Quick Start Guide

Краткое руководство по пилотированию Secret Disk для Linux

Архитектура Secret Disk для Linux

Корпоративная версия Secret Disk для Linux состоит из трех компонентов:

- **Менеджмент-сервер** – сервер, осуществляющий управление зарегистрированными на нем Агентами рабочей станции;
- **Консоль управления** – предоставляет собой графический интерфейс для выполнения административных задач на Менеджмент сервере;
- **Агент рабочей станции** – компонент, непосредственно запускаемый на рабочей станции пользователя и оснащенный механизмами защиты данных.

Технические характеристики

Объект защиты:

- Системный раздел с разметкой GPT или LVM
- Файл-контейнер, монтируемый как виртуальный диск

Поддерживаемые криптографические алгоритмы:

- ГОСТ 34.12-2018, ГОСТ 34.13-2018 (шифрование данных)
- ГОСТ 34.10-2018, ГОСТ 34.11-2018 (аутентификация и проверка целостности)
- ГОСТ Р 34.12-2018 (шифрование системного раздела)

Размер защищаемых ресурсов:

- Виртуальный диск объемом от 100 МБ до 1 ТБ
- Системный раздел от 1 ГБ

Тип аутентификации:

- Двухфакторная аутентификация по ключевому контейнеру пользователя (ККП)
- Двухфакторная аутентификация по usb-токену (совместно с SecurLogon)

Quick Start Guide

Краткое руководство по пилотированию Secret Disk для Linux

1. Подготовка к установке Secret Disk для Linux

Выполнение требований по развертыванию

Для корректного функционирования Агента рабочей станции на виртуальном стенде необходимо соблюдать следующие требования к разметке дискового пространства на АРМ пользователя:

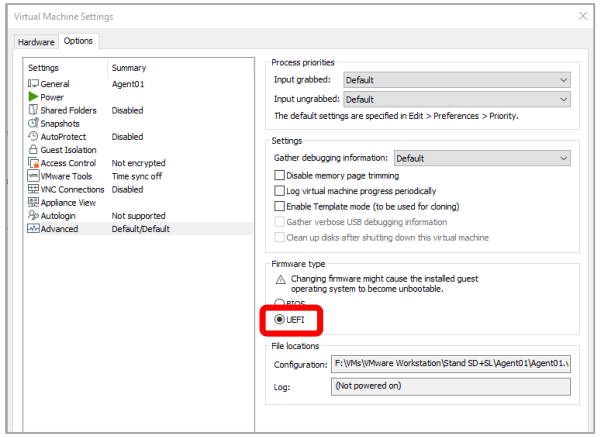
- Выбрать при установке загрузчик EFI
- При установке ОС создать выделенный раздел с точкой монтирования /boot
- Не использовать файловые системы или сторонние продукты, реализующие функции шифрования

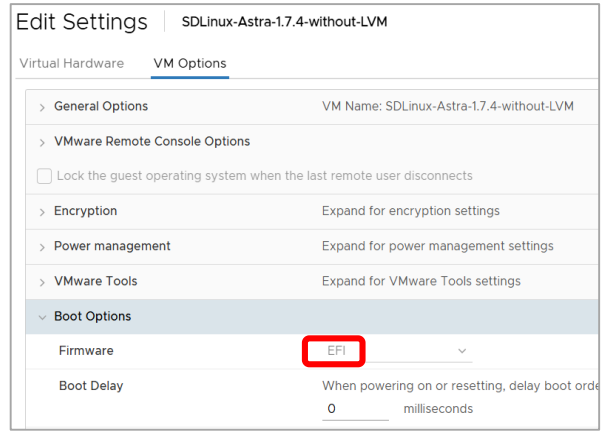
В выделенном разделе «/boot» диска размещается загрузчик Secret Disk. Этот раздел не подлежит шифрованию, потому что компоненты размещенные в этом разделе используются для загрузки операционной системы и должны быть доступны после включения питания компьютера.

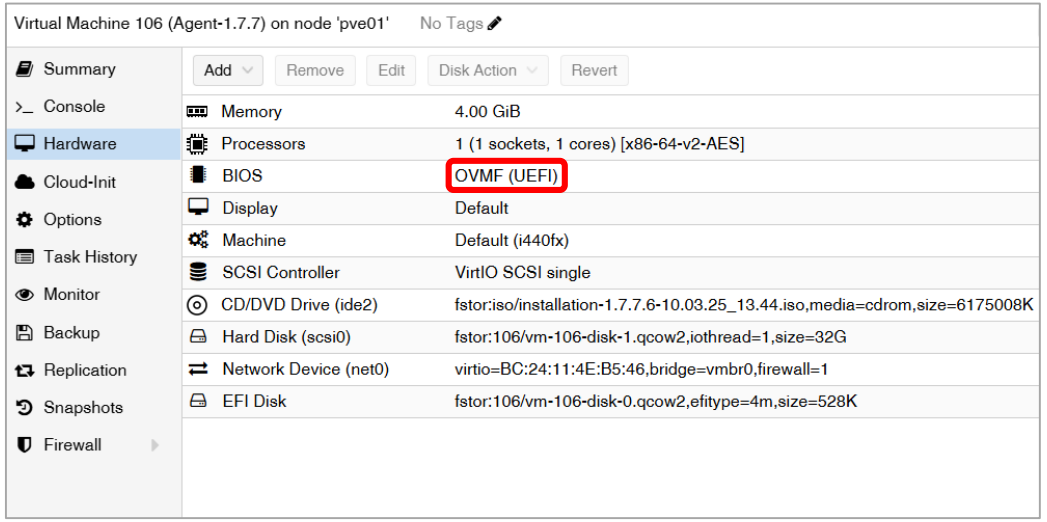
Как выбрать тип загрузчика EFI

Обязательным требованием, при развертывании Агента рабочей станции, является использование именно режима EFI/UEFI. Этот режим по умолчанию применяется в современных аппаратных платформах.

Виртуальные среды напротив, в качестве загрузчика для развертывания виртуальной машины (далее ВМ) по умолчанию используют BIOS. Настройка режима загрузки осуществляется в дополнительных свойствах ВМ, и выполняется для каждой ВМ в отдельности.







Quick Start Guide

Краткое руководство по пилотированию Secret Disk для Linux

1. Подготовка к установке Secret Disk для Linux

Как правильно организовать разметку дискового пространства

В отечественных ОС применяется 4 варианта разметки.

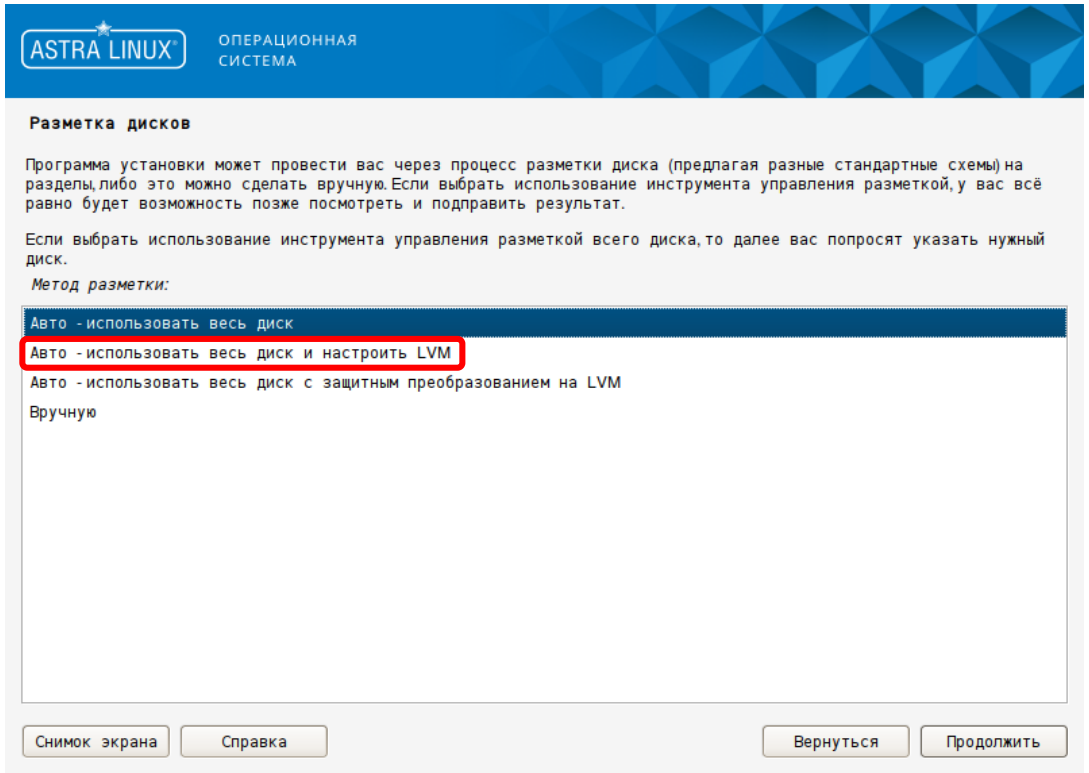
Для Secret Disk нужно выбрать **Авторазметку с использованием всего диска и настройкой LVM** или настроить разметку вручную (в зависимости от вашего опыта).

Авторазметка – использовать весь диск и настроить LVM
Необходимые разделы формируются правильно.
Режим рекомендован к выбору.

Авторазметка – использовать весь диск
В данном режиме не создаётся раздел /boot

Авторазметка – использовать весь диск с защитным преобразованием на LVM
Разделы формируются правильно, но на весь диск устанавливается защитное преобразование (шифрование).
В случае выбора этой разметки Агент рабочей станции не сможет применить защиту системного раздела.

Вручную
В данном режиме пользователь сам определяет конфигурацию разделов ОС.
Рекомендовано к выбору.
Но требуется с вниманием отнестись к рекомендациям данным выше.



Краткое руководство по пилотированию Secret Disk для Linux

2. Установка Менеджмент-сервера

Установка пакетов

Для установки Менеджмент-сервера требуются следующие пакеты:

Название	Описание
sdlinux-crypto	Общий пакет для всех компонентов продукта - криптобиблиотеки и криптоплагин
sdlinux-ms	Менеджмент-сервер
sdlinux-mc	sdproxy и Консоль управления

Варианты установки:

- **Совместно с Менеджмент-сервером**

набор пакетов указан в перечне выше

- **Установка Консоли управления на выделенный АРМ**

на АРМ с Менеджмент-сервером устанавливаются только sdlinux-crypto и sdlinux-ms, на АРМ с Консолью управления - sdlinux-crypto и sdlinux-mc

Установка компонентов сервера выполняется с правами суперпользователя командами apt или dpkg

Синтаксис для команды apt:

```
sudo apt install -y /«destination path»/sdlinux-crypto.x.x.x.xxx.amd64.deb
sudo apt install -y /«destination path»/sdlinux-ms.x.x.x.xxx.amd64.deb
sudo apt install -y /«destination path»/sdlinux-mc.x.x.x.xxx.amd64.deb
```

Синтаксис для команды dpkg:

```
sudo dpkg -i /«destination path»/sdlinux-crypto.x.x.x.xxx.amd64.deb
sudo dpkg -i /«destination path»/sdlinux-ms.x.x.x.xxx.amd64.deb
sudo dpkg -i /«destination path»/sdlinux-mc.x.x.x.xxx.amd64.deb
```

По завершении установки будет запущена служба sdlsd.service, которая и является основной службой Менеджмент-сервера. Для проверки ее состояния используется команда:

```
systemctl status sdlsd
```

```
sdadmin@server:~$ systemctl status sdlsd
● sdlsd.service - SDLinuxServer daemon
     Loaded: loaded (/lib/systemd/system/sdlsd.service; enabled; vendor preset: enabled)
     Active: active (running) since Wed 2025-04-02 15:45:22 MSK; 19h ago
   Main PID: 1552 (sdlsd)
      Tasks: 14 (limit: 2217)
     Memory: 9.1M
        CPU: 2.153s
     CGroup: /system.slice/sdlsd.service
             └─1552 /usr/sbin/sdlsd
```

Quick Start Guide

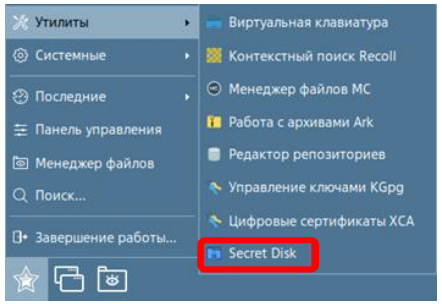
Краткое руководство по пилотированию Secret Disk для Linux

2. Установка Менеджмент-сервера

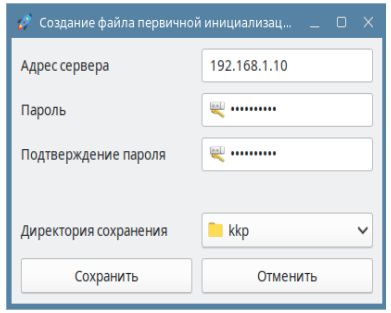
Настройка

На Менеджмент-сервере (при установке на выделенный АРМ - на АРМе, где развернута Консоль управления) запускаем Secret Disk:

Пуск -> Утилиты -> Secret Disk



В открывшемся окне заполняем все поля, вводя данные необходимые для формирования ключевого контейнера пользователя (ККП) Администратора.



- **Адрес сервера** - должен соответствовать реальному адресу Менеджмент-сервера, должен быть назначен статически. После добавления на Менеджмент-сервер ККП Администратора IP-адрес сервера нельзя изменить
- **Пароль/подтверждение пароля** – пароль для ККП
- **Директория сохранения** – место размещения сгенерированного ККП. После генерации ККП может свободно быть перемещен в другое место. Главное – доступность ККП для sdproxy.

ВАЖНО!
Изменение IP-адреса Менеджмент-сервера после добавления ККП Администратора гарантировано приведет продукт в нерабочее состояние

ККП Администратора добавляем на Менеджмент-сервер командой:
`sudo sdlsd -a -k /«destination path»/admin.kkp`
Команда добавляет admin.kkp в базу данных сервера, используя параметры:

- «-a» - добавление admin.kkp в базу данных сервера
- «-k» - указание на место размещения admin.kkp

Вводим пароль, от ККП. В выводе должен отобразиться статус Success, подтверждающий успешную регистрацию Агента на сервере:

```
sdadmin@server:~$ sudo sdlsd -a -k /home/sdadmin/admin.kkp
Password:
Success
```

Далее генерируем ККП для подключения Агента рабочей станции к Менеджмент-серверу. Имя файла выбираем произвольно (в качестве примера файл agent.kkp):

`sudo sdlsd -w -k /«destination path»/agent.kkp -h IP-адрес Менеджмент-сервера`

Командой sdlsd создаем контейнер с ключом для регистрации Агента рабочей станции на Менеджмент-сервере. При этом используем следующие параметры:

- «-w» - создание agent.kkp для аутентификации Агента на сервере
- «-k» - указание на место размещения agent.kkp
- «-h» - указание IP-адреса сервера (при использовании DNS-имени сервера возможно его добавление в данный параметр)

Далее необходимо распространить agent.kkp на все защищаемые АРМ

3. Установка Агента рабочей станции

Установка пакетов

Для установки Агента рабочей станции требуются следующие пакеты:

Название	Описание
sdlinux-crypto	Общий пакет для всех компонентов продукта - криптобиблиотеки и криптоплагин
sdlinux	Агент рабочей станции
sdlinux-agent	Компоненты для сетевого взаимодействия Агента рабочей станции с Менеджмент-сервером
sdlinux-modules	Драйверы шифрования и модули для их работы на различных версиях ядер ОС (kernel)
sdlinux-sdsetup	Компоненты диагностики состава АРМ и дисковой подсистемы, компоненты для предварительной подготовки АРМ к включению защиты системного раздела

Установка компонентов Агента рабочей станции выполняется с правами суперпользователя командами apt или dpkg

Синтаксис для команды apt:

```
sudo apt install -y /«destination path»/sdlinux-crypto.x.x.x.xxx.amd64.deb
sudo apt install -y /«destination path»/sdlinux_x.x.x.xxx.amd64.deb
sudo apt install -y /«destination path»/sdlinux-agent.x.x.x.xxx.amd64.deb
sudo apt install -y /«destination path»/sdlinux-modules.x.x.x.xxx.amd64.deb
sudo apt install -y /«destination path»/sdlinux-sdsetup.x.x.x.xxx.amd64.deb
```

Синтаксис для команды dpkg:

```
sudo dpkg -i /«destination path»/sdlinux-crypto.x.x.x.xxx.amd64.deb
sudo dpkg -i /«destination path»/sdlinux-modules.x.x.x.xxx.amd64.deb
sudo dpkg -i /«destination path»/sdlinux_x.x.x.xxx.amd64.deb
sudo dpkg -i /«destination path»/sdlinux-agent.x.x.x.xxx.amd64.deb
sudo dpkg -i /«destination path»/sdlinux-sdsetup.x.x.x.xxx.amd64.deb
```

Перед началом развертывания компонентов Агента рабочей станции необходимо убедиться, что конфигурация АРМ соответствует требованиям, указанным в начале документа:

- Тип загрузчика обязательно должен быть EFI/UEFI
- Разметка дискового пространства должна иметь отдельный раздел /boot, этот раздел должен быть размещен на диске выделенно, а не папкой в корневом разделе «/»

Краткое руководство по пилотированию Secret Disk для Linux

3. Установка Агента рабочей станции

Настройка

Инициализируем Агента, выполнив команду с правами суперпользователя:
`sudo sdinit -i`

- «-i» указывает на процесс инициализации Агента рабочей станции. При вводе команды допустимо использование и дополнительных флагов.
- «-r» - выбор Датчика случайных чисел (варианты: 0 – биологический, 1- системный),
- «-f» - принудительная переинициализация Агента.

В процессе инициализации система запросит имя учетной записи (далее УЗ) Администратора Secret Disk и пароль для генерации ККП администратора.
Для УЗ Администратора можно использовать любую УЗ, зарегистрированную на АРМ и имеющую профиль пользователя. Этот пользователь не сможет зарегистрироваться на сервере и получить защищенные ресурсы.
После успешного выполнения инициализации проверяем статус службы sdctld.service с помощью команды:
`systemctl status sdctld.service`
Убедитесь, что состояние службы отображается как на рисунке:

```
sdadmin@agent-efi:~$ systemctl status sdctld.service
● sdctld.service - SDCTL daemon
     Loaded: loaded (/lib/systemd/system/sdctld.service; enabled; vendor preset: enabled)
     Active: active (running) since Thu 2025-04-03 16:22:40 MSK; 2min 39s ago
   Main PID: 633 (sdctld)
      Tasks: 3 (limit: 2216)
     Memory: 13.8M
        CPU: 1.592s
     CGroup: /system.slice/sdctld.service
             └─633 /usr/sbin/sdctld
```

Переходите к регистрации Агента на Менеджмент-сервере.
Для этого используйте ранее переданный на АРМ файл ККП рабочей станции.
Регистрация Агента выполняется следующей командой:
`sudo sdagent activate -f /«destination path»/agent.kkp`

После получения сообщения АРМ необходимо перезагрузить. В процессе перезагрузки будет собрана диагностическая информация об АРМ и направлена на сервер для учета в БД.
С этого момента управление созданием и установкой защиты ресурсов на АРМ будет осуществляться средствами Менеджмент-сервера с использованием Консоли управления.

4. Настройка консоли управления

Консоль управления функционирует в web-браузере и не требует отдельных настроек и подготовки.
Консоль запускается автоматически при старте Secret Disk

Краткое руководство по пилотированию Secret Disk для Linux

5. Защита системного раздела

Диагностика параметров АРМ

Проведение диагностики и проверка соответствия АРМ пользователя требованиям для установки защиты системного раздела производятся автоматически, после установки соответствующих программных пакетов.

Для определения готовности АРМ к установке защиты системного раздела необходимо перейти в Параметры рабочей станции. Область «ДИАГНОСТИКА СИСТЕМЫ» отображает первичную диагностическую информацию.

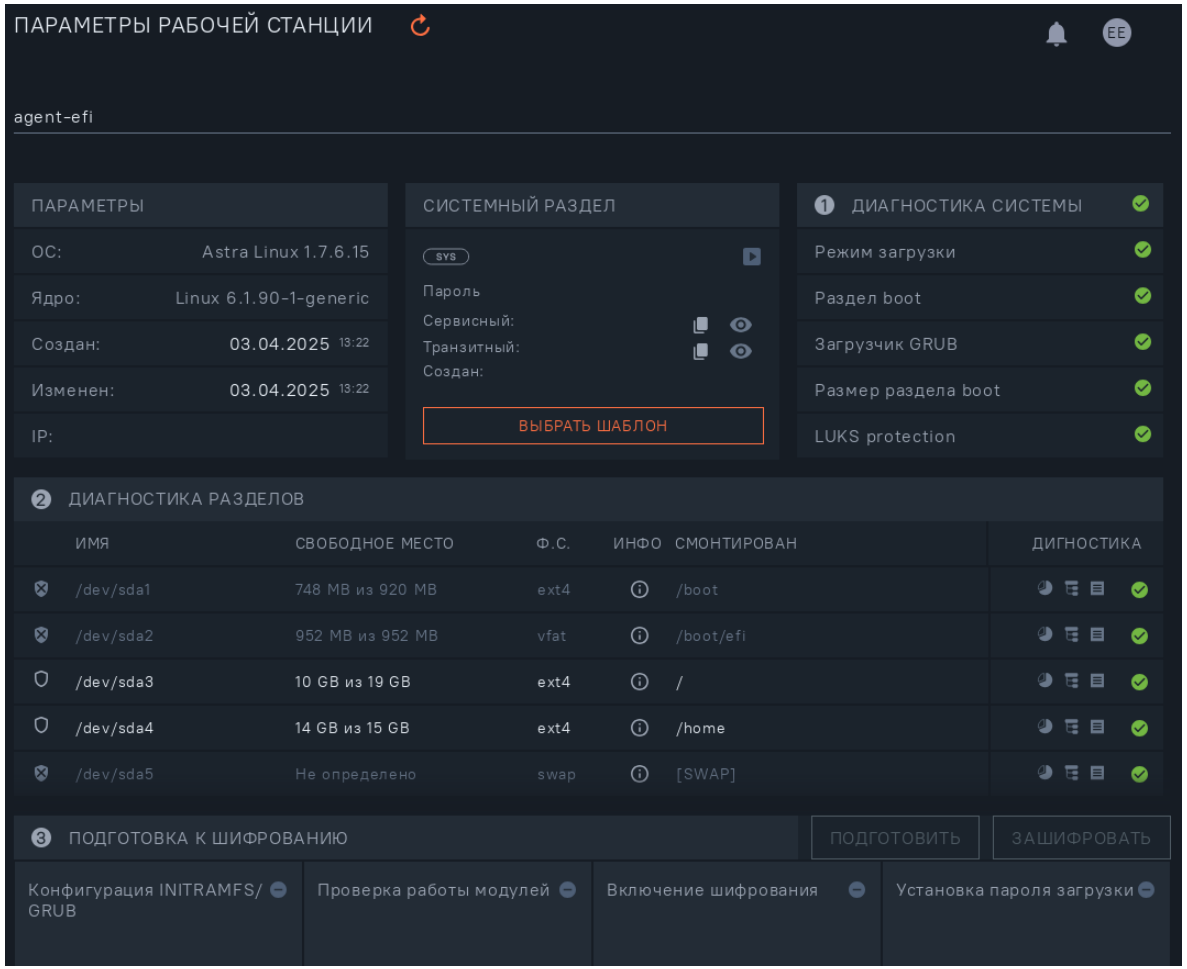
Виды проверок диагностики:

- **Режим загрузки** – в обязательном порядке должен быть выбран EFI/UEFI
- **Раздел boot** – должен быть представлен на диске выделенным разделом
- **Загрузчик GRUB** – в редких случаях применяется загрузчик отличный от GRUB
- **Размер раздела boot** – размер раздела должен быть не меньше 500 МБ.
- **LUKS protection** – диск не должен быть предварительно зашифрован.

Для успешной настройки критически важен положительный результат всех проверок, который отмечается соответствующей пиктограммой ✅

Диагностика разделов диска

Окно «ДИАГНОСТИКА РАЗДЕЛОВ» отображает информацию об имеющихся на АРМ разделах, их размер, тип файловой системы, точка монтирования, системное имя. Часть разделов не может быть зашифрована, и отмечается серым цветом. Для разделов, к которым может применяться шифрование доступен выбор, который осуществляется путем изменения параметра «sdprotect» в значения «allowed» или «not allowed», в файле /var/sercretdisk/sdprarts.json



Краткое руководство по пилотированию Secret Disk для Linux

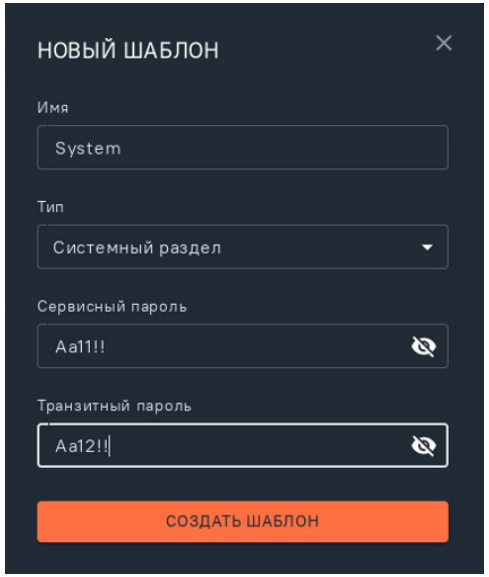
5. Защита системного раздела

Настройка защиты

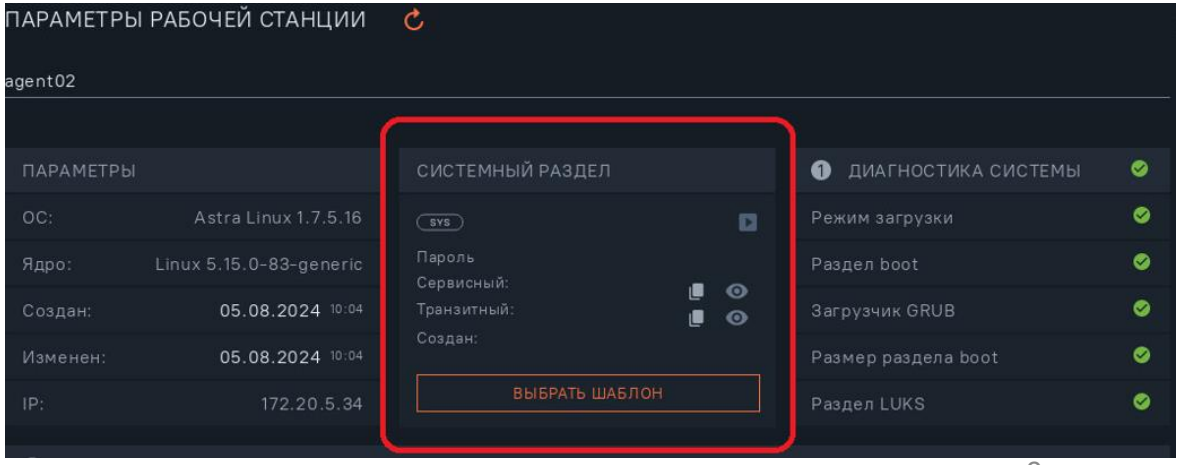
Для запуска установки защиты системного раздела необходимо создать шаблон «Системный раздел». В шаблоне указывается «Имя», «Сервисный пароль» и «Транзитный пароль». «Сервисный пароль» является временным средством аутентификации, применяется в процессе настройки АРМ администратором, включая применение защиты системного раздела.

«Транзитный пароль» применяется при передаче подготовленного и защищенного АРМ пользователю. Пользователь создает собственный пароль загрузки, после чего оба временных пароля (ККП) удаляются из хранилища.

После создания шаблона применяем его в свойствах рабочей станции. Для этого необходимо нажать кнопку «Выбрать шаблон », выбрать нужный, применить его нажатием на кнопку «Добавить ресурс». После чего наименование кнопки «Выбрать шаблон» изменится на имя выбранного шаблона



Шаблоны конфигурации представляют собой простое и удобное средство установки политики шифрования, как для одного АРМ, так и для многих рабочих стаций, в процессе масштабирования системы.
Администратор ИБ подготавливает, заранее один или несколько Шаблонов конфигураций, с различными параметрами и далее добавляет шаблон одному или нескольким АРМ.



Краткое руководство по пилотированию Secret Disk для Linux

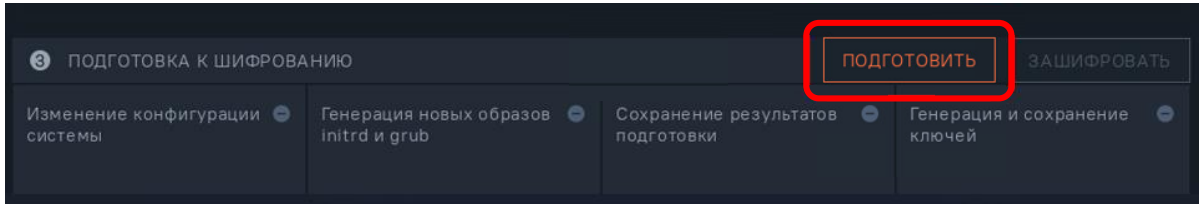
5. Защита системного раздела

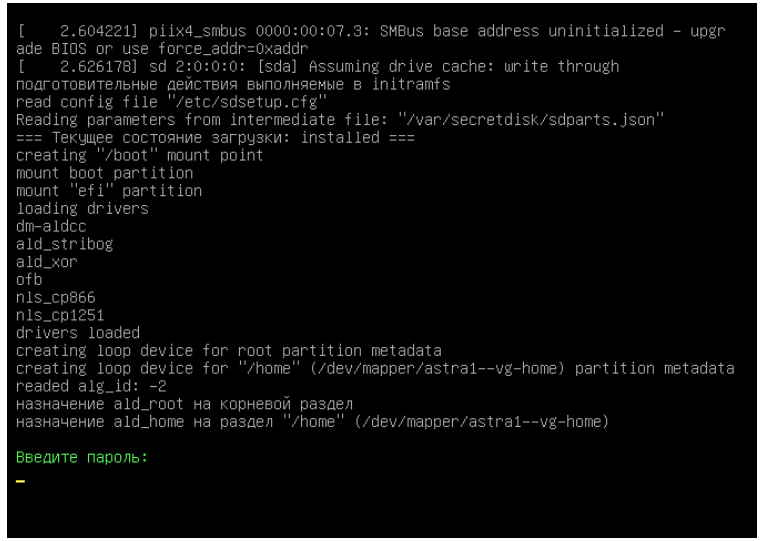
Подготовка АРМ к шифрованию

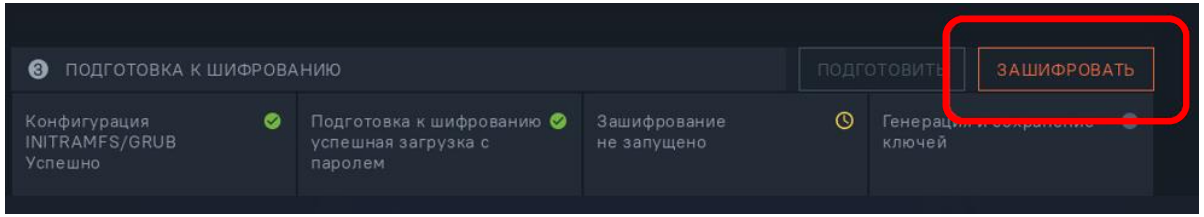
Запускаем процедуру подготовки АРМ нажатием на кнопку «**Подготовить**» в окне «**Подготовка к шифрованию**».
На самом АРМ в логе службы sdagent (/var/log/sd/sdagent.log), будет выводится информация по применению шаблона и подготовки АРМ к установке защиты.

В разделе «**Подготовка к шифрованию**», статус первого пункта перейдет в состояние «**Успешно**». После этого АРМ необходимо перезагрузить для применения изменений к загрузчику ОС. После перезагрузки будет затребован ввод пароля, необходимо ввести «**Сервисный пароль**» указанный в шаблоне.
После загрузки ОС в окне «Подготовка к шифрованию», статус второго пункта перейдет в состояние «**Успешно**».

В процессе подготовки к шифрованию вносятся изменения в порядок загрузки ядра ОС Linux, изменяется конфигурация процесса Init, подключается драйвер шифрования Secret Disk и производится тестовая перезагрузка ядра ОС.
После подготовки и перезагрузки рабочей станции включается тестовый режим шифрования с ключом 0 длины, это обеспечивает мягкое тестирование новой конфигурации АРМ и позволяет не терять контроль над процессом загрузки в случае системного сбоя.







Краткое руководство по пилотированию Secret Disk для Linux

5. Защита системного раздела

Запуск шифрования

Запуск зашифрования системного раздела инициируем нажатием кнопки «**Зашифровать**» в разделе «**Подготовка к шифрованию**».

Отследить статус шифрования в процентах можно в логе службы sdctld (/var/log/sd/sdctld.log)

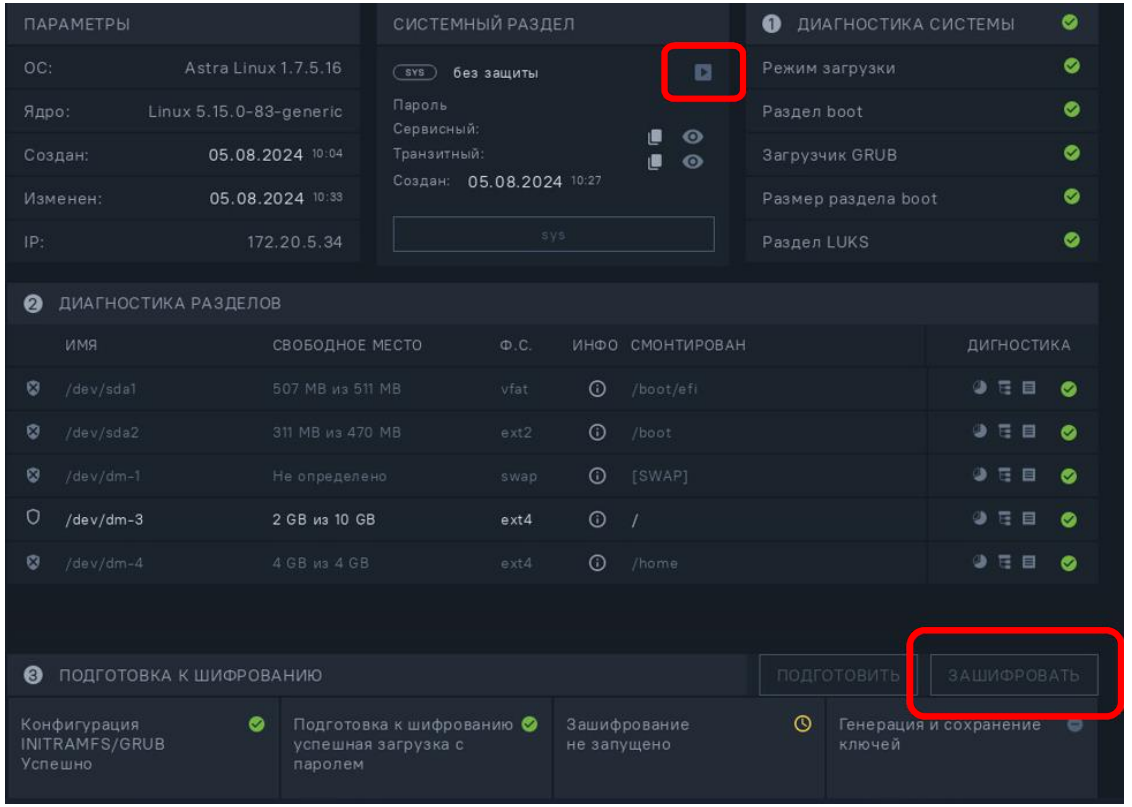
```
[2024-08-05 13:37:17.212] INFO Updated device status [/dev/mapper/ald_home]: encryption in progress[33%]
[2024-08-05 13:37:17.212] INFO Current system status: encryption in progress
[2024-08-05 13:37:17.212] INFO Overall system status: encryption in progress [17%]
[2024-08-05 13:37:17.212] INFO The driver polling attempt will be retried after 30 seconds
[2024-08-05 13:37:47.167] INFO Reenc current db status: encryption in progress
[2024-08-05 13:37:47.177] INFO Updated device status [/dev/mapper/ald_root]: encryption in progress[13%]
[2024-08-05 13:37:47.185] INFO Updated device status [/dev/mapper/ald_home]: encryption in progress[41%]
[2024-08-05 13:37:47.185] INFO Current system status: encryption in progress
[2024-08-05 13:37:47.185] INFO Overall system status: encryption in progress [21%]
```

По завершении процесса зашифрования, в логе будет отображено значение 100%, при этом, в разделе «Подготовка к шифрованию», статус третьего пункта отобразится «**Успешно**».

ℹ Далее необходимо перезагрузить рабочую станцию еще раз для установки постоянного пароля загрузки ОС

ℹ В процессе перезагрузки, необходимо ввести «Транзитный пароль», после чего ввести новый пароль пользователя. Загрузка ОС продолжится, а пароли «Сервисный» и «Транзитный» будут удалены из криптохранилища и воспользоваться ими в дальнейшем будет невозможно.

В разделе «Подготовка к шифрованию», статус четвертого пункта перейдет в состояние «**Успешно**». На этом операция по установке защиты системного раздела считается завершенной. Рабочая станция подготовлена и введена в эксплуатацию.



Статус четвертого пункта отобразится «**Успешно**». ✅