

УТВЕРЖДЕН
РСЮК.10102-01 92 01-ЛУ

**Программная система управления средой виртуализации с
подсистемой безагентного резервного копирования виртуальных
машин «ROSA Virtualization 3.0»**

Руководство по установке

РСЮК.10102-01 92 01

Листов 115

АННОТАЦИЯ

Данное руководство предназначено для системных администраторов, осуществляющих развертывание, сопровождение и контроль функционирования программного средства «Программная система управления средой виртуализации с подсистемой безагентного резервного копирования виртуальных машин «ROSA Virtualization 3.0»» РСЮК.10102-01 (далее – ROSA Virtualization).

В руководстве содержатся сведения о процессе, режимах, параметрах установки и первичной настройки ROSA Virtualization.

Дополнительные сведения об администрировании ROSA Virtualization приведены в документе «Программная система управления средой виртуализации с подсистемой безагентного резервного копирования виртуальных машин «ROSA Virtualization 3.0». Руководство администратора» РСЮК.10102-01 92 01.

СОДЕРЖАНИЕ

1. Общие сведения.....	5
1.1. Назначение и функции ROSA Virtualization.....	5
1.2. Область применения ROSA Virtualization.....	5
1.3. Программное обеспечение ROSA Virtualization.....	5
1.4. Режимы функционирования ROSA Virtualization.....	5
1.4.1. Промышленный режим.....	5
1.4.2. Тестовый режим.....	6
2. Условия выполнения установки.....	7
2.1. Требования к аппаратным средствам ROSA Virtualization.....	7
2.1.1. Требования к серверу для установки гипервизора.....	7
2.1.2. Требования к серверу для установки сервера каталогов LDAP.....	7
2.2. Требования к персоналу.....	8
3. Установка ROSA Virtualization.....	9
3.1. Конфигурация установки ROSA Virtualization.....	9
3.1.1. Стартовая конфигурация.....	9
3.1.2. Базовая конфигурация.....	9
3.2. Установка гипервизора.....	9
3.2.1. Подготовка к установке.....	9
3.2.2. Запуск программы установки.....	12
3.2.3. Параметры установки.....	13
3.2.4. Начало и ход процесса установки.....	35
3.2.5. Завершение установки.....	36
3.2.6. Вход в веб-интерфейс хоста гипервизора.....	38
3.3. Настройка системных параметров хоста гипервизора.....	40
Доступ к консоли с использованием веб-интерфейса.....	40
Доступ к консоли с использованием ssh.....	40
3.3.1. Разрешение имен DNS.....	40
3.3.2. Настройка аутентификации с применением криптографических ключей вместо пароля.....	42
3.4. Подготовка системы хранения данных.....	42
3.4.1. Подготовка хранилища NFS.....	43
3.5. Установка СУСВ.....	44
3.5.1. Развертывание хранилища Gluster.....	45
3.5.2. Процесс установки Виртуальной машины СУСВ.....	53
3.5.3. Установка сертификата ЦС.....	64

Установка сертификата ЦС с использованием веб-браузера Firefox:.....	64
Установка сертификата ЦС в веб-браузере Google Chrome:.....	67
3.5.4. Вход в веб-интерфейс СУСВ.....	74
3.6. Добавление хостов в кластер.....	76
3.6.1. Добавление хостов в кластер с использованием портала администрирования СУСВ.....	76
3.7. Активация лицензии ROSA Virtualization.....	78
3.7.1. Пример активации лицензии ROSA Virtualization.....	78
3.7.2. Пример просмотра информации об лицензии.....	79
3.8. Установка сервера IPA.....	79
3.8.1. Создание ВМ для сервера IPA.....	79
3.8.2. Установка ОС на сервер IPA.....	84
3.8.3. Выполнение сценария установки ПО сервера IPA.....	86
3.8.4. Вход в веб-интерфейс сервера IPA.....	103
3.9. Подключение ROSA Virtualization к службе каталогов LDAP сервера IPA.....	104
3.9.1. Создание служебной учетной записи пользователя с использованием веб- интерфейса.....	104
3.9.2. Создание профиля подключения к службе каталогов LDAP сервера IPA.....	108
Перечень сокращений.....	113

1. ОБЩИЕ СВЕДЕНИЯ

1.1. НАЗНАЧЕНИЕ И ФУНКЦИИ ROSA VIRTUALIZATION

ROSA Virtualization – платформа виртуализации с интегрированной системой управления, предназначенная для развертывания виртуального центра обработки данных (ВЦОД) корпоративного уровня.

ROSA Virtualization предоставляет возможности для создания, управления и функционирования свыше тысячи виртуальных машин (ВМ) в одном ВЦОД с применением дискреционной и ролевой модели доступа, а также других встроенных механизмов обеспечения защиты информации (в том числе использование шифрованных виртуальных дисков).

1.2. ОБЛАСТЬ ПРИМЕНЕНИЯ ROSA VIRTUALIZATION

ROSA Virtualization может эксплуатироваться в центрах обработки данных государственных органов и частных организаций различного масштаба.

Версия ROSA Virtualization, сертифицированная ФСТЭК России, может эксплуатироваться в государственных информационных системах, в том числе, обрабатывающих персональные данные, в значимых объектах критической информационной инфраструктуры, в автоматизированных системах управления производственными и технологическими процессами, а также в информационных системах общего и специального назначения.

1.3. ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ ROSA VIRTUALIZATION

Программное обеспечение ROSA Virtualization состоит из следующих основных функциональных компонентов:

- гипервизор – компонент устанавливается непосредственно на физический сервер без предустановленной ОС и получает прямой доступ к аппаратному оборудованию этого хоста. Гипервизор обеспечивает создание, запуск и функционирование виртуальных машин на своем хосте;
- система управления средой виртуализации (СУСВ) – в базовой конфигурации компонент располагается во внешнем отказоустойчивом хранилище данных. СУСВ предоставляет графический интерфейс для централизованного управления объектами виртуальной среды (гипервизоры, хранилища, кластеры хостов, дата-центры, виртуальные машины и т.п.);
- сервер IPA для идентификации и аутентификации доменных пользователей;
- компонент формирования отчетности;
- клиент для ОС семейства Windows с поддержкой версий от XP SP3 и выше;
- дополнительные компоненты – драйверы паравиртуализации, утилиты и служебные программы.

1.4. РЕЖИМЫ ФУНКЦИОНИРОВАНИЯ ROSA VIRTUALIZATION

В зависимости от целей использования существуют различные режимы функционирования ROSA Virtualization. Наиболее распространенными режимами функционирования являются промышленный и тестовый режимы.

1.4.1. ПРОМЫШЛЕННЫЙ РЕЖИМ

Промышленный режим функционирования ROSA Virtualization рекомендуется к применению во всех сферах, связанных с обработкой важных данных и работой критичных

сервисов организации (например, доменные службы, веб-сервисы, сервисы СУБД, системы документооборота).

В промышленном режиме используются высокопроизводительные модели оборудования, применяется дублирование отдельных узлов аппаратного обеспечения, функционирует система гарантированного питания.

Главным достоинством промышленного режима является повышенная надежность и отказоустойчивость всего вычислительного комплекса, включающая резервирование данных и СУСВ.

К недостаткам промышленного режима функционирования ROSA Virtualization относятся следующие факторы:

- требование к наличию минимум трех аппаратных серверов промышленных моделей для установки гипервизоров при использовании отказоустойчивой файловой системы GlusterFS или не менее двух при использовании внешнего отказоустойчивого хранилища;
- повышенная нагрузка на сетевую подсистему при использовании распределенных отказоустойчивых файловых систем GlusterFS;
- повышенные требования к вспомогательному оборудованию, включая средства резервирования жестких дисков, а также оборудование сетей, электропитания, охлаждения.

Обеспечение высокой надежности и доступности подразумевает правильную организацию и тщательную настройку не только программной, но и аппаратной части вычислительного комплекса.

1.4.2. ТЕСТОВЫЙ РЕЖИМ

Тестовый режим функционирования ROSA Virtualization используется для развертывания платформы виртуализации в лабораториях и учебных классах с целью создания стенда для изучения функций и демонстрации возможностей ROSA Virtualization.

В тестовом режиме возможен вариант с использованием одного хоста для установки и функционирования следующих компонентов ROSA Virtualization:

- гипервизор с рабочими ВМ;
- локальное хранилище с развернутой СУСВ.

Тестовый режим не требует проектирования и создания сложных аппаратных и программных конфигураций для сети и хранилищ, а также не предъявляет повышенных требований к аппаратным компонентам как для создаваемой среды виртуализации, так и для иной инфраструктуры вычислительного комплекса.

При этом тестовый режим функционирования ROSA Virtualization не подходит для использования, если в автоматизированной (информационной) системе планируется обрабатывать важные или критичные данные, а также обеспечивать инфраструктуру высоконагруженными и отказоустойчивыми сервисами.

2. УСЛОВИЯ ВЫПОЛНЕНИЯ УСТАНОВКИ

2.1. ТРЕБОВАНИЯ К АППАРАТНЫМ СРЕДСТВАМ ROSA VIRTUALIZATION

В базовой конфигурации установки аппаратное обеспечение ROSA Virtualization должно состоять из следующих технических средств:

- минимум 3 физических сервера с поддержкой функций аппаратной виртуализации, предназначенных для установки и функционирования гипервизоров, при использовании отказоустойчивой файловой системы GlusterFS;

или:

- минимум 2 физических сервера с поддержкой функций аппаратной виртуализации, предназначенных для установки и функционирования гипервизоров, при использовании внешнего отказоустойчивого хранилища;
- сервер каталогов LDAP (возможно использование существующего корпоративного сервера LDAP для идентификации и аутентификации доменных пользователей или сервера IPA, развернутого на ВМ под управлением ROSA Virtualization);
- система хранения данных;
- сетевая инфраструктура высокого уровня производительности.

2.1.1. ТРЕБОВАНИЯ К СЕРВЕРУ ДЛЯ УСТАНОВКИ ГИПЕРВИЗОРА

Сервер, предназначенный для установки гипервизора, должен соответствовать следующим аппаратным требованиям:

- процессор с количеством ядер не менее 4 и поддержкой функций аппаратной виртуализации AMD-V (для процессора AMD) или Intel VT (для процессора Intel®). Дополнительно в настройках BIOS / UEFI (в общем случае в разделе “Advanced → CPU Configuration”) должен быть включен (установлено значение Enabled) режим аппаратной виртуализации процессора;
- оперативная память не менее 64 ГБ;
- свободное дисковое пространство не менее 100 ГБ;
- сетевой интерфейс не менее 10 Гбит/с – для связи между хостами гипервизоров и системой хранения данных (допускается скорость передачи данных 1 Гбит/с с агрегацией интерфейсов слабонагруженных конфигураций);
- привод DVD / порт USB – для установки ПО.

2.1.2. ТРЕБОВАНИЯ К СЕРВЕРУ ДЛЯ УСТАНОВКИ СЕРВЕРА КАТАЛОГОВ LDAP

Сервер каталогов LDAP (сервер IPA) должен соответствовать следующим аппаратным требованиям:

- процессор архитектуры x86_64;
- оперативная память не менее 2 ГБ;
- свободное дисковое пространство не менее 50 ГБ;
- сетевой интерфейс не менее 1 Гбит/с;
- привод DVD / порт USB – для установки ПО.

Объем разделяемого хранилища системы хранения данных должен составлять не менее 500 ГБ.

2.2. ТРЕБОВАНИЯ К ПЕРСОНАЛУ

Системный администратор, осуществляющий процесс установки и первичной настройки ROSA Virtualization, должен обладать опытом развертывания и сопровождения серверных версий ОС Linux, совместимых с диалектом Red Hat® Enterprise Linux, таких как ROSA “Cobalt” Server, CentOS и т.п.

3. УСТАНОВКА ROSA VIRTUALIZATION

Установка ROSA Virtualization осуществляется администратором в соответствии с заранее выбранной конфигурацией установки – стартовой или базовой.

3.1. КОНФИГУРАЦИЯ УСТАНОВКИ ROSA VIRTUALIZATION

3.1.1. СТАРТОВАЯ КОНФИГУРАЦИЯ

Стартовая конфигурация установки предназначена для дальнейшего использования ROSA Virtualization в тестовом режиме функционирования в качестве стенда для изучения функций и демонстрации возможностей ROSA Virtualization.

Для установки ROSA Virtualization в стартовой конфигурации выполните следующие действия:

- установка гипервизора и настройка системных параметров на хосте;
- подготовка системы хранения данных;
- установка СУСБ;
- активация лицензии ROSA Virtualization.

3.1.2. БАЗОВАЯ КОНФИГУРАЦИЯ

Базовая конфигурация установки предназначена для дальнейшего использования ROSA Virtualization в промышленном режиме функционирования в качестве платформы виртуализации вычислительных центров, связанных с обработкой важных данных и работой критичных сервисов организации.

Для установки ROSA Virtualization в базовой конфигурации выполните следующие действия:

- установка гипервизоров и настройка системных параметров на нескольких хостах;
- подготовка системы хранения данных;
- установка СУСБ;
- добавление хостов в кластер;
- активация лицензии ROSA Virtualization;
- установка сервера IPA в качестве сервера каталогов LDAP для идентификации и аутентификации доменных пользователей и настройка подключения ROSA Virtualization к службе каталогов LDAP сервера IPA.

3.2. УСТАНОВКА ГИПЕРВИЗОРА

Установка гипервизора ROSA Virtualization осуществляется непосредственно на физический сервер без предустановленной ОС.

Для установки гипервизора используется специальная программа Anaconda, которая предоставляет администратору простой и удобный графический интерфейс, а также позволяет изменять размер существующих разделов диска на этапе установки.

3.2.1. ПОДГОТОВКА К УСТАНОВКЕ

По умолчанию дистрибутив ROSA Virtualization поставляется на DVD.

Если привод DVD в компьютере отсутствует, установку можно осуществить с USB-накопителя объемом не менее 8 ГБ. Для этого необходимо записать образ с дистрибутивом ROSA Virtualization на данный носитель, что можно сделать на любом компьютере с приводом DVD и свободным портом USB.

3.2.1.1. ЗАПИСЬ ОБРАЗА ДИСТРИБУТИВА ROSA VIRTUALIZATION НА USB-НАКОПИТЕЛЬ

Для записи образа вставьте диск с дистрибутивом ROSA Virtualization в DVD-привод, подключите USB-накопитель и скопируйте содержимое диска.

На компьютере с установленной ОС семейства Linux для копирования диска выполните следующую консольную команду с правами суперпользователя root:

```
# dd if=/dev/sr0 of=/dev/sdX
```

где **X** – буква диска, соответствующая USB-накопителю.

Примечание – Для получения сведений о подключенных к системе накопителях выполните следующую консольную команду с правами суперпользователя root:

```
# fdisk -l
```

При успешном подключении USB-накопителя в консоль будет выведена информация подобного вида:

```
# fdisk -l
```

Диск /dev/nvme0n1: 60 GiB, 64424509440 байт, 125829120 секторов

Единицы: секторов по 1 * 512 = 512 байт

Размер сектора (логический/физический): 512 байт / 512 байт

Размер I/O (минимальный/оптимальный): 512 байт / 512 байт

Тип метки диска: dos

Идентификатор диска: 0x9ab46fba

Устр-во	Загрузочный	начало	Конец	Секторы	Размер	Идентификатор	Тип
/dev/nvme0n1p1	*	2048	2099199	2097152	1G	83	
Linux							
/dev/nvme0n1p2		2099200	125829119	123729920	59G	8e	
Linux LVM							

Диск /dev/mapper/rv-root: 15,1 GiB, 16257122304 байт, 31752192 секторов

Единицы: секторов по 1 * 512 = 512 байт

Размер сектора (логический/физический): 512 байт / 512 байт

Размер I/O (минимальный/оптимальный): 65536 байт / 65536 байт

Диск /dev/mapper/rv-swap: 3,9 GiB, 4215275520 байт, 8232960 секторов

Единицы: секторов по 1 * 512 = 512 байт

Размер сектора (логический/физический): 512 байт / 512 байт

Размер I/O (минимальный/оптимальный): 512 байт / 512 байт

Диск /dev/mapper/rv-var_log_audit: 2 GiB, 2147483648 байт, 4194304 секторов

Единицы: секторов по 1 * 512 = 512 байт

Размер сектора (логический/физический): 512 байт / 512 байт
Размер I/O (минимальный/оптимальный): 65536 байт / 65536 байт

Диск /dev/mapper/rv-var_log: 8 GiB, 8589934592 байт, 16777216 секторов
Единицы: секторов по 1 * 512 = 512 байт
Размер сектора (логический/физический): 512 байт / 512 байт
Размер I/O (минимальный/оптимальный): 65536 байт / 65536 байт

Диск /dev/mapper/rv-var: 15 GiB, 16106127360 байт, 31457280 секторов
Единицы: секторов по 1 * 512 = 512 байт
Размер сектора (логический/физический): 512 байт / 512 байт
Размер I/O (минимальный/оптимальный): 65536 байт / 65536 байт

Диск /dev/mapper/rv-tmp: 2 GiB, 2147483648 байт, 4194304 секторов
Единицы: секторов по 1 * 512 = 512 байт
Размер сектора (логический/физический): 512 байт / 512 байт
Размер I/O (минимальный/оптимальный): 65536 байт / 65536 байт

Диск /dev/mapper/rv-home: 1 GiB, 1073741824 байт, 2097152 секторов
Единицы: секторов по 1 * 512 = 512 байт
Размер сектора (логический/физический): 512 байт / 512 байт
Размер I/O (минимальный/оптимальный): 65536 байт / 65536 байт

Диск /dev/sda: 3,8 GiB, 4026531840 байт, 7864320 секторов
Единицы: секторов по 1 * 512 = 512 байт
Размер сектора (логический/физический): 512 байт / 512 байт
Размер I/O (минимальный/оптимальный): 512 байт / 512 байт
Тип метки диска: dos
Идентификатор диска: 0x0060d108

Устр-во	Загрузочный	начало	Конец	Секторы	Размер	Идентификатор	Тип
/dev/sda1	*	2048	7864319	7862272	3,8G	e W95 FAT16	(LBA)

Раздел /dev/sda1 с файловой системой W95 FAT16 (LBA) соответствует подключенному к компьютеру USB-накопителю.

Для вывода информации только о подключенных к системе накопителях можно воспользоваться командой `fdisk -l | grep sda`:

```
# fdisk -l | grep sda
Диск /dev/sda: 3,8 GiB, 4026531840 байт, 7864320 секторов
/dev/sda1 *          2048 7864319 7862272    3,8G          e W95 FAT16 (LBA)
```

Раздел `/dev/sda1` соответствует первому подключенному к системе накопителю. При использовании нескольких накопителей они могут быть идентифицированы как `/dev/sdb1`, `/dev/sdc1` и т.д.

3.2.2. ЗАПУСК ПРОГРАММЫ УСТАНОВКИ

Для установки гипервизора загрузите сервер с носителя с дистрибутивом ROSA Virtualization.

Примечание – В настройках BIOS / UEFI установите приоритет загрузки сервера с DVD или USB-накопителя, а также включите режим аппаратной виртуализации процессора.

В процессе загрузки сервера на экране автоматически появится меню, позволяющее запускать программу установки гипервизора в различных режимах (Рисунок 1).

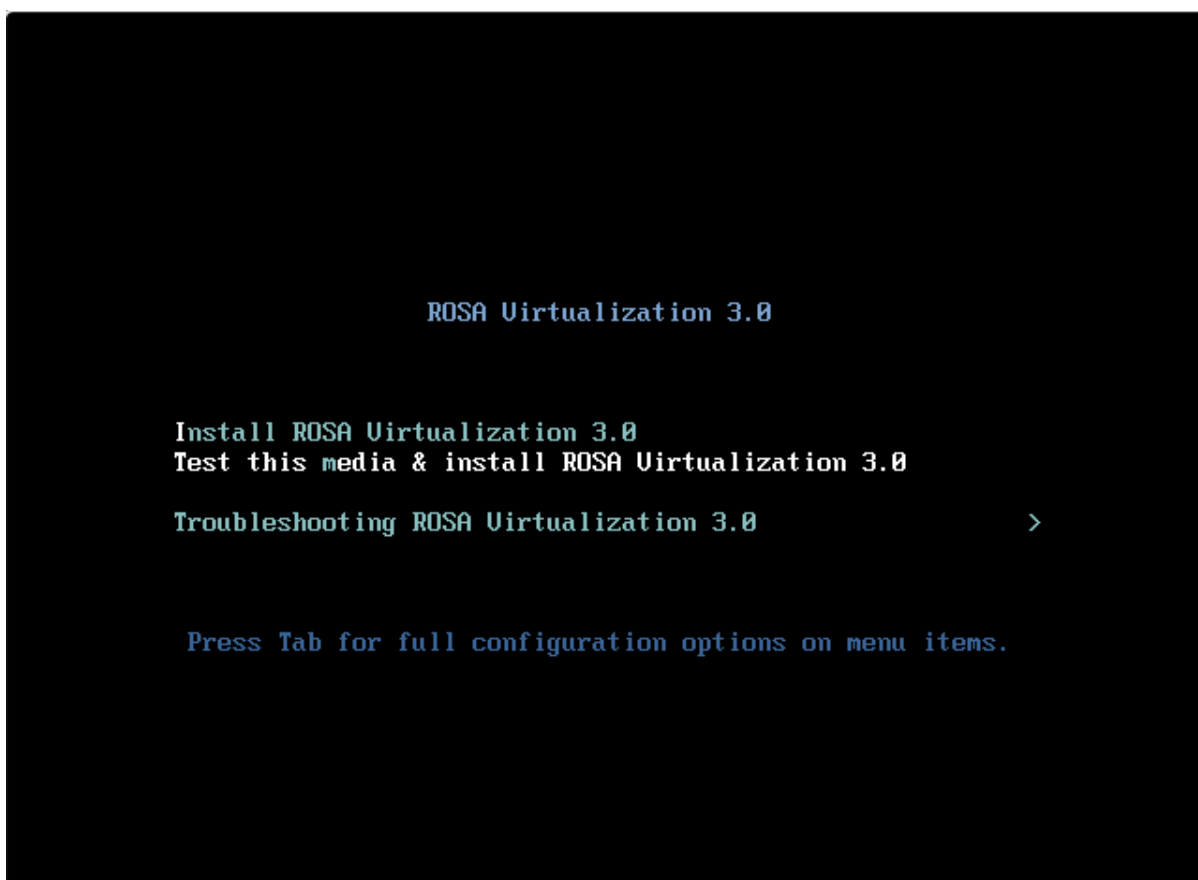


Рисунок 1 - Меню установки

Для запуска графического интерфейса программы установки гипервизора нажмите клавишу `Enter` или дождитесь автоматического старта установки через 60 секунд.

Примечания:

1. В данном руководстве рассматривается вариант установки гипервизора с использованием графического интерфейса программы Anaconda, но в редких случаях (например, когда программа установки не может корректно определить видеокарту) может потребоваться консольный режим установки гипервизора в текстовом интерфейсе программы Anaconda.

В текстовом режиме установки гипервизора будут доступны только стандартные схемы разбиения диска на разделы (например, можно использовать весь диск или удалить существующие разделы, но нельзя добавлять разделы и файловые системы).

2. Для запуска текстового интерфейса программы установки гипервизора нажмите клавишу **Tab**, затем введите через пробел слово `text` в конец строки с параметрами загрузки и нажмите клавишу **Enter**.

3.2.2.1. ВЫБОР ЯЗЫКА ДЛЯ УСТАНОВКИ

После запуска программы установки на экране появится окно приветствия (Рисунок 2), предназначенное для выбора языка интерфейса, который будет использоваться в процессе установки гипервизора.

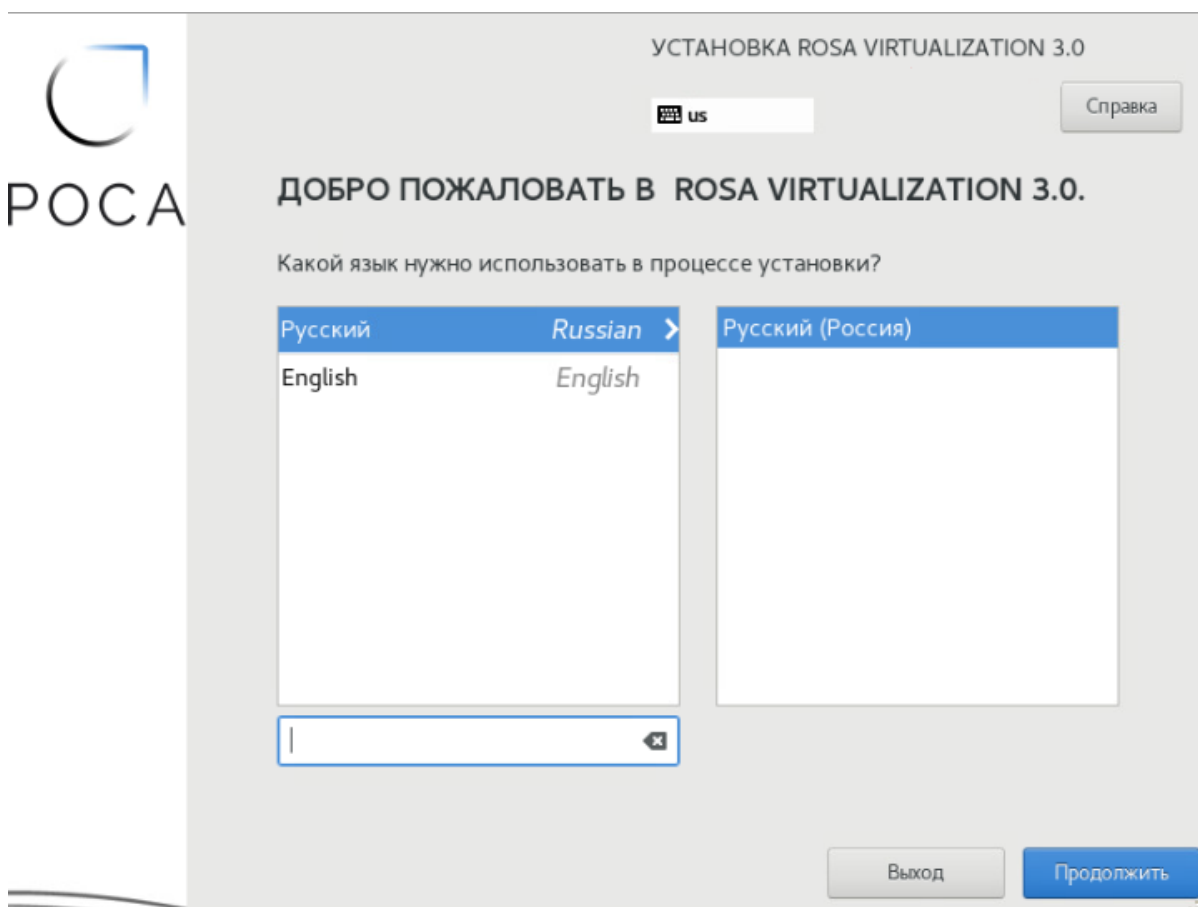


Рисунок 2 - Окно приветствия программы установки

Используя полосу прокрутки и строку поиска выберите из списка в левой области окна необходимый язык интерфейса установки, а в правой области – языковой регион.

По умолчанию язык интерфейса установки – Русский (Россия).

Для перехода к следующему этапу установки нажмите кнопку **Продолжить**.

3.2.3. ПАРАМЕТРЫ УСТАНОВКИ

3.2.3.1. НАСТРОЙКА ПАРАМЕТРОВ УСТАНОВКИ СИСТЕМЫ

На экране появится интерфейс, предназначенный для обзора и последующей настройки параметров установки (Рисунок 3). Вместо последовательного определения параметров программа

установки дает возможность настроить параметры в произвольном порядке, выбирая необходимые секции с требуемыми параметрами в меню “Сводка установки”.

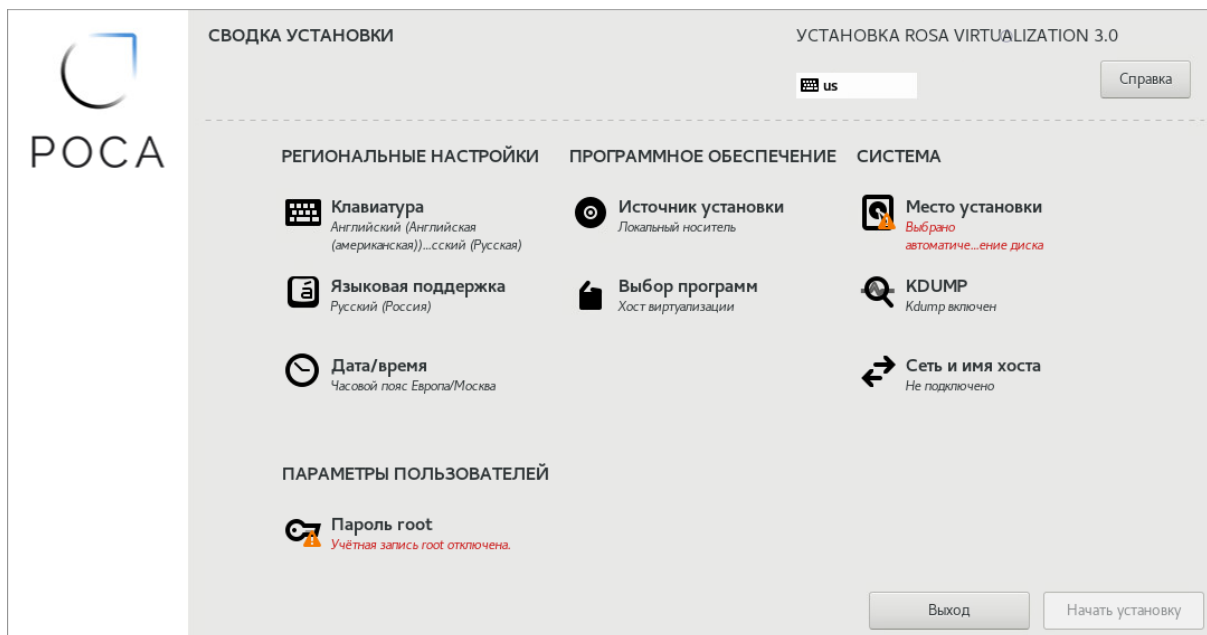


Рисунок 3 - Сводка установки

В меню “Сводка установки” параметры установки распределены по следующим разделам – Региональные настройки, Программное обеспечение, Система, Параметры пользователей.

3.2.3.2. РЕГИОНАЛЬНЫЕ НАСТРОЙКИ

Раздел “Региональные настройки” содержит следующие секции с параметрами установки:

- Клавиатура – интерфейс секции позволяет выбрать раскладку клавиатуры и указать комбинацию клавиш для переключения раскладки. Значения параметров по умолчанию – раскладка “Английская/Русская” с комбинацией клавиш **Alt+Shift** для переключения раскладки;
- Языковая поддержка – интерфейс секции предназначен для добавления дополнительных языков в пользовательский интерфейс гипервизора. Значение параметра по умолчанию – Русский (Россия);
- Дата/время – интерфейс секции предназначен для проверки и при необходимости корректировки автоматически определенных даты, времени и часового пояса, а также для подключения гипервизора к внешним сетевым источникам точного времени по протоколу NTP.

3.2.3.3. НАСТРОЙКА УСТАНОВЛИВАЕМОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Раздел “Программное обеспечение” содержит следующие секции с параметрами установки:

- Источник установки – интерфейс секции позволяет указать расположение установочных файлов (локальный носитель или сетевой репозиторий) и осуществить проверку целостности установочного носителя. Если программа установки гипервизора была запущена с DVD или USB-накопителя, то установочный носитель будет обнаружен автоматически;

- Выбор программ – интерфейс секции предназначен для выбора базового программного окружения, которое будет установлено в процессе инсталляции ПО.

Примечание – Значение параметра по умолчанию – Хост виртуализации (функции гипервизора).

3.2.3.3.1. ВЫБОР ТИПА УСТАНОВЛИВАЕМОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Выбрать тип устанавливаемых компонент можно в меню “Выбор программ” (Рисунок 4).

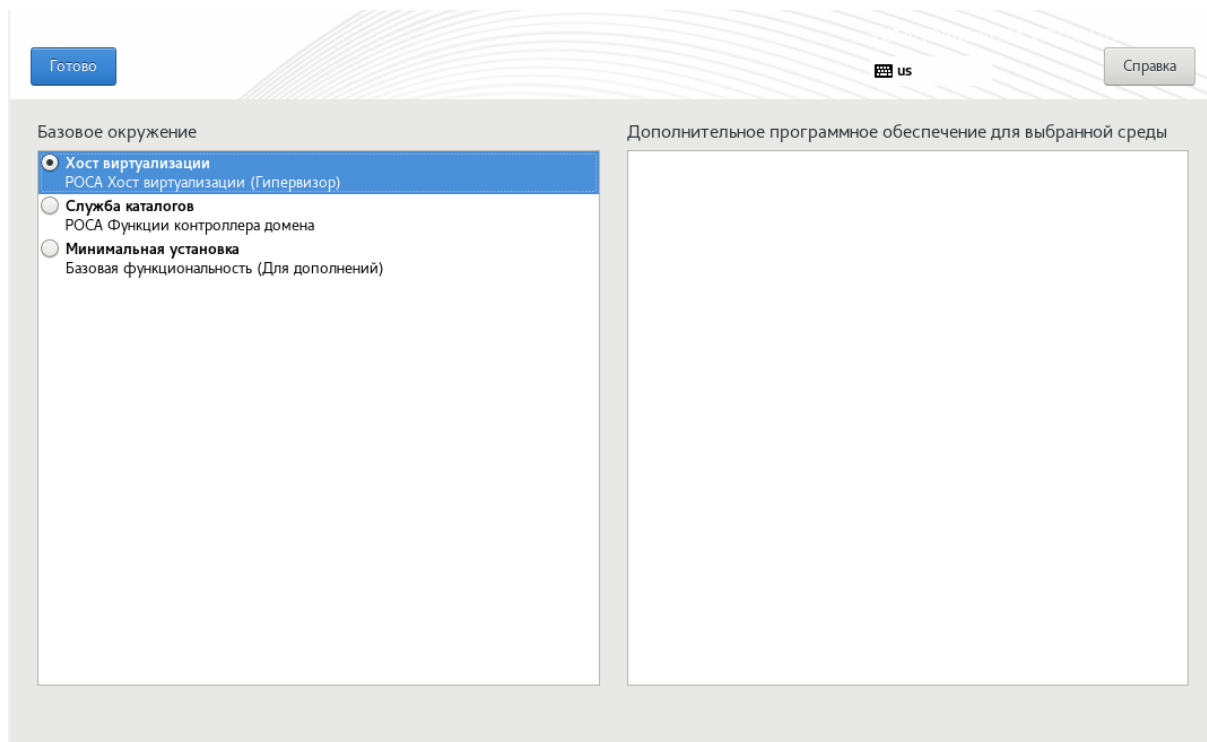


Рисунок 4 - Выбор типа устанавливаемого ПО (выбран тип: Хост виртуализации/Гипервизор)

Доступны следующие компоненты базового окружения:

- Хост виртуализации – выберите данную опцию для установки хоста виртуализации (функции гипервизора).
- Служба каталогов – выберите данную опцию для установки службы каталогов/контроллера домена.
- Минимальная установка – выберите данную опцию для установки минимальной конфигурации сервера

После выбора необходимого компонента нажмите на кнопку “Готово” для возврата на экранную форму “Сводка установки”.

3.2.3.4. НАСТРОЙКА ПАРАМЕТРОВ СИСТЕМЫ, СЕТЕВЫЕ НАСТРОЙКИ, ВЫБОР ИМЕНИ ХОСТА

Раздел “Система” содержит следующие секции с параметрами установки:

- Место установки – интерфейс секции предназначен для выбора диска для установки гипервизора и настройки конфигурации разделов диска в автоматическом или ручном режиме;
- KDUMP – интерфейс секции предназначен для управления (включение / выключение) и настройки резервирования памяти для kdump (механизм сбора статистики о сбоях ядра). Значение параметра по умолчанию – kdump включен с резервированием памяти в автоматическом режиме;
- Сеть и имя хоста – интерфейс секции предназначен для настройки параметров сетевых адаптеров и указания имени хоста гипервизора;

Раздел “Параметры пользователей” содержит секцию “Пароль root”, которая предназначена для установки пароля учетной записи суперпользователя root (администратора гипервизора).

Под наименованием каждой секции приводится информация о текущих параметрах, настроенных автоматически программой установки.

Примечание – Секции, отмеченные восклицательным знаком, являются обязательными для настройки параметров, что также подтверждает сообщение в нижней части окна, выделенное оранжевым фоном – Заполните отмеченные секции, прежде чем перейти к следующему шагу.

Нажмите на наименование секции для перехода к интерфейсу настройки соответствующих параметров.

Примечание – Следующие секции являются обязательными или рекомендуемыми для настройки параметров установки гипервизора:

- Дата/время (см. подпункт 3.2.3.5);
- Целевое устройство установки (см. подпункт 3.2.3.6);
- Сеть и имя хоста (см. подпункт 3.2.3.7);
- Пароль root (см. подпункт 3.2.3.8).

Примечание – Настройка даты/времени с использованием серверов NTP требует подключения к внешним сетевым источникам точного времени. Настройте **Сеть и имя хоста** до начала настройки даты/времени, если вы планируете использовать внешние сетевые источники точного времени.

После настройки всех обязательных и рекомендуемых параметров нажмите кнопку **Начать установку** для старта процесса установки гипервизора (см. пункт 3.2.4).

Для отмены установки нажмите кнопку **Выход** и подтвердите прекращение процесса установки.

3.2.3.5. ДАТА, ВРЕМЯ И ЧАСОВОЙ ПОЯС

Интерфейс секции “Дата/время” предназначен для проверки и при необходимости корректировки автоматически определенных даты, времени и часового пояса, а также для подключения гипервизора к внешним сетевым источникам точного времени по протоколу NTP (Рисунок 5).

Примечание – Для настройки даты/времени с использованием серверов NTP требуется настроенное сетевое подключение (настройка осуществляется в секции **Сеть и имя хоста**), обеспечивающее сетевую доступность серверов NTP.

The screenshot shows the 'ДАТА И ВРЕМЯ' (Date and Time) configuration window of the ROSA COBALI system. At the top, there is a 'Готово' (Ready) button and a language selector set to 'ru'. Below this, the 'Регион' (Region) is set to 'Европа' (Europe) and the 'Город' (City) is set to 'Москва' (Moscow). A 'Сетевое время' (Network time) toggle is present. The main area features a world map with the European region highlighted in green. Below the map, there are controls for time adjustment: up/down arrows for hours and minutes, and a time format selector with radio buttons for '24-часовой формат' (24-hour format) and 'AM/PM'. Date selection is handled by dropdown menus for day (01), month (07), and year (2021). An orange warning banner at the bottom states: 'Для использования NTP нужно сначала настроить сеть' (To use NTP, you need to configure the network first).

Рисунок 5 - Дата, время и часовой пояс

Для настройки времени и часового пояса выберите последовательно регион и город из соответствующих выпадающих списков. Если необходимого города нет в списке, выберите ближайший город в той же часовой зоне.

Примечание – Настройте часовой пояс, даже если вы планируете использовать протокол NTP для синхронизации часов.

Если системные часы показывают неверное время, откорректируйте его с помощью кнопок ▲ (больше) и ▼ (меньше). Для выбора формата отображения времени установите в соответствующее положение переключатель – 24-часовой формат или AM/PM.

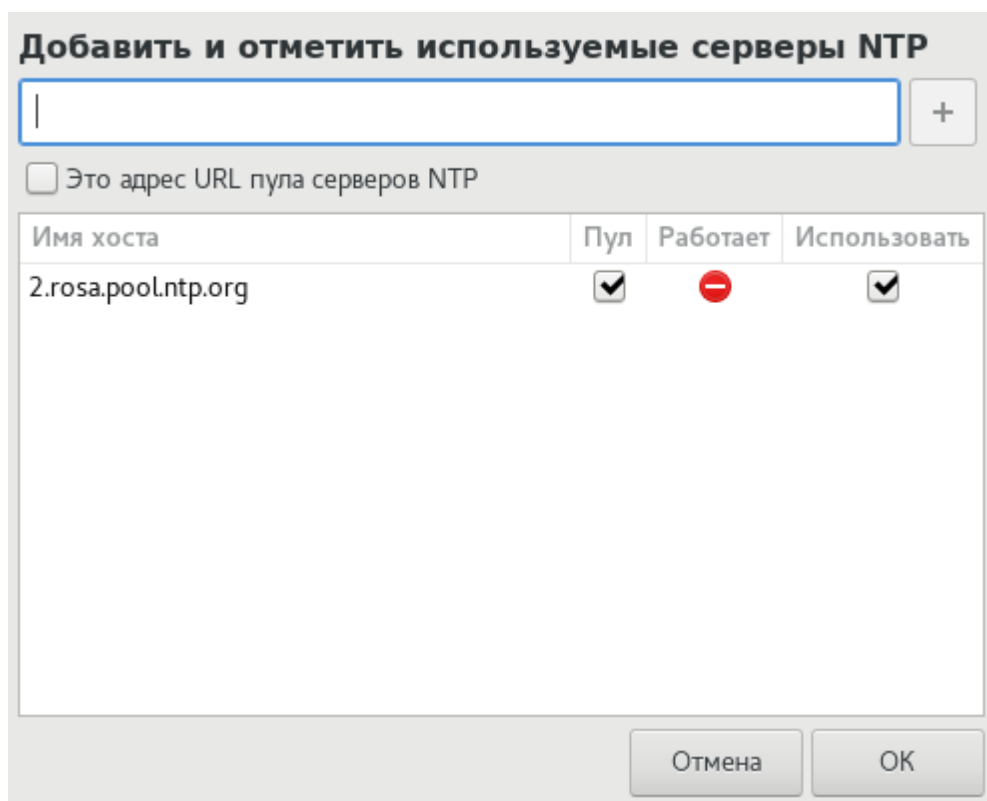
При необходимости скорректируйте дату. Для этого выберите из выпадающих списков текущие значения дня, месяца и года.

Примечание – Для использования внешних сетевых источников точного времени по протоколу NTP необходимо сначала настроить сетевое подключение, обеспечив сетевую доступность серверов NTP.

3.2.3.5.1. НАСТРОЙКА СЕТЕВОГО ВРЕМЕНИ С ИСПОЛЬЗОВАНИЕМ ПРОТОКОЛА NTP

Если сервер подключен к сети, будет доступен переключатель “Сетевое время”. Чтобы включить синхронизацию часов с использованием протокола NTP, установите во включенное положение переключатель “Сетевое время”.

Для настройки синхронизации времени с определенным сервером NTP нажмите кнопку конфигурации . На экране появится модальное окно “Добавить и отметить используемые серверы NTP” (Рисунок 6).

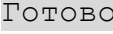


Имя хоста	Пул	Работает	Использовать
2.rosa.pool.ntp.org	☒		☒

Рисунок 6 - Выбор сервера NTP

Для выбора сервера NTP из списка установите флажок “Использовать”. Для добавления дополнительного сервера NTP в список введите имя узла (адрес) и нажмите кнопку . Для завершения настройки нажмите кнопку .

Примечание – Если во время установки выбранный сервер NTP недоступен, системное время будет выставлено, когда сервер NTP станет активным.

После настройки временных параметров нажмите кнопку  для возвращения в меню “Сводка установки”.

3.2.3.6. ВЫБОР МЕСТА УСТАНОВКИ

Интерфейс секции “Целевое устройство установки” предназначен для выбора диска для установки гипервизора и настройки конфигурации разделов диска в автоматическом или ручном режиме (Рисунок 7).

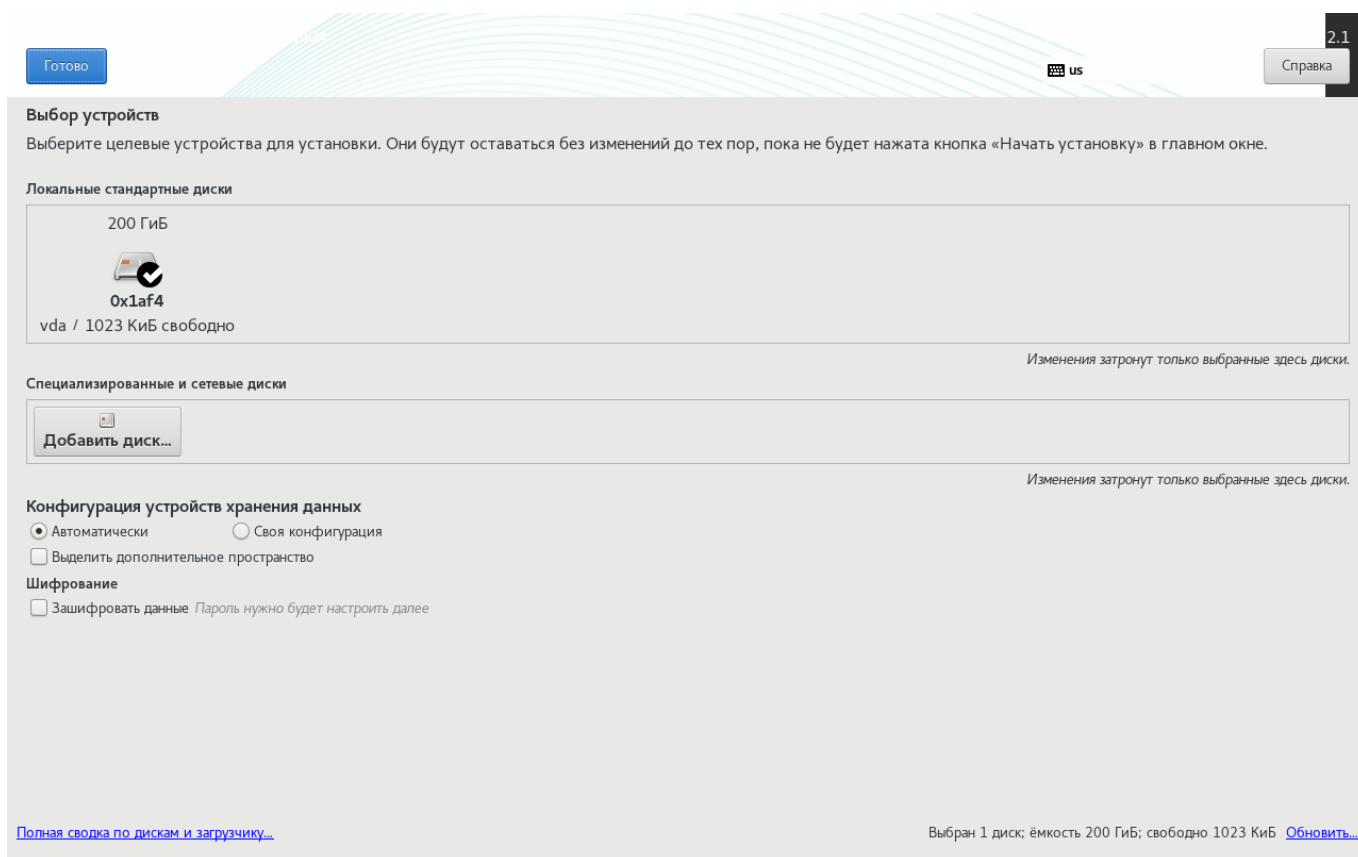


Рисунок 7 - Выбор диска и способа конфигурации разделов

По умолчанию интерфейс отображает только локальные диски, доступные для установки гипервизора. Для каждого диска показаны размер, метка, доступное пространство. Для выбора диска нажмите на блок с информацией о диске. Выбранный для установки диск будет отмечен галочкой. При необходимости и наличии выберите несколько дисков для установки. Если диск не выбран, он не будет использоваться при установке.

Примечание – При необходимости в добавлении дополнительных устройств хранения данных (специализированных накопителей iSCSI, сетевых дисков FCoE SAN, устройств с модулями постоянной памяти NVDIMM) нажмите кнопку **Добавить диск**.

Для новой установки гипервизора с удалением всех существующих данных с выбранного диска установите переключатель “Конфигурация устройств хранения данных” в положение “Автоматически”. Если на выбранном диске недостаточно свободного места для автоматического разбиения или был установлен флажок “Выделить дополнительное пространство”, освободите пространство на диске вручную (см. подпункт 3.2.3.6.1).

Для настройки пользовательской конфигурации и создания разделов диска вручную установите переключатель “Конфигурация устройств хранения данных” в положение “Своя конфигурация” (см. подпункт 3.2.3.6.2).

Примечание – При необходимости в шифровании разделов диска (кроме /boot) установите флажок “Зашифровать данные” (см. подпункт 3.2.3.6.3).

При наличии двух и более дисков, выбранных для установки гипервизора, перейдите по ссылке “Полная сводка по дискам и загрузчику” в интерфейс выбора диска, на котором будет установлен загрузчик (см. подпункт 3.2.3.6.4).

Для продолжения настройки конфигурации диска или возвращения в меню “Сводка установки” нажмите кнопку **Готово**.

3.2.3.6.1. ОСВОБОЖДЕНИЕ ДОПОЛНИТЕЛЬНОГО ПРОСТРАНСТВА НА ДИСКЕ

Интерфейс освобождения дискового пространства содержит список разделов диска (файловых систем) и элементы управления, позволяющие удалять или уменьшать разделы (Рисунок 8).

Примечание – При освобождении пространства будут удалены все данные, которые содержит раздел диска (за исключением случаев сжатия раздела), поэтому предварительно рекомендуется создать резервные копии необходимых данных.

ОСВОБОЖДЕНИЕ ПРОСТРАНСТВА НА ДИСКЕ

Чтобы освободить место, можно удалить ненужные файловые системы. Удаление файловой системы навсегда уничтожит и все данные, которые она содержит.

Диск	Имя	Файловая система	Сколько места на диске можно освободить	Действие
▼ 200 ГиБ 0x1af4	vda	Unknown	200 ГиБ total	Не изменять
└─ Свободное пространство			200 ГиБ	

Не изменять Удалить Уменьшить Удалить всё

1 диск; можно освободить 200 ГиБ (в файловых системах)

Всего выбрано для освобождения: 0
Для установки системных данных необходимо 11,03 ГиБ.

Отмена Освободить пространство

Рисунок 8 - Интерфейс формы для освобождения дискового пространства

В столбце “Сколько места на диске можно освободить” показан потенциально доступный размер дискового пространства.

В столбце “Действие” показан метод освобождения пространства, а сами методы освобождения пространства доступны по нажатию следующих соответствующих кнопок:

- **Не изменять** – не освобождать место в выбранной файловой системе. Это действие установлено по умолчанию;
- **Удалить** – освободить все занятое пространство;
- **Уменьшить** – освободить незанятое пространство в файловой системе. Размер корректируется с помощью ползунка. Это действие недоступно для LVM и RAID;
- **Удалить все** / **Оставить все** – функционирует как переключатель: если выбрать один вариант, название кнопки изменится на второй, и наоборот. Действие применимо ко всем файловым системам.

Выберите файловую систему (раздел) или весь диск, после чего примените необходимые методы освобождения пространства. Когда будет достигнут достаточный объем свободного

дискового пространства для продолжения установки (объем зависит от выбранного базового и дополнительного ПО) нажмите кнопку **Освободить пространство**, которая станет доступной для использования.

3.2.3.6.2. НАСТРОЙКА ПОЛЬЗОВАТЕЛЬСКОЙ КОНФИГУРАЦИИ РАЗДЕЛОВ ДИСКА

Для установки гипервизора рекомендуется создать следующие разделы – /, /boot, /home, /var, /tmp, swap (см. подпункт 3.2.3.6.2.1). Раздел подкачки swap не является обязательным, но при ограниченном количестве оперативной памяти его использование настоятельно рекомендуется. Дополнительно администратор установки может создать другие разделы по своему усмотрению.

Для создания раздела диска необходимо создать точку монтирования (автоматически или вручную) и настроить параметры раздела (тип устройства, тип файловой системы раздела).

Если переключатель “Конфигурация устройств хранения данных” был установлен в положение “Своя конфигурация” на экране появится интерфейс создания разделов диска.

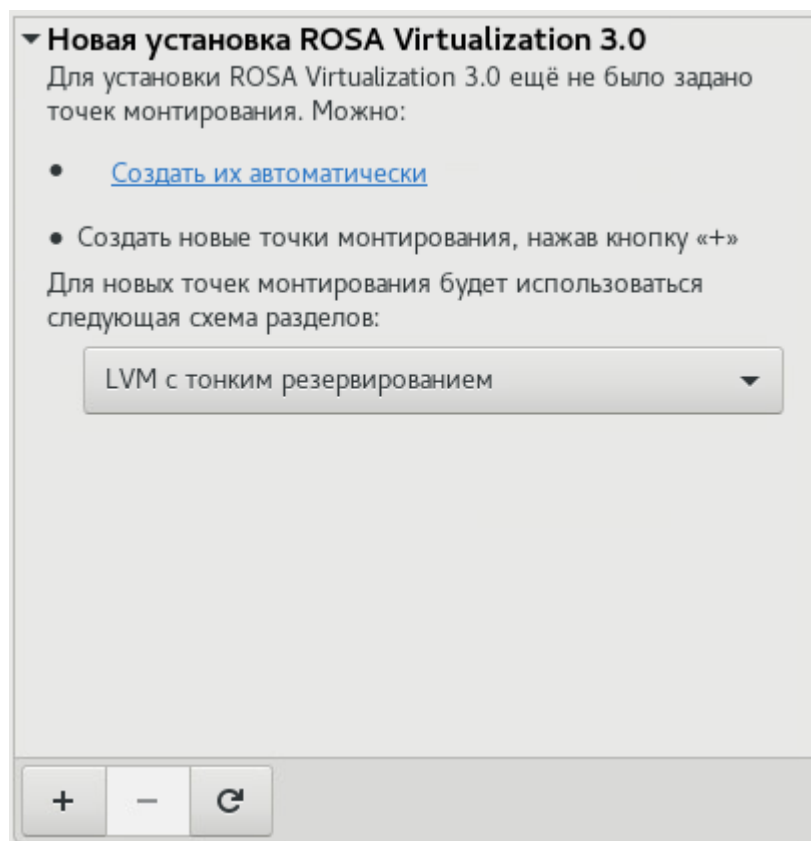


Рисунок 9 - Создание разделов

Примечание – При наличии существующих разделов убедитесь, что на диске достаточно места для установки гипервизора (значение свободного дискового пространства приведено в нижней части окна интерфейса). При необходимости в освобождении дискового пространства удалите ненужные разделы. Для удаления выбранного раздела нажмите кнопку .

АВТОМАТИЧЕСКОЕ СОЗДАНИЕ РАЗДЕЛОВ И ТОЧКИ МОНТИРОВАНИЯ

Для того, чтобы программа установки автоматически создала разделы и точки монтирования, выберите схему разбиения разделов

- Стандартный раздел, LVM с тонким резервированием (схема по умолчанию), LVM

из выпадающего списка и нажмите ссылку “Создать их автоматически”.

В результате будут созданы разделы `/`, `/boot`, `/home`, `/var`, `/tmp` и раздел подкачки `swp`. При этом раздел `/boot` будет создан как стандартный раздел независимо от ранее выбранного значения схемы разделов.

СОЗДАНИЕ ТОЧКИ МОНТИРОВАНИЯ ВРУЧНУЮ

Для создания точки монтирования вручную нажмите кнопку **+**. На экране появится модальное окно “Добавить новую точку монтирования” (Рисунок 10).

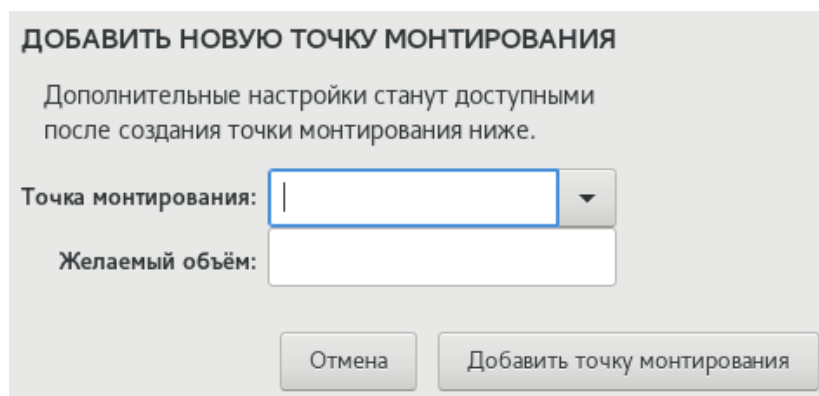


Рисунок 10 - Создание точки монтирования

Выберите раздел для подключения точки монтирования из выпадающего списка в поле Точка монтирования (Рисунок 10) или введите путь к необходимому разделу вручную. Например, `/` для корневого раздела, `/boot` для загрузочного раздела.

Укажите размер раздела в мегабайтах, гигабайтах или терабайтах в поле Желаемый объём. Например, 20 ГБ. Если размер не задан или превышает допустимый, будет занято все доступное дисковое пространство.

Нажмите кнопку **Добавить точку монтирования** (Рисунок 10).

После создания точки монтирования станут доступными (в правой области интерфейса) настройки параметров раздела (Рисунок 11).

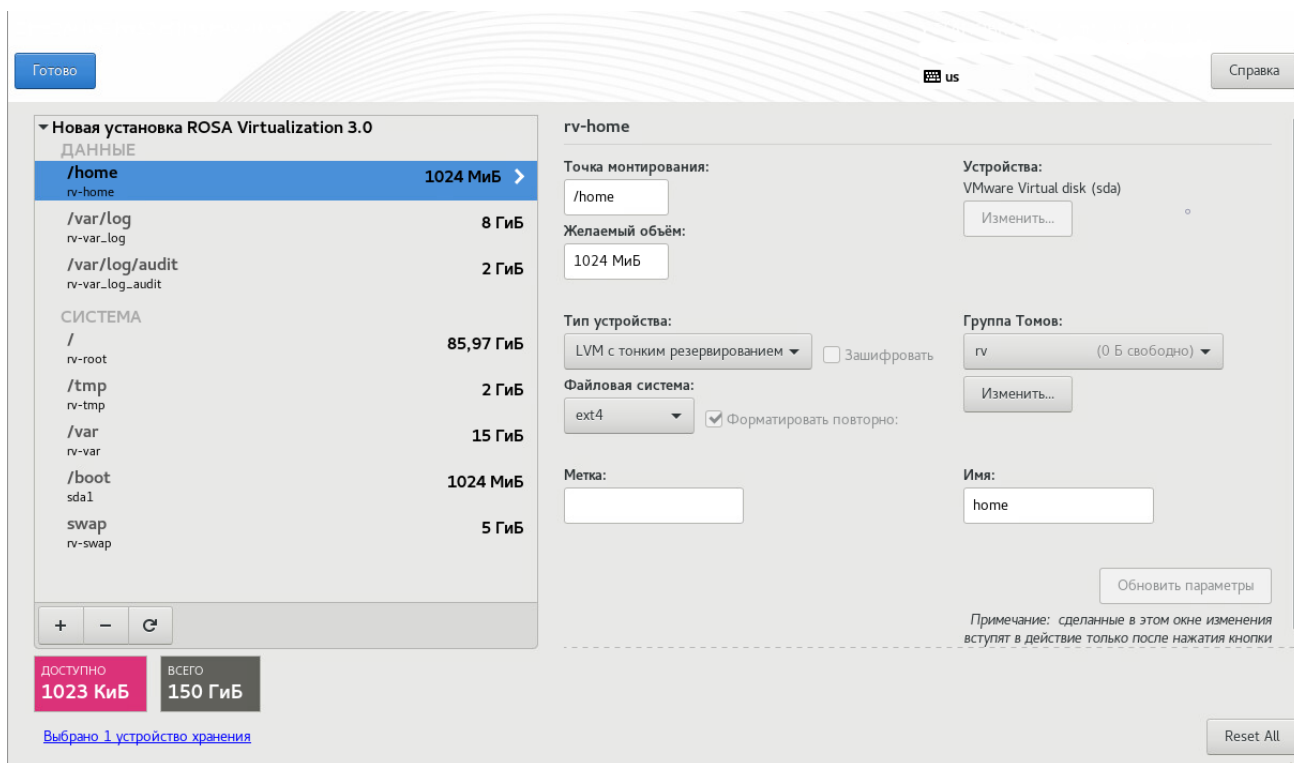


Рисунок 11 - Настройки параметров раздела

Для выбранного раздела доступны следующие параметры настройки:

- Точка монтирования – точка подключения раздела. Например, для корневого раздела введите /, для загрузочного раздела введите /boot, для раздела подкачки указывать точку не нужно, достаточно лишь ввести тип swap;
- Желаемый объём – размер раздела в килобайтах, мегабайтах, гигабайтах или терабайтах. Если единицы не указаны, будут использоваться килобайты;
- Тип устройства – тип раздела. Параметр может принимать следующие значения: Стандартный раздел, LVM, LVM с тонким резервированием (см. подпункт 3.2.3.6.2.2). При наличии двух и более дисков, выбранных для установки гипервизора, также будет доступно значение RAID;
- Файловая система – тип файловой системы. Параметр может принимать следующие значения: XFS, ext4, ext3, ext2, VFAT, swap, biosboot (см. подпункт 3.2.3.6.2.5). Справа от поля расположен флажок для форматирования;
- Метка – уникальная метка раздела;
- Имя – имя тома LVM. Имена стандартных разделов присваиваются автоматически и не меняются. Например, разделу /home может быть присвоено имя sda1.

При необходимости внесите изменения в значения параметров.

Для сохранения изменений нажмите кнопку **Обновить параметры** (Рисунок 11). При этом изменения вступят в силу только после начала установки.

Для завершения настройки нажмите кнопку **Готово** (Рисунок 11).

На экране появится модальное окно “Сводка изменений” (Рисунок 12), где будут перечислены выбранные операции по настройке разделов и файловых систем, включающие создание, изменение размера и удаление.

СВОДКА ИЗМЕНЕНИЙ				
Новые настройки приведут к следующим изменениям, которые вступят в силу после возврата в главное меню и начала установки:				
Порядок	Действие	Тип	Устройство	Точка монтирования
1	удалить форматирование	Unknown	ATA VBOX HARDDISK (sda)	
2	создать форматирование	таблица разделов (MSDOS)	ATA VBOX HARDDISK (sda)	
3	создать устройство	partition	sda1 в ATA VBOX HARDDISK	
4	создать устройство	partition	sda2 в ATA VBOX HARDDISK	
5	создать форматирование	physical volume (LVM)	sda2 в ATA VBOX HARDDISK	
6	создать устройство	lvmvg	rv	
7	создать устройство	lvmthinpool	rv-pool00	
8	создать устройство	lvmthinlv	rv-root	
9	создать форматирование	ext4	rv-root	/
10	создать устройство	lvmthinlv	rv-home	
11	создать форматирование	ext4	rv-home	/home
			Отменить и вернуться к собственной схеме разбиения	
			Принять изменения	

Рисунок 12 - Сводка изменений

Нажмите кнопку **Принять изменения**.

Для отмены изменений нажмите кнопку **Отменить и вернуться к собственной схеме разбиения**.

Для того, чтобы настроить разделы вручную на другом диске, выберите необходимый диск в окне интерфейса секции “Целевое устройство установки” и установите переключатель “Конфигурация устройств хранения данных” в положение “Своя конфигурация”.

3.2.3.6.2.1. ОБЩАЯ СХЕМА РАЗБИЕНИЯ ДИСКА НА РАЗДЕЛЫ

В общем случае при настройке пользовательской конфигурации диска рекомендуется создать следующие разделы:

- корневой раздел файловой системы / (рекомендуемый размер – не менее 10 ГБ);
- загрузочный раздел /boot (рекомендуемый размер – не менее 1 ГБ);
- раздел домашнего каталога /home (рекомендуемый размер – не менее 1 ГБ);
- раздел каталога приложений /var (рекомендуемый размер – не менее 25 ГБ);
- раздел каталога временных файлов /tmp (рекомендуемый размер – не менее 2 ГБ);
- раздел подкачки swap (рекомендуемый размер – не менее 3 ГБ).

Примечания

1. В системах с **BIOS**, использующих таблицу GPT, необходимо создать стандартный раздел biosboot размером 1 МБ, в то время как при наличии на диске области MBR в этом нет необходимости.
2. В системах с **UEFI** необходимо создать стандартный раздел /boot/efi размером не менее 50 МБ (рекомендуемый размер – 200 МБ).
3. Некоторые BIOS не поддерживают загрузку с RAID-контроллеров. В таких случаях раздел /boot следует создать на отдельном диске за пределами RAID-массива.

3.2.3.6.2.2. ТИПЫ РАЗДЕЛОВ

При настройке пользовательской конфигурации диска поддерживается создание разделов следующих типов:

- Стандартный раздел – раздел может содержать файловую систему или пространство подкачки, а также выступать в качестве основы для программного RAID-массива или физического тома LVM;
- LVM – раздел оптимизирует работу жестких дисков. При создании раздела логический том LVM будет создан автоматически;
- LVM с тонким резервированием – раздел перераспределяет свободное пространство между устройствами в зависимости от требований приложений. По мере необходимости пул пространства может наращиваться динамически (см. подпункт 3.2.3.6.2.3);
- RAID – каждому диску выделяется один RAID-раздел. При наличии двух и более дисков, выбранных для установки гипервизора, появится возможность создать программный RAID-массив (см. подпункт 3.2.3.6.2.4).

3.2.3.6.2.3. СОЗДАНИЕ ГРУППЫ ТОМОВ LVM

LVM распределяет пространство между динамически изменяемыми томами. Разделы физического диска представлены в качестве физических томов, которые могут быть объединены в группы. В свою очередь, группы томов могут подразделяться на логические тома, которые по принципу работы аналогичны стандартным дисковым разделам. Таким образом, логические тома LVM функционируют как разделы, которые могут располагаться на нескольких физических дисках.

Группа томов LVM создается через интерфейс настройки параметров раздела. Из выпадающего списка “Тип устройства” выберите значение “LVM с тонким резервированием”. В результате появится список “Группа Томов” с именем созданной группы томов LVM.

Для настройки созданной группы томов LVM нажмите кнопку **Изменить**. На экране появится модальное окно “Настройка группы томов” (Рисунок 13).

НАСТРОЙКА ГРУППА ТОМОВ

Укажите имя для группа томов и выберите ниже как минимум один диск.

Имя:

Описание	Имя
ATA VBOX HARDDISK (VBOX_HARDDISK_VBf69f8e6c-2eb766d9)	sda

☐ Зашифровать

Уровень RAID:

Политика размера:

Рисунок 13 - Настройка группы томов LVM

Введите имя для группы томов LVM и выберите диск / диски для размещения раздела.

При необходимости создайте программный RAID-массив для группы томов LVM (см. подпункт 3.2.3.6.2.4). Из выпадающего списка “Уровень RAID” выберите одно из следующих значений:

- RAID-0 (производительность);
- RAID-1 (избыточность);
- RAID-4 (проверка ошибок);
- RAID-5 (распределенная проверка ошибок);
- RAID-6 (проверка ошибок с избыточностью);
- RAID-10 (производительность, избыточность).

Примечание – Для шифрования раздела группы томов LVM установите флажок “Зашифровать”.

Определите размер группы томов LVM. Из выпадающего списка “Политика размера” выберите одно из следующих значений:

- Автоматически – размер группы томов будет определен с учетом заданных параметров. Вариант является оптимальным, если не требуется оставлять свободное пространство в пределах группы томов;
- Как можно больше – выделяется максимально возможный размер независимо от конфигурации. Вариант подходит для хранения данных в LVM с возможной перспективой добавления новых или наращивания существующих томов;

- Фиксированный – точный размер группы томов устанавливается вручную. Введите в поле необходимое значение размера группы томов.

Нажмите кнопку **Сохранить**.

Если для создания RAID-массива не хватает дисков, в нижней части окна появится сообщение с рекомендуемым количеством.

Примечание – Загрузочный раздел /boot не может располагаться в пределах логического тома LVM.

3.2.3.6.2.4. СОЗДАНИЕ ПРОГРАММНОГО RAID-МАССИВА

RAID-массивы объединяют несколько устройств хранения для обеспечения должного уровня производительности и отказоустойчивости.

RAID-массив создается один раз, после чего состав RAID-массива можно корректировать посредством добавления или исключения дисков.

На каждом диске может быть создан один RAID-раздел. Таким образом, максимальный уровень RAID определяется количеством дисков.

При наличии двух и более дисков, выбранных для установки гипервизора, появится возможность создать программный RAID-массив через интерфейс настройки параметров раздела. Из выпадающего списка “Тип устройства” выберите значение “RAID”. В результате появится список “Уровень RAID” для выбора одного из следующих значений:

- RAID-0 (производительность) – данные распределяются между несколькими дисками. RAID-0 обеспечивает высокий уровень производительности за счет объединения дисков в одно виртуальное устройство. Надежность RAID-0 невысокая, так как отказ одного диска приведет к сбою всего массива. Для создания RAID-0 необходимо как минимум два раздела RAID;

- RAID-1 (избыточность) – использует зеркалирование за счет копирования данных на все диски в составе массива. Дополнительные устройства повышают уровень избыточности. Для создания RAID-1 необходимо как минимум два раздела RAID;

- RAID-4 (проверка ошибок) – данные распределяются между несколькими дисками, но при этом один диск служит для хранения информации о четности, что помогает восстановить данные в случае сбоя. Недостаток такой организации заключается в том, что информация о четности хранится на одном диске, что представляет риск для общей производительности массива. Для создания RAID-4 необходимо как минимум три раздела RAID;

- RAID-5 (распределенная проверка ошибок) – контрольные суммы и данные циклически распределяются между элементами массива. RAID-5 более востребован по сравнению с RAID-4 благодаря параллельной обработке данных. Для создания RAID-5 необходимо как минимум три раздела RAID;

- RAID-6 (проверка ошибок с избыточностью) – аналогичен RAID-5, но контрольные данные копируются на два устройства. Для создания RAID-6 необходимо как минимум четыре раздела RAID (два раздела для основных данных и два раздела для контрольных данных);

- RAID-10 (производительность, избыточность) – данные распределяются между зеркальными наборами дисков. RAID-10 из четырех разделов будет включать две зеркальные пары RAID-1. При этом данные последовательно распределяются между парами аналогично RAID-0. Для создания RAID-10 необходимо как минимум четыре раздела RAID.

Для сохранения изменений нажмите кнопку **Обновить параметры**.

Если для создания RAID-массива не хватает дисков, в нижней части окна появится сообщение с рекомендуемым количеством.

3.2.3.6.2.5. ТИПЫ ФАЙЛОВЫХ СИСТЕМ

При настройке пользовательской конфигурации диска поддерживается создание файловых систем следующих типов:

- XFS – высокопроизводительная масштабируемая файловая система, размер которой может достигать 16 эксабайт (16 миллионов терабайт). XFS поддерживает файлы размером до 8 эксабайт (8 миллионов терабайт) и структуры каталогов с десятками миллионов записей и включает функции журналирования метаданных, что гарантирует быстрое восстановление в случае сбоя, а также поддерживает дефрагментацию и изменение размера без необходимости отключения файловой системы. Максимально допустимый объем файловой системы XFS составляет 500 ТБ;
- ext4 – файловая система, созданная на основе ext3. Преимуществами ext4 являются поддержка больших файловых систем и файлов, быстрое и эффективное распределение пространства, отсутствие ограничений на число подкаталогов в одном каталоге, быстрая проверка файловой системы и надежное ведение журналов. Максимально допустимый объем файловой системы ext4 составляет 50 ТБ;
- ext3 – файловая система, созданная на основе ext2. Главным преимуществом ext3 является поддержка журналов, что сокращает время восстановления файловой системы благодаря отсутствию необходимости в проверке с использованием утилиты fsck;
- ext2 – файловая система поддерживает стандартные типы файлов Unix (обычные файлы, каталоги, символичные ссылки) и позволяет присваивать им имена длиной до 255 знаков;
- VFAT – файловая система Linux, совместимая с FAT и поддерживающая длинные имена файлов ОС семейства Windows;
- swap – раздел подкачки для организации виртуальной памяти. Если в ОЗУ не хватает места для обработки данных, неактивные фрагменты перемещаются в область подкачки, освобождая место для новых страниц;
- biosboot – небольшой стандартный раздел для загрузки систем на базе BIOS с дисков с таблицей разделов GPT.

Примечание – При работе с файлами большого размера (например, диски виртуальных машин) рекомендуется использовать файловую систему XFS.

3.2.3.6.3. ШИФРОВАНИЕ РАЗДЕЛОВ ДИСКА

Шифрование разделов диска позволяет защитить конфиденциальные данные от неавторизованного доступа к серверному оборудованию, но накладывает дополнительные эксплуатационные ограничения.

Для шифрования разделов диска используется механизм LUKS.

Если в секции параметров “Целевое устройство установки” был установлен флажок “Зашифровать данные”, на экране появится интерфейс создания пароля доступа к зашифрованным данным (Рисунок 14).

Примечание – Пароль доступа надо будет вводить каждый раз при загрузке ОС гипервизора, поэтому шифрование разделов диска может быть не целесообразным в промышленном режиме функционирования ROSA Virtualization, так как снижается общая производительность работы с платформой виртуализации. Также обратите внимание, что в случае

утери парольной фразы зашифрованные разделы и их данные будут недоступны, и восстановить доступ будет невозможно.

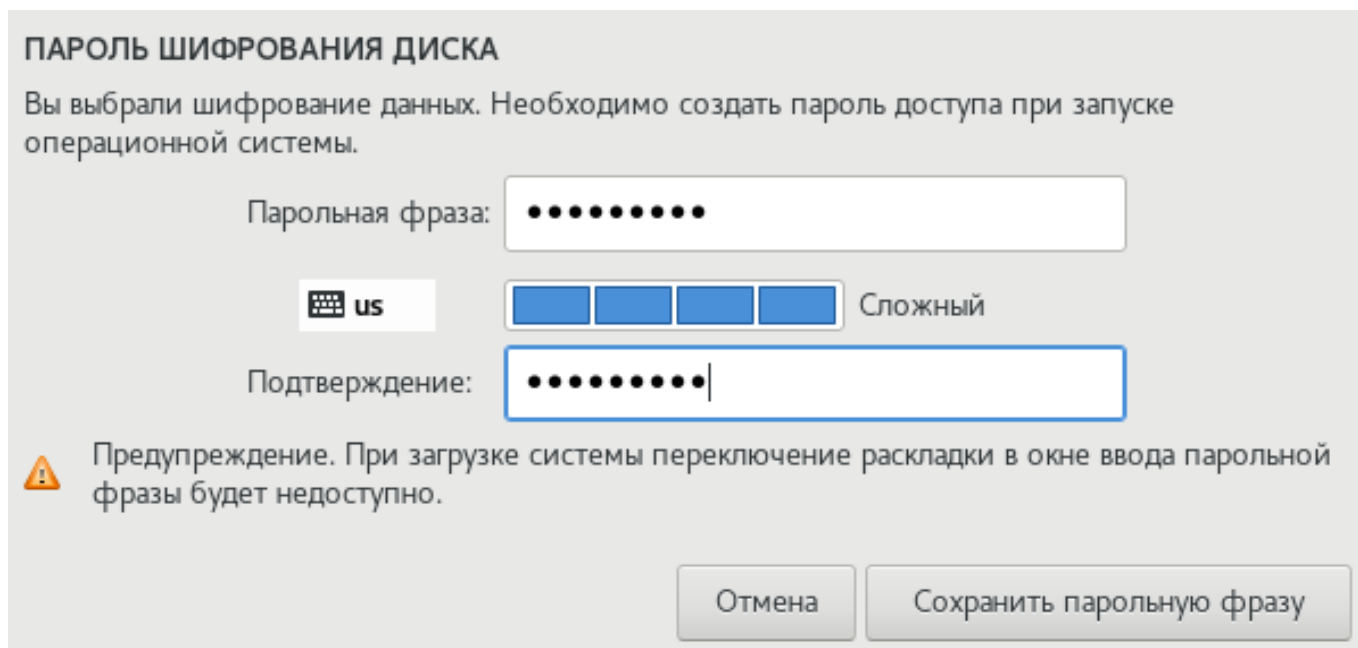


Рисунок 14 - Создание пароля доступа

В поле Парольная фраза введите парольную фразу, при этом обратите внимание на раскладку клавиатуры (Рисунок 14). Для изменения раскладки клавиатуры нажмите на значок . Если введенный пароль является слабым, на экране появится информационное сообщение с предупреждением.

В поле Подтверждение введите пароль доступа еще раз, после чего нажмите кнопку Сохранить парольную фразу.

3.2.3.6.4. ВЫБОР ДИСКА ДЛЯ УСТАНОВКИ ЗАГРУЗЧИКА

Загрузчик – первая программа, запускаемая после включения компьютера, которая передает управление ядру ОС.

ОС гипервизора использует загрузчик **GRUB2**.

При наличии двух и более дисков, выбранных для установки гипервизора, потребуется вручную определить необходимый загрузочный диск (Рисунок 15). Переход по ссылке “Полная сводка по дискам и загрузчику” откроет интерфейс выбора диска, на котором будет установлен загрузчик.

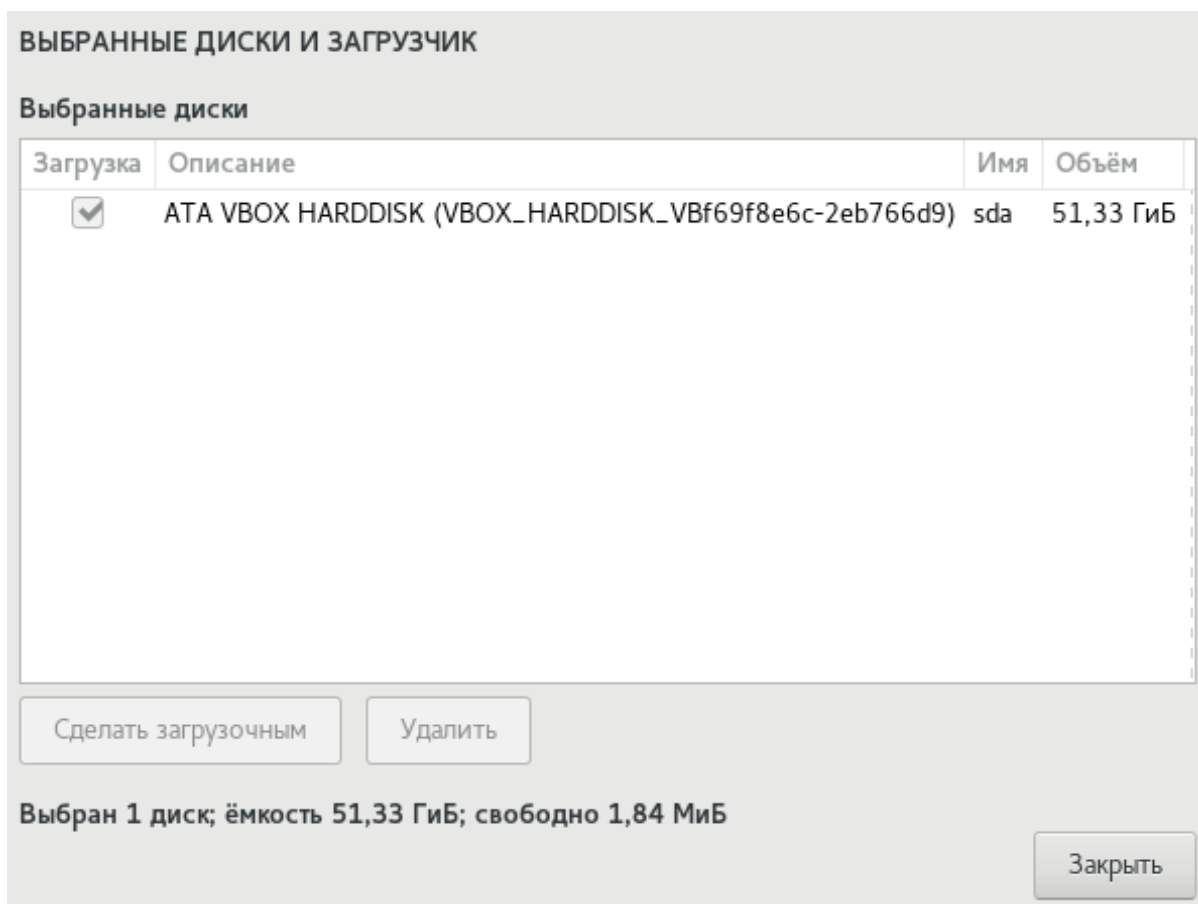


Рисунок 15 - Выбор диска для установки загрузчика

По умолчанию загрузочное устройство отмечено галочкой. Чтобы установить загрузчик на другое устройство, выберите его из списка и нажмите на кнопку **Сделать загрузочным**.

Для возвращения к интерфейсу секции “Целевое устройство установки” нажмите кнопку **Закрыть** (Рисунок 15).

По умолчанию загрузчик GRUB2 будет установлен в область MBR для диска (с корневой файловой системой) размером меньше 2 ТБ, или GPT для диска размером больше 2 ТБ.

3.2.3.7. ИМЯ ХОСТА И СЕТЕВЫЕ ПОДКЛЮЧЕНИЯ ГИПЕРВИЗОРА

Интерфейс секции “Сеть и имя хоста” предназначен для указания имени хоста и настройки параметров сетевых адаптеров гипервизора.

Примечание – Задание имени хоста является обязательным для проведения успешной установки системы.

Примечание – Для установки и начала эксплуатации ROSA Virtualization необходимо настроить как минимум один сетевой адаптер. Подключение остальных сетевых адаптеров допускается выполнить после установки гипервизора, с помощью средств администрирования.

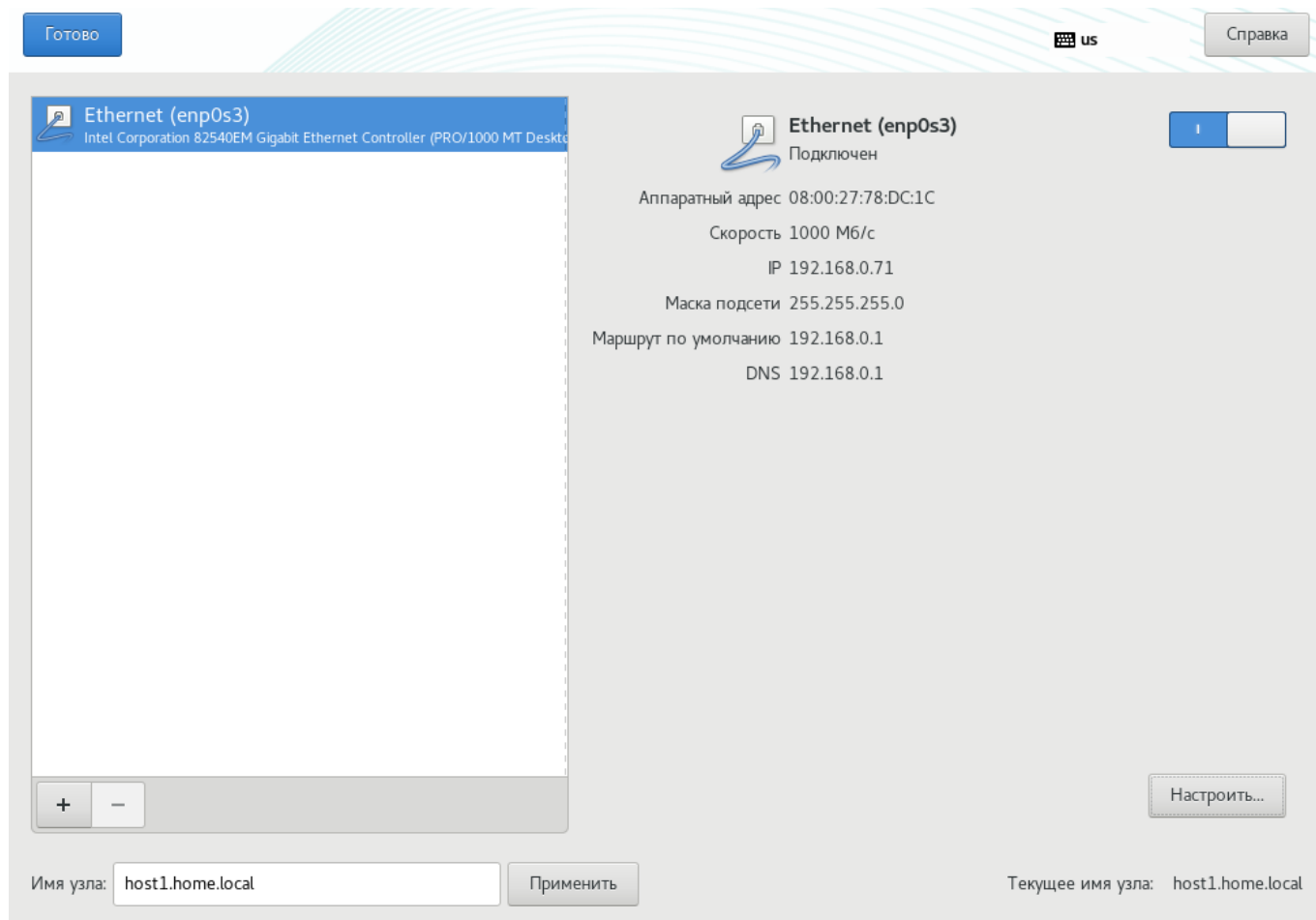


Рисунок 16 - Сетевые адаптеры и имя хоста

3.2.3.7.1. ИМЯ ХОСТА

Имя хоста гипервизора является необходимым параметром для конфигурирования системы на этапе предварительной подготовки к установке

В поле “Имя узла” введите полное доменное имя хоста гипервизора (например, `host1.home.local`) и нажмите кнопку **Применить**. Каждый хост с установленным гипервизором должен иметь уникальное имя в домене.

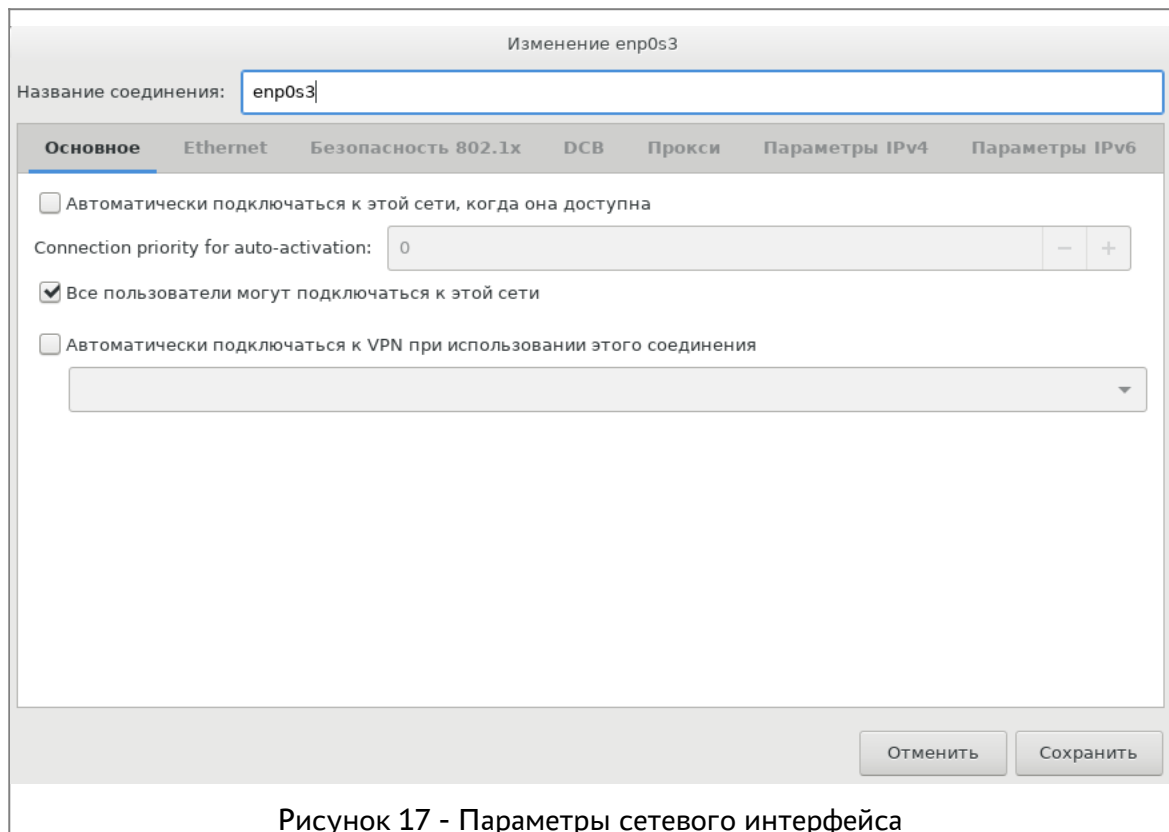
Примечание – Имя хоста гипервизора должно быть действительным именем DNS, в котором разрешается использовать только цифры, символы алфавита и дефис (-). Другие символы в имени хоста (например, нижнее подчеркивание) приведут к сбоям в работе службы DNS. Кроме того, имя хоста должно состоять только из символов в нижнем регистре, прописные буквы в имени хоста не допускаются.

3.2.3.7.2. СЕТЕВЫЕ ПОДКЛЮЧЕНИЯ

Программа установки гипервизора автоматически найдет доступные сетевые интерфейсы и отобразит их списком в левой части окна секции “Сеть и имя хоста”.

Для подключения сетевого интерфейса выберите необходимый адаптер в списке и установите переключатель в положение “I”, а для отключения – в положение “O”.

Для настройки параметров выберите необходимый сетевой интерфейс в списке и нажмите кнопку **Настроить**. На экране появится окно с параметрами интерфейса (перечень доступных параметров зависит от типа сетевого соединения).



Для автоматического подключения необходимого сетевого интерфейса в процессе загрузки ОС гипервизора установите флажок “Автоматически подключаться к этой сети, когда она доступна” во вкладке “Основное” с общими параметрами данного интерфейса.

3.2.3.7.2.1. НАСТРОЙКА ПАРАМЕТРОВ СЕТЕВОГО ПОДКЛЮЧЕНИЯ С АВТОМАТИЧЕСКИМ КОНФИГУРИРОВАНИЕМ ПО ПРОТОКОЛУ DHCP

По умолчанию сетевые параметры IPv4 и IPv6 настраиваются автоматически по протоколу DHCP.

Изменение enp0s3

Название соединения: enp0s3

Основное Ethernet Безопасность 802.1x DCB Прокси **Параметры IPv4** Параметры IPv6

Метод: Автоматический (DHCP)

Additional static addresses

Адрес	Маска сети	Шлюз

Дополнительные серверы DNS:

Дополнительные поисковые домены:

ID клиента DHCP:

☐ Требовать адресацию IPv4 для этого соединения

Маршруты...

Отменить Сохранить

Рисунок 18 - Настройка IPv4 с автоматическим конфигурированием по протоколу DHCP

Примечание – При использовании автоматической настройки сетевых параметров по протоколу DHCP необходимо наличие в сети DHCP сервера, и добавление хоста на корпоративный DNS-сервер, который используется для разрешения имен хостов в домене.

3.2.3.7.2.2. НАСТРОЙКА ПАРАМЕТРОВ СЕТЕВОГО ПОДКЛЮЧЕНИЯ С ИСПОЛЬЗОВАНИЕМ СТАТИЧЕСКОГО IP-АДРЕСА

Для настройки сетевого соединения с использованием статического IP-адреса перейдите на вкладку “Параметры IPv4” и выберите из выпадающего списка “Метод” значение “Вручную”.

Изменение enp0s3

Название соединения: enp0s3

Основное Ethernet Безопасность 802.1x DCB Прокси **Параметры IPv4** Параметры IPv6

Метод: Вручную

Адреса

Адрес	Маска сети	Шлюз
192.168.0.71	255.255.255.0	192.168.0.1

Добавить

Удалить

Серверы DNS: 192.168.0.1

Поисковый домен: home.local

ID клиента DHCP:

☒ Требовать адресацию IPv4 для этого соединения

Маршруты...

Отменить Сохранить

Рисунок 19 - Настройка параметров IPv4 вручную (статический IP адрес)

Нажмите кнопку **Добавить** и введите в соответствующие поля необходимые значения статического IP-адреса интерфейса, маски сети и шлюза.

Примечание – Перед присвоением хосту статического IP-адреса предварительно убедитесь, что данный IP адрес не используется другими хостами в сети, и не входит в диапазон IP-адресов, автоматически выделяемых DHCP сервером.

В поле “Серверы DNS” введите значение IP-адреса корпоративного и / или внешнего публичного DNS-сервера, который используется для разрешения имен хостов в домене (при необходимости укажите несколько IP-адресов DNS-серверов через запятую).

В поле “Поисковый домен” укажите наименование домена (например, home.local).

Установите флажок “Требовать адресацию IPv4 для этого соединения”.

Для применения сделанных изменений нажмите кнопку **Сохранить**.

Для добавления и настройки нового сетевого интерфейса нажмите кнопку **+** в левой нижней части окна секции “Сеть и имя хоста”.

Для удаления выбранного сетевого интерфейса из списка программы установки нажмите кнопку **-**.

После настройки сетевых параметров нажмите кнопку **Готово** для возвращения в меню “Сводка установки”.

Все работы с сетевыми интерфейсами VLAN необходимо выполнять в графическом интерфейсе СУСВ после развертывания Системы и настройки кластера. Если управляющая сеть ovirtmgmt должна быть тегированной изначально, то после установки гипервизора, но до

развертывания СУСВ, следует внести изменения в интерфейс физического сетевого устройства непосредственно на хосте, прописав в нем параметры VLAN, как указано в п. 3.2.5.

3.2.3.8. ПАРОЛЬ ДЛЯ УЧЕТНОЙ ЗАПИСИ СУПЕРПОЛЬЗОВАТЕЛЯ ROOT

Учетная запись суперпользователя `root` предназначена для администрирования ROSA Virtualization. Для учетной записи суперпользователя `root` крайне важно установить надежный пароль, чтобы исключить возможность несанкционированного доступа к ресурсам ROSA Virtualization.

При выборе и использовании пароля рекомендуется следовать следующим правилам:

- длина пароля должна быть не менее 8 символов;
- используйте для пароля не только буквы и цифры, но и спецсимволы (@, #, \$, &, *, %, ! и т.п.);
- используйте для пароля как строчные (в нижнем регистре), так и прописные (в верхнем регистре) буквы;
- не используйте для пароля общеупотребительные слова, в том числе имена собственные. Надежный пароль должен представлять собой бессмысленную комбинацию символов;
- никогда не записывайте пароль (ни на электронных, ни на бумажных носителях);
- никому не сообщайте пароль;
- запомните пароль, чтобы не забыть его.

В окне секции “Пароль `root`” введите и подтвердите пароль для учетной записи суперпользователя.

ПАРОЛЬ ROOT

УСТАНОВКА ROSA COBALI

Готово

us Справка

Учетная запись администратора (root) предназначена для управления системой. Введите пароль root.

Пароль root:

Подтверждение:

Сложный

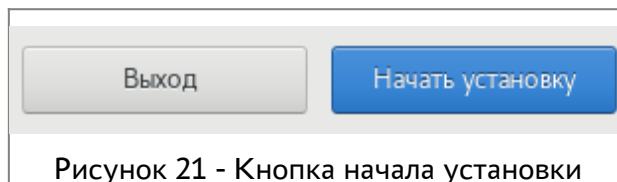
Рисунок 20 - Ввод и подтверждение пароля root

Примечание – При вводе слишком простого пароля программа установки выдаст соответствующее предупреждение, и в этом случае рекомендуется сменить пароль на более надежный.

После ввода пароля нажмите кнопку **Готово** для возвращения в меню “Сводка установки”.

3.2.4. НАЧАЛО И ХОД ПРОЦЕССА УСТАНОВКИ

Для старта процесса установки гипервизора нажмите кнопку **Начать установку**, которая станет доступной в меню “Сводка установки” после настройки обязательных параметров.



Программа установки Anaconda выделит место на выбранном диске и начнет установку гипервизора.

Ход процесса установки отображается на экране в виде индикатора прогресса.

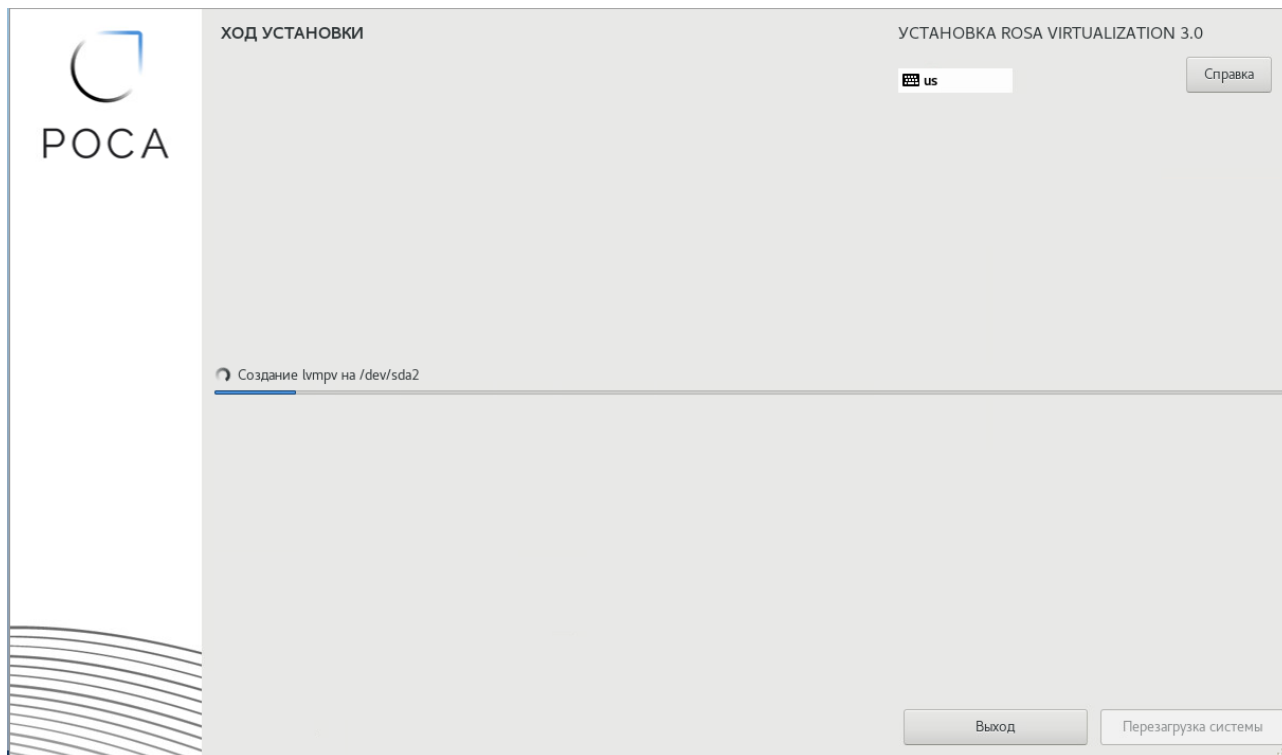


Рисунок 22 - Процесс установки

3.2.5. ЗАВЕРШЕНИЕ УСТАНОВКИ

Для завершения установки нажмите кнопку **Перезагрузка системы**, которая станет доступной после успешного окончания процесса инсталляции гипервизора.

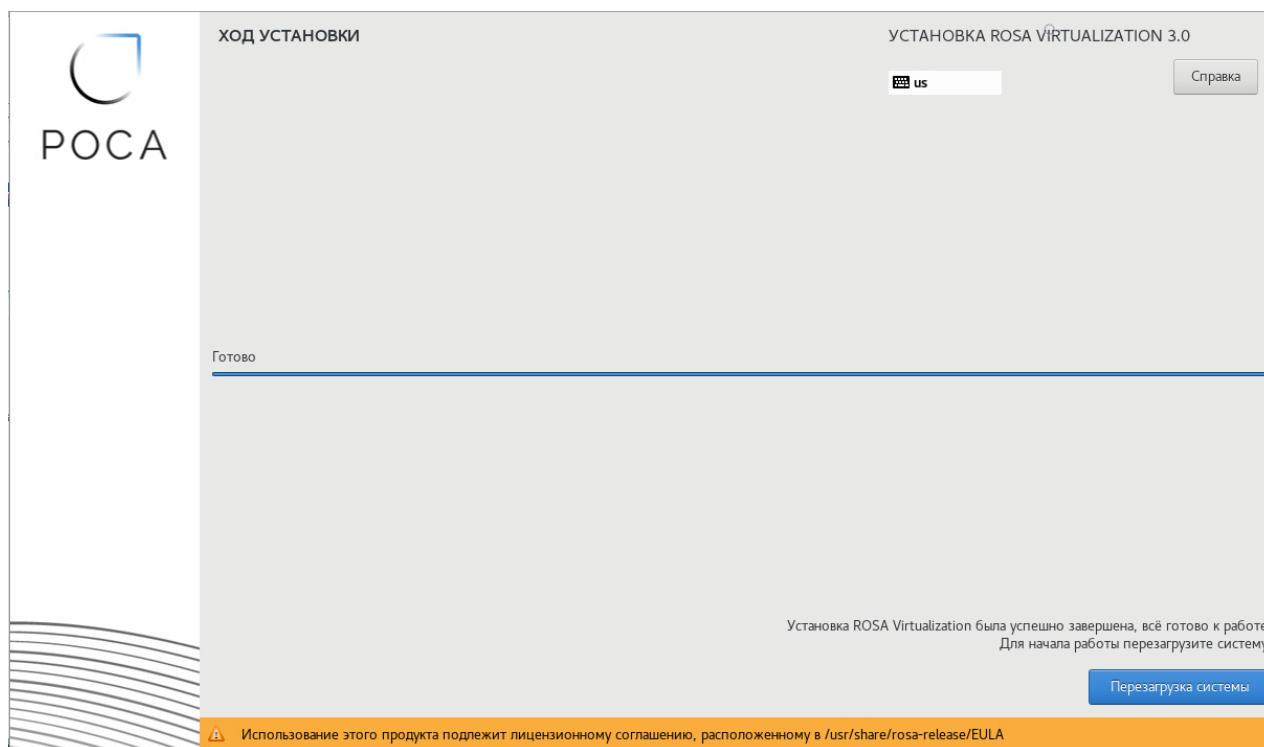


Рисунок 23 - Завершение установки

Извлеките DVD- или USB-накопитель, с которого выполнялась установка.

После перезагрузки системы, в случае если управляющая сеть `ovirtmgmt` должна быть тегированной изначально, необходимо:

- а) убедиться, что на вышестоящем коммутаторе созданы соответствующие VLAN и порт настроен для транкинга;
- б) на хосте гипервизора переименовать (в случае отсутствия — создать с нужным именем) конфигурационный файл физического интерфейса `ifcfg-physical_device` в папке `/etc/sysconfig/network-scripts/` к виду `ifcfg-physical_device.vlanID`, где:
 - `physical_device` — имя физического интерфейса;
 - `vlanID` — номер VLAN.

Например, для физического интерфейса `eth0` и VLAN ID с номером 17 новое имя файла будет таким: `/etc/sysconfig/network-scripts/ifcfg-eth0.17`.

в) настроить конфигурационный файл, для чего указать параметры:

- `ONBOOT` — загрузка интерфейса при старте системы — `"yes"`;
- `TYPE` — тип интерфейса — `"vlan"`;
- `PHYSDEV` — имя физического интерфейса;
- `VLAN` — включение интерфейса как VLAN — `"yes"`;
- `VLAN_ID` — номер VLAN;
- `VLAN_NAME_TYPE` — тип именования VLAN-интерфейса — `"VLAN_NAME_TYPE_RAW_PLUS_VID_NO_PAD"`;
- `DEVICE` — имя сабинтерфейса с указанием родительского интерфейса и VLAN ID;

- BOOTPROTO — метод загрузки (статический или DHCP) — "static";
- IPADDR — статический IP-адрес интерфейса;
- NETMASK — маска подсети;
- GATEWAY — IP-адрес шлюза;
- DNS1 — IP-адрес DNS.

Например:

```
ONBOOT=yes
TYPE=Vlan
PHYSDEV=eth0
VLAN=yes
DEVICE=eth0.17
VLAN_ID=17
VLAN_NAME_TYPE=VLAN_NAME_TYPE_RAW_PLUS_VID_NO_PAD
BOOTPROTO=static
IPADDR=192.168.0.15
NETMASK=255.255.255.0
GATEWAY=192.168.0.1
DNS1=192.168.0.2
DNS2=192.168.0.3
```

г) перезапустить службу сети, чтобы изменения вступили в силу, для чего выполнить команду:

```
systemctl restart NetworkManager.service
```

На этом установка хоста завершена, и нужно выполнить вход в веб-интерфейс администрирования хоста гипервизора для продолжения настройки и установки компонентов ROSA Virtualization.

Примечание – Для развертывания ROSA Virtualization в базовой конфигурации установите как минимум 3 гипервизора на различных хостах.

3.2.6. ВХОД В ВЕБ-ИНТЕРФЕЙС ХОСТА ГИПЕРВИЗОРА

Для доступа к веб-интерфейсу введите в адресной строке браузера (на внешней рабочей станции) доменное имя или IP-адрес хоста гипервизора с обязательным указанием порта подключения – 9090.

Например:

```
https://host1.home.local:9090
```

На экране появится окно авторизации интерфейса.

Для первичной настройки и администрирования хоста гипервизора осуществите вход в интерфейс от имени учетной записи суперпользователя `root`, используя пароль, выбранный ранее (см. секцию 3.2.3.8 Пароль для учетной записи суперпользователя `root`).

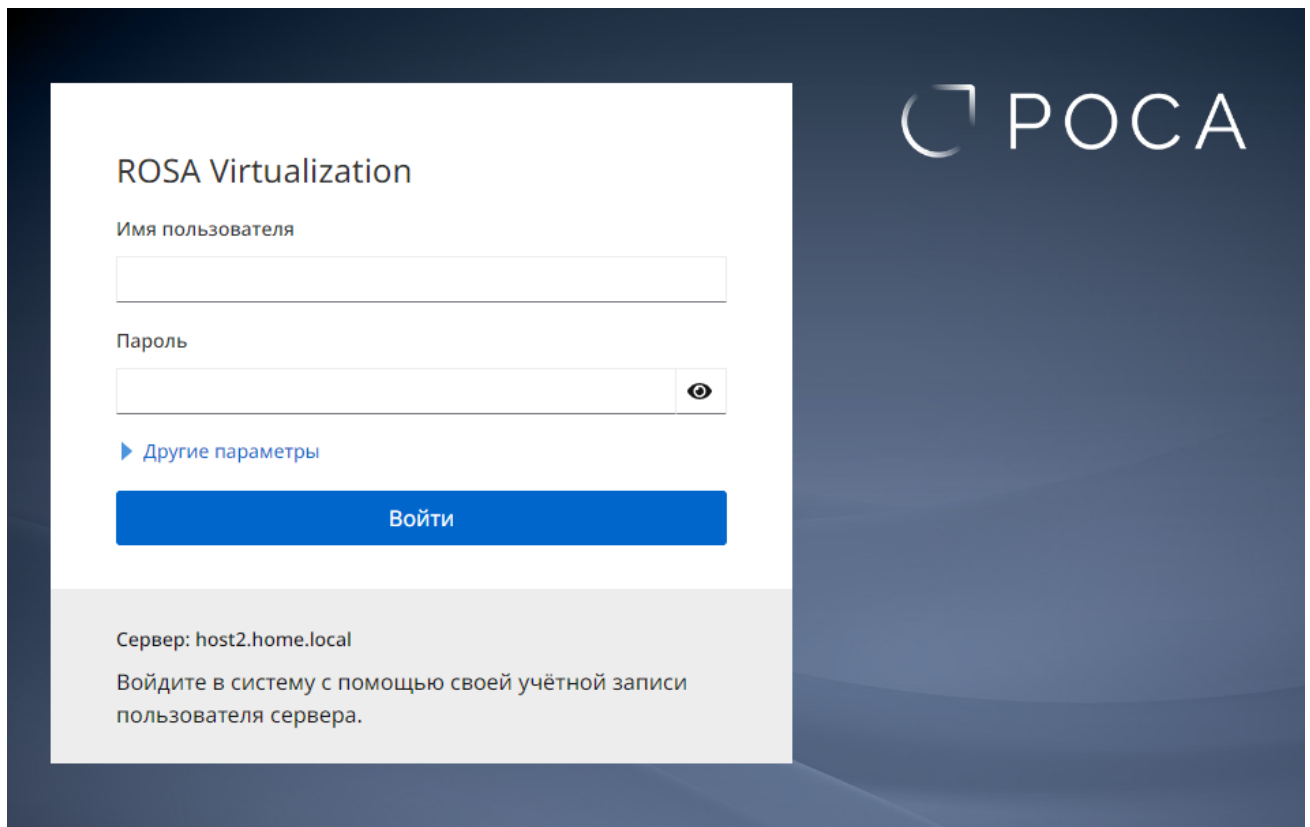


Рисунок 24 - Окно авторизации интерфейса хоста гипервизора

Для входа в интерфейс введите имя (логин) и пароль пользователя в соответствующие поля, после чего нажмите кнопку **Вход в систему**.

В случае успешной авторизации откроется страница интерфейса (вкладка “Обзор”, которая загружается по умолчанию и содержит общие сведения о хосте гипервизора.

Для перемещения по страницам интерфейса используйте необходимые вкладки панели навигации.

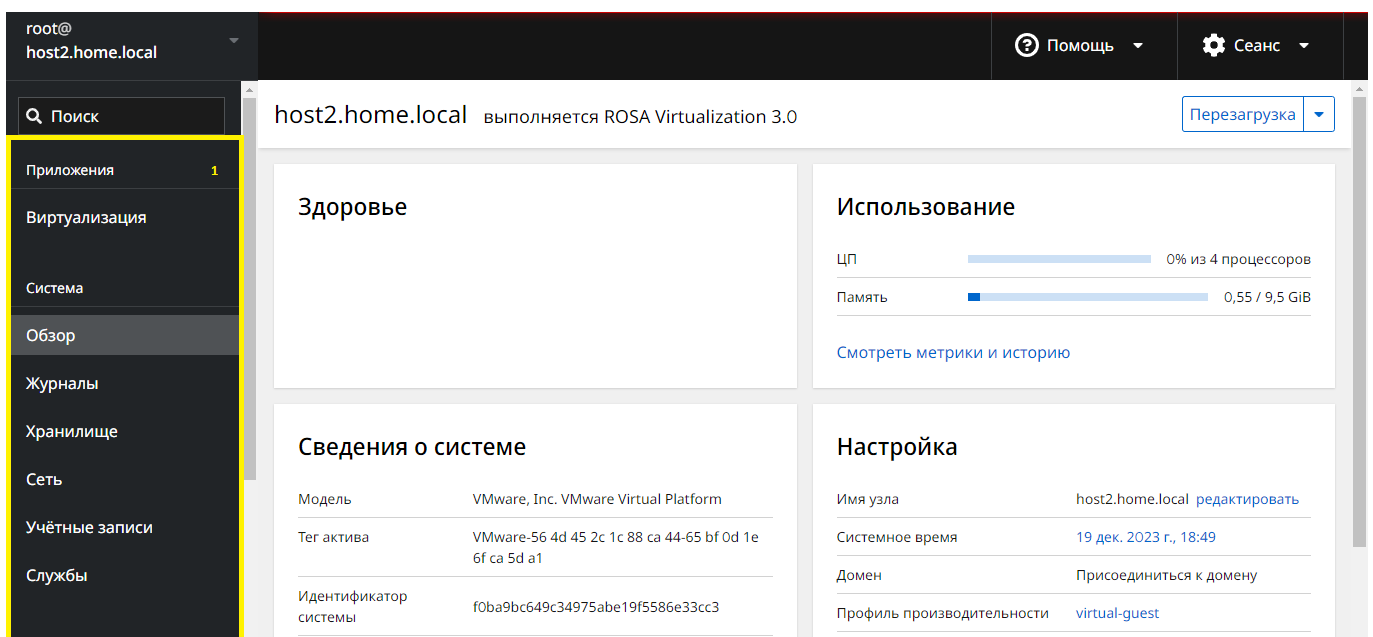


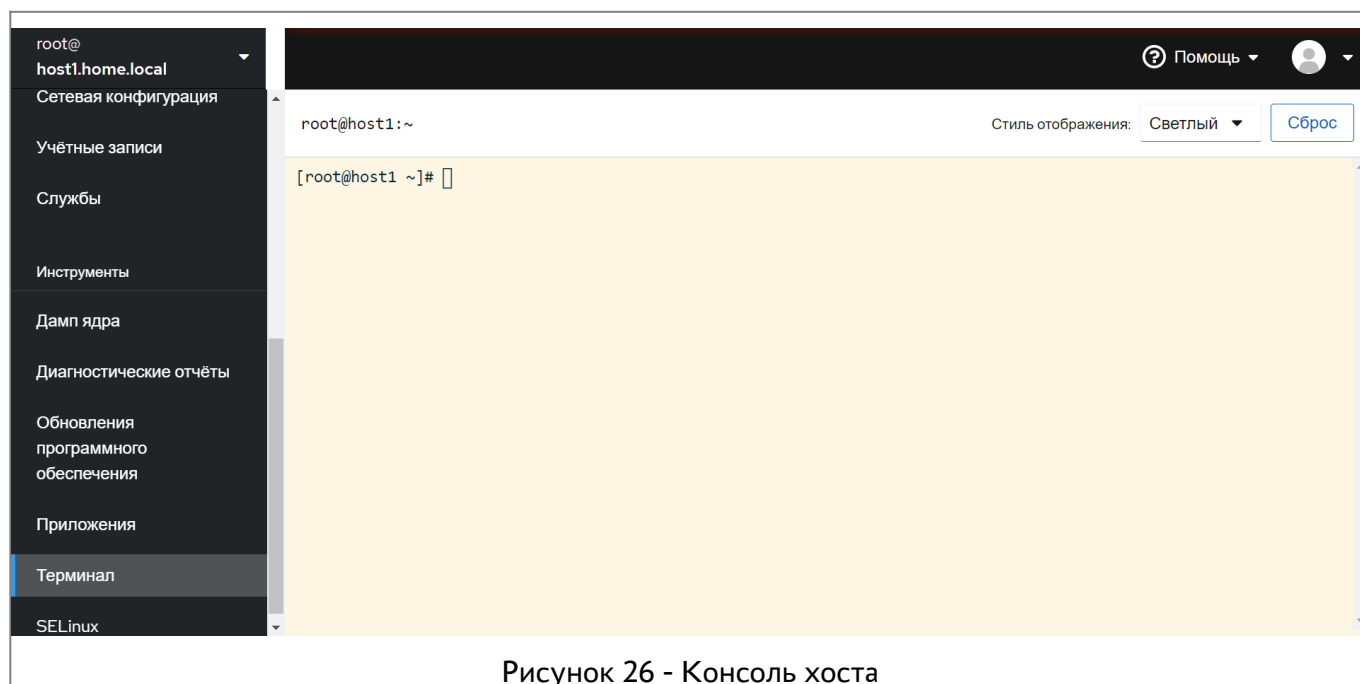
Рисунок 25 - Интерфейс хоста гипервизора (1 – Панель навигации)

3.3. НАСТРОЙКА СИСТЕМНЫХ ПАРАМЕТРОВ ХОСТА ГИПЕРВИЗОРА

Настройка параметров системного окружения осуществляется администратором в консоли *каждого из хостов* с установленным гипервизором.

ДОСТУП К КОНСОЛИ С ИСПОЛЬЗОВАНИЕМ ВЕБ-ИНТЕРФЕЙСА

Для доступа к консоли в веб-интерфейсе хоста перейдите на вкладку “Терминал” панели навигации интерфейса соответствующего хоста гипервизора.



ДОСТУП К КОНСОЛИ С ИСПОЛЬЗОВАНИЕМ SSH

Для доступа к консоли хоста можно воспользоваться SSH соединением.

Для получения доступа к консоли через SSH используйте имя учетной записи суперпользователя `root`, и пароль, выбранный ранее (см. секцию 3.2.3.8 Пароль для учетной записи суперпользователя `root`).

Выполните команду в терминале, указав имя хоста (в примере ниже — имя хоста `host1.home.local`, замените его на имя хоста, развернутого в вашем ЦОД):

```
# ssh root@host1.home.local
```

Примечание — Команды по настройке хоста, указанные в секциях ниже, могут выполняться в консоли с доступом через SSH или в терминале, открытом в браузере веб-интерфейсе администрирования хоста.

3.3.1. РАЗРЕШЕНИЕ ИМЕН DNS

При отсутствии в сети сервера DNS используйте конфигурационный файл `/etc/hosts` для настройки разрешения имен DNS в IP-адреса сетевых ресурсов. Конфигурационный файл `/etc/hosts` содержит построчный список IP-адресов и соответствующих имен DNS для их преобразования при обращении.

3.3.1.1. РЕДАКТИРОВАНИЕ ФАЙЛА /ETC/HOSTS С ИМЕНАМИ ХОСТОВ, ИСПОЛЬЗУЕМЫХ В СИСТЕМЕ

В консоли хоста откройте редактор `mc` и укажите в файле `/etc/hosts` IP-адреса и имена DNS взаимодействующих компонентов ROSA Virtualization – хостов с установленными гипервизорами, ВМ СУСВ и сервера IPA.

Для начала редактирования файла `/etc/hosts` с использованием редактора `mcedit` выполните команду в консоли:

```
# mcedit /etc/hosts
```

После завершения редактирования выйдите из редактора, сохранив результат. Для выхода из редактора можно использовать кнопку `Esc`. Если в файл были внесены изменения, то вам предложат их сохранить, или выйти без сохранения. Выберите опцию «Сохранить при выходе» - «Да» для сохранения внесенных изменений при выходе из редактора.

Примечание – Для сохранения результатов редактирования файла в редакторе `mcedit` нажмите **F2**. Для выхода из редактора нажмите **F10**. При использовании редактора в окне браузера вы можете нажать на кнопки F2 и F10, используя курсор мыши и левую клавишу мыши.

Примечание – Вы также можете использовать для редактирования любой другой текстовый редактор, например `vi`.

Для редактирования файла с использованием редактора `vi` выполните команду:

```
# vi /etc/hosts
```

Для выхода из редактора `vi` необходимо использовать команду `:q`.

Для перехода в режим редактирования в редакторе `vi` (режим INSERT) нажмите клавишу `Insert`. После внесения необходимых изменений нажмите клавишу `Esc`, затем введите команду `:x`.

Пример файла `/etc/hosts` с IP-адресами и именами DNS взаимодействующих компонентов ROSA Virtualization – хостов с установленными гипервизорами, ВМ СУСВ и сервера IPA:

192.168.0.70	vm	vm.home.local	# ВМ СУСВ
192.168.0.71	host1	host1.home.local	# хост гипервизора
192.168.0.72	host2	host2.home.local	# хост гипервизора
192.168.0.73	host3	host3.home.local	# хост гипервизора
192.168.0.74	ipa	ipa.home.local	# сервер IPA

Повторите процедуру редактирования файла `/etc/hosts` на каждом из хостов с установленным гипервизором.

Примечание – Указание в файле `/etc/hosts` IP-адресов и имен DNS взаимодействующих компонентов ROSA Virtualization позволяет обеспечить функционирование системы при недоступном корпоративном DNS сервере.

3.3.2. НАСТРОЙКА АУТЕНТИФИКАЦИИ С ПРИМЕНЕНИЕМ КРИПТОГРАФИЧЕСКИХ КЛЮЧЕЙ ВМЕСТО ПАРОЛЯ

Для использования аутентификации с применением криптографических ключей вместо пароля при взаимодействии между хостами с установленными гипервизорами создайте на каждом хосте закрытый и открытый ключи SSH, а затем скопируйте открытый ключ на другие хосты.

3.3.2.1. СОЗДАНИЕ КЛЮЧЕЙ SSH

Для создания ключей SSH выполните следующую консольную команду:

```
# ssh-keygen -t rsa
```

При создании ключей рекомендуется принимать предложенные значения параметров по умолчанию. Для этого при выводе запросов нажимайте клавишу `Enter`.

3.3.2.2. КОПИРОВАНИЕ ОТКРЫТЫХ КРИПТОГРАФИЧЕСКИХ КЛЮЧЕЙ НА ДРУГИЕ ХОСТЫ

После создания ключей скопируйте открытый ключ на другие хосты. Для этого выполняйте следующую команду последовательно указывая имена всех необходимых хостов:

```
# ssh-copy-id имя_хоста
```

3.3.2.3. НАСТРОЙКА ВЗАИМОДЕЙСТВИЯ ХОСТА С СИСТЕМОЙ ХРАНЕНИЯ ДАННЫХ

Для настройки взаимодействия хоста с системой хранения данных выполните следующие команды:

```
# cat ~/.ssh/id_rsa.pub >> ~/.ssh/authorized_keys  
# ssh -o "StrictHostKeyChecking no" root@`hostname` exit
```

Примечание – При выполнении последней команды переменная ``hostname`` будет автоматически заменена на действительное имя хоста.

Повторите процедуры создания ключей SSH, копирования открытого ключа и настройки взаимодействия по SSH с системой хранения данных на каждом из хостов с установленным гипервизором.

3.4. ПОДГОТОВКА СИСТЕМЫ ХРАНЕНИЯ ДАННЫХ

В качестве системы хранения данных ROSA Virtualization может использоваться существующий корпоративный сервер или специально развернутое хранилище одного из следующих типов:

- Gluster
- NFS

Развертывание хранилища Gluster осуществляется через веб-интерфейс хоста непосредственно в процессе гиперконвергентной инсталляции СУСВ (см. пункт 3.5.1).

Хранилище NFS должно быть подготовлено заранее перед установкой СУСВ.

3.4.1. ПОДГОТОВКА ХРАНИЛИЩА NFS

Подготовка хранилища NFS средствами ROSA Virtualization осуществляется в консоли хоста, предназначенного для установки ВМ СУСВ.

Для доступа к консоли перейдите на вкладку “Терминал” панели навигации интерфейса соответствующего хоста, или откройте консоль хоста через SSH соединение.

3.4.1.1. СОЗДАНИЕ СТРУКТУРЫ КАТАЛОГОВ ДЛЯ ХРАНИЛИЩА NFS

В разделе диска, предназначенном для хранения виртуальных машин и образов, создайте определенную структуру каталогов. Для создания каталогов используйте редактор `mc` или консольную утилиту `mkdir`.

Например, выполните следующую команду:

```
# mkdir -p /data/engine /data/vmstore /data/export /data/iso
```

Измените владельца всех созданных каталогов на служебного пользователя `vds` (`uid=36`) и соответствующую служебную группу `kvm` (`gid=36`). Для этого выполните следующую команду:

```
# chown -R 36:36 /data
```

В редакторе `mc` (запуск редактора осуществляется из командной строки терминала, командой `mcedit`) отредактируйте конфигурационный файл сервера NFS `/etc/exports` так, чтобы предоставить всем хостам в сети доступ к созданным каталогам на чтение и запись. Для этого добавьте в файл `/etc/exports` строки следующего содержания:

```
/data/engine    *(rw)
/data/vmstore   *(rw)
/data/export    *(rw)
/data/iso       *(rw)
```

3.4.1.2. НАСТРОЙКА МЕЖСЕТЕВОГО ЭКРАНА ДЛЯ РАБОТЫ С ХРАНИЛИЩЕМ NFS

Для разрешения входящих соединений к NFS через службу межсетевого экрана `firewalld` выполните следующую команду:

```
# firewall-cmd --permanent --add-service=nfs
```

Для применения изменений перезагрузите конфигурацию межсетевого экрана. Для этого выполните следующую консольную команду:

```
# firewall-cmd --reload
```

3.4.1.3. ЗАПУСК СЕРВЕРА NFS И НАСТРОЙКА АВТОМАТИЧЕСКОГО ЗАПУСКА ПРИ ЗАГРУЗКЕ СИСТЕМЫ

По умолчанию сервер NFS не запускается автоматически при загрузке системы.

Для текущего и автоматического запуска сервера NFS при загрузке системы выполните следующие команды:

```
# systemctl start nfs-server
# systemctl enable nfs-server
```

Примечание – При ранее запущенном сервере NFS для применения изменений, внесенных в конфигурацию через редактирование параметров файла `/etc/exports`, выполните следующую команду:

```
# systemctl reload nfs-server
```

Проверка работоспособности NFS сервера

Для проверки статуса NFS сервера выполните команду:

```
# systemctl status nfs-server
```

Пример выполнения команды по проверке статуса NFS сервера:

```
# systemctl status nfs-server
● nfs-server.service - NFS server and services
   Loaded: loaded (/usr/lib/systemd/system/nfs-server.service; enabled; vendor
  preset: disabled)
   Drop-In: /run/systemd/generator/nfs-server.service.d
            └─order-with-mounts.conf
   Active: active (exited) since Thu 2024-06-06 16:53:59 MSK; 1min 7s ago
   Process: 1783 ExecStart=/bin/sh -c if systemctl -q is-active gssproxy; then
systemctl reload gssproxy ; fi >
   Process: 1707 ExecStart=/usr/sbin/rpc.nfsd (code=exited, status=0/SUCCESS)
   Process: 1702 ExecStartPre=/usr/sbin/exportfs -r (code=exited,
status=0/SUCCESS)
  Main PID: 1783 (code=exited, status=0/SUCCESS)
     Tasks: 0 (limit: 48509)
    Memory: 0B
    CGroup: /system.slice/nfs-server.service

июн 06 16:53:58 vmrvhost1.rosa.lan systemd[1]: Starting NFS server and
services...
июн 06 16:53:59 vmrvhost1.rosa.lan systemd[1]: Started NFS server and services.
```

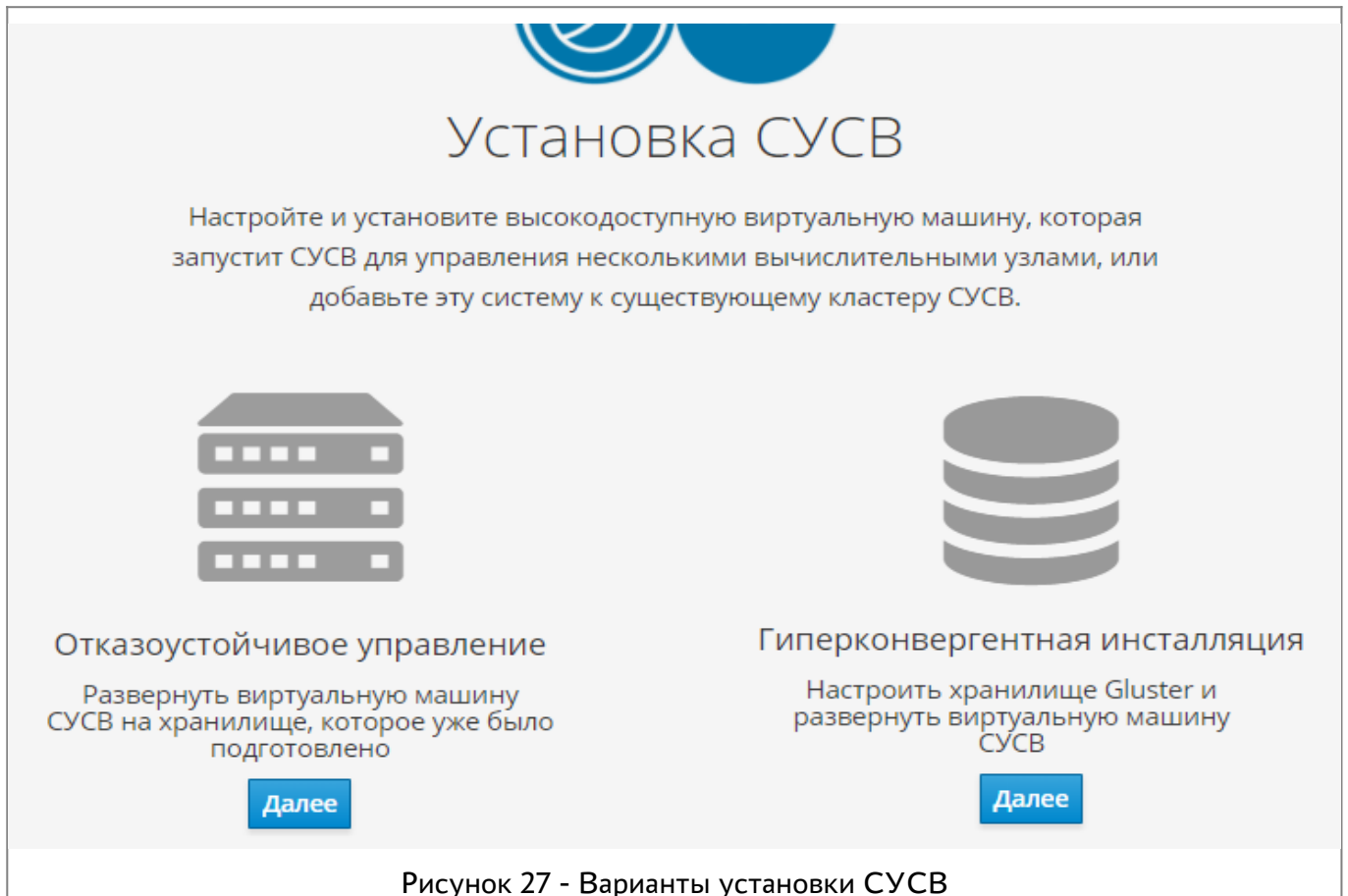
Статус Active: `active` указывает на то, что сервис активен.

3.5. УСТАНОВКА СУСВ

В общем случае установка СУСВ осуществляется через веб-интерфейс хоста (например, `host1.home.local`), на котором будет развернута соответствующая ВМ.

Для выбора одного из вариантов установки СУСВ перейдите на вкладку “Виртуализация” панели навигации интерфейса хоста. На экране появится меню “Установка СУСВ”, в котором способы развертывания СУСВ представлены в виде следующих секций:

- Отказоустойчивое управление;
- Гиперконвергентная инсталляция.



- Для установки СУСВ на заранее подготовленное хранилище нажмите кнопку **Далее** в секции “Отказоустойчивое управление”. Программа установки запустит интерактивный процесс развертывания ВМ СУСВ (см. подпункт 3.5.2).
- Для подготовки хранилища Gluster и последующей установки СУСВ в ходе единого процесса нажмите кнопку **Далее** в секции “Гиперконвергентная инсталляция”. Программа установки запустит интерактивный процесс развертывания хранилища Gluster.

3.5.1. РАЗВЕРТЫВАНИЕ ХРАНИЛИЩА GLUSTER

В окне “Конфигурация Gluster” нажмите кнопку **Запустить установщик Gluster** для перехода к настройке конфигурации хранилища (рисунок 28).

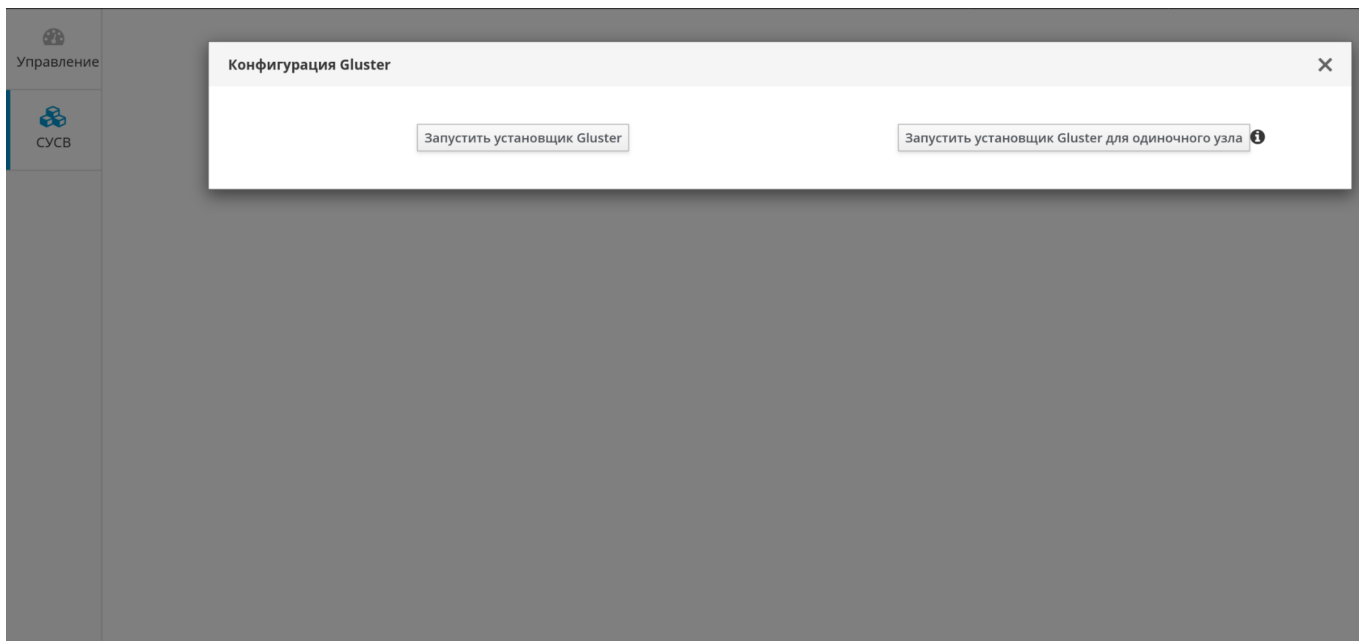


Рисунок 28 - Запуск настройки конфигурации Gluster

Примечание – Если в составе ROSA Virtualization развернут только один хост с установленным гипервизором, то нажмите кнопку **Запустить установщик Gluster для одиночного узла**. Откроется форма помощника настройки конфигурации Gluster для одиночного узла (рисунок 29).

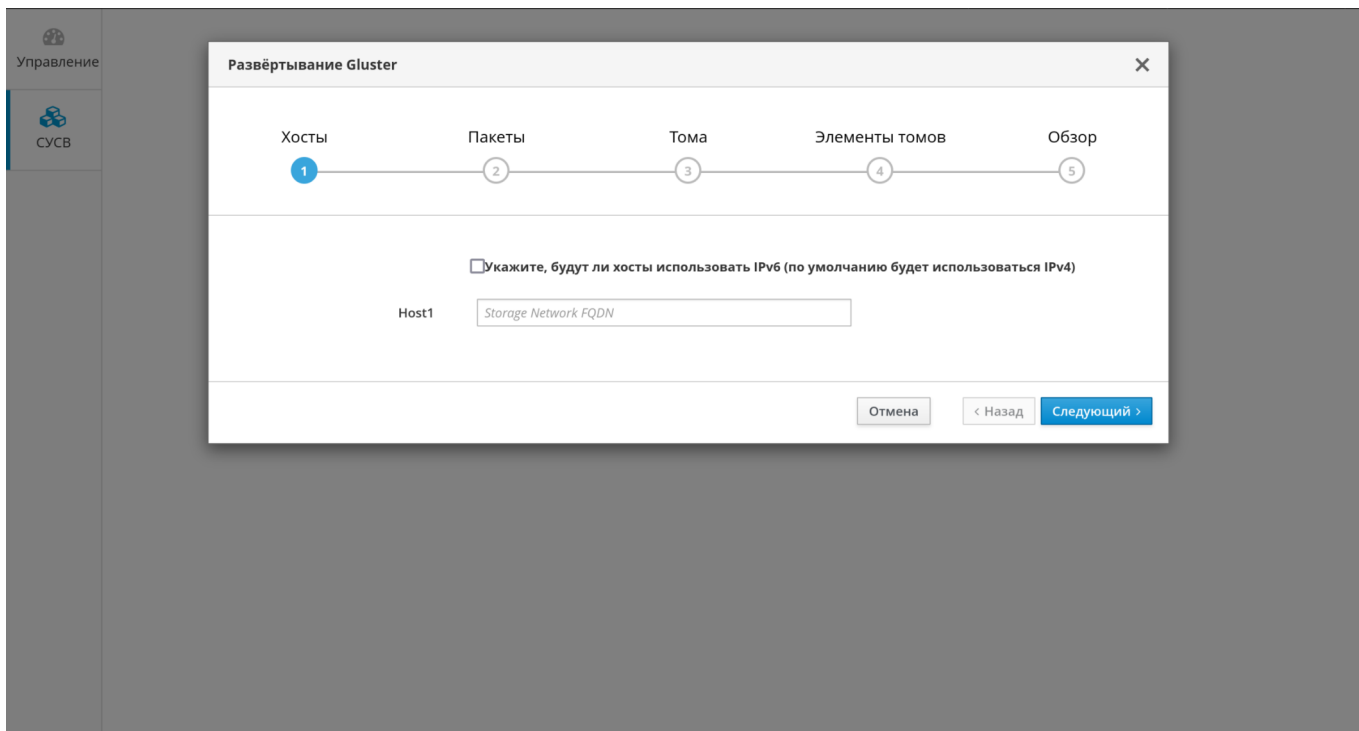


Рисунок 29 - Форма помощника настройки конфигурации Gluster для одиночного узла

Настройка конфигурации Gluster для группы из трёх хостов

На экране появится окно “Развёртывание Gluster”, в котором параметры хранилища распределены по секциям “Хосты”, “Пакеты”, “Томы”, “Элементы томов” и “Обзор” для последовательной настройки конфигурации (рисунок 30).

Развёртывание Gluster

Хосты 1 Пакеты 2 Томы 3 Элементы томов 4 Обзор 5

☒ Использовать одно и то же имя хоста как для сети хранилища, так и для общедоступной сети
☐ Укажите, будут ли хосты использовать IPv6 (по умолчанию будет использоваться IPv4)

Host1 host1.home.local
host1.home.local

Host2 host2.home.local
host2.home.local

Host3 ⓘ host3.home.local
host3.home.local

Отмена < Назад Следующий >

Рисунок 30 - Форма помощника настройки конфигурации Gluster для группы из трех хостов – секция Хосты

В секции “Хосты” введите полные доменные имена развернутых хостов ROSA Virtualization в соответствующие поля. При этом хост, указанный в поле “Host3”, будет являться управляющим сервером общего распределенного хранилища Gluster.

Если указанные имена хостов будут использоваться как для сети хранилища, так и для общедоступной сети установите соответствующий флажок, или отдельно введите имена хостов для общедоступной сети в нижней строке каждого поля.

Для продолжения настройки конфигурации хранилища нажмите кнопку **Следующий**. Для перехода к секции “Хосты” (рисунок 31).

Примечание – В случае появления сообщения об ошибке “Host is not added in known_hosts” выполните процедуру настройки взаимодействия данного хоста с системой хранения данных по SSH (см. пункт 3.3.2).

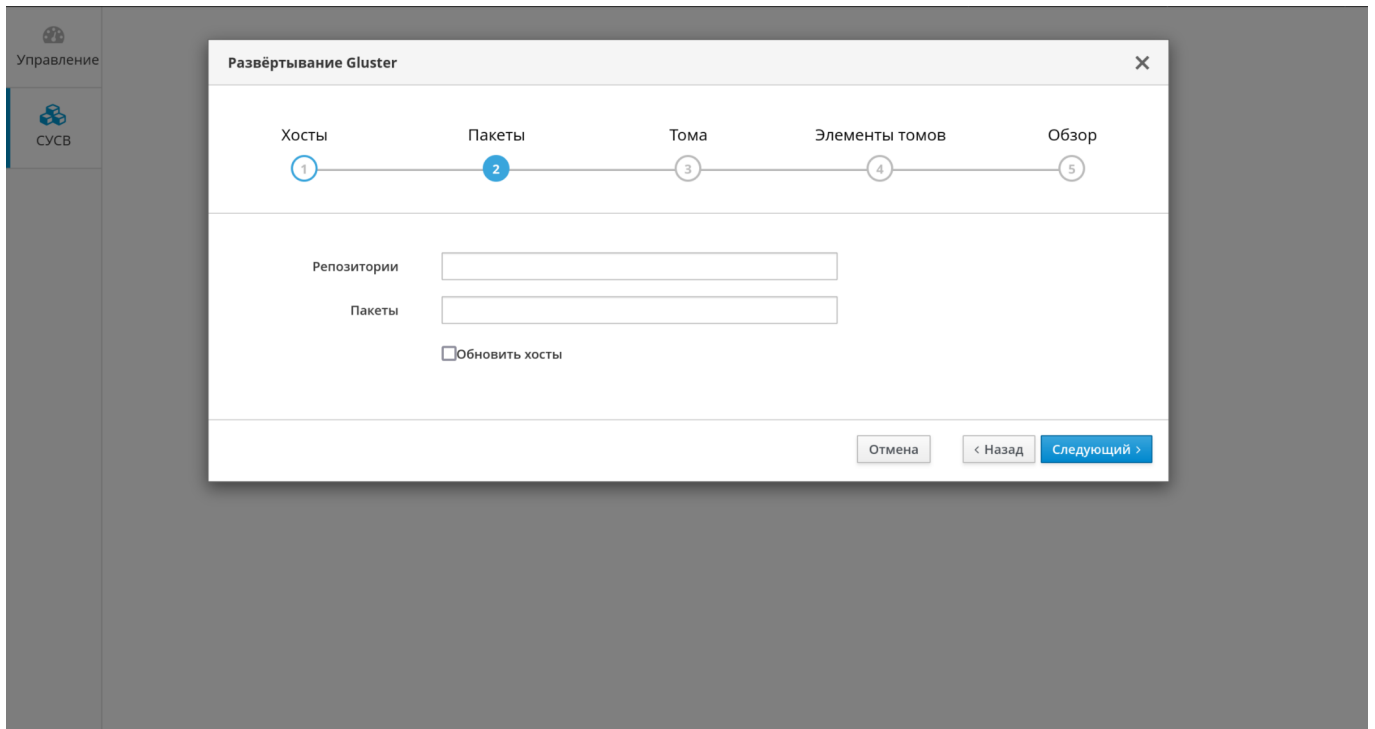


Рисунок 31 - Помощник настройки конфигурации Gluster — секция Пакеты

В секции “Пакеты” нажмите кнопку **Следующий** для продолжения настройки конфигурации хранилища и перехода к секции “Тома” (рисунок 32).

Развёртывание Gluster

Хосты

Пакеты

Томы

Элементы томов

Обзор

Имя	Тип	Арбитр	Каталоги элементов тома	
engine	Replicate	☐	/gluster_bricks/engine/engine	
data	Replicate	☐	/gluster_bricks/data/data	
vmstore	Replicate	☐	/gluster_bricks/vmstore/vmstore	

Добавить том

Первый том в списке будет использоваться для развёртывания виртуализированного ЦУ

Отмена

< Назад

Следующий >

Рисунок 32 - Параметры томов Gluster

В секции “Томы” измените имя тома data на значение iso и добавьте новый том export.

Для добавления нового тома нажмите на функциональную строку **Добавить том** и в поле “Имя” с параметрами нового тома введите значение export.

Примечание – В процессе гиперконвергентной инсталляции корректно настроенным должен быть только домен для хранения виртуальных машин, размещенный на томе vmstore. Параметры остальных томов можно будет отредактировать после завершения установки.

Нажмите кнопку **Следующий** для продолжения настройки конфигурации хранилища и перехода к секции “Элементы томов” (рисунок 33).

Развёртывание Gluster

Хосты
Пакеты
Томы
Элементы томов
Обзор

Информация о Raid

Тип Raid
JBOD

Multipath Configuration

Blacklist Gluster Devices
☒

Конфигурация элемента тома

Выберите хост
host1.home.local

LV Имя	Имя устройства	Размер логического тома (Гбайт)	Включить дедупликацию и сжатие
engine	/dev/sdb	100	☐
iso	/dev/sdb	30	☐
vmstore	/dev/sdb	100	☐
export	/dev/sdb	70	☐

☐ Настройка кэша логического тома

i

Элементы арбитра будут созданы на третьем хосте в списке хостов.

Отмена
Назад
Следующий

Рисунок 33 - Конфигурация элементов томов

В секции “Элементы томов” из выпадающего списка “Тип Raid” выберите значение JBOD, а также при необходимости отредактируйте значения конфигурации элемента для каждого тома.

В графе “Имя устройства” укажите дисковый накопитель (по умолчанию /dev/sdb), предназначенный для развертывания хранилища.

Примечание – Для получения сведений о подключенных к системе накопителях выполните консольную команду `fdisk -l`.

В графе “Размер логического тома (Гбайт)” укажите размер для каждого тома исходя из объема хранилища. При этом размер тома engine должен быть не менее **62 ГБ** свободного дискового пространства для функционирования системы управления.

Примечание – Включать дедупликацию и сжатие томов не рекомендуется.

Нажмите кнопку **Следующий** для перехода к секции “Обзор” (рисунок 34).

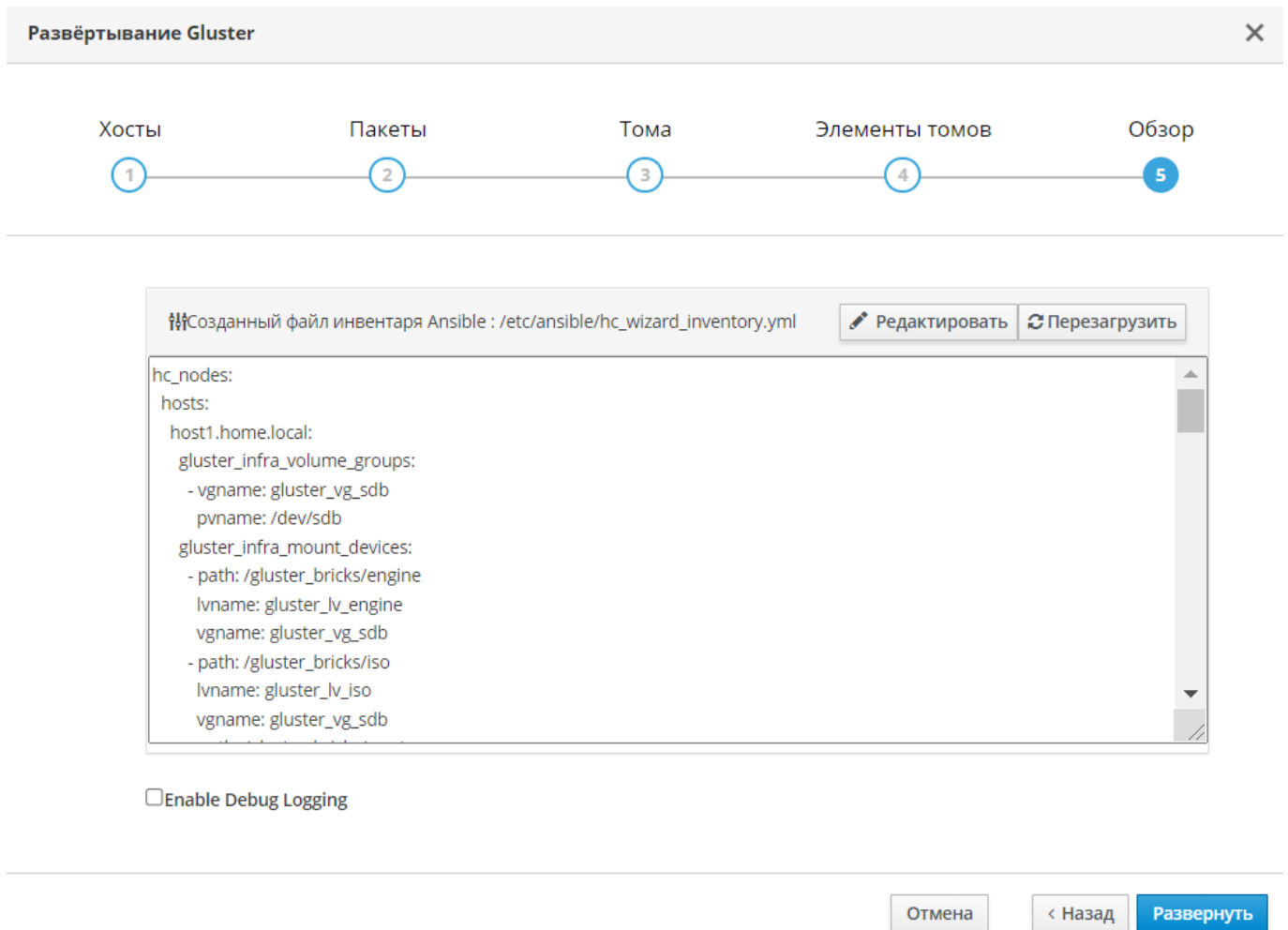


Рисунок 34 - Обзор параметров конфигурации хранилища

В секции “Обзор” нажмите кнопку **Развернуть** для подготовки и установки хранилища в соответствии с заданной конфигурацией.

Ход процесса развёртывания хранилища будет сопровождаться появлением информационных сообщений о действиях, выполненных программой установки (рисунок 35). В случае неудачной установки можно просмотреть сообщения (в том числе, сообщения об ошибках) для выявления проблемы в процессе установки.

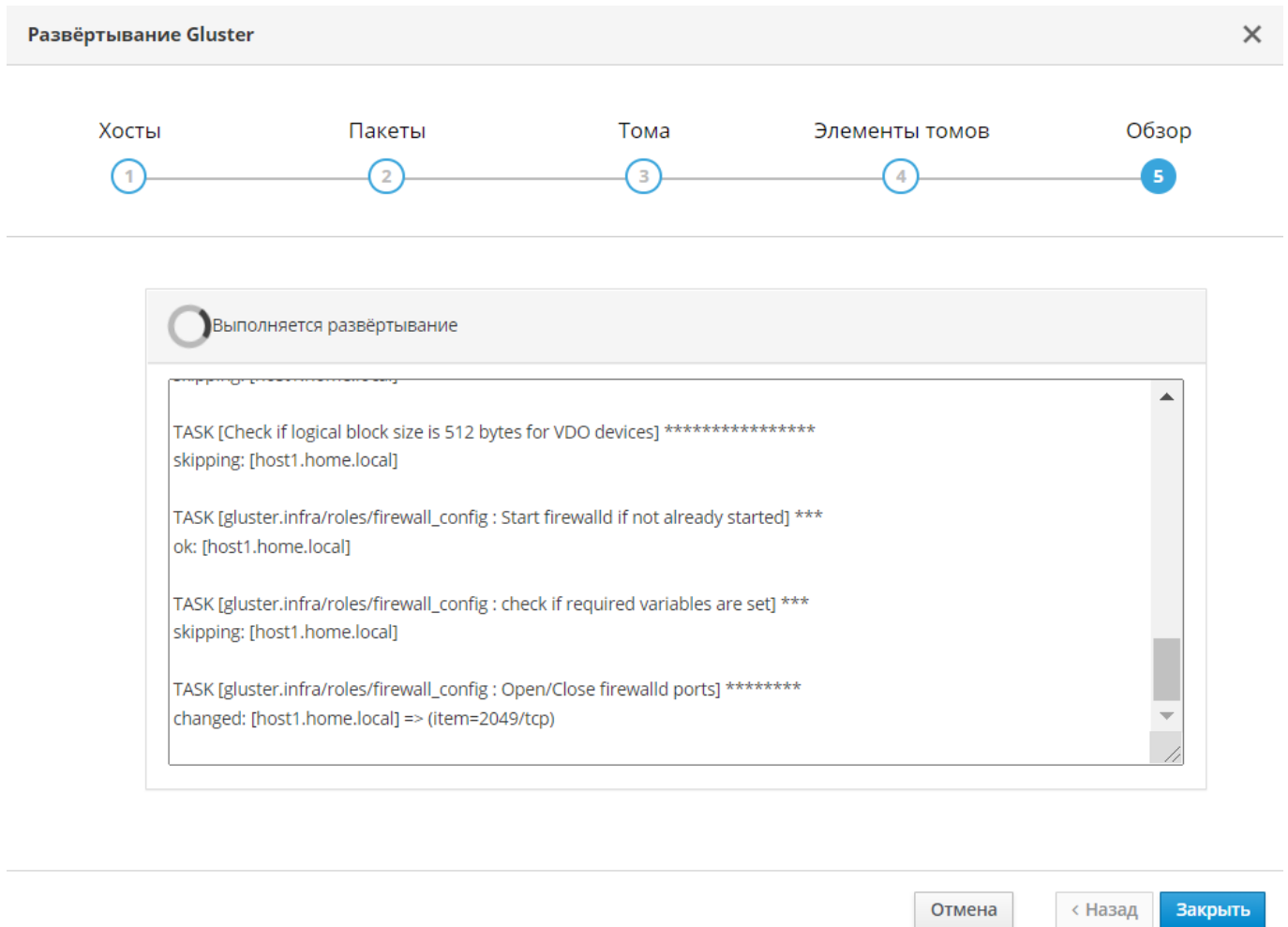


Рисунок 35 - Ход процесса развертывания хранилища

После успешного завершения процесса развертывания хранилища, на экране появится соответствующее сообщение (рисунок 36).

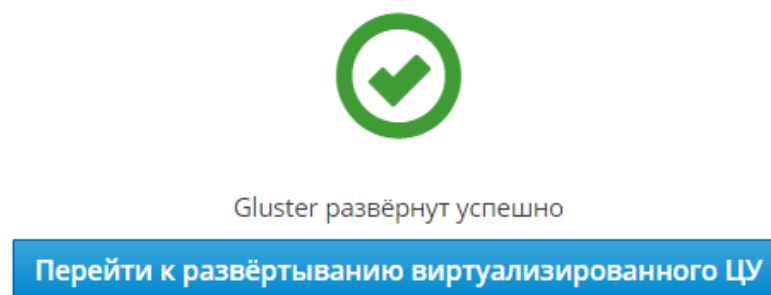


Рисунок 36 - Завершение развертывания хранилища Gluster

Для запуска интерактивного процесса установки ВМ СУСВ на развернутое хранилище Gluster нажмите кнопку Перейти к развёртыванию виртуализированного ЦУ.

3.5.2. ПРОЦЕСС УСТАНОВКИ ВИРТУАЛЬНОЙ МАШИНЫ СУСВ

Перед развертыванием СУСВ программой установки осуществляется предварительная настройка конфигурации.

На экране появится окно “Развертывание виртуализированного ЦУ”, в котором параметры СУСВ распределены по секциям “ВМ”, “ВиртЦУ”, “Подготовка ВМ”, “Хранилище” и “Завершить” для последовательной настройки конфигурации.

3.5.2.1. ЗАДАНИЕ ПАРАМЕТРОВ ВИРТУАЛЬНОЙ МАШИНЫ

Развёртывание виртуализированного ЦУ

ВМ

ВиртЦУ

Подготовка ВМ

Хранилище

Завершить

1

2

3

4

5

Параметры ВМ

Полное доменное имя ВМ виртуализированного ЦУ

vm.home.local

MAC адрес

00:16:3e:64:fd:82

Конфигурация сети

Static

IP адрес ВМ

192.168.0.70

/

24

Адрес шлюза

192.168.0.1

Серверы DNS

192.168.0.1

-

+

Интерфейс моста

ens192

Пароль root

Root SSH Access

Yes

Количество виртуальных ЦП

4

Объем памяти (МиБ)

4096

В 918Мбайт доступно

> Дополнительно

Отмена

< Назад

Следующий >

Рисунок 37 - Параметры ВМ

В секции “ВМ” задайте полное доменное имя ВМ СУСВ (например, `vm.home.local`) в соответствующем поле.

Из выпадающего списка “Конфигурация сети” выберите необходимое значение – DHCP или Static. При выборе значения Static укажите в соответствующих полях IP-адрес ВМ (например, 192.168.0.70), префикс маски подсети (24), адрес шлюза (192.168.0.1) и IP-адрес сервера DNS. Для указания дополнительного сервера DNS нажмите кнопку  и введите IP-адрес в новом поле.

В поле “Пароль root” задайте пароль для учетной записи суперпользователя root ВМ СУСВ.

При указании значения объема оперативной памяти в соответствующем поле учитывайте, что при развертывании ROSA Virtualization в стартовой конфигурации минимальный объем памяти ВМ СУСВ должен составлять не менее 4096 МБ, а при развертывании в базовой конфигурации – не менее 8192 МБ. При этом системе хоста необходимо дополнительно минимум 512 МБ памяти для функционирования гипервизора.

Примечание – Значение по умолчанию в поле “Количество виртуальных ЦП” изменять не рекомендуется.

Настройка параметров в секции Дополнительно

Нажмите на секцию «Дополнительно» для настройки (при необходимости) дополнительных параметров установки.

▼ Дополнительно

Открытый SSH ключ root	
Имя моста	ovirtmgmt
Адрес шлюза	192.168.122.1
Полное доменное имя хоста	vmrvhost1.rosa.lan 
Редактирование файла hosts	☒ 
Pause Host	☐ 
Применить профиль OpenSCAP	☐ 
Тест сети	DNS
Путь к архиву OVA	/path/to/*.ova

Отмена

< Назад

Следующий >

Рисунок 38 - Настройка дополнительных параметров

- **Открытый SSH ключ root**

Параметры открытого ключа SSH для учетной записи администратора (root)

- **Имя моста**

Имя моста, к которому будет подключен СУСВ. Изменять не рекомендуется

- **Адрес шлюза**

Адрес шлюза, используемого СУСВ

- **Полное доменное имя хоста**

Полное доменное имя хоста. Зеленая галочка рядом с именем означает, что доменное имя хоста успешно разрешается.

Примечание – Если рядом с именем хоста не отображается зеленая галочка, то система не может разрешить указанное доменное имя. Проверьте настройки имени хоста в `/etc/hosts` и внесите необходимые изменения.

- **Редактирование файла hosts**

Добавьте строки с IP адресом и именем хоста для самого устройства и для этого хоста в файл `/etc/hosts` на машине виртуализированного ЦУ

- **Pause Host**

Отметьте эту опцию, если вы хотите приостановить установку, чтобы внести изменения вручную. Это приостановит развертывание после настройки engine (СУСВ) и создаст файл блокировки в `/tmp` директории, оканчивающийся на `he_setup_lock`. Развертывание hosted engine продолжится после удаления файла блокировки или через 24 часа, если файл не был удален.

- **Применить профиль OpenSCAP**

Применить изначальный профиль защиты OpenSCAP на ВМ виртуализированного ЦУ.

- **Тест сети**

Опции:

- DNS
- Ping
- TCP
- none

Выберите опцию, каким образом будет осуществляться тестирование сети. При выборе опции **none** тестирование сети осуществляться не будет.

- **Путь к архиву OVA**

Путь к архиву OVA (файл с расширением `*.ova`)

Файл OVA (Open Virtual Appliance) — это каталог OVF, сохраненный в виде архива с использованием формата архивации `.tar`.

Нажмите кнопку **Следующий** для продолжения настройки конфигурации СУСВ и перехода к секции “ВиртЦУ”.

3.5.2.2. НАСТРОЙКА ВИРТУАЛИЗИРОВАННОГО ЦУ

Развёртывание виртуализированного ЦУ

BM

ВиртЦУ

Подготовка BM

Хранилище

Завершить

1

2

3

4

5

Учётные данные виртуализированного ЦУ

Пароль Портала администрирования

.....

Настройка уведомлений

Имя сервера

localhost

Номер порта сервера

25

Адрес электронной почты отправителя

root@localhost

Адрес электронной почты получателя

root@localhost

-

+

Отмена

< Назад

Следующий >

Рисунок 39 - Параметры СУСВ

В секции “ВиртЦУ” задайте пароль для учетной записи admin администратора СУСВ в поле “Пароль Портала администрирования”.

При необходимости и возможности подключения к внешнему почтовому серверу для настройки уведомлений укажите в соответствующих полях имя и номер порта почтового сервера, а также адреса электронной почты отправителя и получателя.

Нажмите кнопку **Следующий** для перехода к секции “Подготовка BM”.

3.5.2.3. ПОДГОТОВКА ВИРТУАЛЬНОЙ МАШИНЫ

Развёртывание виртуализированного ЦУ

BM

ВиртЦУ

Подготовка BM

Хранилище

Завершить

1

2

3

4

5

Ознакомьтесь с конфигурацией. После нажатия кнопки «Подготовить BM», локальная виртуальная машина будет запущена и использована для подготовки служб управления и их данных. Эта операция может занять некоторое время, в зависимости от аппаратных составляющих.

VM

Engine FQDN: vm.home.local
MAC Address: 00:16:3e:6e:8e:Bf
Network Configuration: Static
VM IP Address: 192.168.0.70/24
Gateway Address: 192.168.0.1
DNS Servers: 192.168.0.1
Root User SSH Access: yes
Number of Virtual CPUs: 4
Memory Size (MiB): 4096
Root User SSH Public Key: (None)
Add Lines to /etc/hosts: yes
Bridge Name: ovirtmgmt
Apply OpenSCAP profile: no

Engine

SMTP Server Name: localhost
SMTP Server Port Number: 25
Sender E-Mail Address: root@localhost
Recipient E-Mail Addresses: root@localhost

Отмена

< Назад

Подготовить BM

Рисунок 40 - Обзор параметров конфигурации BM

В секции “Подготовка BM” нажмите кнопку **Подготовить BM** для создания и запуска BM в соответствии с заданной конфигурацией.

После успешного завершения запуска BM, на экране появится соответствующее сообщение.

Развёртывание виртуализированного ЦУ

✕

ВМ

ВиртЦУ

Подготовка ВМ

Хранилище

Завершить

1

2

3

4

5



Выполнено успешно. Переходите к следующему шагу.

Отмена

< Назад

Следующий >

Рисунок 41 - Завершение подготовки ВМ

Нажмите кнопку **Следующий** для перехода к секции “Хранилище”.

3.5.2.4. НАСТРОЙКА ПАРАМЕТРОВ ХРАНИЛИЩА

Развёртывание виртуализированного ЦУ

ВМ

ВиртЦУ

Подготовка ВМ

Хранилище

Завершить

1

2

3

4

5

Настройте домен хранения, в котором будет размещаться диск виртуальной машины управления. Обратите внимание, что ВМ управления должна быть достаточно гибкой и надёжной, чтобы иметь возможность управлять всеми ресурсами развёртывания, поэтому предпочтительным является высокодоступное хранилище.

Параметры хранилища

Обратите внимание, что поддерживаются только тома Gluster без реплики или с тремя репликами.

Тип хранилища

Gluster

Подключение к хранилищу

host1.home.local:/engine

Параметры монтирования

backup-volfile-servers=host2.home.local:h

> Расширенное

Отмена

< Назад

Следующий >

Рисунок 42 - Параметры хранилища типа Gluster

В секции “Хранилище” выберите из выпадающего списка “Тип хранилища” необходимое значение – Gluster, NFS или iSCSI.

Настройка хранилища типа Gluster

При выборе типа хранилища Gluster укажите в поле “Подключение к хранилищу” том engine (например, host1.home.local:/engine) созданного в разделе 3.5.1. Развертывание хранилища Gluster.

Настройка хранилища типа NFS

При выборе типа хранилища NFS укажите в поле “Подключение к хранилищу” путь к хранилищу (например, host1.home.local:/data/engine) созданному в разделе 3.4.1. Подготовка хранилища NFS.

 ПОСА

Развёртывание виртуализированного ЦУ

✕

1

ВМ

2

ВиртЦУ

3

Подготовка ВМ

4

Хранилище

5

Завершить

Настройте домен хранения, в котором будет размещаться диск виртуальной машины управления. Обратите внимание, что ВМ управления должна быть достаточно гибкой и надёжной, чтобы иметь возможность управлять всеми ресурсами развёртывания, поэтому предпочтительным является высокодоступное хранилище.

Параметры хранилища

Тип хранилища	NFS
Подключение к хранилищу	vmrvhost1.rosa.lan:/data/engine
Параметры монтирования	option1=value1,option2=value2

> Расширенное

Отмена

< Назад

Следующий >

Рисунок 43 - Параметры хранилища типа NFS

Настройка расширенных параметров

Для настройки расширенных параметров нажмите на кнопку “Расширенное”

Развёртывание виртуализированного ЦУ

✕

1

BM

2

ВиртЦУ

3

Подготовка VM

4

Хранилище

5

Завершить

Настройте домен хранения, в котором будет размещаться диск виртуальной машины управления. Обратите внимание, что VM управления должна быть достаточно гибкой и надежной, чтобы иметь возможность управлять всеми ресурсами развёртывания, поэтому предпочтительным является высокодоступное хранилище.

Параметры хранилища

Тип хранилища

NFS

Подключение к хранилищу

vmrvhost1.rosa.lan:/data/engine

Параметры монтирования

option1=value1,option2=value2

Расширенное

Размер диска (Гиб)

62

Версия NFS

Auto

Доменное имя хранилища

hosted_storage

Отмена

< Назад

Следующий >

Рисунок 44 - Настройка расширенных параметров для хранилища типа NFS

- Размер диска

Размер диска по умолчанию составляет **62ГБ**. Это размер диска является минимально допустимым значением. При необходимости размер диска можно увеличить, меньший размер диска использовать нельзя.

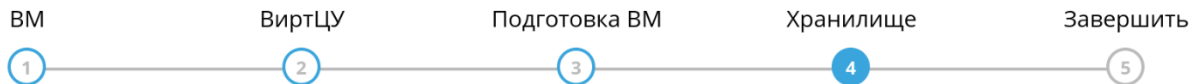
- Версия NFS

Версия NFS по умолчанию — Auto. Данный параметр менять не рекомендуется.

- Доменное имя хранилища

Имя хранилища, по которому оно будет видно в домене.

Настройка хранилища типа iSCSI



Настройте домен хранения, в котором будет размещаться диск виртуальной машины управления. Обратите внимание, что VM управления должна быть достаточно гибкой и надежной, чтобы иметь возможность управлять всеми ресурсами развёртывания, поэтому предпочтительным является высокодоступное хранилище.

Параметры хранилища

Тип хранилища	iSCSI
Адрес IP портала	
Порт портала	3260
Имя пользователя портала	
Пароль портала	
Получение списка целей	

▼ Расширенное

Размер диска (Гиб)	62
Имя пользователя для обнаружения	
Имя пользователя для обнаружения	

Рисунок 45 - Параметры хранилища типа iSCSI

- Адрес IP портала

IP адрес, по которому доступен портал

- Порт портала

Порт, по которому доступен портал (по умолчанию используется порт 3260)

- Имя пользователя портала

Имя пользователя портала, используемое для аутентификации

- Пароль портала

Пароль пользователя портала

Расширенные параметры для настроек хранилища типа iSCSI

- Размер диска

Размер диска по умолчанию составляет **62ГБ**. Это размер диска является минимально допустимым значением. При необходимости размер диска можно увеличить, меньший размер диска использовать нельзя.

- Имя пользователя обнаружения

Имя, по которому пользователь может быть обнаружен

- Пароль пользователя обнаружения

Пароль пользователя

Примечание – С особенностями настроек параметров хранилища iSCSI можно ознакомиться на сайте <http://www.open-iscsi.com/>

При выборе типа хранилища iSCSI нажмите кнопку **Получение списка целей** для настройки параметров хранилища.

Нажмите кнопку **Следующий** для перехода к секции “Завершить”.

3.5.2.5. ЗАВЕРШЕНИЕ РАЗВЕРТЫВАНИЯ ВИРТУАЛИЗИРОВАННОГО ЦУ

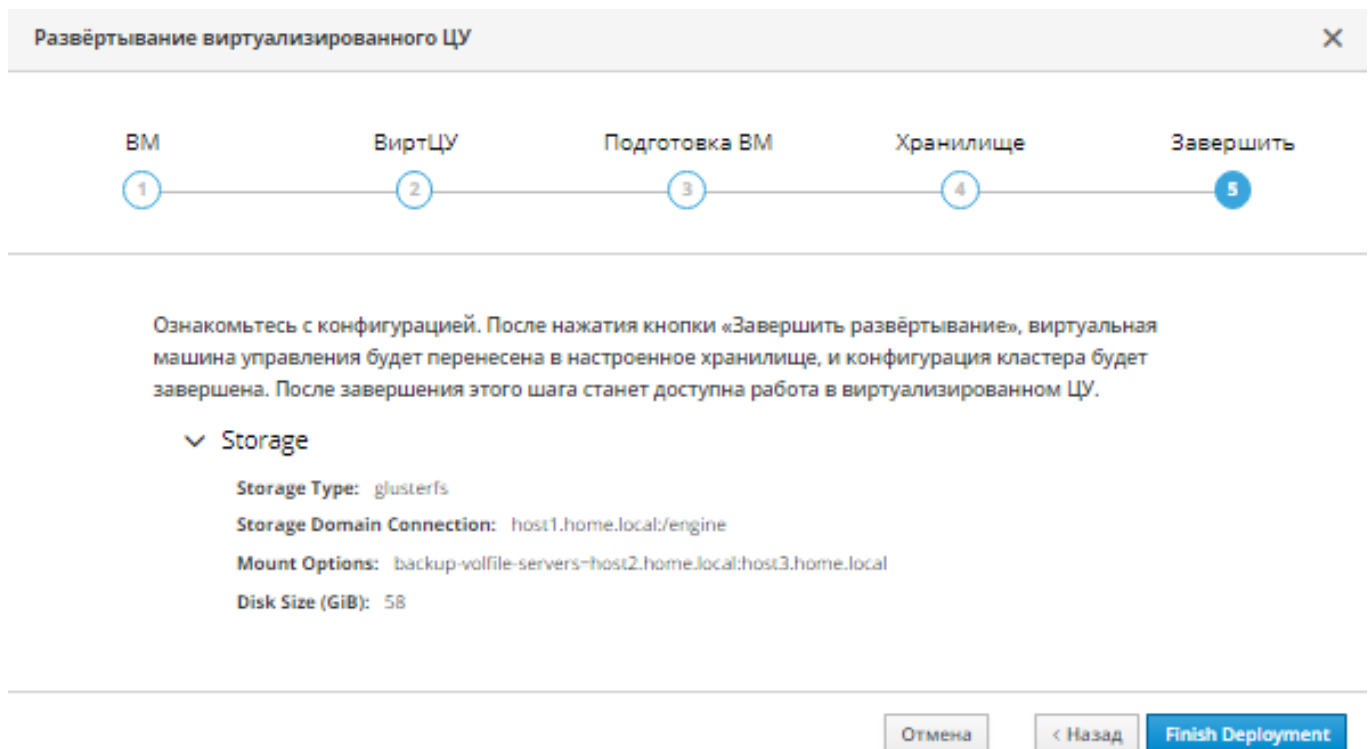
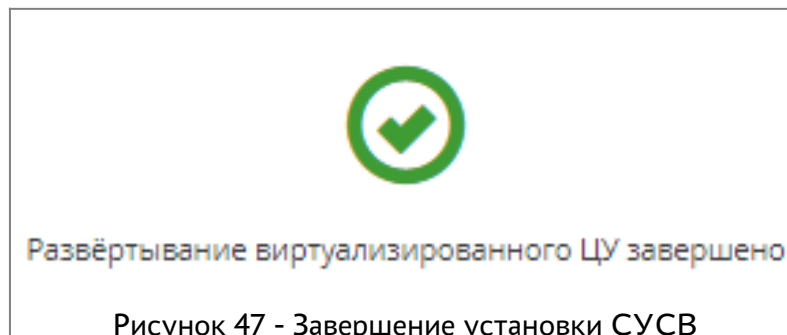


Рисунок 46 - Обзор конфигурации хранилища

В секции “Завершить” нажмите кнопку **Завершить развёртывание** для переноса VM СУСВ в хранилище и завершения процедуры установки СУСВ.

После успешного завершения установки СУСВ на экране, появится соответствующее сообщение и станет доступным вход в веб-интерфейс СУСВ.



Нажмите кнопку **Заккрыть** для завершения работы программы установки СУСВ.

Очистка параметров установки СУСВ

В случае неудачного завершения установки СУСВ осуществите процедуру очистки данных перед повторной установкой. Для этого в консоли хоста дважды выполните следующую команду:

```
# ovirt-hosted-engine-cleanup
```

Установка СУСВ в консольном режиме

При необходимости установку СУСВ можно осуществить в консольном режиме. Для запуска программы установки выполните в консоли хоста следующую команду:

```
# hosted-engine --deploy
```

Далее, следуйте инструкциям текстового интерфейса программы установки.

3.5.3. УСТАНОВКА СЕРТИФИКАТА ЦС

При первом доступе к Порталу администрирования (СУСВ) необходимо установить сертификат, используемый виртуализированным ЦУ, для избежания предупреждений безопасности.

Установка сертификата ЦС с использованием веб-браузера Firefox:

1. Перейдите по адресу URL Портала администрирования и на странице приветствия нажмите на кнопку **СА сертификат центра управления** (Рисунок 48).

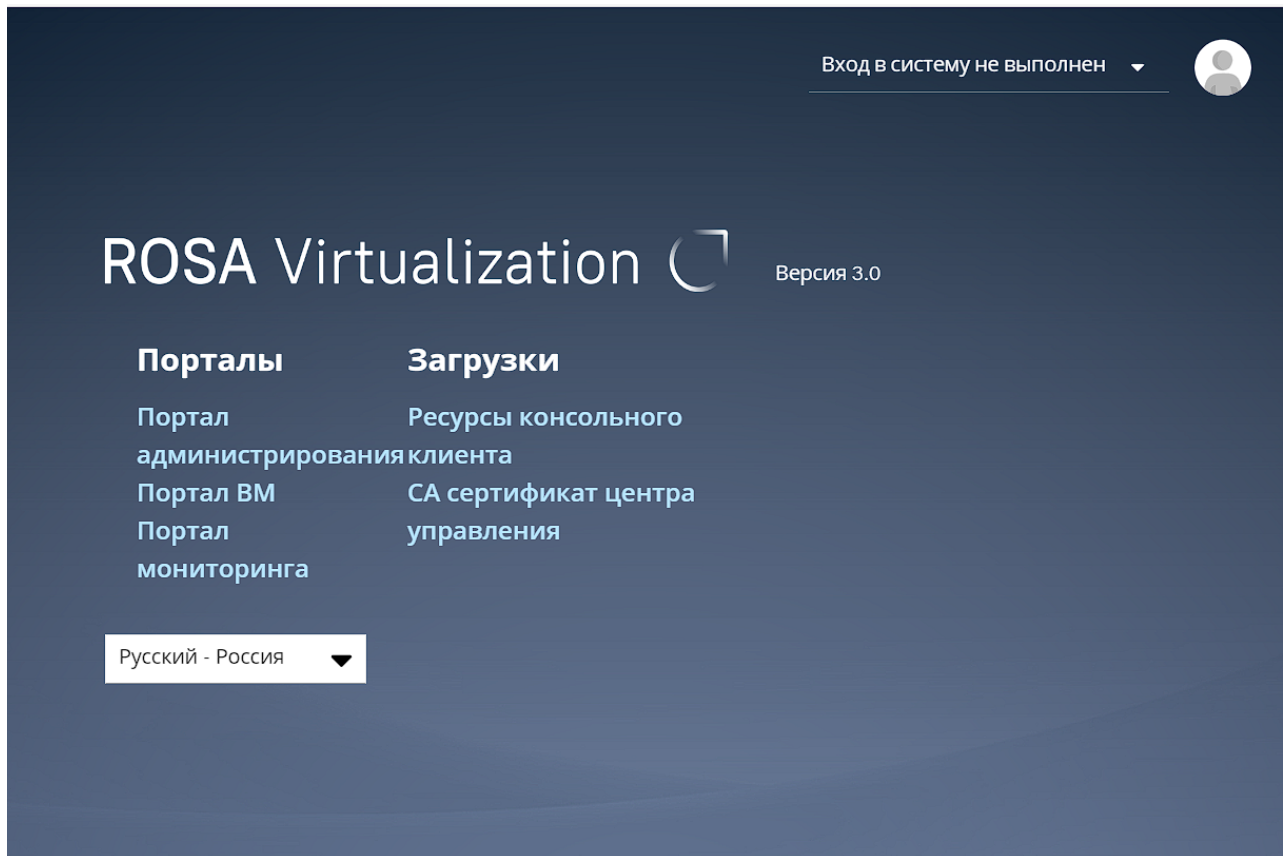


Рисунок 48: Портал входа ROSA Virtualization

2. Будет загружен файл `pki-resource` (без расширения файла).
3. Откройте окно **Параметры/Предпочтения**:
 - Windows: откройте меню Firefox и выберите **Настройки**
 - (URL `about:preferences`)
 - Mac: откройте меню Firefox и выберите **Параметры...**
 - Linux: откройте меню Правка и выберите **Параметры**.
4. Выберите в меню слева секцию **Приватность и защита** и прокрутите вниз содержимое формы до раздела **Сертификаты** (Рисунок 49).

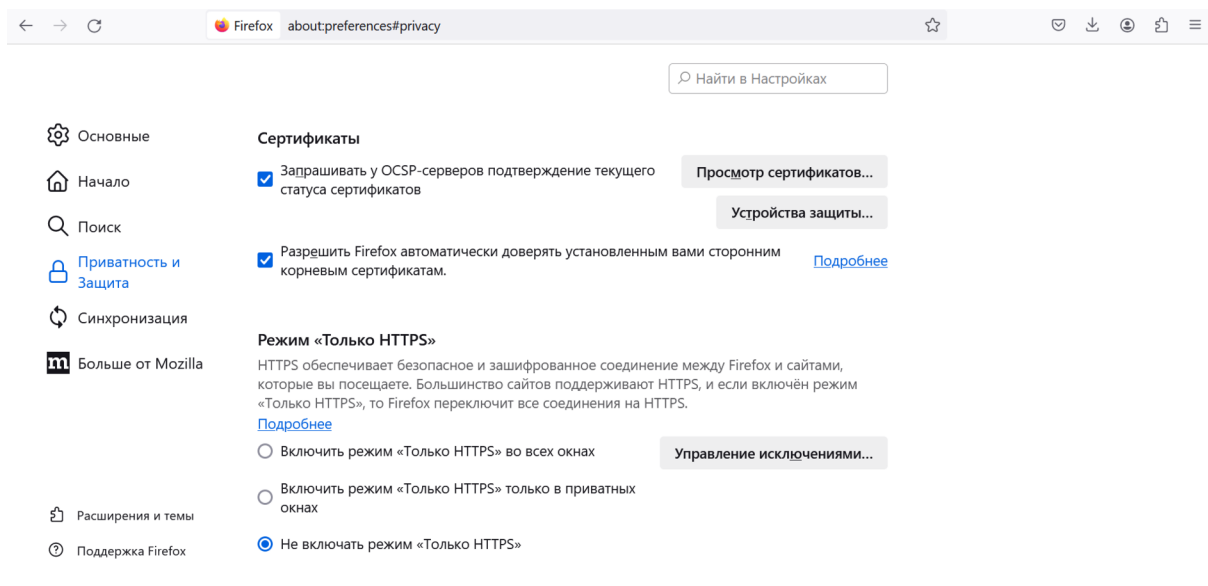


Рисунок 49: Firefox: Секция «Приватность и защита», раздел «Сертификаты»

5. Нажмите **Просмотр сертификатов...**, чтобы открыть **Управление сертификатами** и перейти на вкладку **Центры сертификации** (Рисунок 50).

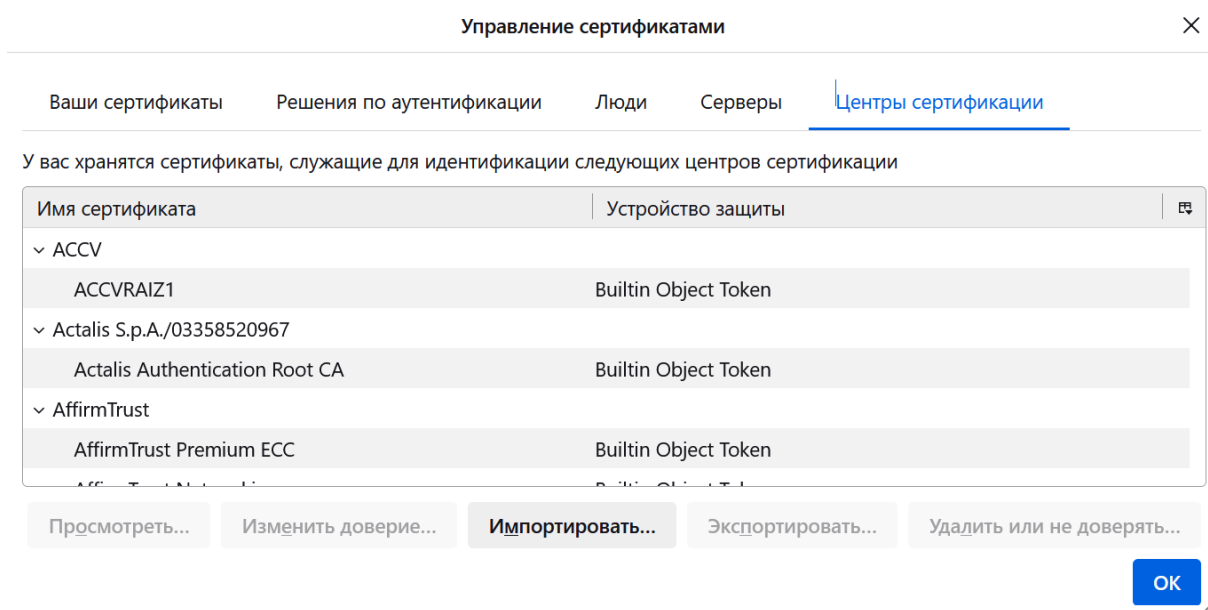


Рисунок 50: Firefox: диалог «Управление сертификатами» — «Центры сертификации»

6. Нажмите на кнопку **Импортировать...** (Рисунок 50)
7. Выберите файл корневого сертификата, который нужно импортировать (для просмотра загруженного файла смените тип файла на **Все файлы**).
8. Отметьте галочками параметры доверия и нажмите **ОК**.
9. В разделе Диспетчера сертификатов нажмите **ОК** и закройте окно **Параметры/Предпочтения**.
10. Убедитесь в том, что все процессы Firefox остановлены.

11. Перезапустите Firefox и перейдите по адресу URL Портала администрирования. Значок замочка в адресной строке указывает на то, что сертификат ЦС установлен.

Установка сертификата ЦС в веб-браузере Google Chrome:

1. Перейдите по адресу URL Портала ВМ и на странице приветствия нажмите на кнопку **СА сертификат центра управления** (Рисунок 48).
2. Будет загружен файл `pki-resource.cer` (расширение файла `.cer`).
3. Перейдите в меню **Настройки** → **Конфиденциальность и безопасность** → **Настроить сертификаты** (Рисунок 51) и нажмите на кнопку справа (квадрат со стрелочкой) для вызова диалога для управления сертификатами.
(URL `chrome://settings/security`)

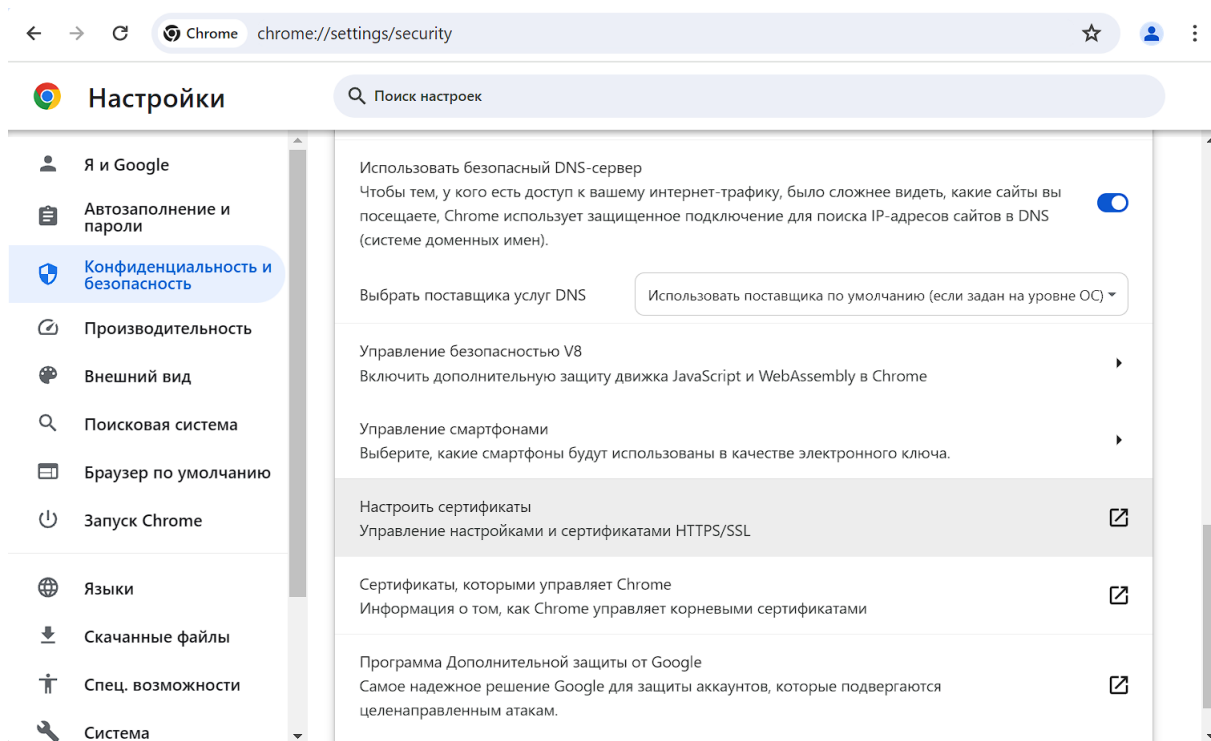


Рисунок 51: Chrome: Настройки → Конфиденциальность и безопасность → Настроить сертификаты

4. В диалоге для управления сертификатами нажмите кнопку **Импорт...** (Рисунок 52)

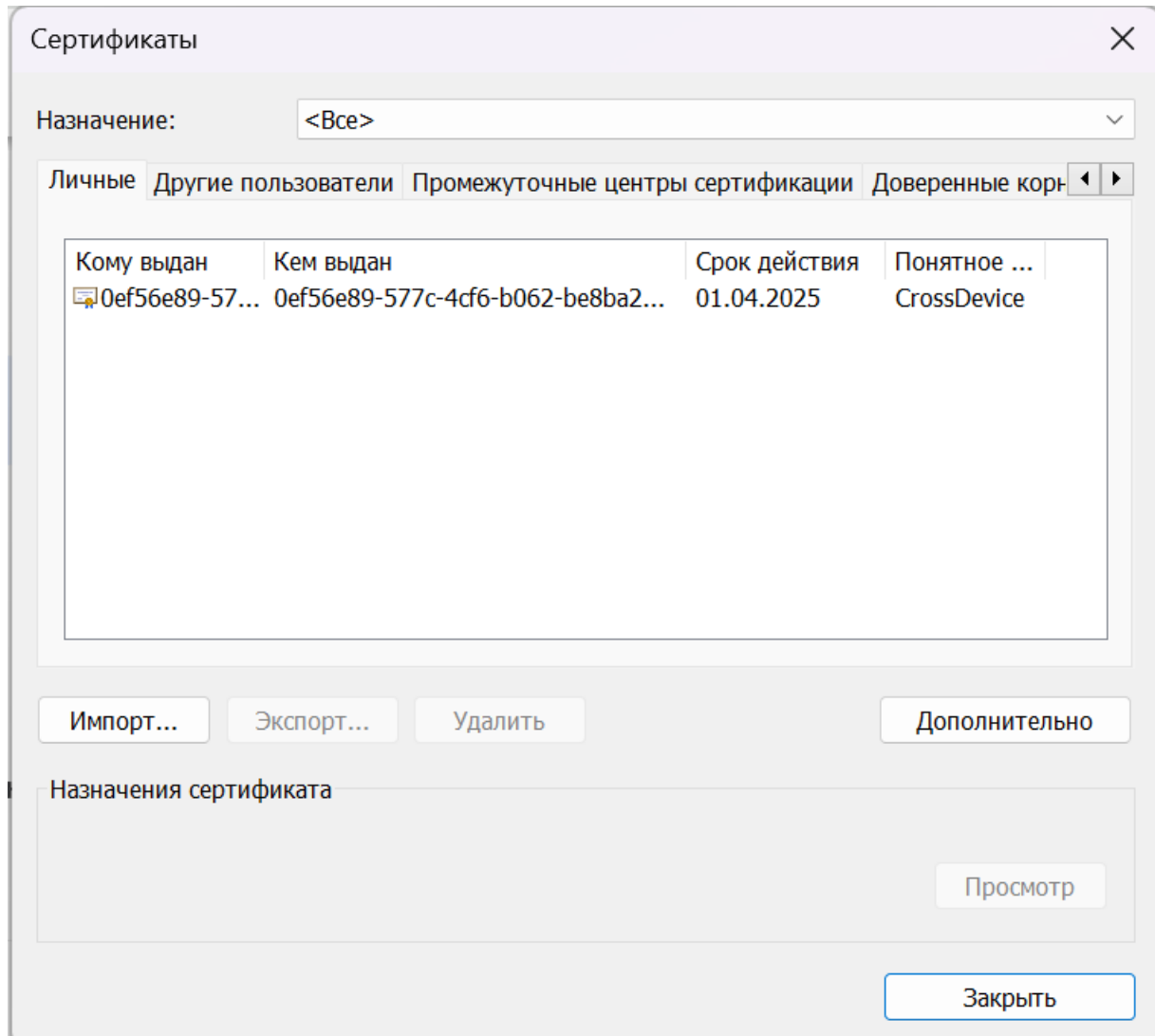


Рисунок 52: Chrome: диалог для управления сертификатами

Откроется окно **Мастер импорта сертификатов** (Рисунок 53)



←  Мастер импорта сертификатов

Мастер импорта сертификатов

Этот мастер помогает копировать сертификаты, списки доверия и списки отзыва сертификатов с локального диска в хранилище сертификатов.

Сертификат, выданный центром сертификации, является подтверждением вашей личности и содержит информацию, необходимую для защиты данных или установления защищенных сетевых подключений. Хранилище сертификатов — это область системы, предназначенная для хранения сертификатов.

Для продолжения нажмите кнопку "Далее".

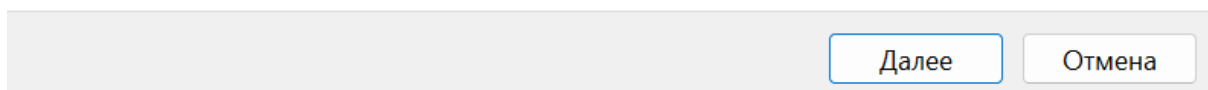


Рисунок 53: Мастер импорта сертификатов (Windows)

Нажмите кнопку **Далее** (Рисунок 53)

5. В Мастере импорта сертификатов укажите **Импортируемый файл** — для этого нажмите на кнопку **Обзор...** (Рисунок 54)



←  Мастер импорта сертификатов

Импортируемый файл

Укажите файл, который вы хотите импортировать.

Имя файла:

Обзор...

Замечание: следующие форматы файлов могут содержать более одного сертификата в одном файле:

Файл обмена личной информацией - PKCS #12 (.PFX,.P12)

Стандарт Cryptographic Message Syntax - сертификаты PKCS #7 (.p7b)

Хранилище сериализованных сертификатов (.SST)

Далее

Отмена

Рисунок 54: Мастер импорта сертификатов — выбор Импортируемый файл

6. Выберите файл корневого **сертификата X.509**, который нужно импортировать (Рисунок 55, для просмотра всех файлов смените тип файла на **Все файлы**, необходим ранее загруженный файл `pki-resource.cer`).

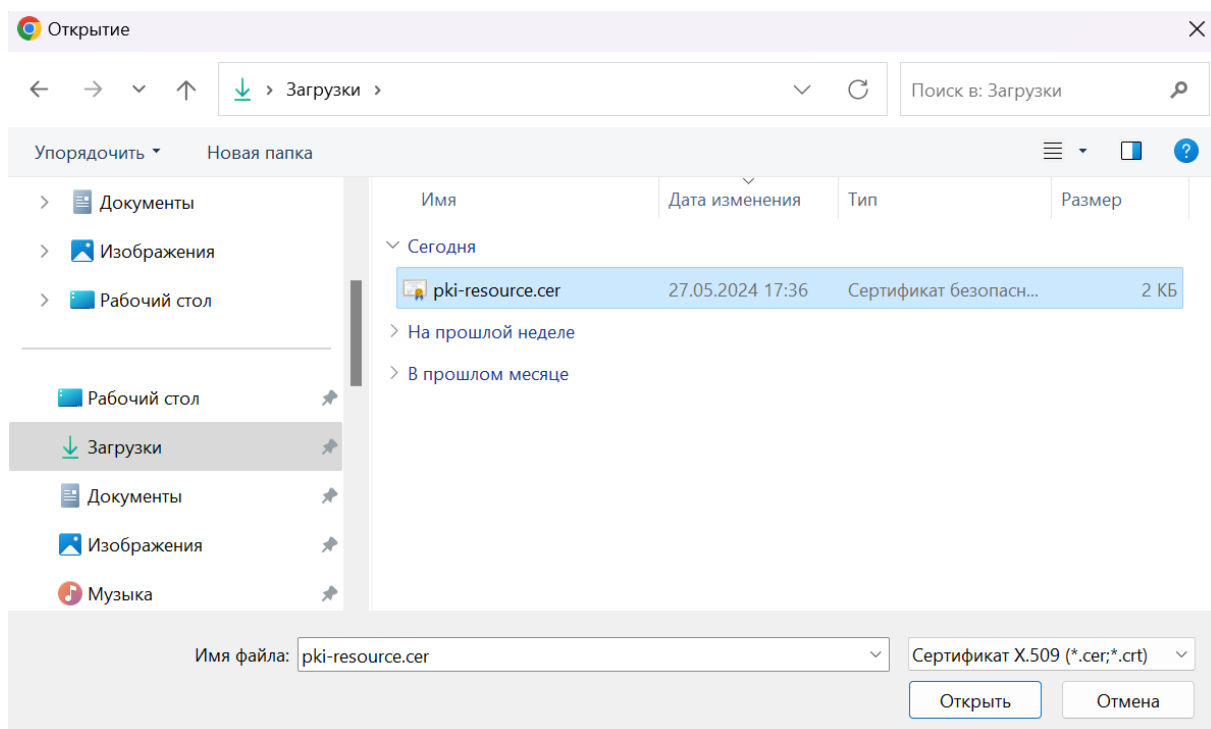


Рисунок 55: Выбор файла корневого сертификата X.509 (Windows)

7. В Мастере импорта сертификатов укажите необходимое **Хранилище сертификатов** — **Доверенные корневые центры сертификации** (Рисунок 56), и нажмите на кнопку **Далее**.

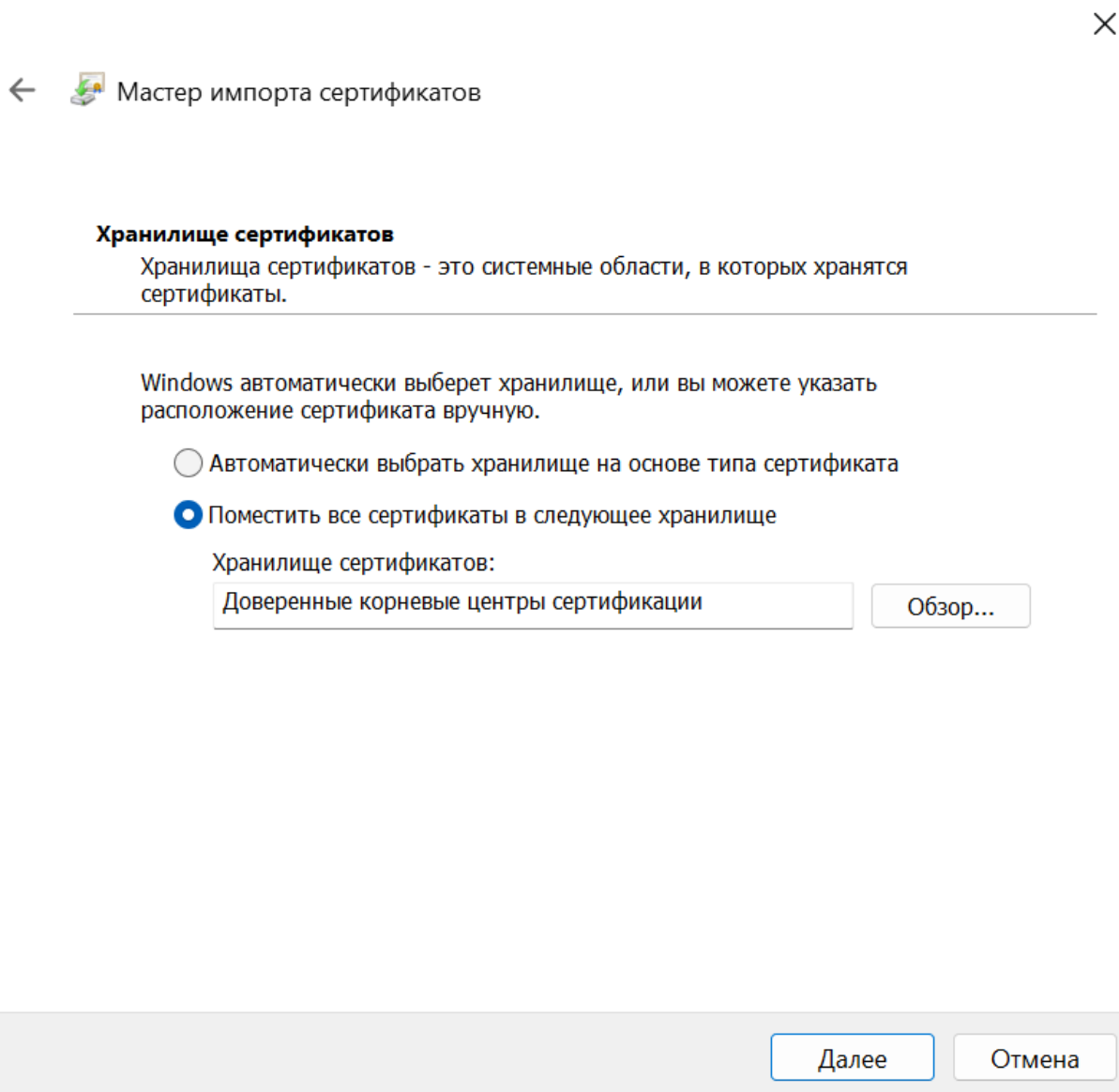


Рисунок 56: Мастер импорта сертификатов: Хранилище сертификатов — Доверенные корневые центры сертификации

- В завершающем диалоге Мастера импорта сертификатов нажмите на кнопку **Готово** (Рисунок 57).



← Мастер импорта сертификатов

Завершение мастера импорта сертификатов

Сертификат будет импортирован после нажатия кнопки "Готово".

Были указаны следующие параметры:

Хранилище сертификатов, выбранное пользователем	Доверенные корневые центры с
Содержимое	Сертификат
Файл	C:\Users\lples\Downloads\pki-res

Рисунок 57: Завершающий диалог Мастера импорта сертификатов

9. Закройте Chrome и убедитесь в том, что все процессы Chrome остановлены.
10. Перезапустите Chrome и перейдите по адресу URL Портала администрирования (СУСВ). Значок замочка в адресной строке указывает на то, что сертификат ЦС установлен (Рисунок 58).

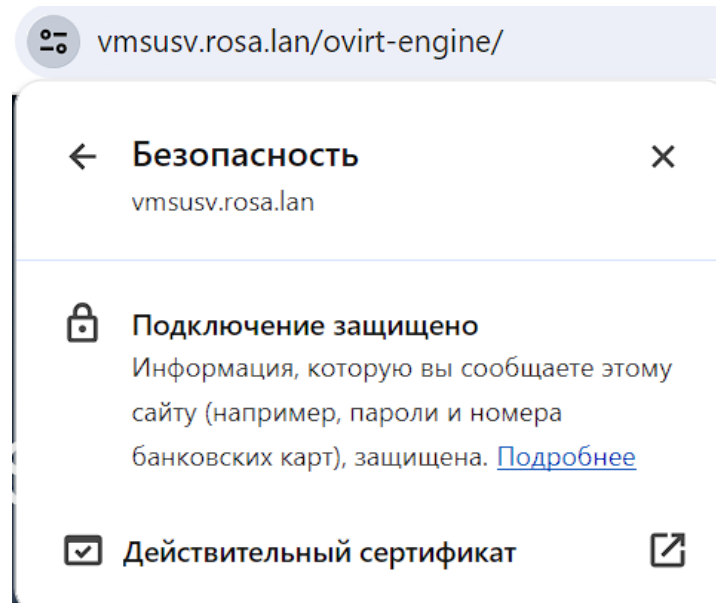


Рисунок 58: Подключение к СУСВ (Портал администрирования) защищено

3.5.4. ВХОД В ВЕБ-ИНТЕРФЕЙС СУСВ

Для доступа к веб-интерфейсу введите в адресной строке браузера (на внешней рабочей станции) доменное имя или IP-адрес ВМ СУСВ.

Например:

```
https://vm.home.local
```

На экране появится окно, содержащее ссылки для перехода к порталу администрирования или порталу ВМ.



Рисунок 59 - Интерфейс выбора портала

Для доступа к административным функциям СУСВ нажмите на ссылку “Портал администрирования” и введите учетные данные (логин и пароль) пользователя admin для авторизации.

В случае успешной авторизации, на экране появится панель мониторинга СУСВ, которая загружается по умолчанию и содержит общую информацию о компонентах ROSA Virtualization.

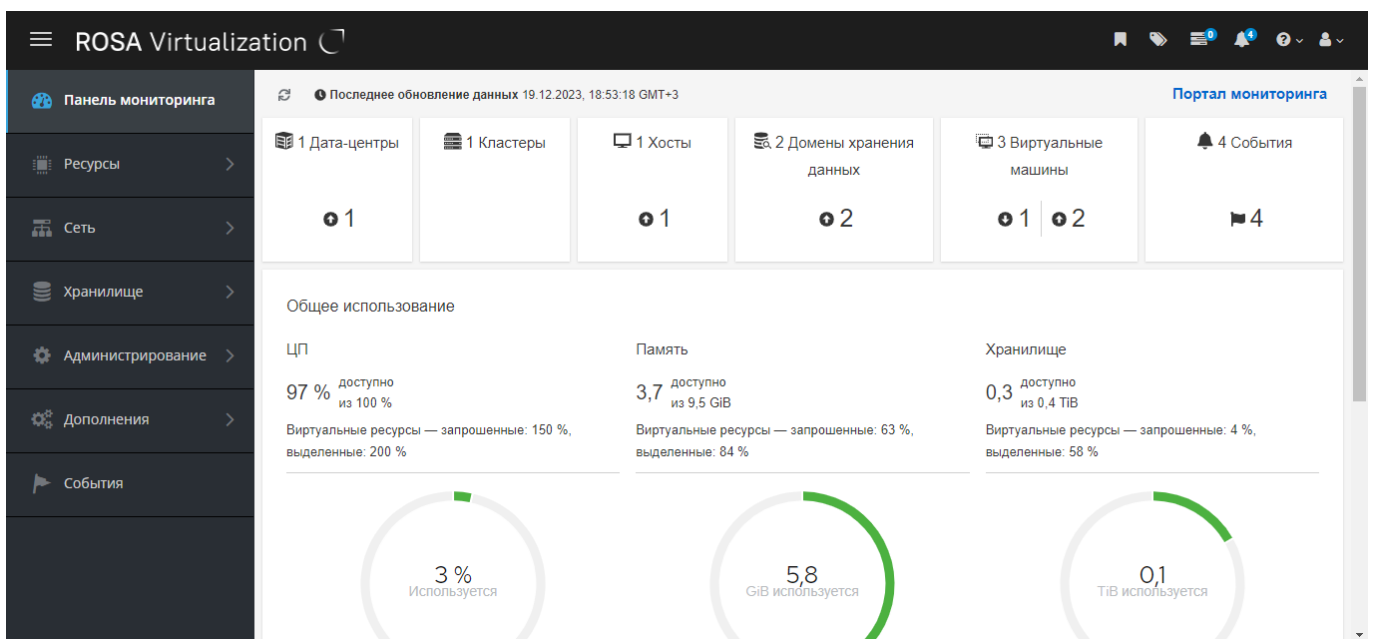


Рисунок 60 - Панель мониторинга СУСВ

Последующий доступ к функциям СУСВ осуществляется через выбор необходимых пунктов в главном меню СУСВ.

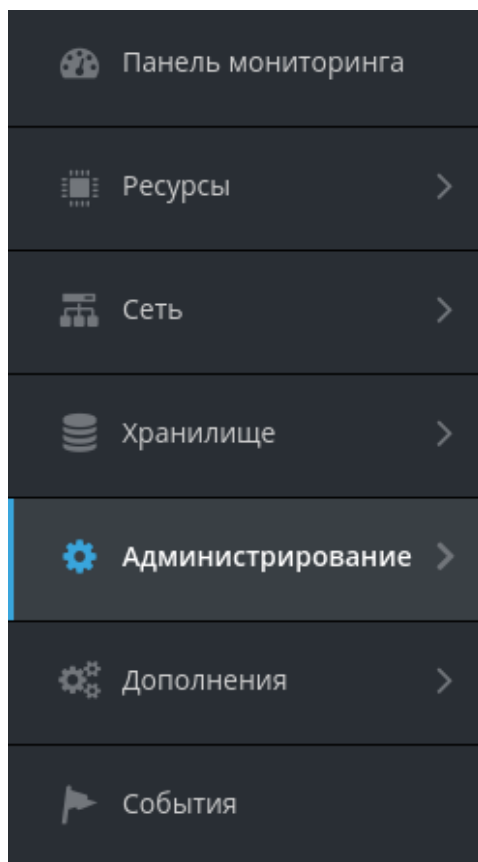


Рисунок 61 - Главное меню СУСВ

3.6. ДОБАВЛЕНИЕ ХОСТОВ В КЛАСТЕР

При разворачивании ROSA Virtualization в базовой конфигурации выполните процедуру добавления *каждого из хостов* с установленным гипервизором в кластер.

Кластер – логическое объединение хостов, которые выступают в качестве общего ресурсного пула для ВМ. При этом ВМ динамически выделяются каждому хосту в кластере и могут мигрировать между хостами.

Каждый хост ROSA Virtualization должен принадлежать определенному кластеру.

Во время установки ROSA Virtualization создается кластер по умолчанию Default, который включает в свой состав только хост с установленным гипервизором и развернутой ВМ СУСВ (например, `host1.home.local`).

3.6.1. ДОБАВЛЕНИЕ ХОСТОВ В КЛАСТЕР С ИСПОЛЬЗОВАНИЕМ ПОРТАЛА АДМИНИСТРИРОВАНИЯ СУСВ

Добавление хостов в кластер осуществляется на портале администрирования СУСВ.

Для добавления хоста выберите пункт “Ресурсы → Хосты” в главном меню СУСВ и нажмите кнопку **Добавить**.

На экране появится вкладка “Общее” окна “Новый хост”.

Новый хост

Общее

Управление питанием

SPM

Консоль и GPU

Ядро

Виртуализированный ЦУ

Схожесть

Хост кластера

Default

Дата-центр: Default

Имя

Комментарий

Имя хоста/IP

Порт SSH

22

Активировать хост после установки

Перезагрузить хост после установки

Аутентификация

Имя пользователя

root

Пароль

Открытый ключ SSH

Дополнительные параметры

OK

Отменить

Рисунок 62: Вкладка “Общее” окна “Новый хост”

В поля “Имя” и “Имя хоста/IP” введите соответственно краткое (например, host2) и полное доменное имя хоста (например, host2.home.local), или его IP адрес.

В поле “Пароль” укажите пароль учетной записи суперпользователя root данного хоста.

Далее, перейдите на вкладку “Виртуализированный ЦУ” и выберите действие “Развернуть”, чтобы данный хост имел возможность запуска СУСВ при выходе из строя хоста, на котором СУСВ выполняется в текущий момент, что повышает надежность и отказоустойчивость ROSA Virtualization.

Для применения всех сделанных изменений нажмите кнопку **OK**.

Для настройки политики энергосбережения, на экране появится окно “Параметры управления питанием”. При необходимости в настройке параметров агента интерфейса низкоуровневого управления питанием хоста нажмите кнопку **Настроить управление питанием** и введите необходимые параметры.

Для завершения процедуры добавления хоста в кластер нажмите кнопку **OK**.

После добавления в кластер статус хоста изменится на значение “Up”.

Повторите процедуру добавления в кластер для каждого из хостов с установленным гипервизором.

3.7. АКТИВАЦИЯ ЛИЦЕНЗИИ ROSA VIRTUALIZATION

Лицензия ROSA Virtualization предназначена для подтверждения уникальности копии программного продукта и устанавливает определенные ограничения по применению, такие как допустимое количество совместно работающих ВМ, задействованных процессорных слотов и т.д. Дополнительно лицензия имеет дату окончания действия, после наступления которой запуск ВМ будет заблокирован.

Файл с лицензией ROSA Virtualization содержит электронный ключ, который необходимо активировать на СУСВ. Поэтому предварительно скопируйте файл с лицензией в один из каталогов ВМ СУСВ (например, /tmp).

Активация лицензии ROSA Virtualization осуществляется консольной утилитой `install-rosa-license`.

Примечание – Для подключения к консоли СУСВ по SSH выполните следующую команду с указанием доменного имени (например, `vm.home.local`) или IP-адреса ВМ СУСВ, а также пароля учетной записи суперпользователя `root` ВМ СУСВ при выводе на экран соответствующего запроса:

```
# ssh root@vm.home.local
root@vm.home.local's password:
```

Для запуска процесса активации лицензии выполните в консоли СУСВ следующую команду:

```
# install-rosa-license
```

При выводе на экран соответствующего запроса введите путь к файлу с лицензией.

Далее, интерактивный сценарий автоматически осуществит активацию лицензии ROSA Virtualization.

3.7.1. ПРИМЕР АКТИВАЦИИ ЛИЦЕНЗИИ ROSA VIRTUALIZATION

```
[root@susv ~]# install-rosa-license
Path to Rosa Virtualization license file (/tmp/license.gz):
The license is successfully installed.
```

Сценарий активации лицензии по умолчанию предполагает наличие файла с лицензией под именем `license.gz` в каталоге `/tmp`. Если вы скопировали файл с лицензией в этот каталог, то достаточно нажать на клавишу Enter.

Если в консоль было выведено сообщение `The license is successfully installed`, то лицензия была успешно активирована.

Примечание – Для просмотра подробной информации и проверки валидности установленной лицензии выполните в консоли СУСВ следующую команду:

```
# rosa-license-info
```

3.7.2. ПРИМЕР ПРОСМОТРА ИНФОРМАЦИИ ОБ ЛИЦЕНЗИИ

```
[root@susv ~]# rosa-license-info  
Verified OK  
VM_Backup appliance is allowed: 1.
```

Лицензия верифицирована.

3.8. УСТАНОВКА СЕРВЕРА IPA

В составе ROSA Virtualization сервер IPA функционирует в качестве сервера каталогов LDAP и предназначен для идентификации и аутентификации доменных пользователей.

Сервер IPA может быть развернут как на отдельном физическом сервере без предустановленной ОС, так и на ВМ под управлением ROSA Virtualization.

Для установки сервера IPA на ВМ под управлением ROSA Virtualization предварительно создайте новую ВМ на портале администрирования СУСВ, а также загрузите образ с дистрибутивом (файл RV-3.0-20240521.0-rv-x86_64-dvd1) в хранилище в подкаталог /iso.

Для установки сервера IPA на отдельный физический сервер используйте DVD диск с дистрибутивом ROSA Virtualization или ранее созданный сменный носитель с записанным на него образом дистрибутива.

3.8.1. СОЗДАНИЕ ВМ ДЛЯ СЕРВЕРА IPA

Для создания новой ВМ для сервера IPA авторизуйтесь на портале администрирования СУСВ. На экране появится интерфейс портала администрирования с главным меню СУСВ.

В главном меню СУСВ выберите пункт “Ресурсы → Виртуальные машины” и нажмите кнопку **Добавить**.

На экране появится вкладка “Общие” окна “Новая ВМ” (Рисунок 63).

Новая ВМ

Общие

Система

Начальный запуск

Консоль

Хост

Высокая доступность

Выделение ресурсов

Параметры загрузки

Генератор случайных чисел

Настраиваемые пользователем параметры

Значок

Foreman/Satellite

Схожесть

Кластер

Шаблон

Операционная система

Тип чипсета/микропрограммы

Оптимизировано для

Default

Blank | (0)

Other OS

Чипсет Q35 с UEFI

Сервер

Дата-центр: Default

Имя

Описание

Комментарий

ID ВМ

Без сохранения состояния

Запустить и приостановить

Защита от удаления

Запечатан

Образы экземпляра

Присоединить

Создать

+

-

Создать экземпляр сетевого интерфейса ВМ, выбрав профиль vNIC

nic1

Выберите элемент...

+

-

Убрать расширенные параметры

OK

Отменить

Рисунок 63. Вкладка “Общие” окна “Новая ВМ”

В поле “Имя” введите уникальное наименование для новой ВМ (например, Server-IPA).

Для создания виртуального диска ВМ нажмите кнопку **Создать**. На экране появится окно “Новый виртуальный диск”.

Новый виртуальный диск

×

Образ

Прямой LUN

Cinder

Программно-управляемый блочный диск

Размер (Гиб)

☐ Забить нулями после удаления

Псевдоним

☒ Загрузочный

Описание

☐ Может быть общим

Интерфейс

☐ Только для чтения

Домен хранилища

☐ Включить освобождение места на диске перед удалением

Политика распределения

☐ Включить инкрементное резервное копирование

Профиль диска

OK

Отменить

Рисунок 64 - Окно “Новый виртуальный диск”

В поле “Размер (Гиб)” укажите размер виртуального диска не менее 62 ГБ.

После настройки опциональных параметров виртуального диска нажмите кнопку **OK** для сохранения указанных значений и возвращения в окно “Новая ВМ”.

Далее, в окне “Новая ВМ” перейдите на вкладку “Система”.

Новая ВМ

Общие

Система

Начальный запуск

Консоль

Хост

Высокая доступность

Выделение ресурсов

Параметры загрузки

Генератор случайных чисел

Настраиваемые пользователем параметры

Значок

Foreman/Satellite

Схожесть

Кластер

Шаблон

Операционная система

Тип чипсета/микропрограммы

Оптимизировано для

Default

Blank | (0)

Other OS

Чипсет Q35 с UEFI

Сервер

Дата-центр: Default

Размер памяти

Максимальный объем памяти

Гарантированная физическая память

Всего виртуальных ЦП

Дополнительные параметры

Общее

Тип экземпляра

Смещение времени аппаратных часов

Политика серийных номеров

Серийный номер, настраиваемый пользователем

1024 Мбайт

4096 Мбайт

1024 Мбайт

1

Настраивается пользователем

(GMT+03:00) Russian Standard Time

Кластер по умолчанию (ID хоста)

Убрать расширенные параметры

OK

Отменить

Рисунок 65. Вкладка “Система”

В поле “Размер памяти” укажите объем используемой оперативной памяти не менее 2 ГБ (Рисунок 65).

Перейдите на вкладку “Параметры загрузки” (Рисунок 66).

Новая ВМ

Общие

Система

Начальный запуск

Консоль

Хост

Высокая доступность

Выделение ресурсов

Параметры загрузки

Генератор случайных чисел

Настраиваемые пользователем параметры

Значок

Foreman/Satellite

Схожесть

Кластер

Шаблон

Операционная система

Тип чипсета/микропрограммы

Оптимизировано для

Дата-центр: Default

Blank | (0)

Other OS

Чипсет Q35 с UEFI

Сервер

Последовательность загрузки:

Первое устройство

Второе устройство

☒ Присоединить CD

☐ Включите меню для выбора загрузочного устройства

CD-ROM

Жесткий диск

RV-3.0-20240521.0-rv-x86_64-dvd1.iso

Рисунок 66. Вкладка “Параметры загрузки”

Установите последовательность загрузки устройств. Для последующей установки ОС с загруженного образа с дистрибутивом сервера IPA выберите из выпадающего списка “Первое устройство” значение “CD-ROM”, а из выпадающего списка “Второе устройство” значение “Жесткий диск” (Рисунок 66).

Установите флажок “Присоединить CD” и выберите из выпадающего списка образ с дистрибутивом (файл RV-3.0-20240521.0-rv-x86_64-dvd1.iso).

Для применения всех сделанных настроек и создания новой ВМ нажмите кнопку **ОК**.

В результате на портале администрирования СУСВ в меню “Ресурсы → Виртуальные машины” появится новая ВМ, созданная для сервера IPA.

После создания новой ВМ настройте параметры виртуального сетевого интерфейса. Для этого во внутреннем меню ВМ нажмите кнопку **Изменить** и во вкладке “Общие” выберите из выпадающего списка необходимое значение (рекомендуемый вариант – ovirtmgmt).

Для перехода к процессу установки ОС на сервер IPA выберите созданную ВМ и нажмите кнопку **Запустить**, а после изменения состояния ВМ нажмите кнопку **Консоль**.

На экране появится интерфейс программы установки ОС.

3.8.2. УСТАНОВКА ОС НА СЕРВЕР IPA

Процесс установки ОС на сервер IPA во многом аналогичен процедуре установки ОС гипервизора, которая полностью и подробно приведена в подразделе 3.2.

Для установки ОС загрузите физический сервер или созданную VM с носителя с дистрибутивом сервера IPA.

На экране последовательно появятся меню программы установки, окно приветствия и меню “Сводка установки”, которое содержит различные секции для настройки параметров установки (Рисунок 67).

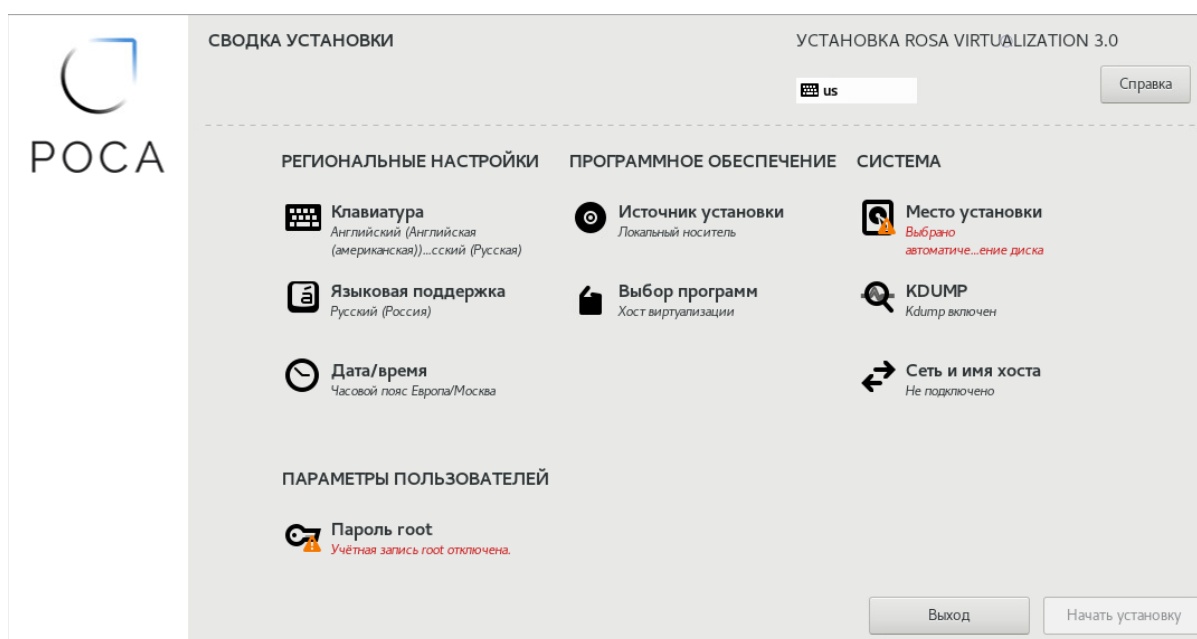


Рисунок 67 - Сводка установки ROSA Virtualization

Под наименованием каждой секции приводится информация о текущих параметрах, настроенных автоматически программой установки.

Нажмите на наименование секции для перехода к интерфейсу настройки соответствующих параметров. После настройки параметров нажмите кнопку **Готово** для возвращения в меню “Сводка установки”.

Следующие секции являются обязательными для настройки параметров установки ОС сервера IPA (Рисунок 67):

- Выбор программ;
- Целевое устройство установки;
- Сеть и имя хоста;
- Пароль root.

В секции “Выбор программ” установите переключатель “Базовое окружение” в положение “**Служба каталогов (функции домена)**” (Рисунок 68) для установки соответствующего базового ПО в систему.

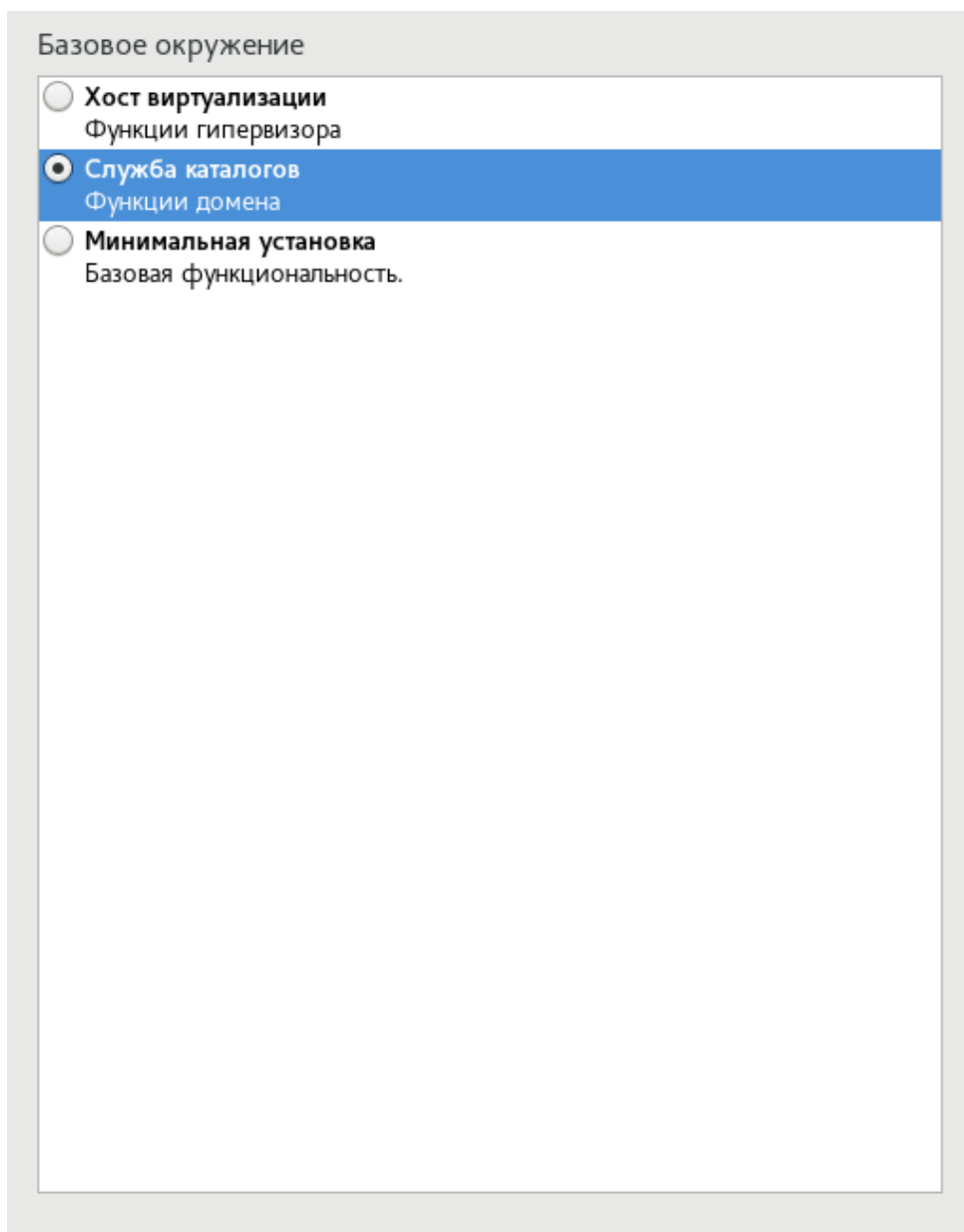


Рисунок 68 - Выбор базового ПО для установки (служба каталогов)

В секции “Целевое устройство установки” выберите необходимый диск и установите переключатель “Конфигурация устройств хранения данных” в положение “Автоматически”.

В секции “Сеть и имя хоста” задайте полное доменное имя сервера IPA (например, `ipa.home.local`), подключите необходимый сетевой интерфейс и настройте параметры сетевого соединения – DHCP или статические значения IP-адреса (например, `192.168.0.74`), маски сети (`255.255.255.0`), шлюза по умолчанию (`192.168.0.1`) и сервера DNS (`192.168.0.1`).

В секции “Пароль root” установите пароль для учетной записи суперпользователя root.

После настройки всех обязательных параметров нажмите кнопку **Начать установку** для старта процесса установки ОС.

После завершения процесса установки нажмите кнопку **Перезагрузка системы**.

На физическом сервере извлеките DVD или USB-накопитель, с которого выполнялась установка, а в настройках ВМ установите приоритет загрузки с жесткого диска.

После перезагрузки ОС, на экране появится строка приглашения командного интерпретатора для входа в систему и дальнейшего выполнения сценария установки и настройки ПО сервера IPA. Вход в систему осуществляется с использованием логина и пароля учетной записи суперпользователя root.

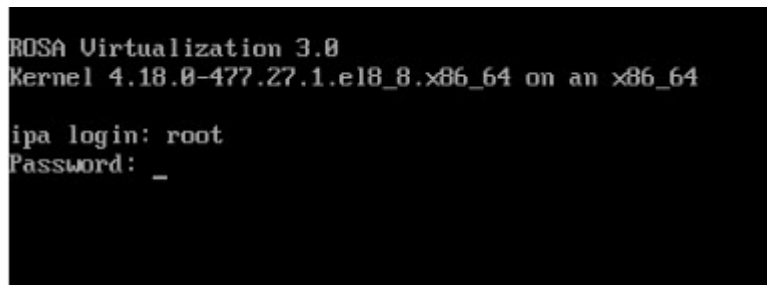


Рисунок 69 - Вход в систему

3.8.3. ВЫПОЛНЕНИЕ СЦЕНАРИЯ УСТАНОВКИ ПО СЕРВЕРА IPA

Установка и настройка ПО сервера IPA осуществляется консольной утилитой (сценарием установки) ipa-server-install.

Примечание – Сценарий установки ipa-server-install создает файл журнала /var/log/ipaserver-install.log. В случае неудачной установки можно просмотреть записи журнала для выявления проблемы в процессе установки.

3.8.3.1. РЕКОМЕНДОВАННАЯ КОНФИГУРАЦИЯ ДЛЯ УСТАНОВКИ СЕРВЕРА IPA

Рекомендуется установить сервер IPA со встроенной службой DNS и со встроенным центром сертификации CA в качестве корневого удостоверяющего центра, что является значением по умолчанию.

3.8.3.2. ЗАПУСК СЦЕНАРИЯ УСТАНОВКИ СЕРВЕРА IPA

Для запуска интерактивного сценария установки сервера IPA осуществите вход в систему от имени учетной записи суперпользователя root и выполните следующую консольную команду:

```
# ipa-server-install

The log file for this installation can be found in /var/log/ipaserver-
install.log
=====
=====

This program will set up the IPA Server.
Version 4.9.11

This includes:
  * Configure a stand-alone CA (dogtag) for certificate management
  * Configure the NTP client (chronyd)
```

- * Create and configure an instance of Directory Server
- * Create and configure a Kerberos Key Distribution Center (KDC)
- * Configure Apache (httpd)
- * Configure SID generation
- * Configure the KDC to enable PKINIT

To accept the default shown in brackets, press the Enter key.

Сценарий установки выведет справочную информацию о действиях, которые будут выполнены, а затем предложит настроить встроенную службу DNS.

Для подтверждения согласия настройки встроенной службы DNS введите yes:

```
Do you want to configure integrated DNS (BIND)? [no]: yes
```

Далее, сценарий установки предложит определенные значения по умолчанию для следующих параметров:

- имя хоста сервера IPA (host name),
- имя домена (domain name),
- имя области Kerberos (realm name):

```
Server host name [ipa.home.local]:  
Please confirm the domain name [home.local]:  
Please provide a realm name [HOME.LOCAL]:
```

Чтобы принять предложенные значения по умолчанию, нажмите клавишу **Enter**.

Для изменения параметра по умолчанию введите необходимое значение, соответствующее установке в вашем ЦОД, и затем нажмите клавишу **Enter**.

Примечание – Указанные выше имя хоста сервера IPA, имя домена и имя области Kerberos являются примером, при установке их необходимо заменить на используемые в организации.

Установите (введите и подтвердите) пароли для суперпользователя службы каталогов LDAP (Directory Manager) и для пользовательской административной учетной записи admin сервера IPA (IPA admin):

```
Certain directory server operations require an administrative user.  
This user is referred to as the Directory Manager and has full access  
to the Directory for system management tasks and will be added to the  
instance of directory server created for IPA.  
The password must be at least 8 characters long.
```

```
Directory Manager password:
```

```
Password (confirm):
```

```
The IPA server requires an administrative user, named 'admin'.  
This user is a regular system account used for IPA server administration.
```

```
IPA admin password:
```

```
Password (confirm):
```

Далее, сценарий установки предложит настроить перенаправление DNS:

```
Do you want to configure DNS forwarders? [yes]:
```

Если перенаправление DNS конфигурировать не нужно, введите no.

Для настройки перенаправления DNS нажмите клавишу **Enter** или введите yes. Сценарий установки запросит и затем добавит IP-адреса средств перенаправления в файл /etc/named.conf.

Пример:

```
Do you want to configure DNS forwarders? [yes]: no
```

```
No DNS forwarders configured
```

Далее, сценарий установки предложит проверить, нужно ли настроить какие-либо обратные записи DNS для IP-адресов, связанных с сервером IPA. Для подтверждения нажмите клавишу **Enter** или введите yes:

```
Do you want to search for missing reverse zones? [yes]:
```

Если в результате поиска будут обнаружены отсутствующие обратные зоны, сценарий установки спросит, нужно ли создать обратные зоны для соответствующих обратных записей DNS. Для подтверждения нажмите клавишу **Enter**:

```
Do you want to create reverse zone for IP 192.168.0.74 [yes]:
```

```
Please specify the reverse zone name [0.168.192.in-addr.arpa.]:
```

```
Using reverse zone(s) 0.168.192.in-addr.arpa.
```

Далее, сценарий установки предложит настроить доменное имя NetBIOS.

```
Trust is configured but no NetBIOS domain name found, setting it now.
```

```
Enter the NetBIOS name for the IPA domain.
```

```
Only up to 15 uppercase ASCII letters, digits and dashes are allowed.
```

```
Example: EXAMPLE.
```

```
NetBIOS domain name [HOME]:
```

Введите доменное имя NetBIOS, для подтверждения нажмите клавишу **Enter**.

Опционально вы можете также настроить сервер NTP (NTP server) или пул адресов точного времени.

```
Do you want to configure chrony with NTP server or pool address? [no]:
```

Сценарий установки выведет в консоль выбранные параметры настройки сервера IPA.

```
The IPA Master Server will be configured with:
```

```
Hostname:          ipa.home.local
```

```
IP address(es): 192.168.0.74
```

```
Domain name:      home.local
```

```
Realm name:       HOME.LOCAL
```

```
The CA will be configured with:
```

```
Subject DN:       CN=Certificate Authority,O=HOME.LOCAL
```

```
Subject base:     O=HOME.LOCAL
```

```
Chaining:         self-signed
```

```
BIND DNS server will be configured to serve IPA domain with:
```

```
Forwarders:       No forwarders
```

```
Forward policy:   only
```

```
Reverse zone(s):  No reverse zone
```

Для подтверждения всех сделанных настроек конфигурации сервера IPA введите **yes**:

```
Continue to configure the system with these values? [no]: yes
```

Сценарий приступит к установке ПО сервера IPA в соответствии с заданной конфигурацией.

После завершения установки ПО сервера IPA, на экране появится соответствующее сообщение, а также сценарий установки порекомендует сделать резервную копию сертификата центра сертификации CA и убедиться в том, что требуемые сетевые порты сервера IPA открыты для входящих соединений.

```
. . .  
Configured /etc/sss/sss.conf  
Systemwide CA database updated.  
Adding SSH public key from /etc/ssh/ssh_host_rsa_key.pub  
Adding SSH public key from /etc/ssh/ssh_host_gost2012_256_key.pub  
Adding SSH public key from /etc/ssh/ssh_host_ecdsa_key.pub  
Adding SSH public key from /etc/ssh/ssh_host_gost2001_key.pub  
Adding SSH public key from /etc/ssh/ssh_host_ed25519_key.pub
```

```
Adding SSH public key from /etc/ssh/ssh_host_gost2012_512_key.pub
SSSD enabled
Configured /etc/openldap/ldap.conf
Configured /etc/ssh/ssh_config
Configured /etc/ssh/sshd_config
Configuring rosa.lan as NIS domain.
Client configuration complete.
The ipa-client-install command was successful
```

```
=====
=====
```

Setup complete

Next steps:

1. You must make sure these network ports are open:

TCP Ports:

- * 80, 443: HTTP/HTTPS
- * 389, 636: LDAP/LDAPS
- * 88, 464: kerberos
- * 53: bind

UDP Ports:

- * 88, 464: kerberos
- * 53: bind
- * 123: ntp

2. You can now obtain a kerberos ticket using the command: 'kinit admin'

This ticket will allow you to use the IPA tools (e.g., ipa user-add) and the web user interface.

Be sure to back up the CA certificates stored in /root/cacert.p12
These files are required to create replicas. The password for these files is the Directory Manager password
The ipa-server-install command was successful

3.8.3.3. ИНИЦИАЛИЗАЦИЯ УЧЕТНОЙ ЗАПИСИ АДМИНИСТРАТОРА СЕРВЕРА IPA

Для получения тикета Kerberos для учетной записи администратора admin необходимо выполнить команду `kinit` с указанием принципала. `kinit` получает и кэширует начальный билет на выдачу билетов для принципала.

Выполните в консоли сервера IPA команду:

```
# kinit admin
```

для получения тикета Kerberos для учетной записи администратора admin. Далее необходимо подтвердить полномочия администратора, введя его пароль.

Пример:

```
# kinit admin
Password for admin@HOME.LOCAL:
```

ПРОВЕРКА УЧЕТНОЙ ЗАПИСИ АДМИНИСТРАТОРА

Для проверки корректной работы сервера и наличия учетной записи администратора используйте команду `ipa user-find admin`, которая осуществляет поиск нужного пользователя и вывод базовых параметров этой учетной записи.

Пример:

```
# ipa user-find admin
-----
установлено соответствие 1 пользователя
-----

Имя учётной записи пользователя: admin
Фамилия: Administrator
Домашний каталог: /home/admin
Оболочка входа: /bin/bash
Псевдоним учётной записи: admin@ROSA.LAN, root@ROSA.LAN
UID: 1645000000
ID группы: 1645000000
Учётная запись отключена: False
-----
Количество возвращённых записей 1
-----
```

В данном примере была обнаружена учетная запись admin, учетная запись включена (не заблокирована).

Примечание – Если при выполнении запроса к серверу IPA выводится сообщение об ошибке вида:

```
# ipa user-find n.petrov
ipa: ERROR: Срок действия билета истек
```

то необходимо обновить тикет Kerberos, выполнив команду `kinit admin` и подтвердить полномочия вводом пароля администратора.

Для проверки наличия действительных (валидных) тикетов Kerberos можно использовать команду `klint`:

```
# klist
Ticket cache: KCM:0
Default principal: admin@ROSA.LAN

Valid starting      Expires            Service principal
13.08.2024 18:48:43  14.08.2024 18:12:29  HTTP/vmipa.rosa.lan@ROSA.LAN
13.08.2024 18:45:31  14.08.2024 18:12:29  krbtgt/ROSA.LAN@ROSA.LAN
```

`Default principal` — принципал, используемый по умолчанию

`Valid starting` — дата и время, начиная с которого начинает действовать тикет Kerberos

`Expires` — дата и время окончания срока действия тикета Kerberos

`Service principal` — принципал службы (ресурс, к которому предоставляется доступ)

Для добавления новых пользователей в каталог пользователей сервера IPA вы можете воспользоваться консольной утилитой

```
# ipa user-add
```

или использовать веб-интерфейс сервера IPA (Рисунок 72).

ПАРАМЕТРЫ КОМАНДЫ ДОБАВЛЕНИЯ НОВОГО ПОЛЬЗОВАТЕЛЯ

Для получения списка актуальных параметров при добавлении нового пользователя можно использовать команду `ipa user-add --help`:

```
# ipa user-add --help
Usage: ipa [global-options] user-add LOGIN [options]

Добавить нового пользователя.
Options:
  -h, --help            show this help message and exit
```

--first=STR	Имя
--last=STR	Фамилия
--cn=STR	Полное имя
--displayname=STR	Отображаемое имя
--initials=STR	Инициалы
--homedir=STR	Домашний каталог
--gecos=STR	GECOS
--shell=STR	Оболочка входа
--principal=PRINCIPAL	Псевдоним учётной записи
--principal-expiration=DATETIME	Окончание действия учётной записи Kerberos
--password-expiration=DATETIME	Окончание действия пароля пользователя
--email=STR	Адрес электронной почты
--password	Запросить пароль у пользователя
--random	Создать случайный пользовательский пароль
--uid=INT	ID пользователя (если не указан, система назначит его самостоятельно)
--gidnumber=INT	ID группы
--street=STR	Адрес
--city=STR	Город
--state=STR	Область/республика
--postalcode=STR	Индекс
--phone=STR	Номер телефона
--mobile=STR	Номер мобильного телефона
--pager=STR	Номер пейджера
--fax=STR	Номер факса
--orgunit=STR	Отдел
--title=STR	Должность
--manager=STR	Руководитель
--carlicense=STR	Номер автомобиля
--sshpubkey=STR	Открытый ключ SSH
--user-auth-type=['password', 'radius', 'otp', 'pkinit', 'hardened', 'idp']	Поддерживаемые типы аутентификации пользователей
--class=STR	Категория пользователей (семантика этого атрибута предназначена для локального разбора)
--radius=STR	Конфигурация прокси RADIUS
--radius-username=STR	Имя пользователя прокси RADIUS
--idp=STR	External IdP configuration
--idp-user-id=STR	A string that identifies the user at external IdP

```
--departmentnumber=STR
                                Номер отдела
--employeenumber=STR  Номер сотрудника
--employeeetype=STR   Тип сотрудника
--preferredlanguage=STR
                                Предпочитаемый язык
--certificate=CERTIFICATE
                                Base-64 зашифрованный сертификат пользователя
--setattr=STR          Установить атрибут для пары имя/значение. Формат:
                                атрибут=значение. Если атрибут многозначный, команда
                                заменяет уже присутствующие значения.
--addattr=STR          Добавить пару атрибут/значение. Формат:
                                атрибут=значение. Атрибут должен быть частью схемы.
--noprivatе           Не создавать личную группу пользователя
--all                 Получить и вывести все атрибуты, возвращаемые
                                сервером. Влияет на содержимое результата исполнения
                                команды.
--raw                 Вывести записи в том виде, в котором они хранятся на
                                сервере. Влияет только на формат вывода данных.
--no-members          Подавить обработку атрибутов участия.
```

Пример добавления нового пользователя с логином a.ivanov, именем Александр, фамилией Иванов и отображаемым именем Александр Иванов.

```
# ipa user-add a.ivanov \
--first="Александр" \
--last="Иванов" \
--displayname="Александр Иванов"
```

По умолчанию пользователь будет добавлен в группу ipausers.

```
# ipa user-add a.ivanov \
> --first="Александр" \
> --last="Иванов" \
> --displayname="Александр Иванов"
-----
Добавлен пользователь "a.ivanov"
-----
Имя учётной записи пользователя: a.ivanov
```

```
Имя: Александр
Фамилия: Иванов
Полное имя: Александр Иванов
Отображаемое имя: Александр Иванов
Инициалы: АИ
Домашний каталог: /home/a.ivanov
GECOS: Александр Иванов
Оболочка входа: /bin/sh
Имя учётной записи: a.ivanov@ROSA.LAN
Псевдоним учётной записи: a.ivanov@ROSA.LAN
Адрес электронной почты: a.ivanov@rosa.lan
UID: 1645000003
ID группы: 1645000003
Пароль: False
Участник групп: ipausers
Доступные ключи Kerberos: False
```

Поле

```
Участник групп: ipausers
```

показывает, что данный пользователь был добавлен в группу ipausers.

Примечание – В примере выше новый пользователь с логином `a.ivanov` был добавлен в каталог пользователей, без указания пароля и срока окончания действия пароля. Для возможности успешного входа в систему должен быть задан пароль учетной записи, и указан срок окончания действия пароля с датой/временем, которые наступят позднее.

ДОБАВЛЕНИЕ ИЛИ СМЕНА ПАРОЛЯ ПОЛЬЗОВАТЕЛЯ

Для добавления или смены пароля пользователя необходимо использовать команду `ipa user-mod user_name --password`, где `user_name` — это имя пользователя.

Пример:

```
# ipa user-mod a.ivanov --password
Пароль:
Введите Пароль ещё раз для проверки:
-----
Изменён пользователь "a.ivanov"
-----
Имя учётной записи пользователя: a.ivanov
Имя: Александр
```

```
Фамилия: Иванов
Домашний каталог: /home/a.ivanov
Оболочка входа: /bin/sh
Имя учётной записи: a.ivanov@ROSA.LAN
Псевдоним учётной записи: a.ivanov@ROSA.LAN
Адрес электронной почты: a.ivanov@rosa.lan
UID: 1645000003
ID группы: 1645000003
Учётная запись отключена: False
Пароль: True
Участник групп: ipausers
Доступные ключи Kerberos: True
```

После запуска команды появится подсказка:

```
Пароль:
```

после которой необходимо указать требуемый (желаемый) пароль пользователя.

Затем появится подсказка:

```
Введите Пароль ещё раз для проверки:
```

и после неё необходимо повторно указать пароль пользователя (для проверки правильности введенного ранее пароля).

При условии что оба введенных после подсказок пароля совпадают, пароль для пользователя будет изменён.

Информация в выводе на терминал:

```
Пароль: True
```

говорит о том, что пароль был успешно создан (изменён).

ИЗМЕНЕНИЯ СРОКА ДЕЙСТВИЯ ПАРОЛЯ ПОЛЬЗОВАТЕЛЯ

Для изменения срока действия пароля пользователя необходимо использовать команду `ipa user-mod user_name --password-expiration`, где `user_name` — это имя пользователя:

Укажите дату/время окончания действия пароля в формате год-месяц-число час:минута:секунда, так чтобы дата и время окончания срока действия учетной записи наступали позднее текущего момента. Например, можно указать дату +3 месяца от текущей даты.

Пример:

```
# ipa user-mod a.ivanov --password-expiration='2024-11-19 12:00:00Z'
-----
```

Изменён пользователь "a.ivanov"

Имя учётной записи пользователя: a.ivanov
Имя: Александр
Фамилия: Иванов
Домашний каталог: /home/a.ivanov
Оболочка входа: /bin/sh
Имя учётной записи: a.ivanov@ROSA.LAN
Псевдоним учётной записи: a.ivanov@ROSA.LAN
Окончание действия пароля пользователя: 20241119120000Z
Адрес электронной почты: a.ivanov@rosa.lan
UID: 1645000003
ID группы: 1645000003
Учётная запись отключена: False
Пароль: True
Участник групп: ipausers
Доступные ключи Kerberos: True

В данном примере *Окончание действия пароля пользователя* - 20241119120000Z (год 2024, месяц 11, число 19, время 12:00, 00 секунд)

Окончание действия пароля пользователя: 20241119120000Z

ИЗМЕНЕНИЯ СРОКА ДЕЙСТВИЯ ПАРОЛЯ ПОЛЬЗОВАТЕЛЯ С ПОМОЩЬЮ ПОЛЯ KRBPASSWORDEXPIRATION

Для изменения срока действия пароля пользователя с помощью модификации поля `krbPasswordExpiration` необходимо использовать команду `ipa user-mod user_name --setattr=krbPasswordExpiration`, где `user_name` — это имя пользователя:

Укажите дату/время окончания действия пароля в формате год-месяц-число-час-минуты-секунды (без дефисов, как в примере ниже):

20250817010000Z - год 2025, месяц 08, число 17, время 01:00, 00 секунд

```
# ipa user-mod n.petrov --setattr=krbPasswordExpiration=20250817010000Z
```

Изменён пользователь "n.petrov"

Имя учётной записи пользователя: n.petrov
Имя: Николай
Фамилия: Петров

```
Домашний каталог: /home/n.petrov
Оболочка входа: /bin/sh
Имя учётной записи: n.petrov@ROSA.LAN
Псевдоним учётной записи: n.petrov@ROSA.LAN
Окончание действия пароля пользователя: 20250817010000Z
Адрес электронной почты: n.petrov@rosa.lan
UID: 1645000005
ID группы: 1645000005
Учётная запись отключена: False
Пароль: True
Участник групп: ipausers
Доступные ключи Kerberos: True
```

ПРОВЕРКИ ДАТЫ И ВРЕМЕНИ ОКОНЧАНИЯ СРОКА ДЕЙСТВИЯ ПАРОЛЯ УЧЕТНОЙ ЗАПИСИ ПОЛЬЗОВАТЕЛЯ

Для проверки даты и времени окончания срока действия пароля учетной записи пользователя используйте команду `ipa user-show user_name --all --raw`, где `user_name` — имя пользователя, и далее фильтр по атрибуту `krbPasswordExpiration`.

Пример 1:

```
# ipa user-show a.ivanov --all --raw | grep krbPasswordExpiration
krbPasswordExpiration: 20241119120000Z
```

Значение поля `krbPasswordExpiration` соответствует дате и времени окончания срока действия пароля учетной записи.

20241119120000Z - год 2024, месяц 11, число 19, время 12:00, 00 секунд

Пример 2:

```
# ipa user-show n.petrov --all --raw | grep krbPasswordExpiration
krbPasswordExpiration: 20250817010000Z
```

20250817010000Z - год 2025, месяц 08, число 17, время 01:00, 00 секунд

ПРОВЕРКА НАЛИЧИЯ ПОЛЬЗОВАТЕЛЯ В КАТАЛОГЕ IPA

Для проверки наличия пользователя в каталоге IPA необходимо выполнить в консоли команду `ipa user-find`.

Если пользователь отсутствует в каталоге, то будет выведено сообщение, что пользователь не найден:

```
# ipa user-find n.petrov
-----
установлено соответствие 0 пользователей
-----
-----
Количество возвращённых записей 0
-----
```

Если пользователь присутствует в каталоге, то будет выведено сообщение с параметрами учетной записи пользователя:

```
# ipa user-find a.ivanov
-----
установлено соответствие 1 пользователя
-----
Имя учётной записи пользователя: a.ivanov
Имя: Александр
Фамилия: Иванов
Домашний каталог: /home/a.ivanov
Оболочка входа: /bin/sh
Имя учётной записи: a.ivanov@ROSA.LAN
Псевдоним учётной записи: a.ivanov@ROSA.LAN
Адрес электронной почты: a.ivanov@rosa.lan
UID: 1645000003
ID группы: 1645000003
Учётная запись отключена: False
-----
Количество возвращённых записей 1
-----
```

Альтернативным способом запроса данных пользователя из каталогов IP является утилита `ldapsearch`. Для проверки наличия пользователя в каталоге или запроса параметров учетной записи пользователя выполните команду `ldapsearch -x uid=<идентификатор пользователя>`, где идентификатор пользователя — это уникальный идентификатор пользователя в системе (UID):

```
# ldapsearch -x uid=a.ivanov
# extended LDIF
#
# LDAPv3
# base <dc=rosa,dc=lan> (default) with scope subtree
```

```
# filter: uid=a.ivanov
# requesting: ALL
#

# a.ivanov, users, compat, rosa.lan
dn: uid=a.ivanov,cn=users,cn=compat,dc=rosa,dc=lan
objectClass: posixAccount
objectClass: ipaOverrideTarget
objectClass: top
gecos:: 0JDQu9C10LrRgdCw0L3QtNGAINCY0LLQsNC90L7Qsg==
cn:: 0JDQu9C10LrRgdCw0L3QtNGAINCY0LLQsNC90L7Qsg==
uidNumber: 1645000003
gidNumber: 1645000003
loginShell: /bin/sh
homeDirectory: /home/a.ivanov
ipaAnchorUUID::
OklQQTPyb3NhLmxhbjpmMDlhZDczMi0lOThlLTExZWYtYmJhZi01MjU0MDAxZD
gyMTY=
uid: a.ivanov

# a.ivanov, users, accounts, rosa.lan
dn: uid=a.ivanov,cn=users,cn=accounts,dc=rosa,dc=lan
givenName:: 0JDQu9C10LrRgdCw0L3QtNGA
sn:: 0JjQstCw0L3QvtCy
uid: a.ivanov
cn:: 0JDQu9C10LrRgdCw0L3QtNGAINCY0LLQsNC90L7Qsg==
displayName:: 0JDQu9C10LrRgdCw0L3QtNGAINCY0LLQsNC90L7Qsg==
initials:: 0JDQmA==
gecos:: 0JDQu9C10LrRgdCw0L3QtNGAINCY0LLQsNC90L7Qsg==
objectClass: top
objectClass: person
objectClass: organizationalperson
objectClass: inetorgperson
objectClass: inetuser
objectClass: posixaccount
objectClass: krbprincipalaux
objectClass: krbticketpolicyaux
objectClass: ipaobject
objectClass: ipasshuser
```

```
objectClass: ipaSshGroupOfPubKeys
objectClass: mepOriginEntry
objectClass: ipantuserattrs
loginShell: /bin/sh
homeDirectory: /home/a.ivanov
uidNumber: 1645000003
gidNumber: 1645000003
ipaNTSecurityIdentifier: S-1-5-21-2240628588-3245565648-2467509467-1003

# search result
search: 2
result: 0 Success

# numResponses: 3
# numEntries: 2
```

Если в каких-либо полях учетной записи используется русский алфавит, то вывод значения данного поля будет закодирован в кодировке base64.

Например, в выводе в консоли выше поле `displayName` закодировано в кодировке base64.

```
displayName:: 0JDQu9C10LrRgdCw0L3QtNGAINCY0LLQsNC90L7Qsg==
```

Для декодирования содержимого поля (и его последующей проверки) в командной строке можно использовать утилиту `base64`.

Пример:

```
# echo "0JDQu9C10LrRgdCw0L3QtNGAINCY0LLQsNC90L7Qsg==" | base64 --decode
Александр Иванов
```

В данном случае содержимое поля `displayName` («отображаемое имя») декодируется как «Александр Иванов».

Также для декодирования кодировки base64 можно использовать утилиту `openssl`.

Пример:

```
# openssl enc -base64 -d <<< "0JDQu9C10LrRgdCw0L3QtNGAINCY0LLQsNC90L7Qsg=="
Александр Иванов
```

Содержимое поля `displayName` («отображаемое имя») декодируется как «Александр Иванов».

3.8.3.4. НАСТРОЙКА МЕЖСЕТЕВОГО ЭКРАНА ДЛЯ СЕРВЕРА IPA

Для открытия необходимых портов сервера IPA в зоне default службы межсетевого экрана firewalld выполните следующую консольную команду:

```
# firewall-cmd --permanent --add-port={80/tcp,443/tcp,389/tcp,\
636/tcp,88/tcp,88/udp,464/tcp,464/udp,53/tcp,53/udp,123/udp}
```

Список требуемых портов для сервера IPA

Служба	Порты модуля	Протокол
HTTP/HTTPS	80, 443	TCP
LDAP/LDAPS	389, 636	TCP
Kerberos	88, 464	TCP и UDP
DNS	53	TCP и UDP
NTP	123	UDP

Примечание – Не следует беспокоиться о том, что сервер IPA использует порты 80 и 389.

- Порт 80 (HTTP) используется для предоставления откликов протокола проверки статуса сертификата (OCSP) и списков аннулирования сертификатов (CRL). Обе программы имеют цифровую подпись и поэтому защищены от атак через посредника (man-in-the-middle).
- Порт 389 (LDAP) использует STARTTLS и GSSAPI для шифрования.

Для применения изменений перезагрузите конфигурацию межсетевого экрана. Для этого выполните следующую консольную команду:

```
# firewall-cmd --reload
```

После установки ПО сервера IPA и настройки межсетевого экрана станет доступным вход в веб-интерфейс управления сервером IPA.

Для проверки статуса работы межсетевого экрана firewalld выполните команду:

```
# systemctl status firewalld.service
• firewalld.service - firewalld - dynamic firewall daemon
   Loaded: loaded (/usr/lib/systemd/system/firewalld.service; enabled; vendor preset: enabled)
   Active: active (running) since Thu 2024-08-15 17:45:08 MSK; 22min ago
     Docs: man:firewalld(1)
  Main PID: 984 (firewalld)
    Tasks: 2 (limit: 10659)
   Memory: 41.6M
    CGroup: /system.slice/firewalld.service
```

```
└─984 /usr/bin/python3.6 -s /usr/sbin/firewalld --nofork --nopicd
```

```
авр 15 17:45:07 vmipa.rosa.lan systemd[1]: Starting firewalld - dynamic firewall daemon...
```

```
авр 15 17:45:08 vmipa.rosa.lan systemd[1]: Started firewalld - dynamic firewall daemon.
```

```
авр 15 17:45:08 vmipa.rosa.lan firewalld[984]: WARNING: AllowZoneDrifting is enabled. This is considered an insecure
```

Статус Active: active (running) говорит о том, что межсетевой экран активен.

3.8.4. ВХОД В ВЕБ-ИНТЕРФЕЙС СЕРВЕРА IPA

Для доступа к веб-интерфейсу введите в адресной строке браузера (на внешней рабочей станции) доменное имя или IP-адрес сервера IPA.

Например:

```
https://ipa.home.local
```

На экране появится окно авторизации интерфейса (Рисунок 70).

Примечание – Первичный вход в интерфейс управления сервером IPA осуществляется от имени учетной записи администратора admin. Предварительно необходимо получить тикет Kerberos для учетной записи admin, выполнив в консоли команду:

```
# kinit admin
```

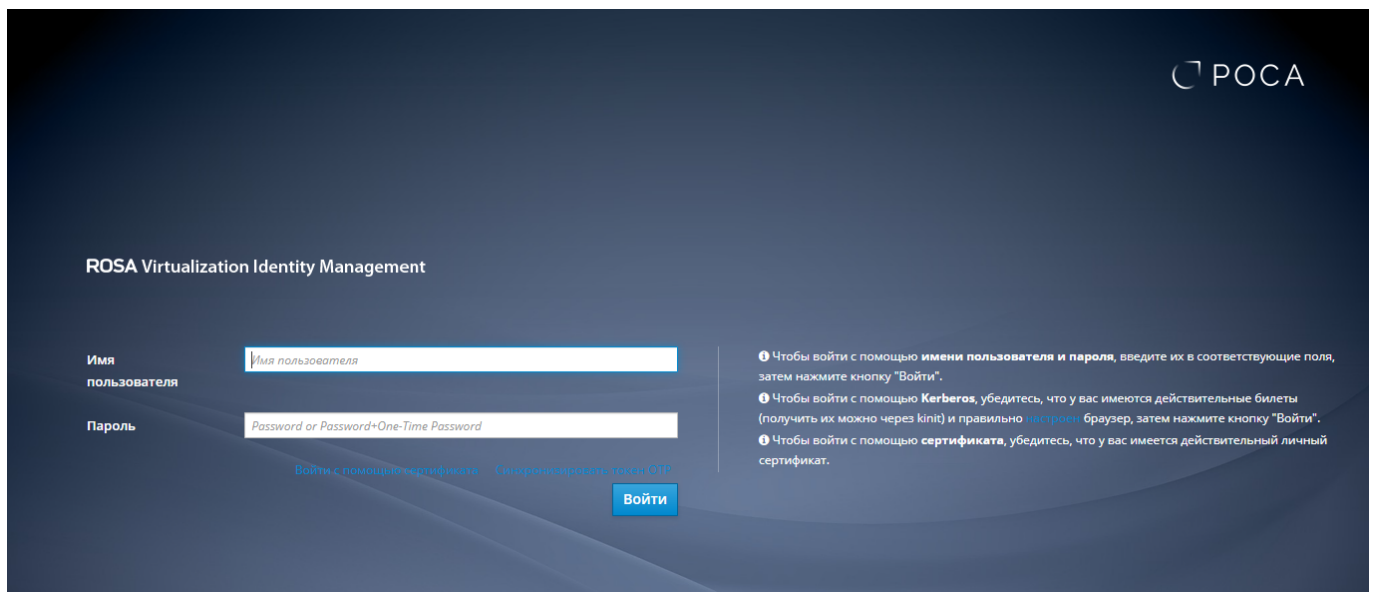


Рисунок 70 - Окно авторизации интерфейса управления сервером IPA

Для входа в интерфейс введите имя (логин) и пароль пользователя в соответствующие поля, после чего нажмите кнопку **Войти**.

После входа в веб-интерфейс сервера IPA будет отображена панель управления сервером IPA. По умолчанию будет открыта вкладка **Идентификация** → **Активные пользователи** (Рисунок 71).

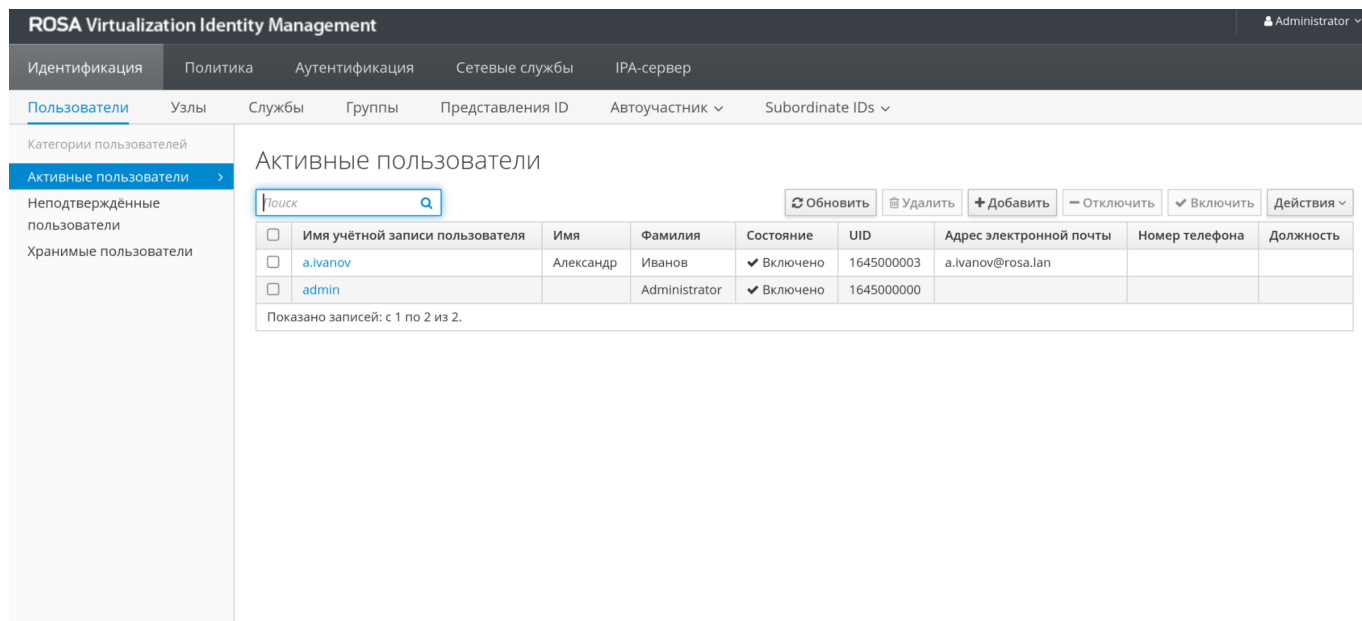


Рисунок 71. Веб-интерфейс сервера IPA — вкладка Идентификация → Активные пользователи

Если вы уже добавили каких-либо пользователей в каталог IPA, используя интерфейс командной строки, то эти пользователи будут отображены в списке активных пользователей (Рисунок 71).

3.9. ПОДКЛЮЧЕНИЕ ROSA VIRTUALIZATION К СЛУЖБЕ КАТАЛОГОВ LDAP СЕРВЕРА IPA

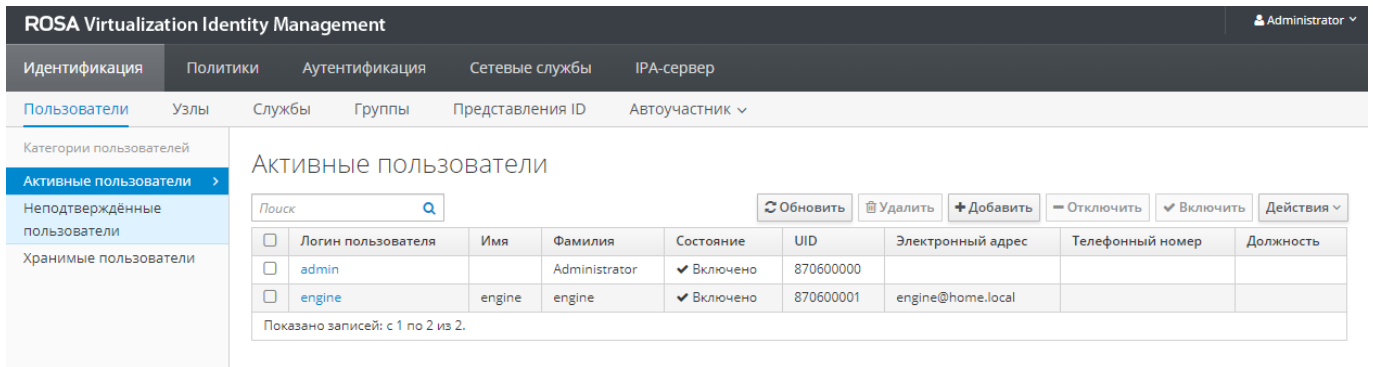
Процедура подключения ROSA Virtualization к службе каталогов LDAP сервера IPA состоит из создания служебной учетной записи пользователя для выполнения запросов поиска в каталоге LDAP и входа на сервер IPA, а также из создания профиля подключения для идентификации и аутентификации доменных пользователей.

- Создание служебной учетной записи пользователя осуществляется в интерфейсе управления сервером IPA.
- Создание профиля подключения осуществляется в консоли СУСВ.

3.9.1. СОЗДАНИЕ СЛУЖЕБНОЙ УЧЕТНОЙ ЗАПИСИ ПОЛЬЗОВАТЕЛЯ С ИСПОЛЬЗОВАНИЕМ ВЕБ-ИНТЕРФЕЙСА

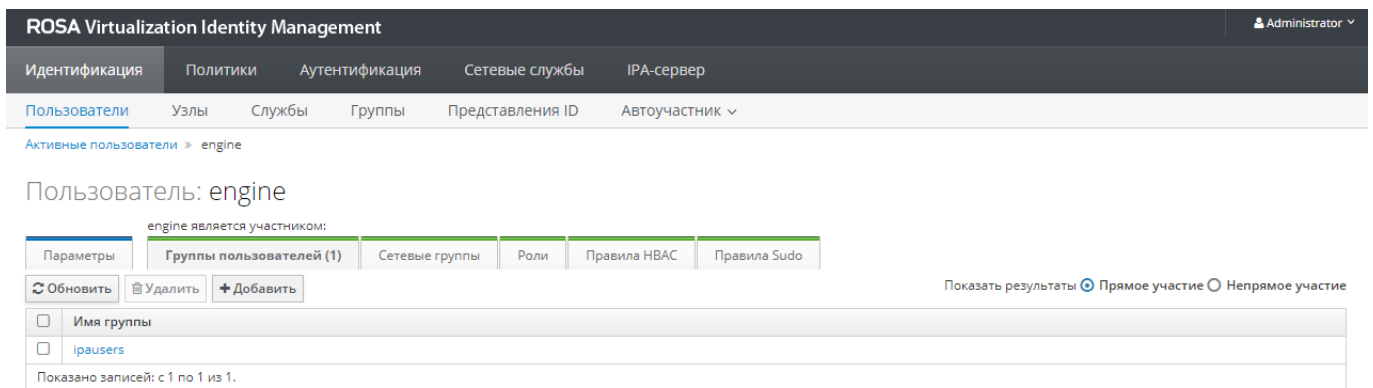
Для создания учетной записи пользователя выполните вход в интерфейс управления сервером IPA от имени учетной записи администратора admin.

В разделе “Идентификация” и в меню “Пользователи” выберите пункт “Активные пользователи”. На экране появится соответствующая страница интерфейса, содержащая список активных пользователей (Рисунок 72).



Нажмите кнопку **Добавить** и задайте логин для нового пользователя (например, engine).

Для добавления пользователя в группы admins и editors нажмите на ссылку с именем пользователя и в открывшемся меню с параметрами перейдите на вкладку “Группы пользователей” (Рисунок 73).



Нажмите кнопку **Добавить**. Откроется окно с интерфейсом выбора групп для пользователя (Рисунок 74).

Добавить пользователя 'engine' в группы пользователей

Доступный фильтр Группы пользователей

Доступно

☐	Имя группы
☐	admins
☐	editors
☐	trust admins

Ожидается

☐	Имя группы
--------------------------	------------

Добавить
Отменить

Рисунок 74 - Интерфейс выбора групп

В списке “Доступно” установите соответствующие флажки для выбора групп admins и editors. Нажмите кнопку переноса . В списке “Ожидается” появятся наименования выбранных групп (Рисунок 75).

Добавить пользователя 'engine' в группы пользователей

Доступный фильтр Группы пользователей

Доступно

☐	Имя группы
☐	trust admins

Ожидается

☐	Имя группы
☐	admins
☐	editors

Добавить
Отменить

Рисунок 75 - Выбор групп admins и editors

Для завершения процедуры выбора групп нажмите кнопку **Добавить** (Рисунок 75).

Для установки пароля новому пользователю перейдите на вкладку “Параметры” и из выпадающего списка, вызываемого нажатием кнопки **Действия**, выберите пункт “Сбросить пароль”.

В поля “Новый пароль” и “Проверить пароль” открывшегося окна “Сбросить пароль” соответственно введите и подтвердите пароль для нового пользователя (Рисунок 76).

Рисунок 76 - Ввод и подтверждение пароля

ИЗМЕНЕНИЯ СРОКА ДЕЙСТВИЯ ПАРОЛЯ СЕРВИСНОЙ УЧЕТНОЙ ЗАПИСИ

Для изменения срока действия пароля пользователя необходимо использовать команду `ipa user-mod user_name --password-expiration`, где `user_name` — это имя пользователя сервисной учетной записи:

Укажите дату/время окончания действия пароля в формате год-месяц-число час:минута:секунда, так чтобы дата и время окончания срока действия учетной записи наступали позднее текущего момента. Например, можно указать дату +3 месяца от текущей даты.

Пример:

```
# ipa user-mod susvengine --password-expiration='2024-11-19 12:00:00Z'
-----
Изменён пользователь "susvengine"
-----
Имя учётной записи пользователя: susvengine
Имя: susv
Фамилия: susv
Домашний каталог: /home/susvengine
Оболочка входа: /bin/sh
Имя учётной записи: susvengine@ROSA.LAN
Псевдоним учётной записи: susvengine@ROSA.LAN
Окончание действия пароля пользователя: 20241119120000Z
Адрес электронной почты: susvengine@rosa.lan
UID: 1645000004
ID группы: 1645000004
Учётная запись отключена: False
Пароль: True
Участник групп: editors, ipausers, admins
Доступные ключи Kerberos: True
```

В данном примере *Окончание действия пароля пользователя* - 20241119120000Z (год 2024, месяц 11, число 19, время 12:00, 00 секунд)

Окончание действия пароля пользователя: 20241119120000Z

Для проверки даты и времени окончания срока действия пароля учетной записи можно воспользоваться следующей командой:

```
# ipa user-show susvengine --all --raw | grep krbPasswordExpiration
krbPasswordExpiration: 20241119120000Z
```

Значение поля `krbPasswordExpiration` соответствует дате и времени окончания срока действия пароля учетной записи.

3.9.2. СОЗДАНИЕ ПРОФИЛЯ ПОДКЛЮЧЕНИЯ К СЛУЖБЕ КАТАЛОГОВ LDAP СЕРВЕРА IPA

Настройка подключения ROSA Virtualization к службе каталогов LDAP сервера IPA осуществляется утилитой `ovirt-engine-extension-aaa-ldap-setup` в консоли СУСВ.

Примечание – Для подключения к консоли СУСВ по SSH выполните следующую команду с указанием доменного имени (например, `vm.home.local`) или IP-адреса ВМ СУСВ, а также пароля учетной записи суперпользователя `root` ВМ СУСВ при выводе на экран соответствующего запроса:

```
# ssh root@vm.home.local
root@vm.home.local's password:
```

3.9.2.1. ЗАПУСК ИНТЕРАКТИВНОГО СЦЕНАРИЯ НАСТРОЙКИ ПОДКЛЮЧЕНИЯ ROSA VIRTUALIZATION К СЛУЖБЕ КАТАЛОГОВ LDAP

Для запуска интерактивного сценария настройки и создания профиля подключения с целью идентификации и аутентификации доменных пользователей выполните в консоли СУСВ следующую команду:

```
# ovirt-engine-extension-aaa-ldap-setup
```

Сценарий настройки предложит выбрать тип реализации сервера LDAP из пронумерованного списка. Для выбора **сервера IPA** введите цифру **6**:

```
Available LDAP implementations:
1 - 389ds
2 - 389ds RFC-2307 Schema
3 - Active Directory
4 - IBM Security Directory Server
5 - IBM Security Directory Server RFC-2307 Schema
6 - IPA
7 - Novell eDirectory RFC-2307 Schema
8 - OpenLDAP RFC-2307 Schema
9 - OpenLDAP Standard Schema
10 - Oracle Unified Directory RFC-2307 Schema
```

```
11 - RFC-2307 Schema (Generic)
12 - RHDS
13 - RHDS RFC-2307 Schema
14 - iPlanet
Please select: 6
```

Далее, сценарий настройки предложит использовать разрешение имени DNS для сервера IPA.

- Если в сети используется сервер DNS, нажмите клавишу **Enter** или введите Yes.
- При отсутствии в сети сервера DNS введите No:

```
Use DNS (Yes, No) [Yes]: No
```

Примечание – При отсутствии в сети сервера DNS доменные имена и IP адреса хостов, СУСВ и сервера IPA должны быть указаны в файле `/etc/hosts` сервера IPA, а также на хостах ROSA Virtualization, и СУСВ. Отредактируйте файл `/etc/hosts` на каждом из перечисленных выше хостов и серверов, указав актуальные доменные имена и IP адреса.

Из пронумерованного списка выберите метод реализации политики службы DNS. При выборе варианта 1 (Single server) введите IP-адрес сервера IPA:

```
Available policy method:
1 - Single server
2 - DNS domain LDAP SRV record
3 - Round-robin between multiple hosts
4 - Failover between multiple hosts
Please select: 1
Please enter host address: 192.168.0.74
```

Примечание – Указанный в выводе консоли выше IP адрес 192.168.0.74 является примером, необходимо указать IP адрес, соответствующий серверу IPA, установленному в вашем ЦОДе.

Далее, сценарий настройки предложит выбрать протокол подключения к каталогу LDAP, а также указать отличительное имя и пароль пользователя для выполнения запросов поиска в каталоге LDAP. Введите значение `plain` для выбора протокола и следующие атрибуты ранее созданной служебной записи пользователя:

```
Please select protocol to use (startTLS, ldaps, plain) [startTLS]:
plain
Enter search user DN (for example uid=username,dc=example,dc=com or leave
empty for anonymous):
uid=engine,cn=users,cn=compat,dc=home,dc=local
Enter search user password:
```

Примечание – Пример выше предполагает, что на сервере IPA, управляющим доменом `home.local`, была создана служебная учетная запись `engine` с отличительным именем (dn) `uid=engine,cn=users,cn=compat,dc=home,dc=local`.

Отличительное имя (уникальное имя) dn - это имя, уникальным образом идентифицирующее каждую запись каталога. При вводе параметров в сценарий установки используйте отличительное имя служебной учетной записи, созданной ранее на сервере IPA для выполнения синхронизации с ROSA Virtualization.

Для проверки корректности указанного отличительного имени dn используйте на сервере IPA в командной строке следующую команду:

```
# ipa user-show engine --all --raw | grep dn:
dn: uid=engine,cn=users,cn=accounts,dc=home,dc=local
```

Далее, сценарий настройки предложит определенные значения по умолчанию для следующих параметров:

```
Please enter base DN (dc=home,dc=local) [dc=home,dc=local]:
Are you going to use Single Sign-On for Virtual Machines (Yes, No) [Yes]:
```

Чтобы принять предложенные значения по умолчанию, нажмите клавишу **Enter**.

Сценарий настройки предложит указать имя для профиля подключения. Введите наименование профиля (например, RV):

```
Please specify profile name that will be visible to users: RV
```

Примечание – Данный профиль будет использоваться для входа в Портал администрирования и Портал VM ROSA Virtualization (Рисунок 77).

Для тестовой проверки подключения укажите имя и пароль ранее созданной служебной записи пользователя (в примере ниже учетная запись имеет имя `engine`):

```
Please provide credentials to test login flow
Enter user name: engine
Enter user password:
```

Сценарий настройки приступит к созданию профиля подключения в соответствии с заданной конфигурацией.

3.9.2.2. ПЕРЕЗАГРУЗКА СЛУЖБЫ OVIRT-ENGINE:

После завершения процедуры создания профиля выполните перезагрузку службы `ovirt-engine`:

```
# systemctl restart ovirt-engine
```

В результате созданный профиль подключения RV станет доступен для выбора в окне авторизации при входе на Портал администрирования СУСВ (Рисунок 77) или на Портал VM.

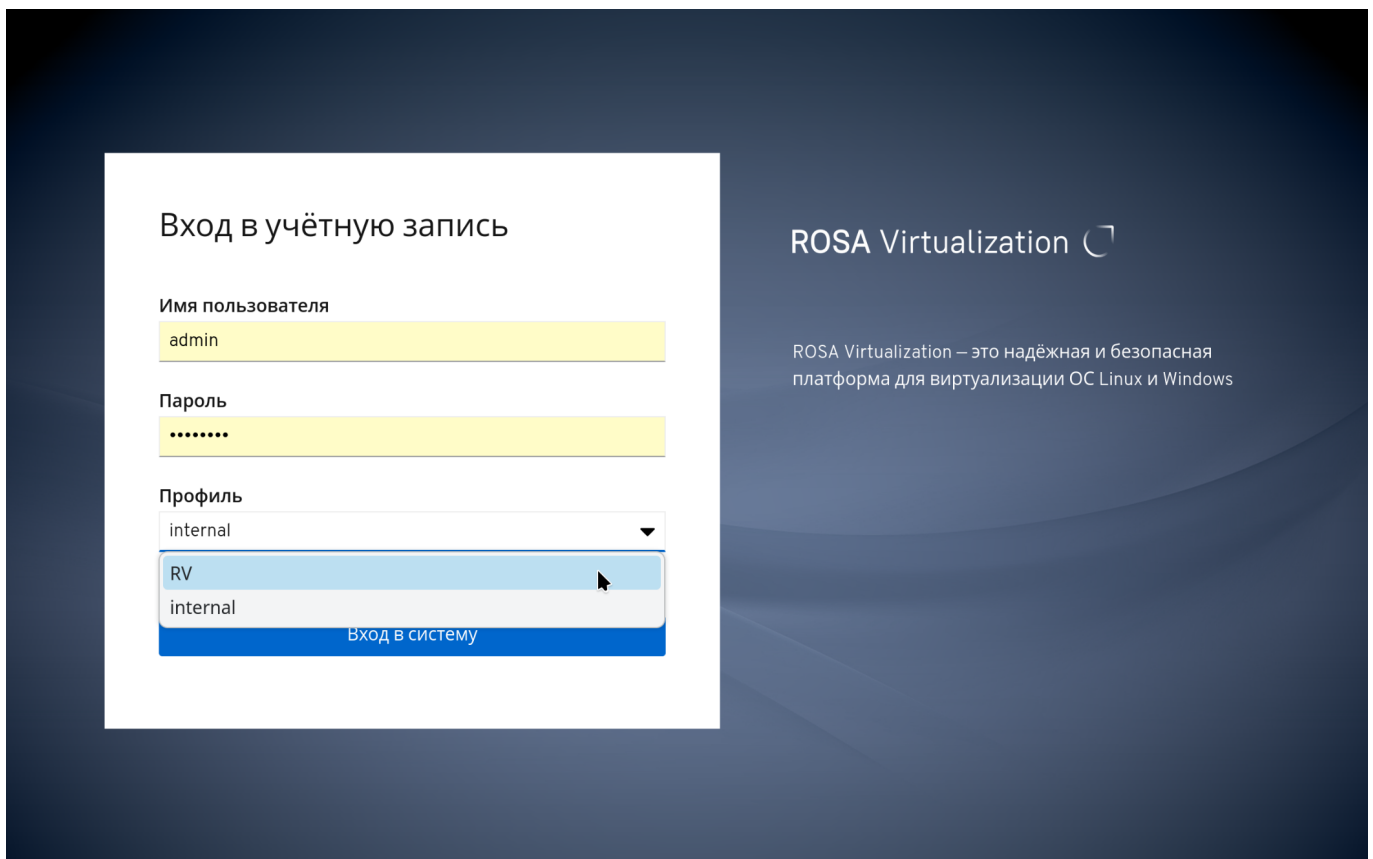


Рисунок 77. Выбор профиля подключения RV в окне авторизации при входе на портал администрирования СУСВ

3.9.2.3. ПРЕДОСТАВЛЕНИЕ ПРАВ ДОСТУПА К РЕСУРСАМ ROSA VIRTUALIZATION ДЛЯ ПОЛЬЗОВАТЕЛЕЙ СЕРВЕРА IPA

Назначение необходимых прав доступа к ресурсам ROSA Virtualization для новых созданных пользователей сервера IPA осуществляется на Портале администрирования СУСВ.

Для доступа к списку пользователей выберите пункт “Администрирование → Пользователи” в главном меню СУСВ. Для редактирования параметров пользователя нажмите на ссылку с именем пользователя.

☰ ROSA Virtualization

Панель мониторинга

Ресурсы

Сеть

Хранилище

Администрирование

Дополнения

События

Администрирование > Пользователи

users:type = user

Добавить Удалить Назначить теги

Пользователь Группа

Имя	Фамилия	Имя пользователя	Поставщик авторизац	Пространство имён	Почтовый адрес
admin		admin	internal-authz	*	admin@localhost
engine	engine	engine	RV	dc=home,dc=local	engine@home.local
mega	odmin	megaadmin	RV	dc=home,dc=local	megaadmin@home.lo...

Рисунок 78 - Список пользователей в форме Администрирование → Пользователи веб-консоли СУСВ

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

Сокращение	Определение
ВМ	Виртуальная машина
ВЦОД	Виртуальный центр обработки данных
ОЗУ	Оперативное запоминающее устройство
ОС	Операционная система
ПО	Программное обеспечение
СУБД	Система управления базами данных
СУСВ	Система управления средой виртуализации
ФСТЭК	Федеральная служба по техническому и экспортному контролю
ЦП	Центральный процессор
ЦУ	Центр управления
BIOS	Basic input / output system – базовая система ввода / вывода
CA	Certification authority – центр сертификации (удостоверяющий центр)
CPU	Central processing unit – центральный процессор
DHCP	Dynamic host configuration protocol – протокол динамической настройки узла
DN	Distinguished Name - имя, уникальным образом идентифицирующее каждую запись каталога LDAP
DNS	Domain name system – система доменных имен
DVD	Digital versatile disc – цифровой многоцелевой диск
FAT	File allocation table – таблица размещения файлов
FCoE	Fibre channel over Ethernet – протокол Fibre Channel, работающий поверх Ethernet
FQDN	Fully qualified domain name – полное доменное имя
GPT	GUID partition table – формат размещения таблиц разделов на диске
GRUB	Grand unified bootloader – унифицированный загрузчик операционной системы
IP	Internet protocol – протокол межсетевого взаимодействия
IPA	Identity, policy and audit – система идентификации и аутентификации пользователей, задания политик доступа и аудита
iSCSI	Internet small computer system interface – версия протокола SCSI, базирующаяся на TCP/IP
JBOD	Just a bunch of disks – массив дисков
LDAP	Lightweight directory access protocol – протокол доступа к каталогам
LUKS	Linux unified key setup – спецификация формата шифрования дисков
LVM	Logical volume management – менеджер логических томов
MBR	Master boot record – главная загрузочная запись
NFS	Network file sharing – протокол сетевого доступа к файловым системам
NTP	Network time protocol – протокол сетевого времени
NVDIMM	Non-volatile dual inline memory module – энергонезависимый двойной

Сокращение	Определение
	встроенный модуль памяти
RAID	Redundant array of independent disks – избыточный массив независимых дисков
SAN	Storage area network – сеть хранения данных
SP	Service pack – пакет обновления программного обеспечения
SSH	Secure shell – защищенная оболочка
UEFI	Unified extensible firmware interface – унифицированный расширяемый интерфейс базового программного обеспечения
USB	Universal serial bus – универсальная последовательная шина
VFAT	Virtual file allocation table – виртуальная таблица размещения файлов
VLAN	Virtual local area network – виртуальная локальная вычислительная сеть

[illegible]