



**БАЗИС.VCONTROL**  
**РУКОВОДСТВО ПО УСТАНОВКЕ**  
Версия 2.2.1

## Оглавление

1. Введение .....	6
1.1 Описание системы Базис.vControl .....	6
1.2 Список используемых сокращений и терминов .....	6
2. Архитектура решения .....	11
2.1 Описание компонентов в архитектуре Базис.vControl .....	11
2.1.1 Бэкенд.....	11
2.1.2 Менеджер агентов (Agent Manager) .....	12
2.1.3 Websocket Server .....	12
2.1.4 Агент .....	12
2.1.5 Хранилище метрик.....	12
2.2 Сетевое взаимодействие компонентов .....	13
3. Требования к программному и аппаратному обеспечению .....	19
3.1 Бэкенд и Фронтенд Базис.vControl .....	20
3.2 PostgreSQL .....	20
3.3 Redis (HA-установка на отдельных хостах) .....	20
3.4 ClickHouse (HA-установка на отдельных хостах) .....	21
3.5 Сервер развертывания (в случае HA-установки) .....	21
3.6 Хосты P-Виртуализации .....	21
3.7 Другие требования.....	23
4. Требования к сетевому взаимодействию .....	24
5. Требования к информационной безопасности .....	25
5.1 Настройка межсетевого экрана.....	25
5.2 Системные учетные записи для работы компонентов продукта .....	25
6. Установка Базис.vControl .....	26
6.1 Подготовка серверов для установки компонентов Базис.vControl .....	26
6.1.1 Подготовка шаблона виртуальной машины для установки компонентов Базис.vControl.....	26
6.1.2 Инсталляция ОС Альт .....	29
6.1.3 Инсталляция Astra Linux.....	35
6.1.4 Дополнительные действия по настройке .....	54
6.1.5 Клонирование VM из шаблона .....	55

# Базис.vControl. Руководство по установке

---

6.2	Установка в конфигурации без отказоустойчивости (не-HA режим).....	56
6.2.1	Установка Бэкенда и Фронтенда Базис.vControl.....	57
6.3	Установка в конфигурации с отказоустойчивостью (HA-режим).....	68
6.3.1	Установка Сервера развертывания.....	69
6.3.2	Пример настройки внешнего сервера Postgres 12 на Альт 9.....	80
6.3.3	Установка Redis-кластера.....	82
6.3.4	Установка ClickHouse-кластера.....	84
6.3.5	Установка Бэкенда и Фронтенда Базис.vControl.....	86
7.	Начало работы.....	88
7.1	Вход в Базис.vControl.....	88
8.	Система хранения данных.....	90
8.1	Импорт кластера ПК Р-Хранилище.....	90
9.	Управление кластерами.....	95
9.1	Создание кластера в Базис.vControl.....	96
10.	Управление хостами.....	101
10.1	Добавление/удаление хоста в кластере обычного типа.....	101
11.	Синхронизация с Active Directory.....	106
12.	Шаблоны и образы.....	108
12.1	Настройки хранилища шаблонов.....	110
12.2	Настройки хранилища образов дисков.....	115
13.	Смена TLS-сертификата для доступа к веб-интерфейсу.....	120
13.1	Конфигурация без отказоустойчивости (не-HA режим).....	120
13.2	Конфигурация с отказоустойчивостью (HA-режим).....	120
14.	Смена IP-адреса сервера Базис.vControl.....	121
14.1	В конфигурации без отказоустойчивости (не-HA режим).....	121
14.2	В конфигурации с отказоустойчивостью (HA-режим).....	121
15.	Обновление Базис.vControl.....	123
15.1	Подготовка репозитория для обновления компонентов Базис.vControl.....	123
15.2	Обновление Бэкенда Базис.vControl.....	123
15.2.1	В конфигурации с отказоустойчивостью (HA-режим).....	123
15.2.2	В конфигурации без отказоустойчивости (не-HA-режим).....	124

15.3	Обновление агентов Базис.vControl.....	125
15.3.1	Возможные проблемы при обновлении агентов .....	125
16.	Приложение.....	126
16.1	Технические учетные записи.....	126
16.1.1	Учетная запись в Базис.vControl, под которой Базис.WorkPlace будет подключаться к API Базис.vControl .....	126
16.2	Поддержка зашифрованных параметров в конфигурации Базис.vControl .....	128
16.2.1	Смена парольной фразы.....	129
16.3	Использование Syslog .....	130
16.3.1	Пример настройки встроенного Syslog-сервера на ОС Альт .....	131
16.3.2	Пример настройки встроенного Syslog-сервера на Astra Linux.....	131
16.3.3	Настройка передачи событий в Syslog .....	132
16.3.4	Изменение уровня логирования Бэкенда .....	133
16.4	Справочник по параметрам конфигурации системы.....	134
16.4.1	Правила редактирования конфигурационных файлов .....	136
16.4.2	Деактивация/активация суперпользователя .....	137
16.4.3	Параметры конфигурации для Бэкенда Базис.vControl.....	138
16.4.4	Параметры конфигурации для Агента Базис.vControl .....	140
16.5	Настройка включения SSO-авторизации в систему.....	141
16.5.1	Настройки в контроллере домена.....	142
16.5.2	Настройки в Бэкенде Базис.vControl.....	143
16.5.3	Настройки в веб-интерфейсе Базис.vControl .....	144
16.5.4	Настройки на сервере развертывания .....	144
16.5.5	Настройки для браузера.....	145
16.5.6	Проверка работы SSO-авторизации .....	146
16.6	Сценарии использования API Базис.vControl.....	147
16.6.1	Добавление открытого SSH-ключа через HTTP API .....	147
16.6.2	Получение статуса компонентов Базис.vControl .....	148
16.7	Поддерживаемые версии PostgreSQL .....	152

17. Ссылки на цитируемые документы ..... 154

## 1. ВВЕДЕНИЕ

### 1.1 Описание системы Базис.vControl

**Базис.vControl** — это простая и гибкая система управления и мониторинга среды виртуализации, работающая на базе **ПК Р-Платформа**.

**Базис.vControl** позволяет управлять гипервизорами **Р-Виртуализации**, виртуальными средами и сетями, размещенными на физических серверах.

Также в рамках единого веб-интерфейса **Базис.vControl** обеспечивает работу подсистемы **Базис.WorkPlace**, которая позволяет создавать и управлять виртуальными рабочими столами.

### 1.2 Список используемых сокращений и терминов

Таблица 1.1 Список используемых сокращений и терминов

Термин	Описание
Ansible	Средство автоматизации установки и настройки ПО по сценариям, описываемым в нотации YAML
База данных, БД	База данных PostgreSQL. Может использоваться сторонний кластер СУБД PostgreSQL. Хранит информацию об инфраструктуре системы.
Балансировщик нагрузки	Программное или аппаратное решение для распределения нагрузки входящих подключений между несколькими узлами сервиса
Виртуальная машина, VM	Программа, которая эмулирует реальный (физический) компьютер со всеми его компонентами (жесткий диск, DVD-ROM, BIOS, сетевые адаптеры и т.д.). Как правило, VM содержит установленную операционную систему и компоненты среды виртуализации (гостевые утилиты, драйверы эмулируемых устройств)
Виртуальное рабочее место, BPM, рабочий стол	Полностью подготовленная для работы виртуальная машина с установленной на ней целевой операционной системой и прикладным ПО, необходимым для выполнения задач. BPM включает компонент Агент BPM и взаимодействует через него с

## Базис.vControl. Руководство по установке

Термин	Описание
	инфраструктурой ВРМ для подключения назначенного пользователя.
Виртуальная среда, ВС	Виртуальная среда — общее именование виртуальных машин и контейнеров виртуализации в Базис.vControl
Базис.vControl	Система управления и мониторинга платформы виртуализации
Базис.WorkPlace, VDI	Система для создания и управления инфраструктурой виртуальных рабочих столов, которые используются для работы на предприятии.
Базис.vControl, VMS	Система, позволяющая управлять различными сервисами Базис.vControl и расширяющая их функциональность
Диск	Жесткий диск хоста или ВМ
Хост, хост виртуализации	Физический сервер, на котором установлено программное обеспечение системы виртуализации (гипервизор)
Agent Manager, Менеджер агентов	Сервис, осуществляющий взаимодействие с агентами, запущенными на физических серверах с установленной системой виртуализации (гипервизором)
API	Программный интерфейс приложения, набор способов и правил для взаимодействия программ между собой
Carbon-Clickhouse	Сервис, отвечающий за хранение метрик в Clickhouse
Clickhouse	Столбцовая система управления базами данных (СУБД) для онлайн-обработки аналитических запросов
CIFS	Стандартный протокол, который обеспечивает доступ к файлам и сервисам на удаленных компьютерах (в том числе и в Интернет). Протокол использует клиент-серверную модель взаимодействия
CIFS-Server	Сервер, предоставляющий доступ к хранилищу данных по протоколу CIFS
CPU	Вычислительное ядро процессора хоста или ВМ

## Базис.vControl. Руководство по установке

Термин	Описание
Deploy-vControl	Сервер развертывания Базис.vControl
DHCP	Протокол, присваивающий компьютерам сетевые опции (маска сети или подсети, адрес DNS-сервера, шлюз, IP-адрес, время (NTP))
DHCP-Server	Сервер, поддерживающий протокол DHCP
HA, HA-кластер	High Availability — высокая доступность, характеристика технической системы, позволяющая снизить риски сбоев, а также минимизировать время плановых простоев. HA-кластер — тип кластера с высокой доступностью
ISC-DHCP-Server	Программа-сервер, обеспечивающая передачу клиентам сведений необходимых для работы в сети TCP/IP
Kerberos	Сетевой протокол аутентификации, позволяющий передавать данные через незащищённые сети для безопасной идентификации. Ориентирован, в первую очередь, на клиент-серверную модель и обеспечивает взаимную аутентификацию — оба пользователя через сервер подтверждают личности друг друга
LDAP, Active Directory, AD, FreeIPA, SambaDC	Служба каталогов пользователей для хранения учетных записей и аутентификации
LDAP-Server	Сервер, обслуживающий службы каталогов пользователей. LDAP-сервер принимает входящие соединения по протоколам TCP или UDP
nginx	Программное обеспечение с открытым исходным кодом, позволяющее создавать веб-сервер. Используется как почтовый сервер или обратный прокси-сервер
NTP	Сетевой протокол для синхронизации внутренних часов компьютера с использованием сетей с переменной латентностью
NTP server	Сервер обслуживания сетевого протокола NTP, применяемого для синхронизации внутренних часов компьютера с использованием сетей с переменной латентностью



Термин	Описание
NFS	Протокол сетевого доступа к файловым системам, за основу взят протокол вызова удалённых процедур (ONC RPC), позволяет монтировать (подключать) удалённые файловые системы через сеть
NFS-Server	Сервер обслуживания сетевого протокола NFS, применяемого для разделения файловых ресурсов путём сетевого доступа к файловым системам
OpenStack	Комплекс проектов свободного программного обеспечения, который может быть использован для создания инфраструктурных облачных сервисов и облачных хранилищ
OpenStackController	Контроллер вычислительных ресурсов, который передает команды гипервизору и управляет виртуальными машинами
PostgreSQL	СУБД из списка поддерживаемых для Базис.vControl: <ul style="list-style-type: none"><li>▪ Postgres Pro 9.6,</li><li>▪ Postgres Pro Enterprise Certified 10.3,</li><li>▪ Postgres Pro Standard Certified 11.5,</li><li>▪ Postgres Pro Enterprise 11.6,</li><li>▪ PostgreSQL 9.5,</li><li>▪ PostgreSQL 9.6,</li><li>▪ Jatoba.</li></ul> Подробнее список описан в разделе приложения <a href="#">Поддерживаемые версии PostgreSQL</a>
Python	Язык программирования
RAM	Оперативная память хоста или VM
Redis	Резидентная система управления базами данных класса NoSQL с открытым исходным кодом, работающая со структурами данных типа «ключ — значение»
Redis-Sentinel	Сервис, обеспечивающий высокую доступность (HA) Базы данных Redis
SSHD	Программа-сервер, обслуживающая запросы программы-клиента ssh

Термин	Описание
SysLog	Протокол для отправки сообщений о событиях на сервер регистрации
SysLog-Server	Сервер регистрации входящих сообщений по протоколу Syslog
TCP	Сетевой протокол передачи данных интернета, предназначенный для управления передачей данных
UDP	Сетевой протокол с использованием пользовательских датаграмм, позволяет компьютерным приложениям посылать сообщения (датаграммы) другим хостам по IP-сети без необходимости предварительного сообщения для установки специальных каналов передачи или путей данных
uwsgi	Веб-сервер и сервер веб-приложений, реализованный для запуска приложений Python через протокол WSGI (и его бинарный вариант uwsgi).
VRRP	Virtual Router Redundancy Protocol — сетевой протокол, предназначенный для увеличения доступности маршрутизаторов, выполняющих роль шлюза по умолчанию
WebSocket	Протокол связи поверх TCP-соединения, предназначенный для обмена сообщениями между браузером и веб-сервером, используя постоянное соединение
YAML	Формат сериализации данных, близкий к языкам разметки, но ориентированный на удобство ввода-вывода структур данных большинства языков программирования

## 2. АРХИТЕКТУРА РЕШЕНИЯ

Таблица 2.1 содержит список компонентов **Базис.vControl**.

Таблица 2.1 Список компонентов Базис.vControl

Название компонента	Назначение
База данных	Хранение информации о виртуальных ресурсах (виртуальные машины, сети), пользователях, группах, ролях, а также информации о физических серверах, входящих в кластер, событиях, алертах и т.д.
Бэкенд	Основное приложение, реализующее управление платформой Базис.vControl. Служит для обеспечения REST API для Фронтенда Базис.vControl, взаимодействует с агентами, выполняет периодические задачи
Агент	Запускается на управляемых хостах (физических серверах). Управляет гипервизором и ОС, запускает стандартные Linux-команды, а также осуществляет мониторинг состояния сервера и гипервизора
Хранилище метрик	Хранение значений метрик для хостов и ВС. Метрики напрямую отправляют агенты, установленные на хостах
Кэш-хранилище	Хранение пользовательских сессий. Кэш для скриншотов ВС
Фронтенд	Реализация WebUI, запускается в браузере пользователя. Статические файлы отдаются nginx

**Бэкенд Базис.vControl**, далее Бэкенд, предоставляет RESTful HTTP API для работы **Фронтенда Базис.vControl** по протоколу HTTPS. Агент общается с **Бэкендом Базис.vControl** через TLS-туннель с помощью средств CurveZMQ.

### 2.1 Описание компонентов в архитектуре Базис.vControl

#### 2.1.1 Бэкенд

Сервис, предоставляющий клиентам возможность управлять платформой виртуализации через протокол REST.

## 2.1.2 Менеджер агентов (Agent Manager)

**Менеджер агентов** осуществляет взаимодействие с агентами, запущенными на физических серверах с установленной системой **Р-Виртуализация**. Двухсторонний протокол взаимодействия между **Менеджером агентов** и агентами управления (далее **Агенты**), установленными на хостах, построен поверх ZeroMQ.

## 2.1.3 Websocket Server

Модуль обеспечивает двухстороннюю связь между **Бэкендом** и **Фронтом** **Базис.vControl**. После **авторизации пользователя** Фронтенд **Базис.vControl\*\*** устанавливает соединение с **WebSocket Server**, чтобы получать сообщения обо всех изменениях на **Бэкенде Базис.vControl**.

## 2.1.4 Агент

При запуске **Агент** устанавливает соединение с **Менеджером агентов** и ждет команды. Также агент служит для отправки уведомлений об изменении окружения операционной системы, **Р-Виртуализации**, запуска/остановки виртуальных сред и данных контроля состояний (мониторинга) хоста и ВС.

При обрыве соединения **Агент** пытается пересоздать соединение. Для проверки соединения **Агент** с равным интервалом посылает heartbeat-сообщения. При пропуске нескольких сообщений подряд **Менеджер агентов** определяет, что **Агент** недоступен, и устанавливает статус, что сервер недоступен, а также создает соответствующее уведомление.

**Агент** использует следующие интерфейсы для управления виртуальной инфраструктурой:

- Р-Виртуализация SDK — основной интерфейс взаимодействия с гипервизором;
- libvirt — интерфейс используется для работы с пробросом физических устройств в ВС и для взаимодействия с QEMU-агентом;
- shell — команды управления, исполняемые в консоли сервера;
- vstorage — управление и мониторинг **ПК Р-Хранилище**;
- vstorage-iscsi — управление iSCSI-ресурсами и **ПК Р-Хранилище**;
- NetworkManager — управление сетевой инфраструктурой хоста.

## 2.1.5 Хранилище метрик

**Хранилище метрик** построено на основе БД ClickHouse.

**Агент** на каждом хосте раз в минуту получает значения метрик с использованием SDK **Р-Виртуализации** и посылает полученные значения напрямую в хранилище метрик, которое в качестве бэкенда для хранения использует БД ClickHouse.



## Базис.vControl. Руководство по установке

Источник (машина)	Служба/приложение источника	Назначение (машина)	Служба/приложение источника	Протокол	Порт	Использование
						программных пакетов
vControl Бэкенд	aptyumdnf	Deploy_v Control	Nginx	TCP	8888	Доступ к репозиторию с пакетами для установки
vControl Бэкенд		NTP server		UDP	123	Синхронизация времени
vControl Бэкенд	nginx	vControl Бэкенд	WebSocket	TCP	8081	Взаимодействие с API
vControl Бэкенд	nginx	vControl Бэкенд	uwsgi	TCP	9080	Взаимодействие с API
vControl Бэкенд	nginx	vControl Бэкенд	nginx	TCP	80	Доступ к API и WEB
vControl Бэкенд	WebSocket	SysLog	Syslog	UDP	514	Запись логов
vControl Бэкенд	WebSocket	vControl Бэкенд*	Redis	TCP	6379	Доступ к Redis для извлечения/вставки данных, репликации
vControl Бэкенд	WebSocket	vControl Бэкенд*	Redis-sentinel	TCP	5000	Получение информации о Redis мастере, обеспечения HA для Redis
vControl Бэкенд	WebSocket	WorkPlace Бэкенд*	Redis	TCP	6379	Доступ к Redis для извлечения/в

## Базис.vControl. Руководство по установке

Источник (машина)	Служба/приложение источника	Назначение (машина)	Служба/приложение источника	Протокол	Порт	Использование
						ставки данных, репликации
vControl Бэкенд	WebSocket	WorkPlace Бэкенд*	Redis-sentinel	TCP	5000	Получение информации о Redis мастере, обеспечения HA для Redis
vControl Бэкенд	uwsgi	vControl Бэкенд*	Clickhouse	TCP	8123	HTTP-доступ к ClickHouse для извлечения/вставки данных
vControl Бэкенд	uwsgi	vControl Бэкенд*	PostgreSQL	TCP	5432	Доступ к БД PostgreSQL
vControl Бэкенд	uwsgi	vControl Бэкенд*	Redis	TCP	6379	Доступ к Redis для извлечения/вставки данных, репликации
vControl Бэкенд	uwsgi	vControl Бэкенд*	Redis-sentinel	TCP	5000	Получение информации о Redis мастере, обеспечение HA для Redis
vControl Бэкенд	uwsgi	WorkPlace Бэкенд	Nginx	TCP	443	Взаимодействие с API
vControl Бэкенд	uwsgi	vControl Бэкенд	AgentManager	TCP	5501+	Общение между Менеджерам

## Базис.vControl. Руководство по установке

Источник (машина)	Служба/приложение источника	Назначение (машина)	Служба/приложение источника	Протокол	Порт	Использование
						и агентов в случае НА инсталляции
vControl Бэкенд	uwsgi	SysLog	Syslog	UDP	514	Запись логов
vControl Бэкенд	uwsgi	NFS-Server		TCP	2049	Доступ к хранилищу шаблонов и образов
vControl Бэкенд	uwsgi	CIFS-Server		TCP, UDP	139(TCP), 445(TCP), 137(UDP), 138(UDP)	Доступ к хранилищу шаблонов и образов
vControl Бэкенд	uwsgi	LDAP-Server		TCP, UDP	636	Взаимодействие с доменными УЗ
vControl Бэкенд	uwsgi	DHCP-Server	ISC-DHCP-Server	TCP	7911	Фиксация IP адреса для VM
vControl Бэкенд	AgentManager	vControl Бэкенд*	Redis	TCP	6379	Доступ к Redis для извлечения/вставки данных, репликации
vControl Бэкенд	AgentManager	vControl Бэкенд*	Redis-sentinel	TCP	5000	Получение информации о Redis мастере,



## Базис.vControl. Руководство по установке

Источник (машина)	Служба/приложение источника	Назначение (машина)	Служба/приложение источника	Протокол	Порт	Использование
						обеспечения HA для Redis
vControl Бэкенд	AgentManager	vControl Бэкенд*	PostgreSQL	TCP	5432	Доступ к БД PostgreSQL
vControl Бэкенд	AgentManager	SysLog	Syslog	UDP	514	Запись логов
vControl Бэкенд	AgentManager	Гипервизор	SShd	TCP	22	Для управления
vControl Бэкенд	AgentManager	vmWare	vCenter			Для управления
vControl Бэкенд	AgentManager	OpenStack	OpenStack Controller			Для управления
vControl Бэкенд*	Clickhouse	vControl Бэкенд*	Clickhouse	TCP	9009	Для репликации в HA режиме
vControl Бэкенд*	Clickhouse	vControl Бэкенд*	Clickhouse-keeper	TCP	2181	Для репликации в HA режиме
vControl Бэкенд*	Clickhouse-keeper	vControl Бэкенд*	Clickhouse-keeper	TCP	2888	Для репликации в HA режиме
vControl Бэкенд*	Carbon-Clickhouse	vControl Бэкенд*	Clickhouse	TCP	8123	HTTP-доступ к ClickHouse для извлечения/вставки данных
vControl Бэкенд	nginx	vControl Бэкенд	ws-сервер	TCP	443	Доступ к VNC-консоли ВС

## Базис.vControl. Руководство по установке

Источник (машина)	Служба/приложение источника	Назначение (машина)	Служба/приложение источника	Протокол	Порт	Использование
vControl Бэкенд	ws-сервер	Гипервизор	VNC-сервер	TCP	5900+ + инкремент от кол. ВС	Подключение к VNC-серверу на гипервизоре. Подробнее на рисунке 2.1
Гипервизор	aptumdnf	vControl Бэкенд	nginx	TCP	8888	Доступ к репозиторию с пакетами для установки
Гипервизор	Агент	vControl Бэкенд	AgentManager	TCP	5001+	Управляющие команды (инкремент на каждый дополн. AgentManager)
Гипервизор	Агент	vControl Бэкенд	Clickhouse	TCP	8123	HTTP-доступ к ClickHouse для извлечения/вставки данных
Гипервизор	Агент	vControl Бэкенд	Carbon-Clickhouse	TCP	2003	Отправка метрик

Схема сетевых взаимодействий Базис.vControl с указанием портов приведена в Приложении "Схема сетевых взаимодействий" к настоящему руководству. Приложение оформлено отдельным файлом в формате pdf/png.

### 3. ТРЕБОВАНИЯ К ПРОГРАММНОМУ И АППАРАТНОМУ ОБЕСПЕЧЕНИЮ

Общие требования к программному и аппаратному обеспечению зависят от выбранной конфигурации развертывания Базис.vControl:

- [Установка в конфигурации без отказоустойчивости](#) (обычный режим) — все компоненты системы разворачиваются на одной виртуальной машине.
- Установка в конфигурации с отказоустойчивостью (HA-режим) — для каждого компонента используется своя виртуальная машина. В минимальной конфигурации требуется 3 виртуальные машины.

Общая схема использования виртуальных машин представлена на рисунке 3.1, ниже для каждого компонента перечислены минимальные системные требования для виртуальных машин.

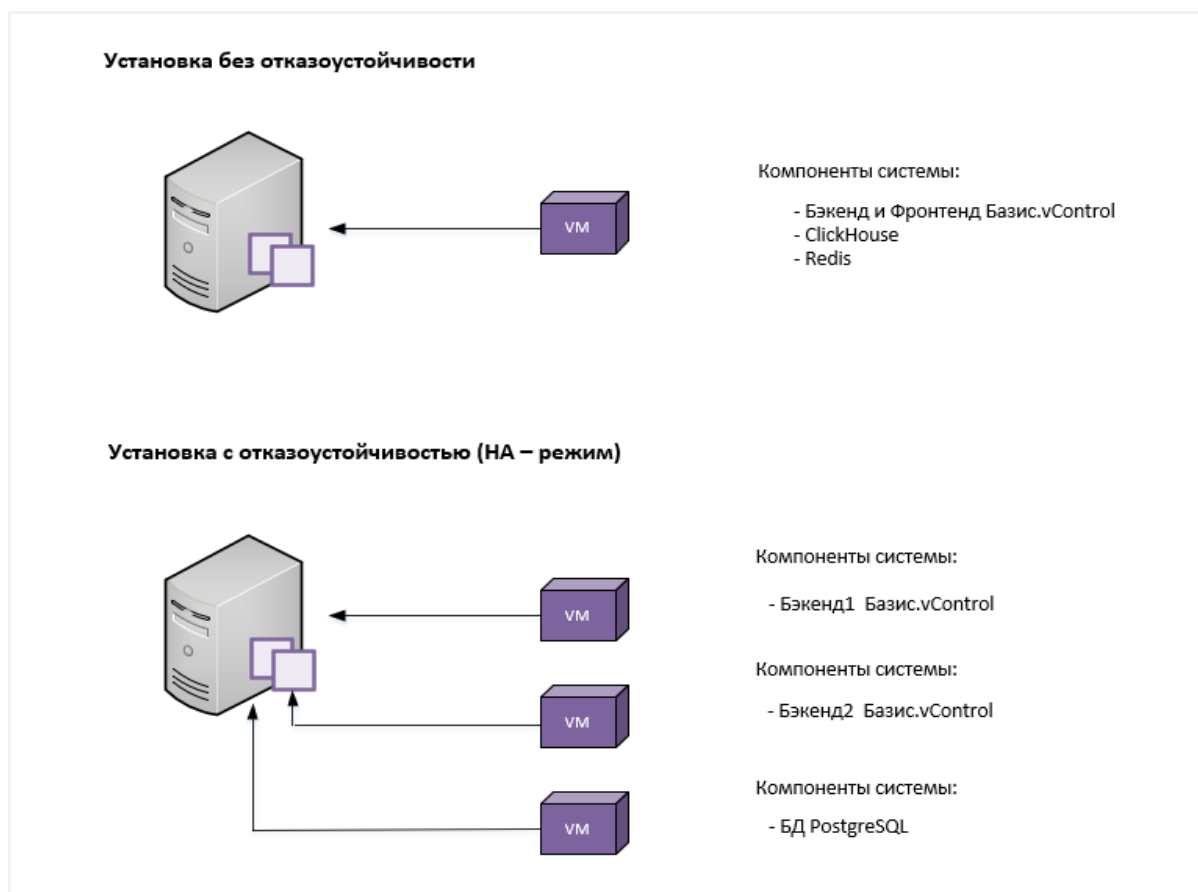


Рисунок 3.1 Использование виртуальных машин в зависимости от конфигурации развертывания Базис.vControl

### 3.1 Бэкенд и Фронтенд Базис.vControl

Система должна функционировать под управлением одной из следующих операционных систем в минимальной установке с systemd:

- Альт 8 СП;
- Альт 9;
- Альт 9.1;
- Альт 10 (установка доступна с версии 10.1);
- Astra Linux версии 1.7.



#### Осторожно

Поддерживаются версии Astra Linux только с установленным обновлением Update 6 ([Бюллетень № 20200722se16](#)).

---

Минимальные системные требования:

- 4 vCPU;
- 10 Гбайт (GB) RAM;
- 100 Гбайт (GB) дискового пространства.

В случае установки **Базис.vControl** не в HA-режиме на виртуальную машину (VM) под управлением **Р-Виртуализации** для обеспечения отказоустойчивости рекомендуется чтобы VM располагалась на хранилище **Р-Хранение** и для нее должен быть включен флаг HA (high availability) с высоким приоритетом.

### 3.2 PostgreSQL

**Базис.vControl** поддерживает СУБД из следующего списка:

- Postgres Pro 9.6;
- Postgres Pro Enterprise Certified 10.3;
- Postgres Pro Standard Certified 11.5;
- Postgres Pro Enterprise 11.6,
- PostgreSQL 9.5,
- PostgreSQL 9.6,
- Jatoba.

Подробнее список с учетом конфигурации развертывания системы описан в разделе приложения [Поддерживаемые версии PostgreSQL](#)

### 3.3 Redis (HA-установка на отдельных хостах)

Требования к операционной системе и ее настройке аналогичны требованиям для установки **Бэкенда** и **Фронтенда Базис.vControl**, за исключением того, что не нужна PostgreSQL.

Минимальные системные требования:

- 1 vCPU;
- 1 Гбайт (GB) RAM;
- 100 Гбайт (GB) дискового пространства.

### 3.4 ClickHouse (HA-установка на отдельных хостах)

Требования к операционной системе и ее настройке аналогичны требованиям для установки **Бэкенда** и **Фронтенда Базис.vControl**, за исключением того, что не нужна PostgreSQL.

Минимальные системные требования:

- 2 vCPU;
- 4 Гбайт (GB) RAM;
- 100 Гбайт (GB) дискового пространства.

### 3.5 Сервер развертывания (в случае HA-установки)

Требования к операционной системе и ее настройке аналогичны требованиям для установки **Бэкенда** и **Фронтенда Базис.vControl**, за исключением того, что не нужна PostgreSQL.

Минимальные системные требования:

- 1 vCPU;
- 1 Гбайт (GB) RAM;
- 100 Гбайт (GB) дискового пространства.

### 3.6 Хосты Р-Виртуализации

Решение **Базис.vControl** предназначено для управления уже установленными и настроенными кластерами виртуализации на базе **Р-Платформа**. Условия для работы:

1. На хостах **Р-Виртуализации** должен быть доступ к стандартным RPM-репозиториям, или же в качестве репозитория должен быть подключен установочный диск **Р-Виртуализации**. Все нестандартные репозитории при установке хоста (и после установки, когда хост уже находится под управлением **Базис.vControl**) должны быть отключены.



### Осторожно

При подключении внешних СХД необходимо обязательно использовать только внешние стандартные репозитории «Росплатформы».

2. (опционально) Настроенный и запущенный кластер **ПК Р-Хранилище**.
3. (опционально) Смонтированные ресурсы **ПК Р-Хранилище** на всех рабочих хостах виртуализации кластера.
4. (опционально) Настроенный и запущенный HA-кластер.
5. Выполненные сетевые настройки всех физических интерфейсов и агрегатов на всех хостах кластера.
6. Выполненные сетевые настройки виртуальных интерфейсов и мостов, обслуживающих управление системой, система хранения и монтирование внешних ресурсов.
7. Открытые в настройках межсетевого экрана порты на хостах, требуемые для подключения (описано в разделе [Требования к информационной безопасности](#)), в случае использования межсетевого экрана.
8. Для использования функционала iSCSI на всех хостах соответствующего кластера **ПК Р-Хранилище** должен стоять пакет *vstorage-iscsi*, а параметр *ISCSI\_ROOT* в конфигурационном файле */etc/vstorage/iscsi/config* должен быть задан и ссылаться на одну и ту же папку, расположенную на смонтированном **ПК Р-Хранилище**.
9. На хостах **Р-Виртуализации** должен быть запущен сервис *firewalld*, через него в процессе установки добавляются правила, разрешающие доступ по VNC в систему, где будет установлено решение **Базис.vControl**.
10. На всех хостах **Р-Виртуализации** должен быть уникальный machine-id, посмотреть который можно командой:

```
cat /etc/machine-id
```

При необходимости сменить machine-id можно командами ниже:

```
sudo rm -f /etc/machine-id
sudo rm -f /var/lib/dbus/machine-id
sudo systemd-machine-id-setup
```

После выполнения этих команд необходимо перезагрузить систему.

### 3.7 Другие требования

1. Время на всех хостах **Р-Виртуализации** и хосте/хостах, где будет развернуты **Бэкенд** и **Фронтенд Базис.vControl**, на серверах Postgres, а также хостах Redis/ClickHouse (в случае HA-установки) должно быть синхронизировано. При разворачивании системы вы можете указать NTP-сервер, с которым будут принудительно синхронизироваться все хосты.
2. Для обеспечения работы **Базис.vControl** с кластерами виртуализации необходимы работающие и настроенные инфраструктурные системы:
  - 1) Опционально может использоваться служба каталогов пользователей (Microsoft Active Directory, LDAP/Kerberos). Необходима сервисная учетная запись, которой доступна операция чтения. Соответствующие параметры должны быть заполнены в настройках. Для некоторых функций может понадобиться зашифрованное соединение.
  - 2) Общее хранилище данных с возможностью доступа по протоколу SMB или NFS для хранения шаблонов/ISO-образов.

### 4. ТРЕБОВАНИЯ К СЕТЕВОМУ ВЗАИМОДЕЙСТВИЮ

Необходимо обеспечить L3-связность:

- Между системой, где будет установлена **Базис.WorkPlace** и **Базис.vControl**;
- Между системой, где будет установлена **Базис.vControl**, и хостами с **P-Виртуализацией**.
- Между системой, где будет установлена **Базис.vControl**, и хостами с Redis (в случае HA-установки).
- Между системой, где будет установлена **Базис.vControl**, и хостами с ClickHouse (в случае установки HA).
- Между системой, которая будет выступать в роли **Сервера развертывания**, и:
  - системой, где будет установлено решение **Базис.vControl**;
  - хостами с Redis;
  - хостами с ClickHouse.



#### Примечание

В операционных системах для каждого перечисленного компонента должны выполняться команды **hostname -s** и **hostname -f** без явных задержек и выводить короткое и полное (FQDN) имена хоста.

---

Видимость хостов **P-Виртуализации** и машин, где будет установлено решение **Базис.vControl**, Redis, ClickHouse, по DNS-именам не обязательна, за исключением видимости между машинами с ClickHouse (настраивается автоматически при установке, не требует дополнительных действий).

Для работы в HA-режиме между машинами, на которых будут стоять **Базис.vControl**, **Бэкенд/Фронтенд**, должен беспрепятственно передаваться (должна быть возможность отправки/получения) VRRP-трафик.



## 5. ТРЕБОВАНИЯ К ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

### 5.1 Настройка межсетевого экрана

При соблюдении требований для установки ОС Linux межсетевой экран дополнительно настраивать не требуется, он по умолчанию отключен. Если необходимо настроить межсетевой экран, то список используемых портов и протоколов, которые используются для настройки, можно посмотреть в таблице 2.2 раздела [Сетевое взаимодействие компонентов](#).

Так как порты на исходящие подключения выбираются системой случайным образом, то ограничивать их не следует ни в ОС Linux, ни на **Р-Виртуализации**.

### 5.2 Системные учетные записи для работы компонентов продукта

В системе, где будет установлено решение **Базис.vControl**, все компоненты работают под своей учетной записью с правами обычного пользователя и без возможности для локального/SSH-входа в систему. Учетные записи и права для этих компонентов создаются автоматически при развертывании системы и не требуют дополнительных настроек. На все действия, которые требуют повышения привилегий, выданы права на использование **sudo**. Правила **sudo** из **/etc/sudoers.d/vms** должны применяться, без этого корректная работа продукта невозможна.

На хостах **Р-Виртуализации** для возможности полного управления хостами агент работает под учетной записью **root**.

## 6. УСТАНОВКА БАЗИС.VCONTROL

### 6.1 Подготовка серверов для установки компонентов Базис.vControl

Все компоненты **Базис.vControl** должны быть запущены на серверах под управлением одной из следующих операционных систем в минимальной установке с systemd:

- Альт 8 СП;
- Альт 9;
- Альт 9.1;
- Альт 10 (установка доступна с версии 10.1);
- Astra Linux версии 1.7;



#### Осторожно

Поддерживаются версии Astra Linux только с установленным обновлением Update 6 ([Бюллетень № 20200722se16](#)).

---

Каждый компонент может быть развернут как на виртуальном сервере (созданном под управлением **Базис.vControl**), так и на физическом сервере.

Данное руководство предполагает, что развертывание производится только на виртуальных машинах.

Ниже описаны шаги по подготовке «эталонной» VM, на базе которой будут созданы VM для размещения всех остальных компонентов **Базис.vControl**.

#### 6.1.1 Подготовка шаблона виртуальной машины для установки компонентов Базис.vControl

1. Подключитесь по SSH к хосту виртуализации под пользователем root. На Windows для этого можно использовать SSH-клиент [PuTTY](#).

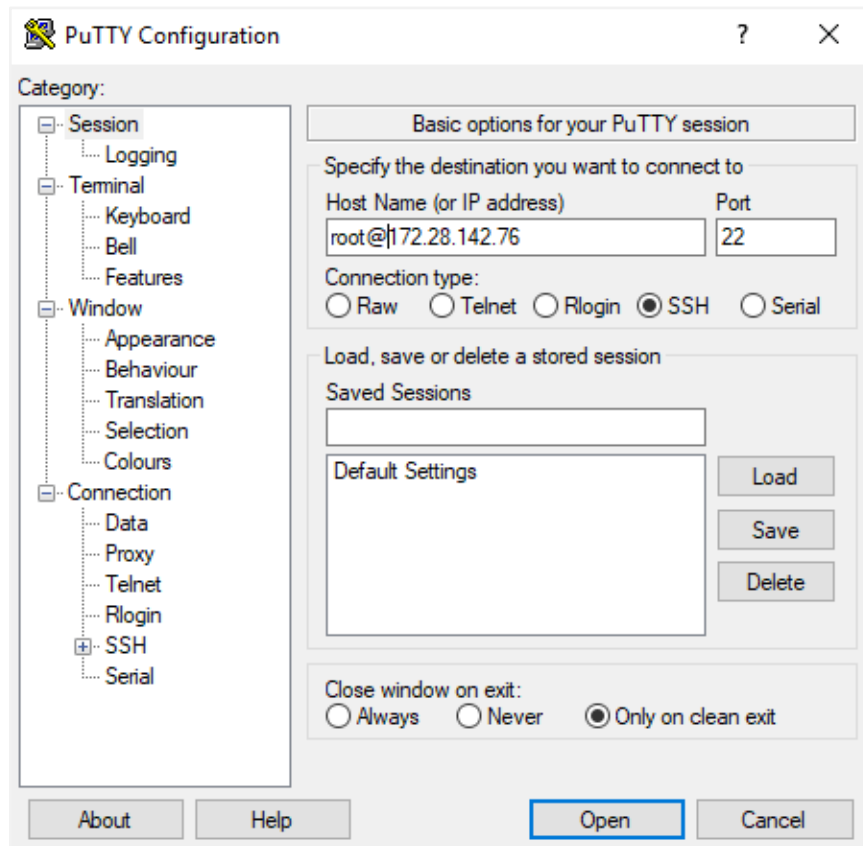


Рисунок 6.1 Подключение по SSH в PuTTY

2. Создайте виртуальную машину средствами командной строки гипервизора. Данная VM будет конвертирована в шаблон, из которого будут созданы VM для других компонентов инфраструктуры **Базис.vControl**. В данном примере мы создаем VM с именем VM01.

```
prlctl create vm01 --distribution linux
prlctl set vm01 --cpus 2 --cpu-sockets 2 --memsize 8192 --
videosize 256 --autostart auto --tools-autoupdate off
prlctl set vm01 --device-set hdd0 --size 60G
```

## Примечание

Для успешной работы шаблона разбейте диск на два раздела: один из разделов должен быть отведен под **/var/log** для записи логов и иметь объем не менее 10 Гбайт.

---

3. Для консольного доступа установите и настройте VNC на созданной VM01 (убедитесь, что VM01 в этот момент остановлена). Установка производится в режиме auto, после ее завершения система сообщит назначенный TCP-порт для доступа по VNC.

```
prlctl stop vm01
prlctl set vm01 --vnc-mode auto --vnc-nopasswd
prlctl start vm01
prlctl list -i vm01
```

Успешный вывод последней команды будет содержать интересующее нас значение порта для доступа по VNC до этой VM (и всех дальнейших VM, созданных по ее шаблону).

```
> Remote display: mode=auto **port=6682** websocket=5703
address=0.0.0.0
```

4. С помощью `scp` скопируйте образ операционной системы, которую нужно будет установить на VM, в общую папку, доступную с VM. В нашем случае образы хранятся в `\\123.123.123.123\1`, а целевая общая папка — `/vstorage/stor1/vmprivate/`.

На Windows для этого можно воспользоваться утилитой [WinScp](#), подключившись к хосту виртуализации.

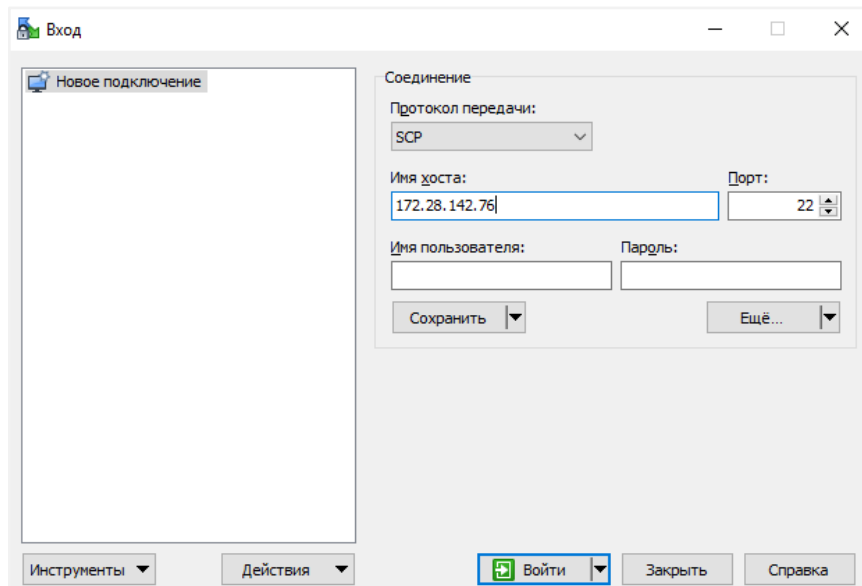


Рисунок 6.2 Окно утилиты WinScp

Далее будут приведены примеры установки ОС Альт и Astra Linux.

5. Примонтируйте скопированный образ (ISO-файл) к виртуальному CDROM-дисководу созданной VM01. Для этого выполните в консоли хоста виртуализации следующую команду (VM должна быть предварительно остановлена):

```
prlctl stop vm01
prlctl set vm01 --device-set cdrom0 --image
/vstorage/stor1/vmprivate/operation-system.iso --enable --connect
prlctl start vm01
```

### 6.1.2 Инсталляция ОС Альт



#### Примечание

Ниже рассматривается установка ОС Альт 10, в качестве репозиториев используйте официальные интернет-репозиторий Альт 10 или установочный диск версии **ALT Server 10.1-x86\_64**.

1. Запустите VM и подключитесь к ней через консоль VNC. При загрузке VM с примонтированного ISO-образа автоматически запустится инсталлятор ОС Альт, и вы увидите его главное окно:

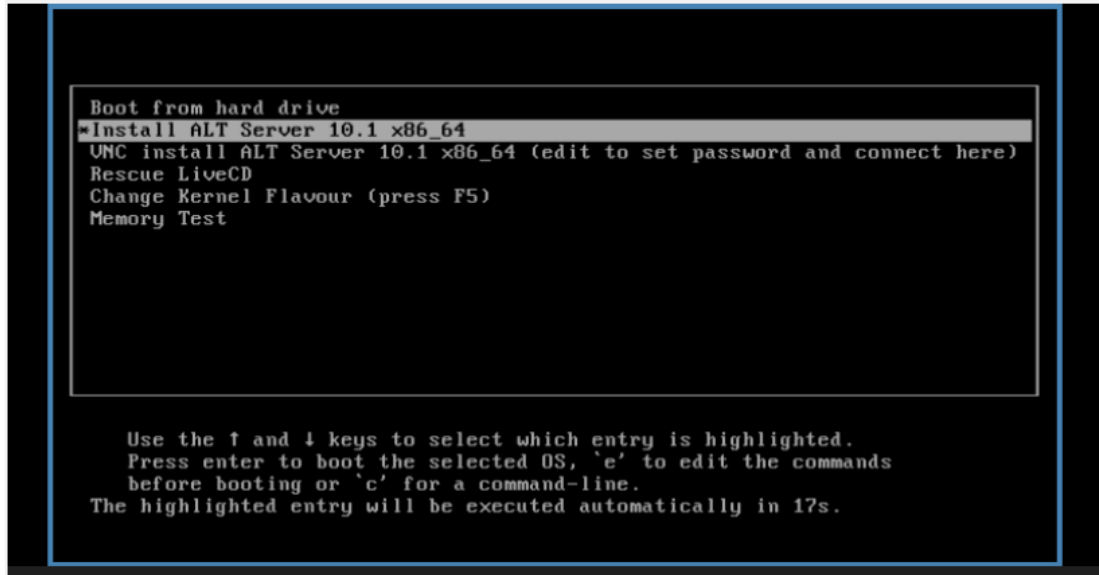


Рисунок 6.3 Главное окно инсталлятора ОС Альт

2. Оставьте языковые настройки по умолчанию.

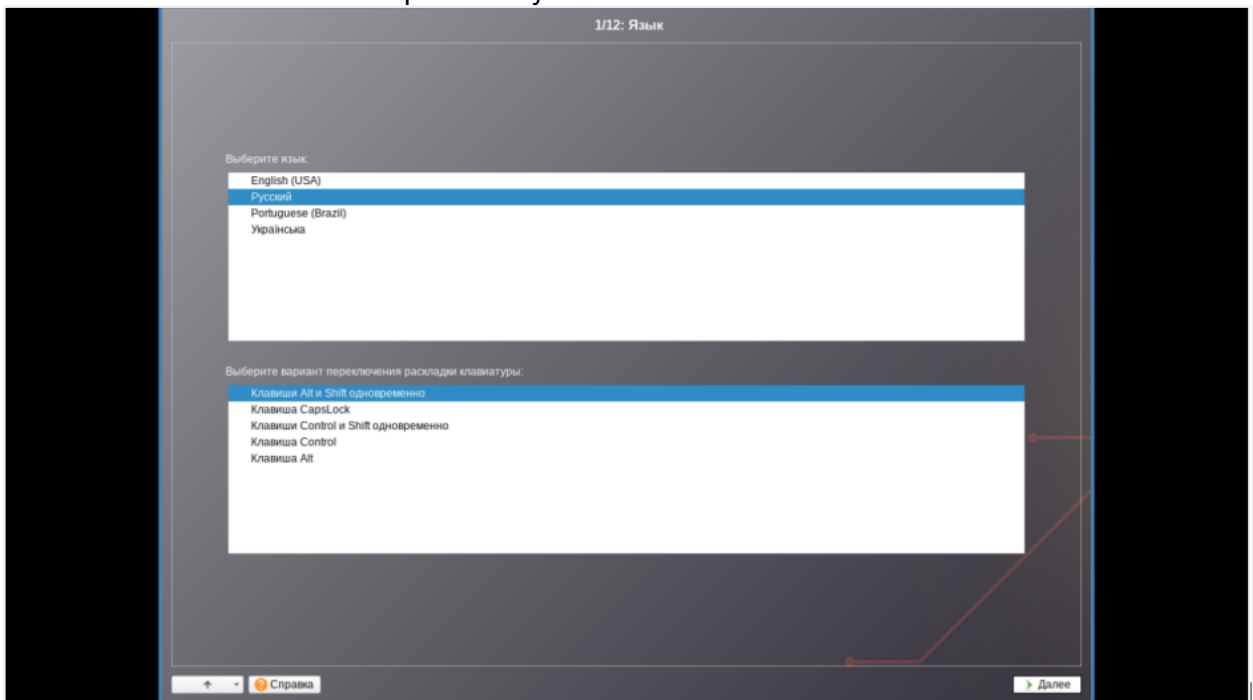


Рисунок 6.4 Выбор языковых настроек ОС Альт

3. Примите лицензионное соглашение.
4. Выберите страну и город для привязки к часовому поясу.
5. Выберите настройки по умолчанию для разбивки диска.

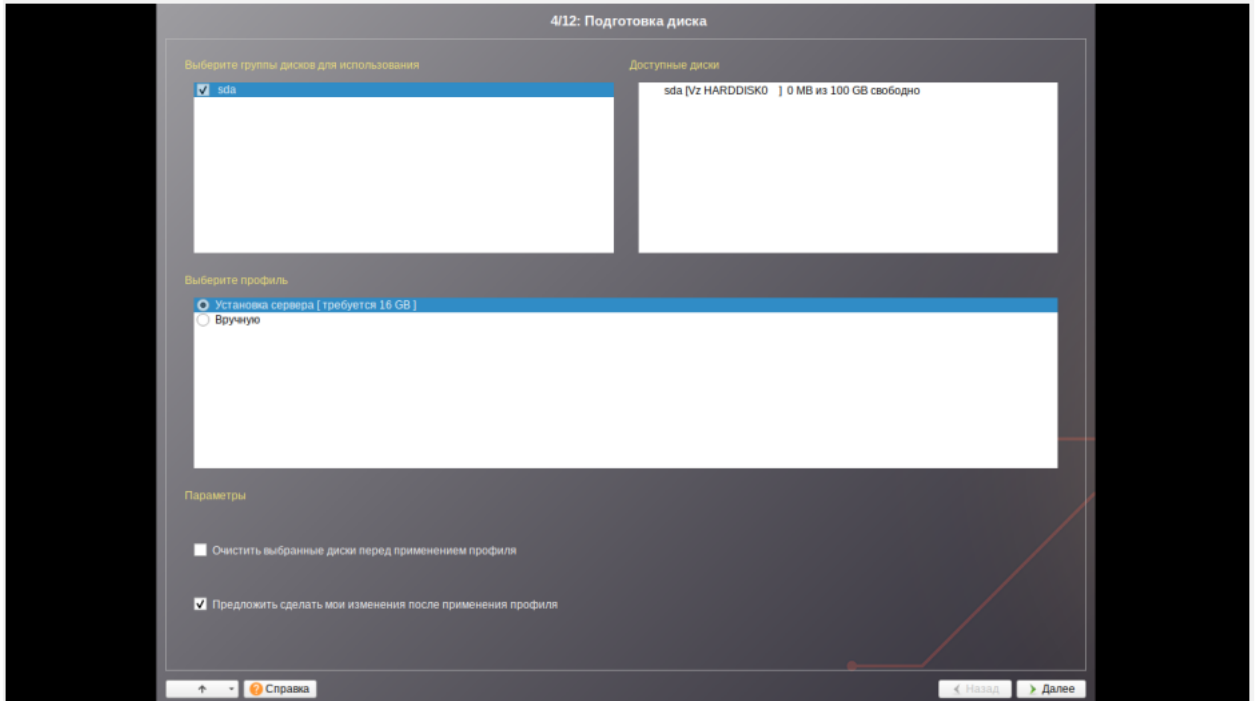


Рисунок 6.5 Этап подготовки диска

6. Выберите установку серверной части.
7. Выберите установку в минимальной комплектации с systemd. Дождитесь установки программного обеспечения.

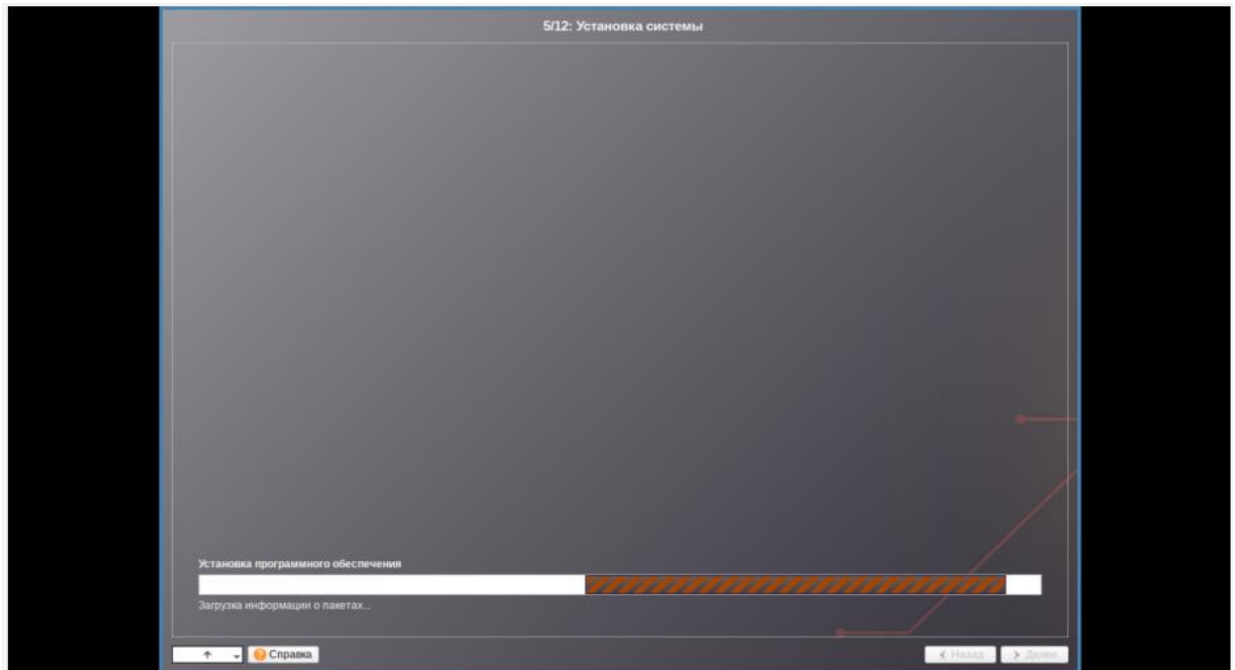


Рисунок 6.6 Установка ОС Альт

## 8. Оставьте настройки по умолчанию для загрузчика.

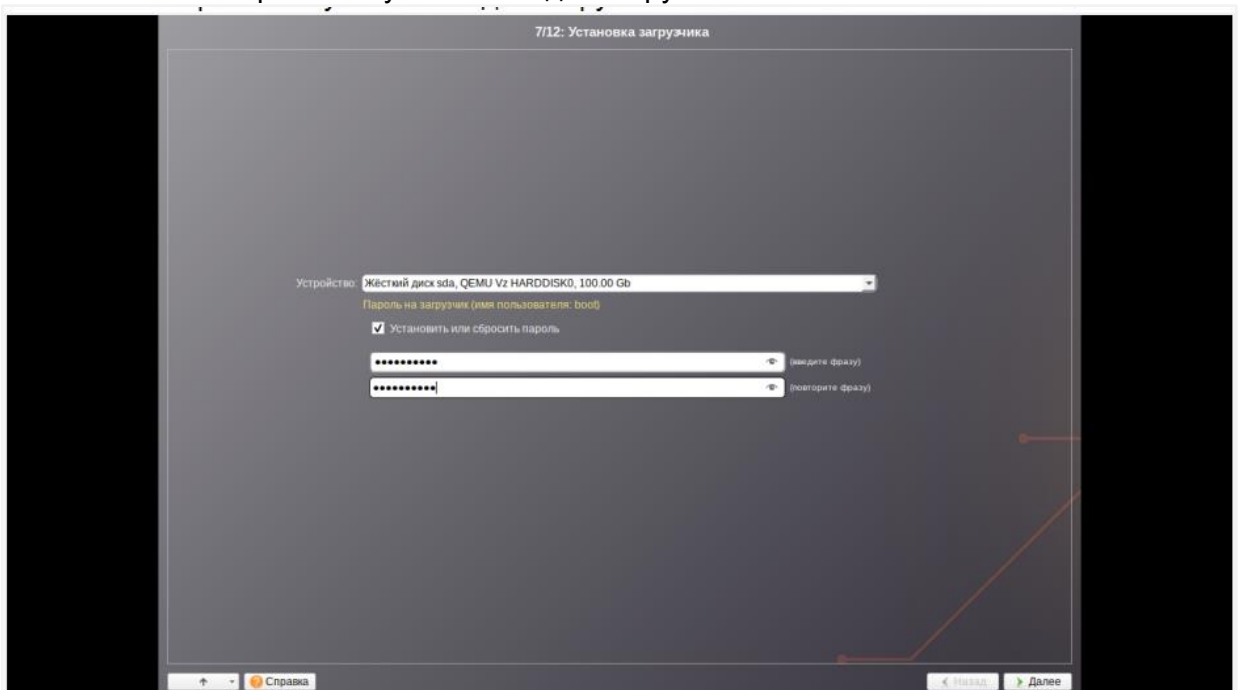


Рисунок 6.7 Настройки для загрузчика



9. Сконфигурируйте настройки сети для протокола IPv4. Информация по IP берется из техзадания/тикета. Не включайте IPv6 на сетевых интерфейсах (не ставьте галочку для настройки IPv6 в интерфейсе во время установки).

- Чтобы автоматически получить IP-адрес от DHCP-сервера, в списке «Конфигурация» выберите «Использовать DHCP».
- Чтобы задать IP-адрес вручную, в списке «Конфигурация» выберите «Вручную», введите IP-адрес в поле «IP» и нажмите кнопку **Добавить**.

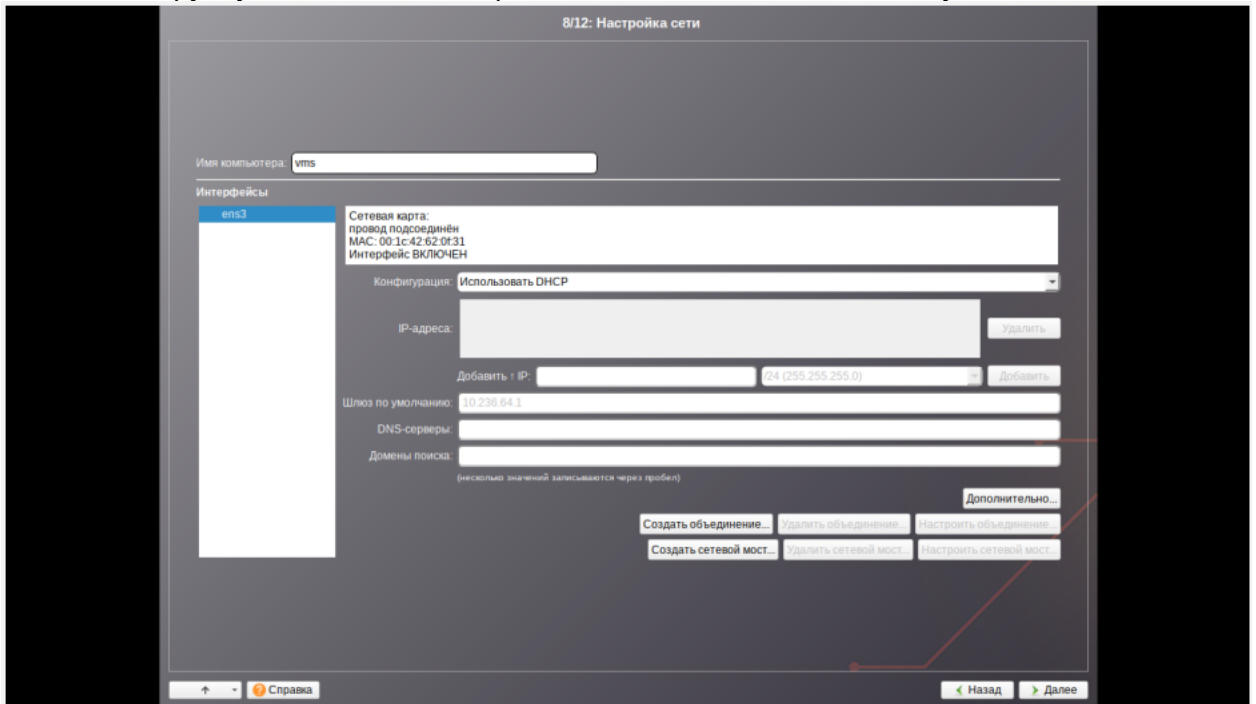


Рисунок 6.8 Настройки сети

10. Задайте пароль для системного администратора.



Рисунок 6.9 Настройка пароля для администратора

11. Создайте пользователя **sa-admin** как service account.

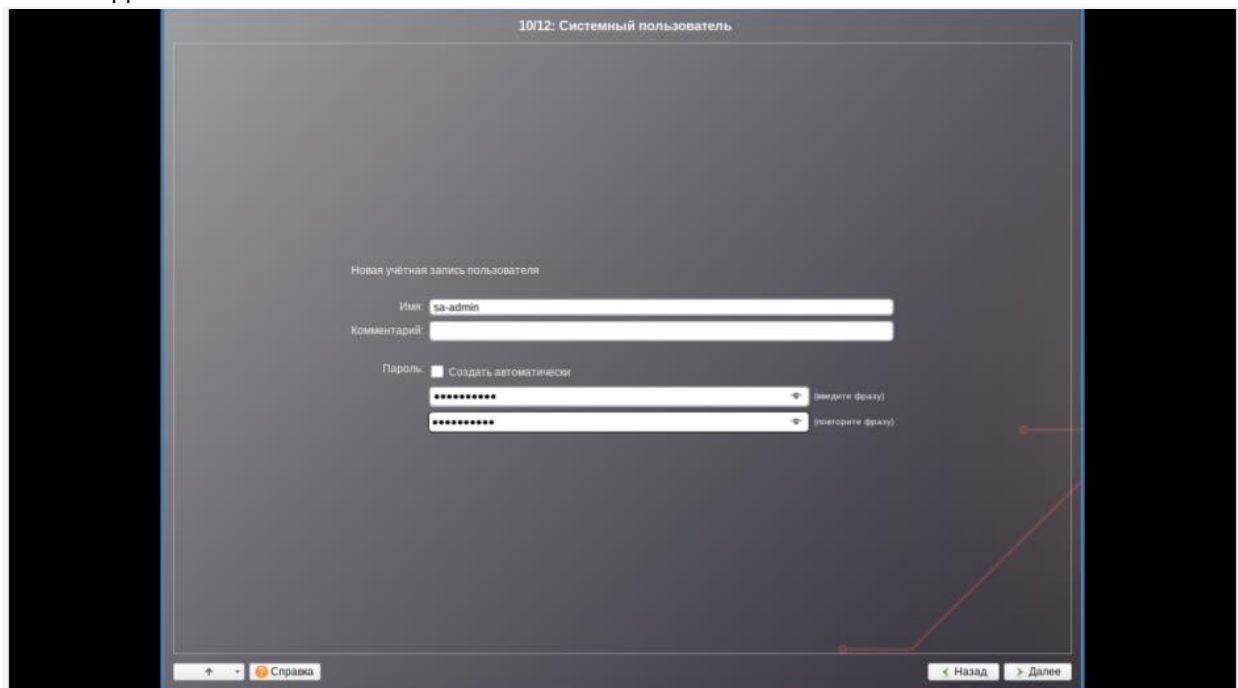


Рисунок 6.10 Настройка системного пользователя

12. После завершения установки и перезагрузки проверьте, не оказался ли включен IPv6, и выключите его, если он активен.

```
echo 'net.ipv6.conf.all.disable_ipv6=1' >> /etc/sysctl.conf &&
sysctl -p /etc/sysctl.conf
echo 'options ipv6 disable=1' >> /etc/modprobe.d/options-
local.conf
```

Затем перезагрузите VM для полного отключения IPv6.

13. Включите доступ по SSH к VM. Для этого отредактируйте следующий параметр в **/etc/openssh/sshd\_config** на VM:

```
PermitRootLogin yes
```

После этого активируйте SSH-сервер, выполнив в консоли VM следующую команду:

```
systemctl enable --now sshd
```

14. При использовании Альт 10 обязательно установите доступные обновления пакетов.

### 6.1.3 Установка Astra Linux

Ниже изложены инструкции по установке Astra Linux выпуска 1.7.



#### Осторожно

Поддерживаются ОС Astra Linux только с установленным и соответствующим выбранному релизу [очередным обновлением](#).



#### Совет

Полноценная установка ОС Astra Linux выполняется согласно инструкции, доступной на [официальном справочном портале](#).

PostgreSQL используется тот же, что идет в составе Astra Linux — дополнительный репозиторий не требуется.

- **Использовать по умолчанию ядро Hardened** — при выборе данного пункта будет обеспечено использование средств ограничения доступа к страницам памяти. В ядро и компилятор внесено несколько изменений, которые увеличивают общую защищенность системы от взлома. Hardened-ядро может блокировать массу потенциально опасных операций.

---

### **Примечание**

Возможны проблемы с работоспособностью сторонних приложений.

---

- **Запретить установку бита исполнения** — при выборе данного пункта будет включен режим запрета установки бита исполнения, что сделает невозможным выполнение shell-скриптов.
- **Включить блокировку консоли** — при выборе данного пункта будет заблокирован консольный вход в систему для пользователя и запуск консоли из графического интерфейса сессии пользователя.
- **Включить блокировку интерпретаторов** — при выборе данного пункта будет заблокировано интерактивное использование интерпретаторов.
- **Включить межсетевой экран ufw** — при выборе данного пункта будет включен межсетевой экран ufw и запущена фильтрация сетевых пакетов в соответствии с заданными настройками.
- **Отключить возможность трассировки ptrace** — при выборе данного пункта будет отключена возможность трассировки и отладки выполнения программного кода.

---

### **Примечание**

Включение данной опции лишит возможности отладки сторонних и работающих нестабильно приложений. Целесообразно при использовании сервера узкой специализации после отладки.

---

Далее приведен пример развертывания Astra Linux Special Edition для установки **Бэкенда**:

1. Примите лицензионное соглашение.
2. Выберите предпочитаемый способ переключения раскладки клавиатуры.
3. Задайте имя для компьютера.

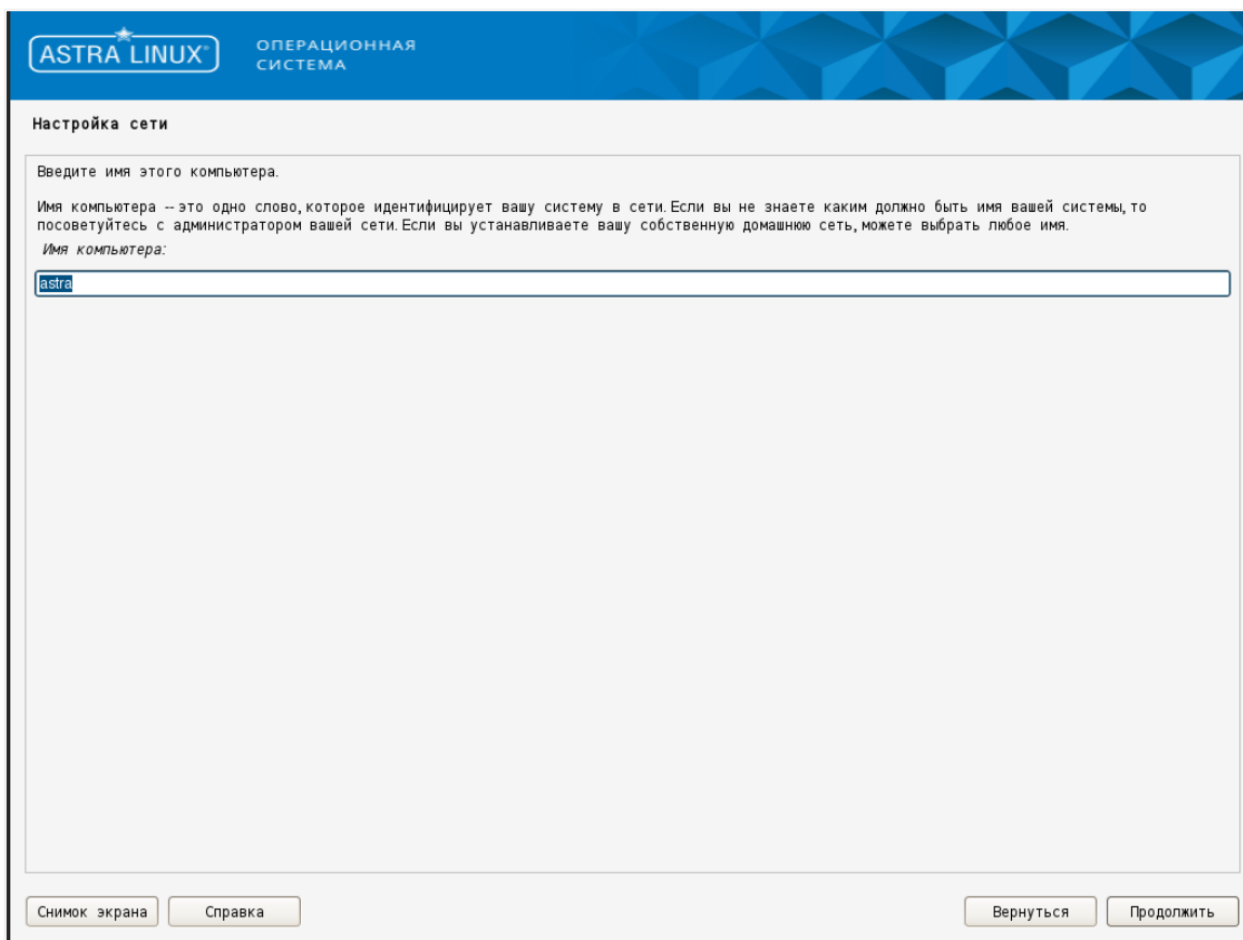


Рисунок 6.11 Настройка имени компьютера

4. Задайте имя учетной записи администратора и укажите пароль.

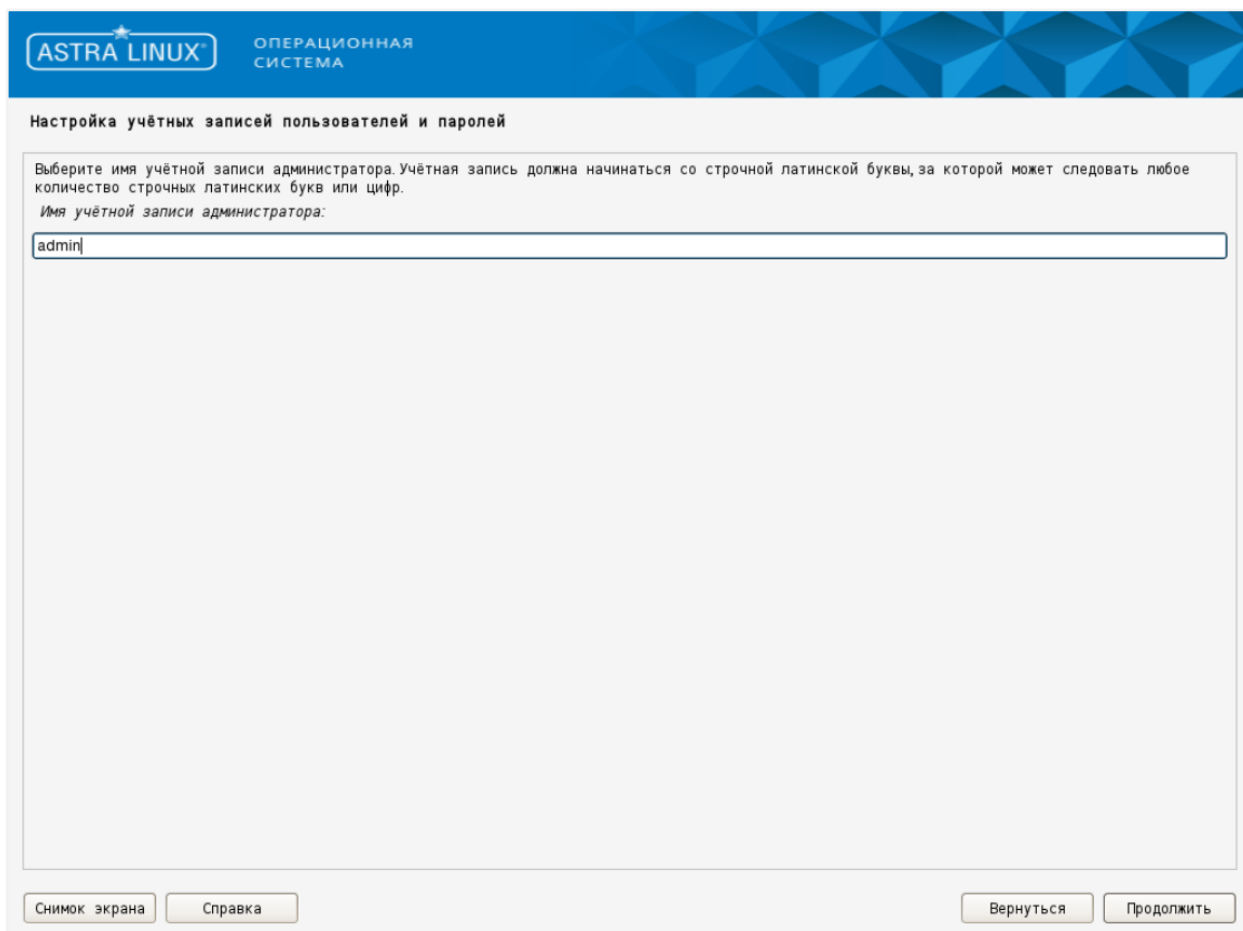


Рисунок 6.12 Настройка имени учетной записи администратора

The screenshot shows the 'Настройка учётных записей пользователей и паролей' (User account configuration) window in Astra Linux. The window title is 'Настройка учётных записей пользователей и паролей'. The main content area contains the following text and controls:

Хороший пароль представляет из себя смесь букв, цифр и знаков препинания, и должен периодически меняться.  
Введите пароль для нового администратора:

●●●●●●●●

Показывать вводимый пароль

Проверка правильности ввода осуществляется путём повторного ввода пароля и сравнения результатов.  
Введите пароль ещё раз:

●●●●●●●●

Показывать вводимый пароль

At the bottom of the window, there are four buttons: 'Снимок экрана' (Screenshot), 'Справка' (Help), 'Вернуться' (Back), and 'Продолжить' (Continue).

Рисунок 6.13 Настройка пароля учетной записи администратора

5. Выберите город для привязки к часовому поясу.

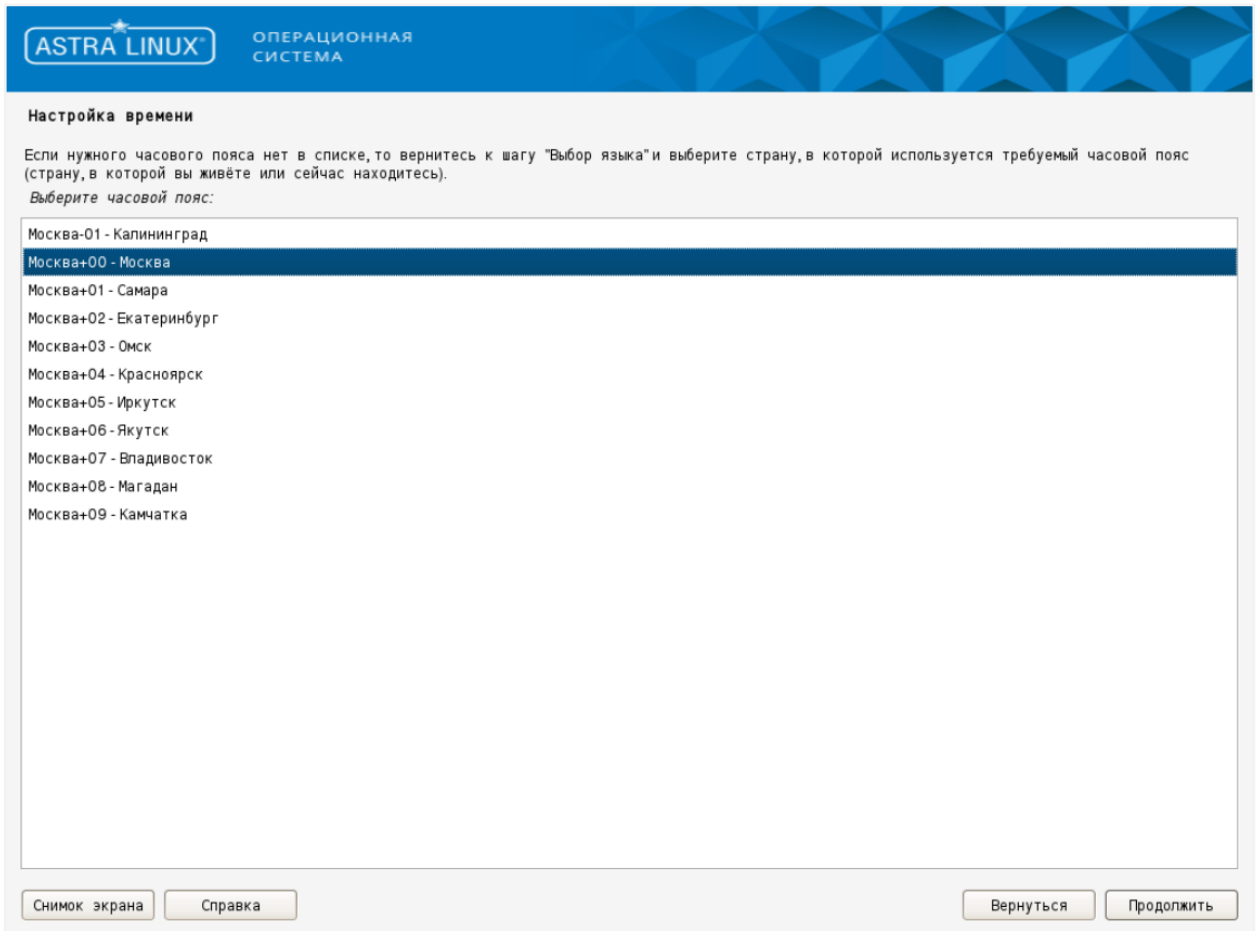


Рисунок 6.14 Выбор города для привязки к часовому поясу

6. Выполните процедуру автоматической разметки диска.



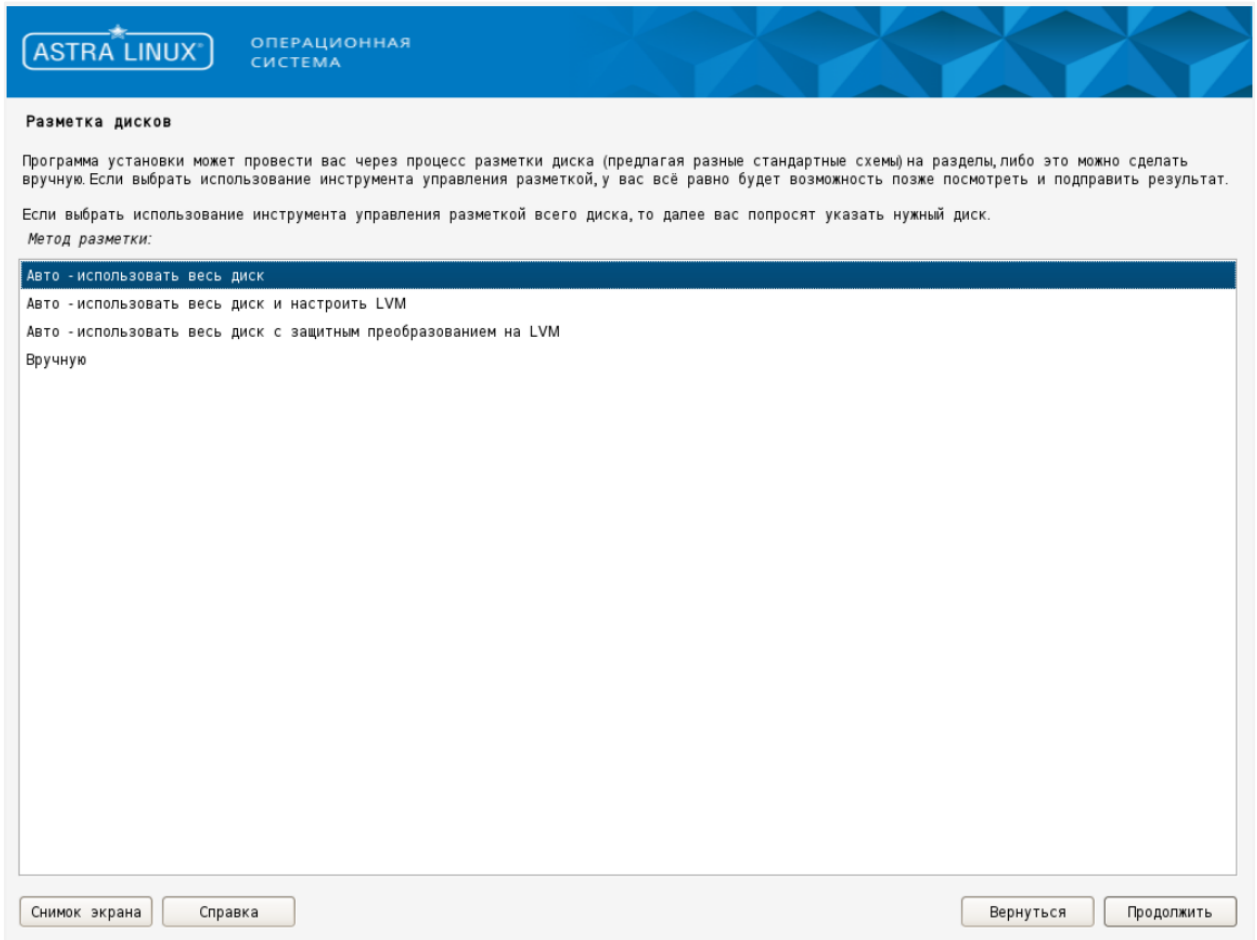


Рисунок 6.15 Автоматическая разметка диска, шаг 1

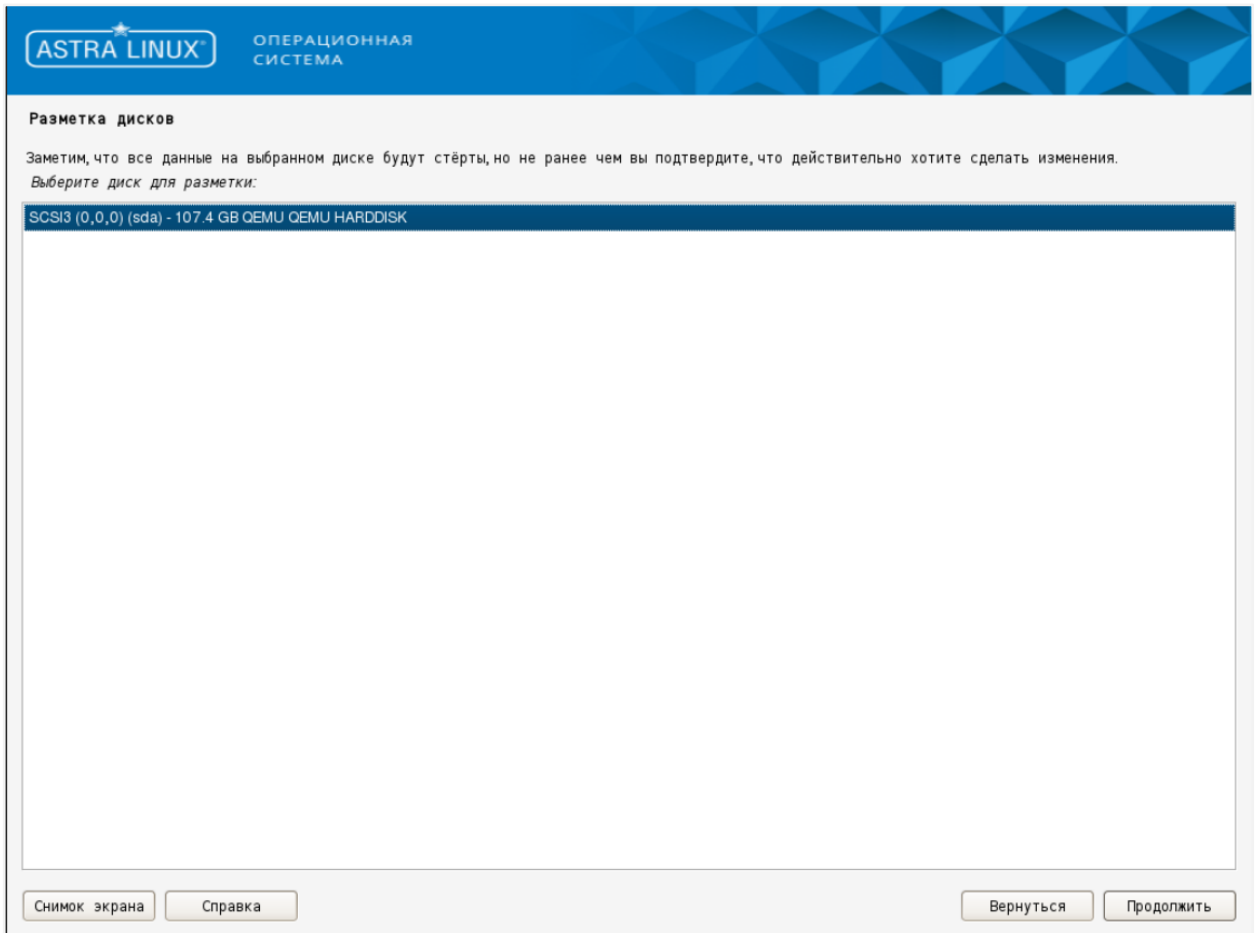


Рисунок 6.16 Автоматическая разметка диска, шаг 2

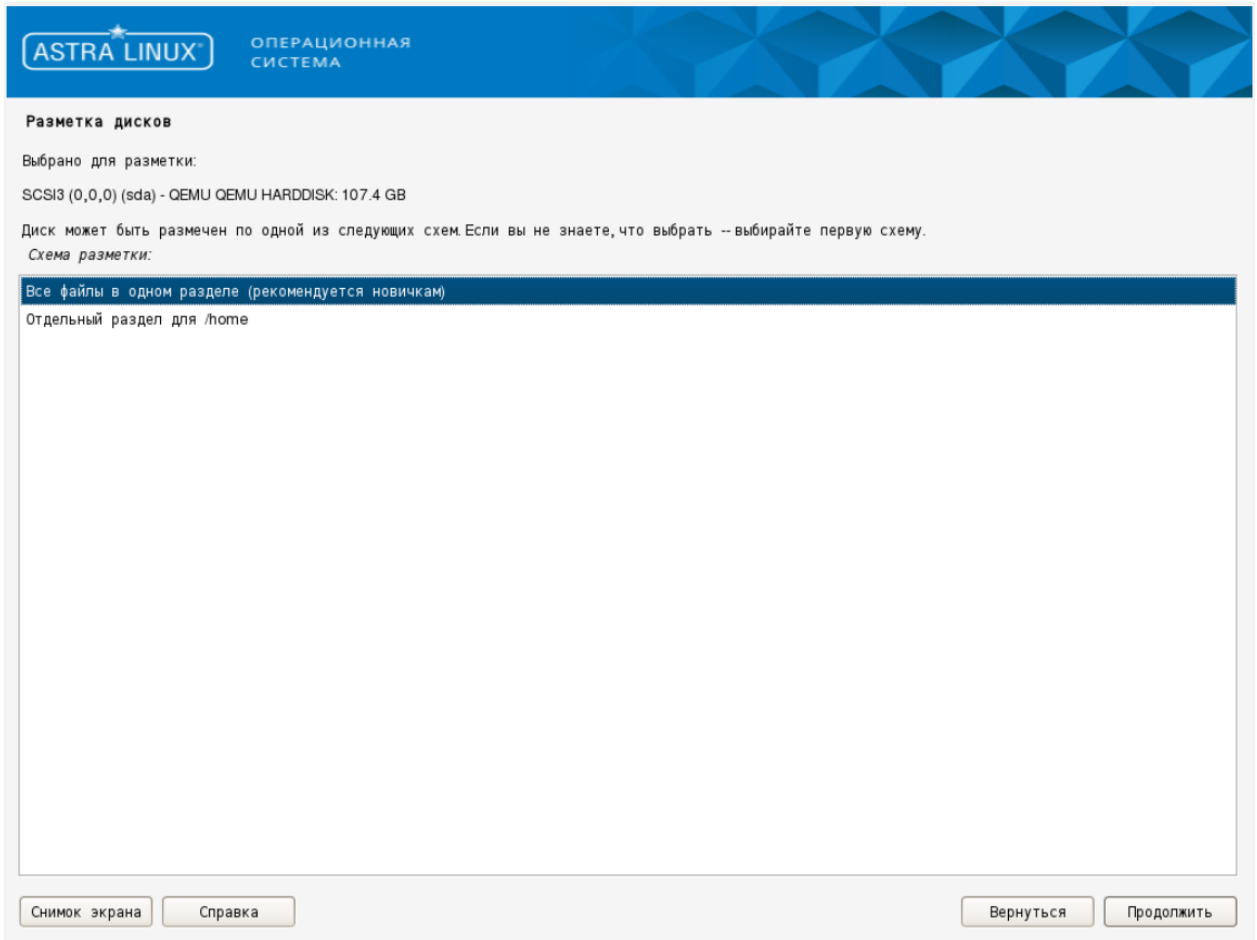


Рисунок 6.17 Автоматическая разметка диска, шаг 3

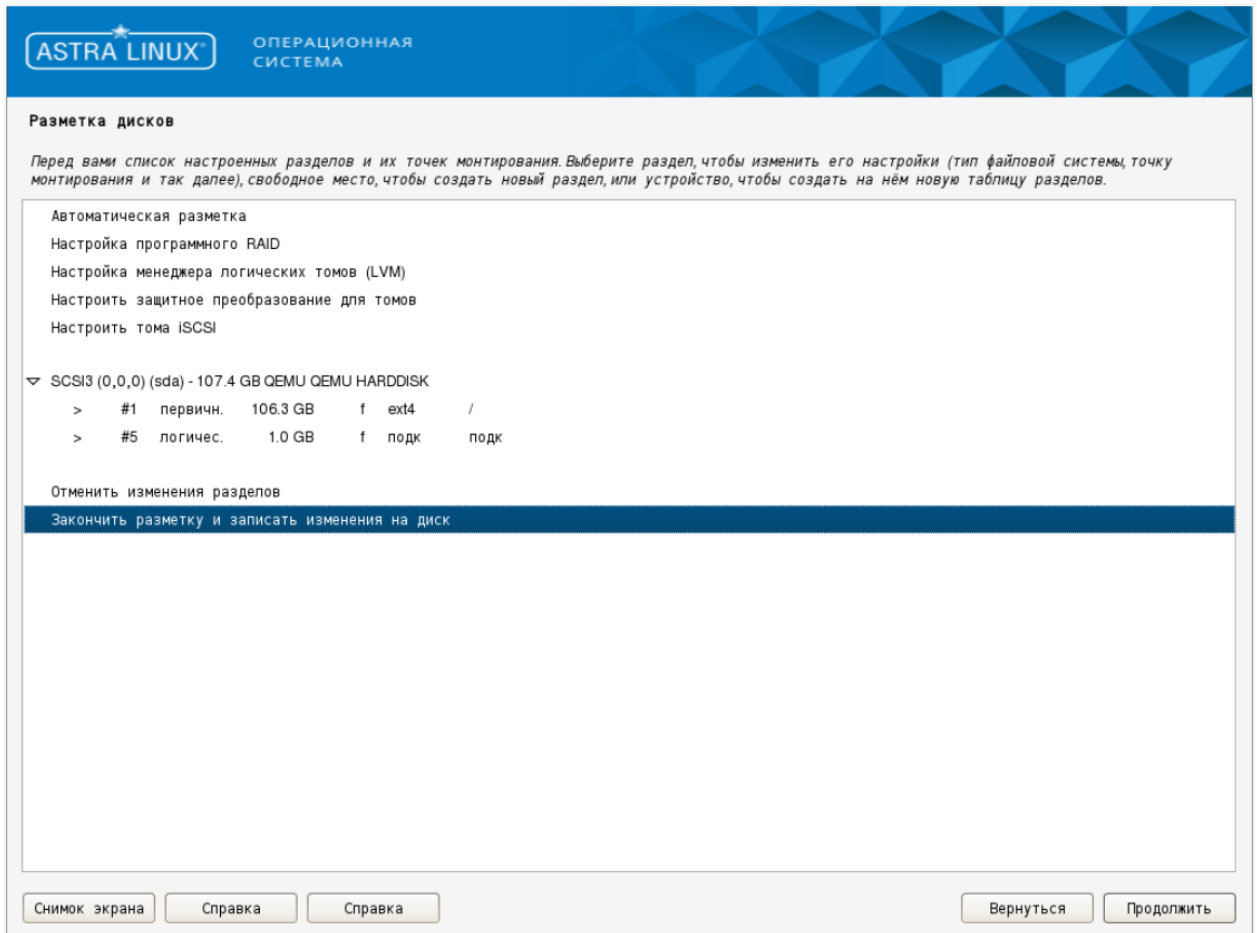


Рисунок 6.18 Автоматическая разметка диска, шаг 4

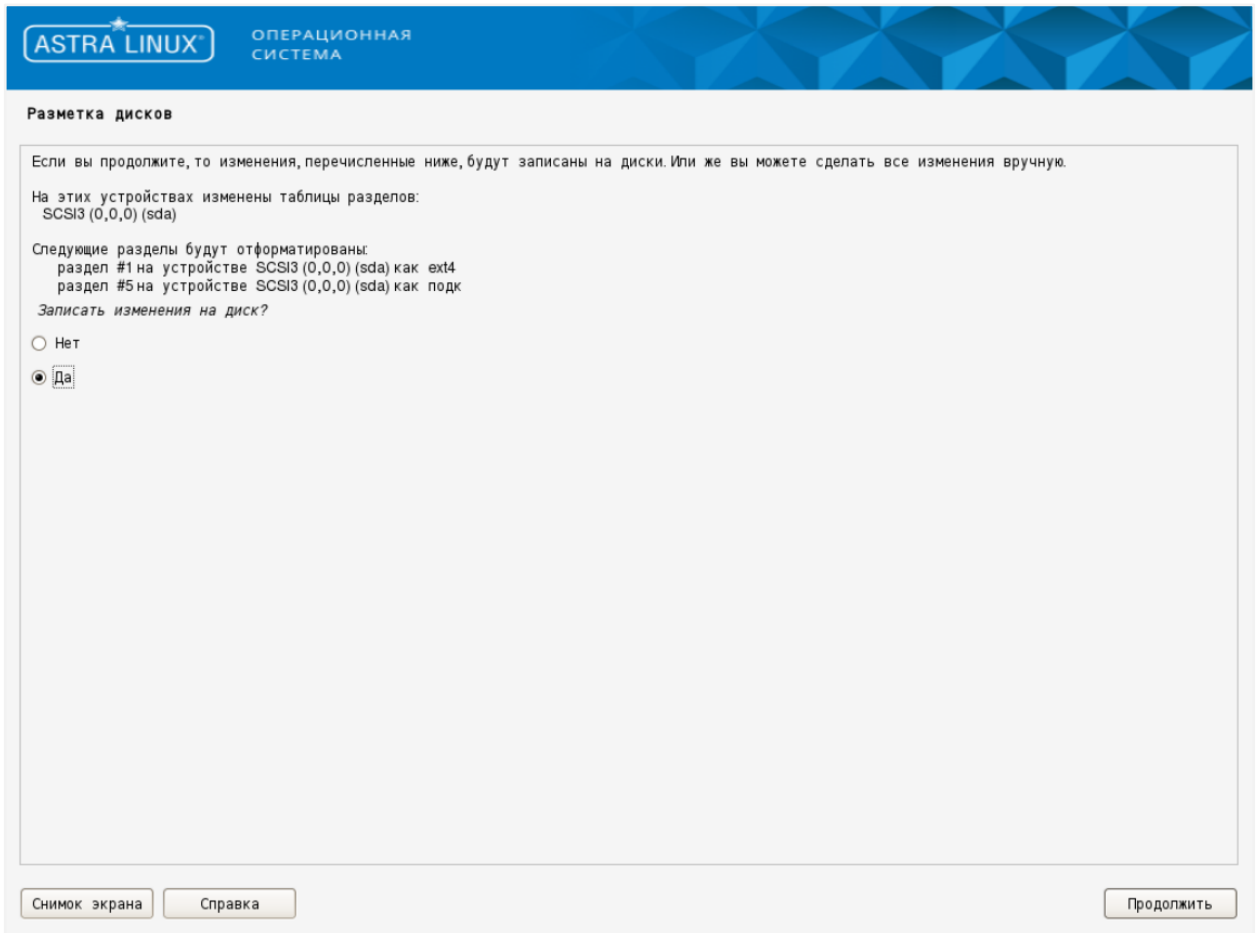


Рисунок 6.19 Автоматическая разметка диска, шаг 5

7. Установите базовую систему.

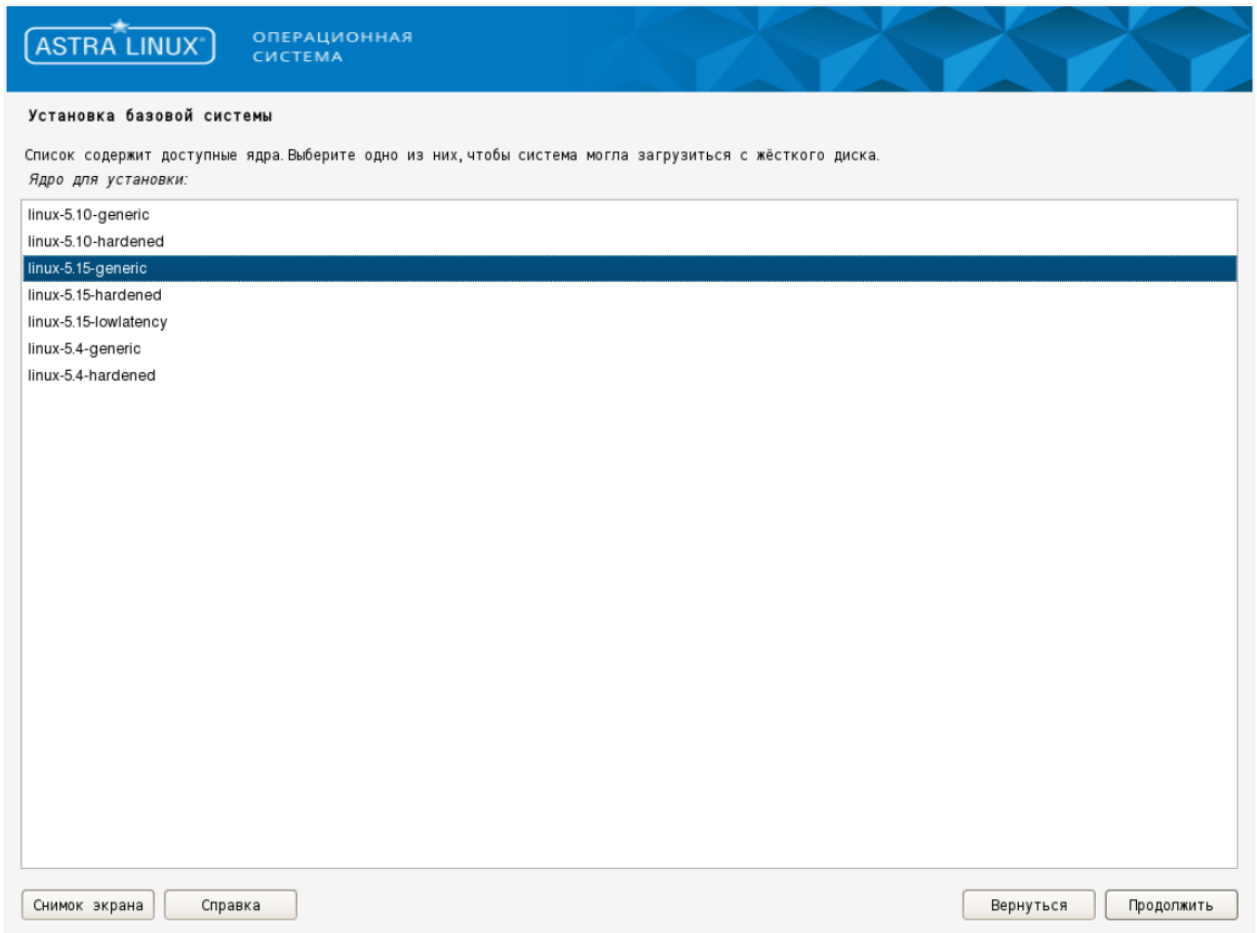


Рисунок 6.20 Установка базовой системы

8. Выберите ПО для установки.

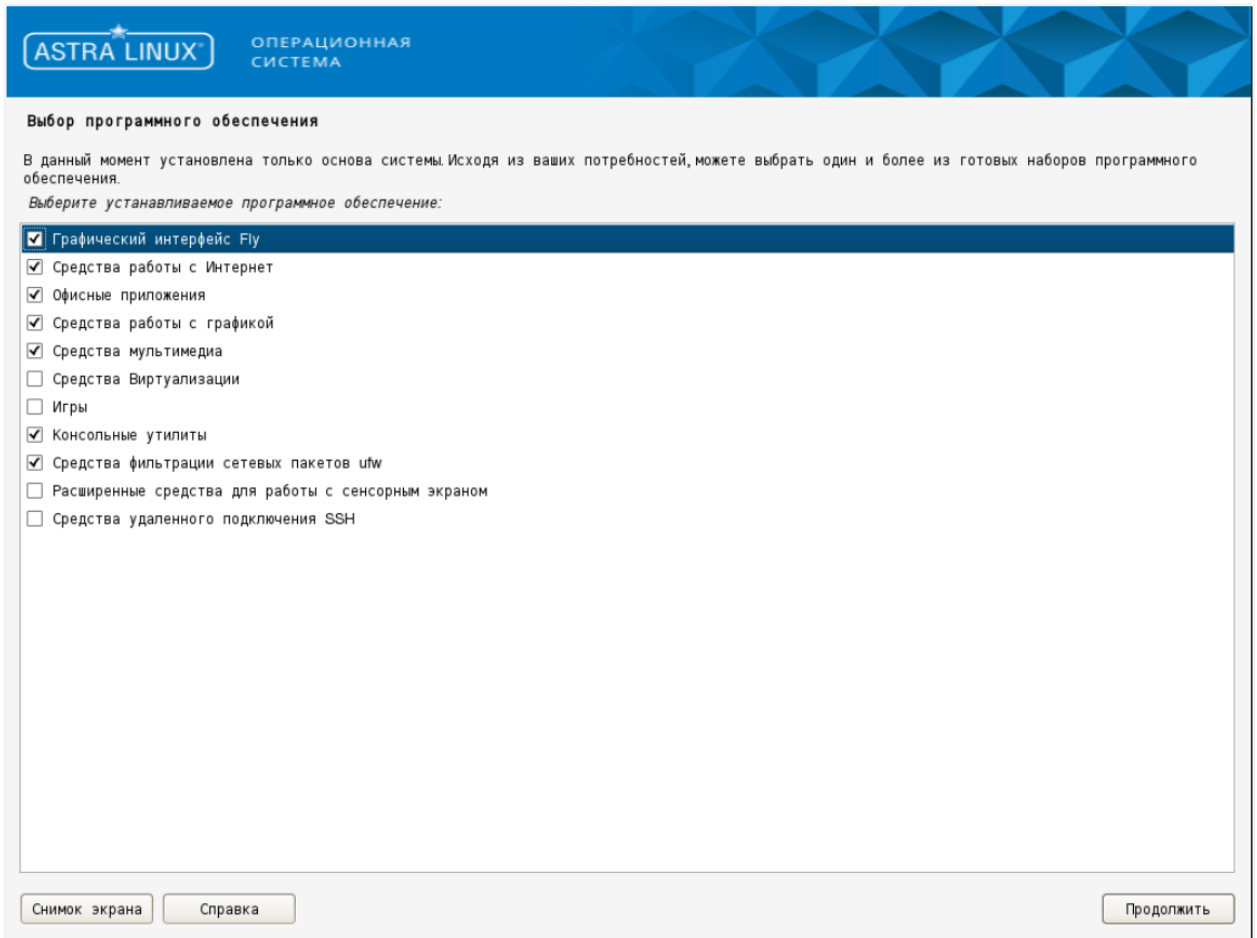


Рисунок 6.21 Выбор программного обеспечения для установки

## 9. Произведите дополнительные настройки ОС.

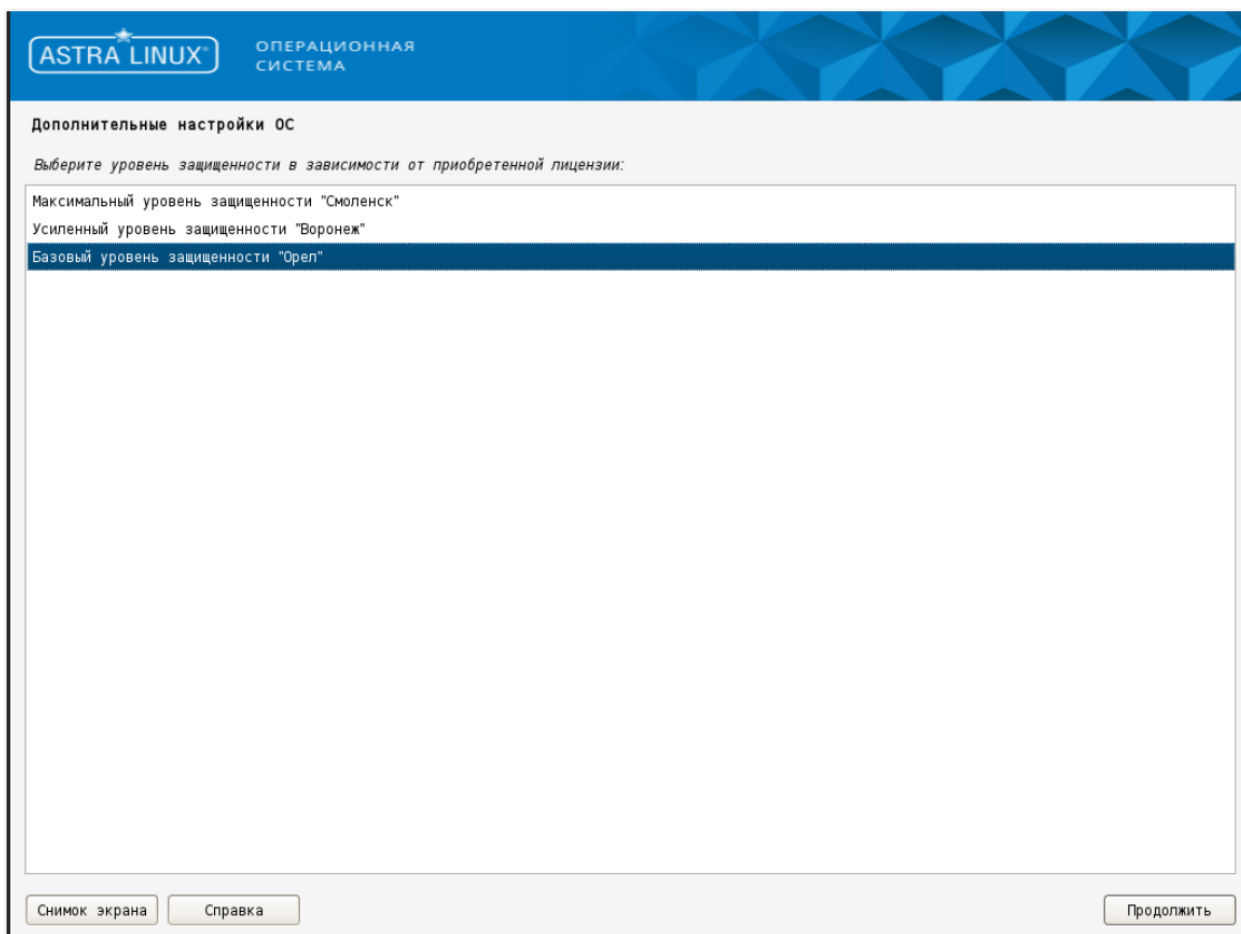


Рисунок 6.22 Дополнительные настройки ОС, шаг 1



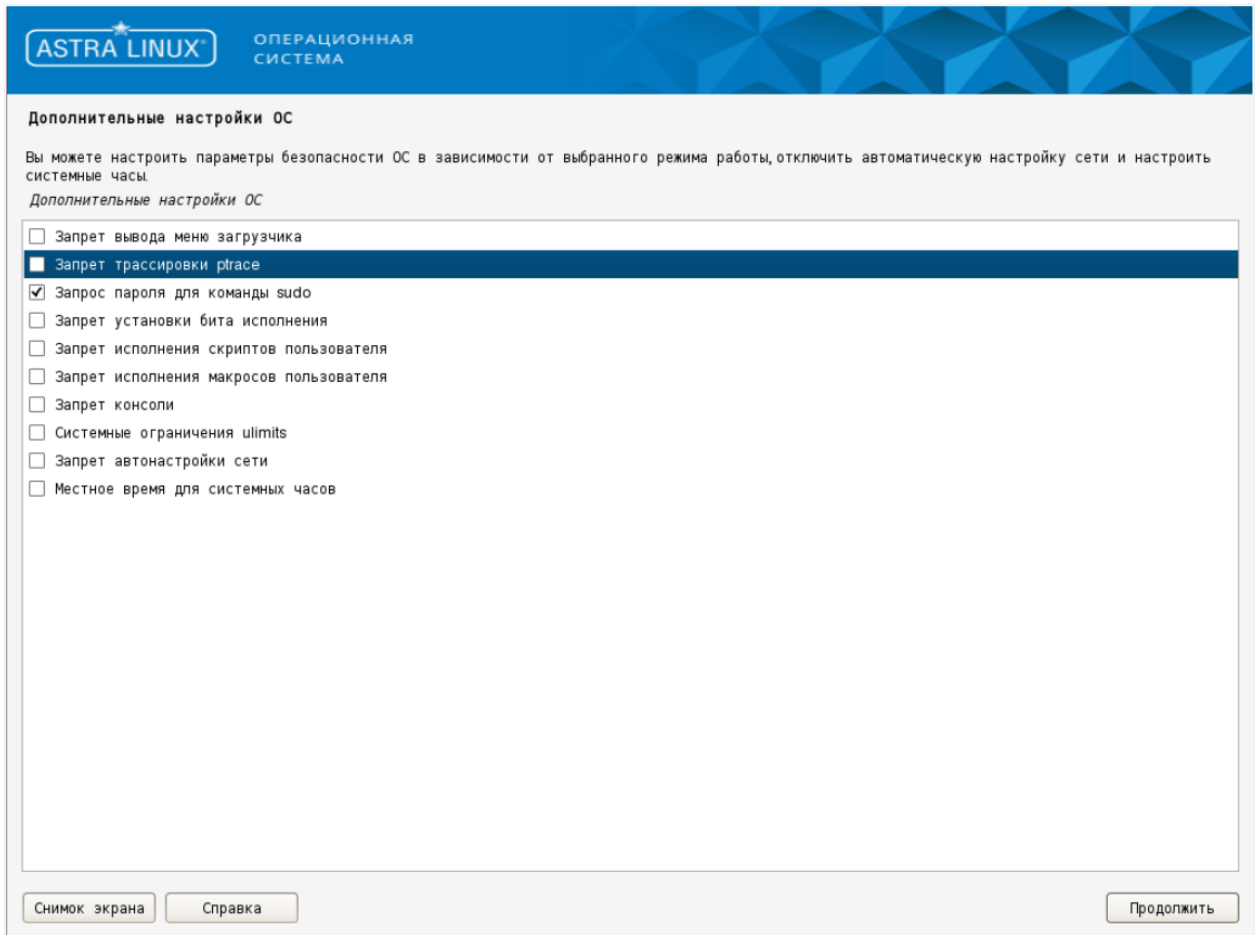


Рисунок 6.23 Дополнительные настройки ОС, шаг 2

10. Выберите установку системного загрузчика на жесткий диск.

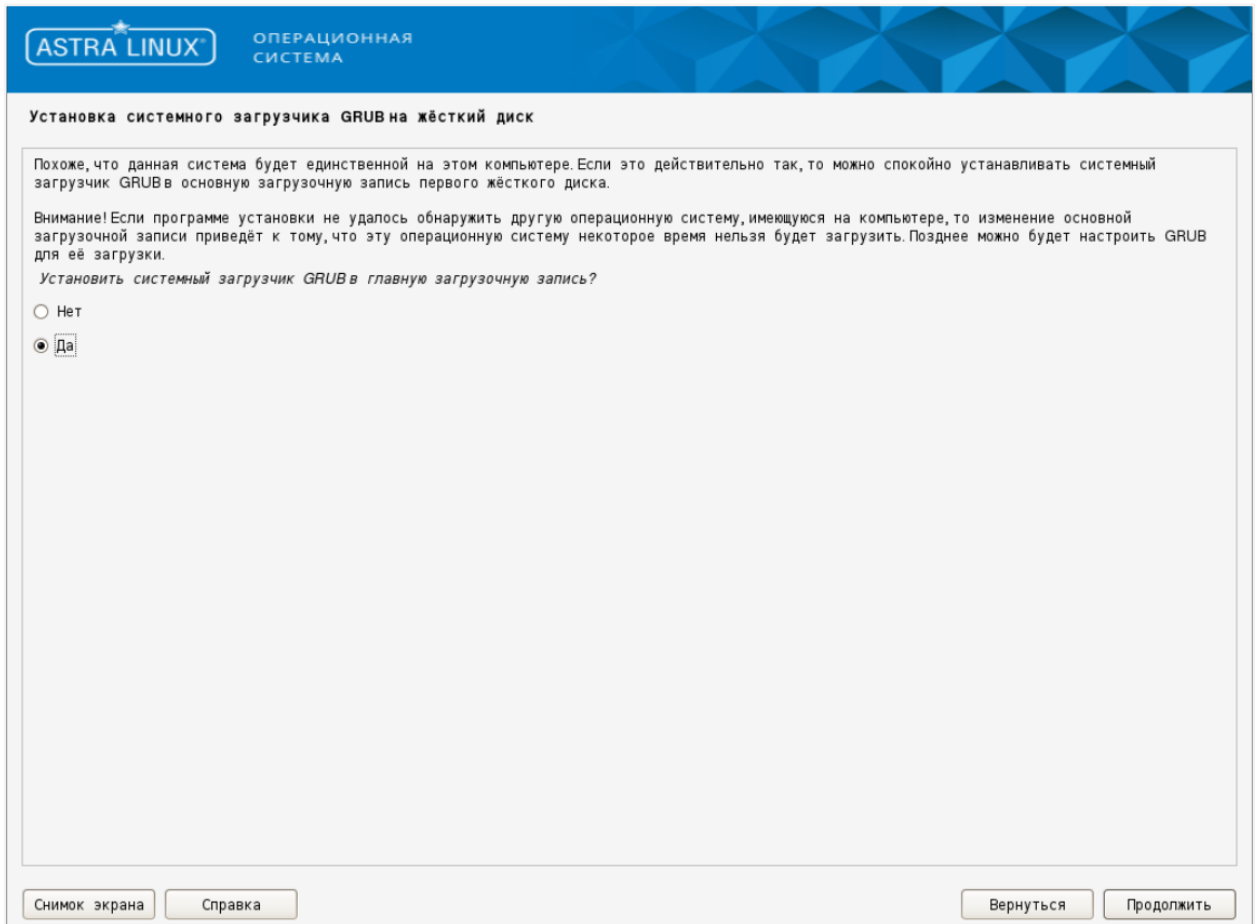


Рисунок 6.24 Выбор места для установки загрузчика

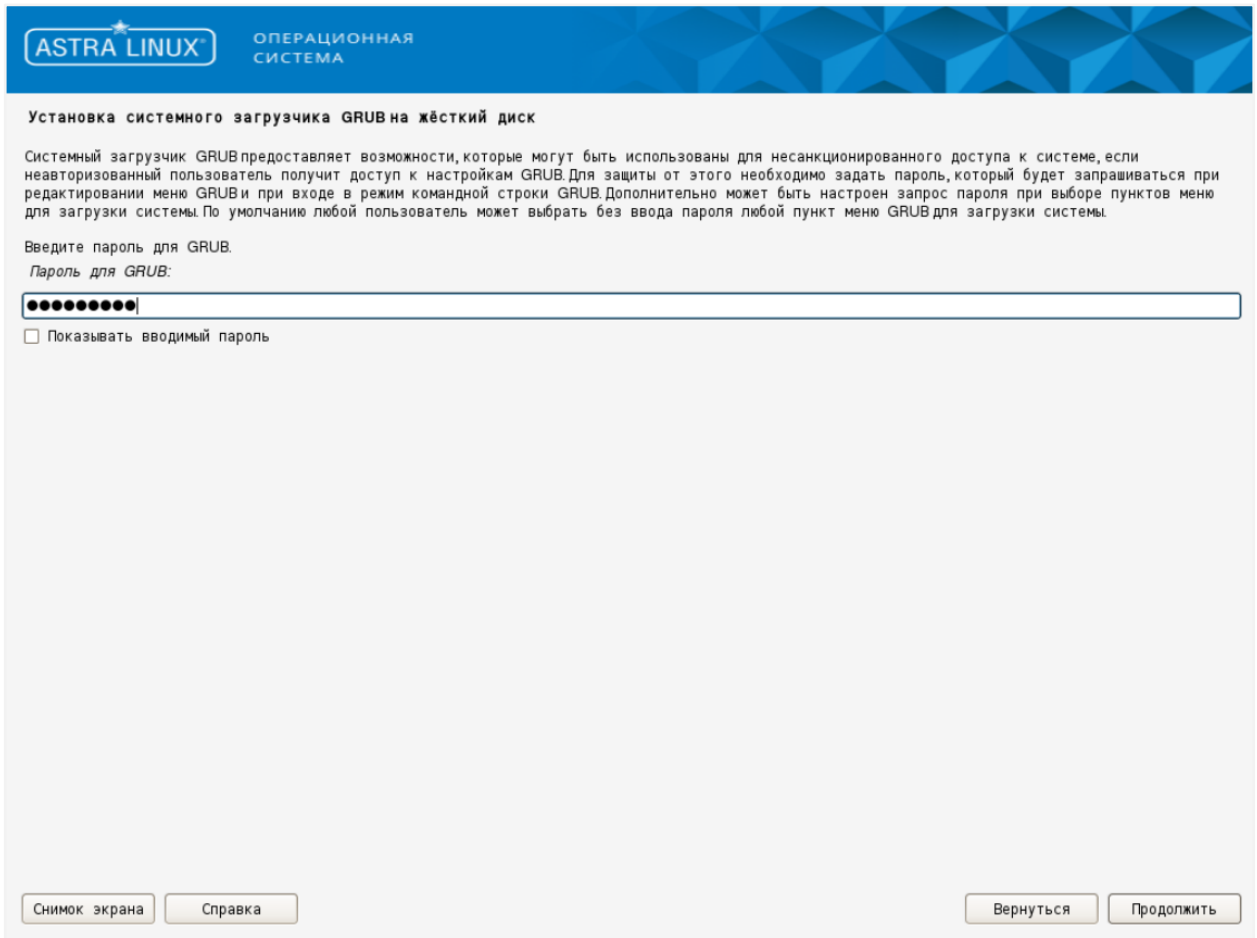


Рисунок 6.25 Защита загрузчика паролем

## 11. Установите системный загрузчик на жесткий диск

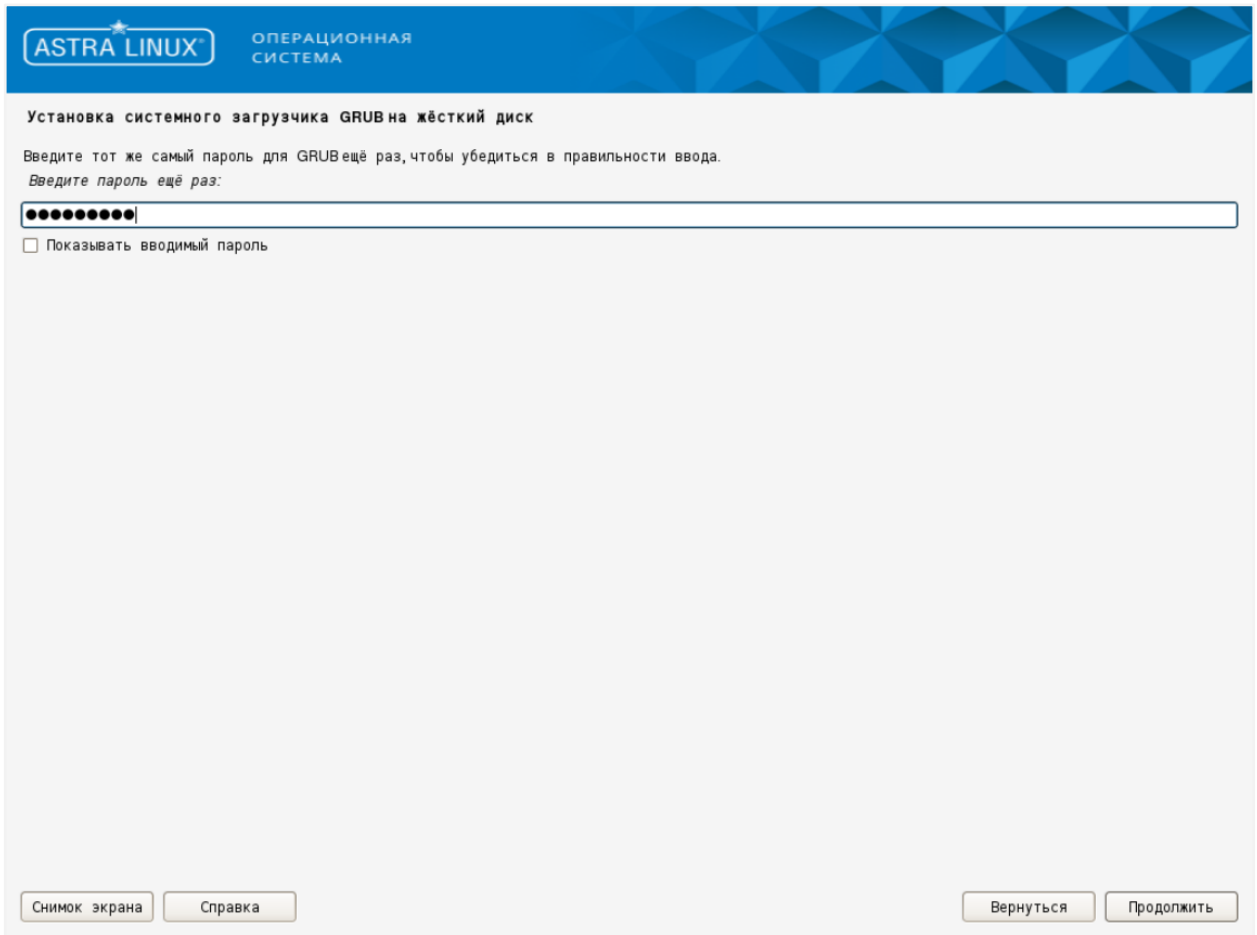


Рисунок 6.26 Повторный ввод пароля

11. Дождитесь завершения процедуры установки ОС.

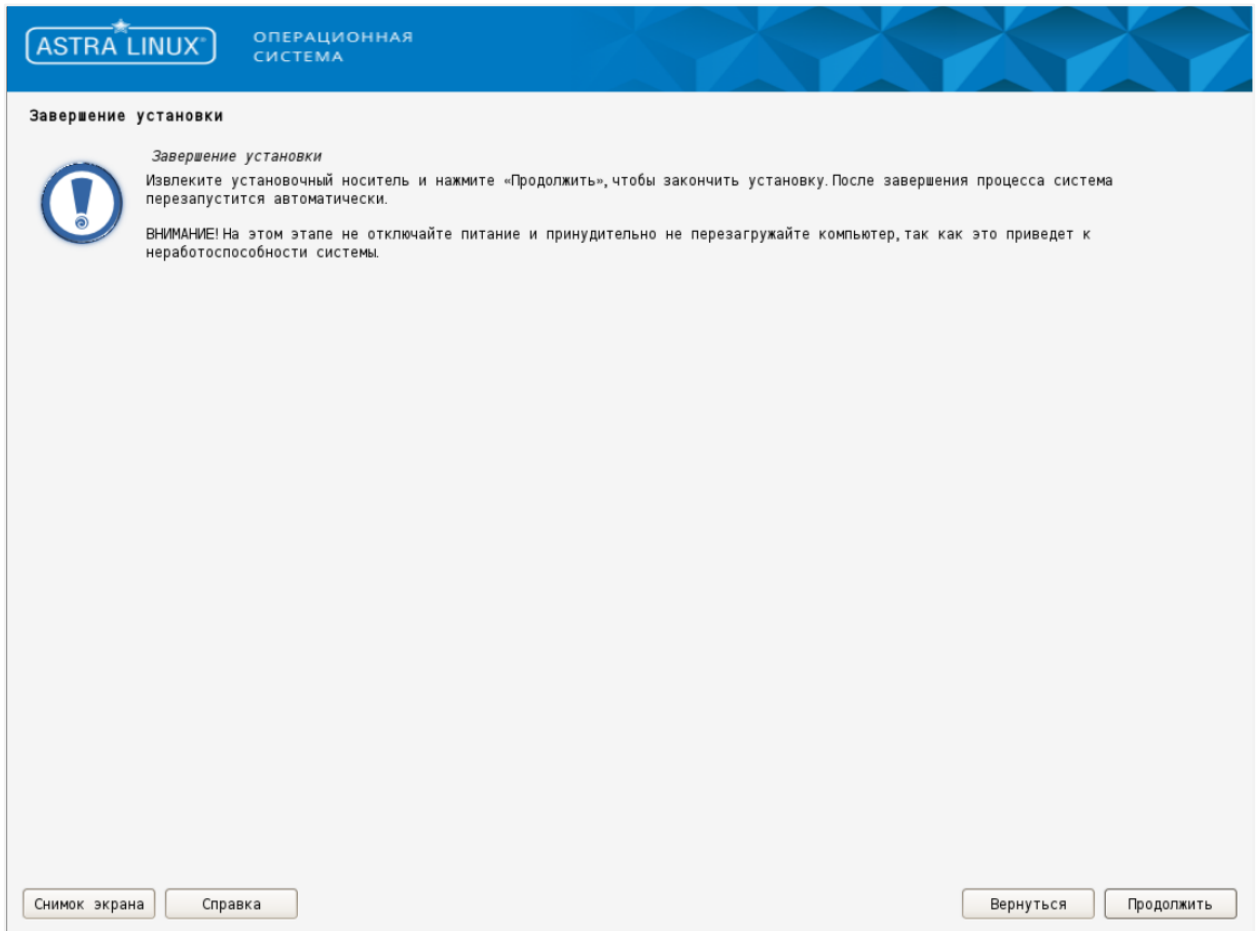


Рисунок 6.27 Уведомление об успешной установке Astra Linux

12. Выполните вход в систему под ранее созданным пользователем.

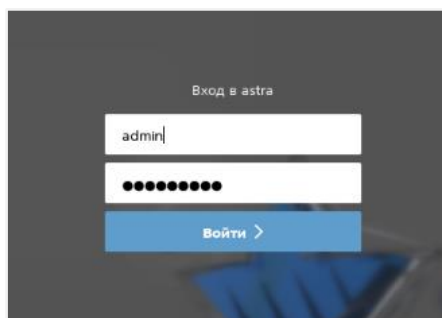


Рисунок 6.28 Вход в систему

13. Откройте на редактирование файл `/etc/network/interfaces` и укажите настройки конфигурации сети.

```
sudo nano /etc/network/interfaces
```

```
auto eth0
allow-hotplug eth0
iface eth0 inet static
address 192.168.21.100
netmask 255.255.255.0
gateway 192.168.21.1
dns-nameservers 192.168.21.225
```

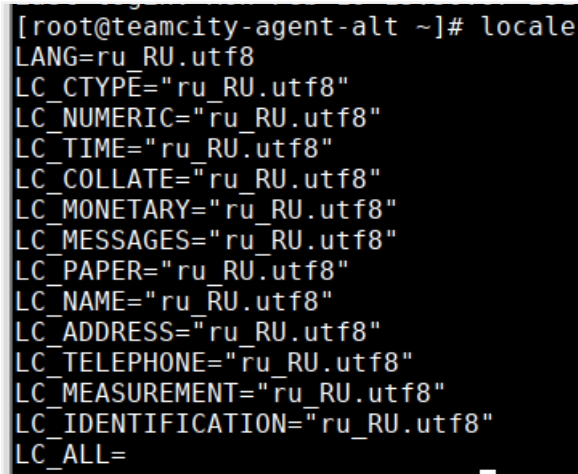
14. Для обновления сетевых настроек выполните команду:

```
sudo systemctl restart networking
```

### 6.1.4 Дополнительные действия по настройке

1. Установите системную локаль ru\_RU.utf8 (допустимо выбрать любую другую локаль, использующую UTF-8, однако при использовании нерусской локали вы лишитесь возможности читать кириллические сообщения об ошибках).

Пример корректного вывода команды **locale** приведен ниже (рисунок 6.29).



```
[root@teamcity-agent-alt ~]# locale
LANG=ru_RU.utf8
LC_CTYPE="ru_RU.utf8"
LC_NUMERIC="ru_RU.utf8"
LC_TIME="ru_RU.utf8"
LC_COLLATE="ru_RU.utf8"
LC_MONETARY="ru_RU.utf8"
LC_MESSAGES="ru_RU.utf8"
LC_PAPER="ru_RU.utf8"
LC_NAME="ru_RU.utf8"
LC_ADDRESS="ru_RU.utf8"
LC_TELEPHONE="ru_RU.utf8"
LC_MEASUREMENT="ru_RU.utf8"
LC_IDENTIFICATION="ru_RU.utf8"
LC_ALL=
```

Рисунок 6.29 Вывод команды locale

Терминал SSH, используемый для подключения к системе, также должен быть настроен на отображение текста в UTF-8.

2. Сделайте из текущей настроенной VM шаблон, из которого вы в дальнейшем будете создавать другие VM для компонентов системы. Для этого выполните следующую команду на хосте виртуализации, где запущена VM01:

```
prlctl stop vm01
prlctl clone vm01 --name templatevm01
prlctl set templatevm01 --template yes
prlctl start vm01
```

Для VM, создаваемых на базе этого шаблона, рекомендуется создать таблицу с именами и IP-адресами VM:

Host name	IP	User	Description

### 6.1.5 Клонирование VM из шаблона

Для создания новых VM на базе созданного выше шаблона сделайте следующее:

1. Создайте новую VM из шаблона, выполнив следующую команду на хосте виртуализации:

```
prlctl create vm02 --ostemplate templatevm01
```

При необходимости созданную VM можно переименовать:

```
prlctl stop vm02
prlctl set vm02 --name vms-deploy
prlctl list -a
prlctl start vms-deploy
```

2. Подключитесь к вновь созданной VM через SSH и укажите для нее уникальное (среди других VM в этой сети) имя хоста в формате FQDN командой:

```
hostnamectl set-hostname hostname
```

3. Задайте для VM уникальный (в рамках текущей сети) IP-адрес, отредактировав файл `/etc/net/ifaces/eth0`.

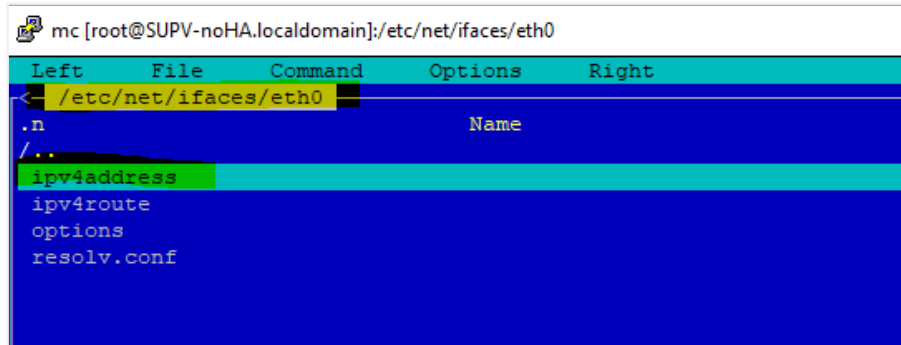


Рисунок 6.30 Добавление IP-адреса для VM

4. Перезагрузите VM для применения обновленных сетевых настроек.
5. Убедитесь, что команды `hostname -s` и `hostname -f` выполняются без явных задержек и выводят короткое и полное (FQDN) имена хоста.

## 6.2 Установка в конфигурации без отказоустойчивости (не-HA режим)



### Осторожно

Если при инсталляции продукта используются FQDN, то с сервера развертывания и всех Бэкендов должны резолвиться используемые имена.

Для не-HA-конфигурации в случае установки **Бэкенда Базис.vControl** на виртуальную машину (VM) под управлением **Р-Виртуализации** VM рекомендуется располагать в хранилище **ПК Р-Хранилище** с включенным флагом HA (high availability) с высоким приоритетом.

Установка Бэкенда и Фронтенда Базис.vControl осуществляются на один хост.



## 6.2.1 Установка Бэкенда и Фронтенда Базис.vControl



### Совет

Основные параметры конфигурации для **Базис.vControl** содержатся в файле `vms-config`. Фактическое содержание параметров должно соответствовать плану развёртывания (если таковой спроектирован заранее).

При установке **Бэкенда Базис.vControl** на Альт 9 должны быть подключены официальные репозитории для этой ОС из сети Интернет.

1. Скопируйте архивы **`vms-deploy-X.tgz`** и **`environment.tgz`** со скриптами установки на сервер, где будет установлен **Бэкенд Базис.vControl**. Распакуйте **`vms-deploy-X.tgz`**.

```
tar -xf vms-deploy-X.tgz
```

2. Скопируйте или переименуйте файл **`deploy/vms-config-example`** в **`deploy/vms-config`**.
3. Установите удобный вам консольный текстовый редактор и настройте необходимые параметры в конфигурационном файле **`deploy/vms-config`**.

```
apt-get install mc
cd deploy
mcedit vms-config
```



### Осторожно

Напрямую править конфигурационные файлы в `/etc/vms*.yaml` или в составе RPM-пакетов нельзя: они будут перезаписаны при следующем обновлении.

Если необходимо изменить какой-то внутренний параметр **Базис.vControl**, который не содержится в **`vms-config`**, то для **Бэкенда** его необходимо прописать в файл переопределений **`backend-overrides`**. Все, что было переопределено в **`backend-overrides`**, добавится в `/etc/vms.yaml`.

При необходимости добавить переопределение после того, как **Бэкенд** был установлен, нужно внести необходимые параметры в **`backend-overrides`** и

переустановить **Бэкенд** (повторить последовательность действий, описанную в этой главе).

Для обнуления ранее прописанных переопределений нужно выполнить переустановку **Бэкенда** с пустым *backend-overrides*.

---



### Осторожно

Напрямую править конфигурационные файлы в */etc/vms-agent\*.yaml* или в составе RPM-пакета нельзя: они будут перезаписаны при следующем обновлении.

Если необходимо изменить какой-то внутренний параметр **Агентов**, который не содержится в *vms-config*, то для агента его необходимо прописать в файл переопределений *agent-overrides*. Все, что было переопределено в *agent-overrides*, добавится в */etc/vms-agent.yaml*.

При необходимости добавить переопределение после того, как агент был установлен, нужно внести необходимые параметры в *agent-overrides*, выполнить установочный скрипт с параметром **-o**:

```
./deploy.sh -o
```

---



### Примечание

Для Astra Linux установка выполняется от непривилегированного пользователя, которому доступно sudo без пароля. Если установка идет при прямом доступе в консоль (не через ssh), то во время логина пользователя *integrity level* должен быть выбран «63».

Затем необходимо переустановить **Агента**, обновив его в веб-интерфейсе.

Для обнуления ранее прописанных переопределений нужно выполнить переустановку **Агента** с пустым *agent-overrides*.

---

Ниже представлен пример содержимого файла *vms-config*, используемого скриптом развёртывания:

```
vms_superuser_name: 'AdminName'
vms_superuser_pass: 'AdminPassword'
vms_superuser_mail: 'username@domain.com'

vdi_enable: false
vdi_api:
  - '192.168.0.12'
  - '192.168.0.13'
  - '192.168.0.14'
vdi_redis_pass: 'RedisPassword'
vdi_redis_hosts:
  - '192.168.0.12'
  - '192.168.0.13'
  - '192.168.0.14'

embedded_pgsql: false
pgsql_vms_db: 'vmsdb'
pgsql_vms_user: 'vmsremote'
pgsql_vms_pass: 'vmsPassword'
pgsql_bind_port: '5432'
pgsql_bind_ip: '192.168.0.253'
# Необязательные параметры:
#pgsql_bind_ip_replicas:
# - '192.168.0.253'
# - '192.168.0.254'
#pgsql_bind_port_replicas: '5433'
#use_pgouncer: false
#pgbouncer_auth_type: 'scram-sha-256'
#pgbouncer_auth_scram_secret: "SCRAM-SHA-
256$4096:ZJAsnmqlOhXer+NxITyIJw==setLxHXQL5F8wb453z5s9j0rYa5s/pImW/Y
SovYNTIDE=:/2zTmWypfeyRjPMwIQdB5eRhI3T1vfJSH4drSrCJ/p8="
#custom_pgsql_pkg_name: 'postgres19.6=9.6.9-alt0.M70C.1'
#custom_pgsql_server_pkg_name: 'postgres19.6-server=9.6.9-
alt0.M70C.1'
#custom_libpq_pkg_name: 'libpq5.9=9.6.9-alt0.M70C.1'

ntp_servers:
  - '192.168.0.254'

ha_deploy: false
external_virtualization: false
clickhouse_on_backend: true
redis_on_backend: true
keepalived_on_backend: true
vips:
  backend:
    vip: '192.168.0.10'
```

```
vrouter_id: '10'
clickhouse:
  vip: '192.168.0.11'
  vrouter_id: '11'

logs:
log_path: /var/log
  backend:
    save_last_days: 30
  agent:
    save_last_days: 30
  clickhouse:
    save_last_month: 6

redis_pass: 'RedisPassword'
```



### Совет

Правила описания параметров в YAML-формате представлены в разделе Приложения [Правила редактирования конфигурационных файлов](#).

---

Описание конфигурационных параметров:

- **stage** — необязательный параметр, задает «имя» текущей установки, применяется для удобства отслеживания исключений в Sentry по конкретным установкам **Базис.vControl**.

Может содержать английские буквы и цифры, тире, подчеркивание.

- **vms\_superuser\_\*** — имя (`_name`), пароль (`_pass`) и адрес эл.почты (`_mail`) администратора **Базис.vControl** с повышенными привилегиями; пароль должен содержать минимум 5 символов.

Процедура деактивации/активации учетной записи изложена в Приложении Деактивация/активация суперпользователя.

- **vdi\_enable** — включить поддержку **Базис.WorkPlace**.

Устанавливается в **true** только в том случае, если производится обновление системы с уже установленным **Базис.WorkPlace**, либо при подключении установленного **Базис.WorkPlace** в новой установке комплекса. При первой установке **Базис.vControl** этот параметр должен быть выставлен в **false**.

- **vdi\_api** — список IP-адресов **Бэкенда/ов Базис.WorkPlace**.

В случае ***vdi\_enable: false*** список может отсутствовать.

- ***vdi\_redis\_pass*** — пароль для доступа к Redis Базис.WorkPlace (параметр ***redis\_pass*** в Базис.WorkPlace).

В случае ***vdi\_enable: false*** пароль может отсутствовать.

- ***vdi\_redis\_host*** — список IP-адресов серверов, на которых установлен Redis для Базис.WorkPlace.

В случае, если при установке BPM использовался параметр ***redis\_on\_backend: true***, то данный список аналогичен списку IP-адресов BPM **Бэкенда/ов Базис.WorkPlace**. В случае ***vdi\_enable: false*** список может отсутствовать.

- ***embedded\_pgsql*** — производить ли установку локальной версии PostgreSQL в системе, куда будет установлен **Бэкенд Базис.vControl**.

При значении ***false*** система будет ожидать, что будут переданы все необходимые параметры для подключения к внешней PostgreSQL. При значении ***true*** будет произведена локальная установка PostgreSQL, при этом параметры ***pgsql\_bind\_port***, ***pgsql\_bind\_ip*** игнорируются (прослушивается 127.0.0.1:5432).

В случае использования внешнего сервера PostgreSQL базу создавать не нужно — установщик **Базис.vControl** сделает это сам. Учетная запись для подключения к серверу должна иметь права на создание базы.

---

### **Примечание**

При использовании внешней установки PostgreSQL количество подключений к БД должно быть минимум 500 (параметр ***max\_connections***).

---

- ***pgsql\_vms\_db*** — имя базы данных для **Базис.vControl** (актуально при ***embedded\_pgsql=true/false***).
- ***pgsql\_vms\_user*** — пользователь, под учетной записью которого **Базис.vControl** будет подключаться к базе (актуально при ***embedded\_pgsql=true/false***).

В случае использования внешней PostgreSQL пользователь должен обладать правами на создание базы данных (***createdb***).

- ***pgsql\_vms\_pass*** — пароль для пользователя, под учетной записью которого будет происходить подключение **Базис.vControl** к базе (актуально при ***embedded\_pgsql=true/false***).
- ***pgsql\_bind\_port*** — слушающий порт для подключений внешней PostgreSQL (актуально при ***embedded\_pgsql=false***).
- ***pgsql\_bind\_ip*** — слушающий IP-адрес для подключений внешней PostgreSQL (актуально при ***embedded\_pgsql=false***).

- ***custom\_pgsql\_pkg\_name*** — опциональный параметр; имя пакета и версия для клиентских библиотек и утилит PostgreSQL.
- ***custom\_pgsql\_server\_pkg\_name*** — опциональный параметр; имя пакета и версия для серверных библиотек и утилит PostgreSQL.
- ***custom\_libpq\_pkg\_name*** — опциональный параметр; имя пакета для указанной версии libpq.

Используется в тех случаях, когда в репозитории присутствует более одной версии PostgreSQL, пакеты которой привязаны к конкретной версии libpq.

---

### **Примечание**

Параметры вида ***custom\_pgsql\_\*\*\**** должны выставляться только в том случае, если есть необходимость использовать другой PostgreSQL взамен используемого по умолчанию в данной системе. Актуально и для локальной установки PostgreSQL-сервера (***embedded\_pgsql: true***), и для использования внешнего сервера PostgreSQL так, как в систему ставится клиент PostgreSQL. По умолчанию ставится:

- для Astra Linux используется Postgres 9.6 из установочного диска ОС;
  - для Альт 8.1 используется версия PostgreSQL из установочного диска ОС.
- 

- ***pgsql\_bind\_ip\_replicas*** (опциональный параметр) — список резервных IP адресов для подключения хостов репликации.

Актуально для HA-инсталляции **vControl/WorkPlace** при обеспечении работы с СУБД PostgreSQL по нескольким IP адресам с автоматическим переключением на резервный адрес.

---

### **Примечание**

При объявлении списка ***pgsql\_bind\_ip\_replicas*** необходимо сконфигурировать реплики на переход в режим чтение/запись при отказе Мастера. Если реплика будет доступна только на чтение, то **Бэкенд WorkPlace/Бэкенд vControl** работоспособен не будет.

---

- ***pgsql\_bind\_port\_replicas*** (опциональный параметр) — порт для хостов реплик (актуально при объявленном списке ***pgsql\_bind\_ip\_replicas***).

Поддерживается указание одного порта для всех реплик. Если переменная ***pgsql\_bind\_port*** не объявлена, либо объявлена без значения, то по умолчанию будет использоваться порт, указанный в ***pgsql\_bind\_port***.

---

### **Осторожно**

При указании нескольких адресов реплик резерв должен становиться Мастером при помощи сторонних средств, т.е. реплика должна стать доступной на запись при недоступности БД по основному адресу. Если реплика будет доступна только на чтение, то **Бэкенд WorkPlace/Бэкенд vControl** работоспособен не будет. Логин/пароль пользователя БД на репликах должны быть те же самые, что и на Мастере.

---

- ***ntp\_servers*** (необязательный параметр) — список NTP-серверов.
  - ***use\_pgouncer*** — использовать pgbouncer для доступа к postgresql. В этом режиме на каждый бэкенд будет установлен pgbouncer; только он будет обращаться напрямую в postgresql, а Базис.Workplace будет подключаться к pgbouncer. Параметр учитывается только при использовании внешнего сервера postgresql (`embedded_pgsql: false`)
- 

### **Примечание**

Все соединения к postgresql (для vControl 800 ) будут равномерно распределены по каждому pgbouncerу на каждом бэкенде (при трех Бэкендах получаем 800/3, т.е. по 266 соединений максимум к postgresql с одного bouncer). Лимит на клиентские подключения к самому bouncer - 2000.

---

- ***pgbouncer\_auth\_type*** — тип авторизации в pgbouncer. По умолчанию параметр имеет значение md5.

Не требует заполнения, если ваш сервер postgresql поддерживает md5 авторизацию. Пример приведен для типа авторизации scram-sha-256.

- ***pgbouncer\_auth\_scram\_secret*** — scram секрет из таблицы postgres.pg\_shadow на сервере postgresql для пользователя postgres\_vdi\_user.

Обязательный параметр при `pgbouncer_auth_type: 'scram-sha-256'`, в остальных случаях не учитывается.

При его наличии в конфигурационном файле на всех серверах (**Бэкенд, хосты Р-Виртуализации**) будет настроен openNTPD/chronyd, и заданные серверы будут использоваться для синхронизации времени.

---



### Осторожно

Если параметр ***ntp\_servers*** не указан, то системный администратор должен сам настроить NTP и обеспечить синхронизацию времени между всеми компонентами системы.

---



### Примечание

Пример получения содержимого переменной `pgbouncer_auth_scram_secret` для пользователя 'ПОЛЬЗОВАТЕЛЬ' из базы на сервере postgres. Запускается из подсистемной учетной записи postgres:

```
psql -Atq -d postgres -c "SELECT passwd FROM pg_shadow
where username='ПОЛЬЗОВАТЕЛЬ';"
```

---

- ***ha\_deploy*** — установка в режиме отказоустойчивости (HA-режим).

При установке в конфигурации без отказоустойчивости параметр должен иметь значение ***false***.

- ***external\_virtualization*** — параметр, отвечающий за использование ClickHouse как внешнего сервиса.

При выставлении этого параметра в ***true*** будет пропущена установка ClickHouse, поэтому требуется использование внешнего кластера ClickHouse.

---



### Осторожно

При выставлении параметра в ***true*** не гарантируется корректная работа с гипервизорами на базе Росплатформы/vCore. Не устанавливайте значение ***true*** для этого параметра, если планируется работа с Росплатформой/vCore.

---

- ***clickhouse\_on\_backend*** — ClickHouse-кластер будет располагаться на хостах Бэкенда.

При этом файл ***clickhouse-hosts*** игнорируется, установка идет на хосты из файла ***backends-hosts***, а настройки секции ***vips.clickhouse.\**** не учитываются.

---



- **redis\_on\_backend** — Redis-кластер будет располагаться на хостах **Бэкенда**, при этом файл **redis-hosts** игнорируется, установка идет на хосте из файла **backends-hosts**.
- **keepalived\_on\_backend** (необязательный параметр) — отвечает за установку сервиса keepalived на хостах Бэкенда, ClickHouse.

При установке параметра в значение **true** инсталлятор разворачивает и настраивает сервис keepalived. При значении параметра **false** необходимо использовать внешний балансировщик.

IP-адрес или FQDN балансировщика указывается в качестве значения в параметрах **vips.backend.vip** и **clickhouse\_ip**.

---

### **Примечание**

При установке параметра **keepalived\_on\_backend** в значение **false** параметр **vrouter\_id** учитываться не будет, т.е. является необязательным.

---

- **vips** — описание настройки VRRP для доступа к backend-хостам и кластеру ClickHouse.

В конфигурационном файле параметры прописываются именно так, как показано в примере выше.

Далее уровень иерархии в параметре обозначен точкой ('vips.');

- **vips.backend.vip** — виртуальный IP-адрес для **Бэкенда Базис.vControl**, который будет перемещаться, если хост выйдет из строя;
- **vips.backend.vrouter\_id** — vrrp router id, который должен задаваться целым числом от 0 до 255 и быть уникальным в рамках L2-сети;
- **vips.clickhouse.vip** — виртуальный IP-адрес для ClickHouse, который будет перемещаться, если хост выйдет из строя;
- **vips.clickhouse.vrouter\_id** — vrrp router id, который должен задаваться целым числом от 0 до 255 и быть уникальным в рамках L2-сети'.

---

### **Осторожно**

При установке в конфигурации с отказоустойчивостью (HA-режим) параметр **vips.clickhouse** является обязательным. Значение параметра не должно совпадать со значением параметра **vips.backend**;

---

- **logs** — описание настройки параметров ротации логов.

В конфигурационном файле параметры прописываются именно так, как показано в примере (см. выше).

Далее уровень иерархии в параметре обозначен точкой.

- **`log_path`** — параметр устанавливает общий путь для хранения всех логов.
- **`logs.backend.save_last_days`** — сколько дней хранить логи **Бэкенда/Менеджера агентов**.

Во избежание слишком сильного разрастания файлов с логами ротация происходит каждый день, логи за предыдущий день сжимаются.

- **`logs.agent.save_last_days`** — сколько дней хранить логи **Агента**.

Во избежание слишком сильного разрастания файлов с логами ротация происходит каждый день, логи за предыдущий день сжимаются.

- **`logs.clickhouse.save_last_month`** — сколько последних месяцев хранить метрики ВС и серверов (загрузка CPU, памяти, диска и т.д.).
- **`logs.veritas_adapter.save_last_days`** — сколько дней хранить данные резервного копирования (настройка адаптера Veritas NetBackup).
- **`redis_pass`** — пароль, который будет использоваться для доступа к Redis Базис.vControl.



### Примечание

Пароль, указанный в качестве значения параметра **`redis_pass`**, используется также для аутентификации в **`redis_sentinel`**.

---

Запустите скрипт установки **Бэкенда** из-под учетной записи `root` следующей командой с указанием пути к файлу с парольной фразой в обязательном параметре **`-v`**:

```
./deploy.sh -s -a environment.tgz -v /path/to/vault-password-file
```



### Примечание

Файл с парольной фразой — это текстовый файл, в котором открытым текстом записывается парольная фраза. С данной парольной фразой через `ansible-vault` шифруются все конфигурационные файлы продукта, содержащие пароли.

---

## Осторожно

Установка **Бэкенда Базис.vControl** будет выполнена успешно только при развертывании системы через SSH. При этом подключение к хосту должно происходить только от пользователя root, подключение непривилегированным пользователем и переключение на root через sudo/su приведет к ошибке развертывания.

Для Astra Linux установка выполняется от непривилегированного пользователя, которому доступно sudo без пароля. Если установка идет при прямом доступе в консоль (не через ssh), то во время логина пользователя *integrity level* должен быть выбран «63».

После выполнения скрипта установка решения **Базис.vControl** будет завершена. При успешной установке будет выведено сообщение с версиями установленных RPM-пакетов с компонентами, например:

```
PLAY RECAP *****
backend-1           : ok=137  changed=49  unreachable=0  failed=0
backend-2           : ok=129  changed=49  unreachable=0  failed=0
backend-3           : ok=129  changed=49  unreachable=0  failed=0

Скала-Р Управление успешно установлен.
Версии установленных компонентоv:
vms-backend:
  version:0.18 build:3246 Пт 02 фев 2018 02:55:58
vms-frontend:
  version:0.18 build:529 Чт 01 фев 2018 20:56:57
vms-frontend-vdi:
  version:0.18 build:529 Чт 01 фев 2018 21:01:44
vms-agent:
  version:0.18 build:970 Пт 02 фев 2018 02:44:04
vms-playbooks:
  version:0.18 build:285 Пт 02 фев 2018 11:49:44
[root@ha-deploy deploy]#
```

Рисунок 6.31 Сообщение об установке Базис.vControl

В случае возникновения ошибок при выполнении скрипта установки их список выводится в консоль; дополнительно, вывод дублируется в лог-файл */opt/vms-playbooks/logs/ansible.log*.

## 6.3 Установка в конфигурации с отказоустойчивостью (HA-режим)

Установка решения в HA-режиме состоит из следующих шагов:

1. Установка **Сервера развертывания**, с которого будет происходить установка остальных компонентов;
2. Установка кластера Redis;
3. Установка кластера ClickHouse;
4. Установка нескольких хостов с **Бэкендом и Фронтом Базис.vControl**;
5. Подключение агентов из WEB UI **Базис.vControl**.

### **Примечание**

Для установки **Базис.vControl** в HA режиме может использоваться только внешний сервер PostgreSQL (параметр *embedded\_psql: false* в конфигурационном файле).

Схема взаимодействия компонентов показана на рисунке 6.32.

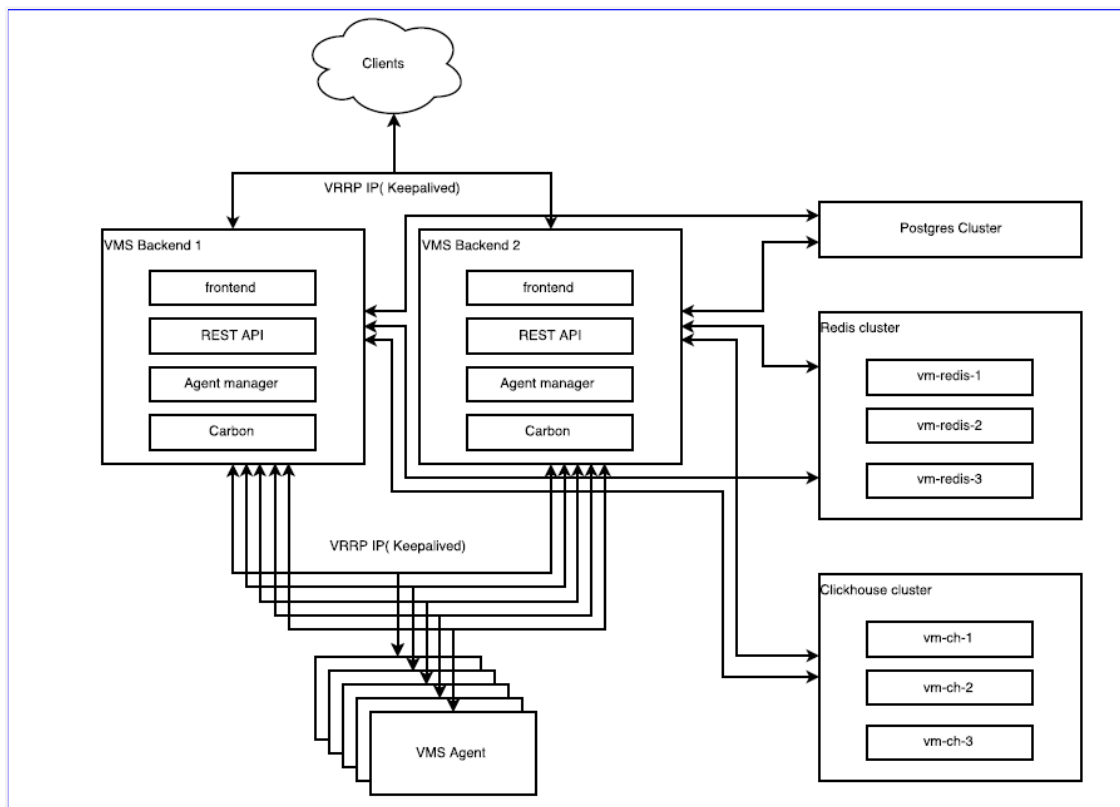


Рисунок 6.32 Установка в конфигурации с отказоустойчивостью на несколько хостов

---

### Примечание

Для Astra Linux установка выполняется от непривилегированного пользователя, которому доступно `sudo` без пароля. Если установка идет при прямом доступе в консоль (не через `ssh`), то во время логина пользователя *integrity level* должен быть выбран «63».

Для ОС Альт установка производится от пользователя `root`.

---

### Совет

Основные параметры конфигурации для **Базис.vControl** содержатся в файле *vms-config*, подготавливаемом на сервере развёртывания (см. ниже). Фактическое содержание параметров должно соответствовать плану развёртывания (если таковой спроектирован заранее).

---

### 6.3.1 Установка Сервера развёртывания

---

#### Осторожно

Если при инсталляции продукта используются FQDN, то с сервера развёртывания и всех Бэкендов должны резолвиться используемые имена.

---

### Примечание

**Сервер развёртывания** нельзя совмещать с другими компонентами **Базис.vControl**.

Если произошла смена IP адреса **сервера развёртывания**, то перед развёртыванием **Бэкендов** необходимо на хостах **Бэкендов** выполнить удаление базовой и дополнительной конфигураций:

---

```
rm -fr /etc/apt/sources.list.d/vms-  
base.yml /etc/apt/sources.list.d/vms-addons.yml
```

---

1. Скопируйте архивы **vms-deploy-X.tgz** и **environment.tgz** со скриптами установки в папку **/root** сервера развертывания **Базис.vControl**.
2. Распакуйте **vms-deploy-X.tgz**.

```
tar -xvzf /root/vms-deploy-X.tgz
```

3. Скопируйте или переименуйте файл **/root/deploy/vms-config-example** в **/root/deploy/vms-config**.
4. Установите удобный вам консольный текстовый редактор и настройте необходимые параметры в конфигурационном файле **/root/deploy/vms-config**:

```
apt-get install mc  
cd /root/deploy  
mcedit vms-config
```



### Осторожно

Напрямую править конфигурационные файлы в **/etc/vms\*.yaml** или в составе RPM-пакетов нельзя: они будут перезаписаны при следующем обновлении.

Если необходимо изменить какой-то внутренний параметр **Базис.vControl**, который не содержится в **vms-config**, то для **Бэкенда** его необходимо прописать в файл переопределений **backend-overrides**. Все, что было переопределено в **backend-overrides**, добавится в **/etc/vms.yaml**.

При необходимости добавить переопределение после того, как **Бэкенд** был установлен, нужно внести необходимые параметры в **backend-overrides** и переустановить **Бэкенд** (повторить последовательность действий, описанную в этой главе).

Для обнуления ранее прописанных переопределений нужно выполнить переустановку **Бэкенда** с пустым **backend-overrides**.

---

Ниже представлен пример содержимого конфигурационного файла vms-config, используемого сценарием развертывания:

```
vms_superuser_name: 'AdminName'
vms_superuser_pass: 'AdminPassword'
vms_superuser_mail: 'username@domain.com'

vdi_enable: false
vdi_api:
  - '192.168.0.12'
  - '192.168.0.13'
  - '192.168.0.14'
vdi_redis_hosts:
  - '192.168.0.12'
  - '192.168.0.13'
  - '192.168.0.14'
vdi_redis_pass: 'RedisPassword'

embedded_pgsql: false
pgsql_vms_db: 'vmsdb'
pgsql_vms_user: 'vmsremote'
pgsql_vms_pass: 'vmsPassword'
pgsql_bind_port: '5432'
pgsql_bind_ip: '192.168.0.253'
# Необязательные параметры:
#pgsql_bind_ip_replicas:
# - '192.168.0.253'
# - '192.168.0.254'
#pgsql_bind_port_replicas: '5433'
#use_pgouncer: false
#pgouncer_auth_type: 'scram-sha-256'
#pgouncer_auth_scram_secret: "SCRAM-SHA-
256$4096:ZJAsnmqlOhXer+NxITyIJw==$etLxHXQL5F8wb453z5s9j0rYa5s/pImW/Y
SovYNTIDE=:/2zTmWypfeyRjPMwIQdB5eRhI3T1vfJSH4drSrCJ/p8="
#custom_pgsql_pkg_name: 'postgresql9.6=9.6.9-alt0.M70C.1'
#custom_pgsql_server_pkg_name: 'postgresql9.6-server=9.6.9-
alt0.M70C.1'
#custom_libpq_pkg_name: 'libpq5.9=9.6.9-alt0.M70C.1'

ntp_servers:
  - '192.168.0.254'

ha_deploy: true
external_virtualization: false
clickhouse_on_backend: true
redis_on_backend: true
keepalived_on_backend: true
```

```
vips:
  backend:
    vip: '192.168.0.10'
    vrouter_id: '10'
  clickhouse:
    vip: '192.168.0.11'
    vrouter_id: '11'

logs:
log_path: /var/log
  backend:
    save_last_days: 30
  agent:
    save_last_days: 30
  clickhouse:
    save_last_month: 6

redis_pass: 'RedisPassword'
```

Описание конфигурационных параметров:

- **stage** — необязательный параметр, задает «имя» текущей установки, применяется для удобства отслеживания исключений в Sentry по конкретным установкам **Базис.vControl**.

Может содержать английские буквы и цифры, тире, подчеркивание.

- **vms\_superuser\_\*** — имя (`_name`), пароль (`_pass`) и адрес эл.почты (`_mail`) администратора **Базис.vControl** повышенными привилегиями; пароль должен содержать минимум 5 символов.

Процедура деактивации/активации учетной записи изложена в Приложении [Деактивация/активация суперпользователя](#).

- **vdi\_enable** — включить поддержку **Базис.WorkPlace**.

Устанавливается в **true** только в том случае, если производится обновление системы с уже установленным **Базис.WorkPlace**, либо при подключении установленного **Базис.WorkPlace** в новой установке комплекса. При первой установке **Базис.vControl** этот параметр должен быть выставлен в **false**.

- **vdi\_api** — список IP-адресов **Бэкенда/ов Базис.WorkPlace**.

В случае **vdi\_enable: false** может отсутствовать.

- **vdi\_redis\_pass** - пароль для доступа к Redis Базис.WorkPlace (параметр **redis\_pass** в Базис.WorkPlace).

В случае **vdi\_enable: false** может отсутствовать.



- ***vdi\_redis\_host*** - список IP-адресов серверов, на которых установлен Redis для Базис.WorkPlace.

В случае, если при установке BPM использовался параметр ***redis\_on\_backend: true***, данный список аналогичен списку IP-адресов BPM **Бэкенда/ов Базис.WorkPlace**. В случае ***vdi\_enable: false*** может отсутствовать.

- ***embedded\_pgsql*** — производить ли установку локальной версии PostgreSQL в системе, куда будет установлен **Бэкенд Базис.vControl**.

При значении ***false*** система будет ожидать, что будут переданы все необходимые параметры для подключения к внешней PostgreSQL. При значении ***true*** будет произведена локальная установка PostgreSQL, при этом параметры ***pgsql\_bind\_port***, ***pgsql\_bind\_ip*** игнорируются (прослушивается 127.0.0.1:5432).

---

### **Примечание**

В случае использования внешнего сервера PostgreSQL базу создавать не нужно — установщик **Базис.vControl** сделает это сам. Учетная запись для подключения к серверу должна иметь права на создание базы.

При использовании внешней установки PostgreSQL количество подключений к БД должно быть минимум 500 (параметр ***max\_connections***).

---

- ***pgsql\_vms\_db*** — имя базы данных для **Базис.vControl**.

Актуально при ***embedded\_pgsql=true/false***.

- ***pgsql\_vms\_user*** — пользователь, под учетной записью которого **Базис.vControl** будет подключаться к базе.

Актуально при ***embedded\_pgsql=true/false***. В случае использования внешней PostgreSQL пользователь должен обладать правами на создание базы данных (***createdb***).

- ***pgsql\_vms\_pass*** — пароль для пользователя, под учетной записью которого будет происходить подключение **Базис.vControl** к базе.

Актуально при ***embedded\_pgsql=true/false***.

- ***pgsql\_bind\_port*** — слушающий порт для подключений внешней PostgreSQL. Актуально при ***embedded\_pgsql=false***.
- ***pgsql\_bind\_ip*** — слушающий IP-адрес для подключений внешней PostgreSQL. Актуально при ***embedded\_pgsql=false***.
- ***custom\_pgsql\_pkg\_name*** — опциональный параметр; имя пакета и версия для клиентских библиотек и утилит PostgreSQL.
- ***custom\_pgsql\_server\_pkg\_name*** — опциональный параметр; имя пакета и версия для серверных библиотек и утилит PostgreSQL.

- ***custom\_libpq\_pkg\_name*** — опциональный параметр; имя пакета для указанной версии libpq.

Используется в тех случаях, когда в репозитории присутствует более одной версии PostgreSQL, пакеты которой привязаны к конкретной версии libpq.

---



### Примечание

Параметры вида ***custom\_pgsql\_\*\*\**** должны выставляться только в том случае, если есть необходимость использовать другой PostgreSQL взамен используемого по умолчанию в данной системе. Актуально и для локальной установки PostgreSQL-сервера (***embedded\_pgsql: true***), и для использования внешнего сервера PostgreSQL так, как в систему ставится клиент PostgreSQL. По умолчанию ставится:

- Для Astra Linux используется Postgres 9.6 из установочного диска ОС.
  - Для Альт 8.1 используется версия PostgreSQL из установочного диска ОС.
- 

- ***pgsql\_bind\_ip\_replicas*** - опциональный параметр; список резервных IP адресов для подключения хостов репликации.

Актуально для HA-инсталляции **vControl/WorkPlace** - при обеспечении работы с СУБД PostgreSQL по нескольким IP адресам с автоматическим переключением на резервный адрес. При объявлении списка ***pgsql\_bind\_ip\_replicas*** необходимо сконфигурировать реплики на переход в режим чтение/запись при отказе Мастера. Если реплика будет доступна только на чтение, то **Бэкенд WorkPlace/Бэкенд vControl** работоспособен не будет.

- ***pgsql\_bind\_port\_replicas*** - опциональный параметр; порт для хостов реплик.

Актуально при объявленном списке ***pgsql\_bind\_ip\_replicas***. Поддерживается указание одного порта для всех реплик. Если переменная ***pgsql\_bind\_port*** не объявлена, либо объявлена без значения, то по умолчанию будет использоваться порт, указанный в ***pgsql\_bind\_port***.

---



### Осторожно

При указании нескольких адресов реплик резерв должен становиться Мастером при помощи сторонних средств, т.е. реплика должна стать доступной на запись при недоступности БД по основному адресу. Если реплика будет доступна только на чтение, то **Бэкенд WorkPlace/Бэкенд vControl** работоспособен не будет. Логин/пароль пользователя БД на репликах должны быть те же самые, что и на Мастере.

---

- ***ntp\_servers*** — список NTP-серверов, необязательный параметр.

При его наличии в конфигурационном файле на всех серверах (**Бэкенд**, хосты **Р-Виртуализации**) будет настроен `openNTPD/chronyd`, и заданные серверы будут использоваться для синхронизации времени.

---

### **Осторожно**

Если параметр ***ntp\_servers*** не указан, то системный администратор должен сам настроить NTP и обеспечить синхронизацию времени между всеми компонентами системы.

---

- ***use\_pgouncer*** — использовать `pgbouncer` для доступа к `postgresql`. В этом режиме на каждый бэкенд будет установлен `pgbouncer`; только он будет обращаться напрямую в `postgresql`, а Базис.Workplace будет подключаться к `pgbouncer`. Параметр учитывается только при использовании внешнего сервера `postgresql` (`embedded_pgsql: false`)
- 

### **Примечание**

Все соединения к `postgresql` (для `vControl 800`) будут равномерно распределены по каждому `pgbouncer` на каждом бэкенде (при трех Бэкендах получаем 800/3, т.е. по 266 соединений максимум к `postgresql` с одного `bouncer`). Лимит на клиентские подключения к самому `bouncer` - 2000.

---

- ***pgbouncer\_auth\_type*** — тип авторизации в `pgbouncer`. По умолчанию параметр имеет значение `md5`.

Не требует заполнения, если ваш сервер `postgresql` поддерживает `md5` авторизацию. Пример приведен для типа авторизации `scram-sha-256`.

- ***pgbouncer\_auth\_scram\_secret*** — `scram` секрет из таблицы `postgres.pg_shadow` на сервере `postgresql` для пользователя `pgsql_vdi_user`.

Обязательный параметр при `pgbouncer_auth_type: 'scram-sha-256'`, в остальных случаях не учитывается. При его наличии в конфигурационном файле на всех серверах (**Бэкенд**, хосты **Р-Виртуализации**) будет настроен `openNTPD/chronyd`, и заданные серверы будут использоваться для синхронизации времени.

---



### Осторожно

Если параметр ***ntp\_servers*** не указан, то системный администратор должен сам настроить NTP и обеспечить синхронизацию времени между всеми компонентами системы.

---



### Примечание

Пример получения содержимого переменной `pgbouncer_auth_scram_secret` для пользователя 'ПОЛЬЗОВАТЕЛЬ' из базы на сервере postgres. Запускается из подсистемной учетной записи postgres:

```
psql -Atq -d postgres -c "SELECT passwd FROM pg_shadow
where username='ПОЛЬЗОВАТЕЛЬ';"
```

---

- ***ha\_deploy*** — установка в режиме отказоустойчивости (HA-режим).

При установке в конфигурации с отказоустойчивостью параметр должен иметь значение ***true***.

- ***external\_virtualization*** — параметр, отвечающий за использование ClickHouse как внешнего сервиса, при выставлении этого параметра в ***true*** будет пропущена установка ClickHouse, поэтому требуется использование внешнего кластера ClickHouse.
- 



### Примечание

При выставлении параметра ***external\_virtualization*** в ***true*** будет пропущена установка ClickHouse, и не гарантируется корректная работа с гипервизорами на базе Росплатформы/vCore. Не устанавливайте значение ***true*** для этого параметра если планируется работа с Росплатформой/vCore.

---

- ***clickhouse\_on\_backend*** — ClickHouse-кластер будет располагаться на хостах **Бэкенда**, при этом файл ***clickhouse-hosts*** игнорируется, установка идет на хосты из файла ***backends-hosts***, а настройки секции ***vips.clickhouse*** \* не учитываются.

- **redis\_on\_backend** — Redis-кластер будет располагаться на хостах **Бэкенда**, при этом файл **redis-hosts** игнорируется, установка идет на хосте из файла **backends-hosts**.
- **keepalived\_on\_backend** — необязательный параметр, отвечает за установку сервиса keepalived на хостах Бэкенда, ClickHouse.

При установке параметра **keepalived\_on\_backend** в значение **true** инсталлятор разворачивает и настраивает сервис keepalived. При значении параметра **false** необходимо использовать внешний балансировщик.

IP-адрес или FQDN балансировщика указывается в качестве значения в параметрах **vips.backend.vip** и **clickhouse\_ip**.



### Примечание

При установке параметра **keepalived\_on\_backend** в значение **false** параметр **vrouter\_id** учитываться не будет, т.е. является необязательным.

---

- **vips** — описание настройки VRRP для доступа к backend-хостам и кластеру ClickHouse.

В конфигурационном файле параметры прописываются именно так, как показано в примере (см. выше). Далее уровень иерархии в параметре обозначен точкой.

- **vips.backend.vip** — виртуальный IP-адрес для **Бэкенда Базис.vControl**, который будет перемещаться, если хост выйдет из строя.
- **vips.backend.vrouter\_id** — vrrp router id, который должен задаваться целым числом от 0 до 255 и быть уникальным в рамках L2-сети.
- **vips.clickhouse.vip** — виртуальный IP-адрес для ClickHouse, который будет перемещаться, если хост выйдет из строя.



### Осторожно

При установке в конфигурации с отказоустойчивостью (HA-режим) параметр **vips.clickhouse** является обязательным. Значение параметра не должно совпадать со значением параметра **vips.backend**.

---

- **vips.clickhouse.vrouter\_id** — vrrp router id, который должен задаваться целым числом от 0 до 255 и быть уникальным в рамках L2-сети.
- **logs** — описание настройки параметров ротации логов.

В конфигурационном файле параметры прописываются именно так, как показано в примере (см. выше).

Далее уровень иерархии в параметре обозначен точкой.

- **`log_path`** — параметр устанавливает общий путь для хранения всех логов.
- **`logs.backend.save_last_days`** — сколько дней хранить логи **Бэкенда/Менеджера агентов**.

Во избежание слишком сильного разрастания файлов с логами ротация происходит каждый день, логи за предыдущий день сжимаются.

- **`logs.agent.save_last_days`** — сколько дней хранить логи **Агента**.

Во избежание слишком сильного разрастания файлов с логами ротация происходит каждый день, логи за предыдущий день сжимаются.

- **`logs.clickhouse.save_last_month`** — сколько последних месяцев хранить метрики ВС и серверов (загрузка CPU, памяти, диска и т.д.).
- **`redis_pass`** — пароль, который будет использоваться для доступа к Redis Базис.vControl.

---

### Примечание

Пароль, указанный в качестве значения параметра **`redis_pass`**, используется также для аутентификации в **`redis_sentinel`**.

---

---

### Осторожно

Напрямую править конфигурационные файлы в **`/etc/vms-agent*.yaml`** или в составе RPM-пакета нельзя: они будут перезаписаны при следующем обновлении.

Если необходимо изменить какой-то внутренний параметр **Агентов**, который не содержится в **`vms-config`**, то для агента его необходимо прописать в файл переопределений **`agent-overrides`**. Все, что было переопределено в **`agent-overrides`**, добавится в **`/etc/vms-agent.yaml`**. При необходимости добавить переопределение после того, как агент был установлен, нужно внести необходимые параметры в **`agent-overrides`** -для этого следует выполнить установочный скрипт с параметром **`-o`**:

```
./deploy.sh -o
```

---

## Примечание

Для Astra Linux установка выполняется от непривилегированного пользователя, которому доступно sudo без пароля. Если установка идет при прямом доступе в консоль (не через ssh), то во время логина пользователя **integrity level** должен быть выбран «63». Затем необходимо переустановить **Агента**, обновив его в веб-интерфейсе.

Для обнуления ранее прописанных переопределений нужно выполнить переустановку **Агента** с пустым **agent-overrides**.

После подготовки конфигурационного файла запустите скрипт развертывания компонентов **Сервера развертывания** из-под учетной записи root следующей командой с указанием пути к файлу с парольной фразой в обязательном параметре **-v**.

```
./deploy.sh -i -a environment.tgz -v /path/to/vault-password-file
```

## Примечание

Файл с парольной фразой — это текстовый файл, в котором открытым текстом записывается парольная фраза. С данной парольной фразой через ansible-vault шифруются все конфигурационные файлы продукта, содержащие пароли.

Для Astra Linux установка выполняется от непривилегированного пользователя, которому доступно sudo без пароля. Если установка идет при прямом доступе в консоль (не через ssh), то во время логина пользователя **integrity level** должен быть выбран «63».

Произойдет установка всех необходимых компонентов для дальнейшей установки **Базис.vControl** в режиме отказоустойчивости. При успешной установке будет выведено соответствующее сообщение (рисунок 6.33):

```
PLAY RECAP *****
deploy-node           : ok=20   changed=6   unreachable=0   failed=0
На локальную систему успешно установлены компоненты деплой ноды Скала-Р Управление.
[root@vms-deploy-deploy]#
```

Рисунок 6.33 Установка компонентов Сервера развертывания Базис.vControl

### 6.3.2 Пример настройки внешнего сервера Postgres 12 на Альт 9

В случае использования внешнего сервера Postgres базу создавать не нужно, установщик **Базис.vControl** сделает это сам (при условии, что сам Postgres будет предварительно установлен вручную на Postgres-сервере). Учетная запись в PostgreSQL для подключения к серверу (параметр *pgsql\_vms\_user* в конфигурационном файле) должна иметь права на создание базы.



#### Примечание

Перед установкой сервера PostgreSQL проверьте его совместимость с вашей версией инфраструктуры Базис.vControl согласно таблице из раздела [Поддерживаемые версии PostgreSQL](#).

Для настройки Postgres-сервера выполните из-под *root* следующие команды.

1. Установите сервер PostgreSQL 12:

```
apt-get install postgresql12-server
```

2. Разрешите пользователю *postgres* использование shell (по умолчанию оно запрещено):

```
usermod -s /bin/bash postgres
```

3. Инициализируйте пустой каталог для хранения файлов БД:

```
/etc/init.d/postgresql initdb
```

4. Включите клиентский доступ к базам данных на уровне хоста (по умолчанию база принимает только локальные подключения):

```
echo "host all all 0.0.0.0/0 md5" >>  
/var/lib/pgsql/data/pg_hba.conf
```

5. Укажите IP-адреса, по которым сервер будет принимать подключения клиентских приложений:



```
sed -i "s/#listen_addresses = 'localhost'/listen_addresses = '*'/"  
/var/lib/pgsql/data/postgresql.conf
```

6. Установите максимальное количество одновременных клиентских подключений к базе:

```
sed -i "s/max_connections = 100/max_connections = 1500/"  
/var/lib/pgsql/data/postgresql.conf
```

7. Добавьте службу Postgres Pro в автозагрузку и запустите ее:

```
systemctl enable postgresql  
systemctl start postgresql  
systemctl status postgresql
```

8. Переключитесь на пользователя *postgres*:

```
su - postgres
```

9. Создайте пользователя и пароль пользователя *vms* для подключения к БД:

```
createuser -P -d -E ИМЯ_ПОЛЬЗОВАТЕЛЯ
```

На запрос ввода пароля введите нужный пароль для пользователя *ИМЯ\_ПОЛЬЗОВАТЕЛЯ*.



### Примечание

Для завершения настройки Postgres-сервера требуется вручную настроить синхронизацию с единым сервером времени. Рекомендуется использовать один и тот же сервер времени для Postgres, хостов **Базис.vControl** и **Базис.WorkPlace**.

Ниже приведены примеры команд для настройки синхронизации:

```
apt-get update  
apt-get install chrony
```

```
systemctl start chronyd.service
systemctl enable chronyd.service
systemctl status chronyd.service
```

Обычно конфигурационный файл по умолчанию либо `/etc/chrony/chrony.conf`, либо `/etc/chrony.conf`.

Далее можно оставить указанные в файле NTP-сервера:

```
pool pool.ntp.org iburst
```

Или добавить строку с известным NTP-сервером, например:

```
server 192.168.21.10 iburst
```

---

### 6.3.3 Установка Redis-кластера

Пример конфигурационного файла для установки кластера Redis содержится в файле ***redis-hosts-example*** архива ***vms-deploy-X.tgz***, распакованного вами на **Сервере развертывания**. Сделайте на его основе реальный конфигурационный файл установки ***redis-hosts***, скопировав или переименовав файл-пример ***redis-hosts-example***.

В файле ***redis-hosts*** описываются серверы, на которые будет установлен Redis-кластер и параметры SSH-подключения к ним для автоматической установки Redis через Ansible. Например:

```
[redis-sentinel]
redis-1 ansible_user=root ansible_host=123.123.123.123
ansible_ssh_pass='AnsiblePassword'
redis-2 ansible_user=root ansible_host=123.123.123.124
ansible_ssh_pass='AnsiblePassword'
redis-3 ansible_user=root ansible_host=123.213.123.125
ansible_ssh_pass='AnsiblePassword'
```

#### Описание параметров:

- ***redis-X*** — имя сервера.
- ***ansible\_user*** — имя пользователя целевого сервера, где будет развернут Redis, с правами root.
- ***ansible\_host*** — IP-адрес целевого сервера, где будет развернут Redis.

- **`ansible_private_key_file`** — локальный путь к файлу с секретным ключом для SSH-доступа к серверу, в случае авторизации по ключу.
- **`ansible_pass`** — пароль для SSH-доступа к серверу, в случае авторизации по паролю.

Для создания Redis-кластера необходимо минимум 3 сервера, при этом штатная работа **Базис.vControl** возможна при выходе из строя не более чем одного Redis-сервера. Если кластер Redis состоит из 5 серверов, то возможен выход из строя 2 серверов. Если кластер состоит из N серверов, то возможен выход из строя N/2 (округляя вниз) серверов. Для правильного функционирования кластера общее количество серверов должно быть нечетным.

Если Redis ставится на те же серверы, что и **Бэкенд Базис.vControl** (параметры **`redis_on_backend: true`** в конфигурационном файле **`vdi-config`**), то верно следующее:

- Redis-кластер будет располагаться на серверах **Бэкенда Базис.vControl**;
- файл **`redis-hosts`** не используется, установка идет на серверы, указанные в файле **`backends-hosts`**.

Шаги по развертыванию Redis-кластера:

1. При необходимости поправьте параметры в **`redis-hosts`**, как указано выше.
2. Установите кластер Redis, выполнив следующую команду:

```
./deploy.sh -r -a environment.tgz
```

---

### **Примечание**

Для Astra Linux установка выполняется от непривилегированного пользователя, которому доступно `sudo` без пароля. Если установка идет при прямом доступе в консоль (не через `ssh`), то во время логина пользователя **`integrity level`** должен быть выбран «63».

---

Произойдет установка Redis-кластера на все серверы, описанные в файле **`redis-hosts`**, в случае успеха будет выведено соответствующее сообщение (рисунок 6.34):

```
PLAY RECAP *****
redis-1      : ok=39   changed=18   unreachable=0   failed=0
redis-2      : ok=41   changed=29   unreachable=0   failed=0
redis-3      : ok=41   changed=29   unreachable=0   failed=0
Установлен redis с sentinel на ноды из redis-hosts.
[root@vms-deploy deploy]#
```

Рисунок 6.34 Сообщение при успешной установке Redis-кластера

В случае возникновения ошибок они будут выведены в консоль. Дополнительно их можно посмотреть в лог-файле установки `/opt/vdi-playbooks/logs/ansible.log`.

### 6.3.4 Установка ClickHouse-кластера

Пример конфигурационного файла для установки кластера ClickHouse содержится в файле **`clickhouse-hosts-example`** архива **`vms-deploy-X.tgz`**, распакованного вами на **Сервере развертывания**. Сделайте на его основе реальный конфигурационный файл установки **`clickhouse-hosts`**, скопировав или переименовав файл-пример **`clickhouse-hosts-example`**.

В файле **`clickhouse-hosts`** описываются серверы, на которые будет установлен ClickHouse-кластер и параметры SSH-подключения к ним для автоматической установки ClickHouse через Ansible. Например:

```
[clickhouse]
clickhouse-1 ansible_user=root ansible_host=123.123.123.123
ansible_ssh_pass='AnsiblePassword'
clickhouse-2 ansible_user=root ansible_host=123.123.123.124
ansible_ssh_pass='AnsiblePassword'
clickhouse-3 ansible_user=root ansible_host=123.123.123.125
ansible_ssh_pass='AnsiblePassword'
```

#### Описание параметров:

- **`clickhouse-X`** — имя сервера;
- **`ansible_user`** — имя пользователя целевого сервера, где будет развернут ClickHouse, с правами root;
- **`ansible_host`** — IP-адрес целевого сервера, где будет развернут ClickHouse;
- **`ansible_private_key_file`** — локальный путь к файлу с секретным ключом для SSH-доступа к серверу, в случае авторизации по ключу;
- **`ansible_pass`** — пароль для SSH-доступа к серверу, в случае авторизации по паролю.

Для создания ClickHouse-кластера необходимо минимум 3 сервера, при этом штатная работа **Базис.vControl** возможна при выходе из строя не более чем одного ClickHouse-сервера. Если кластер Redis состоит из 5 серверов, то возможен выход из строя 2 серверов. Если кластер состоит из N серверов, то возможен выход из строя  $N/2$  (округляя

## Базис.vControl. Руководство по установке

вниз) серверов. Для правильного функционирования кластера общее количество серверов должно быть нечетным.

Если ClickHouse ставится на те же хосты, что и **Бэкенд Базис.vControl** (параметр **clickhouse\_on\_backend: true** в конфигурационном файле **vdi\_config**), то:

- файл **clickhouse-hosts** игнорируется, установка идет на хостах из **backends-hosts**;
- виртуальный IP-адрес через keeralived устанавливается на хостах на те же интерфейсы, на которых находятся IP-адреса из параметра **ansible\_host** соответствующего хоста.

В описываемой здесь последовательности ClickHouse ставится именно на хосты **Бэкенда Базис.vControl**.

Шаги по развертыванию ClickHouse-кластера:

1. Выполните из-под учетной записи root на **Сервере развертывания** в той же папке, где был распакован архив **vms-deploy-X.tgz**, следующую команду:

```
./deploy.sh -c -a environment.tgz
```

### **Примечание**

Для Astra Linux установка выполняется от непривилегированного пользователя, которому доступно sudo без пароля. Если установка идет при прямом доступе в консоль (не через ssh), то во время логина пользователя **integrity level** должен быть выбран «63».

Произойдет установка ClickHouse-кластера на все желаемые серверы (описанные в файле **clickhouse-hosts** или на сервера **Бэкенда**). В случае успеха будет выведено соответствующее сообщение:

```
PLAY RECAP *****
backend-1           : ok=47   changed=21   unreachable=0   failed=0
backend-2           : ok=47   changed=21   unreachable=0   failed=0
backend-3           : ok=47   changed=21   unreachable=0   failed=0
Установлен clickhouse на ноды из clickhouse-hosts.
[root@ha-deploy deploy]#
[root@ha-deploy deploy]#
```

Рисунок 6.35 Сообщение при успешной установке ClickHouse-кластера

В случае возникновения ошибок они будут выведены на консоль. Дополнительно список можно посмотреть в лог-файле установки.

### 6.3.5 Установка Бэкенда и Фронтенда Базис.vControl

---



#### Осторожно

При установке **Бэкенда Базис.vControl** на Альт 9 должны быть подключены официальные репозитории для этой ОС из сети Интернет.

---

Пример конфигурационного файла для установки серверов Бэкенда содержится в файле **backend-hosts-example** архива **vms-deploy-X.tgz**, распакованного вами на **Сервере развертывания**. Сделайте на его основе реальный конфигурационный файл установки **backend-hosts**, скопировав или переименовав файл-пример **backends-hosts-example**.

В файле **backend-hosts** описываются серверы, на которые будут установлены экземпляры **Бэкенда** и параметры SSH-подключения к ним для автоматической установки **Бэкенда** через Ansible. Например:

```
[vms-backends]
backend-1 ansible_user=root ansible_host=123.123.123.123
ansible_ssh_pass='AnsiblePassword'
backend-2 ansible_user=root ansible_host=123.123.123.124
ansible_ssh_pass='AnsiblePassword'
backend-3 ansible_user=root ansible_host=123.123.123.125
ansible_ssh_pass='AnsiblePassword'
```

Описание параметров:

- **backend-X** — имя сервера;
- **ansible\_user** — имя пользователя целевого сервера, где будет развернут **Бэкенд**, с правами root;
- **ansible\_host** — IP-адрес целевого сервера, где будет развернут **Бэкенд**;
- **ansible\_private\_key\_file** — локальный путь к файлу с секретным ключом для SSH-доступа к серверу, в случае авторизации по ключу;
- **ansible\_pass** — пароль для SSH-доступа к серверу, в случае авторизации по паролю.

Виртуальный IP-адрес через keeralived устанавливается на хостах на те же интерфейсы, на которых находятся IP-адреса из параметра **ansible\_host** соответствующего хоста.

Шаги по развертыванию **Бэкендов**:

1. Выполните из-под учетной записи root на **Сервере развертывания** в той же папке, где был распакован архив **vms-deploy-X.tgz**, следующую команду:

```
./deploy.sh -b -a environment.tgz
```

### **Примечание**

Для Astra Linux установка выполняется от непривилегированного пользователя, которому доступно sudo без пароля. Если установка идет при прямом доступе в консоль (не через ssh), то во время логина пользователя **integrity level** должен быть выбран «63».

Произойдет установка **Базис.vControl**. При успешной установке будет выведено соответствующее сообщение с версиями установленных RPM-пакетов с компонентами, пример:

```
PLAY RECAP *****
backend-1      : ok=137  changed=49  unreachable=0  failed=0
backend-2      : ok=129  changed=49  unreachable=0  failed=0
backend-3      : ok=129  changed=49  unreachable=0  failed=0

Скала-Р Управление успешно установлен.
Версии установленных компонентоv:
vms-backend:
  version:0.18 build:3246 Пт 02 фев 2018 02:55:58
vms-frontend:
  version:0.18 build:529 Чт 01 фев 2018 20:56:57
vms-frontend-vdi:
  version:0.18 build:529 Чт 01 фев 2018 21:01:44
vms-agent:
  version:0.18 build:970 Пт 02 фев 2018 02:44:04
vms-playbooks:
  version:0.18 build:285 Пт 02 фев 2018 11:49:44
[root@ha-deploy deploy]# █
```

Рисунок 6.36 Сообщение при успешной установке Базис.vControl

В случае возникновения ошибок их список будет выведен на консоль. Дополнительно список можно посмотреть в лог-файле установки **/opt/vms-playbooks/logs/ansible.log**.

### 7. НАЧАЛО РАБОТЫ

Для доступа в систему по HTTPS укажите в адресной строке IP-адрес сервера, где установлена система **Базис.vControl**. В качестве имени пользователя и пароля используйте данные, указанные при установке решения.

Для первоначальной настройки рекомендуется:

- импортировать кластеры **ПК Р-Хранилище**, в случае их наличия;
- установить **Агент Базис.vControl** на хостах Р-виртуализации;
- подключить AD/OpenLDAP (см. раздел [Синхронизация с Active Directory](#));
- настроить доступ к хранилищам для использования шаблонов и ISO-образов;
- задать необходимую логическую структуру с помощью логических папок;
- создать необходимые пулы ресурсов для ограничения ресурсов;
- задать правила доступа к объектам системы.

#### 7.1 Вход в Базис.vControl

Для начала работы Администратор должен выполнить вход на странице **Базис.vControl** в браузере (рисунок 7.1). Для этого Администратор должен ввести логин и пароль и нажать кнопку **Войти**.

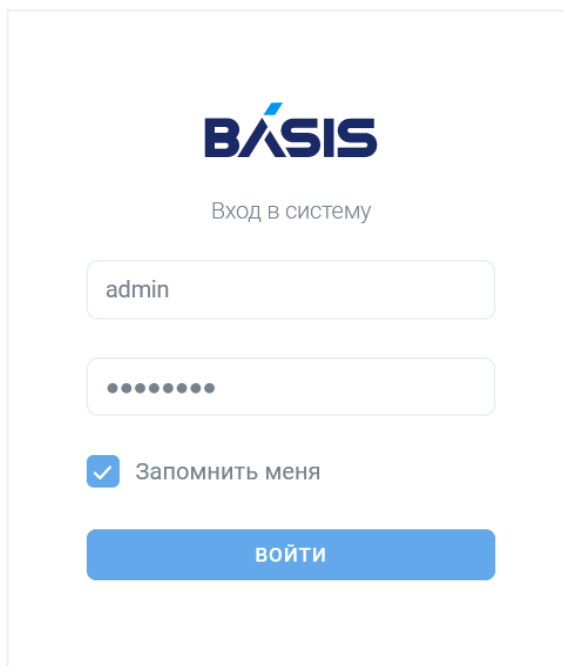


Рисунок 7.1 Вход в систему Базис.vControl

Поставьте галочку для опции «*Запомнить меня*», чтобы система запомнила авторизацию пользователя.





### Примечание

Время хранения таких данных настраивается отдельно и в текущей версии системы **Базис.vControl** составляет 24 часа.

---

После подключения к виртуальной среде рекомендуется указать действительный адрес электронной почты в разделе *Профиль* → *Настройки профиля*.

Администратор **Базис.vControl** может предоставлять другим пользователям права и привилегии определенного уровня (см. раздел интерфейса «*Управление и мониторинг*»). Администратор также может создавать аккаунты пользователей или использовать внешнюю LDAP-совместимую базу данных. Пользователи получают доступ в **Базис.vControl**, используя ту же ссылку, что и администратор виртуальной среды, указывая соответствующие имена пользователей и пароли. Набор действий, которые эти пользователи смогут выполнять в **Базис.vControl**, определяется предоставленными им правами доступа.

## 8. СИСТЕМА ХРАНЕНИЯ ДАННЫХ

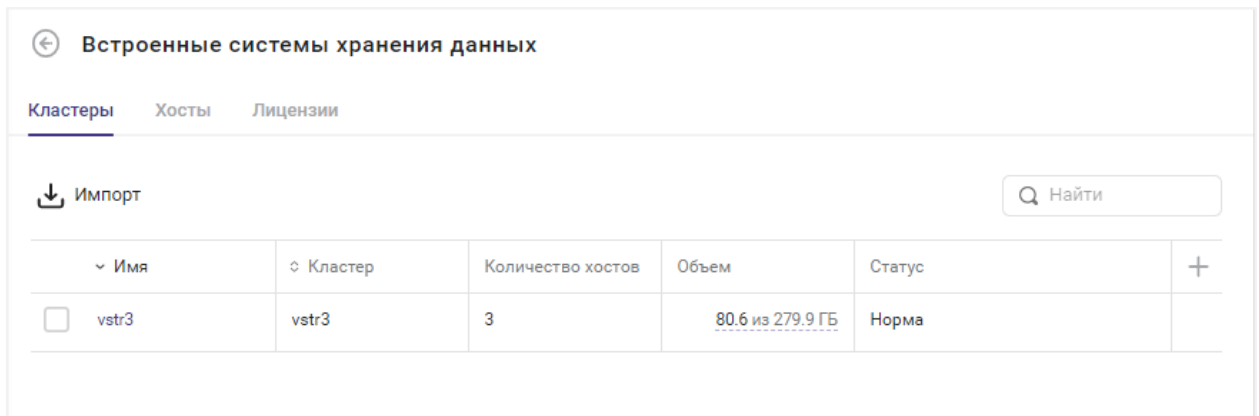
**Система хранения данных (СХД) в Базис.vControl** — это раздел для управления свойствами хранилища данных программного комплекса **ПК Р-Хранилище**. **ПК Р-Хранилище** объединяет дисковое пространство серверов в распределенное, отказоустойчивое и масштабируемое программно определяемое хранилище данных. Архитектура **ПК Р-Хранилище** рассчитана на потерю любого физического сервера или группы серверов целиком, а не только отдельного диска. В **Базис.vControl** кластеры **ПК Р-Хранилище** используются в качестве основы для HA-кластеров.

Раздел *Система хранения данных* включает следующие вкладки:

- **Кластеры** — вкладка для работы с кластерами **ПК Р-Хранилище**, добавленными в **Базис.vControl**.
- **Хосты** — вкладка для работы с хостами **ПК Р-Хранилище**.
- **Лицензии** — вкладка для управления лицензиями, примененными для кластеров **ПК Р-Хранилище**.

### 8.1 Импорт кластера ПК Р-Хранилище

Общее управление кластерами **ПК Р-Хранилище** выполняется в разделе *Встроенные системы хранения данных* на вкладке *Кластеры*.



Имя	Кластер	Количество хостов	Объем	Статус	
<input type="checkbox"/> vstr3	vstr3	3	80.6 из 279.9 ГБ	Норма	

Рисунок 8.1 Встроенные системы хранения данных, вкладка «Кластеры»

В таблице представлена информация о существующих кластерах:

- **Имя** — название кластера **ПК Р-Хранилище** в **Базис.vControl**. При нажатии на название откроется панель управления для выбранного кластера.
- **Имя кластера** — название кластера **ПК Р-Хранилище**.
- **Количество хостов** — количество физических хостов, входящих в состав кластера.
- **Общий объем** — общий объем кластера в гигабайтах.
- **Занятый объем** — занятый объем кластера в гигабайтах.
- **Статус** — статус текущего состояния кластера:

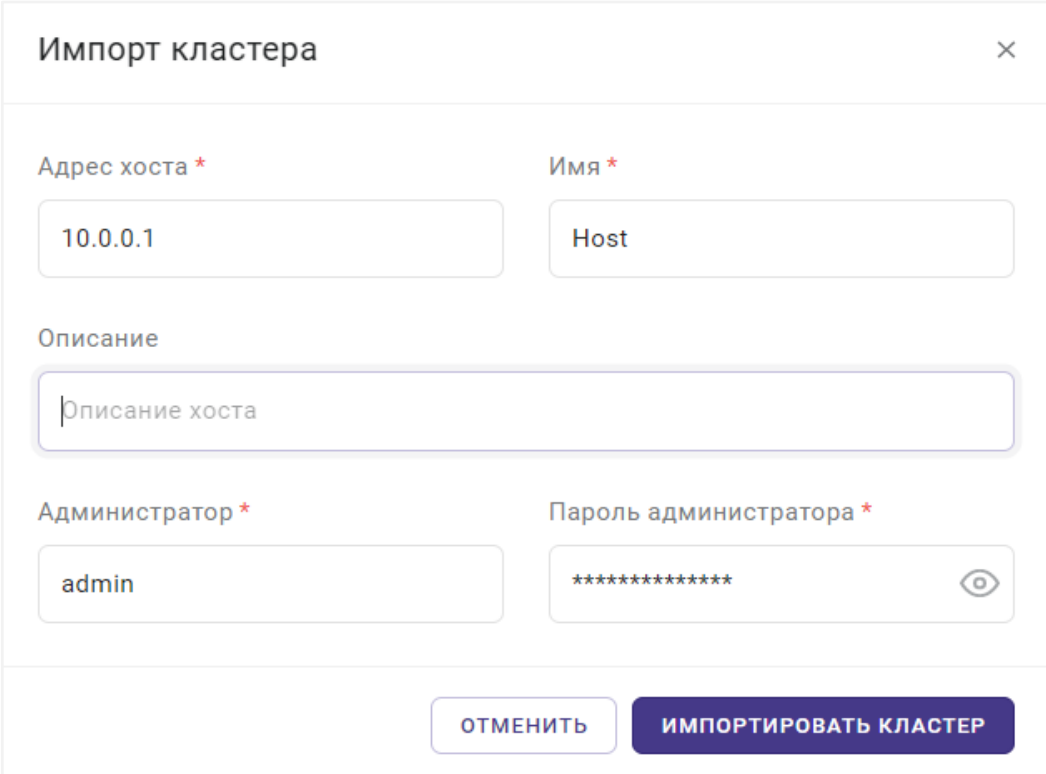
- **Норма** — все chunk-хосты в кластере являются активными;
- **Неизвестно** — недостаточно информации о состоянии кластера;
- **Деградация** — некоторые chunk-хосты в кластере находятся в неактивном состоянии;
- **Сбой** — в кластере находится слишком много неактивных chunk-хостов, автоматическая репликация выключена;
- **SMART Warning** — один и более физических дисков, подключенных к кластеру **ПК Р-Хранилище**, находятся в предотказном состоянии.

На панели инструментов располагаются дополнительные кнопки действий:

- **Импорт кластера** — добавление нового кластера в **Базис.vControl**.
- **Изменить имя** — изменение имени выбранного кластера.
- **Удалить** — удаление выбранного кластера(-ов).

Новый кластер **ПК Р-Хранилище** добавляется в **Базис.vControl** с помощью функции импорта. Для импорта кластера выполните следующие шаги:

1. В боковом меню перейдите в раздел *Система хранения данных*.
2. Откройте вкладку *Кластеры*.
3. Нажмите кнопку **Импорт кластера**.
4. Заполните форму «Импорт кластера» (рисунок 8.2).



The screenshot shows a web form titled "Импорт кластера" (Import Cluster) with a close button (X) in the top right corner. The form contains several input fields:

- Адрес хоста \*** (Host address \*): Input field containing "10.0.0.1".
- Имя \*** (Name \*): Input field containing "Host".
- Описание** (Description): A large text area with a placeholder "Описание хоста" (Host description).
- Администратор \*** (Administrator \*): Input field containing "admin".
- Пароль администратора \*** (Administrator password \*): Password input field containing "\*\*\*\*\*" and a visibility toggle icon (eye).


At the bottom of the form, there are two buttons: "ОТМЕНИТЬ" (Cancel) and "ИМПОРТИРОВАТЬ КЛАСТЕР" (Import Cluster).

Рисунок 8.2 Форма «Импорт кластера»

- **Адрес хоста** — IP-адрес любого хоста, на котором запущен кластер **ПК Р-Хранилище**.
- **Имя** — название хоста в кластере.
- **Описание** — краткое описание хоста.
- **Администратор** — учетная запись пользователя операционной системы хоста с правами администратора.
- **Пароль администратора** — пароль для администратора хоста.



### Примечание

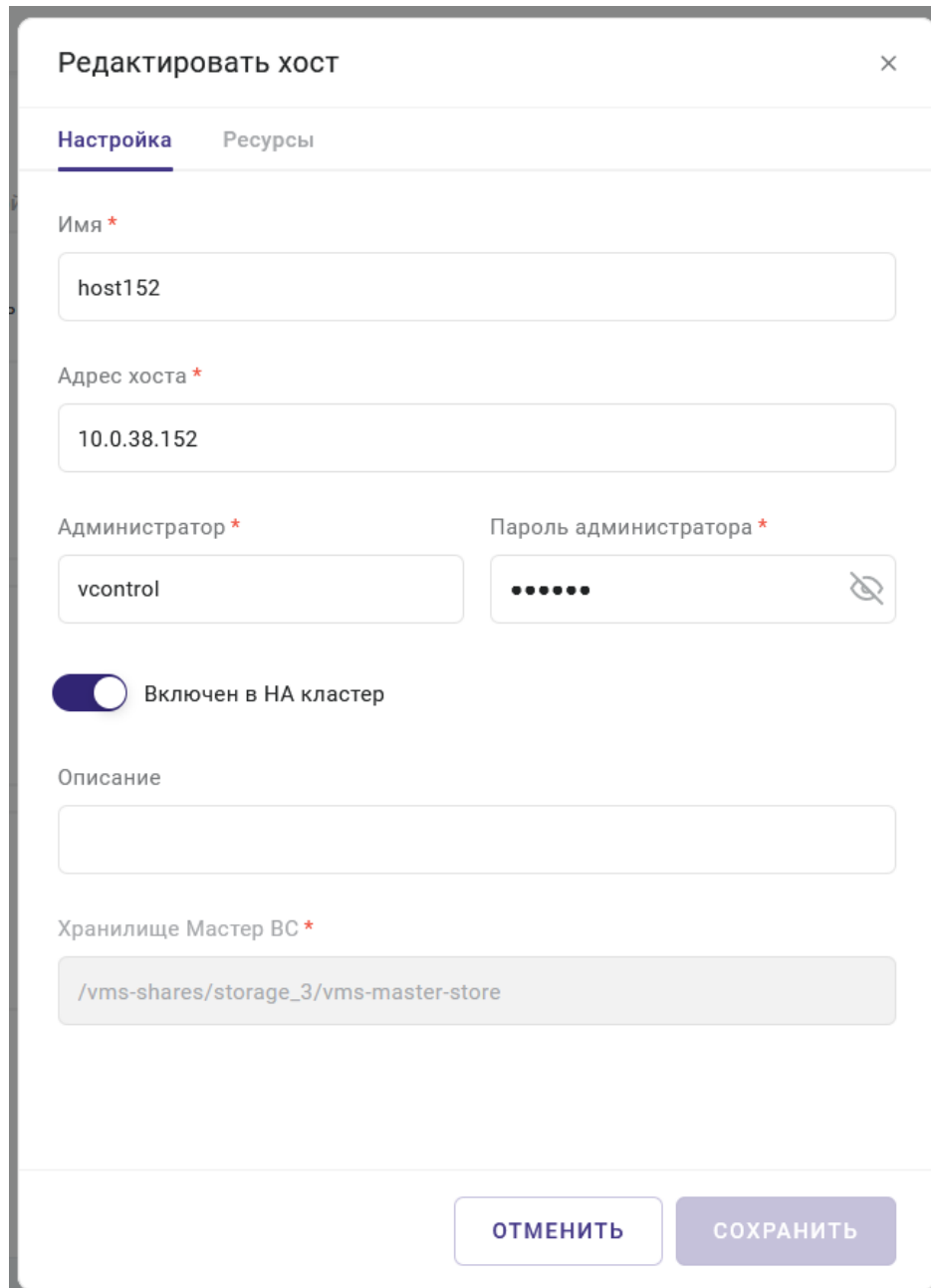
Чтобы увидеть символы вводимого пароля, нажмите на иконку  в поле ввода пароля.

---

#### 5. Нажмите кнопку **Импортировать кластер**.

В процессе импорта кластера **ПК Р-Хранилище** система собирает информацию обо всех хостах, составляющих кластер **ПК Р-Хранилище**, и создает объекты для всех хостов, на которых запущены MDS- и CS-сервисы данного кластера. Пустые хосты создаются с IP-адресами сетевых интерфейсов **ПК Р-Хранилище** в качестве имени.

После завершения импорта кластера необходимо зайти в каждый из добавленных хостов и включить НА, а также заполнить поля: имя, адрес, администратор, пароль администратора:



Редактировать хост

Настройка Ресурсы

Имя \*

host152

Адрес хоста \*

10.0.38.152

Администратор \*

vcontrol

Пароль администратора \*

Включен в HA кластер

Описание

Хранилище Мастер ВС \*

/vms-shares/storage\_3/vms-master-store

ОТМЕНИТЬ СОХРАНИТЬ

Рисунок 8.3 Форма редактирования настроек хоста, опция «Включен в HA кластер»

После этого на каждый из добавленных хостов нужно установить агент.



### Примечание

В случае ошибки импорта кластера (наиболее частые причины — неверное указание реквизитов для подключения по SSH) для данного хоста необходимо

изменить данные подключения: выберите хост в списке на вкладке *Хосты* и нажмите кнопку **Редактировать**. После успешного редактирования необходимо нажать кнопку **Обновить агент**. Также на странице *Хосты* можно удалить хост **ПК Р-Хранилище**, для которого не был импортирован кластер **ПК Р-Хранилище**

---



### Примечание

В случае ошибки установки агента на хосте кластера **Р-Хранилище** можно поменять данные для подключения к хосту: выберите хост в списке *Хосты* и нажмите кнопку **Редактировать**. После успешного редактирования необходимо нажать кнопку **Обновить агент**.

---

### 9. УПРАВЛЕНИЕ КЛАСТЕРАМИ

**Кластер в Базис.vControl** — это объединение хостов, которое можно рассматривать как отдельный объект в системе, обладающий дополнительными свойствами и возможностями работы:

- Кластер логически *объединяет ресурсы* всех подключенных хостов в единое пространство. Это позволяет выполнять задачи, для которых не хватает ресурсов в рамках работы одного хоста.
- Объединение хостов позволяет реализовать механизм *отказоустойчивости*, что обеспечивает корректную работу пользователей с виртуальными средами в случае сбоев в работе хостов.
- В кластере возможно использование функции перераспределения нагрузки на хостах за счет алгоритмов *автобалансировки*. В **Базис.vControl** автобалансировкой занимается планировщик ресурсов, который периодически анализирует загруженность хостов и перераспределяет используемые ресурсы для запуска и работы виртуальных сред с более загруженных хостов на менее загруженные хосты. Планировщик также запускается при обнаружении следующих событий:
  - **Старт виртуальной среды** — выполняется перерасчет ресурсов хоста и кластера, принятие решения о размещении и старта виртуальной среды.
  - **Остановка виртуальной среды** — выполняется перерасчет ресурсов хоста и кластера.
  - **Миграция виртуальной среды** — выполняется выбор и перерасчет ресурсов целевого хоста.
  - **Изменения параметров работающей виртуальной среды** — выполняется перерасчет ресурсов хоста и кластера, принятие решения об изменении ресурсов.
  - **Старт хоста** — выполняется перерасчет ресурсов кластера.
  - **Перевод хоста в режим обслуживания** — выполняется перерасчет ресурсов кластера и перемещение виртуальных сред на остальные узлы кластера.
  - **Изменение параметров работающего хоста** — выполняется перерасчет ресурсов кластера.
  - **Изменение лицензии хоста** — выполняется перерасчет ресурсов хоста и кластера.

В **Базис.vControl** любой хост должен быть в составе кластера. Администратор может создать кластеры следующих типов:

- **HA-кластер** (high availability, высокодоступный) — кластер с механизмом отказоустойчивости. В HA-кластер могут входить только хосты на базе кластера **ПК Р-Хранилище**.
- **Обычный кластер** — логическая группа хостов, подключенных к любому виду хранилища. В таком кластере нет возможности использовать механизм отказоустойчивости.

В созданных кластерах администратор может выполнять следующие действия:

- регулировать объем доступных ресурсов в кластере путем изменения его конфигурации;
- отслеживать суммарные значения потребления ресурсов и состояние запущенных в кластере виртуальных сред.

### 9.1 Создание кластера в Базис.vControl

---



#### Совет

При создании HA-кластера потребуется указать кластер **ПК Р-Хранилище**. Если в системе нет кластеров **ПК Р-Хранилище**, то их нужно создать. Процедура создания такого кластера описана в разделе [Система хранения данных](#).

---



#### Примечание

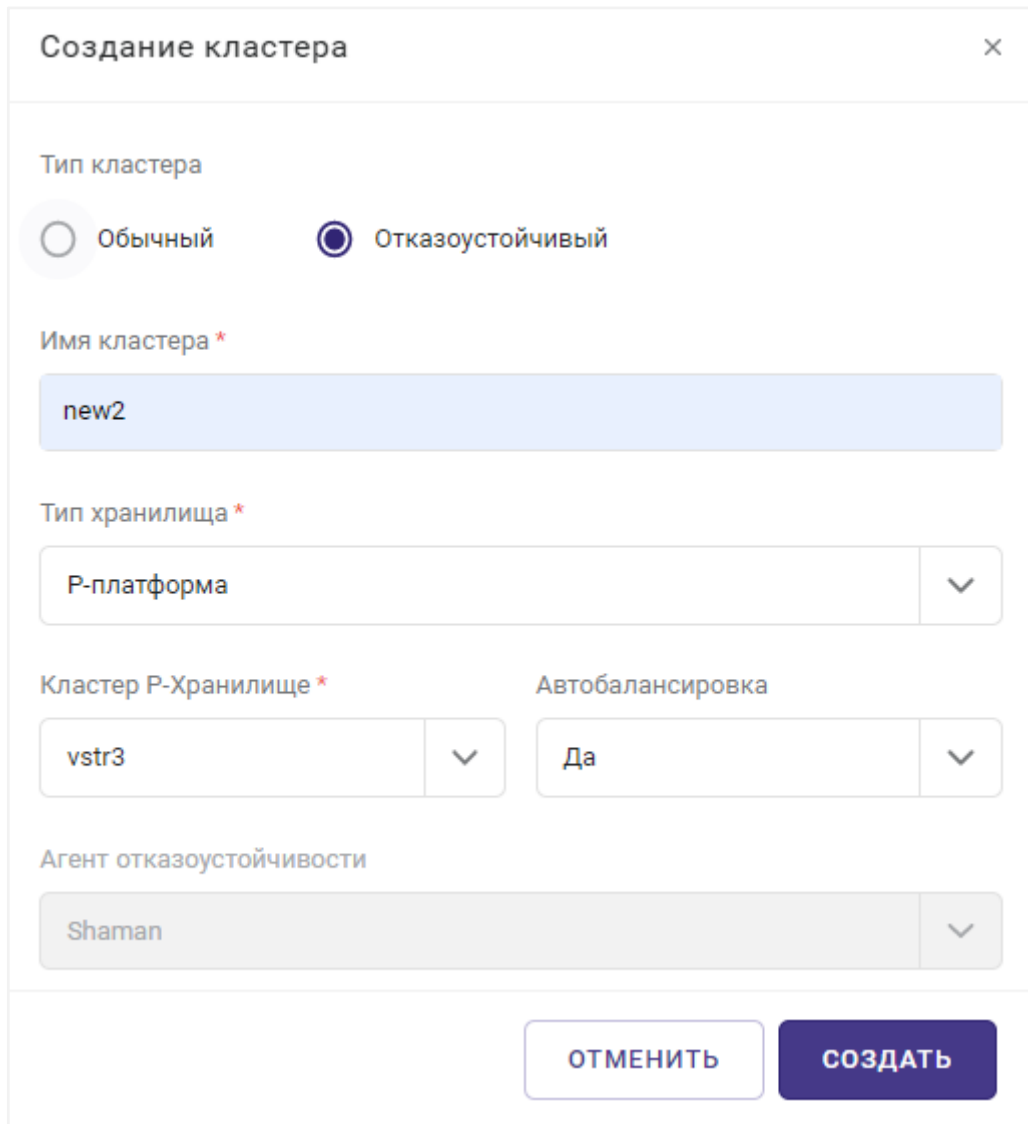
**Примечание.** Кластер любого типа изначально создается пустым, без хостов.

---

Для создания нового кластера выполните следующие шаги:

1. В боковом меню перейдите в раздел *Инфраструктура*.
2. В рабочей области откройте вкладку *Кластеры*.
3. Нажмите кнопку **Создать кластер**.
4. В форме создания нового кластера (рисунок 9.1) выберите тип кластера: «Обычный» или «Отказоустойчивый».
5. Заполните параметры нового кластера. Все поля, отмеченные звездочкой (\*), обязательны для заполнения.





Создание кластера

Тип кластера

Обычный  Отказоустойчивый

Имя кластера \*

new2

Тип хранилища \*

P-платформа

Кластер Р-Хранилище \*

vstr3

Автобалансировка

Да

Агент отказоустойчивости

Shaman

ОТМЕНИТЬ СОЗДАТЬ

Рисунок 9.1 Форма создания кластера

- **Имя кластера** — название кластера;
- **Кластер Р-Хранилище** (*только для HA-кластера*) — кластер **ПК Р-Хранилище**, на базе которого будет работать новый HA-кластер (тут нужно указать кластер **ПК Р-Хранилище**, созданный на предыдущем шаге);
- **Автобалансировка** — автоматическая балансировка нагрузки на хостах кластера.

6. Нажмите кнопку **Создать**.

После создания кластера в форме редактирования его параметров будут доступны дополнительные настройки (рисунок 9.2). Все параметры сгруппированы по следующим

вкладкам: *Настройка*, *Дополнительные настройки*, *Высокая доступность* и *Балансировка*.

### Редактировать кластер ×

**Настройки**   СХД

Имя \*

Хосты  
 × ▼

Настройки ресурсов хостов

Резерв памяти	Overcommit памяти
<input type="text" value="4096"/> МБ	<input type="text" value="9"/>
Резерв CPU	Overcommit CPU
<input type="text" value="6"/> %	<input type="text" value="9"/>

Высокая доступность

Тип хранилища	Хранилище	Агент отказоустойчивости
<input type="text" value="P-хранилище"/> ▼	<input type="text" value="rvstorage"/>	<input type="text" value="Shaman"/> ▼

Балансировка

Режим балансировки кластера \*  
 ▼

Рисунок 9.2 Переход к форме для редактирования настроек кластера

На вкладке *Настройка* для редактирования вынесены общие параметры кластера и настройки ресурсов хостов. Все поля, отмеченные звездочкой (\*), являются обязательными для заполнения.

- **Имя** — название кластера.
- **Хосты** (только для HA-кластера) — список хостов в кластере.
- **Резерв памяти** — объем зарезервированной памяти для каждого хоста в кластере в МБ.
- **Overcommit памяти** — коэффициент для вычисления предельно допустимого объема используемой памяти хоста. Если объем фактически используемой памяти превысит величину физической незарезервированной памяти хоста в Overcommit раз, то система Базис.vControl считает, что у хоста закончились ресурсы памяти.
- **Резерв CPU** — процент зарезервированных ресурсов ЦП для каждого хоста в кластере.
- **Overcommit CPU** — коэффициент для вычисления предельно допустимого количества используемых процессоров хоста. Если количество фактически используемых процессоров превысит количество всех незарезервированных процессоров хоста в Overcommit раз, то система Базис.vControl считает, что у хоста закончились ресурсы центрального процессора.



### Примечание

В настройках отображаются данные о максимальных значениях Overcommit среди всех хостов кластера. Если максимальные значения Overcommit на хостах отличаются, то в настройках кластера будет показано сообщение о наличии этой разницы.

---

На вкладке *Дополнительные настройки* для редактирования вынесены параметры, используемые при настройке Мастер ВС для связанных клонов. Все поля, отмеченные звездочкой (\*), являются обязательными для заполнения.

- **Хранилище Мастер ВС** — путь, где будет располагаться Мастер ВС. Значением по умолчанию является `/vstorage/<cluster-name>/vms-master-stor`.
- **Кэш образов и шаблонов** — путь, где будут располагаться шаблоны и образы, загруженные с общего хранилища. Значением по умолчанию является `/vstorage/<cluster-name>/vms-image-cache`.



### Примечание

Подробнее о работе со связанными клонами описано в документе **Базис.vControl. Руководство администратора**.

---

На вкладке *Высокая доступность* для редактирования вынесены параметры, предназначенные для настройки HA-кластеров.

- **Кластер Р-Хранилище** — кластер ПК Р-Хранилище, на базе которого функционирует HA-кластер. Пустое поле означает, что кластер не использует общее хранилище.

На вкладке *Балансировка* для редактирования вынесены параметры, предназначенные для настройки балансировки нагрузки на хостах кластера.

- **Режим балансировки кластера** — выбор режима балансировки нагрузки на хостах кластера.
- **Выключено** — автобалансировка отключена.
- **Частично автоматически** — планировщик ресурсов рассчитывает наиболее оптимальное расположение для вновь создаваемых или запускаемых виртуальных сред, для уже запущенных виртуальных сред будут рассчитаны оптимальные пути миграции как в режиме «Вручную».
- **Автоматически** — выбор путей и последующая миграция виртуальных сред выполняется в автоматическом режиме с учетом правил связанности. Выбор оптимального расположения выполняется для вновь создаваемых или запускаемых виртуальных сред, также осуществляется миграция уже запущенных виртуальных сред.
- **Вручную** — планировщик ресурсов рассчитывает оптимальные пути миграции запущенных виртуальных сред с учетом правил связанности и выводит список предлагаемых путей миграции на вкладке *Балансировка*. Запуск миграции виртуальных сред по предложенным путям выполняется только в ручном режиме.

## 10. УПРАВЛЕНИЕ ХОСТАМИ

### 10.1 Добавление/удаление хоста в кластере обычного типа

**Хост** (хост виртуализации) в **Базис.vControl** — это физический сервер, на котором установлено программное обеспечение **Р-Виртуализация**. Основной функцией хоста является предоставление физических ресурсов (дисковое пространство, RAM, CPU) для развёртывания и работы виртуальных сред.

Общее управление хостами выполняется в разделе *Инфраструктура* на вкладке *Хосты*.

<input type="checkbox"/> Хост	Имя кластера	Кластер Р-Хранилище	IP-адрес	ОС хоста	Архитектура	CPU	Диск	Память
<input type="checkbox"/> node6-1	cl-fenix2		10.0.38.151	Linux	x64	3%	42%	13%
<input type="checkbox"/> node6-2	cl-fenix2		10.0.38.152	Linux	x64	2%	42%	7%
<input type="checkbox"/> node6-4	cl-fenix2		10.0.38.154	Linux	x64	0%	42%	6%

Рисунок 10.1 Инфраструктура, вкладка «Хосты»



#### Совет

В **Базис.vControl** не поддерживается работа одиночных хостов; любой хост должен быть в составе кластера. Если в системе не заведены кластеры, то их нужно создать. Процедура создания нового кластера описана в разделе [Создание кластера в Базис.vControl](#).

Для добавления хоста в кластер выполните следующие шаги.

- Откройте панель управления кластером, в который следует добавить новый хост, используя один из следующих способов:
  - В боковом меню перейдите в раздел *Инфраструктура* → <Название кластера>.
  - Выполните переход *Инфраструктура* → вкладка *Кластеры* и в открывшемся списке нажмите на название нужного кластера.

2. Нажмите кнопку **Добавить хост** на панели инструментов.
3. Выберите тип нового хоста:
  - **Отдельный хост** — добавление хоста, не использующего ПК Р-Хранилище.
  - **Хост кластера Р-Хранилище** — добавление хоста из списка хостов, входящих в состав кластеров ПК Р-Хранилище.
4. Заполните параметры нового хоста в открывшейся форме. Форма зависит от выбранного ранее типа хоста и описана ниже.
5. Нажмите кнопку **Сохранить** или **Отменить**, чтобы добавить хост в кластер или отменить его создание.

Если был выбран тип «Отдельный хост», то для добавления хоста откроется специальная форма (рисунок 10.2), которую нужно заполнить. Все поля, отмеченные звездочкой (\*), обязательны для заполнения.

### Добавление хоста ✕

**Кластер \*** **Адрес хоста \***

cl-fenix2 ▼ 10.0.0.1

**Имя хоста \***

new2

**Описание хоста**

Краткое описание хоста

**Администратор \*** **Пароль администратора \***

admin \*\*\*\*\* 👁

**Права доступа**

**Пользователь** **Роль**

admin ▼ Администратор И... ▼ 🗑

+ ДОБАВИТЬ

ОТМЕНИТЬ СОЗДАТЬ

Рисунок 10.2 Форма добавления отдельного хоста

- **Кластер** — кластер, в состав которого будет входить новый хост.
- **Адрес хоста** — IP-адрес хоста.
- **Имя** — название хоста.
- **Описание** — краткое описание хоста.

- **Администратор** — учетная запись пользователя операционной системы хоста с правами администратора.
- **Пароль администратора** — пароль для учетной записи администратора.
- **Права доступа** — пользователь или группа пользователей **Базис.vControl**, которые будут использовать данный хост, и их роль.



### Совет

В блоке «Права доступа» в левом выпадающем списке выбирается пользователь или группа пользователей, в правом выпадающем списке — роль для указанного пользователя или группы. При необходимости можно добавить в раздел «Права доступа» несколько пар вида «пользователь + роль», нажав на иконку плюса напротив последней записи.

---

При добавлении в кластер хоста типа «хост кластера **Р-Хранилище**» откроется форма выбора существующих в системе хостов кластера **ПК Р-Хранилище** (рисунок 10.3). Выберите хост из выпадающего списка и нажмите кнопку **Добавить**.



## Редактировать кластер ✕

**Настройки** СХД

Имя \*

Хосты  
 ✕ ▼

hwnode01	<input checked="" type="checkbox"/>
hwnode02	<input checked="" type="checkbox"/>

**ЗАКРЫТЬ**

6 % 9

**Высокая доступность**

Тип хранилища	Хранилище	Агент отказоустойчивости
<input type="text" value="P-хранилище"/> <span>▼</span>	<input type="text" value="rvstorage"/>	<input type="text" value="Shaman"/> <span>▼</span>

**Балансировка**

Режим балансировки кластера \*  
 ▼

Рисунок 10.3 Форма добавления хоста кластера ПК P-Хранилище

## 11. СИНХРОНИЗАЦИЯ С ACTIVE DIRECTORY

Администратор может автоматизировать процесс добавления пользователей в **Базис.vControl** с помощью подключения внешней базы данных. Такая база должна удовлетворять следующим условиям:

- к базе должен быть сетевой доступ от **Бэкенда/ов Базис.vControl**;
- база использует протокол LDAP для доступа к каталогам (поддерживаются Active Directory, SambaDC, OpenLDAP, FreeIPA).

Регистрация и последующая настройка такой базы в **Базис.vControl** выполняется на вкладке *Синхронизация с LDAP* в разделе *Управление и Мониторинг* → *Управление Пользователями* (рисунок 11.1).

The screenshot shows the 'LDAP Synchronization' configuration page. At the top, there is a breadcrumb trail: 'Управление пользователями > Синхронизация с LDAP'. Below this is a navigation menu with tabs: 'Пользователи', 'Группы', 'Роли', 'Правила доступа', 'Синхронизация с LDAP' (which is active), 'Заблокированные логины', and 'Заблокированные IP адреса'. The main content area is titled 'Настройки подключения' and contains several input fields: 'Тип' (set to 'Active Directory'), 'Хост' section with 'Сервер\*' (10.10.10.10) and 'Порт\*' (Введите порт), a '+ ДОБАВИТЬ' button, 'Base DN\*' (Введите основной LDAP Distinguis), 'User DN\*' (admin), 'Пароль учетной записи LDAP\*' (masked with dots), and 'Атрибут выборки пользователя'. A 'СОХРАНИТЬ' button is at the bottom right.

Рисунок 11.1 Вкладка «Синхронизация с LDAP»

Для регистрации базы пользователей в **Базис.vControl** заполните поля на вкладке *Синхронизация с LDAP*. Все поля, отмеченные звездочкой (\*), обязательны для заполнения.

- **Тип** — тип внешней базы пользователей: Active Directory или OpenLDAP.

---

### **Примечание**

Службы внешних каталогов Active Directory и SambaDC настраиваются при выборе типа «Active Directory», а OpenLDAP и FreeIPA при выборе типа «OpenLDAP».

---

- **Хост** — IP-адрес и номер порта для доступа к серверу базы по протоколу LDAP. Чтобы добавить дополнительный сервер, нажмите справа кнопку **+**, чтобы удалить — кнопку **-**.
- **Base DN** (Base Distinguished Name) — объект каталога, начиная с которого производится поиск в базе.
- **User DN** (User Distinguished Name) — уникальное имя учетной записи в базе, через которую будет происходить синхронизация со **Базис.vControl**.
- **Пароль** — пароль от учетной записи, указанной в поле «User DN».
- **Поле для выборки** — поле, по которому будет производиться поиск в базе.

Пример заполнения полей:

```
Хост: <IP address> порт: 389
Base DN: dc=example,dc=loc
User DN: cn=ldaproot,dc=example,dc=loc
Пароль: \*****\*
Поле для выборки: uid
```

После внесения изменений в форму их следует сохранить нажатием на кнопку **Сохранить**.

---

### **Примечание**

Если соединение с удаленной базой пользователей невозможно, то появится соответствующее сообщение об ошибке.

---

## 12. ШАБЛОНЫ И ОБРАЗЫ

В качестве хранилища шаблонов и образов в **Базис.vControl** используются сетевые папки, доступные по протоколу CIFS или NFS на внешнем файловом сервере. Папки, предназначенные для использования в качестве хранилища, должны быть подготовлены заранее и доступны по сети для **Бэкенда Базис.vControl** и хостов виртуализации. На серверах должна быть подготовлена учетная запись для сетевого доступа к этим папкам.

Для настройки доступа **Бэкенда Базис.vControl** к сетевым папкам, которые будут использоваться в качестве хранилища шаблонов и образов, в веб-интерфейсе **Базис.vControl** нужно зайти в раздел *Шаблоны и Образы* → *Настройка хранилища* и далее заполнить все необходимые поля в разделах *Шаблоны* и *Образы*. Подробнее действия по настройке описаны в разделах [Настройки хранилища шаблонов](#) и [Настройки хранилища образов дисков](#).

**Базис.vControl** не использует в работе формат шаблонов, предоставляемый **Р-Платформой**, т.е. созданные ранее шаблоны **Р-Платформы** невозможно использовать без конвертирования в формат **Базис.vControl**.

Для конвертирования шаблона ВС, созданного в **ПК Р-Платформа**, необходимо создать из шаблона ВС. Далее эту ВС клонировать в шаблон **Базис.vControl**, выбрав опцию *Клонировать в шаблон* в списке ВС или в панели управления ВС. Шаблон **Базис.vControl** состоит из описания конфигурации ВС и образов дисков ВС.

Для создания нового шаблона необходимо создать новую, эталонную ВС, на которую нужно установить все необходимое ПО и драйверы для дальнейшей работы ВС. Для создания шаблона перейдите в раздел *Пулы ресурсов* → *Виртуальные среды*, выделите

строку с ВС, после нажмите кнопку **...** и выберите действие «Клонировать в шаблон» (рисунок 12.1).

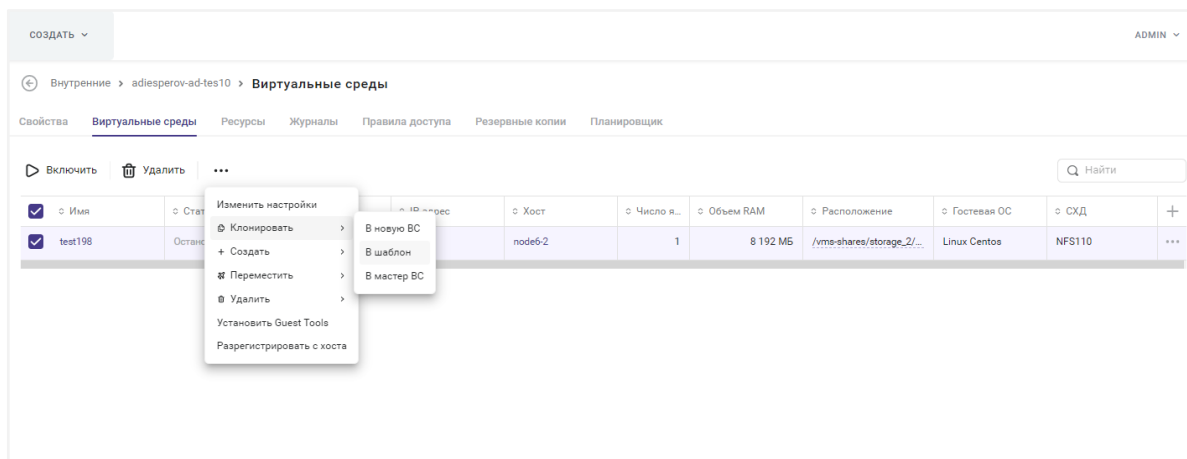


Рисунок 12.1 Расположение действия «Клонировать в шаблон»

Для просмотра списка шаблонов виртуальных сред и ISO образов дисков, которые доступны в **Базис.vControl**, перейдите в раздел бокового меню *Шаблоны и образы* (рисунок 12.2).

<input type="checkbox"/>	Имя	Статус	Описание	CPU	Ядер	RAM	Видеопамять	Гостевая ОС	Виртуализация	Создано	+
<input type="checkbox"/>	Basis-Alt9.2-agent-1...	Готово	Рабочий шаблон	1000	2	8192 МБ	64 МБ	Linux Other	Виртуальная Машина	04.05.23 в 15	
<input type="checkbox"/>	AV-iso-test-not-enabl...	Готово	CD не включен, бе...	1000	2	8192 МБ	64 МБ	Windows 10	Виртуальная Машина	04.05.23 в 15	
<input type="checkbox"/>	avm-astra171-fresh	Готово	Astra 1.7.1 OreI, us...	1000	4	12288 МБ	64 МБ	Linux Other	Виртуальная Машина	04.05.23 в 15	
<input type="checkbox"/>	adies-redos	Готово	Jakarta	1000	2	8192 МБ	64 МБ	Linux Other	Виртуальная Машина	04.05.23 в 15	
<input type="checkbox"/>	kv-Win-agent-1982r-l...	Готово	local users: grieg, ...	1000	2	12288 МБ	64 МБ	Windows 10	Виртуальная Машина	04.05.23 в 15	
<input type="checkbox"/>	AV-iso-test-enable-b...	Готово	Включен, без дис...	1000	2	8192 МБ	64 МБ	Windows 10	Виртуальная Машина	04.05.23 в 15	
<input type="checkbox"/>	yi_astra1.7+agent 1...	Готово		1000	4	11520 МБ	64 МБ	Linux Other	Виртуальная Машина	04.05.23 в 15	
<input type="checkbox"/>	0-Win10x64-templat...	Готово	user:basis_ready fo...	1000	2	12288 МБ	64 МБ	Windows 10	Виртуальная Машина	04.05.23 в 15	
<input type="checkbox"/>	avm-win10-agent-ad...	Готово		1000	4	12288 МБ	64 МБ	Windows 10	Виртуальная Машина	04.05.23 в 15	
<input type="checkbox"/>	FreeRadius	Готово	шаблон ради сохр...	1000	2	8192 МБ	64 МБ	Linux Centos	Виртуальная Машина	04.05.23 в 15	
<input type="checkbox"/>	yi-astra17-agent198...	Готово		1000	2	8192 МБ	64 МБ	Linux Other	Виртуальная Машина	04.05.23 в 15	

Рисунок 12.2 Шаблоны и образы, вкладка «Шаблоны»

Шаблоны виртуальных сред и образы дисков располагаются в разных хранилищах, поэтому настраиваются отдельно в соответствующем разделе. Информация о библиотеках представлена на двух вкладках: *Шаблоны* и *Образы*.

## Примечание

**Базис.vControl** имеет возможность управления кластерами, развернутыми на нескольких разных площадках. Тем не менее, все кластеры системы делят между собой единое хранилище образов и шаблонов. Из-за этого возрастает нагрузка на маршрутизатор, так как файлы, размещенные в сети одного кластера, будут распространяться по сетям остальных.

Без учета этих ограничений, для управления несколькими площадками требуется лишь объединить сети маршрутизатором. Для увеличения производительности можно воспользоваться сторонними средствами для организации хранения данных в обеих сетях (DFS, NFS).

### 12.1 Настройки хранилища шаблонов

Шаблоны виртуальных сред располагаются в специальном хранилище. Параметры этого хранилища могут быть настроены с помощью формы, открываемой по нажатию на кнопку **Настройки хранилища** в панели инструментов вкладки *Шаблоны* (рисунок 12.2). Параметры хранилища представлены на двух вкладках: *Настройка* (рисунок 12.3) и *Хосты* (рисунок 12.4).

На вкладке *Настройка* для редактирования вынесены общие параметры хранилища шаблонов. Все поля, отмеченные звездочкой (\*), являются обязательными для заполнения.

### Настройки хранилища ×

**Настройка** Хосты

Протокол

CIFS ▼

Имя сетевой папки \*  Сервер \*  Логин \*

Домен пользователя  Пароль \*  🔒

Версия протокола cifs  ▼ Режим безопасности  ▼

Рисунок 12.3 Форма настройки параметров хранилища шаблонов, вкладка Настройка


- **Статус** — не редактируемое поле, отражает текущее состояние доступности хранилища шаблонов.
- **Сервер** — IP-адрес сервера хранилища шаблонов.
- **Имя сетевой папки** — название сетевой папки, в которой располагается хранилище шаблонов. Есть возможность указать конкретную папку внутри сетевой папки (например, «V1\Templates», где «Templates» — каталог внутри сетевой папки).

### Примечание

В процессе подключения сетевой папки на всех хостах, работающих под управлением **Базис.vControl**, происходит монтирование указанной в настройках сетевой папки в локальный путь **/vms-shares/hdd**. Система осуществляет периодические проверки доступности сетевой папки на всех хостах, в случае ошибок создается сообщение в журнале событий.

- **Протокол** — название сетевого протокола для удаленного доступа к сетевым ресурсам. В зависимости от выбранного протокола в форме появляются дополнительные поля для заполнения:
  - **CIFS:**
    - **Логин** — логин пользователя, который система будет использовать для подключения к сетевой папке.
    - **Домен пользователя** — домен пользователя, в случае если это требуется для аутентификации. Поле может оставаться пустым.
    - **Пароль** — пароль пользователя, который система использует для подключения к сетевой папке.

### Совет

Чтобы увидеть символы вводимого пароля, нажмите иконку  в поле ввода пароля.

- **Версия протокола cifs** — версия протокола SMB (Server Message Block, сетевой протокол прикладного уровня для удаленного доступа к сетевым ресурсам). В выпадающем списке выберите нужную версию протокола или оставьте значение «Не задано».
- **Режим безопасности** — режим определяет способ шифрования паролей, которыми обмениваются сервер и клиент (даже если пароли не нужны). В выпадающем списке доступны режимы:
  - ▽ **Не задано** — режим безопасности выключен;
  - ▽ **none** — попытка подключения в качестве нулевого пользователя, то есть без логина/имени;
  - ▽ **ntlm** — использование хэширования пароля на основе протокола NTLM (NT LAN Manager, протокол сетевой аутентификации).
- **NFSv3:**



- **Только чтение** — сетевой ресурс будет доступен только в режиме чтения.
- **NFSv4:**
  - **Только чтение** — сетевой ресурс будет доступен только в режиме чтения.

---

### **Примечание**

При использовании сетевых ресурсов NFS в режиме «Только чтение» будет недоступна функция клонирования ВС в шаблон.

---

- **Kerberos** — при выборе опции включается аутентификация посредством сетевого протокола Kerberos, а в форме появятся дополнительные поля для заполнения:
  - ▽ **Логин** — логин пользователя, который система будет использовать для подключения к сетевой папке.
  - ▽ **Домен пользователя** — домен пользователя, в случае если это требуется для аутентификации. Поле может оставаться пустым.
  - ▽ **Пароль** — пароль пользователя, который система использует для подключения к сетевой папке.
- **RC4 DES** — при выборе опции в шифровании используется arcfour-hmac des-cbc-crc des-cbc-md5.

На вкладке также располагаются дополнительные кнопки действий:

- **Синхронизировать** — запуск процесса синхронизации хранилища и метаданных о нем в **Базис.vControl**.

---

### **Совет**

Используйте кнопку **Синхронизировать** для обновления списка шаблонов на вкладке *Шаблоны* при их ручном переносе в хранилище.

---

- **Сохранить** — сохранение параметров хранилища после внесения изменений.

### **Примечание**

Для сохранения внесенных изменений не требуется повторное указание пароля. Исключением является сохранение нового пароля пользователя.

- **Отключить** — отключение хранилища шаблонов от **Базис.vControl**. После отключения все текущие шаблоны перестанут быть доступны для использования в **Базис.vControl**.

На вкладке *Хосты* администратор может посмотреть список хостов, использующих хранилище шаблонов, а также их текущие статусы.

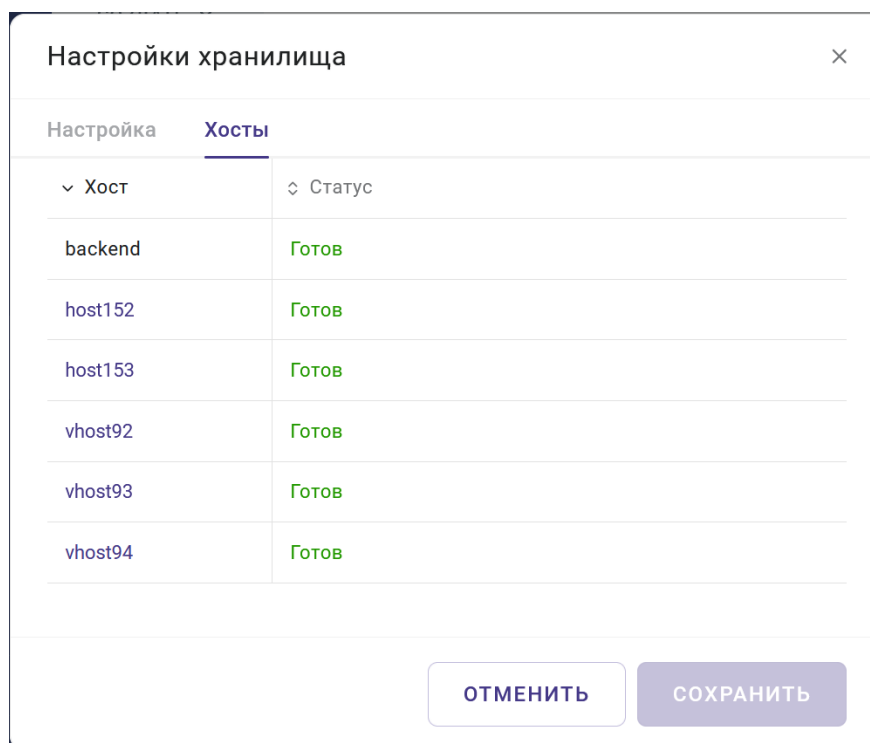


Рисунок 12.4 Форма настройки параметров хранилища шаблонов, вкладка *Хосты*

- **Хост** — имя хоста, использующего хранилище шаблонов. При нажатии на имя хоста откроется панель управления хостом.
- **Статус** — статус состояния доступности хранилища на хосте, может иметь следующие значения:
  - **Ошибка** — хранилище шаблонов не настроено;
  - **Готов** — хранилище шаблонов настроено и готово для работы.

### 12.2 Настройки хранилища образов дисков

**Базис.vControl** позволяет использовать для подключения в виртуальные среды образы дисков (ISO-файлы), расположенные во внешней библиотеке, доступной по протоколу CIFS или NFS. При отсутствии подготовленного хранилища необходимо создать сетевое хранилище и разместить в нем необходимые образы дисков.

Для быстрой работы с образами, размещенными в хранилище образов дисков, **Базис.vControl** добавляет используемые образы в кэш на распределенной системе хранения данных (пути могут быть изменены в конфигурации агента):

- `/vstorage/<Имя кластера ПК Р-Хранилище>/vms-image-cache/` — если хост является частью кластера **ПК Р-Хранилище**;
- `/var/cache/vms_local_cache` — если хост не является частью кластера **ПК Р-Хранилище**.

В соответствии с настройками агентов кэш может автоматически очищаться. В случае если размер образов в кэше достигает указанного в конфигурации размера, система удаляет наиболее старые неиспользуемые образы в соответствии с настройками.

В случае если ISO-образ из библиотеки подключается к ВС, **Базис.vControl** сначала добавляет образ в кэш; если образ еще отсутствует в библиотеке, далее монтирует файл из кэша в CD-ROM ВС.

Поиск образов происходит рекурсивно, т.е. в систему добавляются образы из всех подпапок на сетевой папке. Образы ISO, впервые синхронизированные в **Базис.vControl**, добавляются недоступными для монтирования к ВС. Для изменения доступности необходимо воспользоваться функцией изменения доступности в списке образов дисков.

Образы дисков располагаются в специальном хранилище. Параметры этого хранилища могут быть настроены с помощью формы, открываемой по нажатию на кнопку **Настройки хранилища** в панели инструментов вкладки **Образы**. Параметры хранилища представлены на двух вкладках: *Настройка* и *Хосты*.

На вкладке *Настройка* для редактирования вынесены общие параметры хранилища образов. Все поля, отмеченные звездочкой (\*), являются обязательными для заполнения.

Настройки хранилища

Настройка Хосты

СИНХРОНИЗИРОВАТЬ ОТКЛЮЧИТЬ

Протокол

CIFS

Имя сетевой папки \* Сервер \* Логин \*

/mnt/sata900/iso 10.0.38.102 admin

Домен пользователя Пароль \*

Версия протокола cifs Режим безопасности

Не задано Не задано

ОТМЕНИТЬ СОХРАНИТЬ

Рисунок 12.5 Форма настройки параметров хранилища образов дисков, вкладка «Настройка»

- **Статус** — нередатируемое поле, отражает текущее состояние доступности хранилища образов дисков.
- **Сервер** — IP-адрес сервера хранилища образов дисков.
- **Имя сетевой папки** — название сетевой папки, в которой располагается хранилище образов дисков. Есть возможность указать конкретную папку внутри сетевой папки (например, «V1\Templates», где «Templates» — каталог внутри сетевой папки).




### Примечание

В процессе подключения сетевой папки на всех хостах, работающих под управлением **Базис.vControl**, происходит монтирование указанной в настройках сетевой папки в локальный путь `/vms-shares/iso`. Система периодически проверяет доступность сетевой папки на всех хостах, в случае ошибок создается сообщение в журнале событий.

- **Протокол** — название сетевого протокола для удаленного доступа к сетевым ресурсам. В зависимости от выбранного протокола в форме появляются дополнительные поля для заполнения:
  - **CIFS:**
    - **Логин** — логин пользователя, который система будет использовать для подключения к сетевой папке.
    - **Домен пользователя** — домен пользователя, в случае если это требуется для аутентификации. Поле может оставаться пустым.
    - **Пароль** — пароль пользователя, который система использует для подключения к сетевой папке.



### Совет

Чтобы увидеть символы вводимого пароля, нажмите иконку  в поле ввода пароля.

- **Версия протокола cifs** — версия протокола SMB (Server Message Block, сетевой протокол прикладного уровня для удаленного доступа к сетевым ресурсам). В выпадающем списке выберите нужную версию протокола или оставьте значение «Не задано».
- **Режим безопасности** — режим определяет способ шифрования паролей, которыми обмениваются сервер и клиент (даже если пароли не нужны). В выпадающем списке доступны режимы:
  - ▽ **Не задано** — режим безопасности выключен;
  - ▽ **none** — попытка подключения в качестве нулевого пользователя, то есть без логина/имени;
  - ▽ **ntlm** — использование хэширования пароля на основе протокола NTLM (NT LAN Manager, протокол сетевой аутентификации).
- **NFSv3:**

- **Только чтение** — сетевой ресурс будет доступен только в режиме чтения.
  - **NFSv4:**
    - **Только чтение** — сетевой ресурс будет доступен только в режиме чтения.
- 



### Примечание

При использовании сетевых ресурсов NFS в режиме «Только чтение» будет недоступна загрузка ISO-образа через интерфейс **Базис.vControl**.

---

- **Kerberos** — при выборе опции включается аутентификация посредством сетевого протокола Kerberos, а в форме появятся дополнительные поля для заполнения:
  - ▽ **Логин** — логин пользователя, который система будет использовать для подключения к сетевой папке.
  - ▽ **Домен пользователя** — домен пользователя, в случае если это требуется для аутентификации. Поле может оставаться пустым.
  - ▽ **Пароль** — пароль пользователя, который система использует для подключения к сетевой папке.
- **RC4 DES** — при выборе опции в шифровании используется arcfour-hmac des-cbc-crc des-cbc-md5.

На вкладке также располагаются дополнительные кнопки действий:

- **Синхронизировать** — запуск процесса синхронизации хранилища и метаданных о нем в **Базис.vControl**.
- 



### Совет

Используйте кнопку **Синхронизировать** для обновления списка образов дисков на вкладке *Образы*.

---

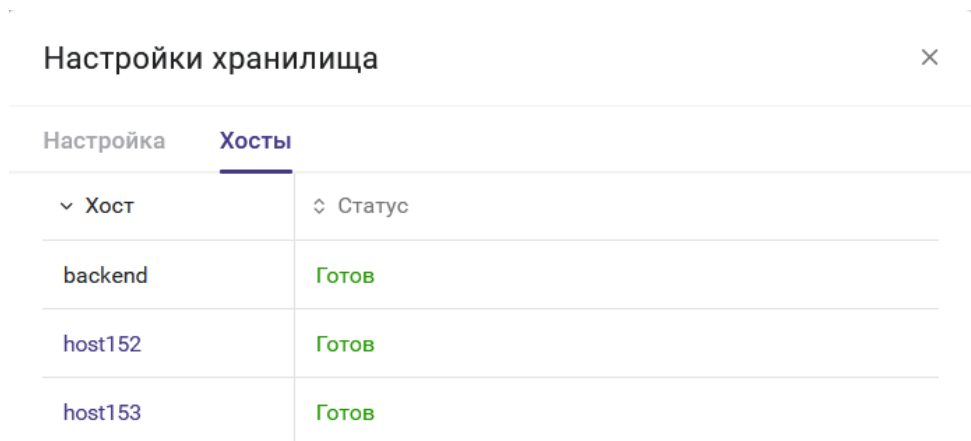
- **Сохранить** — сохранение параметров хранилища после внесения изменений.

## Примечание

Для сохранения внесенных изменений не требуется повторное указание пароля. Исключением является сохранение нового пароля пользователя.

- **Отключить** — отключение хранилища образов дисков от **Базис.vControl**. После отключения все текущие образы дисков перестанут быть доступны для использования в **Базис.vControl**.

На вкладке *Хосты* администратор может посмотреть список хостов, использующих хранилище образов дисков, а также их текущие статусы.



Настройки хранилища	
Настройка	Хосты
▼ Хост	↕ Статус
backend	Готов
host152	Готов
host153	Готов

Рисунок 12.6 Форма настройки параметров хранилища образов дисков, вкладка «Хосты»

- **Хост** — имя хоста, использующего хранилище образов дисков. При нажатии на имя хоста откроется панель управления хостом.
- **Статус** — статус состояния доступности хранилища на хосте, может иметь следующие значения:
  - **Ошибка** — хранилище образов дисков не настроено;
  - **Готов** — хранилище образов дисков настроено и готово для работы.

### 13. СМЕНА TLS-СЕРТИФИКАТА ДЛЯ ДОСТУПА К ВЕБ-ИНТЕРФЕЙСУ

#### 13.1 Конфигурация без отказоустойчивости (не-HA режим)

При первой установке **Базис.vControl** генерирует самоподписанный TLS-сертификат. Для установки другого сертификата нужно разместить сертификат и ключ в любой папке в системе, где было установлено решение **Базис.vControl**, и выполнить в консоли следующую команду:

```
/opt/vms-playbooks/bin/deploy-cert.sh -s /tmp/certs -k /tmp/key
```

Параметры:

- **-s** — путь к файлу с сертификатом;
- **-k** — путь к файлу с секретным (приватным) ключом, соответствующим сертификату.

Оба файла должны быть в pem-формате. Сертификат **Базис.vControl**, CA-сертификат или вся цепочка сертификации могут находиться в одном файле, переданном в параметре **-s**.

Если необходимо обновить/заменить сертификат, достаточно выполнить процедуру, описанную выше. При обновлении решения **Базис.vControl** через архив **vms-deploy-X.tgz** будет сохранен и использоваться уже установленный сертификат.

#### 13.2 Конфигурация с отказоустойчивостью (HA-режим)

Все действия аналогичны выполняемым для конфигурации без отказоустойчивости, за исключением того, что все действия должны выполняться на **Сервере развертывания**.



# 14. СМЕНА IP-АДРЕСА СЕРВЕРА БАЗИС.VCONTROL

## 14.1 В конфигурации без отказоустойчивости (не-НА режим)

Для смены IP-адреса сервера **Базис.vControl** выполните следующее:

1. Измените IP-адрес сетевого интерфейса операционной системы, в которой установлен бэкенд **Базис.vControl**. Если будет использоваться совершенно новый адрес, он должен соответствовать всем требованиям, описанным в разделе [Требования к сетевому взаимодействию](#).
2. Убедитесь, что у всех серверов, где установлены агенты, есть L3-связность с новым IP-адресом сервера **Базис.vControl**.
3. В веб-интерфейсе **Базис.vControl** зайдите в раздел *Инфраструктура* → *Хосты*, выделите всех агентов и нажмите кнопку **Обновить агент**.

При обновлении система не должна использоваться: не должно быть активности в веб-интерфейсе или на хостах **Базис.vControl**, также не должно быть активных задач в системе.

## 14.2 В конфигурации с отказоустойчивостью (НА-режим)

Чтобы изменить виртуальный IP-адрес или адреса конкретного хоста, нужно выполнить следующие действия:

1. Измените IP-адрес сетевого интерфейса операционной системы хоста. Если будет использоваться совершенно новый адрес, он должен соответствовать всем требованиям, описанным в разделе [Требования к сетевому взаимодействию](#).
2. Пропишите новый адрес в конфигурационном файле **backends-hosts** на **Сервере развертывания**.
3. Переустановите все **Бэкенды** (см. раздел [Обновление Бэкенда Базис.vControl](#)).
4. Если на хосте **Бэкенда** также располагались кластеры ClickHouse или Redis, то переустановите их (см. разделы [Установка Redis в отказоустойчивой конфигурации](#) и [Установка ClickHouse в отказоустойчивой конфигурации](#)).
5. Если был изменен виртуальный IP-адрес, то нужно выполнить следующие действия:
  - 1) Пропишите виртуальный IP-адрес в **vms-config** на **Сервере развертывания**.
  - 2) Переустановите хосты **Бэкенда**.
  - 3) Убедитесь, что у всех серверов, где установлены агенты, есть L3-связность с новым IP-адресом сервера **Базис.vControl**.
  - 4) В веб-интерфейсе **Базис.vControl** зайдите в раздел *Инфраструктура* → *Хосты*, выделите всех агентов и нажмите кнопку **Обновить агент**.
6. Если был изменен виртуальный IP-адрес, используемый БД Метрик Clickhouse:
  - 1) Пропишите виртуальный IP-адрес в **vms-config** на **Сервере развертывания Базис.vControl**.



### Примечание

Подробное описание конфигурационных параметров для **vms-config** приведено в разделе [Основные параметры конфигурации Базис.vControl](#).

---

- 2) Переустановите хосты ClickHouse.
- 3) Переустановите хосты **Бэкенда Базис.vControl**.
- 4) Убедитесь, что у всех серверов, где установлены **Бэкенды Базис.vControl/Базис.WorkPlace**, есть L3-связность с новым виртуальным IP-адресом ClickHouse.
- 5) Пропишите виртуальный IP-адрес в **vdi-config** на **Сервере развертывания Базис.WorkPlace**.
- 6) Переустановите хосты **Бэкенда Базис.WorkPlace**.

При обновлении система не должна использоваться: не должно быть активности в веб-интерфейсе или на хостах **Базис.vControl**, также не должно быть активных задач в системе.

## 15. ОБНОВЛЕНИЕ БАЗИС.VCONTROL

### 15.1 Подготовка репозитория для обновления компонентов Базис.vControl

Необходимо получить от производителя дистрибутив **vms-deploy-X.tgz** с новой версией Базис.vControl.



#### Совет

Перед обновлением рекомендуется переименовать папку «deploy» от предыдущего обновления для сохранения находящихся в ней конфигурационных файлов.

---

### 15.2 Обновление Бэкенда Базис.vControl

#### 15.2.1 В конфигурации с отказоустойчивостью (HA-режим)

---



#### Примечание

Перед обновлением сделайте сравнение текущих конфигурационных файлов и примеров. При обнаружении новых параметров добавьте их в текущий конфигурационный файл.

При обновлении значение параметра **vdi\_enable** в конфигурационном файле **vms-config** можно оставить без изменений, нет необходимости обязательно выставлять значение **false**.

---

Обновление происходит посредством установки новой версии из **vms-deploy-X.tgz** (см. раздел Установка в конфигурации с отказоустойчивостью (HA-режим)). Перед обновлением необходимо сохранить все конфигурационные файлы: **vms-config**, **backends-hosts**, **redis-hosts**, **clickhouse-hosts**.

Обновление следует проводить в следующем порядке:

1. Обновление **Сервера развертывания**.
2. Обновление кластеров Redis и ClickHouse. Обновление выполняется при наличии отдельных указаний при передаче релиза, в противном случае кластеры можно оставить без изменений.
3. Обновление **Бэкенда**.

### 4. Обновление **Агентов** из веб-интерфейса **Базис.vControl**.

#### **Примечание**

Накопленные метрики будут утеряны при обновлении системы Базис.vControl до версии 2.0 в связи с повышением версии ClickHouse. Рекомендуется заранее подготовить отчеты о ресурсах кластера перед обновлением.

При обновлении система не должна использоваться: не должно быть активности в веб-интерфейсе или на хостах **Базис.vControl**, также не должно быть активных задач в системе.

#### **Примечание**

При выставлении параметра **external\_virtualization** в значение true и обновлении существующей системы с ранее установленным инсталлятором Базис.vControl ClickHouse, будут удалены все данные, связанные с ClickHouse. Описание параметра приведено в разделе [Установка Сервера развертывания](#).

### 15.2.2 В конфигурации без отказоустойчивости (не-HA-режим)

#### **Примечание**

Перед обновлением сделайте сравнение текущих конфигурационных файлов и примеров. При обнаружении новых параметров добавьте их в текущий конфигурационный файл.

При обновлении значение параметра **vdi\_enable** в конфигурационном файле **vms-config** можно оставить без изменений, нет необходимости обязательно выставлять значение **false**.

Описание конфигурационных параметров для **vms-config** приведено в разделе [Установка в конфигурации без отказоустойчивости \(не-HA режим\)](#).

Обновление происходит аналогично установке и в той же последовательности, но с использованием новой версии из **vms-deploy-X.tgz** (см. раздел [Установка в конфигурации без отказоустойчивости \(не-HA режим\)](#)). Перед обновлением необходимо сохранить все конфигурационные файлы: **vms-config**, **backends-hosts**, **redis-hosts**, **clickhouse-hosts**.

При обновлении система не должна использоваться: не должно быть активности в веб-интерфейсе или на хостах **Базис.vControl**, также не должно быть активных задач в системе.

### 15.3 Обновление агентов Базис.vControl

Чтобы обновить агентское приложение, выполните в интерфейсе **Базис.vControl** следующие действия:

- зайдите в список хостов кластера, который необходимо обновить;
- выберите хосты, которые необходимо обновить, и нажмите кнопку **Обновить агент**.

После того как задача будет выполнена, на выбранных хостах будет установлена последняя версия агента. При обновлении система не должна использоваться: не должно быть активности в веб-интерфейсе или на хостах **Базис.vControl**, также не должно быть активных задач в системе, кроме задач обновления Агента.

#### 15.3.1 Возможные проблемы при обновлении агентов

Если при обновлении **Агентов Базис.vControl** возникает ошибка вида:

```
Deploy ext storage for <Node 'hpe-amd-node02', ip: 172.29.224.54,
node_id=2> returned non-zero return-code 2.
Error at host 'hpe-amd-node02' (id=2): line replacedtask mount-storage
: VmConfigCacheEnabled should be disabled in /etc/vz/dispatcher.xml
```

то для ее решения выполните следующие шаги:

1. Подключитесь к хосту виртуализации по SSH.
2. Откройте для редактирования файл `/etc/vz/dispatcher.xml` и измените значение параметра `<VmConfigCacheEnabled>1</VmConfigCacheEnabled>` на `<VmConfigCacheEnabled>0</VmConfigCacheEnabled>`.
3. Сохраните файл.
4. Выполните команду:

```
systemctl restart prl-disp
```

## 16. ПРИЛОЖЕНИЕ

### 16.1 Технические учетные записи

#### 16.1.1 Учетная запись в Базис.vControl, под которой Базис.WorkPlace будет подключаться к API Базис.vControl

Для создания учетной записи для **Базис.WorkPlace**, которая будет использоваться при подключении к API **Базис.vControl**, выполните следующие шаги:

1. В боковом меню перейдите в раздел *Управление и мониторинг* → *Управление пользователями*.
2. Откройте вкладку *Пользователи*.
3. Нажмите кнопку **Создать пользователя**.
4. Заполните форму «Создание пользователя» (рисунок 16.1), указав значения в обязательных полях. Остальные поля можно оставить по умолчанию.

- **Логин** — vdi.
- **Пароль** — желаемый пароль.

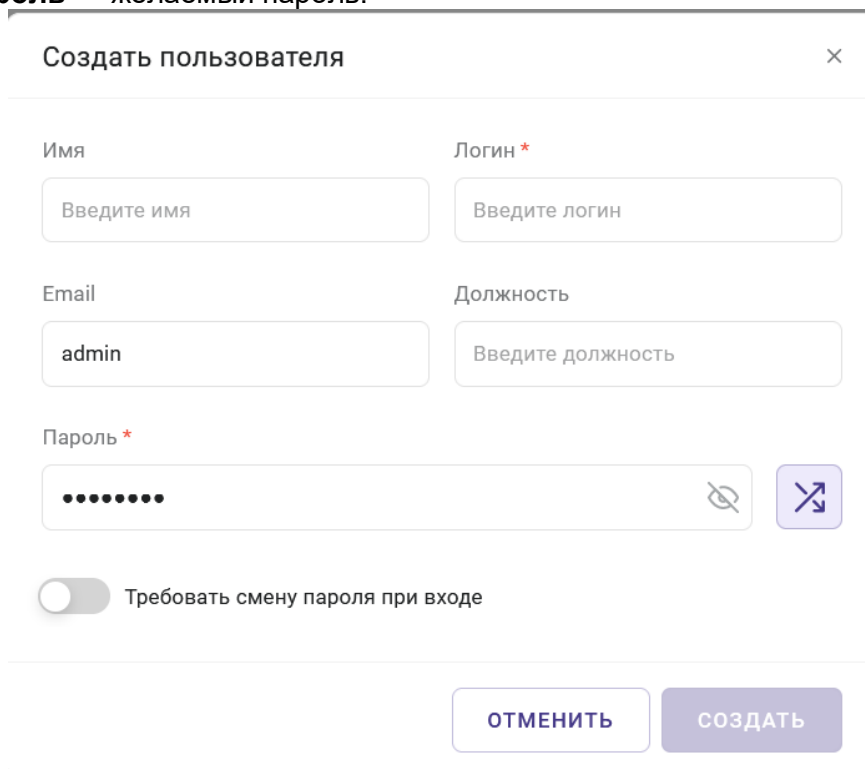


Рисунок 16.1 Форма «Создание пользователя»



### Осторожно

Если в качестве логина используется что-то отличное от **vdi** (например, **service-vdi**), то нужно указать в **Базис.vControl**, что пароль на эту учетную запись не должен истекать. Для этого добавьте дополнительные параметры в файл **backend-overrides**, расположенный в папке **deploy** на сервере развертывания:

```
user:
  password:
    expiration_disabled_for:
      - service-vdi
  disable_audit_for:
    - service-vdi
```

Все отступы в параметрах должны быть сохранены. После выполните переразвертывание **Бэкендов Базис.vControl**.

---

5. Нажмите кнопку **Создать**.
6. Откройте вкладку *Правила доступа*.
7. Нажмите кнопку **Назначить роль**.
8. Заполните форму «Назначить роли пользователя» (рисунок 16.2), указав следующие значения:
  - **Пользователи и группы** — vdi.
  - **Доступные роли** — Главный администратор.

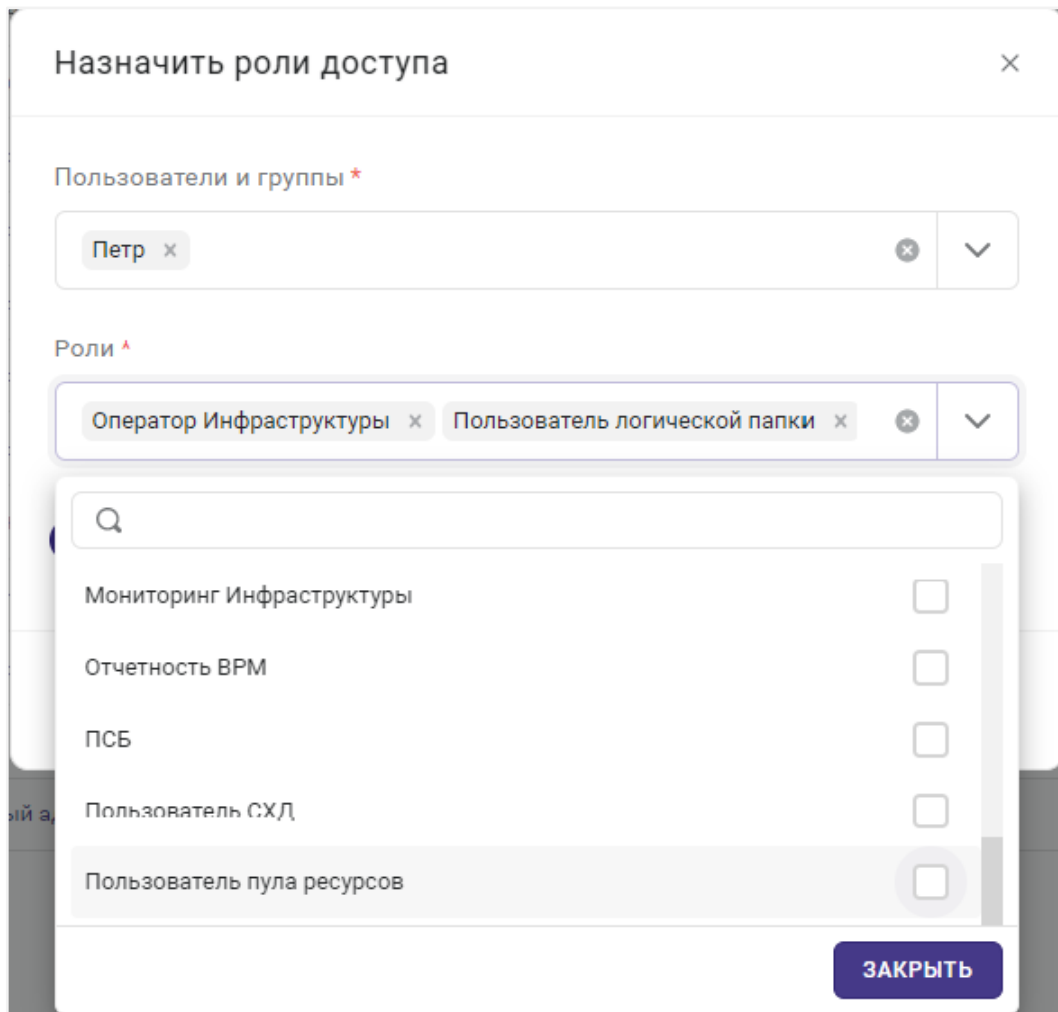


Рисунок 16.2 Форма «Назначить роли доступа»

9. Нажмите кнопку **Назначить**.

Созданный таким образом пользователь и его пароль должны быть указаны соответственно в параметрах `vms_user` и `vms_password` при установке **Базис.WorkPlace**.

## 16.2 Поддержка зашифрованных параметров в конфигурации Базис.vControl

**Базис.vControl** поддерживает шифрование данных подключения и паролей, которые хранятся в базе данных и хостах с компонентами **Базис.vControl** (в том числе хостах виртуализации). К этим данным относятся:

- пароли для подключения к серверам Redis;



- пароли для подключения к базе данных;
- пароли сущностей в базе данных:
  - node,
  - file\_share,
  - email\_settings,
  - ldap\_settings.

Шифрование данных настраивается при установке компонентов системы и выполняется с помощью механизмов Ansible Vault. На этапе подготовки системы к установке параметры в конфигурационных файлах не зашифрованы, поэтому для обеспечения безопасности доступ к секретным данным необходимо ограничить организационно-техническими мерами:

- Установку **Сервера развертывания** и **Бэкенда Базис.vControl** производить из-под отдельной учетной записи с необходимыми правами администратора.
- Конфигурационные параметры для установки и обновления системы рекомендуется хранить отдельно на внешнем носителе и/или на зашифрованном разделе/контейнере.

Для настройки шифрования потребуется создать файл с парольной фразой и потом указать к нему путь через параметр `-v` при запуске скрипта установки **deploy.sh**. С данной парольной фразой через `ansible-vault` шифруются все конфигурационные файлы продукта, содержащие пароли. Установка компонентов системы подробно описана в разделах [Установка Бэкенда и Фронтенда Базис.vControl](#) (не-НА режим) и [Установка Сервера развертывания](#) (НА режим). В приложении Справочник по параметрам конфигурации системы представлен пример конфигурационного файла для **Бэкенда Базис.vControl**, который получается после применения шифрования.



### Примечание

Параметры, изменяемые в конфигурационных файлах через файл переопределений **backend-overrides**, указываются без шифрования.

---

### 16.2.1 Смена парольной фразы

---



#### Осторожно

Парольную фразу можно менять только в рамках одной и той же версии системы **Базис.vControl**. Запрещается совмещать смену парольной фразы с обновлением системы.

---

Для смены парольной фразы требуется повторное переразвертывание компонентов системы с указанием пути к файлу с новой парольной фразой в обязательном параметре **-v**: С данной парольной фразой через `ansible-vault` шифруются все конфигурационные файлы продукта, содержащие пароли.

- Для переразвертывания **Бэкендов Базис.vControl** в не-НА режиме следует выполнить команду:

```
./deploy.sh -s -a environment.tgz -v /path/to/vault-password-file
```

---

### Осторожно

Установка **Бэкенда Базис.vControl** будет выполнена успешно только при развертывании системы через SSH. При этом подключение к хосту должно происходить только от пользователя `root`, подключение непривилегированным пользователем и переключение на `root` через `sudo/su` приведет к ошибке развертывания.

- 
- Для переразвертывания в НА режиме следует сначала обновить парольную фразу на **Сервере развертывания**, а потом обновить **Бэкенды Базис.vControl**:

```
./deploy.sh -i -a environment.tgz -v /path/to/vault-password-file  
./deploy.sh -b -a environment.tgz
```

---

### Примечание

Для Astra Linux переразвертывание выполняется от непривилегированного пользователя, которому доступно `sudo` без пароля. Если переразвертывание идет при прямом доступе в консоль (не через `ssh`), то во время логина пользователя ***integrity level*** должен быть выбран «63».

---

## 16.3 Использование Syslog

### 16.3.1 Пример настройки встроенного Syslog-сервера на ОС Альт

В качестве внешнего сервера для приема логов по протоколу Syslog можно использовать ОС Альт.

Для активации Syslog-сервера выполните следующие действия:

1. Отредактируйте файл `/etc/sysconfig/syslogd`, добавив в опции старта службы ключ `-r`, например:

```
# cat /etc/sysconfig/syslogd
# Options to syslogd
# -m 0 Disables 'MARK' messages.
# -r Enables logging from remote machines.
# -x Disables DNS lookups on messages received with -r.
#
# See syslogd(8) for more details.
SYSLOGD_OPTIONS='-u syslogd -j /var/resolv -r'
```

2. Перезапустите `syslogd`:

```
systemctl restart syslogd
```

### 16.3.2 Пример настройки встроенного Syslog-сервера на Astra Linux

В качестве внешнего сервера для приема логов по протоколу Syslog можно использовать Astra Linux.

Для активации Syslog-сервера выполните следующие действия:

1. Добавьте файл `/etc/rsyslog.d/30-remote.conf` с содержимым:

```
module(load="imudp")
input(type="imudp" port="514")

module(load="imtcp")
input(type="imtcp" port="514")
```

2. Перезапустите `rsyslog`

```
systemctl restart rsyslog
```

### 16.3.3 Настройка передачи событий в Syslog

Система позволяет включить передачу данных во внешний Syslog-сервер.

Для включения отправки на внешний Syslog-сервер событий, отображаемых в разделах *Управление и мониторинг* → *Журналы и Управление и мониторинг* → *События аудита*, выполните следующие шаги:

1. В боковом меню перейдите в раздел *Управление и мониторинг* → *Настройки системы*.
2. Найдите секцию *Отправка нотификаций*.
3. Укажите в параметрах значения хоста и порта syslog-сервера:
  - **agent\_manager.periodic.send\_events\_notifications.syslog\_settings.host** — хост syslog-сервера для событий.
  - **agent\_manager.periodic.send\_events\_notifications.syslog\_settings.port** — порт syslog-сервера для событий.
4. Нажмите кнопку **Сохранить** в левом верхнем углу для сохранения внесенных изменений.

Период запуска задачи отправки уведомлений о событиях определяется параметром **agent\_manager.periodic.send\_events\_notifications.period** и по умолчанию равен 5 минутам.

Дополнительно в секции *Отправка нотификаций* можно настроить следующие параметры уведомлений о событиях:

- **agent\_manager.periodic.send\_events\_notifications.max\_event\_age** - события старше, чем это количество секунд, не будут обрабатываться;
- **agent\_manager.periodic.send\_events\_notifications.events\_query\_limit** - количество обрабатываемых за раз событий;
- **agent\_manager.periodic.send\_events\_notifications.events\_per\_message** - максимальное количество сгруппированных событий в одном сообщении;
- **agent\_manager.periodic.send\_events\_notifications.preferred\_language** - язык сообщений с событиями (ru, en);
- **agent\_manager.periodic.send\_events\_notifications.message\_headers** - конфигурация заголовков сообщений;
- **agent\_manager.periodic.send\_events\_notifications.syslog\_settings** - конфигурация syslog отправки уведомлений о событиях;
- **agent\_manager.periodic.send\_events\_notifications.syslog\_settings.vendor** - значение поля vendor для отправляемых событий;
- **agent\_manager.periodic.send\_events\_notifications.syslog\_settings.product** - значение поля product для отправляемых событий;

- **agent\_manager.periodic.send\_events\_notifications.syslog\_settings.cef\_version** - значение поля `cef_version` для отправляемых событий;
- **agent\_manager.periodic.send\_events\_notifications.syslog\_settings.preferred\_language** - язык для событий;

Внутренние события и сообщения **Бэкенда Базис.vControl** и **Менеджера агентов Базис.vControl** по умолчанию записываются в локальный текстовый файл. Для включения отправки этих сообщений на внешний Syslog-сервер выполните следующие шаги:

1. В боковом меню перейдите в раздел *Управление и мониторинг* → *Настройки системы*.
2. Найдите секцию *Логирование*.
3. Укажите в параметрах необходимые значения:
  - **logging.syslog** — включение отправки сообщений syslog-серверу.
  - **logging.syslog\_only** — включение отправки сообщений syslog-серверу без создания локальных текстовых файлов на **Бэкендах Базис.vControl**, все сообщения будут отправляться на удаленный сервер.
  - **logging.handlers.AppSyslog.level** — уровень логирования в syslog.
4. Нажмите кнопку **Сохранить** в левом верхнем углу для сохранения внесенных изменений.

### 16.3.4 Изменение уровня логирования Бэкенда

Система имеет два уровня логирования:

**INFO** — уровень логирования по умолчанию, при котором в логи записываются только факты операций и их результаты;

**DEBUG** — расширенный уровень логирования, при котором записываются дополнительные блоки информации по операциям и расширенные сообщения об ошибках. Такой режим позволяет вести отладку решения при первоначальном деплое или решении каких-то сложных технических проблем.

Для изменения уровня логирования выполните следующие шаги:

1. В боковом меню перейдите в раздел *Управление и мониторинг* → *Настройки системы*.
2. Найдите секцию *Логирование*.
3. Укажите в параметре **logging.handlers.AppFile.level** необходимое значение уровня логирования.
4. Нажмите кнопку **Сохранить** в левом верхнем углу для сохранения внесенных изменений.

## 16.4 Справочник по параметрам конфигурации системы

Администратор **Базис.vControl** может изменить настройки системы двумя способами:

- Указать новые значения параметров в разделе *Управление и мониторинг* → *Настройки системы*.
- Вручную внести изменения в файлы конфигурации *vms-config* и *backend-overrides*.

В разделе *Настройки системы* представлен ограниченный набор настроек. Изменения этих настроек вступают в силу сразу после сохранения новых значений и без необходимости повторного развертывания системы.

Имя	Значение	По умолча...	Описание
<b>Политика паролей</b>			
user.password.min_length	8	8	Минимально допустимая длина
user.password.max_length	256	256	Максимально допустимая длина
user.password.expiration_time	5184000	5184000	Время истечения действия пароля, секунды
user.token.ttl	86400	86400	Время жизни токена аутентификации АПИ, секунды
user.password_token.ttl	3600	3600	Время жизни токена сброса пароля, секунды
user.max_attempt_count	4	4	Максимальное допустимое количество попыток неверного ввода пароля
user.lockout_time	900	900	Время блокировки пользователя после исчерпания попыток ввода пароля, секунды
user.ip_max_attempt_count	15	15	Максимальное допустимое количество попыток неверного ввода пароля
user.ip_lockout_time	900	900	Время блокировки IP после исчерпания попыток ввода пароля, секунды
user.max_number_of_parallel_service_logins	10	10	Максимальное число параллельных логинов сервисных пользователей BPM
user.password.allowed_symbols[0].symbols	abcdefghijklmnopqrstuvwxyz	abcdefghijklmnopqrstuvwxyz	Группа допустимых символов
user.password.allowed_symbols[0].min_count	1	1	Минимальное кол-во символов в группе
user.password.allowed_symbols[1].symbols	ABCDEFGHIJKLMNOPQRSTUVWXYZ	ABCDEFGHIJKLMNOPQRSTUVWXYZ	Группа допустимых символов

Рисунок 16.3 Общий вид раздела «Настройки системы»

Раздел представляет собой форму с набором параметров, сгруппированных по категориям. Для каждого параметра представлена следующая информация:

- **Имя** — наименование параметра в рамках **Базис.vControl**.
- **Значение** — текущее значение параметра.
- **По умолчанию** — подсказка с информацией о значении по умолчанию для данного параметра.
- **Описание** — подсказка с кратким описанием назначения параметра.

Для изменения параметра через интерфейс выполните следующие шаги:

1. В общем списке найдите параметр, который необходимо изменить.



### Совет

Для быстрого перехода к нужному параметру воспользуйтесь формой поиска в правом верхнем углу.

---

2. В поле «Значение» укажите новое значение параметра.
3. Нажмите кнопку **Сохранить** в левом верхнем углу для сохранения внесенных изменений.

Настройки имеют следующий механизм обновления значений параметров:

- При сохранении настроек новые значения параметров записываются в базу данных системы.
- Если были изменены настройки **Агента Базис.vControl**, то эти изменения отправляются на все агенты хостов и записываются в файле */etc/vms-agent.yaml*.
- Сервисы **Бэкенда** используют настройки, которые хранятся в базе данных системы. Если в базе данных настройка не переопределена, то значения параметров считываются из конфигурационных файлов.

Если необходимо изменить параметры, которые не отображены в разделе *Настройки системы*, то их следует задать в конфигурационных файлах в YAML-формате:

- **vms-config** — основной файл для настройки конфигурации **Базис.vControl**.
- **backend-overrides** — файл для переопределения значений дополнительных параметров системы, не содержащихся в **vms-config**. Переопределять можно все параметры из описанных ниже разделов. Все, что было переопределено в **backend-overrides**, добавится в */etc/vms.yaml*.



### Примечание

При необходимости добавить переопределение после того, как **Бэкенд** был установлен, нужно внести необходимые параметры в **backend-overrides** и переустановить **Бэкенд**.

Для обнуления ранее прописанных переопределений нужно выполнить переустановку **Бэкенда** с пустым **backend-overrides**.

---

- **agent-overrides** — файл для переопределения значений дополнительных параметров **Агента Базис.vControl**, не содержащихся в **vms-config**.

Переопределять можно все параметры из описанных ниже разделов. Все, что было переопределено в `agent-overrides`, добавится в `/etc/vms-agent.yaml`.

---

### Примечание

При необходимости добавить переопределение после того, как агент был установлен, нужно внести необходимые параметры в `agent-overrides`, выполнить установочный скрипт с параметром `-o`:

```
./deploy.sh -o
```

---

### Примечание

Для Astra Linux установка выполняется от непривилегированного пользователя, которому доступно `sudo` без пароля. Если установка идет при прямом доступе в консоль (не через `ssh`), то во время логина пользователя *integrity level* должен быть выбран «63». Затем необходимо переустановить **Агента**, обновив его в веб-интерфейсе. Для обнуления ранее прописанных переопределений нужно выполнить переустановку **Агента** с пустым `agent-overrides`.

---

### 16.4.1 Правила редактирования конфигурационных файлов

Описание значений параметров системы в конфигурационных файлах задается в YAML-формате. В рамках данного формата при редактировании файлов следует придерживаться основных правил:

- Комментарии начинаются с символа «решетки» (`#`), могут начинаться в любом месте строки и продолжаются до конца строки.
- Для формирования структуры параметров используются отступы только из пробелов, символ табуляции запрещен.
- Значения вида «параметр-значение» и «параметр-подпараметр» представлены двоеточием с пробелом (`:`).
- Списки обозначаются начальным дефисом (`-`) с одним членом списка на строку, либо члены списка заключаются в квадратные скобки (`[ ]`) и разделяются запятой и пробелом (`,`).
- Строковые значения параметров заключаются в одиночные кавычки.
- Параметры, имеющие в названии URL, должны начинаться с `http://` или `https://`.



В данном документе описание параметров приводится в виде строк, в которых элементы YAML-структуры разделены точкой (.), последний элемент является названием параметра.

В качестве примера рассмотрим запись значения «true» для параметра ***image.cache.vstorage\_cache\_enabled***:

```
image:
  cache:
    vstorage_cache_enabled: true
```

### 16.4.2 Деактивация/активация суперпользователя

Для деактивации учётной записи суперпользователя - администратора **Базис.vControl** с повышенными привилегиями - необходимо:

1. На бэкенде **Базис.vControl** выполнить команду:

```
/opt/vms/bin/vmsmngr superadmin --deactivate
```

2. При успешном выполнении дождитесь сообщения о завершении операции. После данных действий суперпользователь будет деактивирован.

При необходимости активации учётной записи суперпользователя необходимо проделать следующие шаги:

1. На бэкенде **Базис.vControl** выполнить активацию суперпользователя, обязательно указывая его **login** или **email**. В противном случае суперпользователь не будет активирован:

```
/opt/vms/bin/vmsmngr superadmin --login=admin
```

либо:

```
/opt/vms/bin/vmsmngr superadmin --email=admin@email.com
```

2. При успешном выполнении дождитесь сообщения о завершении операции. После данных действий суперпользователь будет активирован.

Чтобы узнать **login** и **email** суперпользователя наберите команду:

```
/opt/vms/bin/vmsmngr superadmin
```

### 16.4.3 Параметры конфигурации для Бэкенда Базис.vControl

Ниже представлен пример содержимого конфигурационного файла для **Бэкенда Базис.vControl**. Файл предоставлен в ознакомительных целях, ручная правка не подразумевается. Во время установки/обновления системы файл генерируется автоматически на основании переданных для установки параметров.

```
stage: somestage

database:
  uri: !vault |
      $ANSIBLE_VAULT;1.1;AES256

74323339323534616534373233303733313266336531396331393138316361623838
336532386435

6139376363623730376632656130613061393139663562320a646264383061636532
643466303566

34383834636662353235613561346564353536613963303230643565343733663730
313339666466

3030633162663936350a636166666561303862326331623965356330656436313334
636530343232

34653733613236613432346565336433656335623766343961376537656666396137
306433353230

64623162633862316437306463393066396531666531363337303361333532663038
666431663731
      626338623663613932323232393139383435

memdb:
  password: !vault |
      $ANSIBLE_VAULT;1.1;AES256

45376434636637376139346139623532353236363964333464353063643163346133
633431643832

3535353462636637366464323435306361356433663363650a353534653132616430
663862616439
```

```
31643932613332393662316361663231326163393938303035323066326637663866
346438383565

3230376666656333660a343834316165393238363139373162396234623738323463
373436613735
    6535
    sentinel: vmscache
    hosts:
      - [ 123.123.123.123, 5000]
      - [ 123.123.123.124, 5000]
      - [ 123.123.123.125, 5000]

metricsdb:
  url: http://123.123.123.123:8123/

api:
  entry_point:

sentry:
  backend: ""
  js: ""

agent_manager:
  agent_port: "5001"
  backend_port: "5501"
  backends_bind_host: "123.123.123.124"
  agents_bind_host: "123.123.123.124"

logging:
  handlers:
    AppFile:
      level: "DEBUG"
  timezone: "Europe/Moscow"

ws:
  host: 123.123.123.123
  port: 8081
  vdi_redis:
    password: !vault |
      $ANSIBLE_VAULT;1.1;AES256

73393433353937376164393037343438303132353635366535663839363832343737
663262333366

3238346163643463393530373435626263376535623137630a383366393964623032
393331336238

39396336366433323231653965386161373539313462336561323935366337333735
```

```
313733316430

3831313131353062630a363338386434386464616130306639353064393862656664
326635343363
    6539
  hosts:
    - [ 123.123.123.126 , 5000]
    - [ 123.123.123.127 , 5000]
    - [ 123.123.123.128 , 5000]
  sentinel: vdicache

vault:
  password_file: /opt/vms-playbooks/playbooks/deploy
```

Описание параметров:

---



### Совет

Правила описания параметров в YAML-формате представлены в разделе Приложения [Правила редактирования конфигурационных файлов](#).

---



### Примечание

Полный список параметров с описанием представлен в разделе *Управление и мониторинг* → *Настройки системы*.

---

#### 16.4.4 Параметры конфигурации для Агента Базис.vControl

Ниже представлен пример содержимого конфигурационного файла для **Агента Базис.vControl**. Файл предоставлен в ознакомительных целях, ручная правка не подразумевается. Во время установки/обновления системы файл генерируется автоматически на основании переданных для установки параметров.

```
stage: deploy
agent:
  agent_manager_host: "127.0.0.1" # ip agent manager, всегда
127.0.0.1, так как трафик идет через тоннель
  identity: "3" # идентификатор агента, присваивается agent manager
```

```
при установке агента
sentry:
  agent:
    http://ff7411e84a584317a344c17cf3fa2f28:4185f91bd460426da292d9d924b1
    2a31@domain.ru/5 # данные для доступа к sentry
```

Описание параметров:

---



### Совет

Правила описания параметров в YAML-формате представлены в разделе [Правила редактирования конфигурационных файлов](#).

---



### Примечание

Полный список параметров с описанием представлен в разделе *Управление и мониторинг* → *Настройки системы*.

---

## 16.5 Настройка включения SSO-авторизации в систему

Доступна SSO-авторизация для бесшовного входа пользователей в инфраструктуру **Базис.vControl** внутри домена. Для включения данной функции администратору необходимо:

- настроить контроллер домена;
- настроить **Бэкенд Базис.vControl** и внести соответствующие изменения в веб-интерфейсе системы;
- внести изменения в ***backend-overrides*** на **Сервере развертывания**;
- настроить браузер для автоматического входа;
- проверить корректность выполненных настроек.

Перед началом работы администратор должен проверить выполнение следующих требований:

1. Придумайте свободный FQDN в домене, в котором требуется настроить SSO для инфраструктуры **Базис.vControl** (в примере ниже используется ***vms-vip.sk.local***).

2. Для этого FQDN в Active Directory должна быть A запись, ссылающаяся либо на виртуальный IP-адрес **Базис.vControl** в случае установки с отказоустойчивостью, либо на адрес **Бэкенда Базис.vControl** в случае установки без отказоустойчивости.
3. Время с контроллером домена должно быть синхронизировано на всех **Бэкендах Базис.vControl** и машинах, которые будут работать в веб-интерфейсе **Базис.vControl** с SSO-авторизацией.
4. **Базис.vControl** должна быть настроена на авторизацию в домене, к которому требуется подключить SSO. Для всех пользователей домена, которые будут работать в веб-интерфейсе **Базис.vControl**, должны быть выданы соответствующие права внутри системы.
5. Клиентская машина должна быть присоединена к домену. Учетная запись, из-под которой производится сквозная аутентификация, должна быть доменной.
6. Все имена машин, что будут прописаны в **krb5.conf**, должны успешно резолвиться в IP-адреса на всех **Бэкендах Базис.vControl**.

### 16.5.1 Настройки в контроллере домена

На контроллере домена нужно добавить пользователя Active Directory, затем привязать к нему SPN и сгенерировать keytab. Для этого выполните следующие шаги:

1. В консоли PowerShell на контроллере домена запустите команду для добавления пользователя:

```
New-ADUser -Name "vms-web-sso" -GivenName "vms-web-sso" -Surname "vms-web-sso" -SamAccountName "vms-web-sso" -AccountPassword (Read-Host -AsSecureString "Password:") -DisplayName "vms-web-sso" -Enabled $true -PasswordNeverExpires $true -UserPrincipalName HTTP/vms-vip.sk.local@SK.LOCAL
```

- В качестве имени пользователя в примере указано **vms-web-sso**.
- В параметре **-UserPrincipalName** значение **vms-vip.sk.local** является FQDN для инфраструктуры **Базис.vControl**, а значение **@SK.LOCAL** — Kerberos realm.

На запрос пароля введите желаемый пароль.

2. Запустите команду генерации keytab:

```
ktpass -princ HTTP/vms-vip.sk.local@SK.LOCAL -mapuser vms-web-sso -pass 'P@$w0rd' -crypto ALL -ptype KRB5_NT_PRINCIPAL -out vms.keytab -setupn -setpass
```

- Значение **P@\$\$w0rd** является паролем для созданной ранее учетной записи **vms-web-ss0**.
- **vms.keytab** — файл, в который будет выгружен keytab пользователя.

### 16.5.2 Настройки в Бэкенде Базис.vControl

1. Создайте файл **krb5.conf** следующего содержания (регистр следует соблюдать):



#### Осторожно

При копировании **krb5.conf** из примера в итоговом файле не должно быть пробелов перед параметрами.

---

```
[logging]
default = FILE:/var/log/krb5libs.log
kdc = FILE:/var/log/krb5kdc.log
admin_server = FILE:/var/log/kadmind.log
[libdefaults]
dns_lookup_kdc = false
dns_lookup_realm = false
forwardable = true
ticket_lifetime = 24h
default_realm = SK.LOCAL
default_keytab_name=/etc/vms.keytab
[realms]
SK.LOCAL = {
kdc = ad.sk.local
default_domain = SK.LOCAL
admin_server = ad.sk.local
}
[domain_realm]
.sk.local = SK.LOCAL
sk.local = SK.LOCAL
```

- **SK.LOCAL** — realm для домена sk.local, как правило совпадает с именем домена.
- **default\_domain** — определяет домен, который используется для трансляции Kerberos 4 spn в Kerberos 5 spn.
- **kdc** — имя или адрес KDC для заданного Kerberos realm.

- **admin\_server** — определяет хост, на котором работает сервер администрирования. Обычно это главный сервер Kerberos.
- В секции **[domain\_realm]** описывается трансляция между именем домена или hostname в realm Kerberos.



### Совет

Более подробную информацию можно прочитать через **man krb5.conf** на Бэкенде Базис.vControl.

---

2. Проверьте выполнение пункта №6 из предварительных требований.
3. Переместите сгенерированный ранее keytab-файл в **/etc/vms.keytab** и задайте следующие права доступа:

```
chown root:vms /etc/vms.keytab
chmod 440 /etc/vms.keytab
```

4. Проверьте корректность выполненных настроек:

```
kinit -kV -p HTTP/vms-vip.sk.local
```

В случае успеха должны получить сообщение: «Authenticated to Kerberos v5». Затем выполните команду **kdestroy**.

### 16.5.3 Настройки в веб-интерфейсе Базис.vControl

В настройках системы следует задать значение для поля **kerberos.server**. Для этого выполните следующие шаги:

1. Перейдите в раздел *Управление и мониторинг* → *Настройки системы*.
2. Перейдите в блок настроек *LDAP, Kerberos*.
3. В параметре **kerberos.server** в качестве значения укажите данные, используемые в качестве SPN, в примере выше: **HTTP/vms-vip.sk.local**. Убедитесь, что ввели значение без каких-либо пробелов в начале или конце.

### 16.5.4 Настройки на сервере развертывания

1. Добавьте в файл переопределений **backend-overrides** следующее:



```
config_js:  
  show_sso_auth: true
```

Все отступы в параметрах должны быть сохранены.

2. Выполните переразвертывание **Бэкендов Базис.vControl**.

### 16.5.5 Настройки для браузера

#### 16.5.5.1 Internet Explorer

Для настройки браузера Internet Explorer выполните следующие шаги:

1. Перейдите в раздел настроек: *Свойства браузера* → *Безопасность* → *Местная интрасеть* → *Сайты* → *Дополнительно*.
2. В строке **Добавить в зону следующий узел** введите значение «https://vms-vip.sk.local», где «vms-vip.sk.local» замените на используемый вами FQDN.
3. Нажмите **Добавить**.

Уровень безопасности для указанной зоны должен быть задан по умолчанию. Если для зоны были заданы дополнительные настройки, то включите в них опцию **Автоматический вход в сеть с текущим именем пользователя и паролем**.

#### 16.5.5.2 Microsoft Edge

---

#### **Примечание**

Данные рекомендации относятся к версии 87.0.664.47 и выше.

---

Если FQDN уже добавлен в *Местная интрасеть* через Internet Explorer согласно инструкции выше, то в браузере Microsoft Edge не нужно делать дополнительных настроек. В ином случае в Microsoft Edge нужно настроить GPO AuthServerAllowlist так, как описано в [официальном справочном руководстве](#) (добавить **vms-vip.sk.local** в AuthServerAllowlist, где «vms-vip.sk.local» замените на используемый вами FQDN).

#### 16.5.5.3 Google Chrome

---

#### **Примечание**

Данные рекомендации относятся к версии 87.0.4280.66 и выше.

---

Если FQDN уже добавлен в *Местная интрасеть* через Internet Explorer согласно инструкции выше, то в браузере Google Chrome не нужно делать дополнительных настроек. В ином случае Google Chrome нужно запускать с параметром:

```
--auth-server-whitelist="https://vms-vip.sk.local"
```

- «vms-vip.sk.local» замените на используемый вами FQDN.

Также можно включить данный параметр через GPO согласно шаблону из [официального справочного руководства](#).

### 16.5.5.4 Mozilla Firefox



#### Примечание

Данные рекомендации относятся к версии 83.0 и выше.

Для настройки браузера Mozilla Firefox выполните следующие шаги:

1. Откройте в адресной строке браузера URL конфигурирования: about:config.
2. Дождитесь появления предупреждения и нажмите **Принять риск и продолжить**.
3. С помощью строки поиска найдите параметр **network.negotiate-auth.trusted-uris** и введите значение «https://vms-vip.sk.local», где «vms-vip.sk.local» замените на используемый вами FQDN.

### 16.5.6 Проверка работы SSO-авторизации

Для проверки корректности выполненных настроек следует зайти в систему по адресу: <https://vms-vip.sk.local> (FQDN используемый ранее). В случае успешной настройки в форме входа появится новая опция **Войти под доменным пользователем** (рисунок 16.4), при нажатии которой должна произойти сквозная SSO-авторизация.

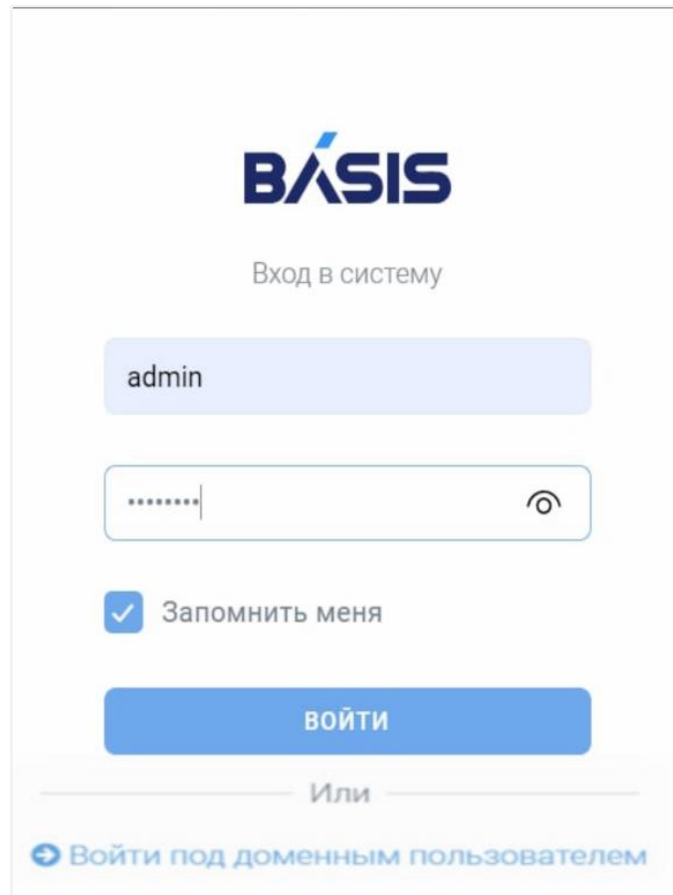


Рисунок 16.4 Вход в систему с возможностью SSO-авторизации

Если не была выполнена настройка браузера по добавлению FQDN **vms-vip.sk.local** в доверенные для хоста, то при первом входе в систему потребуется ввести логин и пароль доменного пользователя.

## 16.6 Сценарии использования API Базис.vControl

### 16.6.1 Добавление открытого SSH-ключа через HTTP API

---

#### **Примечание**

Добавление открытого ключа доступно только для авторизованного пользователя с правами **Хост** → **SSH консоль**. Для аутентификации с сохранением cookies выполните команду:

---

```
$ curl -i -X POST -H "Content-Type:application/json" -d
'{"login": "Your_login", "password": "Your_password"}'
'https://123.123.123.123/api/0/auth' -k -c /tmp/cookies
```

При запросе своим клиентом необходимо запомнить cookie `api_token` и использовать для последующих запросов.

---

Добавление открытых ключей для авторизации по SSH можно произвести через API-запрос следующего вида:

```
POST /api/0/node/<node>/public_key(node, key_data, expiration_seconds)
```

где:

- **node (id)** — идентификатор хоста;
- **key\_data (str)** — содержимое открытого ключа;
- **expiration\_seconds (int)** — срок действия ключа. Если в запросе этот параметр не указан, используется конфигурационный параметр сервера **conf.node.public\_key\_max\_expiration**, по умолчанию он равен  $30*60$  (30 минут). Истечение времени жизни ключа проверяется периодической задачей раз в минуту.

Возвращаемые значения:

- **public\_key\_info (dict)** — информация о публичном ключе;
- **task\_info (dict)** — информация об асинхронной задаче.

На данный момент система поддерживает только формат ключа RSA.

### 16.6.2 Получение статуса компонентов Базис.vControl

Для получения информации об инфраструктуре **Базис.vControl** и статусов работы ее компонентов можно послать GET HTTP-запрос следующего вида:

```
http://123.123.123.123/api/0/status?no_cache=true
```

Параметр **no\_cache** определяет актуальность данных в ответе: либо информация будет взята из кэша (`false`), либо будет собрана актуальная на момент запроса информация (`true`).

Для успешного выполнения запроса требуется наличие учетной записи с правами на просмотр инфраструктуры, выданными на уровне корня. В случае авторизованного запроса возвращается ответ в статусе 200, содержащий JSON-документ вида:

```
{
  "request_id": "id-123",
  "status": {
    "backends": [
      {
        "address": "127.0.0.1:443",
        "alive": true
      },
      {
        "address": "177.77.225.77:443",
        "alive": true
      }
    ],
    "clickhouse": [
      {
        "host": "127.0.0.1",
        "is_up": true,
        "port": 8123
      }
    ],
    "db": {
      "address": "127.0.0.1:5432",
      "read": true,
      "write": true
    },
    "managers": [
      {
        "address": "177.77.225.77:5501",
        "alive": true
      },
      {
        "address": "10.10.10.83:5501",
        "alive": true
      }
    ],
    "memdb": {
      "address": "10.10.10.83:6379",
      "read": true,
      "write": true
    },
    "redis": [
      {
        "host": "10.10.10.83",
        "is_master": true,
        "objective_alive": true,
        "port": 6379,
        "role_reported": "master",

```

```
    "subjective_alive": true
  },
  {
    "host": "10.10.10.82",
    "is_master": false,
    "objective_alive": true,
    "port": 6379,
    "role_reported": "slave",
    "subjective_alive": false,
    "master": {
      "host": "?",
      "port": 0,
      "connected_to_master": false
    }
  },
  {
    "host": "10.10.10.81",
    "is_master": true,
    "objective_alive": true,
    "port": 6379,
    "role_reported": "slave",
    "subjective_alive": true,
    "master": {
      "host": "10.10.10.83",
      "port": 6379,
      "connected_to_master": true
    }
  }
],
"sentinel": [
  {
    "host": "10.10.10.81",
    "port": 5000,
    "alive": true
  },
  {
    "host": "10.10.10.82",
    "port": 5000,
    "alive": true
  },
  {
    "host": "10.10.10.83",
    "port": 5000,
    "alive": true
  }
],
"vip": {
  "address": "177.77.225.77",
```

```
        "alive": true
    }
}
}
```

- ***is\_cached*** — флаг, означающий что ответ взят из кэша.
- ***timestamp*** — время, когда был сделан оригинальный ответ (POSIX-время).
- секция ***backends*** — данные о состоянии **Бэкендов Базис.vControl**:
  - **address** — IP-адрес.
  - **alive** — статус работоспособности: true — активен, false — сбой.
- секция ***clickhouse*** — данные о состоянии БД метрик:
  - **host** — IP-адрес хоста.
  - **port** — порт подключения.
  - **alive** — статус работоспособности: true — активен, false — сбой.
- секция ***db*** — данные о состоянии БД:
  - **address** — IP-адрес.
  - **read** — статус доступности БД на чтение: true — доступна, false — сбой.
  - **write** — статус доступности БД на запись: true — доступна, false — сбой.
- секция ***managers*** — данные о состоянии **Менеджеров Агентов Базис.vControl**:
  - **address** — IP-адрес.
  - **alive** — статус работоспособности: true — активен, false — сбой.
- секция ***memdb*** — данные о состоянии КЭШ БД (Redis):
  - **address** — IP-адрес.
  - **read** — статус доступности КЭШ БД на чтение: true — доступна, false — сбой.
  - **write** — статус доступности КЭШ БД на запись: true — доступна, false — сбой.
- секция ***redis*** — данные о состоянии Redis-серверов в кластере:
  - **host** — IP-адрес узла.
  - **port** — порт подключения.
  - **is\_master** — флаг того, является ли данный узел master-узлом в кластере.
  - **subjective\_alive** — флаг того, находится ли данный узел в субъективно рабочем состоянии.
  - **objective\_alive** — флаг того, находится ли данный узел в объективно рабочем состоянии.
  - **role\_reported** — передаваемый тип узла в кластере: master или slave.
- секция ***sentinel*** — данные о состоянии Redis-sentinels:

- **host** — IP-адрес узла.
  - **port** — порт подключения.
  - **is\_master** — флаг того, является ли данный узел master-узлом в кластере.
  - **subjective\_alive** — флаг того, находится ли данный узел в субъективно рабочем состоянии.
  - **objective\_alive** — флаг того, находится ли данный узел в объективно рабочем состоянии.
  - **role\_reported** — передаваемый тип узла в кластере: master или slave.
- секция **vip** — данные о virtual IP:
    - **address** — IP-адрес.
    - **alive** — статус работоспособности: true — активен, false — сбой.

### 16.7 Поддерживаемые версии PostgreSQL

#### **Примечание**

Для open source версий PostgreSQL (9.6 и выше) в случае установки в non-HA режиме подразумевается, что пакеты берутся из репозитория дистрибутива Linux, на который ставится продукт.

Таблица 16.1 Поддерживаемые версии PostgreSQL

Продукт	Версия	ОС и тип развертывания
Postgres 15	PostgresProStandart	Astra Linux Орел 1.7: HA, non-HA Astra Linux Смоленск 1.7: HA, non-HA
Postgres 15	PostgresProStandart Certified	Astra Linux Смоленск 1.7: HA, non-HA
Postgres 15	PostgresProEnterprise Certified	Astra Linux Смоленск 1.7: HA, non-HA
Postgres 9.6	Open Source	Альт 8 СП: HA, non-HA Альт 9.2: HA, non-HA
Postgres 10	Open Source	Альт 8 СП: HA, non-HA Альт 9.2: HA, non-HA Альт 10.1: HA, non-HA



Продукт	Версия	ОС и тип развертывания
Postgres 11	Open Source	Альт 8 СП: HA, non-HA Альт 9.2: HA, non-HA Альт 10.1: HA, non-HA Astra Linux 1.7.3: HA, non-HA Astra Linux 1.7.4: HA, non-HA
Postgres 12	Open Source	Альт 8 СП: HA, non-HA Альт 9.2: HA, non-HA Альт 10.1: HA, non-HA
Postgres 13	Open Source	Альт 10.1: HA, non-HA
Postgres 14	Open Source	Альт 10.1: HA, non-HA Astra Linux 1.7.3: HA, non-HA Astra Linux 1.7.4: HA, non-HA
Postgres 15	Open Source	Альт 10.1: HA, non-HA

## 17. ССЫЛКИ НА ЦИТИРУЕМЫЕ ДОКУМЕНТЫ



### Примечание

Ниже приведен список ссылок на документацию, состав которой может периодически обновляться. Для составления документа **Базис.vControl. Руководство по установке** использовалась доступная актуальная информация.

Таблица 17.1 Ссылки на цитируемые документы

Описание	Ссылка
Описание работы СУБД ClickHouse	<a href="https://clickhouse.yandex/docs/ru/table_engines/replication.html">https://clickhouse.yandex/docs/ru/table_engines/replication.html</a>
Описание функционала и работы сетевого хранилища данных Redis Sentinel	<a href="https://redis.io/topics/sentinel">https://redis.io/topics/sentinel</a>
Инструкции по установке Postgres Pro для HA	Идет в составе пакета документации