь PARSEC-привилегию `0x1000` (`PARSEC_CAP_UNSAFE_SETXATTR`). Привилегия может быть получена с использованием утилиты `execaps`:

```
sudo execaps -c 0x1000 tar .......
```

ВНИМАНИЕ! Восстановление расширенных атрибутов файлов с использованием `unsecure_setxattr` возможно только в случае, если атрибуты восстанавливаются с помощью системного вызова `setxattr` путем установки атрибута `security.PDPL`. Использование `unsecure_setxattr` не влияет на возможность изменения мандатных атрибутов файлов системными вызовами `pdpl_set_path`, `pdpl_set_fd`.

Комплекс программ Bacula позволяет системному администратору управлять процессами резервного копирования и восстановления данных, находить и восстанавливать утраченные или поврежденные файлы, а также проверять резервные копии, в том числе в гетерогенных сетях.

Утилита `rsync` предоставляет возможности для локального и удаленного копирования (резервного копирования) или синхронизации файлов и каталогов с минимальными затратами трафика.

Утилиты командной строки `tar`, `cpio`, `gzip` представляют собой традиционные инструменты создания резервных копий и архивирования ФС.

Порядок выполнения операций резервного копирования и восстановления объектов ФС с сохранением и восстановлением мандатных атрибутов и атрибутов аудита описан в РУСБ.10015-01 97 01-1.

18.1. Виды резервного копирования

Существуют следующие виды резервного копирования:

- полное резервное копирование — сохранение резервной копии всех файлов системы. Процедура занимает много времени и требует место для хранения большого объема. Как правило, выполняется в тех случаях, когда не влияет на основную работу системы, или для создания базовой резервной копии данных. В дальнейшем может выполняться дифференциальное или инкрементное резервное копирование;
- дифференциальное резервное копирование — сохранение копий изменившихся с последнего полного резервного копирования файлов. Требования к объему хранения и времени создания меньше, чем при полном копировании. Время восстановления незначительно за счет прямой перезаписи файлов;
- инкрементное резервное копирование — сохранение изменений файлов с момента последнего инкрементного копирования. Требует минимального количества времени и места для создания копии, но усложняет последующее восстановление, поскольку необходимо последовательное восстановление всех инкрементных копий с момента последнего полного резервного копирования.

18.2. Планирование резервного копирования

Планирование резервного копирования заключается в рассмотрении и определении следующих вопросов:

- что именно и как часто должно архивироваться;
- какие виды резервного копирования и на какие носители должны применяться;
- как часто и каким образом будут восстанавливаться файлы при необходимости;
- каким образом пользователи могут запросить ранее сохраненные файлы.

План резервного копирования должен периодически пересматриваться для отражения изменений как в системе, так и в используемых технологиях или условиях функционирования.

18.2.1. Составление расписания резервного копирования

При составлении расписания резервного копирования определяется что, когда и на каком носителе должно сохраняться.

Должна существовать возможность восстановления любого файла в любой момент времени. Например, требуется восстановить файл не более, чем однодневной давности. Для этого может использоваться комбинация полного и обновляемого (дифференциального или инкрементного) резервного копирования. Полное резервное копирование позволяет сохранить копии всех файлов системы, обновляемое — только изменившиеся со времени последнего архивирования. Обновляемое может иметь несколько уровней, например, обновление по отношению к последней обновляемой резервной копии.

Для восстановления отдельных файлов при таком многоуровневом расписании может понадобиться полная резервная копия, если файл не изменялся в течение месяца; копия первого уровня, если файл не изменялся в течение недели; копия второго уровня при ежедневной работе с этим файлом. Такая схема несколько сложнее, однако требует меньших ежедневных временных затрат.

Примечание. Расписание резервного копирования должно быть доведено до пользователей.

18.2.2. Планирование восстановления системы

При составлении плана резервного копирования следует определить:

1) план действий на случай аварийной ситуации;
2) как при необходимости может быть восстановлена система или отдельные файлы;
3) где хранятся и насколько доступны носители с резервными копиями и не могут ли они быть повреждены при сбоях на компьютере.

Примечание. Необходимо периодически выполнять проверку исправности носителей с архивами резервных копий. Проверка может включать в себя чтение содержимого копии после сохранения или выборочную проверку файлов резервной копии.

18.3. Комплекс программ Bacula

Bacula — это сетевая клиент-серверная система резервного копирования и восстановления данных. Благодаря модульной архитектуре ее можно масштабировать до больших сетей, состоящих из сотен компьютеров.

Bacula состоит из следующих основных компонентов:

- Bacula Director — диспетчер. Это центральная программа, координирующая все выполняемые операции. Функционирует в фоновом режиме;
- Bacula Console — консоль Bacula. Она позволяет администратору взаимодействовать с центральной программой;
- Bacula File — клиентская программа (клиент), которая устанавливается на каждый обслуживаемый компьютер;
- Bacula Storage — хранилище данных. Программа, взаимодействующая с физическими или логическими носителями для копирования и восстановления данных;
- Bacula Catalog — программа, отвечающая за индексирование и организацию базы резервных данных.

Bacula обеспечивает сохранение расширенных атрибутов каталогов и файлов, а также их последующее восстановление при необходимости (см. РУСБ.10015-01 97 01-1).

Порядок использования Bacula описан на примере системы со следующей инфраструктурой:

- выделенный сервер для функционирования Bacula Director — главный сервер, осуществляющий резервное копирование;
- выделенный сервер для функционирования Bacula Storage — рабочая станция, на которой будут размещаться резервные копии данных;
- персональный компьютер для функционирования Bacula File — рабочая станция, с которой будут копироваться данные и на которую будут восстанавливаться резервные копии данных.

18.3.1. Настройка СУБД для Bacula

Для хранения каталога резервных копий используется СУБД. Настройку СУБД необходимо выполнить до запуска компонентов Bacula.

Для настройки необходимо выполнить следующие действия:

1) установить СУБД на сервер, где будет работать Bacula Director:

```
sudo apt install postgresql-<версия>
```

2) через менеджер пакетов Synaptic по ключевому слову «bacula» необходимо установить все пакеты, кроме тех, где в названии фигурирует «-sqlite3». При установке Bacula в появившемся окне настройки совместимости с БД снять флаг автоматической настройки и нажать **[Далее]**;

3) подготовить СУБД для работы с Bacula, выполнив следующие действия:

а) в файле `/etc/postgresql/<версия>/<кластер>/postgresql.conf` для прослушивания всех IP-адресов указать:

```
listen_addresses = '*'
```

б) в файле `/etc/postgresql/<версия>/<кластер>/pg_hba.conf` добавить узел Bacula Director с IP-адресом `11.11.11.21` и указать метод аутентификации `trust` для всех соединений:

```
local all postgres trust
local all all trust
host all all 127.0.0.1/32 trust
host all all 11.11.11.21/24 trust
```

ВНИМАНИЕ! Метод аутентификации `trust` рекомендуется использовать только в доверенной сети;

в) выполнить перезапуск СУБД:

```
sudo pg_ctlcluster <версия> <кластер> restart
```

г) присвоить пароль для пользователя `postgres` командой:

```
sudo passwd postgres
```

на запрос системы ввести пароль для пользователя `postgres`;

д) присвоить пароль для пользователя `bacula` командой:

```
sudo passwd bacula
```

на запрос системы ввести пароль для пользователя `bacula`;

е) запустить интерактивный терминал `psql` и подключиться к предустановленной БД `template1` от имени пользователя `postgres`:

```
psql template1 postgres
```

ж) создать пользователя `bacula` и назначить для него пароль, а также предоставить данному пользователю административные права:

```
CREATE ROLE bacula;
ALTER USER bacula PASSWORD '<пароль_СУБД-пользователя_bacula>';
```

```
ALTER USER bacula LOGIN SUPERUSER CREATEDB CREATEROLE;
```

з) выйти из интерактивного терминала `psql`:

```
\q
```

4) запустить интерактивный терминал `psql` и подключиться к БД `postgres` через порт подключения, по умолчанию порт `5432`:

```
psql postgres -p 5432 -U postgres
```

затем выполнить команды:

а) создать БД с именем `bacula-db`, задать для БД кодировку и классификацию символов, а также указать шаблон создаваемой БД:

```
CREATE DATABASE bacula-db WITH ENCODING = 'SQL_ASCII'
LC_COLLATE = 'C' LC_CTYPE = 'C' TEMPLATE = 'template0';
```

б) назначить владельцем БД `bacula-db` пользователя `bacula`:

```
ALTER DATABASE bacula-db OWNER TO bacula;
```

в) выйти из интерфейса управления `psql`:

```
\q
```

5) на сервере Bacula Director отредактировать сценарий создания таблиц `/usr/share/bacula-director/make_postgresql_tables`:

а) в строке `db_name` указать имя БД `bacula-db`:

```
db_name=bacula-db
```

б) в строке `psql` указать IP-адрес Bacula Director и порт подключения `5432`:

```
psql -U bacula -h 11.11.11.21 -p 5432 -f - -d ${db_name}
$* <<END-OF-DATA
```

6) на сервере Bacula Director отредактировать сценарий назначения привилегий `/usr/share/bacula-director/grant_postgresql_privileges`:

а) в строке `db_user` указать имя СУБД-пользователя `bacula`:

```
db_user=bacula
```

б) в строке `db_name` указать имя БД `bacula-db`:

```
db_name=bacula-db
```

в) в строке `db_password` указать пароль СУБД-пользователя `bacula`:

```
db_password=<пароль_СУБД-пользователя_bacula>
```

г) в строке `$bindir/psql` указать СУБД-пользователя `bacula`, IP-адрес Bacula Director и порт подключения `5432`:

```
$bindir/psql -U bacula -h 11.11.11.21 -p 5432 -f - -d
```

```
${db_name} $* <<END-OF-DATA
```

7) для корректного функционирования отредактированных сценариев:

а) предоставить пользователю `postgres` право чтения БД меток безопасности локальных пользователей:

```
sudo usermod -a -G shadow postgres
sudo setfacl -d -m u:postgres:r /etc/parsec/macdb /etc/parsec/capdb
sudo setfacl -R -m u:postgres:r /etc/parsec/macdb /etc/parsec/capdb
sudo setfacl -m u:postgres:rx /etc/parsec/macdb /etc/parsec/capdb
```

б) назначить метку безопасности пользователю `bacula` (нулевую классификационную метку, категорию целостности не назначать):

```
sudo pdpl-user bacula -l 0:0
```

Подробное описание инструмента `pdpl-user` приведено на справочной странице `man pdpl-user`;

8) выполнить сценарии для создания таблиц и назначения привилегий пользователю `bacula`:

```
sudo /usr/share/bacula-director/make_postgresql_tables
sudo /usr/share/bacula-director/grant_postgresql_privileges
```

При успешном создании таблиц будет выведено следующее сообщение:

```
Creation of Bacula PostgreSQL tables succeeded.
```

При успешном назначении привилегий будет выведено следующее сообщение:

```
Privileges for user bacula granted on database bacula-db.
```

18.3.2. Настройка Bacula

Для функционирования системы резервного копирования и восстановления данных необходимо настроить следующие компоненты Bacula в конфигурационных файлах:

- `/etc/bacula/bacula-dir.conf` — настройка Bacula Director;
- `/etc/bacula/bacula-sd.conf` — настройка Bacula Storage;
- `/etc/bacula/bacula-fd.conf` — настройка Bacula File;
- `/etc/bacula/bconsole.conf` — настройка Bacula Console.

Описание основных секций конфигурационных файлов и задаваемых в них параметрах приведены в таблице 58.

Таблица 58

Параметр	Описание
`Director`	Параметры конфигурации диспетчера Bacula Director. Указывается имя, пароль и IP-адрес диспетчера, а также настройки взаимодействия с другими компонентами
`JobDefs`	Шаблон задания для резервного копирования или восстановления данных. Задаются типовые параметры, которые могут быть использованы для конкретных заданий
`Job`	Параметры конкретного задания резервного копирования или восстановления данных
`Schedule`	Расписание запуска заданий
`FileSet`	Определяются каталоги и файлы, включаемые в резервную копию, а также задаются параметры их обработки, такие как алгоритмы вычисления контрольных сумм и сжатия файлов, сохранения прав доступа и т.п.
`Client`	Параметры конфигурации клиента Bacula File, с которого будет выполняться копирование данных. Указывается имя, пароль и IP-адрес клиента, а также настройки взаимодействия с другими компонентами
`Storage`	Параметры конфигурации хранилища Bacula Storage. Указывается имя, IP-адрес хранилища, максимальное количество одновременно выполняемых заданий и другие параметры
`Catalog`	Параметры подключения к базе данных, в которой хранится информация о резервных копиях
`Messages`	Настройка уведомлений о результатах выполнения заданий. Позволяет задать куда будут направляться уведомления (например, на диспетчер) и что в них будет фиксироваться (например, сведения об ошибках, предупреждениях или успешных и неуспешных действиях)
`Pool`	Настройка группы томов хранилища Bacula Storage для упорядоченного хранения резервных копий по типу данных или сроку их хранения
`Device`	Параметры устройств хранения информации. Указывается физический путь к устройству хранения, является ли носитель информации съемным и другие параметры
`Autochanger`	Настройка автосменщика носителей информации. Осуществляет виртуальную группировку устройств хранения информации для обращения к ним как к единому целому

Подробное описание всех параметров и возможных для них значений приведены в официальной документации системы резервного копирования Bacula.

При корректировке конфигурационных файлов следует задавать в секциях уникальные имена для параметра `Name`, а неиспользуемые параметры и секции рекомендуется оставить со значениями по умолчанию.

18.3.2.1. Настройка Bacula Director

Настройка Bacula Director осуществляется на сервере с IP-адресом `11.11.11.21` в конфигурационном файле `/etc/bacula/bacula-dir.conf`:

1) в секции `Director` задать значения параметров `Name`, `Password` и `DirAddress`, остальные параметры оставить со значениями по умолчанию:

```
Director {

Name = bacula-dir # имя Bacula Director

DIRport = 9101 # прослушиваемый порт

QueryFile = "/etc/bacula/scripts/query.sql" # путь к сценарию,
# содержащему SQL-запросы для работы с Bacula Catalog

WorkingDirectory = "/var/lib/bacula" # каталог, в котором хранятся
# статус-файлы Bacula Director

PidDirectory = "/run/bacula" # pid-файл службы Bacula Director

Maximum Concurrent Jobs = 1 # максимальное количество выполняемых
# заданий (не рекомендуется одновременно запускать более одного задания)

Password = "<пароль_bacula-dir>" # пароль Bacula Director

Messages = Daemon # конфигурация уведомлений из секции Messages

DirAddress = 11.11.11.21 # IP-адрес Bacula Director

}
```

2) в секции `JobDefs` задать значения параметров для шаблонного задания, параметры которого могут быть использованы другими заданиями:

```
JobDefs {

Name = "DefaultJob" # имя задания

Type = Backup # тип задания (Backup, Restore и т.д.)

Level = Incremental # уровень резервного копирования
# (Full, Incremental, Differential и т.д.)

Client =bacula-fd # имя Bacula File, заданное в bacula-fd.conf
```

```
FileSet = "Full Set" # имя набора файлов из секции FileSet

Schedule = "WeeklyCycle" # имя расписания из секции Schedule

Storage = bacula-sd # имя Bacula Storage, заданное в bacula-sd.conf

Messages = Standard # конфигурация уведомлений о выполняемых заданиях
# из секции Messages (Standard, ErrorsOnly и т.д.)

Pool = File # имя пула (группы томов) из секции Pool для записей
# резервного копирования

SpoolAttributes = yes # включена буферизация атрибутов файлов

Priority = 10 # приоритет выполнения задания
# от 1 (максимальный) до 1000 (минимальный)

Write Bootstrap = "/var/lib/bacula/%c.bsr" # файл, в котором хранится
# информация откуда извлекать данные при восстановлении

}
```

3) в секции `Storage` для настройки подключения к хранилищу Bacula Storage задать следующие значения параметров:

```
Storage {

Name = bacula-sd # имя Bacula Storage

Address = 11.11.11.22 # IP-адрес Bacula Storage

SDPort = 9103 # порт подключения

Password = "<пароль_bacula-sd>" # пароль Bacula Storage

Device = Autochanger1 # имя устройства хранения, указанное
# в файле bacula-sd.conf

Media Type = File1 # имя, которое будет использовано Bacula для
# восстановления данных

Maximum Concurrent Jobs = 1 # максимальное количество выполняемых
# заданий (не рекомендуется одновременно запускать более одного задания)

}
```

4) в секции Job, которая используется для настройки заданий резервирования файлов клиента, задать следующие параметры:

```
Job {

Name = "BackupClient1" # имя задания

JobDefs = "DefaultJob" # имя шаблонного задания

}
```

5) в секции Job, которая используется для настройки заданий резервирования файлов Bacula Catalog, задать следующие параметры:

```
Job {

Name = "BackupCatalog" # имя задания

JobDefs = "DefaultJob" # имя шаблонного задания

Level = Full # уровень резервного копирования

FileSet="Catalog" # имя для набора восстанавливаемых файлов
# из секции FileSet

Schedule = "WeeklyCycleAfterBackup" # имя расписания запуска задания
# из секции Schedule

Write Bootstrap = "/var/lib/bacula/%n.bsr" # файл с информацией откуда
# извлекать данные при восстановлении

}
```

6) в секции Job, которая используется для настройки заданий восстановления файлов клиента, задать следующие параметры:

```
Job {

Name = "RestoreFiles" # имя задания

Type = Restore # тип задания (резервирование, восстановление и т.д.)

Client=bacula-fd # имя Bacula File, заданное в bacula-fd.conf

FileSet="Full Set" # имя набора восстанавливаемых файлов
# из секции FileSet
```

```
Storage = bacula-sd # имя Bacula Storage, заданное в bacula-sd.conf

Pool = File # имя пула (группы томов) Bacula Storage, где находится
# резервная копия файлов/каталогов клиента

Messages = Standard # тип уведомлений о выполняемых заданиях

Where = /restore/ # путь восстановления на клиенте

}
```

7) в секции FileSet, которая используется для настройки наборов файлов и параметров для клиента, задать следующие параметры:

```
FileSet {

Name = "Full Set" # имя набора файлов

Include { # секция, содержащая пути к резервируемым файлам/каталогам

Options { # секция, определяющая параметры резервирования
# файлов/каталогов

signature = MD5 # алгоритм вычисления контрольных сумм файлов

compression = GZIP # алгоритм сжатия файлов

recurse = yes # необходимость рекурсивного резервирования

aclsupport = yes # необходимость сохранения прав, назначенным файлам
# и каталогам (например, назначенным с помощью setfacl)

xattrsupport = yes # указывает на возможность включения
# поддержки расширенных атрибутов
# (обязательный параметр для работы с метками безопасности)

}

File = /home # путь к файлам/каталогам, которые должны быть включены
# в список резервируемых

}

Exclude { # секция содержит пути к файлам/каталогам, которые необходимо
# исключить из списка резервируемых
```

```
File = /tmp

}

}
```

8) в секции Schedule, которая используется для настройки расписания обработки файлов при выполнении заданий клиента, задать следующие параметры:

```
Schedule {

Name = "WeeklyCycle" # имя расписания

Run = Full 1st sun at 23:05 # тип, периодичность и время запуска
# полного резервного копирования

Run = Differential 2nd-5th sun at 23:05 # тип, периодичность и время
# запуска дифференциального резервного копирования

Run = Incremental mon-sat at 23:05 # тип, периодичность и время запуска
# инкрементального резервного копирования

}
```

9) в секции Schedule, которая используется для настройки расписания обработки файлов при выполнении заданий для Bacula Catalog, задать следующие параметры:

```
Schedule {

Name = "WeeklyCycleAfterBackup" # имя расписания

Run = Full sun-sat at 23:10 # тип, периодичность и время запуска
# полного резервного копирования

}
```

10) в секции FileSet, которая используется для настройки наборов файлов и параметров для Bacula Catalog, задать следующие параметры:

```
FileSet {

Name = "Catalog" # имя Bacula Catalog

Include { # секция, содержащая пути к резервируемым файлам/каталогам

Options { # секция, определяющая параметры резервирования
# файлов/каталогов
```

```
signature = MD5 # алгоритм вычисления контрольных сумм файлов

compression = GZIP # алгоритм сжатия файлов

recurse = yes # необходимость рекурсивного резервирования

aclsupport = yes # необходимость сохранения прав, назначенным файлам
# и каталогам (например, назначенным с помощью setfacl)

xattrsupport = yes # указывает на возможность включения поддержки
# расширенных атрибутов
# (обязательный параметр для работы с метками безопасности)

}

File = "/var/lib/bacula/bacula.sql" # путь к файлам/каталогам, которые
# должны быть включены в список резервируемых

}

}
```

11) в секции `Client` для настройки клиента необходимо задать следующие параметры:

```
Client {

Name = bacula-fd # имя Bacula File

Address = 11.11.11.23 # IP-адрес Bacula File

FDPort = 9102 # порт прослушивания

Catalog = BaculaCatalog # имя Bacula Catalog, заданное в секции Catalog
# для параметра Name

Password = "<пароль_bacula-fd>" # пароль Bacula File

File Retention = 60 days # период, в течении которого информация
# о файлах хранится в БД

Job Retention = 6 months # период, в течении которого информация
# о заданиях хранится в БД

AutoPrune = yes # автоматическое удаление из БД записей о заданиях
# и файлах, срок хранения которых истек в соответствии с периодами
```

```
# параметров File Retention и Job Retention

}
```

12) в секции `Catalog` указать параметры доступа к БД, а также назначить уникальное имя данного Bacula Catalog:

```
Catalog {

Name = BaculaCatalog # имя Bacula Catalog

dbaddress = 11.11.11.21 # адрес сервера СУБД

dbport = 5432 # порт подключения на сервере

dbname = bacula-db # имя БД на сервере СУБД

dbuser = bacula # имя СУБД-пользователя

dbpassword = <пароль_СУБД-пользователя_bacula>

}
```

13) в секции `Pool`, которая используется для файлов, указать параметры группы томов хранилища Bacula Storage:

```
Pool {

Name = File # имя пула, указывается в заданиях резервного копирования

Pool Type = Backup # тип пула (например, Backup, Copy или Cloned)

Recycle = yes # возможность автоматической очистки или перезаписи тома
# пула

Volume Retention = 365 days # период, в течение которого информация
# о заданиях и файлах хранится в БД

AutoPrune = yes # автоматическое удаление из БД записей о заданиях
# и файлах, срок хранения которых истек в соответствии с периодом
# параметра Volume Retention

Maximum Volume Bytes = 50G # максимальный объем тома в пуле

Maximum Volumes = 100 # максимальное количество томов в пуле

Label Format = "Vol-" # начальные символы имен томов пула
```

```
}
```

Далее следует установить права на чтение и запись пользователю `bacula` и назначить его владельцем конфигурационного файла `bacula-dir.conf`:

```
sudo chmod 644 /etc/bacula/bacula-dir.conf
sudo chown root:bacula /etc/bacula/bacula-dir.conf
```

Чтобы настроить доступ к Bacula Console необходимо:

1) отредактировать конфигурационный файл `/etc/bacula/bconsole.conf`:

```
Director {

Name = bacula-dir # имя Bacula Director, заданное в bacula-dir.conf

DIRport = 9101 # прослушиваемый порт

address = 11.11.11.21 # IP-адрес Bacula Director

Password = "<пароль_bacula-dir>" # пароль Bacula Director

}
```

2) перезапустить Bacula Director командой:

```
sudo systemctl restart bacula-director
```

18.3.2.2. Настройка Bacula Storage

Bacula Storage отвечает за непосредственную работу с устройством хранения данных. Bacula поддерживает широкий спектр устройств от оптических дисков до ленточных библиотек. В описываемой конфигурации используется следующий вариант — жесткий диск с файловой системой ext3.

Настройка Bacula Storage осуществляется на сервере с IP-адресом `11.11.11.22` в конфигурационном файле `/etc/bacula/bacula-sd.conf`, для этого необходимо:

1) указать основные параметры хранилища:

```
Storage {

Name = bacula-sd # имя Bacula Storage

SDPort = 9103 # прослушиваемый порт
```

```
WorkingDirectory = "/var/lib/bacula" # каталог, в котором хранятся
# статус-файлы Bacula Storage

Pid Directory = "/run/bacula" # pid-файл службы Bacula

Maximum Concurrent Jobs = 1 # максимальное количество выполняемых
# заданий (не рекомендуется одновременно запускать более одного задания)

SDAddress = 11.11.11.22 # IP-адрес Bacula Storage

}
```

2) для подключения диспетчера к хранилищу указать следующие параметры:

```
Director {

Name = bacula-dir # имя Bacula Director, которому разрешено
# подключаться к Bacula Storage

Password = "<пароль_bacula-sd>" # пароль Bacula Storage

}
```

3) для настройки автосменщика носителей информации (виртуальной группировки устройств хранения, входящих в одну библиотеку, и обращения к ним как к единому целому) настроить параметры в секции `Autochanger`:

```
Autochanger {

Name = Autochanger1 # имя автосменщика

Device = FileChgr1-Dev1, FileChgr1-Dev2 # имена устройств хранения,
# относящихся к автосменщику

Changer Command = "" # при виртуальной группировки устройств хранения
# значение не требуется

Changer Device = /dev/null # значение при использовании виртуальной
# группировки устройств хранения

}
```

4) для устройств хранения `FileChgr1-Dev1` и `FileChgr1-Dev2` создать соответственно каталоги `files1` и `files2`, назначить владельцем пользователя `bacula` и предоставить ему полный доступ:

```
sudo mkdir -p /backups/files1/
sudo chmod 755 /backups/files1/
```

```
sudo chown bacula:bacula /backups/files1/

sudo mkdir -p /backups/files2/
sudo chmod 755 /backups/files2/
sudo chown bacula:bacula /backups/files2/
```

5) в конфигурационном файле `/etc/bacula/bacula-sd.conf` задать параметры устройств хранения `FileChgr1-Dev1` и `FileChgr1-Dev2`, а также настроить уведомления для хранилища:

```
Device {

Name = FileChgr1-Dev1 # имя устройства хранения

Media Type = File1 # логический тип носителя

Archive Device = /backups/files1 # путь к каталогу, в котором будут
# размещаться резервные копии

LabelMedia = yes # автоматическая разметка новых томов

Random Access = Yes # возможность доступа к данным в непоследовательном
# (произвольном) порядке

AutomaticMount = yes # поддержка автоматического монтирования

RemovableMedia = no # физическое извлечение устройства хранения
# (при наличии устройства)

AlwaysOpen = no # состояние открытия устройства хранения
# (yes - устройство открыто всегда, no - устройство открывается
# при выполнении задания)

Maximum Concurrent Jobs = 1 # максимальное количество выполняемых
# заданий (не рекомендуется одновременно запускать более одного задания)

}

Device {

Name = FileChgr1-Dev2 # имя устройства хранения

Media Type = File1 # логический тип носителя

Archive Device = /backups/files2 # путь к каталогу, в котором будут
# размещаться резервные копии
```

```
LabelMedia = yes # автоматическая разметка новых томов

Random Access = Yes # возможность доступа к данным в непоследовательном
# (произвольном) порядке

AutomaticMount = yes # поддержка автоматического монтирования

RemovableMedia = no # физическое извлечение устройства хранения
# (при наличии устройства)

AlwaysOpen = no # состояние открытия устройства хранения
# (yes - устройство открыто всегда, no - устройство открывается при
# выполнении задания)

Maximum Concurrent Jobs = 1 # максимальное количество выполняемых
# заданий (не рекомендуется одновременно запускать более одного задания)

}

Messages {

Name = Standard # имя шаблона уведомлений для заданий

director = bacula-dir = all # все уведомления будут направлены
# на Bacula Director

}
```

6) установить права на чтение и запись пользователю `bacula` и назначить его владельцем конфигурационного файла `bacula-sd.conf`:

```
sudo chmod 644 /etc/bacula/bacula-sd.conf
sudo chown root:bacula /etc/bacula/bacula-sd.conf
```

7) перезапустить Bacula Storage командой:

```
sudo systemctl restart bacula-sd
```

18.3.2.3. Настройка Bacula File

Настройка Bacula File (клиента) осуществляется на рабочей станции с IP-адресом `11.11.11.23` в конфигурационном файле `/etc/bacula/bacula-fd.conf`, для этого необходимо:

1) в секции `Director` настроить возможность подключения диспетчера к клиенту:

```
Director {
```

```
Name = bacula-dir # имя Bacula Director, которому разрешено
подключаться к Bacula File

Password = "<пароль_bacula-fd>" # пароль Bacula File

}
```

2) в секции FileDaemon указать основные параметры клиента:

```
FileDaemon {

Name = bacula-fd # имя Bacula File

FDport = 9102 # прослушиваемый порт

WorkingDirectory = /var/lib/bacula # каталог, в котором хранятся
# статус-файлы Bacula File

Pid Directory = /run/bacula # pid-файл службы Bacula File

Maximum Concurrent Jobs = 1 # максимальное количество выполняемых
# заданий (не рекомендуется одновременно запускать более одного задания)

Plugin Directory = /usr/lib/bacula # каталог хранения подключаемых
# расширений для дополнительной функциональности
# (например, использование внешних сценариев)

FDAddress = 11.11.11.23 # IP-адрес Bacula File

}
```

3) в секции Messages для настройки уведомлений клиента установить следующие параметры:

```
Messages {

Name = Standard # имя шаблона уведомлений для заданий

director = bacula-dir = all # все уведомления будут направлены
# на Bacula Director

}
```

4) установить права на чтение и запись пользователю bacula и назначить его владельцем конфигурационного файла bacula-fd.conf:

```
sudo chmod 644 /etc/bacula/bacula-fd.conf
```

```
sudo chown root:bacula /etc/bacula/bacula-fd.conf
```

5) перезапустить Bacula File командой:

```
sudo systemctl restart bacula-fd
```

18.3.2.4. Проверка работоспособности Bacula

Для проверки работоспособности компонентов Bacula необходимо:

1) на сервере Bacula Director с IP-адресом `11.11.11.21` выполнить команду для входа в консоль:

```
sudo bconsole
```

2) при корректной настройке всех компонентов будет открыта консоль Bacula. Для вывода диалогового сообщения с возможностью проверки статуса одного или всех компонентов необходимо ввести следующую команду:

```
status
```

3) ввести цифру от «1» до «6», где:
   - «1» — статус Bacula Director;
   - «2» — статус Bacula Storage;
   - «3» — статус Bacula Client;
   - «4» — статус связи компонентов Bacula;
   - «6» — статус всех компонентов;

4) выход из консоли осуществляется следующей командой:

```
exit
```

18.3.2.5. Резервное копирование данных

Для создания резервной копии необходимо:

1) на сервере Bacula Director с IP-адресом `11.11.11.21` выполнить команду для входа в консоль:

```
sudo bconsole
```

2) в консоли выполнить команду для запуска задания резервного копирования:

```
run
```

3) в отобразившемся меню выбрать задание, нажав необходимую цифру на клавиатуре (например, «1»):

```
Select Job resource (1-3): 1
```

4) после вывода списка параметров задания необходимо указать вариант продолжения работы (yes — выполнить задание, no — отменить задание, mod — изменить параметры задания):

```
OK to run? (yes/mod/no): yes
```

5) для проверки уведомления о выполнении задания ввести команду:

```
messages
```

В случае успешного выполнения задания будет выведено сообщение со строкой:

```
Termination: Backup OK
```

18.3.2.6. Восстановление данных из резервной копии

Для восстановление данных из резервной копии необходимо:

1) на сервере Bacula Director с IP-адресом 11.11.11.21 выполнить команду для входа в консоль:

```
sudo bconsole
```

2) в консоли выполнить команду для инициализации восстановления данных и выбора режима восстановления:

```
restore
```

3) в отобразившемся меню выбрать пункт 3 для ввода задания:

```
Select item: (1-13): 3
```

4) ввести идентификатор нужного задания или несколько идентификаторов нужных заданий, разделенных запятой:

```
Enter JobId(s), comma separated to restore: 10,11,12
```

5) указать параметр маркировки и определить, что необходимо восстановить. Например, для восстановления всех файлов в задании:

```
mark *
```

6) подтвердить выполнение командой:

```
done
```

7) после вывода информации о файлах, выбранных для восстановления, необходимо указать вариант продолжения работы (yes — выполнить задание, no — отменить задание, mod — изменить параметры задания):

```
OK to run? (yes/mod/no): yes
```

8) для проверки уведомления о восстановлении данных ввести команду:

```
messages
```

В случае успешного восстановления данных будет выведено сообщение со строкой:

```
Termination: Restore OK
```

Данные из резервной копии будут восстановлены в каталоге /restore/ на рабочей станции с Bacula File.

Также управление Bacula возможно с помощью графической утилиты bacula-console-qt.

18.4. Утилита копирования rsync

Все действия при использовании команды rsync выполняются от имени учетной записи администратора с использованием механизма sudo.

В таблице 59 приведены некоторые наиболее часто используемые параметры команды rsync.

Таблица 59

Параметр	Назначение
-v, --verbose	Подробный вывод
-z, --compress	Сжимать трафик
-r, --recursive	Выполнять копирование рекурсивно
-p, --perms	Сохранять дискретные права доступа
-t, --times	Сохранять время доступа к файлам
-g, --group	Сохранять группу
-o, --owner	Сохранять владельца
-A, --acls	Сохранять списки контроля доступа ACL (включает -p)
-X, --xattrs	Сохранять расширенные атрибуты (в том числе мандатные атрибуты)

Подробное описание команды приведено в man для rsync.

Пример

Следующая команда сделает копию домашнего каталога на 192.168.0.1

```
sudo rsync -vzrptgoAX /home/ admin@192.168.0.1:/home_bak
```

В данном примере должен быть создан каталог /home_bak на сервере и установлены на него максимальные метки с ccnr.

ВНИМАНИЕ! Не рекомендуется использовать параметр -l для копирования символических ссылок при создании резервной копии домашних каталогов пользователей.

18.5. Утилиты архивирования

При создании архива командами tar и gzip передается список файлов и каталогов, указываемых как параметры командной строки. Любой указанный каталог просматривается рекурсивно. При создании архива с помощью команды cpio ей предоставляется список объектов (имена файлов и каталогов, символические имена любых устройств, гнезда доменов UNIX, поименованные каналы и т. п.).

Все действия при использовании команд tar, cpio и gzip выполняются от имени учетной записи администратора с использованием механизма sudo.

Подробное описание команд приведено в руководстве man для tar, cpio и gzip.

18.5.1. tar

Команда tar может работать с рядом дисковых накопителей, позволяет просматривать архивы в ОС.

В таблице 60 приведены основные параметры команды tar.

Таблица 60

Параметр	Назначение
--acls	Сохраняет (восстанавливает) списки контроля доступа (ACL) каталогов и файлов, вложенных в архив
-c, --create	Создает архив
-x, --extract, --get	Восстанавливает файлы из архива на устройстве, заданном по умолчанию или определенном параметром f
--xattrs	Сохраняет (восстанавливает) расширенные атрибуты каталогов и файлов, вложенных в архив
-f, --file name	Создает (или читает) архив с name, где name — имя файла или устройства, определенного в /dev, например, /dev/rmt0
-Z, --compress, --uncompress	Сжимает или распаковывает архив с помощью compress
-z, --gzip, --gunzip	Сжимает или распаковывает архив с помощью gzip
-M, --multi-volume	Создает многотомный архив
-t, --list	Выводит список сохраненных в архиве файлов
-v, --verbose	Выводит подробную информацию о процессе

Подробное описание команды приведено в man для tar.

В примерах приведены варианты использования команды tar.

Примеры:

1. Копирование каталога /home на специальный раздел жесткого диска /dev/hda4

```
tar -cf /dev/hda4 /home
```

Параметр f определяет создание архива на устройстве /dev/hda4.

2. Применение сжатия при архивировании

```
tar -cvfz /dev/hda4 /home | tee home.index
```

Параметр v заставляет tar выводить подробную информацию, параметр z указывает на сжатие архива с помощью утилиты gzip. Список скопированных файлов направляется в home.index.

3. Использование команды find для поиска измененных в течение одного дня файлов в каталоге /home и создание архива home.new.tar с этими файлами:

```
find /home -mtime 1 -type f -exec tar -rf home.new.tar {} \;
```

4. Если надо посмотреть содержимое архива, то можно воспользоваться параметром -t команды tar:

```
tar -tf home.new.tar
```

5. Для извлечения файлов из архива необходимо указать путь к архиву либо устройству и путь к месту извлечения. Если архив (каталога /home) был создан командой:

```
tar -czf /tmp/home.tar /home
```

то извлекать его надо командой:

```
tar -xzf /tmp/home.tar /
```

6. Использование команды tar для создания архивов в ФС ОС, а не только на устройствах для архивирования (можно архивировать группу файлов с их структурой каталогов в один файл, для чего передать имя создаваемого файла с помощью параметра f вместо имени устройства)

```
tar cvf /home/backup.tar /home/dave
```

С помощью tar архивируется каталог с вложенными подкаталогами.

При этом создается файл /home/backup.tar, содержащий архив каталога /home/dave и всех файлов в его подкаталогах.

Обычно при использовании команды tar следует делать входом верхнего уровня каталог. В таком случае файлы при восстановлении будут располагаться в подкаталоге рабочего каталога.

Предположим, в рабочем каталоге имеется подкаталог data, содержащий несколько сотен файлов. Существует два основных пути создания архива этого каталога. Можно войти в подкаталог и создать в нем архив, например:

```
pwd
/home/dave
cd data
pwd
/home/dave/data
tar cvf .. /data.tar *
```

Будет создан архив в каталоге /home/dave, содержащий файлы без указания их расположения в структуре каталогов. При попытке восстановить файлы из архива data.tar подкаталог не будет создан, и все файлы будут восстановлены в текущем каталоге.

Другой путь состоит в создании архива каталога, например:

```
pwd
/home/dave
tar cvf data.tar data
```

Будет создан архив каталога, в котором первой будет следовать ссылка на каталог. При восстановлении файлов из такого архива будет создан подкаталог в текущем каталоге, и файлы будут восстанавливаться в нем.

Можно автоматизировать выполнение данных команд, поместив их в файл crontab суперпользователя. Например, следующая запись в файле crontab выполняет резервное копирование каталога /home ежедневно в 01:30:

```
30 01 *** tar -cvfz /dev/hda4 /home > home index
```

При необходимости более сложного архивирования используется язык сценариев оболочки, которые также могут быть запущены с помощью cron (см. 4.4.1.2).

Порядок использования команды tar для сохранения и восстановления мандатных атрибутов файлов описан в РУСБ.10015-01 97 01-1.

18.5.2. cpio

Для копирования файлов используется команда общего назначения `cpio`.

Команда используется с параметром `-o` для создания резервных архивов и с параметром `-i` — для восстановления файлов. Команда получает информацию от стандартного устройства ввода и посылает выводимую информацию на стандартное устройство вывода.

Команда `cpio` может использоваться для архивирования любого набора файлов и специальных файлов. Она пропускает сбойные сектора или блоки при восстановлении данных, архивы могут быть восстановлены в ОС

Недостатком команды `cpio` является необходимость использовать язык программирования оболочки для создания соответствующего сценария, чтобы обновить архив.

В таблице 61 приведены основные параметры команды `cpio`.

Таблица 61

Параметр	Назначение
`-o`	Создание архива в стандартное устройство вывода
`-l`	Восстановление файлов из архива, передаваемого на стандартное устройство ввода
`-t`	Создание списка содержимого стандартного устройства ввода

Подробное описание команды приведено в `man cpio`.

Примеры:

1. Копирование файлов из каталога `/home` в архив `home.cpio`

```
find /home/* | cpio -o > /tmp/home.cpio
```

2. Восстановление файлов из архива `home.cpio` с сохранением дерева каталогов и создание списка в файле `bkup.index`

```
cpio -id < /tmp/home.cpio > bkup.index
```

3. Использование команды `find` для поиска измененных за последние сутки файлов и сохранение их в архив `home.new.cpio`

```
find /home -mtime 1 -type f | cpio -o > /tmp/home.new.cpio
```

4. Восстановление файла `/home/dave/notes.txt` из архива `home.cpio`

```
cpio -id /home/dave/notes.txt < home.cpio
```

Для восстановления файла с помощью `cpio` следует указывать его полное имя.

Можно автоматизировать выполнение данных команд, поместив их в файл `crontab` суперпользователя. Например, следующая запись в файле `crontab` выполняет резервное копирование каталога `/home` ежедневно в 01:30:

```
30 01 *** ls /home : cpio –o > /tmp/home.cpio
```

При необходимости более сложного резервного копирования можно создать соответствующий сценарий оболочки. Запуск подобных сценариев также может быть осуществлен посредством `cron`.

Создание резервных копий означает определение политики создания резервных копий для снижения потерь и восстановления информации после возможной аварии системы.

19. КОНТРОЛЬ ПОДКЛЮЧАЕМЫХ УСТРОЙСТВ

В состав ОС входит средство контроля подключения устройств (СКПУ). Механизм работы СКПУ основан на правилах `udev`. Подробное описание правил `udev` приведено на справочной странице `man udev`.

СКПУ обеспечивает контроль подключения к шине USB различных устройств (сканеры, съемные накопители, видеокамеры и т.п.). Для таких устройств в СКПУ можно подготовить следующие типы правил:

1) блокирующее — устанавливает запрет на использование устройства;
2) разрешающее — устанавливает разрешение на использование устройства;
3) назначающее правило — устанавливает разрешение на использование устройства и назначает права доступа, правила регистрации событий и метку безопасности. Назначающие правила можно подготовить только для следующих типов устройств:
   - носители информации или устройства для их считывания (flash-накопители, SD-карты, внешние HDD/SSD, floppy-привод, оптический привод и т.д.);
   - устройства, для взаимодействия с которыми используется протокол MTP (цифровые фотокамеры, смартфоны, электронные книги и т.д.);
   - аудиоустройства (микрофоны, колонки, переходники USB/Jack и т.д.);
   - видеоустройства (веб-камеры, адаптеры видеозахвата и т.д.).

В СКПУ можно подготовить блокирующие и разрешающие правила для группы устройств определенного типа. Для многосоставных устройств, в которых объединены устройства различных типов (например, веб-камера с интегрированным микрофоном), можно включить режим усиленной блокировки (см. 19.4.4).

В ОС каждому разделу съемного накопителя соответствует отдельный файл устройства. При этом не допускается создавать отдельные правила для съемного накопителя и для его раздела. Если на съемном накопителе находится несколько разделов, то правило СКПУ будет применено ко всем разделам на этом накопителе. При подготовке съемного накопителя к использованию в ОС рекомендуется руководствоваться принципом «одно устройство — один дисковый раздел».

Для управления правилами и непосредственно механизмом работы СКПУ используется инструмент командной строки `pdac-adm`. С помощью этого инструмента можно:

1) вывести перечень подключенных устройств и их статус, а также идентификационные параметры. Кроме того, можно вывести правила классификации, по которым определяется тип устройства (подробнее см. 19.1);
2) добавить, изменить или удалить правило СКПУ (см. 19.2);
3) запустить генерацию правил `udev` на основе правил СКПУ (см. 19.3);

4) выключить или включить СКПУ, а также управлять режимами его работы (см. 19.4).

19.1. Информация об устройствах и их типах

19.1.1. Идентификационные параметры устройств

При создании правил используются следующие идентификационные параметры устройств:

1) `serial` — серийный номер;

2) `model` — идентификатор модели;

3) `vendor` — идентификатор производителя;

4) `dev` — путь к файлу устройства, который размещен в каталоге `/dev/`. Используется для удобства добавления правил СКПУ. При сохранении правила будет автоматически заменен на серийный номер устройства.

Примечание. Определить значения идентификационных параметров устройств, которые подключены в ОС, можно с помощью инструмента `pdac-adm` (см. 19.1.2).

Для указания типа устройств применяется идентификационный параметр `type`, который принимает одно из следующих значений:

1) `storage` — носители информации, устройства для их считывания;

2) `printer` — принтеры, сканеры, МФУ;

3) `security_cardreader` — устройства безопасности, считыватели карт, токены;

4) `image_mtp` — устройства, для взаимодействия с которыми используется протокол MTP;

5) `audio` — аудиоустройства;

6) `video` — видеоустройства;

7) `communication` — устройства связи (LAN-адаптеры, WIFI-антенны и т.д.);

8) `hub` — хабы, переходники;

9) `hid` — интерфейсные устройства (клавиатуры, мыши, беспроводные ресиверы, MIDI-клавиатуры и т.д.);

10) `other` — прочие устройства (персональные медицинские устройства, микроконтроллеры и другие специфические устройства).

В СКПУ можно подготовить блокирующие и разрешающие правила для группы устройств одного типа.

Также в СКПУ применяется идентификационный параметр `bus`, для которого обязательно нужно указать значение `usb`. Этот параметр используется для подготовки блокирующего или разрешающего правила для шины USB.

При подключении устройства в ОС производится автоматическое определение его типа и наименование шины подключения. Для этого используются специальные правила классификации. Изменение этих правил не предусмотрено.

Для просмотра правил классификации выполнить команду:

```
sudo pdac-adm classification [параметры]
```

Описание параметров приведено в таблице 62.

Таблица 62

Параметр	Описание
`types`	Вывести правила классификации, по которым определяется тип устройства. При выполнении команды без параметров `types` и `buses` будет выведен перечень всех правил классификации
`buses`	Вывести правило классификации, по которому определяется наименование шины подключения. При выполнении команды без параметров `types` и `buses` будет выведен перечень всех правил классификации
`-H`, `--no-headers`	При выводе не отображать заголовки столбцов
`-J`, `--json`	Выводить информацию в формате JSON

19.1.2. Вывод информации об устройствах

Для вывода информации об устройствах, которые подключены в ОС, выполнить команду:

```
sudo pdac-adm devices [параметры]
```

Описание параметров приведено в таблице 63.

Таблица 63

Параметр	Описание
`tree`	Вывести перечень устройств в соответствии с порядком их подключения. При выполнении команды без параметра `tree` будет выведен перечень, в котором устройства сгруппированы по типам и шинам, к которым эти устройства подключены. Примечание. Одновременное использование параметров `tree` и `-e` не допускается
`-a`, `--all`	Дополнительно вывести информацию о всех составных частях устройств, для которых в СКПУ можно подготовить правила. Например, если у USB-накопителя `/dev/sdb` имеется раздел `/dev/sdb1`, то также будет выведена информация об этом разделе

Окончание таблицы 63

Параметр	Описание
`-H, --no-headers`	При выводе не отображать заголовки столбцов
`-J, --json`	Выводить информацию в формате JSON
`-V, --verbose`	Выводить подробную информацию

Примечание. Для действия `devices` допускается любой из вариантов укороченной записи: `device`, `devic`, `devi` или `dev`.

При выполнении команды без параметра `tree` будет выведена таблица, состоящая из следующих столбцов:

1) `BUS/TYPE/DEVICE` — наименование шины, типа устройств или экземпляра устройства;

2) `STATUS` — статус устройства, установленный в соответствии с правилами udev. Может принимать одно из следующих значений:

   а) `allowed` — использование устройства разрешено;

   б) `blocked` — использование устройства запрещено;

3) `INHERITED` — порядок присвоения статуса. Может принимать одно из следующих значений:

   а) `by bus` — статус был унаследован от шины;

   б) `by type` — статус был унаследован от типа устройств;

   в) `by rule` — статус установлен в соответствии с правилом;

4) `IDENTIFICATION` — значения идентификационных параметров.

При выполнении команды с параметром `tree` в таблице после столбца `INHERITED` будут дополнительно выведены следующие столбцы:

1) `TYPE` — тип устройства;

2) `BUS` — наименование шины, к которой подключено устройство.

Примечание. Будут выведены только устройства, для которых был автоматически определен их тип по правилам классификации (см. 19.1.1)

.

Примеры:

1. Пример вывода команды без параметра `tree`:

```
BUS/TYPE/DEVICE                                          STATUS  INHERITED
IDENTIFICATION
```

```
Устройства интерфейса USB (usb)                          allowed
bus=usb
Носители информации (storage)                            allowed
bus=usb,type=storage
JetFlash (Transcend Information, Inc.)                   allowed
serial=06ZC7LCZYRBQNCDY,vendor=8564,model=1000,dev=/dev/bus/usb/001~
Устройства безопасности, считыватели карт (security_~ allowed
bus=usb,type=security_cardreader
58200 (Broadcom Corp.)                                   allowed
serial=0123456789ABCD,vendor=0a5c,model=5842,dev=/dev/bus/usb/001/0~
Видеоустройства (video)                                  allowed
bus=usb,type=video
Integrated_Webcam_HD (Microdia)                          allowed
serial=CN0XYXJ28LG0028JAFM3A00_Integrated_Webcam_HD,vendor=0c45,mod~
Хабы, переходники (hub)                                  allowed
bus=usb,type=hub
2.0 root hub (Linux Foundation)                          allowed
serial=0000:00:0d.0,vendor=1d6b,model=0002,dev=/dev/bus/usb/003/001
3.0 root hub (Linux Foundation)                          allowed
serial=0000:00:0d.0,vendor=1d6b,model=0003,dev=/dev/bus/usb/004/001
4-Port_USB_3.0_Hub (Realtek Semiconductor Corp.)         allowed
serial=Generic_4-Port_USB_3.0_Hub,vendor=0bda,model=0423,dev=/dev/~
2.0 root hub (Linux Foundation)                          allowed
serial=0000:00:14.0,vendor=1d6b,model=0002,dev=/dev/bus/usb/001/001
4-Port_USB_2.0_Hub (Realtek Semiconductor Corp.)         allowed
serial=Generic_4-Port_USB_2.0_Hub,vendor=0bda,model=5423,dev=/dev/~
3.0 root hub (Linux Foundation)                          allowed
serial=0000:00:14.0,vendor=1d6b,model=0003,dev=/dev/bus/usb/002/001
2.0 root hub (Linux Foundation)                          allowed
serial=vhci_hcd.0,vendor=1d6b,model=0002,dev=/dev/bus/usb/005/001
3.0 root hub (Linux Foundation)                          allowed
serial=vhci_hcd.0,vendor=1d6b,model=0003,dev=/dev/bus/usb/006/001
Интерфейсные устройства (hid)                            allowed
bus=usb,type=hid
Unifying Receiver (Logitech, Inc.)                       allowed
serial=Logitech_USB_Receiver,vendor=046d,model=c534,dev=/dev/bus/~
Прочие устройства (other)                                allowed
bus=usb,type=other
D-Link_DWA-160_Xtreme_N_Dual_Band_USB_Adapter_rev.~ allowed
serial=20130629,vendor=2001,model=3c21,dev=/dev/bus/usb/001/009
```

2. Пример вывода команды с параметром `tree`:

```
BUS/TYPE/DEVICE                                          STATUS  INHERITED
TYPE           BUS  IDENTIFICATION
```

```
2.0 root hub (Linux Foundation)                          allowed
hub            usb  serial=0000:00:0d.0,vendor=1d6b,model=0002,de~
3.0 root hub (Linux Foundation)                          allowed
hub            usb  serial=0000:00:0d.0,vendor=1d6b,model=0003,de~
4-Port_USB_3.0_Hub (Realtek Semiconductor Corp.)     allowed
hub            usb  serial=Generic_4-Port_USB_3.0_Hub,vendor=0bda~
2.0 root hub (Linux Foundation)                          allowed
hub            usb  serial=0000:00:14.0,vendor=1d6b,model=0002,de~
58200 (Broadcom Corp.)                                   allowed
security_card~ usb  serial=0123456789ABCD,vendor=0a5c,model=5842,~
Integrated_Webcam_HD (Microdia)                          allowed
video          usb  serial=CN0XYXJ28LG0028JAFM3A00_Integrated_Web~
4-Port_USB_2.0_Hub (Realtek Semiconductor Corp.)     allowed
hub            usb  serial=Generic_4-Port_USB_2.0_Hub,vendor=0bda~
JetFlash (Transcend Information, Inc.)               allowed
storage        usb  serial=06ZC7LCZYRBQNCDY,vendor=8564,model=100~
Unifying Receiver (Logitech, Inc.)                   allowed
hid            usb  serial=Logitech_USB_Receiver,vendor=046d,mode~
D-Link_DWA-160_Xtreme_N_Dual_Band_USB_Adapter_rev.C~ allowed
other          usb  serial=20130629,vendor=2001,model=3c21,dev=/d~
3.0 root hub (Linux Foundation)                          allowed
hub            usb  serial=0000:00:14.0,vendor=1d6b,model=0003,de~
2.0 root hub (Linux Foundation)                          allowed
hub            usb  serial=vhci_hcd.0,vendor=1d6b,model=0002,dev=~
3.0 root hub (Linux Foundation)                          allowed
hub            usb  serial=vhci_hcd.0,vendor=1d6b,model=0003,dev=~
```

19.2. Управление правилами СКПУ

19.2.1. Наследование и приоритет правил

В СКПУ установлена следующая иерархия объектов контроля (сущностей, для которых можно подготовить правило):

1) шина, к которой может быть подключено устройство;
2) тип устройства;
3) экземпляр устройства.

Правила наследуются сверху вниз в соответствии с иерархией. При этом чем ниже ступень иерархии, тем выше приоритет применения правила.

Пример

Для запрета использовать любые носители информации, кроме одного разрешенного USB-накопителя, требуется добавить одно блокирующее правило для устройств типа `storage` и одно разрешающее правило для конкретного экземпляра USB-накопителя.

19.2.2. Синтаксис правила СКПУ

В СКПУ можно подготовить правила только для тех устройств, для которых может быть автоматически определен их тип по правилам классификации (см. 19.1.1).

Используется следующий синтаксис правил:

```
[параметры_правила],<тип_правила>,<идентификационные_параметры>,
[параметры_доступа]
```

где `[параметры_правила]` — дополнительные параметры правила, которые перечисляются через запятую в формате `<параметр>=<значение>`. Для правила могут быть заданы значения следующих параметров:

1) `name` — наименование правила. Если параметр не указан, то правилу будет присвоено наименование вида `<тип_устройства>_<идентификационные_параметры>_<тип_правила>`.

Примечание. Если в правиле указаны идентификационные параметры конкретного экземпляра устройства, то вместо префикса <тип_устройства> используется условное наименование `device`;

2) `active` — флаг применимости (активности). Может принимать одно из следующих значений:

а) `true` — правило активно, т.е. правило будет применено при подключении устройства;

б) `false` — правило не активно, т.е. правило не будет применено при подключении устройства. Если параметр не указан, то параметру будет присвоено значение `true`;

3) `desc` — описание правила. Если параметр не задан, то у правила не будет описания;

`<тип_правила>` — тип правила, может принимать одно из следующих значений:

1) `allow` — разрешающее или назначающее. Для назначающего правила необходимо дополнительно задать `[параметры_доступа]`;

2) `block` — блокирующее;

<идентификационные_параметры> — идентификационные параметры (см. 19.1.1), которые перечисляются через запятую в формате <параметр>=<значение>;

[параметры_доступа] — параметры доступа для устройства, которые необходимо указать в назначающем правиле. Параметры доступа перечисляются через запятую в формате <параметр>=<значение>. Допускается не задавать значения для всех параметров доступа. В этом случае будут установлены значения по умолчанию. В набор включены следующие параметры доступа:

1) owner — имя пользователя, который будет назначен пользователем-владельцем. Значение по умолчанию root;

2) group — наименование группы пользователей, которая будет назначена группой-владельцем. Значение по умолчанию root;

3) mode — набор прав доступа (в формате строки из трех восьмеричных цифр). Значение по умолчанию 660;

4) audit — флаги аудита. Значение по умолчанию 0x0:0x0;

5) pdpl — метка безопасности. Значение по умолчанию 0:0:0x0:0x0!.

ВНИМАНИЕ! Параметры доступа назначаются комплексно. Если в правиле СКПУ указан хотя бы один параметр доступа, то для остальных параметров будут заданы значения, установленные по умолчанию в СКПУ.

Примечания:

1. Назначающие правила можно подготовить только для следующих типов устройств:

а) storage (носители информации, устройства для их считывания);

б) image_mtp (устройства, для взаимодействия с которыми используется протокол MTP);

в) audio (аудиоустройства);

г) video (видеоустройства).

2. Если [параметры_доступа] в правиле не заданы, то монтирование ФС блочных устройств будет выполняться по правилам, которые описаны в 19.6.

3. Мандатное управление доступом к устройствам реализуется только на уровне защищенности «Смоленск» при включенном мандатном управлении доступом. В правилах, применяемых на уровне защищенности, отличном от «Смоленск», в метке безопасности должен быть задан нулевой уровень конфиденциальности и должны отсутствовать категории конфиденциальности.

Примеры:

1. Разрешающее правило для устройства с идентификатором производителя `152d` и идентификатором модели `0580`:

```
allow,vendor=152d,model=0580
```

2. Назначающее правило для USB-накопителя с серийным номером `DD564198838FA`:

```
allow,serial=DD564198838FA,owner=astra
```

В представленном примере при подключении в ОС устройству будут назначены следующие значения параметров доступа:

а) пользователь-владелец `astra`;

б) группа-владелец `root` (значение по умолчанию);

в) набор прав доступа `660` (значение по умолчанию);

г) флаги аудита `0x0:0x0` (значение по умолчанию);

д) метка безопасности `0:0:0x0:0x0!` (значение по умолчанию).

3. Правило с наименованием `dev_2` и описанием «`flashdisk-2`», разрешающее использование устройства, для которого был создан файл `/dev/sdb1`:

```
name=dev_2,desc="flashdisk-2",allow,dev=/dev/sdb1
```

Примечание. В процессе сохранения этого правила идентификационный параметр `dev` будет автоматически заменен на `serial`.

19.2.3. Добавление правила СКПУ

Для добавления нового правила применяется следующая команда:

```
sudo pdac-adm rules add <правило>
```

где `<правило>` — правило подключения устройства (см. 19.2.2).

Примечание. Для действия `rules` допускается любой из вариантов укороченной записи: `rule` или `rul`.

ВНИМАНИЕ! Запрещается создавать несколько правил, в которых указаны одни и те же идентификационные параметры.

19.2.4. Просмотр правил СКПУ

Для просмотра правил СКПУ применяется следующая команда:

```
sudo pdac-adm rules
```

Примечание. Для действия `rules` допускается любой из вариантов укороченной записи: `rule` или `rul`.

Будет выведена таблица, состоящая из следующих столбцов:

1) `TYPE` — тип правила (см. 19.2.2);

2) `ACTIVE` — флаг применимости (активности), может принимать одно из следующих значений:

   а) `yes` — правило активно, т.е. правило будет применено при подключении устройства;

   б) `no` — правило не активно, т.е. правило не будет применено при подключении устройства;

3) `NAME` — наименование правила;

4) `EXPRESSIONS` — идентификационные параметры устройства (см. 19.1.1), которые перечислены через запятую в формате `<параметр>==<значение>`;

5) `ASSIGNATIONS` — параметры доступа (см. 19.2.2), которые перечислены через запятую в формате `<параметр>==<значение>`;

6) `DESCRIPTION` — описание правила.

Пример

Вывод после выполнения команды:

```
TYPE  ACTIVE   NAME              EXPRESSIONS
ASSIGNATIONS     DESCRIPTION
allow yes      device_152d_05~   vendor==152d,model==0580
allow yes      device_DD56419~   serial==DD564198838FA
pdpl=0:0:0x0:0x0!,audit=0x0:0x0,rights=astra,root~
allow yes      dev_2             serial==E5B92A75EAE94DB4
flashdisk-2
```

Правила СКПУ хранятся в файле `/etc/parsec/PDAC/devices.cfg`.

Примечание. Если в правиле заданы значения параметров доступа, то в файле `/etc/parsec/PDAC/devices.cfg` для параметра `type` (тип правила) будет указано значение `by_rule` (назначающее правило).

Пример

Содержание файла /etc/parsec/PDAC/devices.cfg:

```
device_152d_0580_allow :
{
type = "allow";
enabled = true;
description = "";
expressions = ( "vendor==152d", "model==0580" );
};
device_DD564198838FA_allow :
{
type = "by_rule";
enabled = true;
description = "";
expressions = ( "serial==DD564198838FA" );
user = "astra";
group = "root";
mode = "660";
pdpl = "0:0:0x0:0x0!";
audit = "0x0:0x0";
};
dev_2 :
{
type = "allow";
enabled = true;
description = "flashdisk-2";
expressions = ( "serial==E5B92A75EAE94DB4" );
};
```

19.2.5. Изменение правила СКПУ

Допускается изменить значения параметров правила, а также добавить, изменить и удалить параметры доступа.

ВНИМАНИЕ! Изменение наименование правила и идентификационных параметров устройства не предусмотрено. Вместо этого необходимо удалить правило, а затем создать новое.

Для изменения имеющегося правила применяется следующая команда:

```
sudo pdac-adm rules modify <имя_правила> [тип_правила],[параметры_правила],
[параметры_доступа]
```

где <имя_правила> — наименование правила. Если при добавлении правила не было задано его наименование, то по умолчанию правилу было присвоено наименование вида <тип_устройства>_<идентификационные_параметры>_<тип_правила>
Примечание. Если в правиле указаны идентификационные параметры конкретного экземпляра устройства, то вместо префикса <тип_устройства> используется условное наименование device;

[тип_правила] — тип, который требуется назначить правилу.
ВНИМАНИЕ! При изменении типа правила его наименование не меняется. Например, если для разрешающего правила device_DD564198838FA_allow заменить его тип на блокирующее, то в наименовании этого правила по-прежнему будет суффикс allow;

[параметры_правила] — новые значения параметров правила (флаг применимости и описание). Параметры доступа перечисляются через запятую в формате <параметр>=<значение>. Указываются только те параметры доступа, значения которых требуется изменить;

[параметры_доступа] — новые значения параметров доступа. Параметры доступа перечисляются через запятую в формате <параметр>=<значение>. Указываются только те параметры доступа, значения которых требуется изменить. Если для какого-то параметра требуется установить значение по умолчанию, то для такого параметра необходимо задать пустое значение.

Примечания:

1. Для действия rules допускается любой из вариантов укороченной записи: rule или rul.
2. Для ключа modify допускается любой из вариантов укороченной записи: modif, modi или mod.

Если при подготовке правила не были указаны параметры доступа, то их можно добавить.

ВНИМАНИЕ! Параметры доступа назначаются комплексно. Если в правиле СКПУ указан хотя бы один параметр доступа, то для остальных параметров будут заданы значения, установленные по умолчанию в СКПУ (см. 19.2.2).

Пример

В правило dev_2 добавить параметры доступа:

1) пользователь-владелец astra;
2) группа-владелец astra;
3) набор прав доступа 770;
4) флаги аудита 0x0:0x0 (значение по умолчанию);
5) метка безопасности 0:0:0x0:0x0! (значение по умолчанию).

Команда изменения правила:

```
sudo pdac-adm rules modify dev_2 owner=astra,mode=770,group=astra
```

Т.к. для параметров audit и pdpl необходимо задать значения, которые используются по умолчанию, то в команде они не указаны.

Если в правиле нужно изменить параметры доступа, то в команде следует указать один или несколько параметров с новыми значениями. Если параметр не указан в команде, то он останется без изменений.

Примеры:

1. В правиле dev_2 изменить флаги аудита и метку безопасности:

```
sudo pdac-adm rules modify dev_2 audit=0x21:0x21,pdpl=1:0:0x0:0x0!
```

2. В правиле dev_2 задать следующие значения параметров доступа:
   а) пользователь-владелец flashowner;
   б) группа-владелец users;
   в) набор прав доступа 640;
   г) флаги аудита 0xa1:0x21;
   д) метка безопасности 1:0:0x2:0x0!.

Команда изменения правила:

```
sudo pdac-adm rules modify dev_2 owner=flashowner,group=users,mode=640,\
audit=0xa1:0x21,pdpl=1:0:0x2:0x0!
```

Если в правиле для каких-либо параметров доступа нужно установить значение по умолчанию, то для этих параметров, но не для всех одновременно, задать пустые значения.

Примеры:

1. В правиле dev_2 для группы-владельца установить значение по умолчанию (root):

```
sudo pdac-adm rules modify dev_2 group=
```

2. В правиле dev_2 установить значения по умолчанию для флагов аудита (0x0:0x0) и метки безопасности (0:0:0x0:0x0!):

```
sudo pdac-adm rules modify dev_2 audit=,pdpl=
```

Если в правиле нужно удалить все параметры доступа, то для всех параметров доступа одновременно задать пустые значения.

Пример

В правиле dev_2 удалить все параметры доступа:

```
sudo pdac-adm rules modify dev_2 owner=,group=,mode=,audit=,pdpl=
```

Примечание. Если в правиле не заданы параметры доступа, то монтирование ФС блочных устройств будет выполняться по правилам, которые описаны в 19.6.

Правило можно временно выключить (деактивировать). В этом случае правило не будет применено при подключении устройства.

Пример

Временно выключить правило dev_2 и изменить его описание:

```
sudo pdac-adm rules modify dev_2 active=false,desc="временно выключено"
```

19.2.6. Удаление правил СКПУ

19.2.6.1. Удаление правила с заданным наименованием

Для удаления правила СКПУ применяется следующая команда:

```
sudo pdac-adm rules delete <имя_правила>
```

где <имя_правила> — наименование правила. Если при добавлении правила не было задано его наименование, то по умолчанию правилу было присвоено наименование вида <тип_устройства>_<идентификационные_параметры>_<тип_правила>

Примечание. Если в правиле указаны идентификационные параметры конкретного экземпляра устройства, то вместо префикса <тип_устройства> используется условное наименование device.

Примечания:

1. Для действия rules допускается любой из вариантов укороченной записи: rule или rul.
2. Для ключа delete допускается любой из вариантов укороченной записи: delet, dele или del.

Пример

Удалить правило с наименованием dev_2:

```
sudo pdac-adm rules delete dev_2
```

19.2.6.2. Удаление правила с заданными значениями параметров

В СКПУ можно удалить правило, в котором один или несколько параметров имеют указанные значения. Для этого применяется команда:

```
sudo pdac-adm rules delete <параметр>=<значение>[,<параметр>=<значение>]
```

Примечания:

1. Для действия rules допускается любой из вариантов укороченной записи: rule или rul.
2. Для ключа delete допускается любой из вариантов укороченной записи: delet, dele или del.

Пример

Удалить правило для устройства с серийным номером 234567890126:

```
sudo pdac-adm rules delete serial=234567890126
```

С помощью этой команды можно удалить только одно правило. Если указанные значения параметров содержатся в нескольких правилах, то в выводе команды будет отображено предупреждение и список правил, который соответствует указанным параметрам:

```
pdac-adm: deleting multiple rules is prohibited: <перчень_правил>
```

В случае если требуется одновременно удалить нескольких правил, то в команде необходимо указать параметр `--force` или `-f`. Рекомендуется предварительно выполнить команду без этого параметра, чтобы просмотреть перечень правил, которые будут удалены.

Пример

Удалить все активные правила, в которых пользователем-владельцем назначается `astra`:

```
sudo pdac-adm rules delete active=true,user=astra --force
```

19.3. Применение правил в ОС

Чтобы правила СКПУ начали применяться в ОС, необходимо на их основе сгенерировать правила `udev`. Генерацию правил `udev` требуется выполнять после любых действий с правилами в СКПУ — создание, удаление или изменение.

Для генерации правил `udev` на основе правил СКПУ выполнить команду:

```
sudo pdac-adm commit
```

или

```
sudo pdac-adm generate
```

Если к компьютеру были подключены какие-либо устройства, то для применения сгенерированных правил требуется переподключить эти устройства или выполнить команду:

```
sudo udevadm trigger
```

Также правила будут применены после перезагрузки ОС.

19.4. Управление СКПУ

С помощью инструмента `pdac-adm` можно:

1) включить или выключить СКПУ (см. 19.4.1);
2) включить или выключить регистрацию событий, связанных с контролем подключения устройств (см. 19.4.2);
3) включить или выключить режим защиты критически важных устройств (см. 19.4.3);
4) включить или выключить режим усиленной блокировки многосоставных устройств (см. 19.4.4).

Для вывода справки инструмента `pdac-adm` выполнить команду:

```
sudo pdac-adm --help
```

Примечание. Для параметра `-help` допускается укороченная запись `-h`.

Для вывода информации о версии инструмента pdac-adm выполнить команду:

```
sudo pdac-adm --version
```

Примечание. Для параметра `-version` допускается укороченная запись `-v`.

19.4.1. Включение и выключение СКПУ

По умолчанию СКПУ включено. При этом при подключении устройств применяются системные правила `udev`, созданные при установке пакета `systemd`, или пользовательские правила `udev`, подготовленные с помощью других средств.

Для включения и выключения СКПУ используется следующая команда:

```
sudo pdac-adm state [enable|disable]
```

или

```
sudo pdac-adm status [enable|disable]
```

Выполнение команды без указания параметра отображает текущее состояние СКПУ. Описание параметров приведено в таблице 64.

Таблица 64

Параметр	Описание
`disable`	Выключить СКПУ. При этом правила `udev` , сгенерированные на основе правил СКПУ, будут удалены. Но файл с правилами СКПУ `/etc/parsec/PDAC/devices.cfg` сохранится
`enable`	Включить СКПУ. При этом на основе имеющихся правил СКПУ будут сгенерированы правила `udev`

Для вступления изменений в силу требуется перезагрузка ОС.

19.4.2. Включение и выключение регистрации событий

С помощью инструмента `pdac-adm` можно включить или выключить регистрацию событий, связанных с контролем подключения устройств (регистрация результатов применения блокирующих, разрешающих или назначающих правил при подключении устройств).

По умолчанию регистрация событий выключена

Для включения и выключения регистрации событий используется команда:

```
sudo pdac-adm audit [enable|disable]
```

где параметр `enable` используется для включения регистрации событий;
параметр `disable` используется для выключения регистрации событий.

Изменения будут применены сразу.

Выполнение команды без параметра отображает текущее состояние регистрации событий.

19.4.3. Режим защиты от блокировки критически важных устройств

Режим защиты от блокировки критически важных устройств предотвращает случайную блокировку устройств ввода (клавиатура, мышь и т.д.).

При включении этого режима игнорируются имеющиеся блокирующие правила для устройств типа `hub` и `hid`. Кроме того, устанавливается запрет на изменение или удаление этих правил. Также для устройств типа `hub` и `hid` игнорируется наследование блокирующего правила шины подключения устройств.

Режим защиты от блокировки критически важных устройств включен по умолчанию. Для выключения и включения этого режима используется команда:

```
sudo pdac-adm protect-critical-devices [enable|disable]
```

где параметр `enable` используется для включения режима защиты от блокировки критически важных устройств;
параметр `disable` используется для выключения режима защиты от блокировки критически важных устройств.

Изменения будут применены сразу.

Выполнение команды без параметра отображает текущее состояние режима защиты от блокировки критически важных устройств.

19.4.4. Режим усиленной блокировки многосоставных устройств

Режим усиленной блокировки многосоставных устройств обеспечивает блокировку устройств, в которых объединены устройства различных типов, например веб-камера с интегрированным микрофоном.

При включении этого режима многосоставное устройство будет заблокировано, если имеется блокирующее правило для хотя бы одного из типов устройств в его составе. Например, использование веб-камеры с интегрированным микрофоном будет запрещено, даже если имеется разрешающее правило для устройств типа `video`, но при этом также имеется блокирующее правило для устройств типа `audio`.

Режим усиленной блокировки многосоставных устройств по умолчанию выключен. Для включения и выключения этого режима используется команда:

```
sudo pdac-adm force-deny [enable|disable]
```

где параметр `enable` используется для включения режима усиленной блокировки многосоставных устройств;
параметр `disable` используется для выключения режима усиленной блокировки многосоставных устройств.

Изменения будут применены сразу.

Выполнение команды без параметра отображает текущее состояние режима усиленной блокировки многосоставных устройств.

19.5. Управление подключением устройств с помощью графической утилиты

Контроль подключения устройств также можно настроить с использованием модуля «Устройства и правила» графической утилиты `astra-systemsettings` («Параметры системы»),

описание модуля приведено в электронной справке. Для вызова модуля можно использовать команду:

```
astra-systemsettings astra_kcm_devices_and_rules
```

19.6. Монтирование съемных накопителей

Для того, чтобы устройство могло быть примонтировано, на нем должна быть размечена файловая система (устройство должно быть отформатировано).

Для монтирования ФС блочных устройств в командной строке используется инструмент `mount`, который позволяет:

- монтировать ФС произвольных блочных устройств в произвольные точки монтирования. Выполнение такого монтирования доступно только администраторам;
- непривилегированным пользователям из системной группы `floppy` монтировать ФС оптических дисков в каталог `/media/cdrom0`. Правило монтирования задано в файле `/etc/fstab`;
- непривилегированным пользователям из системной группы `floppy` монтировать ФС определенных типов в каталог `/run/user/<UID>/media/<UUID_монтируемой_ФС>/`. Список типов ФС задан в файле `/etc/fstab.pdac`.

Примечание. Пользователям из системной группы `cdrom` разрешено выполнять операции чтения и записи в ФС оптических дисков, но не разрешено монтировать эти ФС.

В команде монтирования с использованием инструмента `mount` необходимо указать наименование файла устройства и наименование точки монтирования. Остальные параметры монтирования выбираются из файлов `/etc/fstab` и `/etc/fstab.pdac`.

Для монтирования различных типов ФС разделов USB-накопителей в файл `/etc/fstab.pdac` включены следующие записи:

```
/dev/*fat       /run/user/*/media/*  auto    pdac,noauto,nodev,defaults  0 0
/dev/*ntfs*     /run/user/*/media/*  auto    pdac,noauto,nodev,iocharset=utf8,\
defaults  0 0
/dev/sd*ext*    /run/user/*/media/*  auto    pdac,nodev,noauto,defaults  0 0
/dev/sd*iso9660 /run/user/*/media/*  iso9660 pdac,nodev,noexec,noauto,\
defaults  0 0
/dev/sd*        /run/user/*/media/*  auto    owner,group,nodev,noexec,noauto,\
iocharset=utf8,defaults  0 0
```

Для монтирования различных типов ФС оптических дисков в файл /etc/fstab.pdac включены следующие записи:

```
/dev/s*udf        /run/user/*/media/*  udf      pdac,nodev,noexec,noauto,\
defaults  0 0
/dev/sr*iso9660   /run/user/*/media/*  iso9660  pdac,nodev,noexec,noauto,\
defaults  0 0
```

Для монтирования ФС оптических дисков в каталог /media/cdrom0/ включена следующая строка в файл /etc/fstab:

```
/dev/sr0    /media/cdrom0   udf,iso9660   user,noauto 0 0
```

Эта запись необходима для корректной работы инструмента apt при установке пакетов с оптического диска. При этом остается возможность монтировать любой оптический диск в каталог /media/cdrom0. Если для установки пакетов оптические диски не используются, то эту строку рекомендуется удалить.

Примечание. Установить запрет на монтирование ФС пользователями из системной группы floppy можно с помощью инструмента astra-mount-lock (см. РУСБ.10015-01 97 01-1).

Для непривилегированных пользователей из системной группы floppy доступно полуавтоматическое монтирование в графической среде (в утилите fly-fm «Менеджер файлов» или с помощью инструмента fly-reflex-service из окружения рабочего стола, см. электронную справку).

19.7. Безопасная эксплуатация ОС при подключении съемных накопителей

При обработке в системе конфиденциальной информации рекомендуется настраивать и контролировать использование съемных накопителей. Способы контроля подключения устройств:

- редактирование файла /etc/fstab.pdac;
- ограничение доступа с помощью назначающих правил;
- исключение пользователей из групп floppy и cdrom;
- применение блокирующего правила для устройств типа storage;
- включение запрета на монтирование съемных накопителей пользователями из группы floppy с помощью инструмента astra-mount-lock (см. РУСБ.10015-01 97 01-1).

При размещении конфиденциальной информации на съемных накопителях с твердотельными носителями информации (SSD, Flash) следует учитывать их технические особенности. Механизм очистки освобождаемых блоков ФС не может гарантировать полное удаление конфиденциальной информации, записанной на такой накопитель.

Кроме того, наличие физического доступа к любому устройству хранения информации позволяет прочитать с него все записанные данные, независимо от наличия и содержания меток безопасности. При использовании съемных накопителей для хранения конфиденциальной информации должны быть выполнены следующие требования:

- ограничен физический доступ к съемным накопителям;
- применено защитное преобразование информации, которая хранится на съемном накопителе.

19.8. Использование устройств в ненулевой сессии

По умолчанию всем подключаемым устройствам присваивается нулевая метка безопасности. В ненулевой сессии (на уровне конфиденциальности, отличном от 0) можно использовать устройство, для которого задано назначающее правило. Назначающее правило для локальных пользователей необходимо подготовить в СКПУ (см. 19.2) или с использованием модуля «Устройства и правила» графической утилиты «Параметры системы» (см. электронную справку). Назначающее правило для пользователей домена FreeIPA необходимо подготовить в веб-интерфейсе контроллера домена (см. 19.9). При этом в правиле должны быть указаны значения следующих параметров доступа:

- пользователи, которым разрешено использование устройства;
- метка безопасности устройства.

Устройство можно использовать (например, монтировать с правами на чтение, запись и выполнение) на том уровне конфиденциальности сессии пользователя, который задан в правиле для этого устройства. В сессии пользователя, уровень конфиденциальности которой выше заданного в правиле, устройство можно использовать только с правами на чтение.

Для USB-накопителей правила мандатного управления доступом применяется к дисковыми разделам. Если на USB-накопителе находится несколько разделов, то метка безопасности, заданная в назначающем правиле, будет назначена всем разделам.

ФС ext2, ext3, ext4 и XFS обеспечивают хранение расширенных атрибутов файловых объектов. В расширенных атрибутах может быть размещена информация о владельцах и правах доступа, а также метка безопасности файлового объекта.

Раздел USB-накопителя с ФС, поддерживающей расширенные атрибуты файловых объектов, следует подготовить для использования на ненулевом уровне конфиденциальности. Для этого назначить его корневой ФС уровень конфиденциальности, который задан в правиле

для этого USB-накопителя (или будет задан), а также назначить пользователя-владельца и группу-владельца. Чтобы подготовить раздел USB-накопителя, необходимо:

1) примонтировать ФС раздела USB-накопителя. Каталог монтирования должен располагаться внутри каталога, имеющего атрибут `ccnr` и уровень конфиденциальности не ниже уровня, который требуется назначить USB-накопителю. В ОС монтирование устройства по умолчанию осуществляется в каталог `/run/user/<UID>/media/<UUID_монтируемой_ФС>/` (каталог `/run/` имеет максимальный в ОС уровень конфиденциальности и атрибут `ccnr`);

2) назначить каталогу монтирования уровень конфиденциальности, который задан в правиле для этого USB-накопителя (или будет задан):

```
sudo pdpl-file <уровень> /run/<каталог_монтирования>
```

3) назначить для каталога монтирования пользователя-владельца и группу-владельца:

```
sudo chown -R <имя_пользователя>:<имя_группы> /run/<каталог_монтирования>
```

4) размонтировать устройство.

ВНИМАНИЕ! В случае если включен мандатный контроль целостности, то действия по подготовке раздела USB-накопителя должны осуществляться от имени администратора с высокой меткой целостности.

19.9. Контроль подключения устройств в домене FreeIPA

На компьютерах, входящих в домен FreeIPA, также можно ограничить доступ к устройству. Для этого следует создать назначающее правило в веб-интерфейсе контроллера домена.

Устройства идентифицируются на основе выражений сопоставления, которые применяются в правилах `udev`. В большинстве случаев достаточно использовать серийный номер (атрибут `ID_SERIAL`). Если использование серийного номера невозможно, необходимо указать один или несколько других атрибутов устройства (идентификатор модели, идентификатор производителя и т.п).

Для создания назначающего правила необходимо:

1) получить значение идентификационного параметра (атрибута), который используется в правилах `udev`. Для этого:

а) подключить устройство к компьютеру;

б) вывести перечень атрибутов подключенного устройства:

```
sudo udevadm info --query=property --name=/dev/<файл_устройства>
```

Пример

Атрибуты USB-накопителя:

```
DEVPATH=/devices/pci0000:00/0000:00:14.0/usb3/3-3/3-3:1.0/\
host0/target0:0:0/0:0:0:0/block/sda
DEVNAME=/dev/sda
DEVTYPE=disk
DISKSEQ=14
MAJOR=8
MINOR=0
SUBSYSTEM=block
USEC_INITIALIZED=33632934153
ID_BUS=usb
ID_MODEL=USB_DISK_2.0
ID_MODEL_ENC=USB\x20DISK\x202.0\x20\x20\x20\x20
ID_MODEL_ID=4100
ID_SERIAL=_USB_DISK_2.0_070A38235B908E23-0:0
ID_SERIAL_SHORT=070A38235B908E23
ID_VENDOR_ENC=\x20\x20\x20\x20\x20\x20\x20\x20
ID_VENDOR_ID=13fe
ID_REVISION=PMAP
ID_TYPE=disk
ID_INSTANCE=0:0
```

в) зафиксировать значение требуемого атрибута устройства (например, `ID_SERIAL` — серийный номер);

2) в веб-интерфейсе контроллера домена FreeIPA создать назначающее правило. Для этого:

а) открыть вкладку «Политика»;

б) из выпадающего списка «Политика PARSEC» выбрать «Учтенные устройства»;

в) на открывшейся странице «Учтенные устройства» нажать **[Добавить]**;

г) в открывшемся окне «Добавить» подготовить правило:

- задать условное наименование устройства;
- указать пользователя-владельца и группу-владельца.

ВНИМАНИЕ! В качестве группы-владельца не допускается указывать служебную доменную группу `ipausers`. Для использования в назначающих правилах рекомендуется создать отдельные доменные группы;

- в строке «Атрибуты устройства» нажать **[Добавить]** и в открывшемся поле ввода вставить выражение сопоставления устройства в формате правил `udev`.

Пример

Выражение сопоставления устройства по серийному номеру:

```
ENV{ID_SERIAL}=="_USB_DISK_2.0_070A38235B908E23-0:0"
```

- установить флаг «Правила учета включены»;
- нажать **[Добавить и изменить]**;

д) на открывшейся странице «Учтенное устройство: <наименование>» изменить (если необходимо) значения параметров доступа:

- во вкладке «Параметры» — набор прав доступа и уровень конфиденциальности;
- во вкладке «Категории конфиденциальности устройств» — набор категорий конфиденциальности;
- во вкладке «Маска аудита успеха» — флаги успешных событий;
- во вкладке «Маска аудита отказа» — флаги неуспешных событий.

По умолчанию установлены следующие значения параметров доступа:

- набор прав доступа: 640;
- флаги аудита: 0x0:0x0;
- метка безопасности: 0:0:0x0:0x0!;

е) на странице «Учтенное устройство: <наименование>» во вкладке «Параметры» нажать **[Сохранить]**.

На компьютерах, входящих в домен FreeIPA, генерация правил `udev` осуществляется службой `sssd` при входе в сессию пользователя домена.

Если к компьютеру были подключены какие-либо устройства, то для применения созданных или измененных правил доступа к устройствам требуется переподключить эти устройства или выполнить команду:

```
sudo udevadm trigger
```

Также правила будут применены после перезагрузки ОС.

После применения правил пользователь-владелец или пользователи из группы-владельца, указанные в правиле, смогут монтировать ФС дисковых разделов USB-накопителя.

Устройство, для которого создано назначающее правило, можно использовать в ненулевой сессии (на уровне конфиденциальности, отличном от 0). Для этого в веб-интерфейсе управления доменом FreeIPA необходимо назначить ему соответствующий уровень конфиденциальности:

1) открыть вкладку «Политика»;

2) из выпадающего списка «Политика PARSEC» выбрать «Учтенное устройства»;
3) на открывшейся странице «Учтенное устройства» выбрать устройство;
4) на открывшейся странице «Учтенное устройство: <наименование>»:
   а) во вкладке «Параметры» из выпадающего списка «Уровень конфиденциальности устройства» выбрать нужный уровень конфиденциальности;
   б) нажать **[Сохранить]**.

Порядок использования устройств в ненулевой сессии описан в 19.8.

19.10. Блокировка USB-устройств в режиме «Мобильный»

Блокировка USB-устройств в режиме «Мобильный» осуществляется с помощью утилиты USBGuard. Утилита позволяет управлять блокировкой подключаемых устройств, создавая правила.

Настройка работы USBGuard осуществляется в конфигурационном файле `/etc/usbguard/usbguard-daemon.conf`.

Для управления блокировкой USB-устройств в графическом интерфейсе реализован модуль KCM. Доступ к модулю ограничивается политикой Polkit.

Администратор при подключении USB-устройства настраивает доступ к нему, создавая правила. Если при включенной службе блокировки USB-устройств будет подключено USB-устройство, для которого отсутствует правило, то данное устройство будет заблокировано. Порядок использования модуля KCM для блокировки USB-устройств описан в электронной справке («Документация — Графический интерфейс — Режим «Мобильный»).

20. ПОДДЕРЖКА СРЕДСТВ ДВУХФАКТОРНОЙ АУТЕНТИФИКАЦИИ

Повышение надежности аутентификации возможно достичь путем использования многофакторной аутентификации, предполагающей применение нескольких типов аутентификационных факторов

К факторам, которые могут быть использованы, относятся:

- ввод пароля или PIN-кода;
- ввод одноразовых паролей (скрэтч-карты);
- предоставление физического устройства или носителя, содержащего аутентификационную информацию (смарт-карта, USB-токен и т. п.);
- предоставление биометрической информации (отпечатки пальцев, изображение сетчатки глаза и т. п.).

На практике в большинстве случаев используется двухфакторная аутентификация на основе ввода пароля с одновременным предоставлением пользователем физического устройства (носителя), содержащего дополнительную аутентификационную информацию. Дополнительной аутентификационной информацией в этом случае обычно является размещенный на устройстве сертификат пользователя.

Для обеспечения двухфакторной аутентификации с помощью внешнего носителя используются следующие средства и технологии:

- PKCS (Public Key Cryptography Standard) — группа стандартов защитного преобразования с открытым ключом, в частности, стандарты PKCS-11, PKCS-12, PKCS-15, относящиеся к работе с токенами;
- X.509 — стандарт, определяющий форматы данных и процедуры распределения открытых ключей с помощью сертификатов с цифровыми подписями, которые предоставляются центрами аутентификации;
- OpenSC — набор программных утилит и библиотек для работы с носителями аутентификационной информации пользователя (смарт-карты, USB-токены), содержащие функции аутентификации, преобразования и цифровой подписи. Поддерживает стандарты PKCS-11, PKCS-15;
- OpenCT — набор драйверов устройств для работы с носителями аутентификационной информации (устаревший);
- OpenSSL — программное средство для работы с протоколом SSL/TLS. Позволяет создавать ключи RSA, DH, DSA и сертификаты X.509, подписывать их, формировать файлы сертификатов CSR и CRT. Также имеется возможность тестирования SSL/TLS соединений. Поддерживает механизм динамически подключаемых библиотек алгоритмов защитного преобразования данных, т.е. механизм подключения внешних модулей, содержащих дополнительные алгоритмы. С использованием ука-

занного механизма обеспечивает работу с алгоритмами защитного преобразования данных в соответствии с требованиями ГОСТ (пакет библиотеки алгоритмов ГОСТ `libgost-astra`);

- PC/SC — набор спецификаций для доступа к смарт-картам;

- PKINIT (Public Key Cryptography for Initial Authentication in Kerberos) — стандарт использования защитного преобразования с открытым ключом в качестве фактора аутентификации в протоколе аутентификации Kerberos (см. 8.1.4).

Двухфакторная аутентификация может применяться как в случае использования локальной аутентификации, так и в случае использования ЕПП.

20.1. Аутентификация с открытым ключом (инфраструктура открытых ключей)

Аутентификация на основе ключей использует ключевую пару: один ключ «открытый» (публичный), который доступен каждому, и второй ключ «закрытый» (секретный), который доступен только владельцу. В процессе аутентификации используются алгоритмы с открытым ключом для проверки подлинности пользователя. При этом закрытый ключ находится непосредственно у пользователя, а открытый ключ по защищенным каналам связи передается в те системы, которые должны с его помощью проверять подлинность пользователя.

В качестве электронного представления ключей используются цифровые сертификаты. Сертификат является подтверждением принадлежности открытого ключа. Цифровой сертификат устанавливает и гарантирует соответствие между открытым ключом и его владельцем. Сертификаты выдаются специальными уполномоченными организациями — центрами аутентификации. Сертификаты могут быть использованы не только для аутентификации, но и для предоставления избирательных прав доступа, в том числе и права подписи других сертификатов.

В рамках изолированной информационной системы средством выработки и подписывания цифровых сертификатов могут быть использованы различные программные средства, например, `openssl`. В этом случае такое средство может выступать в роли локального центра аутентификации для создания ключевых пар и сертификатов клиентов и серверов системы.

При доступе к ресурсам информационных систем часто используются механизмы защитного преобразования, основанные на ассиметричных алгоритмах и сертификатах открытого ключа. Применение указанных механизмов в информационных системах обеспечивается инфраструкторой открытых ключей PKI, которая включает в себя набор аппаратных и программных средств, политик и процедур создания, управления, распространения, использования и отзыва цифровых сертификатов.

В основе PKI лежит использование защитного преобразования с открытым ключом и несколько основных принципов:

- закрытый ключ известен только его владельцу;
- центр аутентификации создает сертификат открытого ключа, таким образом подтверждая этот ключ;
- никто не доверяет друг другу, но все доверяют центру аутентификации;
- центр аутентификации подтверждает или опровергает принадлежность открытого ключа заданному лицу, которое владеет соответствующим закрытым ключом.

20.2. Средства поддержки двухфакторной аутентификации

20.2.1. Общие сведения

В ОС поддерживается механизм двухфакторной аутентификации пользователей с использованием токенов.

Для аутентификации пользователей используется модуль `pam-csp`, реализованный на основе стандартного PAM-модуля `libpam-csp`.

PAM-модуль `libpam-csp` обрабатывает два события:

- аутентификация пользователя;
- смена пароля пользователя.

Для доступа к токенам используется стандартная библиотека `opensc-pkcs11`, позволяющая модулю `libpam-csp` работать с любыми токенами различных производителей, поддерживающими эту библиотеку.

Контроль пользовательской сессии осуществляется с использованием службы `csp-monitor`. Для взаимодействия службы с токенами используется библиотека `opensc-pkcs11`.

Служба `csp-monitor` принимает от `pam_csp` по шине DBus сообщения о входе и выходе пользователя с использованием токена и поддерживает список текущих пользовательских сессий с информацией об использованных для входа токенах.

Служба `csp-monitor` осуществляет мониторинг подключений и отключений USB-устройств и если какой-либо токен из числа участвующих в аутентификации пользователя был извлечен, то блокирует все сессии данного пользователя. Для разблокировки сессии пользователь должен подключить токен и ввести PIN-код.

Служба `csp-monitor` управляется как юнит `systemd`. Для просмотра статуса службы выполнить команду:

```
systemctl status csp-monitor
```

ВНИМАНИЕ! При использовании решения `pam_csp` совместно с FreeIPA для параметра доменной политики паролей «минимальный срок действия пароля» должно быть задано значение 0.

20.2.2. Настройка клиентской машины

Для установки модуля `libpam-csp` выполнить установку соответствующего пакета от имени администратора командой:

```
apt install libpam-csp
```

Далее необходимо задать команду принудительной смены пароля. Для локальных пользователей на компьютере пользователя выполнить команду от имени администратора:

```
passwd --expire <имя_пользователя>
```

Для доменных пользователей необходимо использовать соответствующие инструменты администрирования домена.

При установке пакета `libpam-csp` автоматически будет установлен пакет для службы `csp-monitor`.

Во время установки пакета модуль `pam_csp` регистрируется первым в цепочках PAM-модулей в двух PAM-профилях:

```
/etc/pam.d/common-auth
/etc/pam.d/common-password
```

20.2.3. Инициализация токена

Процесс инициализации токена одинаков для локальных и доменных пользователей.

До передачи токена пользователю выполняется его подготовка на компьютере администратора, ответственного за подготовку.

Для выполнения подготовки токена на компьютере должны быть установлены пакеты:

- `opensc-pkcs11` версии не ниже 0.19.0-2;
- `ifd-rutokens` версии не ниже 1.0.4 (для Rutoken S и Rutoken ECP);
- пакеты других интерфейсных модулей, необходимые для используемой модели токена.

Для установки пакета `opensc-pkcs11` выполнить от имени администратора команду:

```
sudo apt install opensc-pkcs11
```

Установка интерфейсных модулей выполняется в соответствии с инструкциями производителей соответствующих токенов.

Процедура инициализации зависит от используемой модели токена.

Для инициализации токена Rutoken S выполнить последовательно следующие команды:

```
pkcs15-init --erase-card
pkcs15-init --create-pkcs15 --so-pin "87654321" --so-puk "" --pin "12345678"
pkcs15-init --store-pin --label "User PIN" --auth-id 02 --pin "12345678" \
     --puk ""
```

Для инициализации токена Rutoken ECP выполнить последовательно следующие команды:

```
pkcs15-init --erase-card -p rutoken_ecp
pkcs15-init --create-pkcs15 --so-pin "87654321" --so-puk ""
pkcs15-init --store-pin --label "User PIN" --auth-id 02 --pin "12345678" \
     --puk "" --so-pin "87654321" --finalize
```

Проверить, что токен успешно инициализирован, можно с помощью команды:

```
pkcs15-tool -D
```

20.2.4. Использование токена

При первичном использовании токена для входа в свою сессию пользователь должен подключить токен и в соответствующих полях ввести свои логин и пароль. При появлении окна с дополнительным приглашением:

```
Supply token PIN:
```

ввести PIN токена (текущий PIN токена пользователю сообщает администратор).

Далее пользователю будет предложено сменить PIN:

```
Supply new token PIN:
Retype new token PIN:
```

При этом можно указать новый PIN (рекомендуется), введя его два раза, или два раза нажать клавишу **<Enter>**, чтобы оставить текущий PIN (не рекомендуется).

После первичного ввода PIN произойдет генерация нового случайного пароля, его назначение учетной записи пользователя и будет выполнен вход в систему. В дальнейшем в токене будет храниться 16-символьный пароль, недоступный без знания PIN.

При последующих входах в систему пользователю нужно подключить токен и далее в соответствующих полях ввести логин и PIN токена.

Пример

Диалог при терминальном входе

```
login: user
Supply token PIN:
```

При необходимости сменить пароль пользователь должен подключить токен, войти в систему и затем:

1) при первичном входе — выполнить в командной строке команду `passwd`. При этом будут запрошены текущие пароль и PIN:

```
passwd
Введите ПИН-код :
Введите текущий пароль :
Введите новый ПИН-код :
Введите новый ПИН-код еще раз :
```

2) при последующих входах — выполнить в командной строке команду `passwd`. При этом будет запрошен текущий PIN:

```
passwd
Введите ПИН-код :
Введите новый ПИН-код :
Введите новый ПИН-код еще раз :
```

Для локального пользователя администратор может подготовить токен со сгенерированным паролем заранее. Для этого следует подключить токен и выполнить команду:

```
passwd <имя_пользователя>
Введите ПИН-код :
Введите новый ПИН-код :
Введите новый ПИН-код еще раз :
ПИН-код успешно изменен.
passwd: пароль успешно изменен
```

20.2.5. Разблокировка сессии с ненулевой меткой конфиденциальности с помощью PIN-кода

Токен возможно использовать для входа в сессию с ненулевым уровнем конфиденциальности. При этом для того чтобы функция разблокировки сессии по PIN-коду работала корректно, необходимо произвести следующие настройки:

1) присвоить сокету `/var/run/pcscd/pcscd.comm` привилегию `PARSEC_CAP_PRIV_SOCK`, добавив в раздел `[Socket]` файла `/lib/systemd/system/pcscd.socket` строку:

```
CapabilitiesParsec=PARSEC_CAP_PRIV_SOCK
```

2) перезапустить службу `pcscd`:

```
sudo systemctl daemon-reload
sudo systemctl stop pcscd.service
sudo systemctl stop pcscd.socket
sudo systemctl start pcscd.service
```

3) обеспечить корректную работу модуля `pam_p11`, входящего в состав `libpam-p11`. Для этого в каталоге `/home` каждого доступного пользователю уровня конфиденциальности должен находиться файл `.euid/authorized_certificates`. Данный файл можно после настройки модуля `pam_p11` скопировать из каталога `/home` пользователя нулевого уровня конфиденциальности в каталоги `/home` других уровней конфиденциальности.

20.3. Управление сертификатами

Для обеспечения аутентификации с открытым ключом в информационной системе необходимо иметь набор ключевых пар и сертификатов ресурсов сети (серверов или служб) и ее клиентов (пользователей). Формирование и подписывание сертификатов выполняет-

ся с помощью центра аутентификации информационной системы. Процедура получения необходимого набора сертификатов заключается в следующем:

1) формируются ключи и корневой сертификат центра аутентификации;
2) для каждого сервера или клиента генерируется ключевая пара;
3) на основе полученной ключевой пары формируется заявка (запрос) на сертификат;
4) с помощью центра аутентификации по заявке выписывается сертификат;
5) полученная ключевая пара и сертификат сохраняются в соответствующие места системы.

Генерация ключевых пар и работа с сертификатами осуществляется согласно инструкции производителя соответствующего токена.

20.4. Настройка доменного входа (ЕПП)

При использовании ЕПП для аутентификации пользователей применяется доверенная аутентификация Kerberos (см. 8.1.4). По умолчанию аутентификация производится по паролю пользователя. В то же время существует стандарт использования защитного преобразования с открытым ключом в качестве фактора аутентификации в протоколе аутентификации Kerberos PKINIT (Public Key Cryptography for Initial Authentication in Kerberos). Это позволяет применять сертификаты и, следовательно, устройства PKCS-11 для аутентификации по Kerberos.

Для используемого варианта Kerberos (MIT Kerberos V5) возможности PKINIT реализуются пакетом расширения `krb5-pkinit`. При этом для проведения аутентификации используется подгружаемый модуль аутентификации `libpam-krb5`.

ВНИМАНИЕ! Перед настройкой доменного входа с помощью сертификатов с устройств PKCS-11 должны быть выполнены следующие условия:

1) установлена и соответствующим образом настроена служба домена;
2) настроен домен ЕПП и созданы необходимые пользователи;
3) на компьютеры домена установлен пакет расширения `krb5-pkinit`;
4) получен или создан корневой сертификат CA.

21. СООБЩЕНИЯ АДМИНИСТРАТОРУ И ВЫЯВЛЕНИЕ ОШИБОК

21.1. Диагностические сообщения

При возникновении проблем в процессе функционирования ОС появляются диагностические сообщения трех типов: информационные, предупреждающие и сообщения об ошибках (примеры приведены в таблицах 65–67, соответственно). Администратор должен проанализировать диагностические сообщения и принять меры по устранению появившихся проблем.

Таблица 65 – Информационные сообщения

Сообщение ОС	Описание	Файл
`Setting hostname to <>`	Установка имени хоста <>	`hostname`
`Setting domainname to <>`	Установка имени домена <>	`hostname`
`Statistics dump initiated`	Вывод статистики запущен	`named`
`Query logging is now on`	Регистрация очередей включена	`named`
`Query logging is now off`	Регистрация очередей выключена	`named`
`Unknown host`	Неизвестный хост	`dnsquery`
`Non reloadable zone`	Неперезагружаемая зона	`named`
`Reconfig initiated`	Переконфигурирование запущено	`named`
`Zone not found`	Зона не найдена	`named`

Таблица 66 – Предупреждающие сообщения

Сообщение ОС	Описание	Действия по устранению проблемы	Файл
`<>: You can't change the DNS domain name with this command`	Неверное использование команды	Использовать соответствующую команду	`hostname`
`Could not find any active network interfaces`	Активные сетевые интерфейсы не найдены	Активировать сетевой интерфейс	`sendmail`
`You must be root to change the host name`	Недостаточно прав для изменения имени хоста	Обратиться к администратору	`dnsdomainname`

Таблица 67 – Сообщения об ошибках

Сообщение ОС	Описание	Действия по устранению проблемы	Файл
`Unknown server error`	Неизвестная ошибка сервера	Изменить права доступа	`dnsquery`
`Resolver internal error`	Внутренняя ошибка резольвера	Изменить права доступа	`dnsquery`

Окончание таблицы 67

Сообщение ОС	Описание	Действия по устранению проблемы	Файл
`Superblock last mount time (значение времени) is in the future`	Неверная установка времени	См. 21.3	См. 21.3

21.2. Выявление ошибок

В состав ОС входит инструмент `sosreport`, предназначенный для сбора информации о конфигурации системы и диагностических данных о работе ОС и ее компонентов. Инструмент включает модули для сбора информации о работе отдельных подсистем и программ из состава ОС.

На основе собранных данных создается диагностический архив с отчетом, который может храниться локально, централизованно или отправляться техническим специалистам. Дополнительно возможно создавать XML/HTML-отчеты.

Перечень основных параметров, используемых с инструментом `sosreport`, приведен в таблице 68.

Таблица 68

Параметр	Описание
`-l`	Вывести список доступных модулей и их параметры. Модули, которые не могут использоваться с текущей конфигурацией, выводятся отдельно
`-n <имя_модуля>`	Отключить указанный модуль. Отключение нескольких модулей выполняется повторением параметра или заданием списка модулей через запятую
`-e <имя_модуля>`	Включить указанный модуль. Включение нескольких модулей выполняется повторением параметра или заданием списка модулей через запятую
`-o <имя_модуля>`	Включить только указанный модуль (неуказанные модули будут автоматически отключены). Включение нескольких модулей выполняется повторением параметра или заданием списка модулей через запятую
`-k <имя_модуля>.<параметр_модуля> [=<значение>]`	Задать параметры модуля. Включает указанный параметр модуля, может также задавать значение параметра модуля
`-a`	Установить для всех логических параметров всех включенных модулей значение `True`
`-v`	Увеличить детализацию протоколирования. Может выполняться несколько раз для добавления дополнительных сообщений

Продолжение таблицы 68

Параметр	Описание
`--no-postproc`	Отключить постобработку собранных данных для всех модулей. В архиве с собранными данными не будет замаскирована/очищена конфиденциальная информация. Такие данные, как пароли, SSH-ключи, сертификаты будут сохранены в виде простого текста. Чтобы отключить постобработку для определенного модуля, использовать с параметром `-k` параметр `postproc` модуля, например `-k logs.postproc=off`
`-s <корневая_файловая_система>`	Указать другую корневую файловую систему. Возможно использовать для создания отчета работы контейнера или образа
`-c {auto/always/never}`	Установить режим использования `chroot`. Когда используется `-s`, команды по умолчанию выполняются с заданной файловой системой (если только они не отключены определенным модулем). Параметр `-c` переопределяет использование заданной корневой файловой системы: - значение `always` — всегда использовать корневую файловую систему, заданную параметром `-s`; - `never` — никогда не использовать корневую файловую систему, заданную параметром `-s` (команды всегда будут выполняться в пространстве хоста)
`--tmp-dir <путь>`	Задать временный каталог для копирования данных и архива отчета
`--list-profiles`	Вывести список доступных профилей и включенных в них модулей
`-p <имя_профиля>`	Выполнить модули, включенные в указанный профиль. Несколько профилей могут быть заданы через запятую, при этом будут выполнены модули всех указанных профилей
`--log-size`	Установить ограничение на размер (в МиБ) набора журналов. Ограничение применяется отдельно для каждого набора журналов, собранных любым модулем
`--all-logs`	Собирать данные всех возможных журналов регистрации событий, включая из незаданных областей и игнорируя ограничения по размеру. В данном случае может быть значительно увеличен размер отчетов
`-z <метод_сжатия>`	Задать метод сжатия отчета
`--encrypt-pass <пароль>`	Аналогично `--encrypt-key`, но защита архива выполняется установкой пароля
`--batch`	Создать архив отчета без интерактивных запросов пользователю

Окончание таблицы 68

Параметр	Описание
`--case-id <идентификатор_архива>`	Задать идентификатор архива. Может содержать цифры, латинские буквы, запятые и точки

Более подробное описание инструмента доступно в `man sosreport`.

Для использования инструмента `sosreport` в графическом режиме доступна утилита `fly-sosreport`. Описание утилиты приведено в электронной справке.

ВНИМАНИЕ! В настоящее время инструмент `sosreport` отмечен как устаревший и в будущем будет исключен из состава. Вместо него следует использовать новый инструмент, вызываемый командой `sos report`. Новый инструмент работает идентично старому и использует те же параметры.

21.3. Циклическая перезагрузка компьютера по причине неверной установки времени

При возникновении сбоя, связанного с циклической перезагрузкой компьютера, необходимо во время загрузки ОС при появлении на экране заставки с мерцающей надписью «Astra Linux Special Edition» нажать клавишу **<Esc>**. Если среди отобразившихся сообщений есть сообщение вида:

```
/dev/sda1: Superblock last mount time (Wed Feb 15 12:41:05 2017,
            now = Mon Feb 15 12:45:37 2016) is in the future.
```

то сбой связан с неверной установкой времени.

Для устранения сбоя необходимо войти в меню настройки BIOS (UEFI) и проверить выставленное системное время. Если системное время отстает от реального, то, возможно, это связано с отказом элемента питания системной платы. В этом случае необходимо заменить элемент питания на системной плате в соответствии с указаниями инструкции к техническому средству и установить корректное системное время.

Если системное время в меню настроек BIOS (UEFI) установлено верно, но циклическая перезагрузка продолжается, то сбой может быть связан с неверным переводом времени на будущую дату и обратно. Данный сбой происходит если установить системное время на будущую дату, затем загрузить ОС и установить верное текущее время или сразу установить системное время на прошедшую дату. Для устранения данного сбоя необходимо:

1) в меню настроек BIOS (UEFI) установить системное время на будущую дату, при этом дата должна быть позже даты, указанной в сообщении об ошибке при загрузке;

2) загрузить ОС;

3) создать файл `/etc/ef2fsck.conf` с содержимым:

```
[options]
broken_system_clock = true
```

4) создать файл `/etc/initramfs-tools/hooks/e2fsck-conf.sh` с содержимым:

```
#!/bin/sh

PREREQ=""
prereqs()
{
   echo "$PREREQ"
}

case $1 in
prereqs)
   prereqs
   exit 0
   ;;
esac

. /usr/share/initramfs-tools/hook-functions
CONFFILE=/etc/e2fsck.conf
CONFDIR=`dirname "$CONFFILE"`
if [ -f "$CONFFILE" ]
then
   mkdir -p ${DESTDIR}${CONFDIR}
   cp $CONFFILE ${DESTDIR}${CONFDIR}
fi
```

5) в терминале выполнить команду:

```
sudo update-initramfs -u
```

6) перезагрузить ОС и установить текущее время в качестве системного.

ПЕРЕЧЕНЬ ТЕРМИНОВ

Закрытый ключ — сохраняемый в тайне ключ из ключевой пары, принадлежащий владельцу и не подлежащий распространению.

Ключ — параметр в виде последовательности псевдослучайных чисел (не предназначен для защиты информации в контексте использования для целей, установленных в документации изделия; к ключам не предъявляются требования по источнику псевдослучайных чисел, криптографической стойкости, времени действия и т. п.).

Ключевая пара — упорядоченная пара математически однозначно связанных ключей, определяющих взаимосвязанные защитные преобразования.

Открытый ключ — ключ из ключевой пары, который может быть сделан общедоступным.

Сертификат открытого ключа — артефакт, содержащий открытый ключ, информацию о владельце ключа и подтверждающий принадлежность открытого ключа владельцу, защищенный с применением закрытого ключа.

Хеш — строка бит, являющаяся выходным результатом функции хеширования.

Центр аутентификации — программный компонент, реализующий возможность подтверждения подлинности ключей с помощью сертификатов.

Цифровая подпись — результат преобразования хеша для его защиты от несанкционированного доступа с использованием закрытого ключа (не предназначена для криптографической защиты информации).

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

БД — база данных
ВМ — виртуальная машина
ЕПП — единое пространство пользователей
КСЗ — комплекс средств защиты
ЛВС — локальная вычислительная сеть
МКЦ — мандатный контроль целостности
НСД — несанкционированный доступ
ОС — операционная система специального назначения «Astra Linux Special Edition»
ПО — программное обеспечение
СЗИ — средства защиты информации
СЗФС — сетевая защищенная файловая система
СУБД — система управления базами данных
ФС — файловая система
ЦА — центр аутентификации

AD — Active Directory (служба каталогов)
ACL — Access Control List (список контроля доступа)
API — Application Programming Interface (программный интерфейс приложения)
ARP — Address Resolution Protocol (протокол разрешения адресов)
BIOS — Basic Input-Output system (базовая система ввода-вывода)
BIND — Berkeley Internet Name Domain (пакет программного обеспечения для поддержки DNS, разработанный в Калифорнийском университете, г. Беркли)
BOOTP — Bootstrap Protocol (простой протокол динамической конфигурации хоста)
BSD — Berkeley Software Distribution (программное изделие Калифорнийского университета)
CA — Certification Authority (центр аутентификации)
CephFS — Ceph File System (файловая система Ceph)
CIFS — Common Internet File System (общий протокол доступа к файлам Интернет)
DC — Domain Controller (контроллер домена)
DDNS — Dynamic Domain Name System (динамическая система доменных имен)
DHCP — Dynamic Host Configuration Protocol (протокол динамической конфигурации хоста)
DIB — Directory Information Base (информационная база каталога)
DIT — Directory Information Tree (информационное дерево каталога)
DN — Distinguished Name (уникальное имя)
DNS — Domain Name System (система доменных имен)
FTP — File Transfer Protocol (протокол передачи файлов)
FQDN — Fully Qualified Domain Name (полностью определенное имя домена)
GID — Group Identifier (идентификатор группы)
HTTP — HyperText Transfer Protocol (протокол передачи гипертекста)
IDE — Integrated Drive Electronics (встроенный интерфейс накопителей)

IMAP — Internet Message Access Protocol (протокол доступа к сообщениям в сети Интернет)

IP — Internet Protocol (межсетевой протокол)

IPA — Identity, Policy, and Audit (система по управлению идентификацией пользователей, задания политик доступа и аудита для сетей на базе Linux и Unix)

IPC — InterProcess Communication (межпроцессное взаимодействие)

KDC — Key Distribution Center (центр распределения ключей)

KRA — Key Recovery Authority (служба восстановления ключей)

KVM — Kernel-based Virtual Machine (программное решение, обеспечивающее виртуализацию в среде Linux на платформе, которая поддерживает аппаратную виртуализацию на базе Intel VT (Virtualization Technology) либо AMD SVM (Secure Virtual Machine))

LDAP — Lightweight Directory Access Protocol (легковесный протокол доступа к службам каталогов)

LPR — Line Printer Remote (удаленный линейный принтер)

LVM — Logical Volume Manager (менеджер логических томов)

MAC — Mandatory Access Control (мандатное управление доступом)

MDA — Mail Delivery Agent (агент доставки электронной почты)

MDS — Metadata Server (сервер метаданных)

MIT — Massachusetts Institute of Technology (Массачусетский Технологический Институт)

MON — Monitor (монитор)

MTA — Mail Transfer Agent (агент пересылки сообщений)

MTU — Maximum Transfer Unit (максимальная единица передачи)

MUA — Mail User Agent (клиент электронной почты)

NAT — Network Address Translation (преобразование сетевых адресов)

NFS — Network File System (сетевая файловая система)

NIS — Network Information Service (сетевая информационная служба)

NSS — Name Service Switch (диспетчер службы имен)

NTP — Network Time Protocol (протокол сетевого времени)

OCI — Open Container Initiative (проект, который разрабатывает открытые стандарты для сред контейнеризации)

OSD — Object Storage Device (устройство хранения объектов)

PAM — Pluggable Authentication Modules (подключаемые модули аутентификации)

PID — Process Identifier (идентификатор процесса)

PKI — Public Key Infrastructure (инфраструктура открытых ключей)

PTP — Precision Time Protocol (протокол точного времени)

POP3 — Post Office Protocol Version 3 (почтовый протокол, версия 3)

QEMU — Quick Emulator (средства эмуляции аппаратного обеспечения)

RADOS — Reliable Autonomic Distributed Object Store (безотказное автономное распределенное хранилище объектов)

RBD — RADOS block device (блочное устройство)

RFC — Request For Comments (общее название технических стандартов сети Интернет)

RPC — Remote Procedure Call (удаленный вызов процедур)
RTS — Real Time Clock (время, установленное в аппаратных часах компьютера)
SASL — Simple Authentication and Security Layer (простая аутентификация и слой безопасности)
SATA — Serial ATA (последовательный интерфейс обмена данными с накопителями информации, является развитием интерфейса IDE)
SCSI — Small Computer System Interface (системный интерфейс малых компьютеров)
SMB — Server Message Block (блок сообщений сервера)
SPICE — Simple Protocol for Independent Computing Environments (простой протокол для независимой вычислительной среды)
SQL — Structured Query Language (язык структурированных запросов)
SSH — Secure Shell Protocol (протокол защищенной передачи информации)
SSL — Secure Sockets Layer (протокол защищенных сокетов)
SSSD — System Security Services Daemon (системная служба, управляющая доступом к удаленным каталогам и механизмам аутентификации)
TCP — Transmission Control Protocol (протокол управления передачей данных)
TSIG — Transaction Signature (метод аутентификации для защиты запросов и ответов)
TLS — Transport Layer Security (протокол защиты транспортного уровня)
TTL — Time To Live (время жизни IP-пакета)
UDP — User Datagram Protocol (протокол пользовательских дейтаграмм)
UEFI — Unified Extensible Firmware Interface (унифицированный расширяемый микропрограммный интерфейс)
UID — User Identifier (идентификатор пользователя)
URI — Uniform Resource Identifier (унифицированный идентификатор ресурса)
UTC — Universal Time Coordinated (универсальное скоординированное время)
UUID — Universally Unique IDentifier (всемирно уникальный идентификатор)
VFS — Virtual File System (виртуальная файловая система)
VIP — Virtual IP-adress (виртуальный IP-адрес)
VNC — Virtual Network Computing (система удаленного доступа к рабочему столу компьютера)
VPN — Virtual Private Network (виртуальная частная сеть)
VRRP — Virtual Redundancy Routing Protocol (сетевой протокол виртуального резервирования маршрутизаторов, предназначенный для увеличения доступности)
XCA — X window system Certification Authority (графический инструмент создания и управления центром аутентификации)

Лист регистрации изменений									
Изм.	Номера листов (страниц)				Всего листов (страниц) в документе	Номер документа	Входящий номер сопроводительного документа и дата	Подпись	Дата
	измененных	замененных	новых	аннулированных					