.1

БАЗИС.WORKPLACE
РУКОВОДСТВО ПО УСТАНОВКЕ

ВЕРСИЯ 2.2.1

Оглавление

1. ВВЕДЕНИЕ

1.1 Описание системы Базис.WorkPlace

Решение **Базис.WorkPlace** (**Виртуальное рабочее место**) интегрировано с системой управления виртуальными средами **Базис.vControl**.

Решение **Базис.WorkPlace** необходимо для создания и управления единой средой удаленных рабочих столов конечных пользователей. Такое решение позволяет управлять доступом к IT-ресурсам, обеспечивать удаленный доступ сотрудников к ресурсам из других филиалов или из внешней среды. Также достигается экономия средств за счет использования аппаратных тонких клиентов и нетбуков вместо обычных, более дорогих в обслуживании рабочих станций.

Основные функциональные возможности **Базис.WorkPlace**:

- Поддержка различных протоколов для доступа в виртуальную среду для кроссплатформенной работы (GNU/Linux → GNU/Linux, GNU/Linux → Windows, Windows → Windows, Windows → GNU/Linux).
- Поддержка в виртуальных средах ПО, требующего выделенных графических адаптеров (например, рабочие места САПР-/CAD-проектировщиков) в зависимости от используемых протоколов доставки рабочего стола.
- Кроссплатформенная печать из виртуальных сред на локально установленные принтеры без дополнительного администрирования (не требуется установка драйверов локального принтера в виртуальные машины — в зависимости от протоколов доставки рабочего стола).
- Сквозная аутентификация на рабочем столе, в том числе с использованием двухфакторной аутентификации, а также «проброс» средств аутентификации (USB-токенов) в виртуальный рабочий стол.

Система Базис.WorkPlace может быть интегрирована с внешними каталогами учетных записей пользователей:

- Microsoft Active Directory,
- OpenLDAP,
- FreeIPA,
- SambaDC.

При этом поддерживается работа политики безопасности срока действия паролей учетных записей, а Клиент Базис.WorkPlace позволяет менять просроченный пароль внешних учетных записей. Также Базис.WorkPlace имеет собственные настройки политики безопасности срока действия паролей, которые могут накладываться на доменную политику, усиливая ее.

1.2 Список используемых терминов и сокращений

Термин	Описание
Агент ВРМ	Приложение, которое устанавливается на виртуальной машине и настраивается на работу с Бэкендом Базис.WorkPlace. Агент устанавливается в ВМ, из которой должен быть сделан шаблон рабочего стола
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 виртуализации и расширяющая их функциональность
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
Брокер	Брокер подключения к удаленному рабочему столу - программное обеспечение, которое позволяет клиентам получать доступ к различным типам размещенных на сервере рабочих столов и приложений
Бэкенд Базис.WorkPlace	Основная часть комплекса Базис.WorkPlace. Осуществляет хранение информации об инфраструктуре Базис.WorkPlace, настройки политик, безопасности, выполняет операции по управлению элементами инфраструктуры Базис.WorkPlace. В состав Бэкенда Базис.WorkPlace входят база данных, API-бэкенд и Менеджер диспетчеров подключений
Виртуальная машина, ВМ	Программа, которая эмулирует реальный (физический) компьютер со всеми его компонентами (жесткий диск, DVD-ROM, BIOS, сетевые адаптеры и т.д.). Как правило, ВМ содержит установленную операционную систему и компоненты среды виртуализации (гостевые утилиты, драйверы эмулируемых устройств)

Термин	Описание
Виртуальная среда, ВС	Общее именование виртуальных машин, управляемых средствами Базис.vControl и функционирующих на хосте в составе кластера на ресурсах, выделяемых гипервизором
Виртуальное рабочее место, ВРМ, рабочий стол	Полностью подготовленная для работы виртуальная машина с установленной на ней целевой операционной системой и прикладным ПО, необходимым для выполнения задач. ВРМ включает компонент Агент ВРМ и взаимодействует через него с инфраструктурой ВРМ для подключения назначенного пользователя
Горячий резерв пула сессионных рабочих столов, горячий резерв, ГР	Определенное количество рабочих столов в пуле сессионных рабочих столов, которые созданы, но не ассоциированы с конкретными пользователями. Выдаются пользователю в момент подключения его к пулу, когда у пользователя нет ассоциированного рабочего стола (подключение в первый раз, или, когда рабочий стол удален/переведен в горячий резерв). Такие рабочие столы создаются заранее, чтобы сократить время ожидания пользователя при подключении к рабочему столу в пуле, т.к. без горячего резерва рабочий стол (и его ВМ) будет создаваться только при подключении пользователя
Двухфакторная аутентификация	Использование нескольких источников информации о пользователе (например Логин/пароль + токен с сертификатом)
Диск	Жесткий диск хоста или ВМ
Диспетчер подключений, ДП	Точка входа для пользователей в инфраструктуру Базис.WorkPlace. Диспетчер подключений принимает подключения пользователей, проверяет права доступа и производит подключение пользователей к назначенным рабочим столам. Является необходимым узлом для подключения пользователя к Базис.WorkPlace. Инфраструктура ВРМ может содержать несколько диспетчеров подключений
Кластер Redis	Отказоустойчивый кластер из серверов Redis

Термин	Описание
Клиент Базис.WorkPlace	Приложение, которое устанавливается на устройстве доступа пользователя. Производит подключение к Диспетчеру подключений. После аутентификации и выбора рабочего стола туннелирует подключения клиента протокола через диспетчер подключений в требуемый рабочий стол
Менеджер диспетчеров подключений (Брокер-менеджер, BrokerManager)	Часть Бэкенда Базис.WorkPlace. Выполняет операции по управлению диспетчерами подключений и их подключениями. Выполняет периодические операции, необходимые для соблюдения политик и поддержания инфраструктуры BPM в заданном состоянии. Управляет горячим резервом пулов сессионных рабочих столов, обеспечивает подготовку рабочих столов при подключении пользователей
Пул рабочих столов	Объединение рабочих столов в едином пуле ресурсов Базис.vControl. Пул может содержать отдельные рабочие столы, назначенные отдельным пользователям. Через пул рабочих столов можно также задавать общие настройки для рабочих столов. Рабочие столы в этом пуле могут быть созданы из разных шаблонов в зависимости от задач, которые должен выполнять пользователь
Пул сессионных рабочих столов	Пул рабочих столов, в котором рабочие столы создаются на основе одного заданного шаблона для массового использования большого количества однотипных рабочих мест. Права задаются массово через группу пользователей. Возможно изменение шаблона, которое приводит к пересозданию всех незанятых рабочих столов. Имеет Горячий резерв
САПР/CAD	Система автоматизированного проектирования
Сервер Redis	Сервер оперативной БД для хранения текущей информации о подключениях и статусе компонентов решения
Сервер развертывания Базис.WorkPlace	Сервер или ВМ, с которых производится развертывание решения в отказоустойчивой конфигурации. Используется только для развертывания, в работе системы не участвует

Термин	Описание
Сквозная аутентификация	Аутентификация пользователя в рабочих столах по однократно введенному логину/паролю в Клиент Базис.WorkPlace
Тонкий клиент	Облегченный программно-аппаратный комплекс, используемый в качестве компьютера для запуска клиента Базис.WorkPlace
Устройство доступа, УД	Компьютер, ноутбук или тонкий клиент, используемый пользователем для доступа в инфраструктуру Базис.WorkPlace
Фронтенд BPM	Интерфейс взаимодействия между администратором Базис.WorkPlace и основной программно-аппаратной частью (Бэкенд BPM). Фронтенд BPM является частью Фронтенда Базис.vControl
Хост, хост виртуализации	Физический сервер, на котором установлено программное обеспечение гипервизора, расширяющего возможности хостовой ОС по разделению ресурсов (виртуализации)
Шаблон рабочего стола	Шаблон в системе Базис.vControl для создания ВМ и рабочих столов. В операционной системе шаблона рабочего стола должен быть установлен и настроен Агент BPM
ACL	Список контроля доступа.
Ansible	Средство автоматизации установки и настройки ПО по сценариям, описываемым в нотации YAML
API-бэкенд	Принимает команды от Фронтенда BPM на проведение операций над объектами инфраструктуры и элементами Базис.WorkPlace. Взаимодействует с API Базис.vControl |
ClickHouse	Колоночная/столбцовая ситема управления базами данных, предназначенная для онлайн обработки аналитических запросов
CPU; RAM; HDD (ресурсы)	Вычислительное ядро процессора хоста или ВМ; Оперативная память хоста или ВМ; Жесткий диск хоста или ВМ

Термин	Описание
High Availability, HA	Высокая доступность, характеристика технической системы, позволяющая снизить риски сбоев, а также минимизировать время плановых простоев
Isc-dhcp-server	Программа-сервер, обеспечивающая передачу клиентам сведений, необходимых для работы в сети TCP/IP, по запросам клиентов
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 протокола легковесного доступа к каталогам (LDAP)
NFS server	Сервер обслуживания сетевого протокола NFS, применяемого для разделения файловых ресурсов путём сетевого доступа к файловым системам
NTP server	Сервер обслуживания сетевого протокола NTP, применяемого для синхронизации внутренних часов компьютера с использованием сетей с переменной латентностью
nginx	Веб-сервер и почтовый прокси-сервер, работающий на Unix-подобных операционных системах
PKI (public key infrastructure)	Система кодирования (на основе шифров), обеспечивающая защищённость обмена данными в глобальных сетях (Интернет). Предоставляет каждой стороне обмена цифровые сертификаты, подтверждающие аутентичность (передающей стороны)

Термин	Описание
PostgreSQL	СУБД из списка поддерживаемых для Базис.vControl. Список поддерживаемых версий СУБД приведён в требованиях к программному и аппаратному обеспечению. Подробный список приведён в разделе приложения Поддерживаемые версии PostgreSQL
Python	Язык программирования
RADIUS	Сервер протокола AAA (Authentication, Authorization и Accounting), разработанный для передачи сведений между центральной платформой AAA и оборудованием Dial-Up доступа (NAS, Network Access Server) и системой биллинга
Redis	Сервис, обеспечивающий высокую доступность (HA) базы данных Redis
Samba	Сервер, предоставляющий доступ к хранилищу данных по протоколу CIFS
Syslog	Сервер регистрации входящих сообщений по протоколу Syslog
Sentry	Платформа для централизованного отслеживания и регистрации ошибок, используется в качестве хранилища возникших исключений в работе BPM
SNMP Agent	Агент стандартного протокола Интернета, предназначенного для управления устройствами в IP-сетях на основе архитектур UDP/TCP
SSO	Аутентификация пользователя в удаленном рабочем столе и использованием токена аутентификации Kerberos
uwsgi	Веб-сервер для запуска приложений по протоколу WSGI
VRRP	Virtual Router Redundancy Protocol — сетевой протокол, предназначенный для увеличения доступности маршрутизаторов, выполняющих роль шлюза по умолчанию

Термин	Описание
WebSocket	Протокол полнодуплексной связи поверх TCP-соединения, предназначенный для обмена сообщениями между браузером и веб-сервером в режиме реального времени
YAML	Формат сериализации данных, близкий к языкам разметки, но ориентированный на удобство ввода-вывода структур данных большинства языков программирования

1.3 Дополнительные ресурсы

Название документа	Краткое описание
Базис.WorkPlace. Руководство пользователя	Описание приложения Клиент Базис.WorkPlace, установка и принципы работы пользователя с приложением.
Базис.WorkPlace. Руководство администратора	Описание системы Базис.WorkPlace. Инструкции по работе и управлению удаленными рабочими столами.
Базис.WorkPlace. Руководство по установке	Инструкции по установке и настройке компонентов Базис.WorkPlace. Описание требований к инфраструктуре.
Базис.vControl. Руководство Администратора	Описание системы управления виртуализацией Базис.vControl. Инструкции по работе с системой.
Базис.vControl. Руководство по установке	Инструкции по установке и настройке компонентов Базис.WorkPlace. Описание требований к инфраструктуре.

1.4 Архитектурный состав компонентов

Представленная ниже таблица 1.4 содержит список архитектурных компонентов решения **Базис.WorkPlace**:

Таблица 1.4 Список архитектурных компонентов Базис.WorkPlace

Название компонента	Назначение и основные функции
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 инфраструктурой. Использует REST API Фронтенда Базис.vControl, взаимодействует с агентами, выполняет периодические задачи
Агент	Запускается на гостевых операционных системах (в виртуальных средах/машинах). Использует гостевые утилиты для получения информации местного значения (о гостевой системе)
Клиент	Реализация клиента доступа к BPM, запускаемого в рабочей среде пользователя (на УД). Статичные файлы отдаются nginx

2. ПОДГОТОВКА К УСТАНОВКЕ

Решение **Базис.WorkPlace** включает следующие основные компоненты (см. выше Архитектурный состав компонентов):

1. **Бэкенд Базис.WorkPlace** (может быть установлено несколько Бэкендов).
    1) **API Базис.WorkPlace** (для взаимодействия с Фронтендом).
    2) **Менеджер диспетчеров подключений**.
    3) **БД PostgreSQL**.
2. **Диспетчер подключений** (может быть установлено несколько).
3. **Агент Базис.WorkPlace** (встраивается в гостевые системы).
4. **Клиент Базис.WorkPlace** (обеспечивает работу пользователя на стороне устройства доступа).

2.1 Варианты установки

В данный момент для Базис.WorkPlace поддерживаются два режима установки:

- HA-режим (High Availability, высокая доступность);
- обычный, не-HA режим.

HA-режим отличается от обычного резервированием (дублированием) всех хостов, на которых развернуты компоненты решения.

2.2 Схема взаимодействия компонентов

Схема взаимодействия системы **Базис.WorkPlace** (включая **Базис.vControl**) показана на иллюстрации ниже (рисунок 2.1).

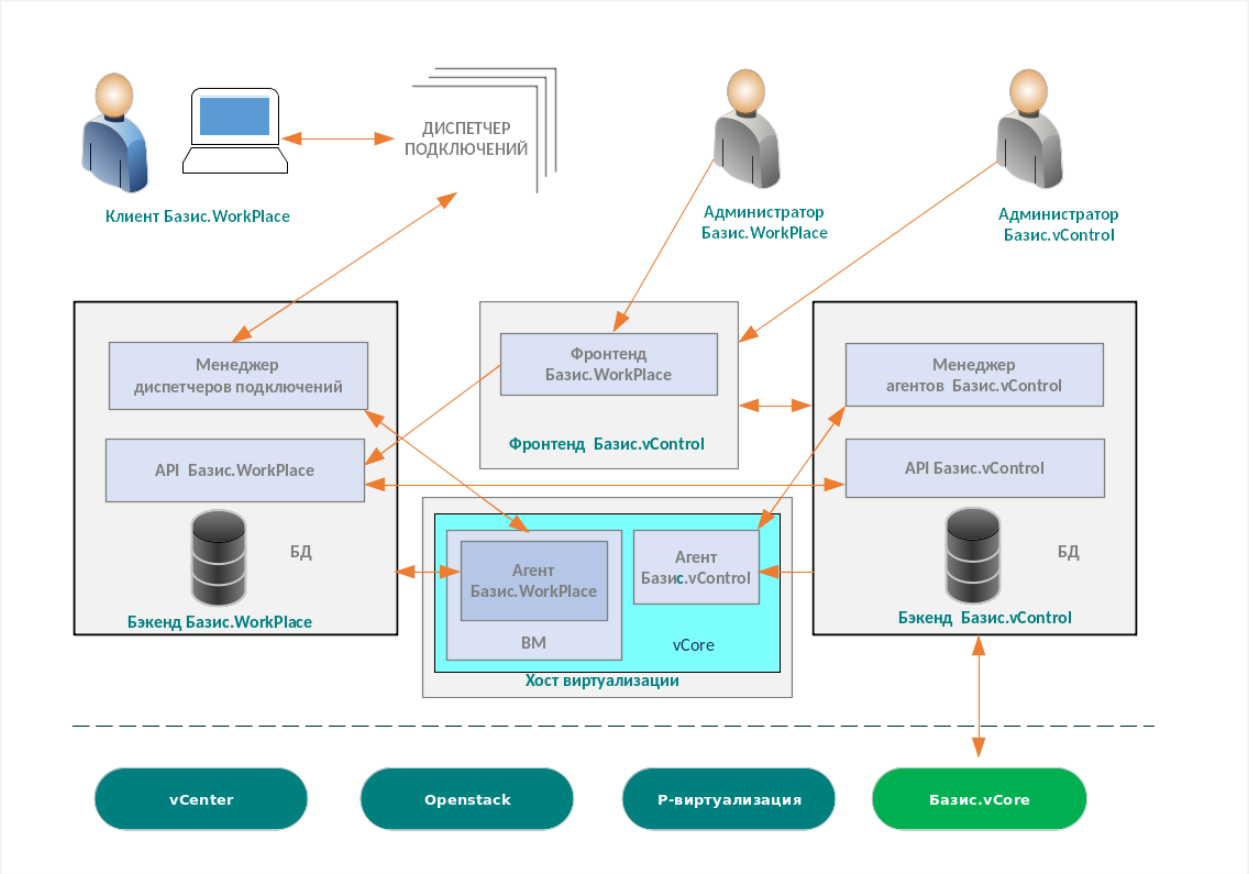

Рисунок 2.1 Взаимодействие Базис.Workplace и Базис.vControl

Примечание

Хост виртуализации (vCore) интегрируется с той и другой инфраструктурой. Поддерживаемые системы виртуализации показаны формализовано (ниже пунктирной линии).

2.3 Планирование системы

Решение **Базис.WorkPlace** предполагает установку следующих компонентов:

1. Виртуальная машина (ВМ) или отдельный физический сервер для одного **Диспетчера подключений** как минимум.

Если планируется использовать несколько **Диспетчеров подключений**, то необходимо установить одну ВМ или один отдельный сервер для каждого **Диспетчера подключений**.

2. ВМ или отдельный сервер для **Бэкенда BPM**.

   Самый простой сценарий работы подразумевает, что база данных (БД) и все компоненты **Бэкенда Базис.WorkPlace** располагаются на одном сервере.

3. Опционально возможно использование внешней базы данных, размещенной на другом сервере/ВМ.

   В таком случае может потребоваться отдельная ВМ или физический сервер для компонентов БД.

4. При установке в HA-режиме — отдельная ВМ или физический сервер для **Сервера развертывания**.

   Сервер развертывания – ресурс, из которого будет управляться процесс установки всех других компонентов.

5. При установке в HA-режиме — три или более отдельных ВМ или физических серверов для кластера Redis (в случае, когда они будут ставиться отдельно от **Бэкенда Базис.WorkPlace**).

   При этом не допускается использование того же Redis-кластера, который используется для **Базис. vControl**. Опционально, существует возможность поставить Redis-кластер на те же ВМ или сервера, что и **Бэкенды Базис.WorkPlace**.

Общая рекомендация: для компонентов **Бэкенда Базис.WorkPlace** и БД необходимо выделить физический сервер, не входящий в кластер, в котором будут находиться продуктивные ВМ рабочих столов. При этом работа этих компонентов в ВМ является типовым сценарием.

В зависимости от сценария использования могут понадобиться дополнительные сетевые сервисы, такие как DHCP-сервер, DNS-серверы, серверы Microsoft AD или LDAP или других поддерживаемых служб каталогов. Если используются внешние каталоги учетных записей, потребуются технические учетные записи для проведения аутентификации пользователей и добавления/удаления рабочих столов из домена.

При планировании физических и виртуальных сетей требуется учитывать, что минимальная сетевая связность должна быть обеспечена в соответствии со схемой взаимодействия компонентов (рисунок 2.1). Подробнее о требованиях к сетевой связности см. раздел Требования к сетевому взаимодействию

2.4 Подготовка инфраструктурного окружения

Под **инфраструктурным окружением** понимаются сервисы, обеспечивающие слаженное взаимодействие компонентов инфраструктуры Базис.vControl и Базис.WorkPlace, при поддержке таких служб как NTP, AD/LDAP.

1. На всех физических серверах с установленными средствами виртуализации и виртуальных серверах (ВМ, на которых развернуты компоненты инфраструктуры), серверах Postgres, хостах Redis, системные часы должны быть синхронизированы (обеспечение единого отсчёта времени).

   При развертывании системы возможно указать сервер NTP, с которого будет синхронизироваться время на всех серверах и управляющих виртуальных машинах.

2. В случае использования внешних каталогов учетных записей понадобится предварительно установленная и настроенная служба каталогов.

   Должна быть выделена учетная запись, которой доступны операции чтения/редактирования других учетных записей (смена пароля других учетных записей, просмотр свойств пользователей, добавление компьютера в домен, удаление компьютера из домена). Данная техническая учетная запись заполняется в коннекторе к службе каталогов, доступном из раздела *Безопасность* (вкладка *Службы каталогов* фронтенда **Базис.WorkPlace**, встроенного в интерфейс управления инфраструктурой).

Осторожно

Следует учесть, что выполнение некоторых операций может потребовать TLS-подключения к Microsoft Active Directory по отдельному порту. Например, при смене пароля в любом случае будет использоваться SSL-подключение независимо от того, как настроен коннектор подключения к LDAP/AD.

3. В сети с рабочими столами должен находиться DHCP-сервер, выдающий IP-адреса всем рабочим столам.

   Фактически, динамическое распределение IP-адресов в одном диапазоне (подсети) обеспечивает сетевое взаимодействие рабочих столов с Диспетчерами подключений.

2.4.1 Подготовка учетной записи в AD

Создайте в AD учетную запись ***vdi-svc*** (другие имена также допустимы) с правами Администратора Домена. Если по каким-либо причинам нет возможности использовать учетную запись администратора домена в коннекторе Microsoft Active Directory, то можно создать отдельную учетную запись и делегировать ей полномочия.

Примечание

Рекомендуется использовать учетную запись администратора домена, а не отдельную учетную запись с набором прав. Это позволит избежать проблем в назначении разрешений и работе функционала системы.

Подготовка учетной записи включает делегирование полномочий в домене на следующие операции:

- добавление компьютера в домен / удаление компьютера из домена;
- просмотр свойств пользователей.

Осторожно

По умолчанию смена пароля пользователя BPM производится от его же имени. Если для изменения пароля должна использоваться сервисная учетная запись, то у нее должны быть права на смену пароля пользователя, и в конфигурации **Бэкенда Базис.WorkPlace** для параметра ***use_admin_account_for_password_change*** должно быть выставлено значение ***True***. Подробнее параметры конфигурации **Бэкенда Базис.WorkPlace** описаны в разделе Описание параметров конфигурации для Бэкенда Базис.WorkPlace.

Для этого в оснастке *Active Directory Users and Computers* выберите домен и нажмите на него правой кнопкой мыши, а затем выберите пункт *Delegate Control* (рисунок 2.2).

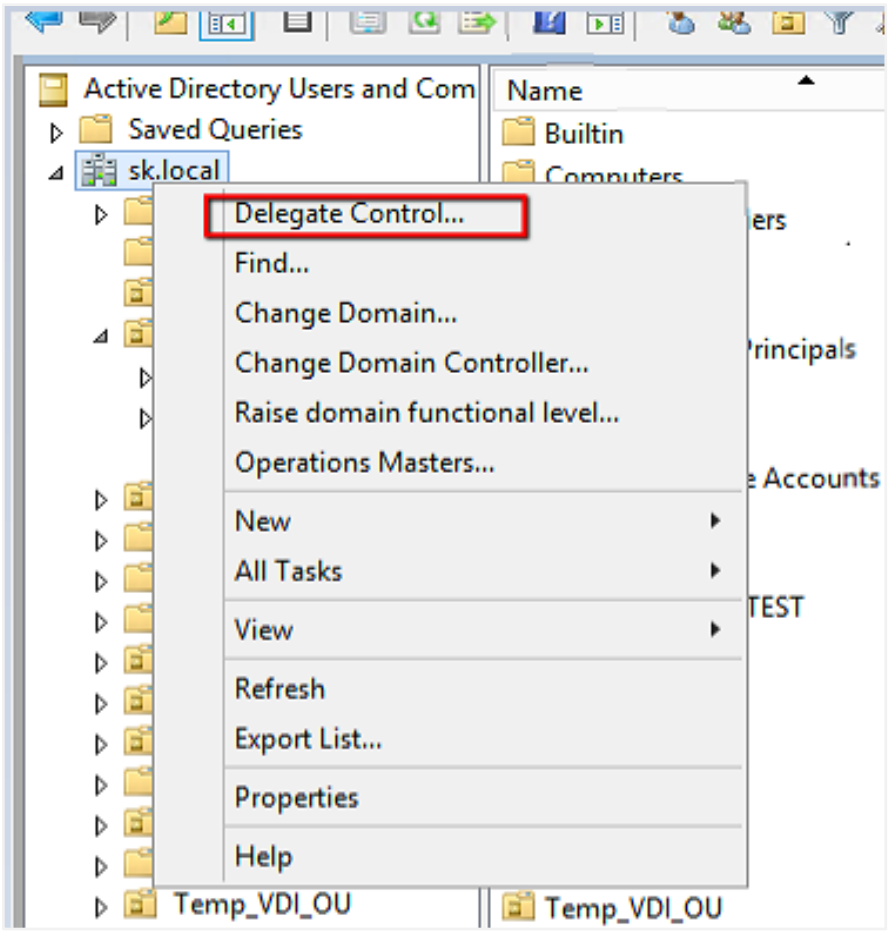

Рисунок 2.2 Делегирование полномочий в Microsoft Active Directory

Запустится мастер делегирования полномочий (Delegation of Control Wizard), в котором необходимо выбрать пользователя, который будет использоваться в качестве сервисной учетной записи для синхронизации с Microsoft Active Directory. На шаге делегирования полномочий выберите следующие общие задачи (Рисунок 2.3):

- Read all user information (прочитать всю информацию о пользователе);
- Join a computer to the domain (ввести компьютер в домен).

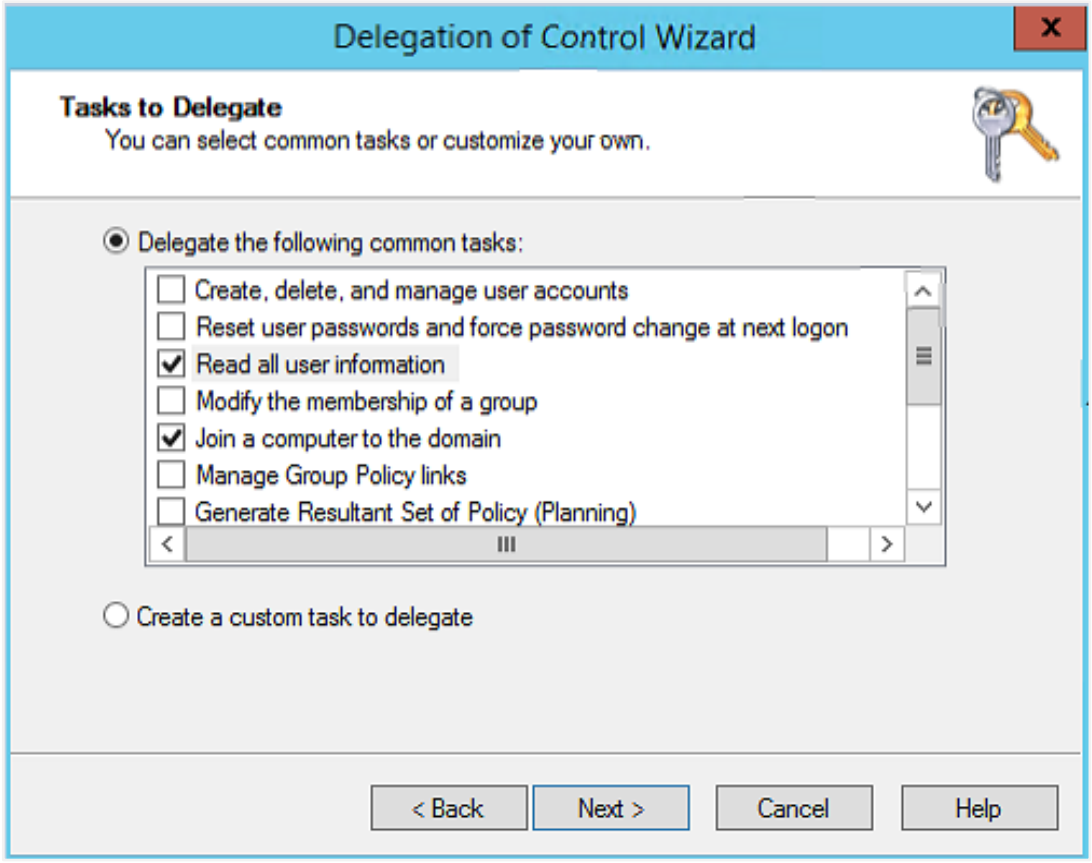

Рисунок 2.3 Выбор общих задач для делегирования полномочий

На последнем шаге проверьте установленные параметры и завершите работу мастера, нажав кнопку *Finish*.

Осторожно

Опцию ***Reset user passwords and force password change at next logon*** следует указывать в том случае, если сервисная учетная запись будет использована для смены паролей пользователей.

При этом следует учитывать, что если в Microsoft Active Directory используется политика паролей (GPO или FGPP), то **Бэкенд Базис.WorkPlace** будет делать попытку смены пароля от имени учетной записи пользователя в KDC через протокол Kerberos в следующих случаях:

- Истек срок действия пароля (учетная запись пользователя будет уже заблокирована);
- Администратор вручную выставил требование пользователю о смене пароля при следующем входе в систему.

Для работы функции смены пароля при интеграции с внешним каталогом LDAP на стороне Microsoft Active Directory должен быть настроен файл ***krb5.conf***. Подробнее о его настройке описано в разделе Инструкция по настройке смены пароля при использовании OpenLDAP.

После завершения операции перейдите в настройки прав в Microsoft Active Directory — Properties — и установите для выбранного пользователя дополнительные права (рисунок 2.4 — рисунок 2.9):

- Create Computer objects;
- Delete Computer objects;
- Reset password.

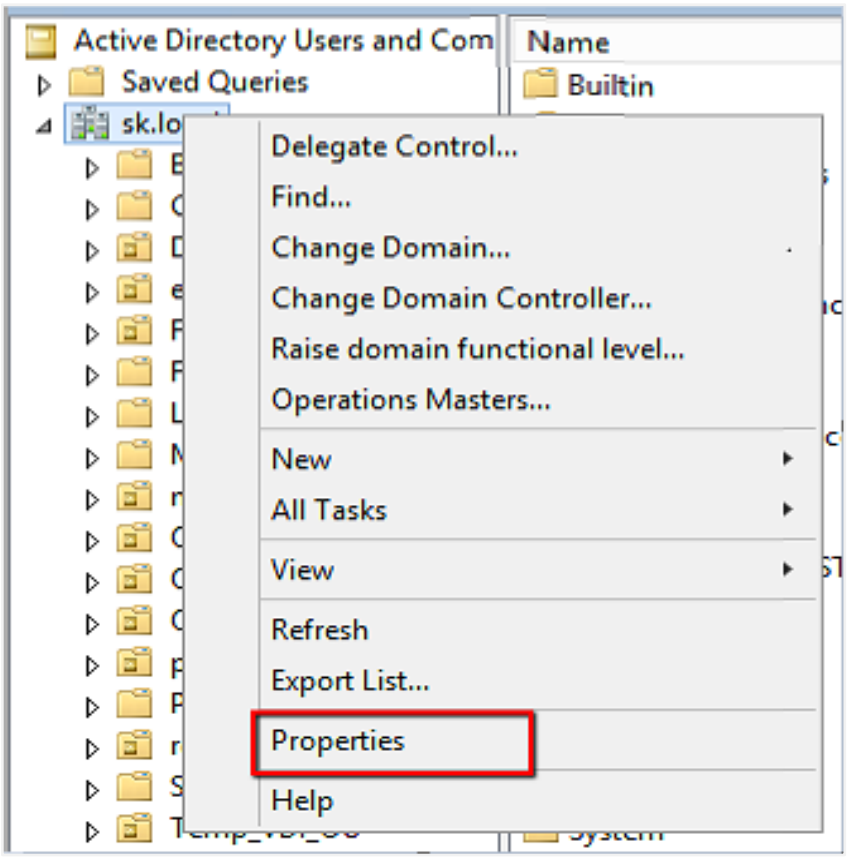

Рисунок 2.4 Настройки прав пользователя в Microsoft Active Directory. Шаг 1

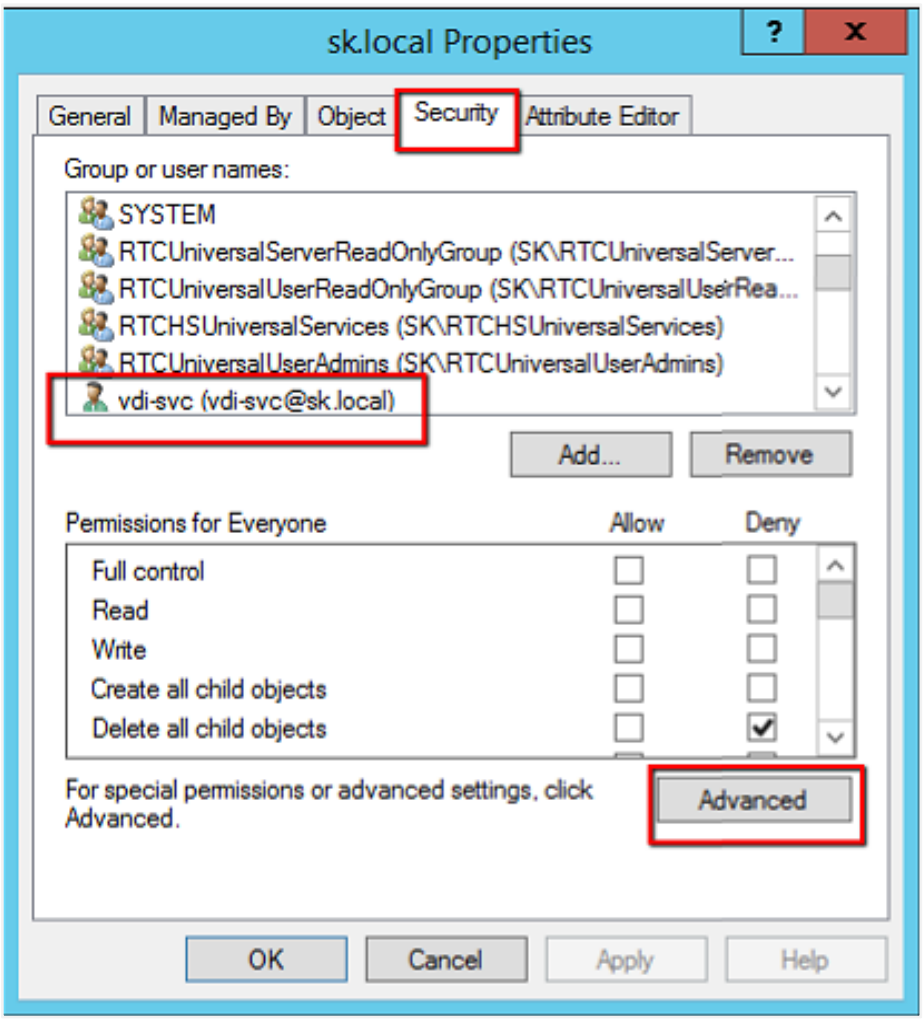

Рисунок 2.5 Настройки прав пользователя в Microsoft Active Directory. Шаг 2

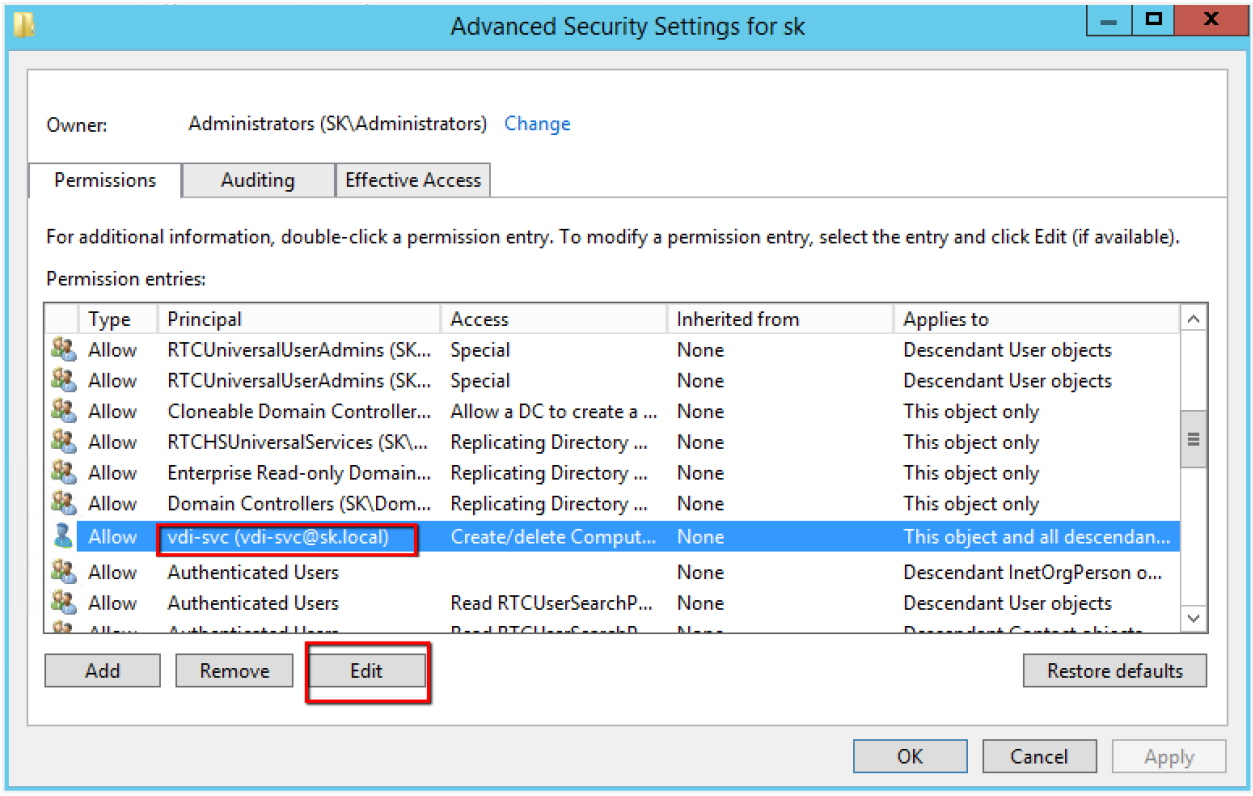

Рисунок 2.6 Настройки прав пользователя в Microsoft Active Directory. Шаг 3

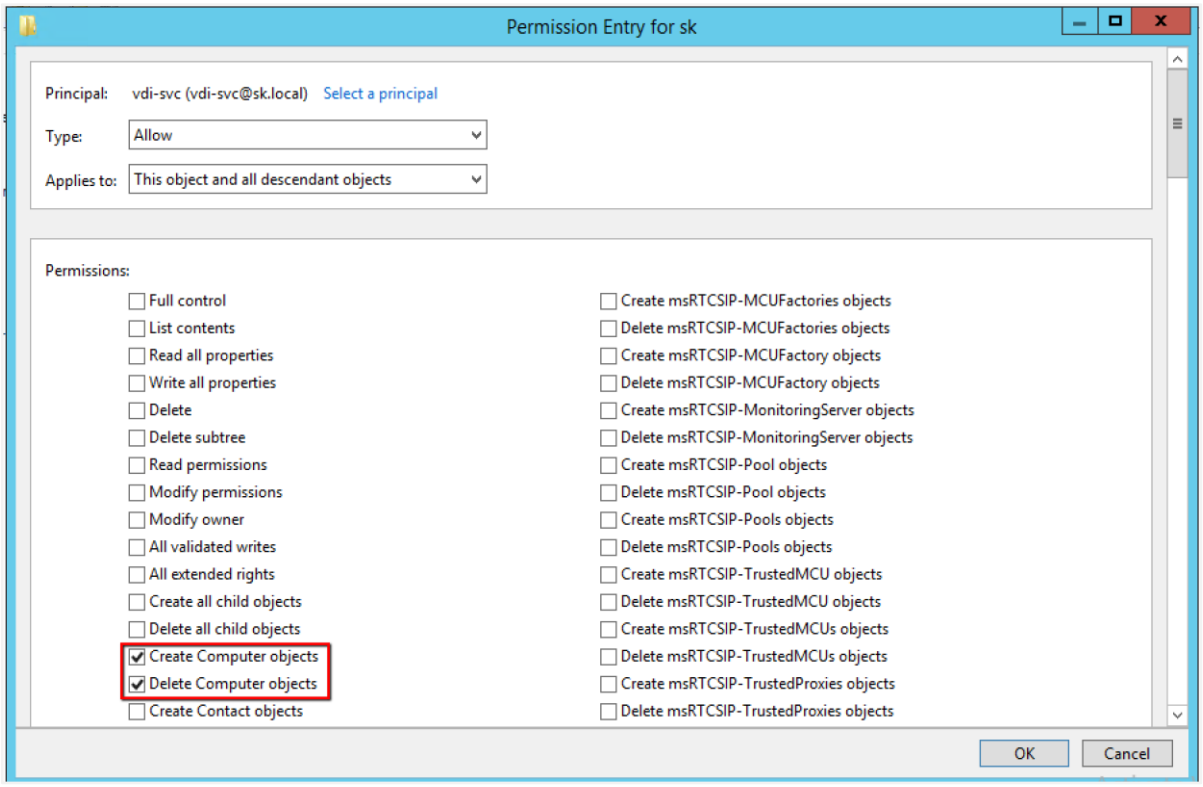

Рисунок 2.7 Настройки прав пользователя в Microsoft Active Directory. Шаг 4

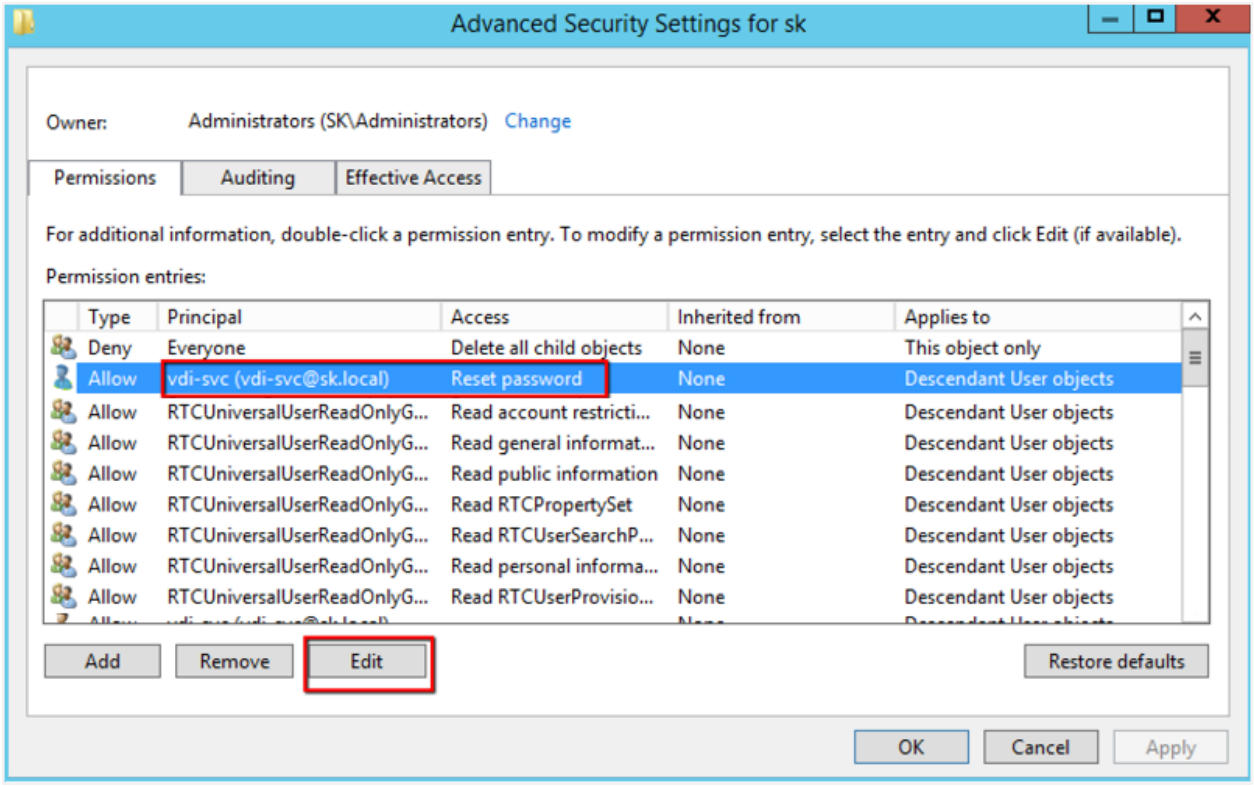

Рисунок 2.8 Настройки прав пользователя в Microsoft Active Directory. Шаг 5

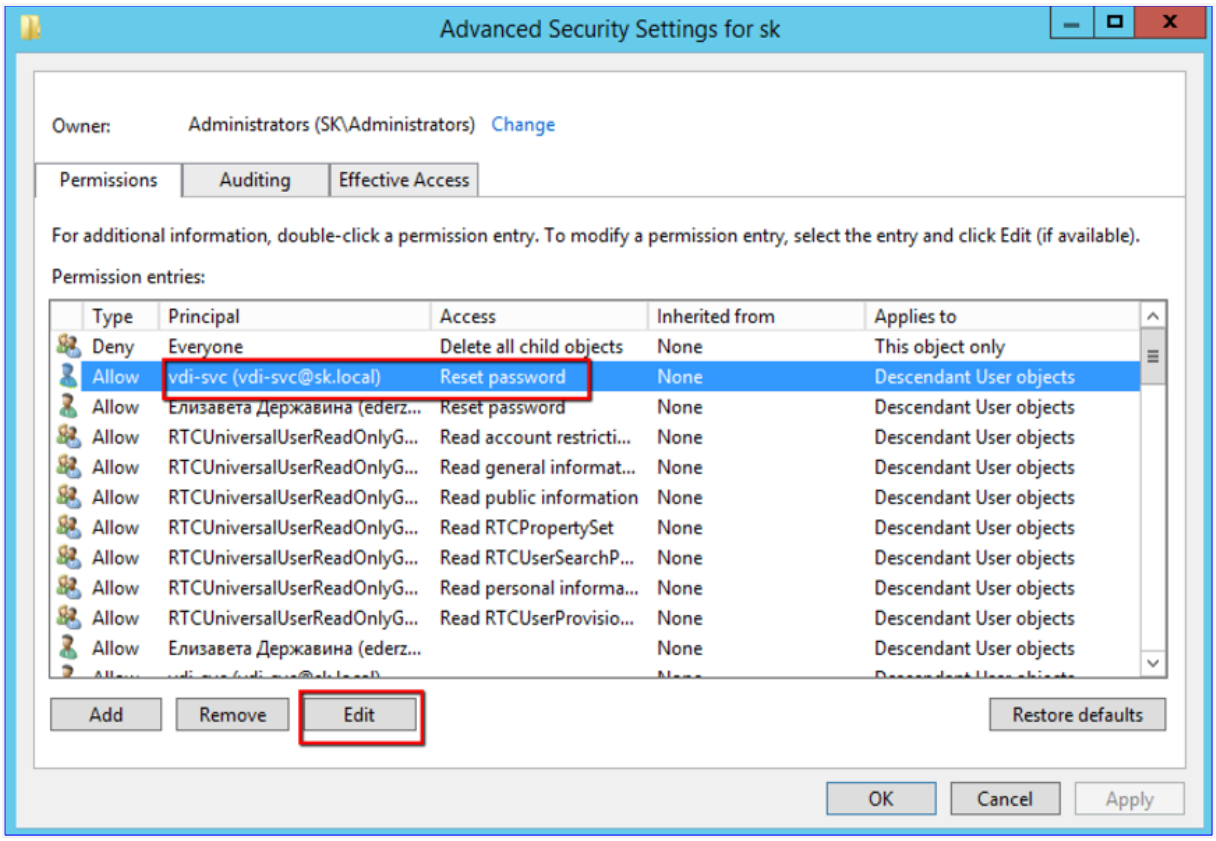

Рисунок 2.9 Настройки прав пользователя в Microsoft Active Directory. Шаг 6

Задав необходимые права, сохраните изменения и закройте оснастку управления Microsoft Active Directory. После сохранения всех прав созданного пользователя в системе **Базис.WorkPlace** можно использовать их в качестве учетной записи для коннектора Microsoft Active Directory.

2.4.2 Минимальные требования к аппаратному и программному обеспечению

В таблице 2.1 представлены поддерживаемые операционные системы для компонентов **Базис.WorkPlace** в зависимости от архитектуры процессора.

Таблица 2.1 Требования к операционным системам и архитектуре процессора

Архитектура процессора / Компонент	x86_64	Байкал-М	Эльбрус

Архитектура процессора / Компонент	x86_64	Байкал-М	Эльбрус
Диспетчер подключений	▪ Альт 8 СП ▪ Альт 9 ▪ Альт 10 ▪ Astra Linux 1.7	—	—
Бэкенд Базис.WorkPlace (Менеджер диспетчеров подключений), Сервер Redis, Сервер развертывания	▪ Альт 8 СП ▪ Альт 9 ▪ Альт 10 ▪ Astra Linux 1.7	—	—
Агент Базис.WorkPlace	▪ Альт 8 СП ▪ Альт 9 ▪ Альт 10 ▪ Astra Linux 1.7 ▪ РЕД ОС 7.3 ▪ Windows 7SP1-10 ▪ Windows Server 2012R2-2019	—	—
Клиент Базис.WorkPlace	▪ Альт 8 СП ▪ Альт 9 ▪ Альт 10 ▪ Astra Linux 1.7 ▪ РЕД ОС 7.3 ▪ Windows 7SP1-10 ▪ Windows Server 2012R2-2019 ▪ Kaspersky OS	Альт 9	Альт 9

Ниже перечислены остальные требования к аппаратному и программному обеспечению для компонентов **Базис.WorkPlace**.

- **Фронтенд Базис.WorkPlace**

Базис.WorkPlace не имеет своего фронтенда. Используется **Фронтенд Базис.vControl**. Дополнительных требований к **Фронтенду Базис.vControl** не предъявляется.

- **Бэкенд Базис.WorkPlace (Менеджер диспетчеров подключений)**

  - **Процессор**: 4 ядра (высокая частота является предпочтительной);
  - **Оперативная память**: 8 Гбайт;
  - **Дисковое пространство**: 60 Гбайт и более (включая ресурсы для БД).

- **Диспетчер подключений**

  - **Процессор**: 2 ядра (высокая частота является предпочтительной);
  - **Оперативная память**: 4 Гбайт;
  - **Дисковое пространство**: 60 Гбайт;
  - **Сетевое подключение**: в зависимости от планируемой нагрузки, но рекомендуется от 1 Гбит/с.

- **Сервер Redis** (используется при HA-развертывании)

  - **Процессор**: 1 ядро (высокая частота является предпочтительной);
  - **Оперативная память**: 1 Гбайт;
  - **Дисковое пространство**: 60 Гбайт.

- **Сервер развертывания** (используется при HA-развертывании)

  - **Процессор**: 1 ядро (высокая частота является предпочтительной);
  - **Оперативная память**: 1 Гбайт;
  - **Дисковое пространство**: 60 Гбайт.

- **Агент Базис.WorkPlace**

  Работа **Агента Базис.WorkPlace** подразумевает незначительные дополнительные требования к ресурсам операционной системы, которыми можно пренебречь (около 100 Мбайт памяти, около 100 Мбайт дискового пространства).

- **Клиент Базис.WorkPlace**

  Работа **Клиента Базис.WorkPlace** подразумевает незначительные дополнительные требования к ресурсам операционной системы, которыми можно пренебречь (около 100 Мбайт памяти, около 100 Мбайт дискового пространства).

  - **Приложение протокола доставки рабочего стола**:

    – VNC — TigerVNC;
    – RDP — Microsoft RDP версии 8.0 и выше;
    – RX — RX@Etersoft.

  - **Сервер протокола доставки рабочего стола**:

- RDP — Microsoft RDP версии 8.0 и выше;
- VNC — TurboVNC;
- RX — RX@Etersoft.

2.4.3 Требования к сетевому взаимодействию

2.4.3.1 Общие требования

Необходимо обеспечить L3-связность:

- Между системой, где будет установлена **Базис.WorkPlace** и **Базис.vControl**.
- Между системой, где будет установлена **Базис.WorkPlace** и хостами с Redis (в случае HA-установки).
- Между **Менеджером диспетчеров подключений Базис.WorkPlace** и **Диспетчером подключений Базис.WorkPlace**.
- Между **Диспетчером подключений Базис.WorkPlace** и виртуальными машинами, которые будут выступать в роли рабочих столов BPM.
- Между **Менеджером диспетчеров подключений Базис.WorkPlace** и виртуальными машинами, которые будут выступать в роли рабочих столов BPM.
- Между системой, которая будет выступать в роли **Сервера развертывания**, и:
  - системой, где будет установлено решение **Базис.WorkPlace**;
  - хостами, где будут установлены **Диспетчеры подключений**;
  - хостами с Redis.

> **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.

2.4.3.2 Базис.WorkPlace и Базис.vControl

Между серверами, где будут установлены решения **Базис.WorkPlace** и **Базис.vControl**, должна быть L3-связность. **Фронтенд Базис.vControl** обращается в API **Базис.WorkPlace** через TCP-порт 80. **Бэкенд Базис.WorkPlace** также обращается в API **Базис.vControl** через TCP-порт 443.

2.4.3.3 Диспетчеры подключений

Диспетчеры подключений должны находиться в единой сети (или иметь L3-связанность) со следующими компонентами:

1. **Бэкенд Базис.WorkPlace**.

2. **Клиенты Базис.WorkPlace**.
3. **Агенты Базис.WorkPlace**.

Сети могут быть разделены как физически (в этом случае **Диспетчеры подключений** будут иметь три разных сконфигурированных сетевых адаптера, адреса которых необходимо указать при развертывании: ***broker_in_ip_for_client, broker_out_ip_to_backend, broker_out_ip_to_vm***), так и иметь один интерфейс в единой L3-сети.

Разделение на сети для **Диспетчера подключений** происходит через параметры:

- ***broker_in_ip_for_client*** в файле установки ***broker-hosts*** — IP-адрес в сети, через которую к **Диспетчеру подключений** будут подключаться **Клиенты Базис.WorkPlace**;
- ***broker_out_ip_to_backend*** в файле установки ***broker-hosts*** — IP-адрес в сети, через которую **Диспетчер подключений** связывается с **Менеджером диспетчеров подключений**;
- ***broker_out_ip_to_vm*** в файле установки ***broker-hosts*** — IP-адрес в сети, через которую **Диспетчер подключений** связывается с ВМ, которые обеспечивают виртуальные рабочие столы.

2.4.3.4 Бэкенд Базис.WorkPlace (Менеджер диспетчеров подключений)

- **Бэкенды Базис.WorkPlace** должны иметь связность с:
  - серверами БД;
  - серверами Redis;
  - серверами других **Бэкендов**, в случае работы в режиме высокой доступности (HA);
  - серверами **Диспетчеров подключений**;
  - виртуальными машинами (**Агентами Базис.WorkPlace**).
- Со всех **Бэкендов Базис.WorkPlace** должен быть доступ на TCP/9000:
  - на все **Бэкенды Базис.vControl** / VIP адрес **Базис.vControl** в случае установки ClickHouse на те же хосты, что и **Бэкенды Базис.vControl**, или в случае установки **Базис.vControl** в конфигурации без отказоустойчивости;
  - на все хосты, куда поставлен ClickHouse, в случае установки ClickHouse на отдельные от **Бэкенда Базис.vControl** системы.

2.4.3.5 Сервер развертывания

Сервер развертывания должен иметь возможность подключиться ко всем серверам, участвующим в инфраструктуре HA.

2.4.4 Требования к информационной безопасности

В таблице 2.2 представлено описание, используемое для настройки межсетевого экрана инфраструктуры **Базис.WorkPlace**.

Таблица 2.2 Описание сетевых взаимодействий компонентов Базис.WorkPlace

Источник (машина)	Служба/приложение источника	Назначение (машина)	Служба/приложение источника	Протокол	Порт	Использование
Deploy_WorkPlace	Ansible	WorkPlace Бэкенд	SSHd	TCP	22	Автоматизированная установка программных пакетов
Deploy_WorkPlace	Ansible	WorkPlace ДП	SSHd	TCP	22	Автоматизированная установка программных пакетов
WorkPlace Бэкенд	aptyumdnf	Deploy_WorkPlace	nginx	TCP	8888	Доступ к репозиторию с пакетами для установки
WorkPlace Бэкенд		NTP server		UDP	123	Синхронизация времени
WorkPlace Бэкенд	nginx	WorkPlace Бэкенд	WebSocket	TCP	8081	Взаимодействие с API
WorkPlace Бэкенд	nginx	WorkPlace Бэкенд	uwsgi	TCP	9080	Взаимодействие с API
WorkPlace Бэкенд	WebSocket	WorkPlace Бэкенд*	Redis	TCP	6379	Доступ к Redis для извлечения/вставки данных, репликации

Источник (машина)	Служба/приложение источника	Назначение (машина)	Служба/приложение источника	Протокол	Порт	Использование
WorkPlace Бэкенд	WebSocket	WorkPlace Бэкенд*	Redis-sentinel	TCP	5000	Получение информации о Redis мастере, обеспечения HA для Redis
WorkPlace Бэкенд	WebSocket	SysLog	Syslog	UDP	514	Запись логов
WorkPlace Бэкенд	uwsgi	WorkPlace Бэкенд	BrokerManager	TCP	7501(+)	Связь Бэкендов между собой в HA режиме (инкремент на каждый дополнительный BrokerManager)
WorkPlace Бэкенд	uwsgi	WorkPlace Бэкенд*	PostgreSQL	TCP	5432	Доступ к БД PostgreSQL
WorkPlace Бэкенд	uwsgi	SysLog	Syslog	UDP	514	Запись логов
WorkPlace Бэкенд	BrokerManager	LDAP-Server		TCP,UDP	636	Взаимодействие с доменными УЗ
WorkPlace Бэкенд	BrokerManager	Kerberos		TCP,UDP	88(TCP), 464(TCP), 464(UDP)	Проверка подлинности УЗ клиента

Источник (машина)	Служба/приложение источника	Назначение (машина)	Служба/приложение источника	Протокол	Порт	Использование
WorkPlace Бэкенд	BrokerManager	PKI		TCP,UDP	80,389	Для взаимодействия с PKI инфраструктурой (нач. с версии 2.2)
WorkPlace Бэкенд	BrokerManager	RADIUS		UDP	1812,1813, 1645,1646	Для обеспечния 2хфакторной авторизации
WorkPlace Бэкенд	uwsgi	WorkPlace Бэкенд	SNMP Agent	UDP	161,162	Для обеспечения HA и получения статусов Бэкендов Workplace
WorkPlace Бэкенд	BrokerManager	WorkPlace Бэкенд*	PostgreSQL	TCP	5432	Доступ к БД PostgreSQL
WorkPlace Бэкенд	BrokerManager	vControl Бэкенд	nginx	TCP	8081	Для взаимодействия WorkPlace и vControl
WorkPlace Бэкенд	BrokerManager	SysLog	Syslog	UDP	514	Запись логов
WorkPlace ДП	Брокер	Deploy_WorkPlace	nginx	TCP	8888	Доступ к репозиторию с пакетами установки

Источник (машина)	Служба/приложение источника	Назначение (машина)	Служба/приложение источника	Протокол	Порт	Использование
WorkPlace ДП	Брокер	WorkPlace Бэкенд	BrokerManager	TCP	6501(+)	Для взаимодействия между Брокер и BrokerManager (инкремент на каждый дополнительный BrokerManager)
WorkPlace ДП	Брокер	Виртуальная машина		TCP	44495, 3389, 22	Доп. канал до рабочего стола (для проброса устройств) 3389/RDP, 22/RX
WorkPlace Клиент	Клиент Basis.Workplace	WorkPlace ДП	nginx	TCP	443	HTTPS-доступ для скачивания клиента
WorkPlace Клиент	Клиент Basis.Workplace	WorkPlace ДП	Брокер	TCP	9999	Проксирование протоколов доставки рабочих столов
WorkPlace Клиент	Клиент Basis.Workplace	WorkPlace ДП	Брокер	TCP	9989	Авторизация и получение списка рабочих столов

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

Примечание

Исходящие подключения между всеми элементами инфраструктуры происходят по случайным портам; блокирование каких-либо исходящих портов нежелательно.

Для развертывания серверных компонентов решения **Базис.WorkPlace** требуется доступ по TCP/22 (SSH-подключение для выполнения скриптов развертывания) ко всем серверам инфраструктуры, с сервера **Бэкенда Базис.WorkPlace** или с **Сервера развертывания** (при отказоустойчивом варианте решения).

2.4.4.1 Системные учетные записи для работы компонентов продукта

Бэкенд Базис.WorkPlace и **Диспетчер подключений** работают в системе под выделенной учетной записью с правами обычного пользователя и без возможности для локального/SSH-входа в систему. Все действия, которые требуют повышения привилегий, исполняются с использованием ***sudo (su)***. Учетные записи и права для этих компонентов создаются автоматически при развертывании системы и не требуют дополнительных настроек.

Для взаимодействия **Бэкенда Базис.WorkPlace** и **Бэкенда Базис.vControl** используется сервисная учетная запись **Базис.vControl**. Ее потребуется создать и указать в конфигурационном файле при развертывания решения Базис.WorkPlace.

2.4.5 Поддерживаемые токены и смарт-карты

Для сценария аутентификации решение **Базис.WorkPlace** поддерживает работу следующих токенов и смарт-карт:

1. ESMART Token ГОСТ;
2. Рутокен ЭЦП 2.0;
3. eToken;
4. JaCarta.

3. УСТАНОВКА БАЗИС.WORKPLACE

3.1 Варианты установки

В данный момент для Базис.WorkPlace поддерживаются два режима установки:

- HA-режим (High Availability, высокая доступность).
- Обычный, не-HA режим.

HA-режим отличается от обычного резервированием (дублированием) всех хостов, на которых развернуты компоненты решения.

3.2 Подготовка серверов для установки компонентов Базис.WorkPlace

Все компоненты **Базис.WorkPlace** 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.

Каждый компонент может быть развернут как на виртуальном сервере (под управлением системы виртуализации), так и на физическом сервере. Данное руководство предполагает, что развертывание производится только на виртуальных машинах.

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

3.2.1 Подготовка шаблона виртуальной машины для установки компонентов Базис.WorkPlace

1. Подключитесь по SSH к мастер-ноде под пользователем root. На Windows для этого можно использовать SSH-клиент PuTTY.

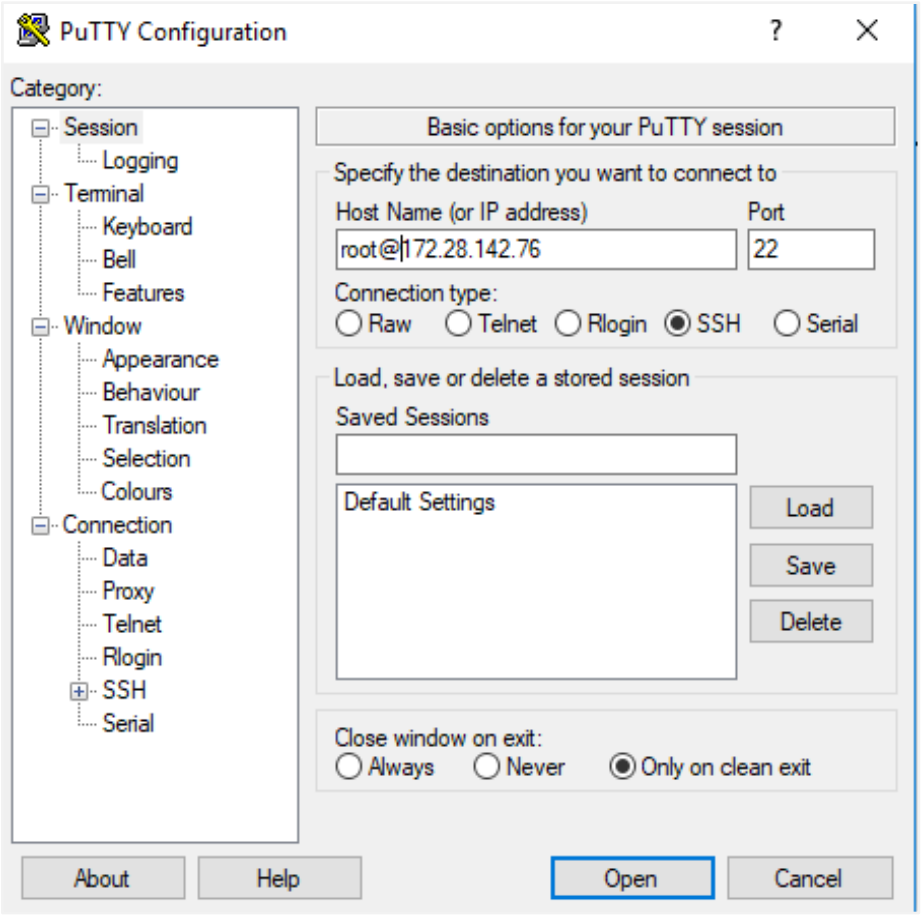

Рисунок 3.1 Подключение по SSH в PuTTY

2. Создайте виртуальную машину средствами виртуализации. Данная ВМ будет конвертирована в шаблон, из которого будут созданы ВМ для других компонентов Базис.WorkPlace.
3. Для консольного доступа установите и настройте VNC на созданной ВМ (убедитесь, что ВМ в этот момент остановлена). Установка производится в режиме auto, после ее завершения система сообщит назначенный TCP-порт для доступа по VNC к данной ВМ (и всех дальнейших ВМ, созданных по ее шаблону).
4. С помощью scp скопируйте образ операционной системы, которую нужно будет установить на ВМ, в общую папку, доступную с ВМ. В нашем случае образы хранятся в ***\\10.0.30.4\v1***, а целевая общая папка — ***/vstorage/stor1/vmprivate/***.

   На Windows для этого можно воспользоваться утилитой WinScp, подключившись к мастер-ноде.

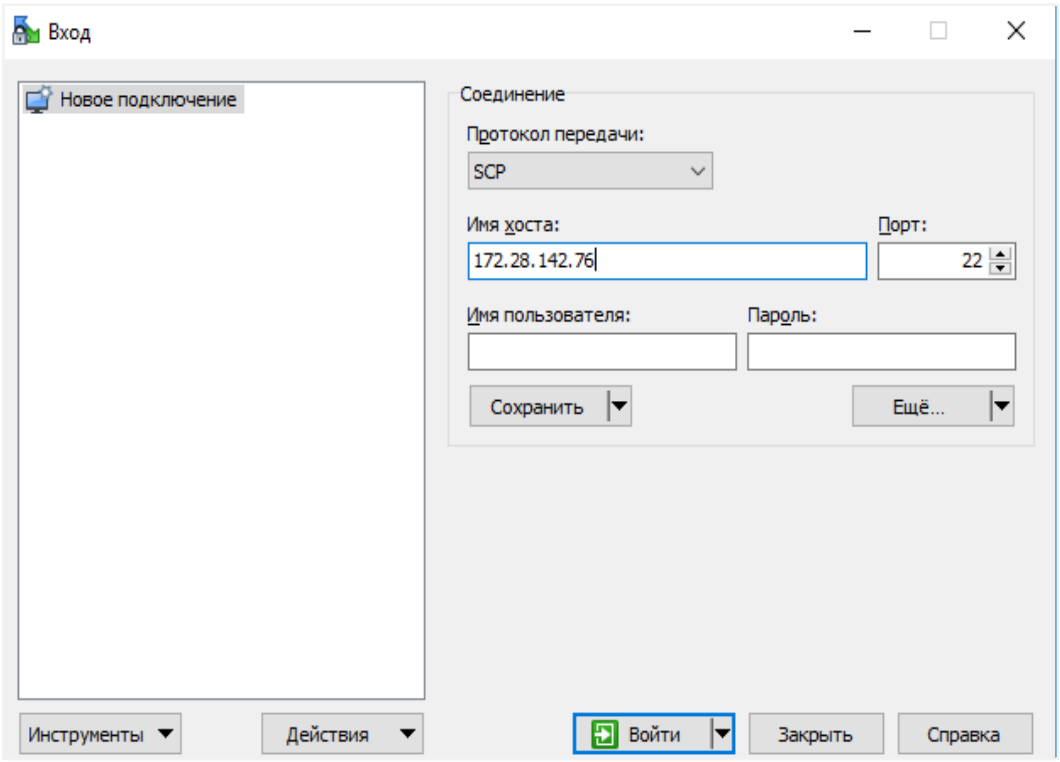

Рисунок 3.2 Окно утилиты WinScp

Далее будут приведены примеры установки ОС Альт и Astra Linux.

5. Примонтируйте скопированный образ (ISO-файл) к виртуальному дисководу CD-ROM созданной ВМ. Для этого выполните в консоли мастер-ноды следующую команду (ВМ должна быть предварительно остановлена).

3.2.2 Инсталляция ОС Альт

Примечание

Ниже рассмотрены действия по установке ALT Linux Server P10 (10.1). Используйте официальный Интернет-репозиторий в качестве источника программных пакетов, скачиваемых перед инсталляцией.

Установка ОС Альт 9 выполняется аналогично; используйте официальные репозитории (рекомендованные поставщиком ОС). Дополнительная информация:

https://www.altlinux.org/Репозитории_ALT_Linux https://www.basealt.ru/repository

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

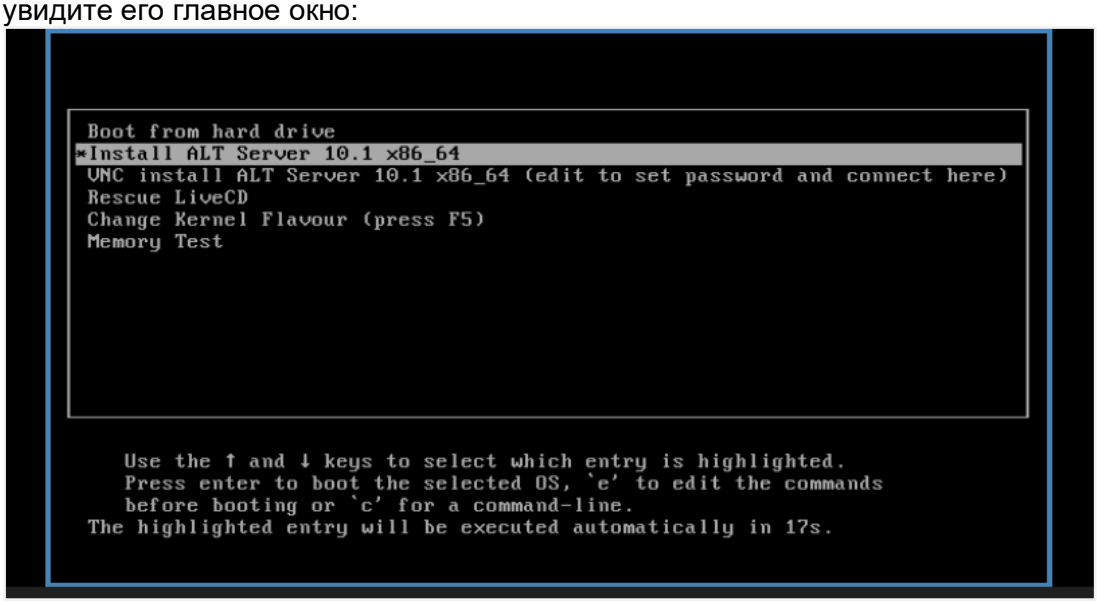

Рисунок 3.3 Главное окно инсталлятора ОС Альт

2. Оставьте языковые настройки по умолчанию.

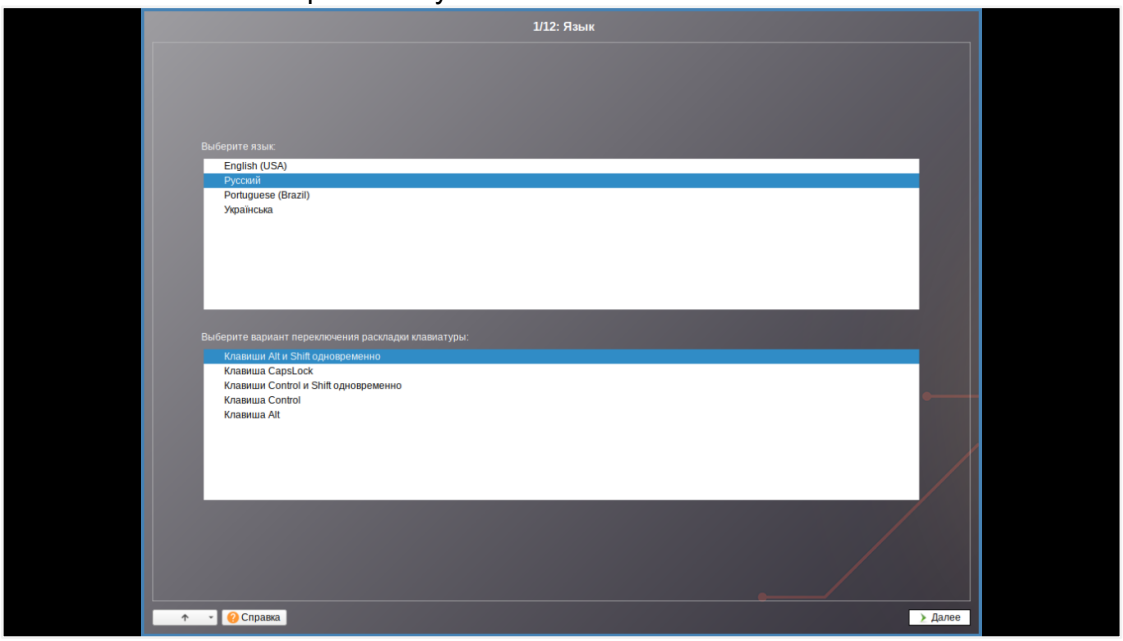

Рисунок 3.4 Выбор языковых настроек ОС Альт

3. Примите лицензионное соглашение.

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

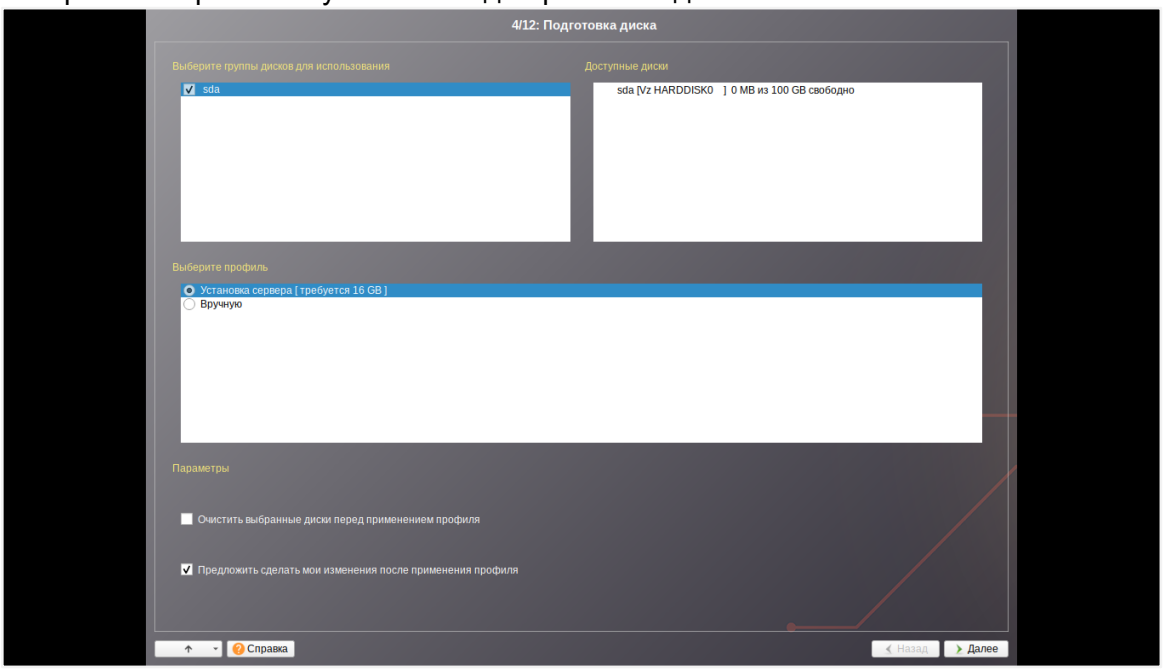

Рисунок 3.5 Этап подготовки диска

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

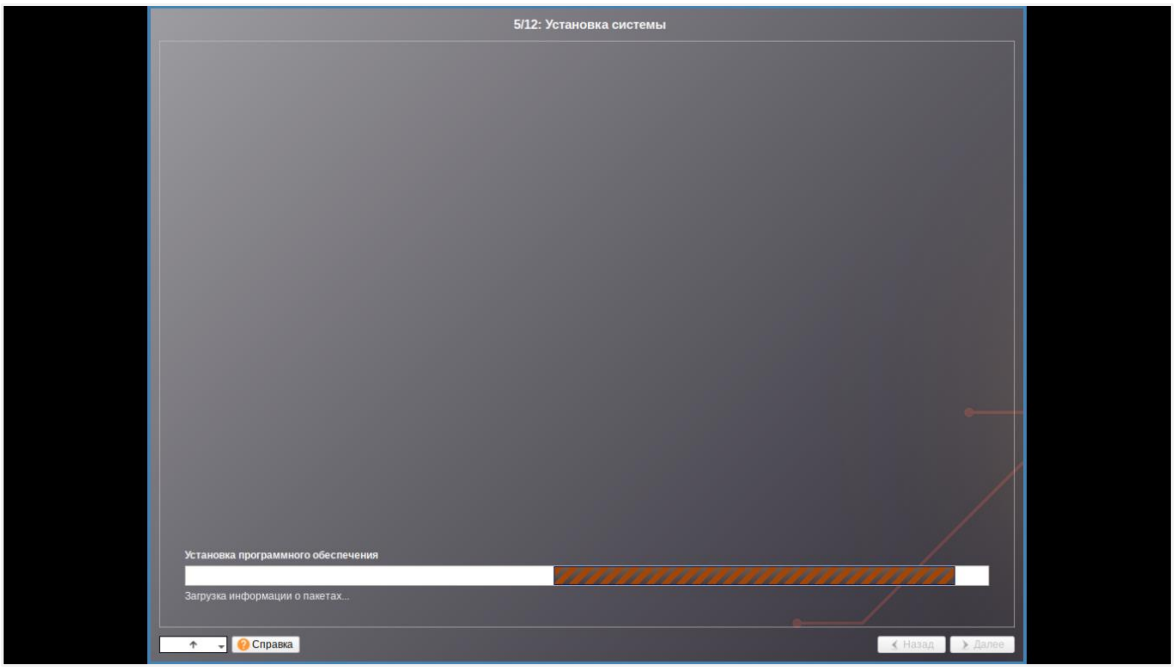

Рисунок 3.6 Установка ОС Альт

8. Оставьте настройки по умолчанию для загрузчика.

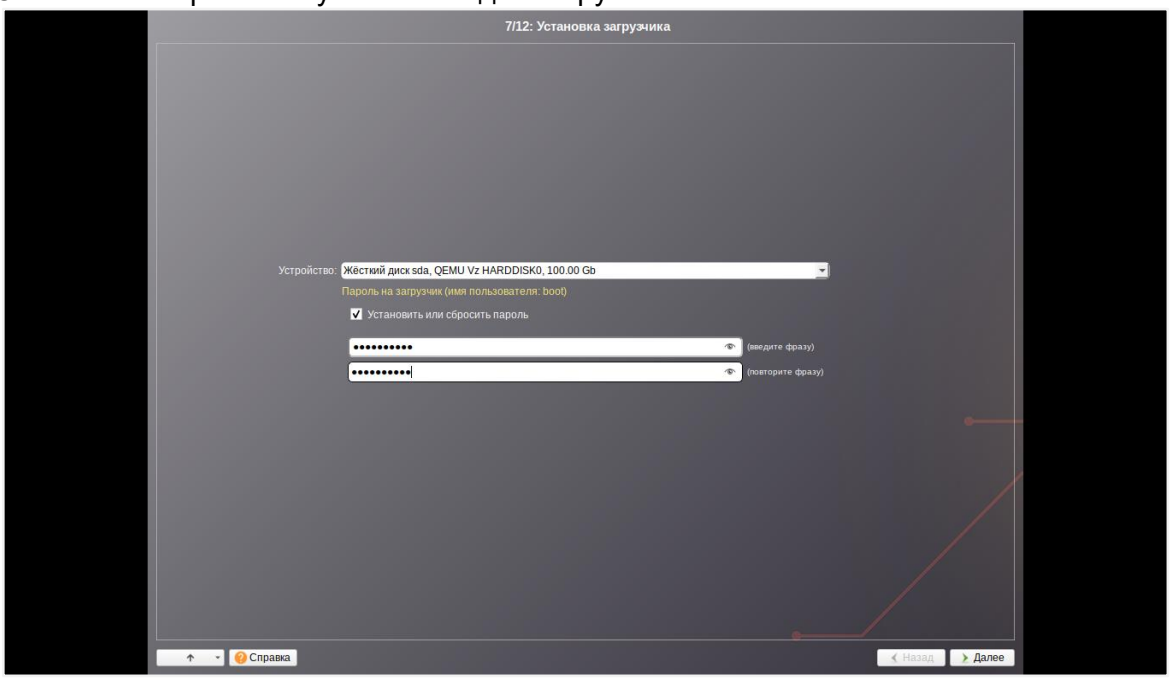

Рисунок 3.7 Настройки для загрузчика

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**.

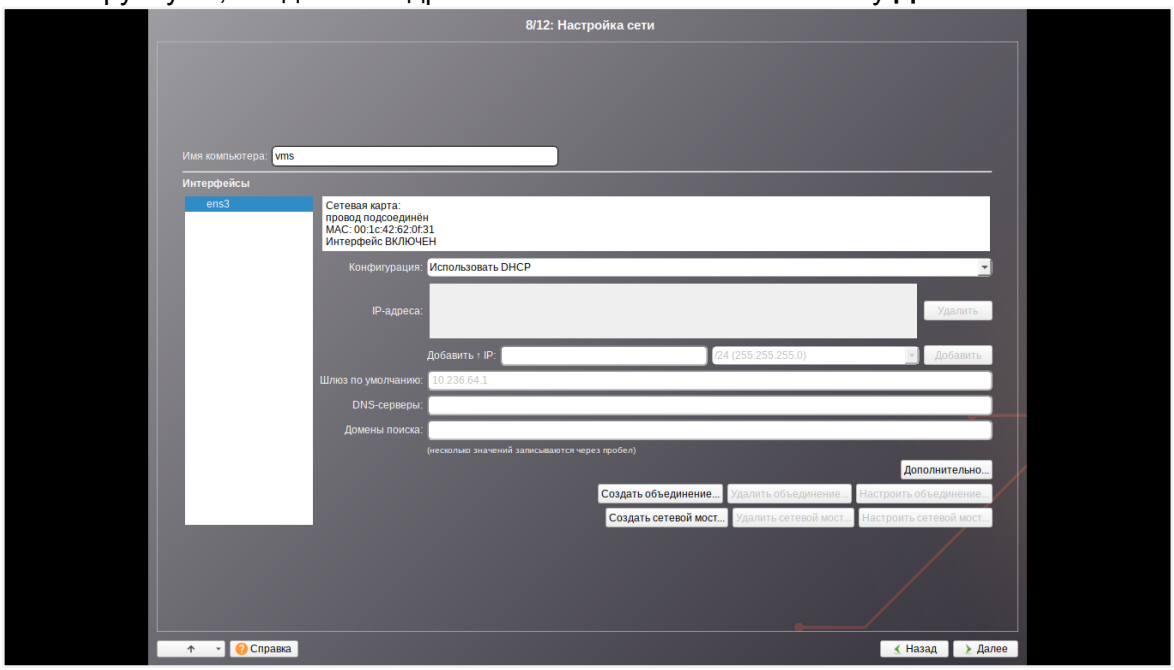

Рисунок 3.8 Настройки сети

10. Задайте пароль для системного администратора.

Рисунок 3.9 Настройка пароля для администратора

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

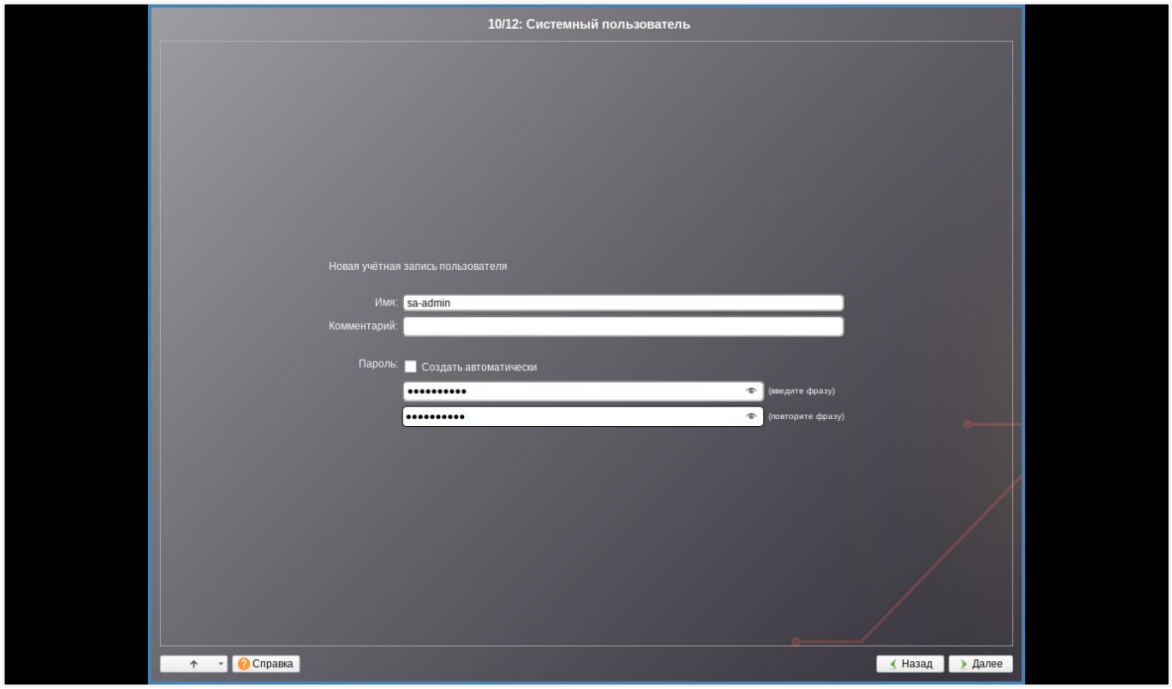

Рисунок 3.10 Настройка системного пользователя

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 ВМ для полного отключения IPv6.

13. Включите доступ по SSH к ВМ. Для этого отредактируйте следующий параметр в ***/etc/openssh/sshd_config*** на ВМ:

```
PermitRootLogin yes
```

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

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

Осторожно

При использовании Альт 8 СП обязательно установите доступные обновления пакетов.

3.2.3 Инсталляция Astra Linux

Инсталляция Astra Linux выполняется согласно инструкции, доступной на официальном справочном портале (wiki.astralinux.ru).

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 блокирован консольный вход в систему для пользователя и запуск консоли из графического интерфейса сессии пользователя.
- **Включить блокировку интерпретаторов** — при выборе данного пункта будет блокировано 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.

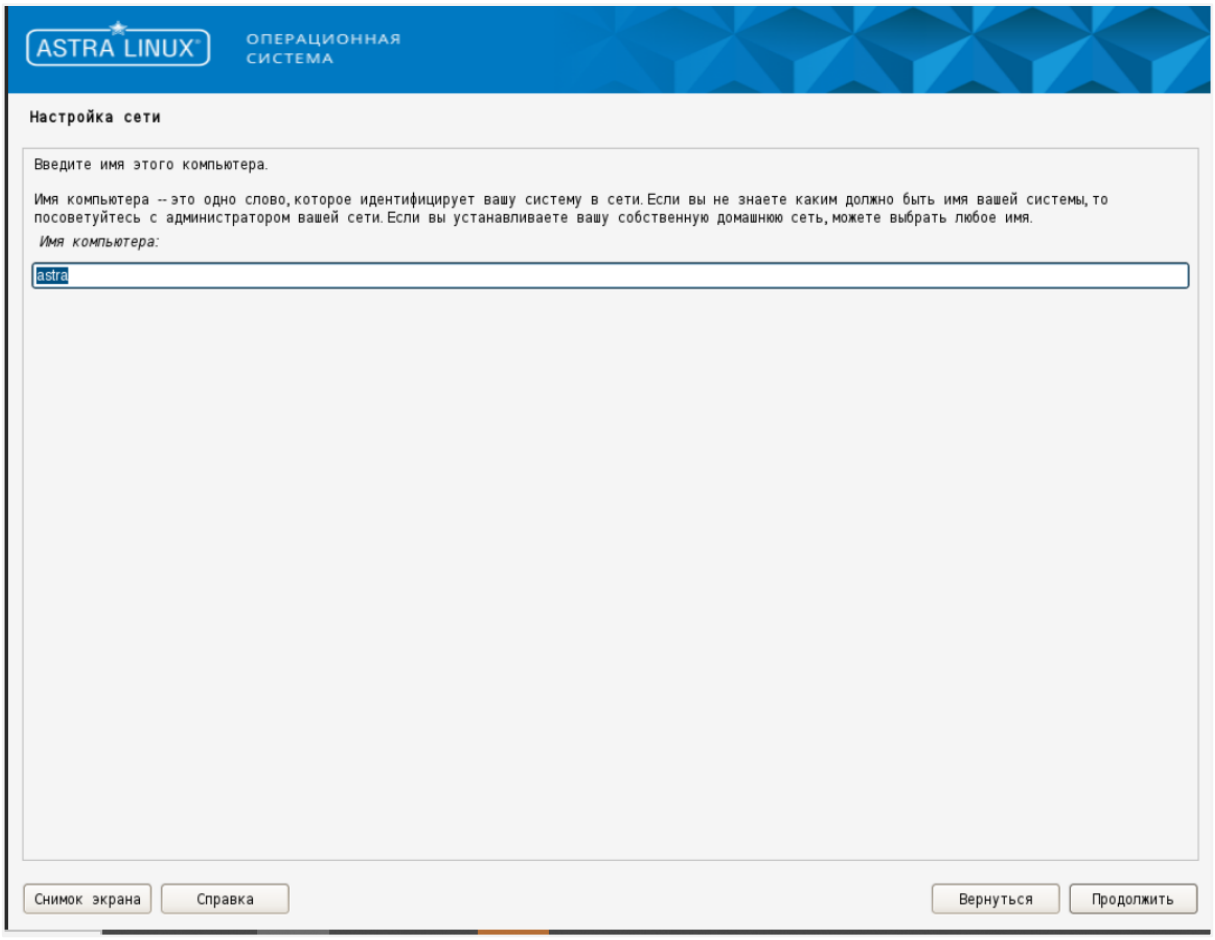

Рисунок 3.11 Настройка имени компьютера

4. Задайте имя учетной записи администратора и укажите пароль.

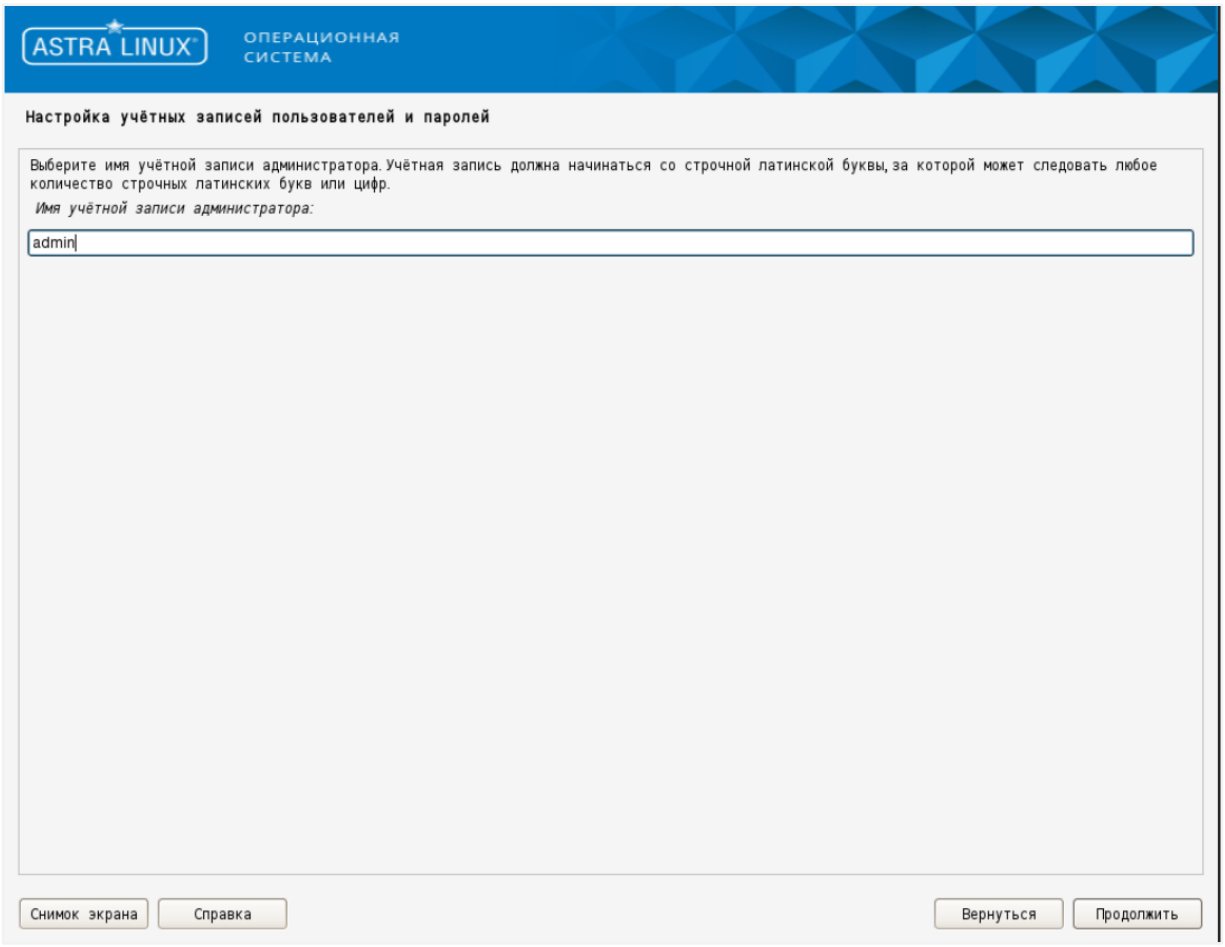

Рисунок 3.12 Настройка имени учетной записи администратора

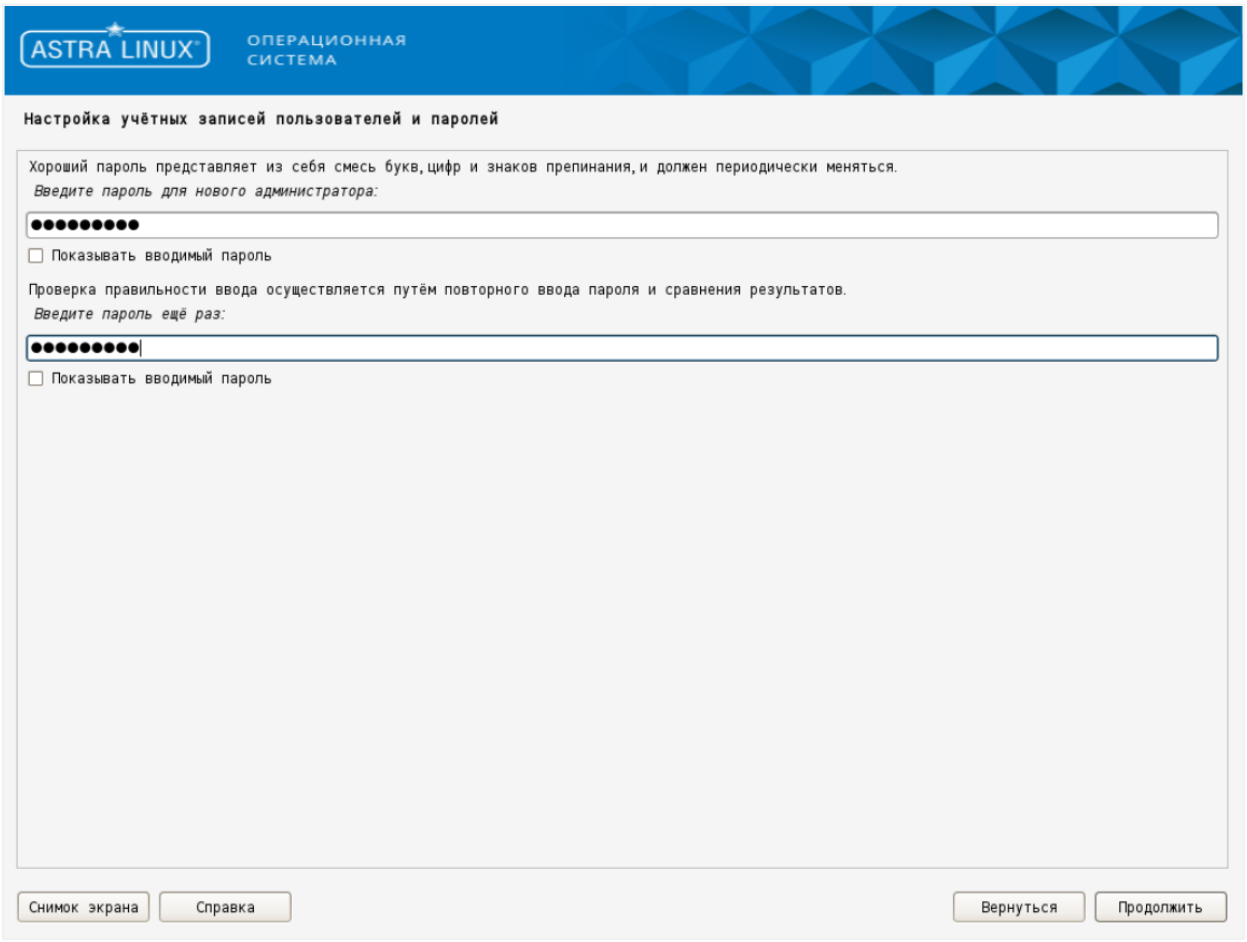

Рисунок 3.13 Настройка пароля учетной записи администратора

5. Выберите город для привязки к часовому поясу.

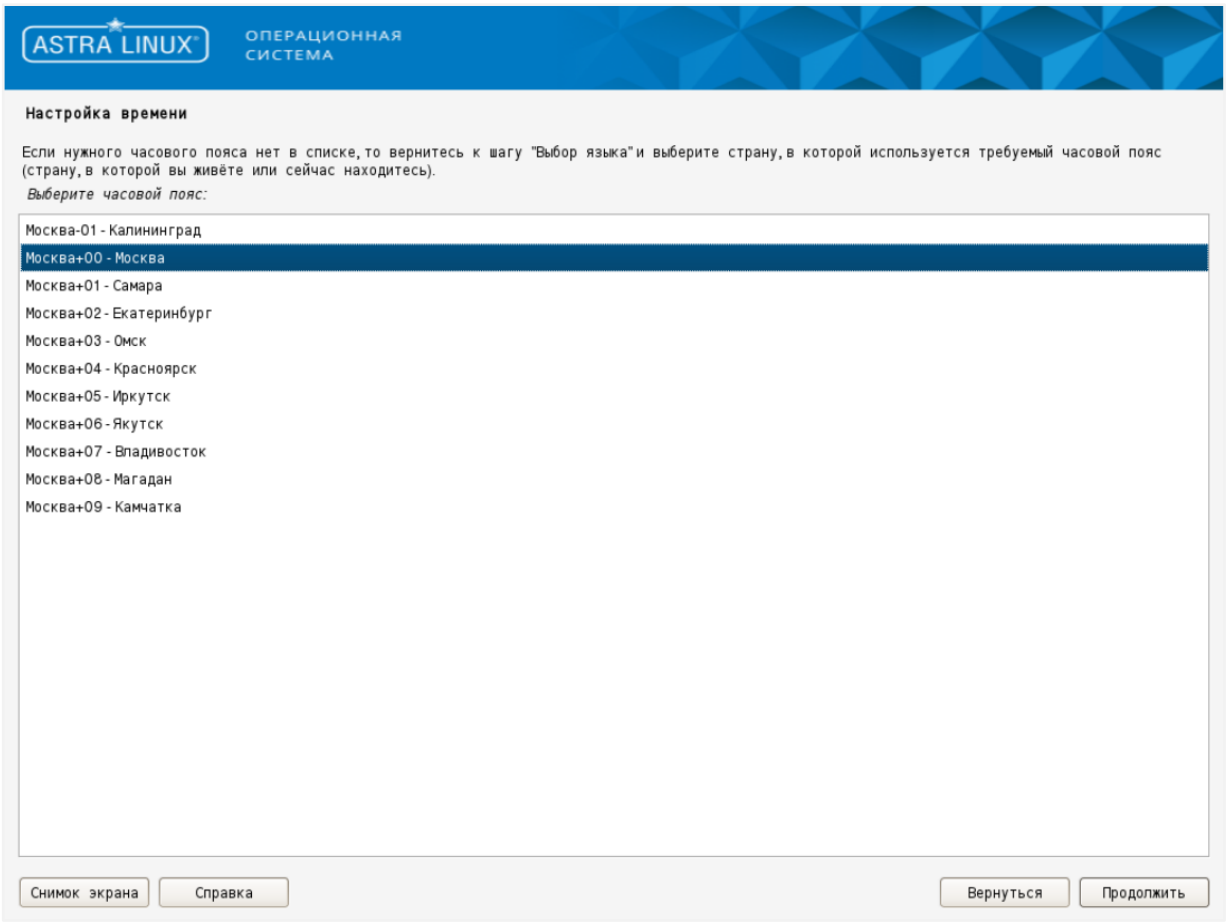

Рисунок 3.14 Выбор города для привязки к часовому поясу

6. Выполните процедуру автоматической разметки диска.

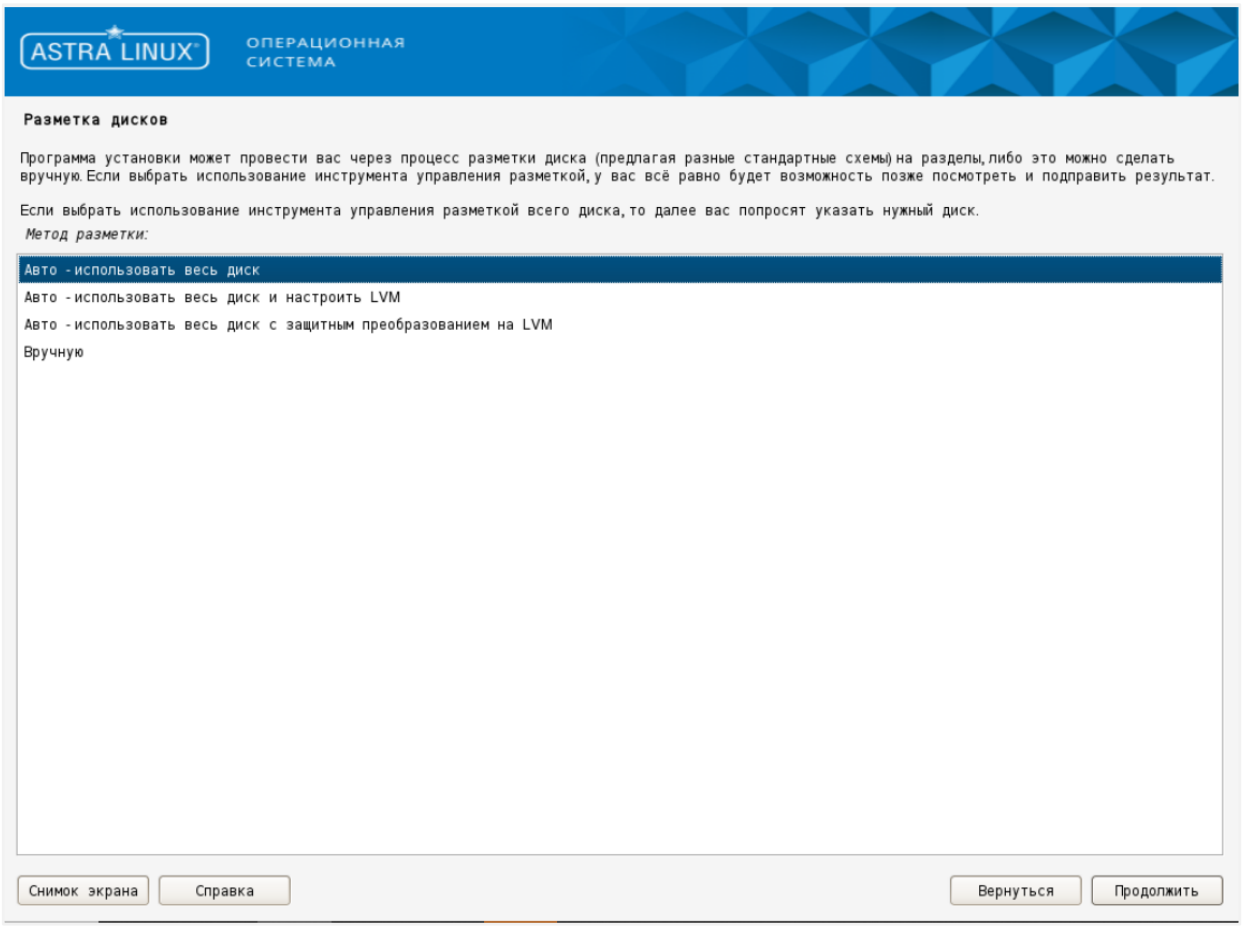

Рисунок 3.15 Автоматическая разметка диска, шаг 1

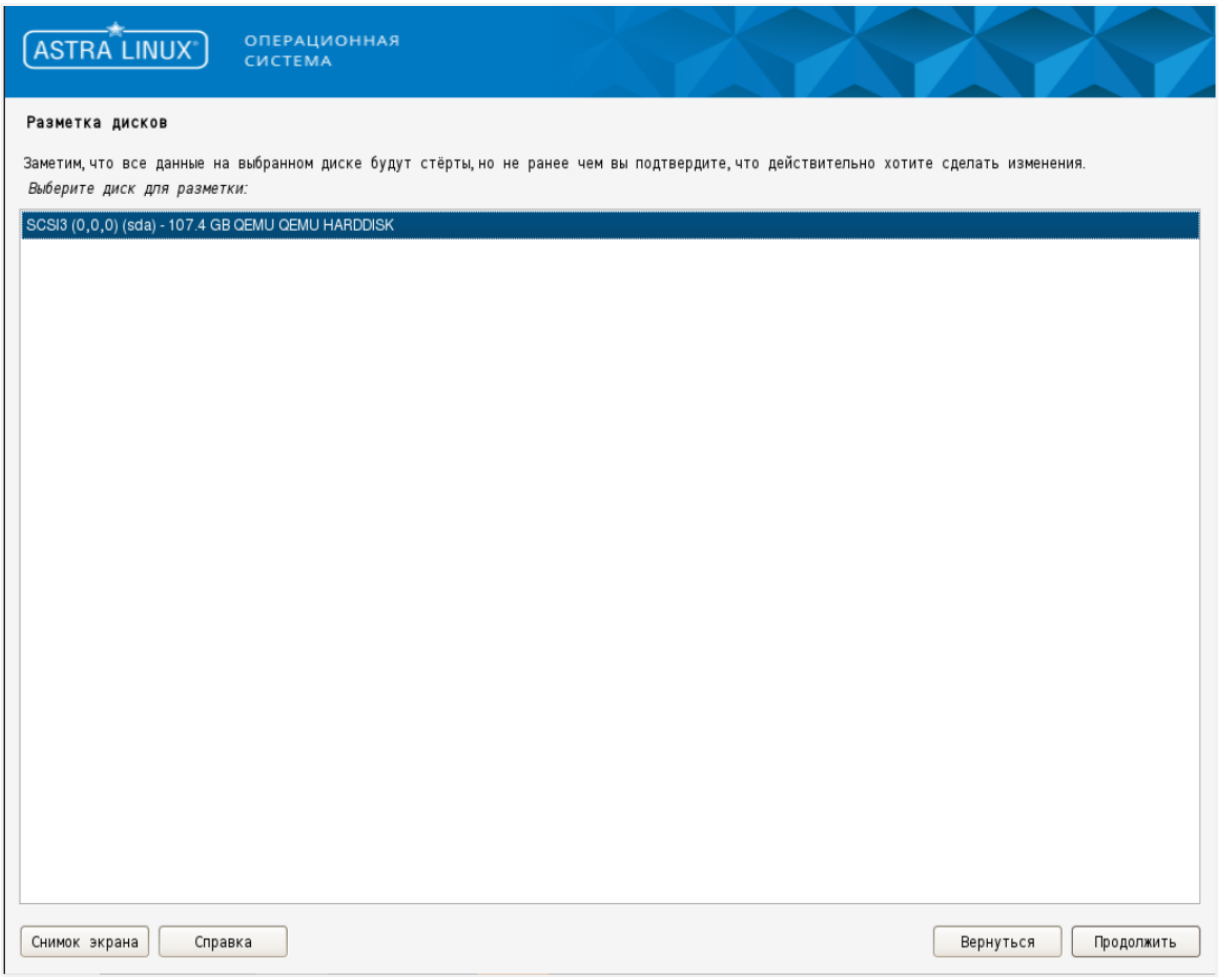

Рисунок 3.16 Автоматическая разметка диска, шаг 2

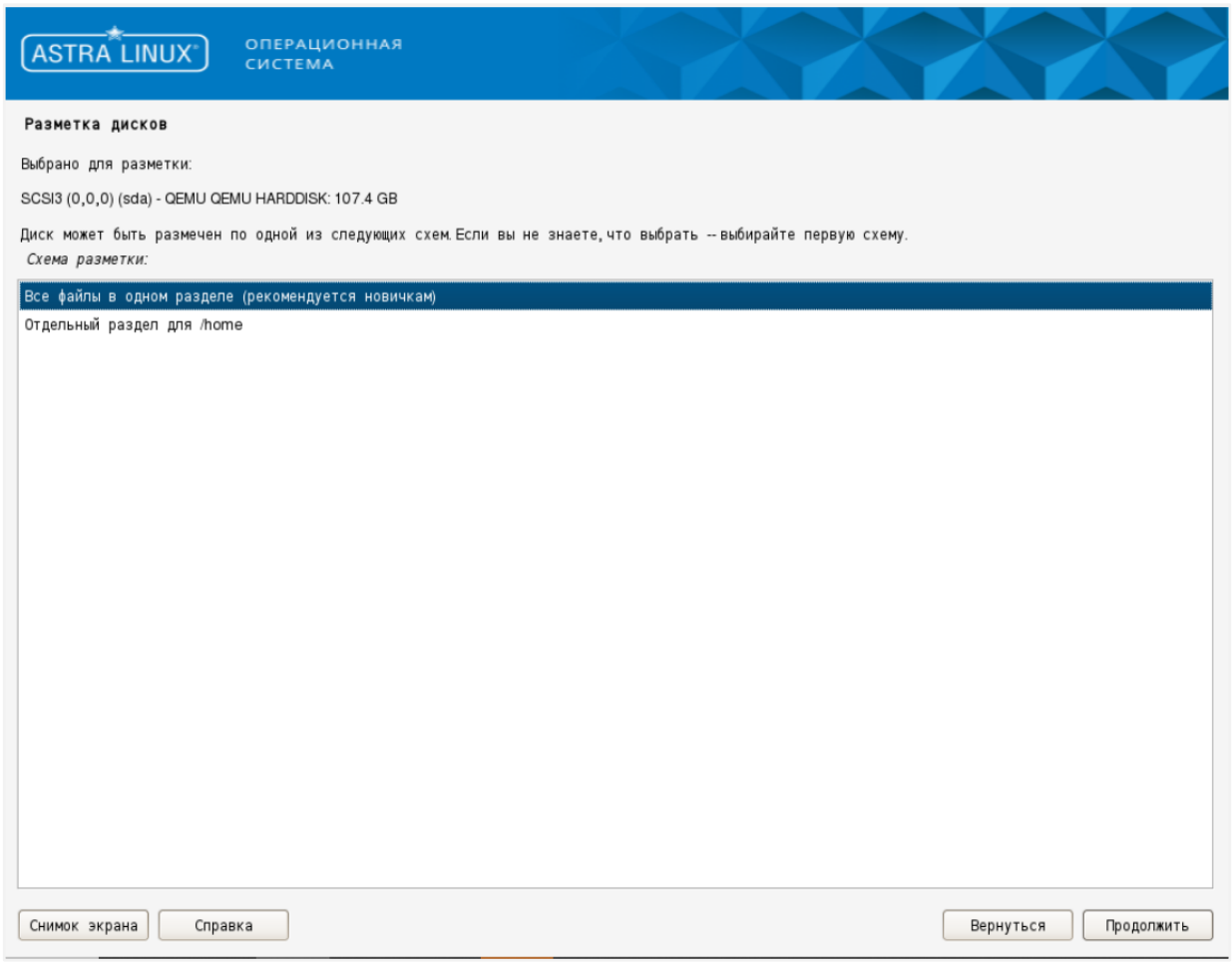

Рисунок 3.17 Автоматическая разметка диска, шаг 3

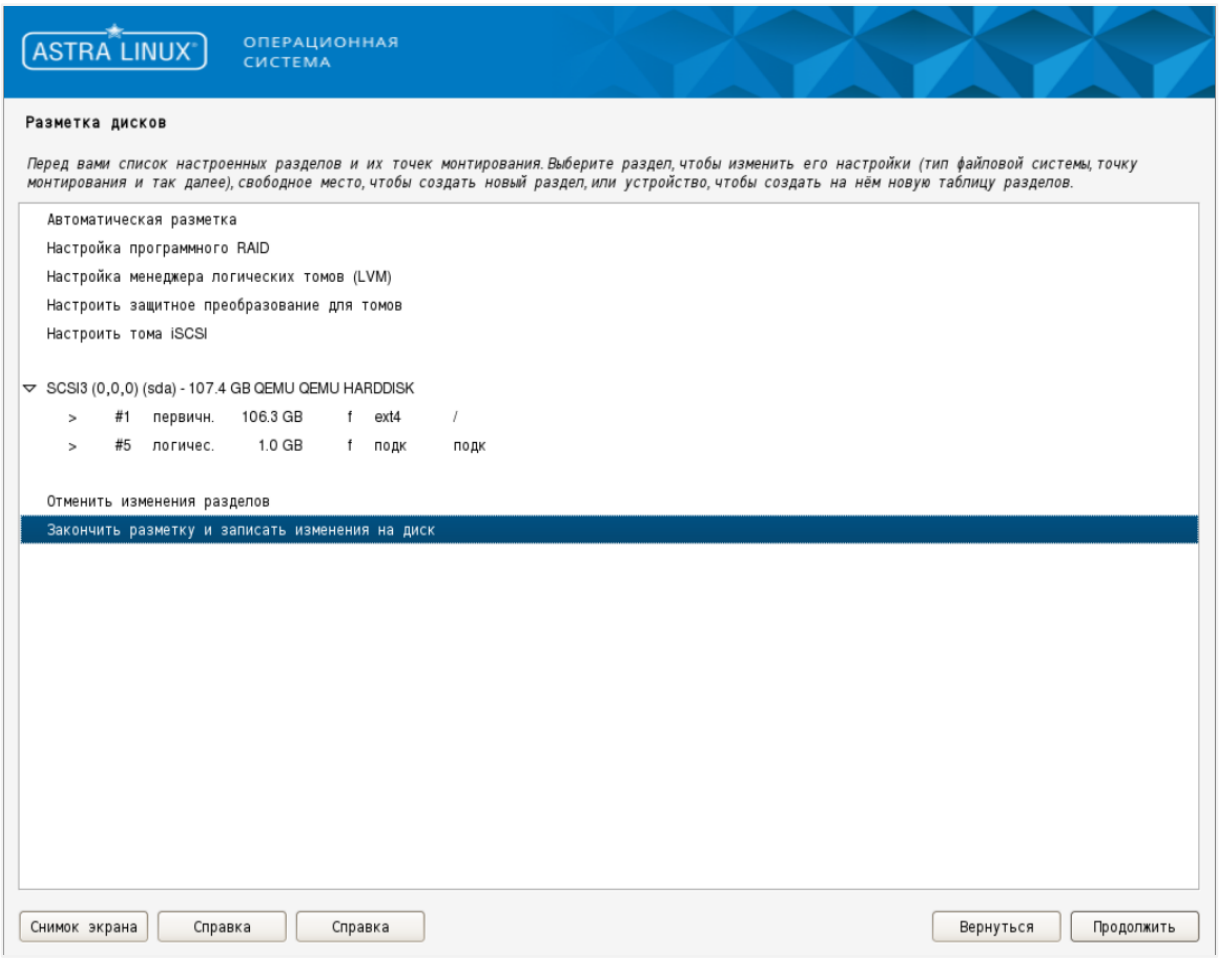

Рисунок 3.18 Автоматическая разметка диска, шаг 4

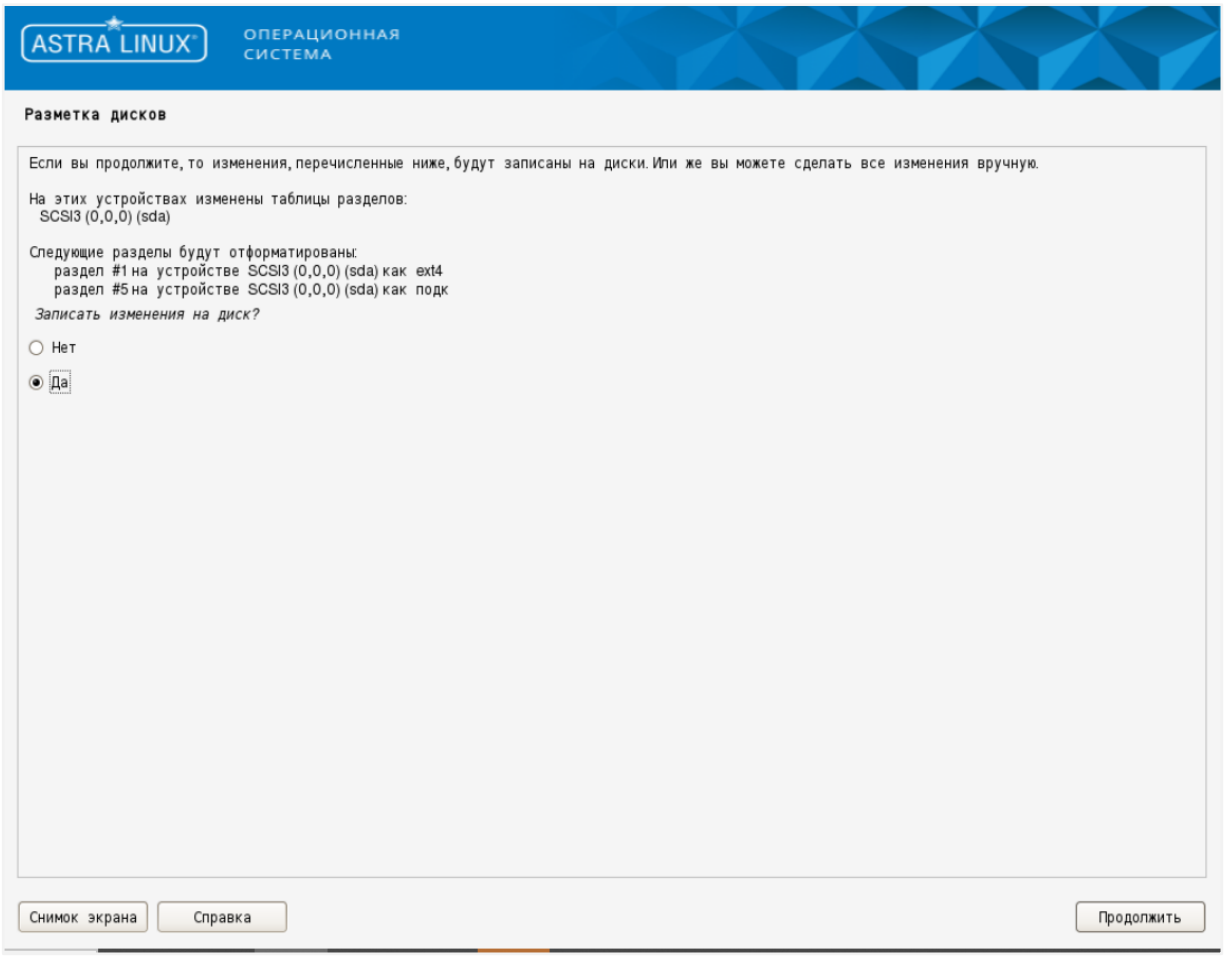

Рисунок 3.19 Автоматическая разметка диска, шаг 5

7. Установите базовую систему.

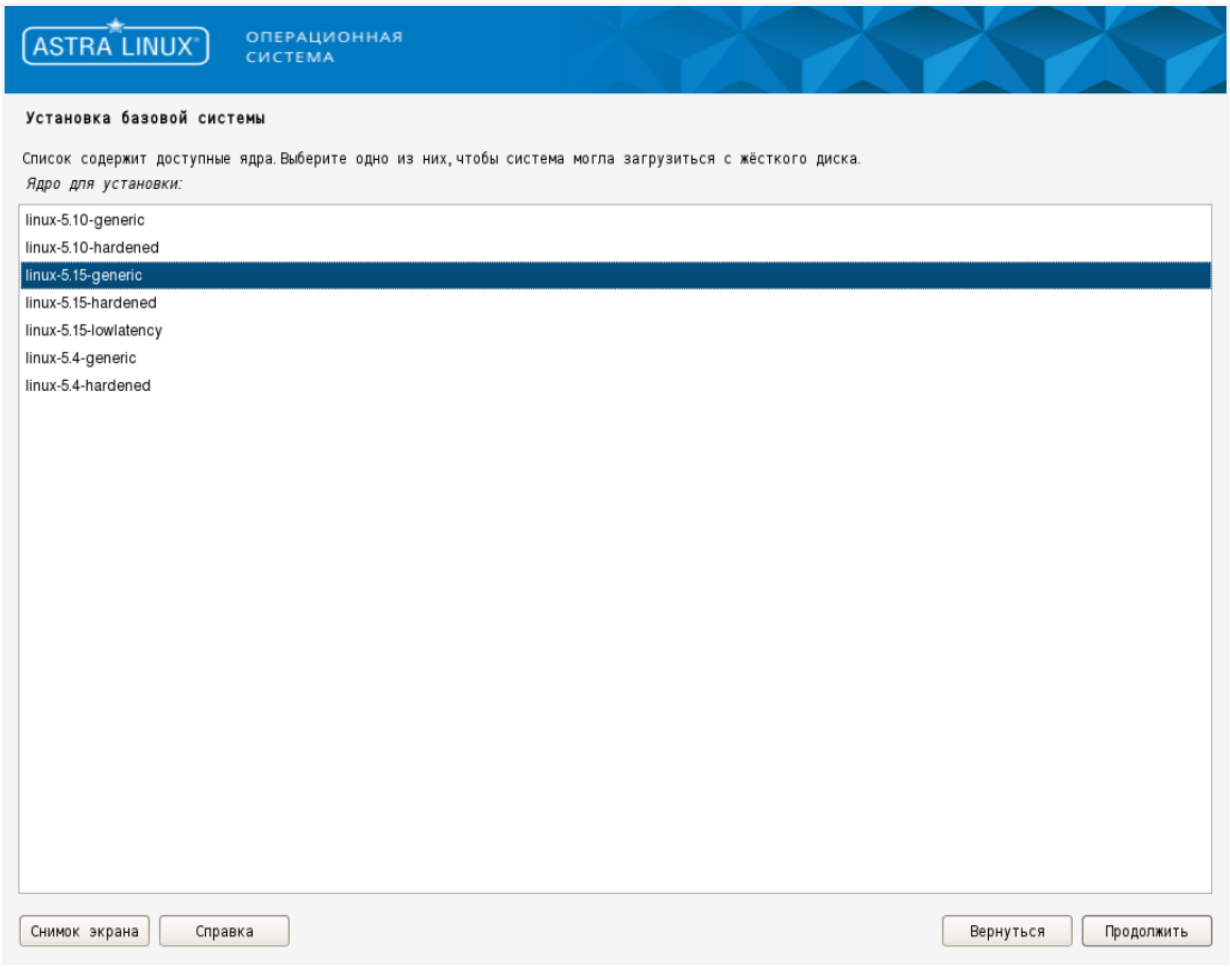

Рисунок 3.20 Установка базовой системы

8. Выберите ПО для установки.

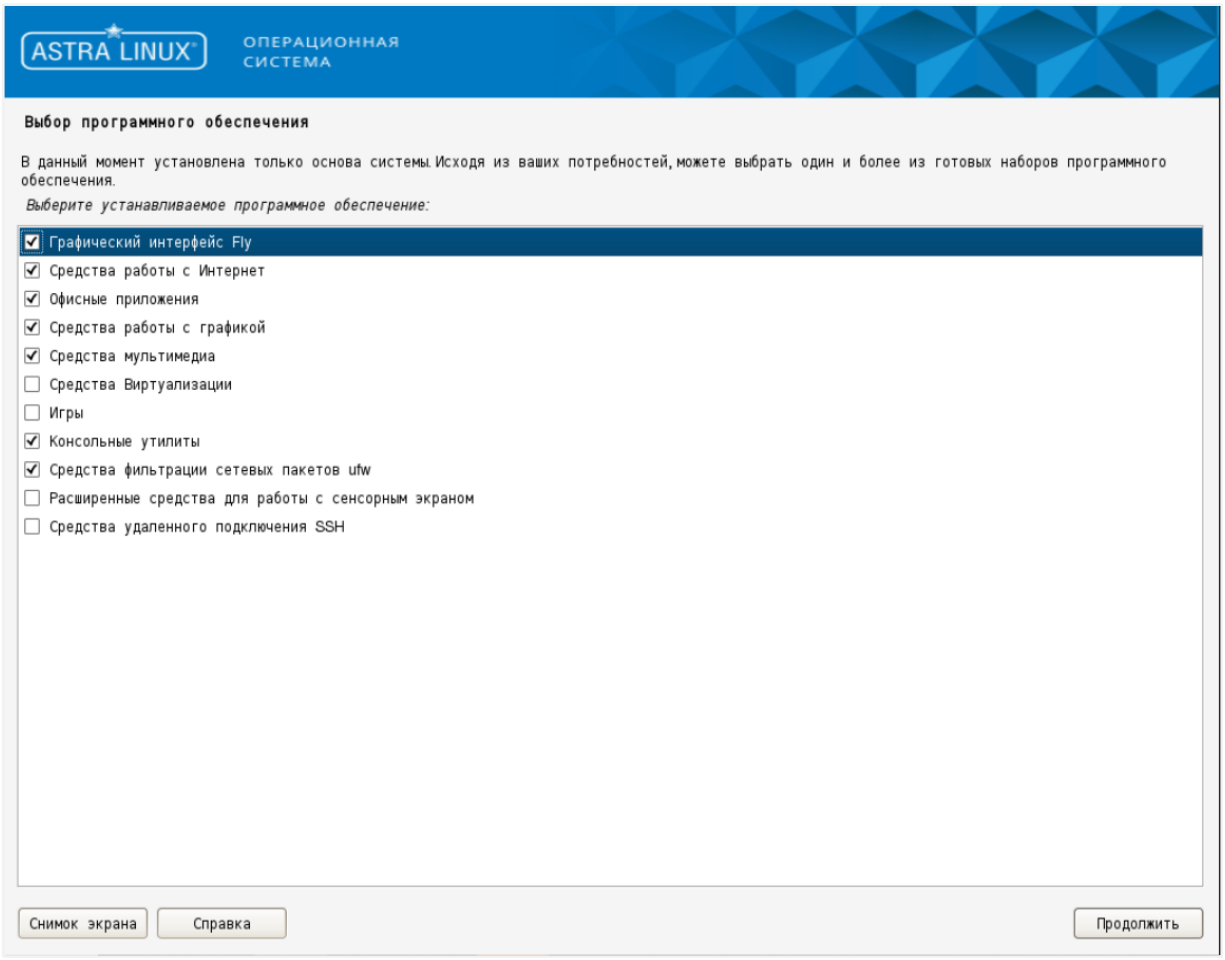

Рисунок 3.21 Выбор программного обеспечения для установки

9. Произведите дополнительные настройки ОС.

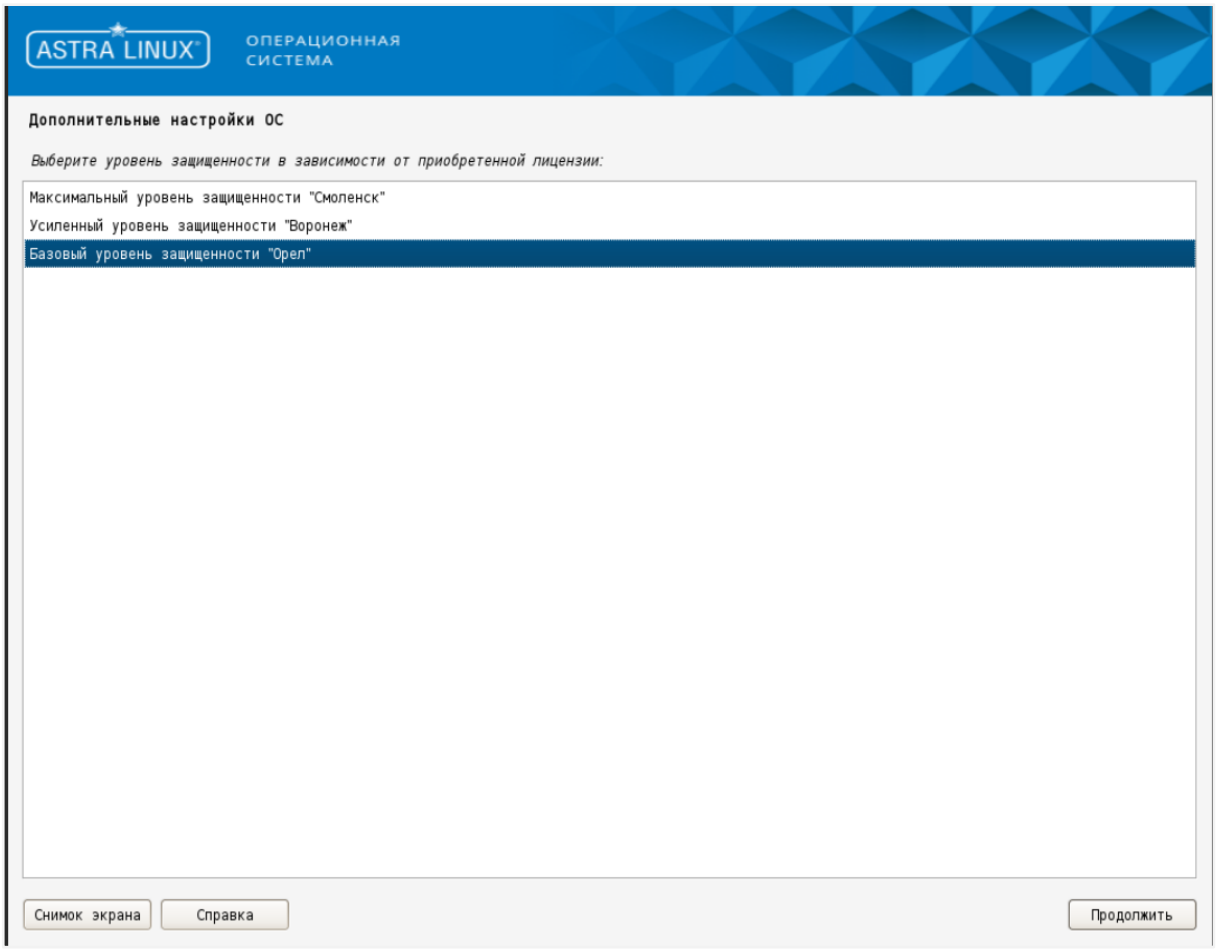

Рисунок 3.22 Дополнительные настройки ОС, шаг 1

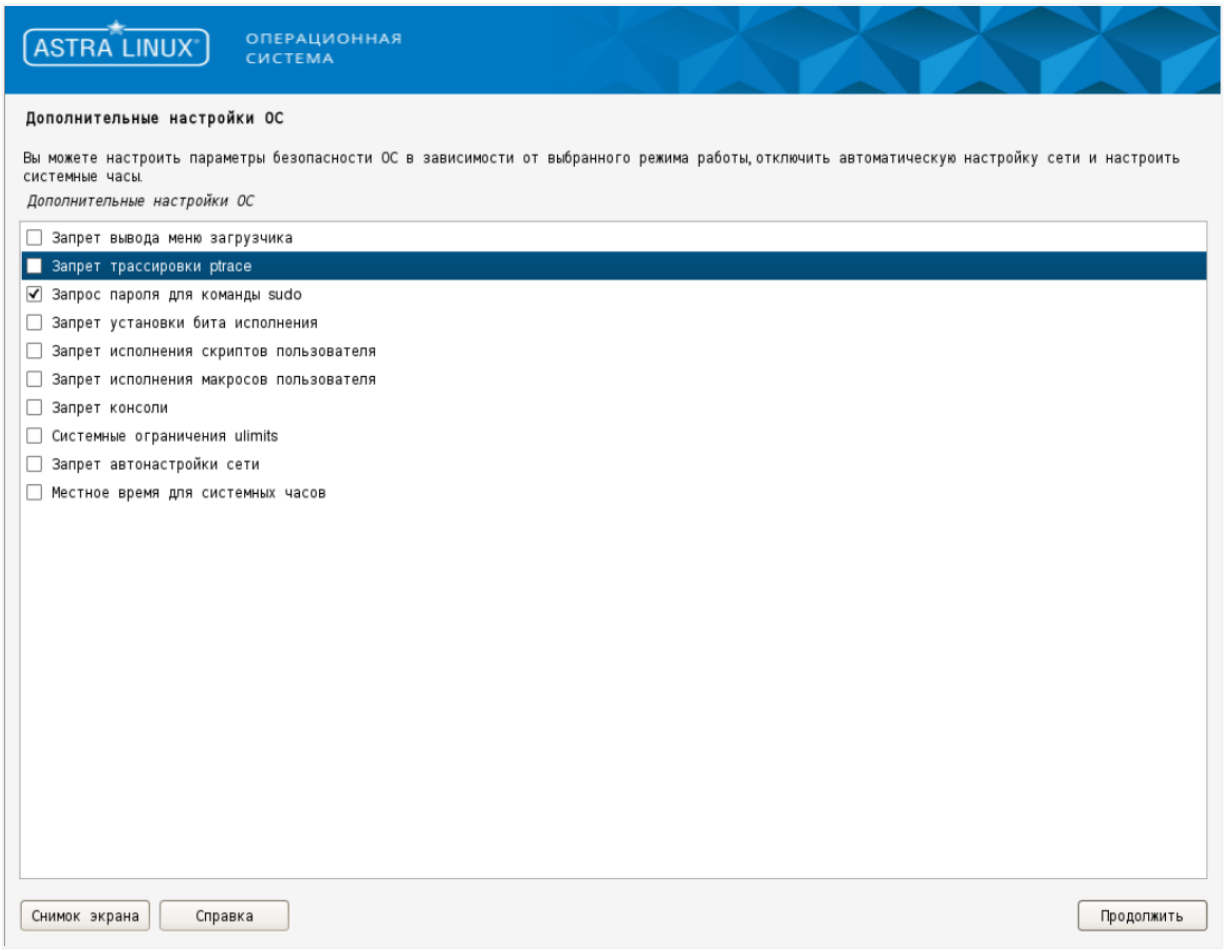

Рисунок 3.23 Дополнительные настройки ОС, шаг 2

10. Выберите установку системного загрузчика на жесткий диск.

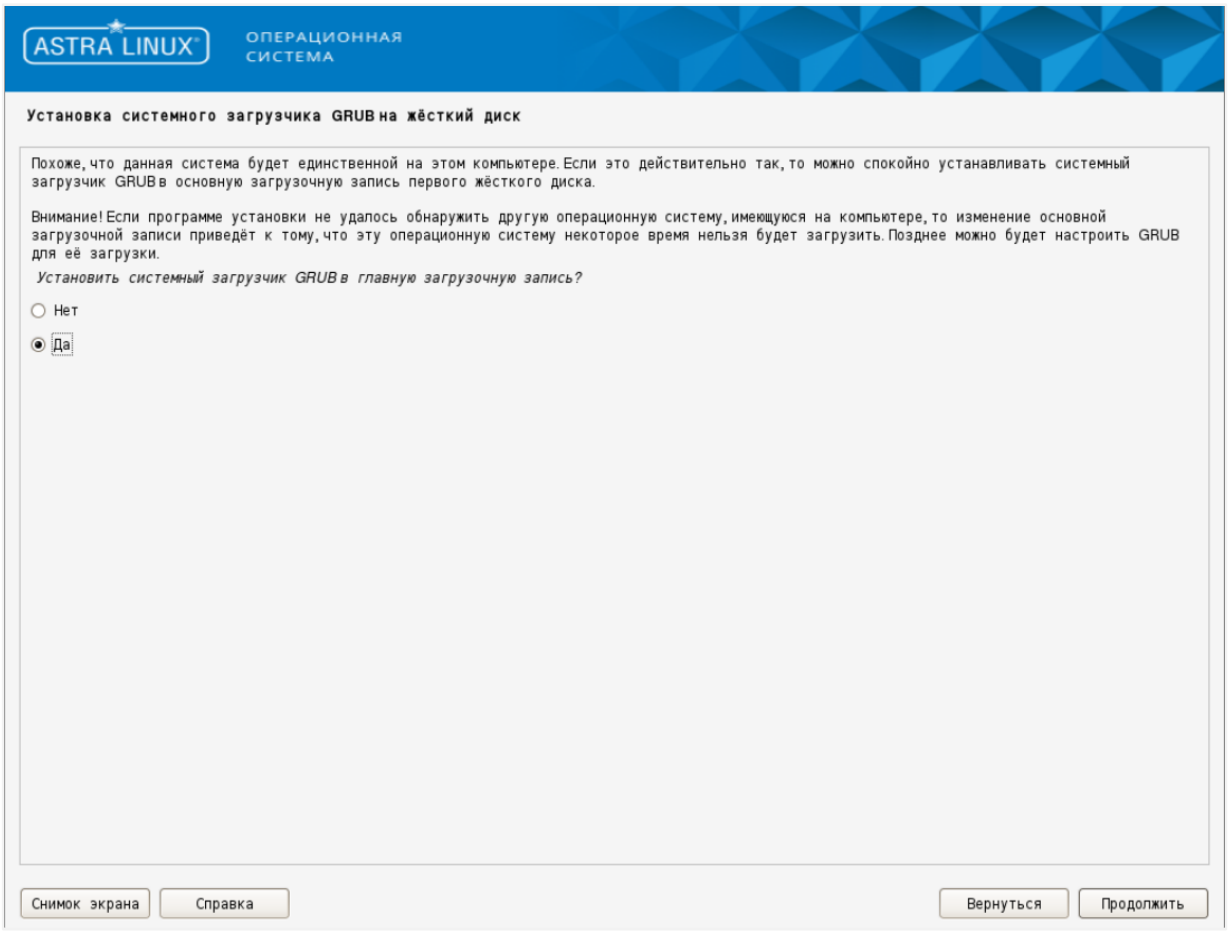

Рисунок 3.24 Выбор места для установки загрузчика

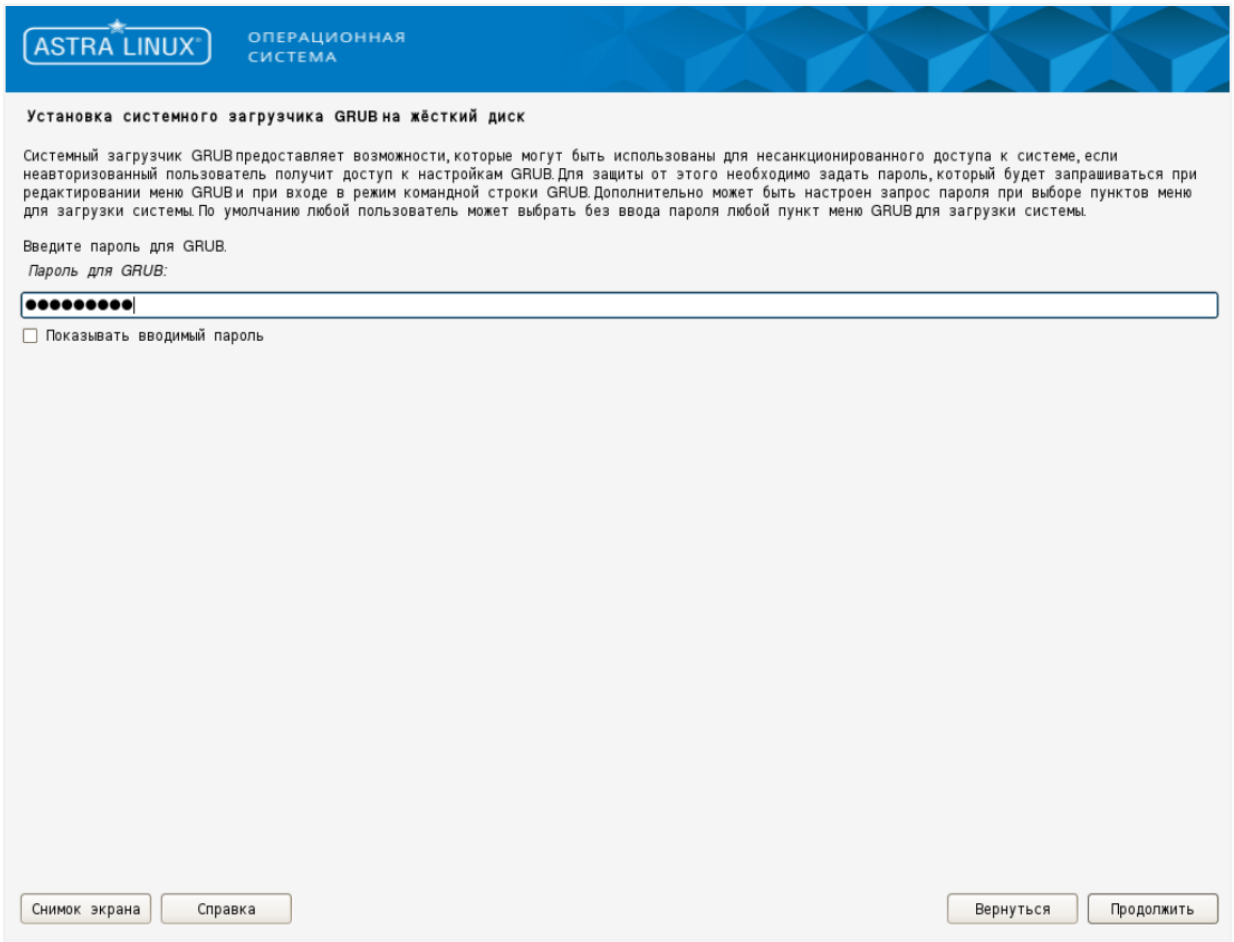

Рисунок 3.25 Защита загрузчика паролем

11.Установите системный загрузчик на жесткий диск.

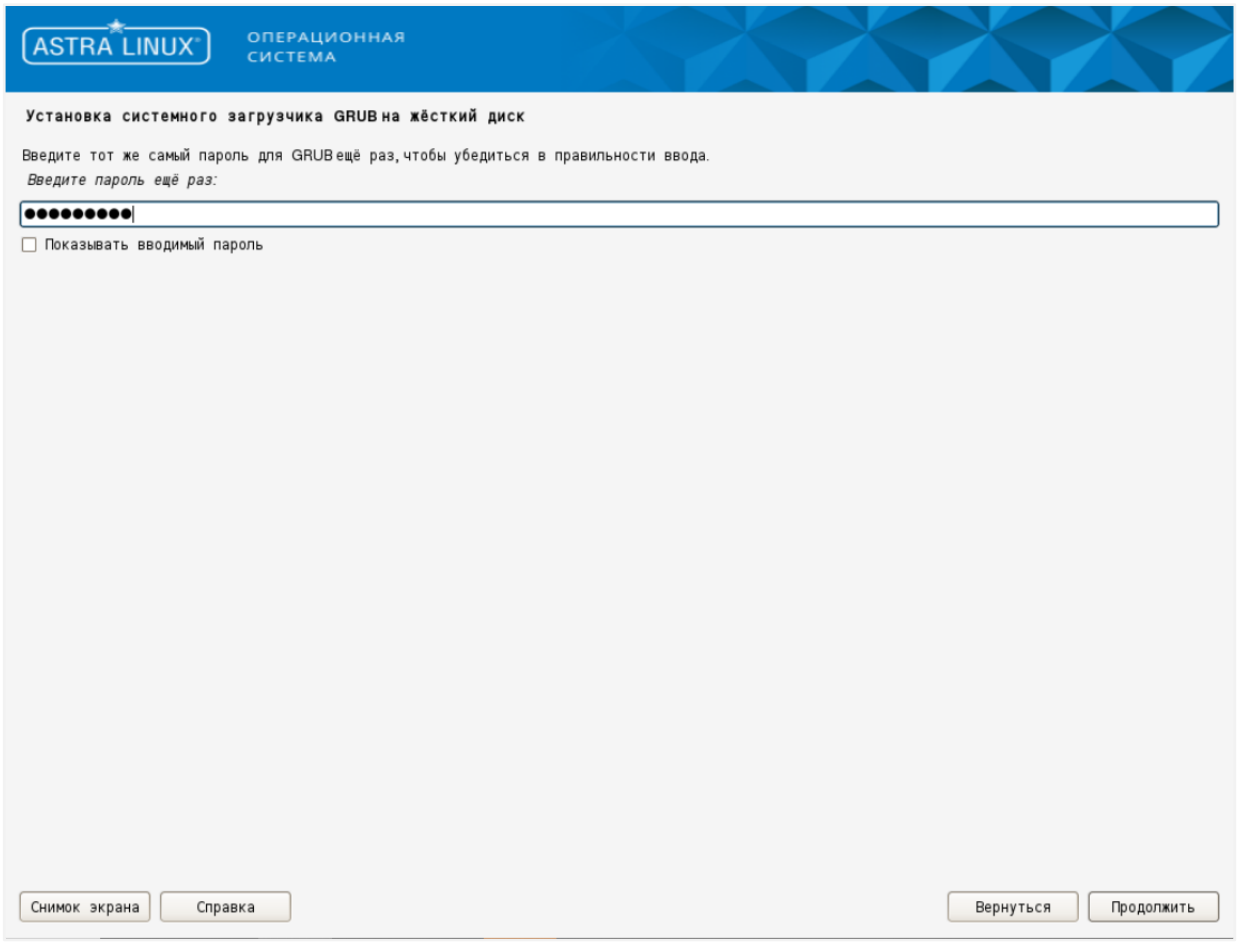

Рисунок 3.26 Повторный ввод пароля

12.Дождитесь завершения процедуры установки ОС.

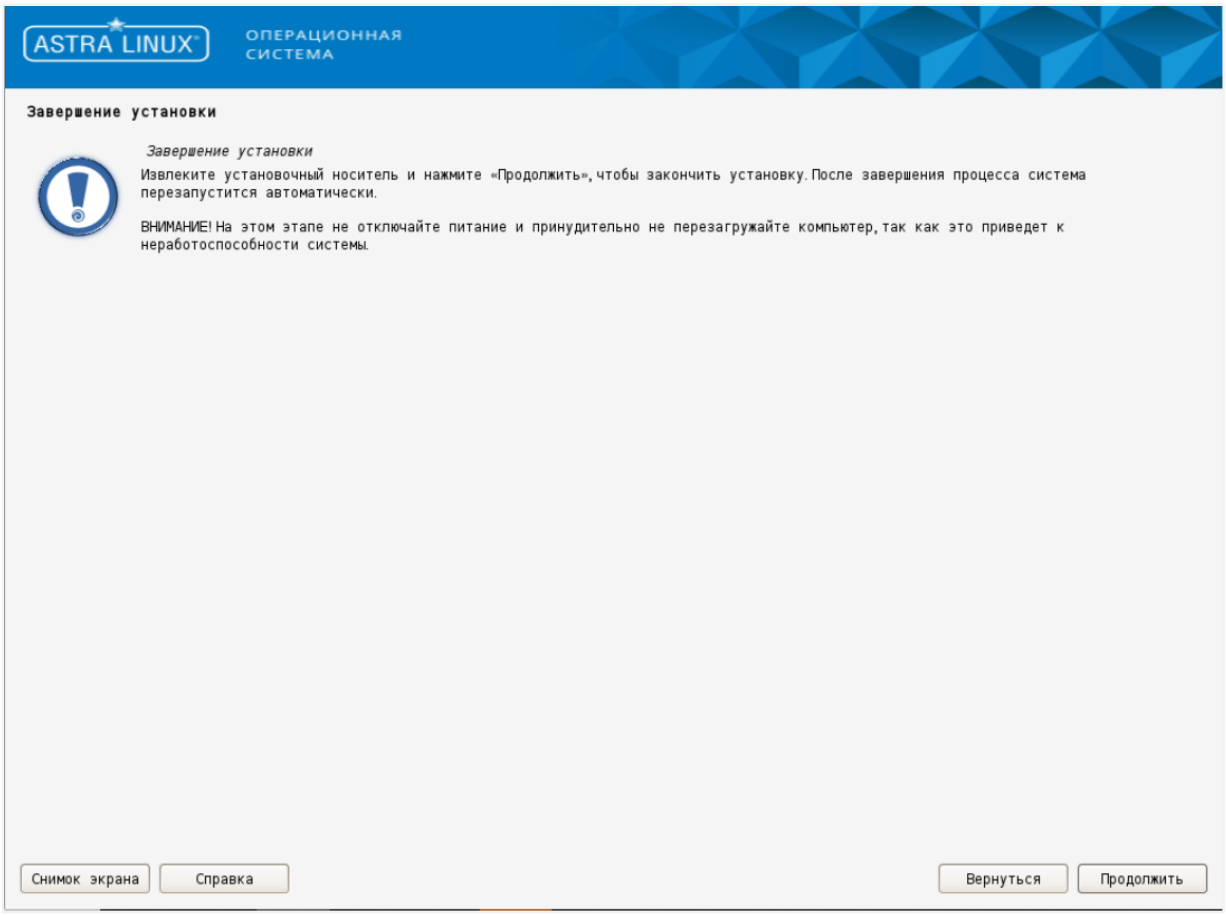

Рисунок 3.27 Уведомление об успешной установке Astra Linux

13.Выполните вход в систему под ранее созданным пользователем.

Рисунок 3.28 Вход в систему

14. 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
```

15. Для обновления сетевых настроек выполните команду:

```
sudo systemctl restart networking
```

3.2.4 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:

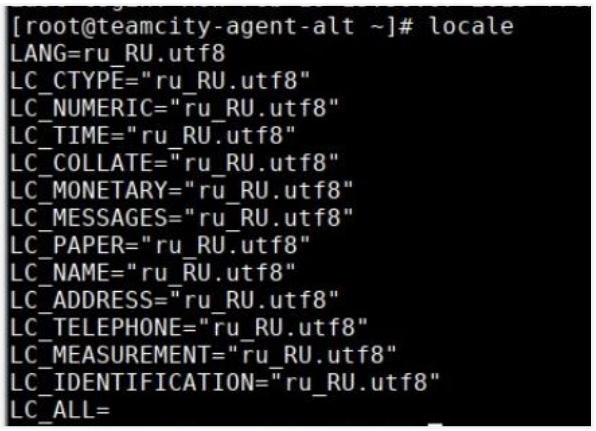

Рисунок 3.29 Вывод команды locale

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

2. Сделайте из текущей настроенной ВМ шаблон, из которого вы в дальнейшем будете создавать другие ВМ 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 ВМ, создаваемых на базе этого шаблона, рекомендуется создать таблицу с именами и IP-адресами ВМ:

Host Name	IP	User	Description

3.2.5 Клонирование ВМ из шаблона

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

1. Создайте новую ВМ из шаблона.

   При необходимости переименуйте созданную ВМ.

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

```
hostnamectl set-hostname hostname
```

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

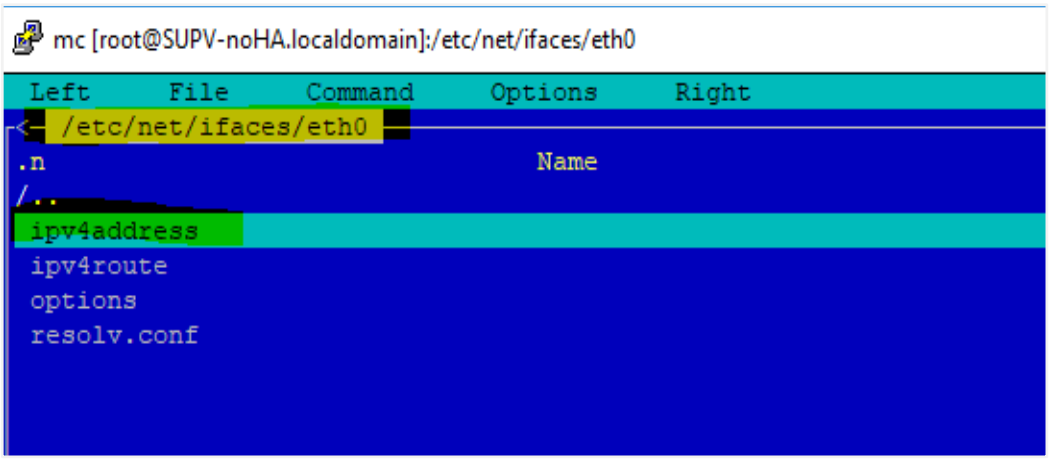

Рисунок 3.30 Добавление IP-адреса для ВМ

4. Перезагрузите ВМ 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.

3.3 Установка в обычном (не-HA) режиме

3.3.1 Установка Бэкенда Базис.WorkPlace

Осторожно

При установке **Бэкенда Базис.WorkPlace** на Альт 9 должны быть подключены официальные репозитории для этой ОС из интернета.

1. Скопируйте и распакуйте архив vdi-deploy-X.tgz со скриптами установки на сервере, где будет установлен **Бэкенд Базис.WorkPlace.**

```
tar -xf vdi-deploy-X.tgz
cd deploy
```

2. Установите удобный вам консольный текстовый редактор и настройте необходимые параметры в конфигурационном файле ***vdi-config.***

```
apt-get install mc
```

```
mcedit vdi-config
```

Примечание

Если необходимо изменить какой-либо внутренний параметр **Базис.WorkPlace**, который не содержится в ***vdi-config***, то его необходимо прописать в файл переопределений ***backend-overrides***. Файл имеет YAML-формат, правила описания параметров представлены в разделе Правила редактирования конфигурационных файлов. Все что было переопределено в ***backend-overrides,*** добавится в ***/etc/vdi.yaml***. Переопределять можно все параметры, которые описаны в документации. Прописывать их нужно в том виде, как они прописаны в соответствующих конфигурационных файлах в RPM.

Примечание

Напрямую править конфигурационные файлы в ***/etc/vdi*.yaml*** или в составе RPM нельзя, они будут перезаписаны при следующем обновлении. Если необходимо внести дополнительные параметры в конфигурацию после того, как был установлен **Бэкенд Базис.WorkPlace**, нужно внести параметры в ***backend-overrides*** и переустановить **Бэкенд Базис.WorkPlace**. Для обнуления ранее прописанных переопределений нужно выполнить переустановку **Бэкенд Базис.WorkPlace** с пустым ***backend-overrides***.

Пример содержимого конфигурационного файла ***vdi-config-example***:

```
vms_api_url: 'https://vms.local'
vms_user: 'UserName'
vms_password: 'vmsPassword'
vms_tls_verification: false

clickhouse_ip: 192.168.0.11
clickhouse_secure: false
clickhouse_tls_verification: false
clickhouse_cluster_name: vcontrol
```

```
embedded_pgsql: false
pgsql_vdi_db: 'vdidb'
pgsql_vdi_user: 'vdiremote'
pgsql_vdi_pass: 'vdiPassword'
pgsql_bind_port: '5432'
pgsql_bind_ip: '192.168.0.252'

#Необязательные параметры:
#use_pgbouncer: false
#pgbouncer_auth_type: 'scram-sha-256'
#pgbouncer_auth_scram_secret: "SCRAM-SHA-
256$4096:ZJAsnmqlOhXer+NxITyIJw==$etLxHXQL5F8wb453z5s9j0rYa5s/pImW/YSo
vYNTIDE=:/2zTmWypfeyRjPMwIQdB5eRhI3T1vfJSH4drSrCJ/p8="

ntp_servers:
  - '192.168.0.254'

logs:
  backend:
     save_last_days: 30
  broker:
     save_last_days: 30

ha_deploy: true

redis_on_backend: true
redis_pass: 'RedisPassword'

vm_agents_bind_host: 192.168.0.123

# Необязательные параметры:
#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'

#broker_cert: /tmp/broker.crt
#broker_key: /tmp/broker.key

#keepalived on_backend: true
```

Описание параметров:

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

установкам **Базис.WorkPlace**. Может содержать английские буквы и цифры, тире, подчеркивание.

- ***vms_api_url*** — адрес пользовательского интерфейса (Web UI) **Базис.vControl**.
- ***vms_user*** — имя пользователя в **Базис.vControl**, под которым **Базис.WorkPlace** будет подключаться к API **Базис.vControl**. Является отдельной технической учетной записью, занесенной в исключения политики паролей.
- ***vms_passwd*** — пароль пользователя, созданного при установке **Базис.vControl** (параметр **Пароль**).
- ***vms_tls_verification*** — проверять сертификат при подключении к API **Базис.vControl**. Если **Базис.vControl** используется с корректным сертификатом, необходимо использовать значение true, если сертификат самоподписанный или недоверенный, значение должно быть false.
- ***embedded_pgsql*** — производить ли установку локальной версии PostgreSQL на сервер, где будет установлен **Бэкенд Базис.WorkPlace.** При значении ***false*** система будет использовать параметры для подключения к внешней PostgreSQL. При значении ***true*** будет произведена локальная установка PostgreSQL из подключенного репозитория, а параметры ***pgsql_bind_port, pgsql_bind_ip*** будут игнорироваться (прослушивается ***127.0.0.1:5432***). В случае использования внешнего сервера PostgreSQL базу создавать не нужно, при развертывании это будет сделано автоматически. Учетная запись для подключения к серверу должна обладать правами на создание базы.

Примечание

При использовании внешней установки PostgreSQL максимальное количество подключений должно быть не ниже 200 (параметр ***max_connections***).

- ***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 (***embeded_pgsql: true***), и для использования внешнего сервера PostgreSQL так, как в систему ставится клиент PostgreSQL. По умолчанию:

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

- ***use_pgbouncer*** — использовать pgbouncer для доступа к postgresql.

  В этом режиме на каждый бэкенд будет установлен pgbouncer, и 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 Workplace 1500) будут равномерно распределены по каждому pgbouncery на каждом бэкенде (при трех бэкендах получаем 1500/3, т.е. по 500 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.

Примечание

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

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

- ***ntp_servers*** — список NTP-серверов, необязательный параметр. Включает синхронизацию времени на всех серверах (**Бэкенд Базис.WorkPlace** и **Диспетчеров подключений**) с заданными NTP-серверами с использованием chronyd.

Осторожно

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

- ***logs*** — секция настройки параметров ротации лог-файлов.
- ***logs.backend.save_last_days*** — количество дней, в течении которого хранятся лог-файлы **Бэкенда Базис.WorkPlace/Менеджера диспетчеров подключений**. Ротация лог-файлов происходит каждый день, каждый предыдущий день архивируется. Лог-файлы старше указанного количества дней удаляются из файловой системы.
- ***logs.broker.save_last_days*** **—** количество дней, в течении которого хранятся лог-файлы **Диспетчера подключений**. Ротация лог-файлов происходит каждый день, каждый предыдущий день архивируется. Лог-файлы старше указанного количества дней удаляются из файловой системы.
- ***clickhouse_ip*** — адрес, значение которого зависит от типа развертывания **Базис.vControl**:
  - в HA режиме это VIP адрес ClickHouse **Базис.vControl** (параметр ***vips.clickhouse*** в **Базис.vControl**);
  - в non-HA режиме это адрес сервера **Бэкенда Базис.vControl**.
- ***clickhouse_secure*** — использование шифрованного соединения tls/ssl для взаимодействия с компонентами ClickHouse.

  По умолчанию: false.

- ***clickhouse_tls_verification*** — проверка сертификата, предоставляемого третьей стороной, при подключении к внешнему кластеру Clickhouse.

  По умолчанию: false. Актуально при clickhouse_secure: true. Предполагается, что необходимый корневой сертификат уже установлен в операционной системе в хранилище сертификатов по умолчанию.

Примечание

ВАЖНО настроить соответствующий порт для ssl/tls, по умолчанию 9440.

- ***clickhouse_cluster_name*** — имя ClickHouse кластера, в котором нужно создавать реплицированные таблицы.

  По умолчанию: vcontrol.

Примечание

Если параметр ***clickhouse_cluster_name*** не определен или не заполнен, то создается нереплицируемая таблица в ClickHouse, заданном в параметре ***clickhouse_ip***, если параметр определен, то при инсталляции Базис.WorkPlace будут создаваться реплицируемые таблицы в указанном кластере.

В случае HA-инсталляции Базис.vControl для Базис.WorkPlace, при использовании ClickHouse от Базис.vControl, параметр должен иметь значение ***vcontrol:***

```
clickhouse_cluster_name: vcontrol
```

В случае nonHA инсталляции v.Control для Базис.WorkPlace, при использовании ClickHouse от Базис.vControl, параметр должен ***отсутствовать***.

Если для Базис.WorkPlace используется кластер ClickHouse, предоставляемый третьей стороной, параметр должен иметь значение ***ИМЯ_КЛАСТЕРА_CLICKHOUSE_ТРЕТЬЕЙ_СТОРОНЫ***.

Если в инсталляции Базис.WorkPlace используется nonHA ClickHouse, предоставляемый третьей стороной, параметр должен ***отсутствовать***.

- ***ha_deploy*** — установка в режиме отказоустойчивости, при установке не в HA-конфигурации должно быть в false.
- ***redis_pass*** — пароль доступа к Redis.

Примечание

Пароль, указанный в качестве значения параметра ***redis_pass***, используется так же для аутентификации в ***redis-sentinel***.

- ***vm_agents_bind_host*** — IP-адрес, используемый для связи с ВС Агентами.

Примечание

Данный параметр является опциональным при установке **Бэкенда Базис.WorkPlace**, но является обязательным, если требуется подключение функциональности для работы с физическими ПК в **Базис.WorkPlace**.

Если на **Бэкенде** всего один IP-интерфейс, то будет использоваться заданное в параметре значение, либо будет прописан адрес, через который идет шлюз по умолчанию (default gw) на системе. Если значение не указано, а IP-интерфейсов на **Бэкенде** несколько, то при установке возникнет ошибка.

Параметр также может быть задан на конкретный **Бэкенд** через конфигурационный файл ***backends-hosts***.

- ***broker_cert*** — опциональный параметр; путь к сертификату для **Диспетчера подключений** в pem формате. Может быть задано на конкретный **Диспетчер подключений** в ***broker-hosts***.
- ***broker_key*** — опциональный параметр; путь к секретному ключу (rsa/gost) сертификата для **Диспетчера подключений** в pem формате. Может быть задано на конкретный **Диспетчер подключений** в ***broker-hosts***.

Совет

Через ***broker-hosts*** можно переопределить параметры ***broker_cert*** и ***broker_key*** на конкретный **Диспетчер подключений**. Пример:

```
node1 ansible_user=root ansible_host=192.168.0.18
ansible_ssh_private_key_file='/tmp/key'
broker_in_ip_for_client=192.168.0.18
broker_out_ip_to_vm=192.168.0.18
broker_out_ip_to_backend=192.168.0.18
broker_cert=/tmp/broker2.crt broker_key=/tmp/broker2.key
```

Если для конкретного **Диспетчера подключений** или в ***vdi-config*** параметры ***broker_cert*** и ***broker_key*** не определены, то генерируется один самоподписанный сертификат для всех **Диспетчеров подключений**, для которых эти параметры не определены.

Если параметры ***broker_cert*** и ***broker_key*** определены в ***vdi-config*** или на хост в ***broker-hosts***, то используются сертификат и ключ из них.

- ***broker_cert_key_type*** — опциональный параметр; тип ключа для подписи сертификата: rsa или gost. Параметр нужен только для генерации самоподписанного сертификата, если явно передан сертификат в ***broker_cert***, то его тип определится автоматически.
- ***broker_cert_key_bit*** — опциональный параметр; битность ключа для подписи сертификата при генерации самоподписанного сертификата:
  - ***broker_cert_key_bit.rsa*** — для rsa ключа,
  - ***broker_cert_key_bit.gost*** — для gost ключа.
- ***keepalived_on_backend*** — необязательный параметр, отвечает за установку сервиса keepalived на хостах Бэкенда.

  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 протокола VRRP для доступа к хостам **Бэкенда Базис.WorkPlace**:
  - ***vips.backend.vip*** — виртуальный IP-адрес для **Бэкенда Базис.WorkPlace**, который будет перемещаться, если хост выйдет из строя;
  - ***vips.backend.vrouter_id*** — идентификационный номер VRRP-роутера, который должен задаваться целым числом от 0 до 255 и быть уникальным в рамках L2-сети;
- ***snmp_agent_deploy*** — для установки SNMP Агента при развертывании **Бэкенда Базис.WorkPlace** параметр должен иметь значение ***true***, в противном случае – ***false***.

Примечание

Все настройки параметров, необходимые для автоматической установки SNMP Агента при развертывании **Бэкенда Базис.WorkPlace**, приведены в разделе Установка SNMP Агента.

Файл конфигурации имеет YAML-формат, правила описания параметров представлены в разделе Правила редактирования конфигурационных файлов.

3. Разверните сконфигурированное решение следующей командой с указанием пути к файлу с парольной фразой в обязательном параметре ***-v***:

Примечание

Файл с парольной фразой — это текстовый файл, в котором открытым текстом записывается парольная фраза.

```
./deploy.sh -s -a environment-vdi.tgz -w vdi-agent-updates.tar.gz
-v /path/to/vault-password-file
```

Осторожно

Установка **Бэкенда Базис.WorkPlace** 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».

По итогам выполнения команды **Бэкенд Базис.WorkPlace** будет установлен на текущий сервер. В консоль будет выведен отчет об успешной установке.

Пример успешного завершения операции развертывания **Бэкенда Базис.WorkPlace** (рисунок 3.31):

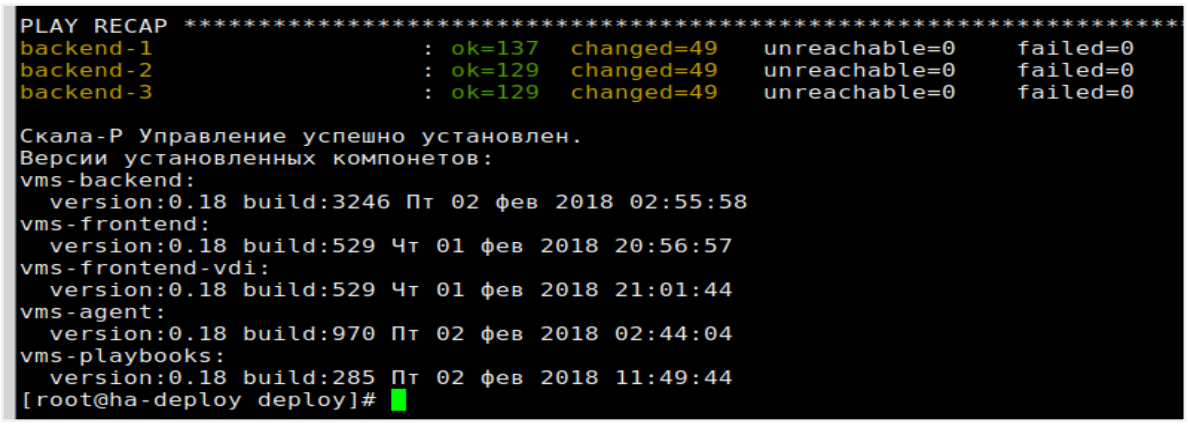

Рисунок 3.31 Пример успешного развертывания Бэкенда Базис.WorkPlace

В случае некорректной работы список ошибок выводится в консоль. Их детали можно посмотреть в лог-файле установки ***/opt/vdi-playbooks/logs/ansible.log***.

Осторожно

При установке **Менеджера диспетчеров подключений Базис.WorkPlace** на систему с множественной адресацией (multihome) привязка компонент **Бэкенда Базис.WorkPlace** производится к тому адаптеру, с которого производится обращение к шлюзу по умолчанию. Для перепривязки **Бэкенда Базис.WorkPlace** к другому адаптеру выполните следующие шаги:

1. Привяжите шлюз по умолчанию к требуемому адаптеру.
2. Повторно запустите скрипт установки.

```
./deploy.sh -s
```

3. Привяжите шлюз по умолчанию к прежнему адаптеру.
4. На хосте перезапустите службы **Бэкенда** и **Менеджера диспетчеров подключений Базис.WorkPlace**.

```
systemctl restart vdi-backend vdi-broker-manager.target
```

1. Если в процессе работы **Менеджеров диспетчеров подключений Базис.WorkPlace** потребуется перезапустить его службы, это можно сделать следующей командой:

```
systemctl restart vdi-backend vdi-broker-manager.target
```

3.3.1.1 Установка Бэкенда Базис.WorkPlace с использованием внешней БД

Осторожно

При установке **Бэкенда Базис.WorkPlace** на Альт 9 должны быть подключены официальные репозитории для этой ОС из интернета.

Установка полностью аналогична Установке Бэкенда Базис.WorkPlace за исключением того, что параметр ***embedded_pgsql*** должен иметь значение ***false***, также должны быть заполнены следующие параметры:

- ***pgsql_vdi_db*** — имя базы данных.
- ***pgsql_vdi_user*** — логин пользователя для подключения **Базис.WorkPlace** к базе данных. В случае использования внешней PostgreSQL пользователь должен обладать правами на создание базы данных (***createdb***). В случае использования общего PostgreSQL-сервера рекомендуется использовать логин, отличный от используемого для **Базис.vControl**.
- ***pgsql_vdi_pass*** — пароль пользователя для подключения **Базис.WorkPlace** к базе данных.
- ***pgsql_bind_port*** — TCP-порт, который используется для подключения к PostgreSQL.
- ***pgsql_bind_ip*** — IP-адрес, который используется для подключения к PostgreSQL.

3.3.2 Установка Диспетчера подключений Базис.WorkPlace

Осторожно

При установке **Диспетчера подключений Базис.WorkPlace** на Альт 9 должны быть подключены официальные репозитории для этой ОС из интернета.

1. Для установки **Диспетчеров подключений** используется тот же пакет, что и для установки **Бэкенда Базис.WorkPlace**. На том же сервере, где производилась установка **Базис.WorkPlace**, в той же директории, где находится пакет для установки (распакованный архив ***vdi-deploy-X.tgz***), вносятся изменения в файл ***broker-hosts***. В этом файле описываются серверы (IP-адреса подготовленных серверов или виртуальных машин с операционной системой, установленной аналогично решению **Бэкенд Базис.WorkPlace**) **Диспетчеров подключений** и параметры SSH-подключения к ним. Скопируйте или переименуйте файл ***broker-hosts-example*** в ***broker-hosts***. Пример содержимого файла ***broker-hosts-example***:

```
[vdi-brokers]
broker_name1 ansible_user=root ansible_host=123.123.123.123
ansible_ssh_private_key_file='/tmp/key'
broker_in_ip_for_client=123.123.123.123
broker_out_ip_to_vm=123.123.123.123
broker_out_ip_to_backend=123.123.123.123
broker_name2 ansible_user=root ansible_host=123.123.123.125
ansible_ssh_pass='AnsiblePassword'
broker_in_ip_for_client=123.123.123.125
broker_out_ip_to_vm=123.123.123.125
broker_out_ip_to_backend=123.123.123.125
```

Примечание

Если необходимо изменить какой-либо внутренний параметр **Диспетчера подключений**, который не содержится в ***vdi-config***, то его необходимо прописать в файл переопределений ***broker-overrides***. Файл имеет YAML-формат, правила описания параметров представлены в разделе Правила редактирования конфигурационных файлов. Все, что переопределено в ***broker-overrides,*** добавится в ***/etc/vdi-broker.yaml***. Переопределять можно все параметры, которые описаны в документации. Прописывать их нужно в таком же виде, как они прописаны в соответствующих конфигурационных файлах в RPM.

Примечание

Напрямую править конфигурационные файлы в ***/etc/vdi-broker-*.yaml*** или в составе RPM нельзя, они будут перезаписаны при следующем обновлении. Если необходимо внести дополнительные параметры в конфигурацию после того как **Диспетчер подключений Базис.WorkPlace** был установлен, нужно внести параметры в ***broker-overrides*** и переустановить **Диспетчер подключений Базис.WorkPlace**. Для обнуления ранее прописанных переопределений нужно выполнить переустановку **Диспетчера подключений Базис.WorkPlace** с пустым ***broker-overrides***.

Описание параметров:

- ***broker_name*** — имя сервера.
- ***ansible_user*** — должен быть root.
- ***ansible_host*** — IP-адрес сервера, через который будет происходить SSH-подключение и установка компонентов.
- ***ansible_private_key_file*** — 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.
- ***broker_in_ip_for_client*** — IP-адрес, к которому подключаются клиенты.
- ***broker_out_ip_to_vm*** — IP-адрес, с которого **Диспетчер подключений** подключается к виртуальным машинам рабочих столов.

- ***broker_out_ip_to_backend*** — IP-адрес, с которого **Диспетчер подключений** соединяется с **Менеджером диспетчеров подключений**.

2. Рекомендуется, чтобы файл ***broker-hosts*** со списком **Диспетчеров подключений** содержал те же имена серверов, что и реальные имена хостов и названия серверов (***hostname -f***), которые будут использованы для добавления в **Базис.WorkPlace** через **Фронтенд Базис.WorkPlace**.
3. Под учетной записью root, находясь в каталоге с установочными файлами, выполните следующую команду:

```
./deploy.sh -e -a environment-vdi.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».

В случае если требуется включить возможность скачивания дистрибутивов **Клиента Базис.WorkPlace** через браузер с **Диспетчера подключений**, то в команде через параметр ***-c*** укажите файл, содержащий набор пакетов **Клиента Базис.WorkPlace** для всех поддерживаемых платформ:

```
./deploy.sh -e -a environment-vdi.tgz -c vdi-client.tar.gz
```

Произойдет установка всех необходимых компонентов на все серверы, описанные в файле ***broker-hosts***, и после завершения работы скриптов установки **Диспетчеры подключений** будут готовы к подключению к **Базис.WorkPlace**.

Критерием удачной установки **Диспетчеров подключения** является сообщение (рисунок 3.32):

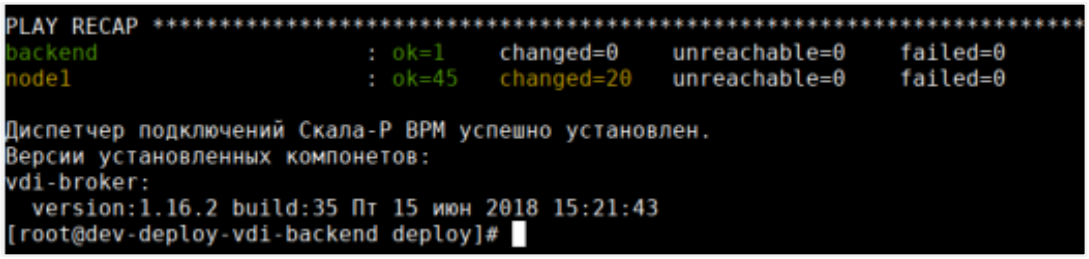

Рисунок 3.32 Установка диспетчеров подключения

В случае возникновения ошибок, они будут выведены на консоль, дополнительно их можно просмотреть в лог-файле установки ***/opt/vdi-playbooks/logs/ansible.log***.

Если в процессе работы **Диспетчера подключений Базис.WorkPlace** потребуется перезапустить его службы, это можно сделать следующей командой:

```
systemctl restart vdi-broker
```

4. Добавление **Диспетчера подключений** в инфраструктуру **Базис.WorkPlace** производится через **Фронтенд Базис.WorkPlace** в разделе **Диспетчеры подключений**. Имя **Диспетчера подключений** должно совпадать с hostname **Диспетчера подключений** для успешной связи компонентов решения (***hostname -f***). Подробнее добавление **Диспетчера подключений** описано в **Руководстве администратора Базис.WorkPlace**.

> **Примечание**
>
> После регистрации диспетчера подключений в **Фронтенде Базис.WorkPlace**, службу диспетчера подключений необходимо перезапустить.

3.3.3 Подготовка Базис.vControl для работы со Базис.WorkPlace

Решения **Базис.vControl** и **Базис.WorkPlace** обладают общим интерфейсом (Web UI). Чтобы включить в **Базис.vControl** пользовательский интерфейс **Базис.WorkPlace**, необходимо после развертывания **Базис.WorkPlace** провести повторное развертывание **Бэкенда Базис.vControl** с дополнительными параметрами в конфигурационном файле ***vms-config***:

```
vdi_enable: true
vdi_api:
  - 'http://123.123.123.109'
```

```
vdi_redis_pass: 'RedisPassword'
vdi_redis_hosts:
  - '123.123.123.166'
  - '192.168.0.2'
  - '192.168.0.3'
```

где:

- ***vdi_enable*** — включение поддержки **Базис.WorkPlace**.
- ***vdi_api*** — список IP-адресов **Бэкенда/ов Базис.WorkPlace.**
- ***vdi_redis_pass*** - Пароль для доступа к Redis Базис.WorkPlace (параметр ***redis_pass*** в Базис.WorkPlace).
- ***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**.

Потери данных системы при повторном развертывании **Бэкенда Базис.vControl** не произойдет, однако следует проводить такое обновление в периоды обслуживания.

3.4 Установка в режиме высокой доступности (HA)

3.4.1 Общая информация

Для установки **Базис.WorkPlace** в отказоустойчивом режиме (HA) целевые серверы должны быть подготовлены аналогично не HA-режиму (см. раздел «Подготовка серверов для установки компонентов Базис.WorkPlace».

Этапы установки системы в HA-режиме:

1. Установка сервера развертывания (***vdi-deploy***), с которого будет происходить установка остальных компонентов (при помощи Ansible).
2. Установка кластера Redis (минимум три сервера).
3. Установка нескольких серверов с **Бэкендом Базис.WorkPlace**.
4. Установка нескольких **Диспетчеров подключений**.

> **Примечание**
>
> Для установки **Базис.vControl** в HA режиме может использоваться только внешний сервер PostgreSQL (параметр ***embeded_psql: false*** в конфигурационном файле).

> **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».

3.4.2 Подготовительные шаги

1. Скопируйте архив **vdi-deploy-X.tgz** на машину, которая будет использоваться в качестве сервера развертывания.
2. Распакуйте его:

```
tar -xf vdi-deploy-X.tgz
cd deploy
```

В процессе распаковки будет создана директория ***deploy/*** в которой будут содержаться конфигурационные файлы ****-config-example.***

3. Скопируйте или переименуйте все файлы ****config-example*** в ****-config***. Например:

```
cp vdi-config-example vdi-config
cp backends-hosts-example backends-hosts
cp broker-hosts-example broker-hosts
cp redis-hosts-example redis-hosts
```

4. Убедитесь, что на всех виртуальных машинах, где будут развернуты компоненты Базис.WorkPlace, примонтирован оригинальный образ установочного диска ОС Альт (подробнее этот процесс описан в разделе Подготовка серверов для установки компонентов Базис.WorkPlace).

   В большинстве случаев для этого будет необходимо запустить на мастер-ноде следующую команду:

```
prlctl set vdibm01 --device-set cdrom0 --image
/vstorage/stor1/vmprivate/altlinux-7.0.5-20170624-spt-x86_64-ru-
```

```
install-dvd5-official.iso --enable --connect
```

3.4.3 Установка сервера развертывания

Пример конфигурационного файла для сервера развертывания содержится в файле ***vdi-config-example*** архива ***vdi-deploy-X.tgz***. Сделайте на его основе реальный конфигурационный файл установки ***vdi-config***, скопировав или переименовав файл-пример ***vdi-config-example***. Чтобы обеспечить успешные установки при обновлении системы, после удачного развертывания рекомендуется сохранять ***vdi-config*** дополнительно, чтобы его можно было использовать повторно.

Пример содержимого конфигурационного файла ***vdi-config***:

```
vms_api_url: 'https://vms.local'
vms_user: 'UserName'
vms_password: 'vmsPassword'
vms_tls_verification: false

clickhouse_ip: 192.168.0.11
clickhouse_secure: false
clickhouse_tls_verification: false
clickhouse_cluster_name: vcontrol

embedded_pgsql: false
pgsql_vdi_db: 'vdidb'
pgsql_vdi_user: 'vdiremote'
pgsql_vdi_pass: 'vdiPassword'
pgsql_bind_port: '5432'
pgsql_bind_ip: '192.168.0.252'

# Необязательные параметры:
#pgsql_bind_ip_replicas:
# - '192.168.0.253'
# - '192.168.0.254'
#pgsql_bind_port_replicas: '5433'
#use_pgbouncer: false
#pgbouncer_auth_type: 'scram-sha-256'
#pgbouncer_auth_scram_secret: "SCRAM-SHA-
256$4096:ZJAsnmqlOhXer+NxITyIJw==$etLxHXQL5F8wb453z5s9j0rYa5s/pImW/YSo
vYNTIDE=:/2zTmWypfeyRjPMwIQdB5eRhI3T1vfJSH4drSrCJ/p8="

ntp_servers:
  - '192.168.0.254'
```

```
logs:
log_path: /var/log
  backend:
    save_last_days: 30
  broker:
    save_last_days: 30

ha_deploy: true

redis_on_backend: true
redis_pass: 'RedisPassword'

vm_agents_bind_host: 192.168.0.123

# Необязательные параметры:
#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'

#broker_cert: /tmp/broker.crt
#broker_key: /tmp/beroker.key

#keepalived on_backend: true
```

Описание параметров:

- ***stage*** — необязательный параметр, задает «имя» текущей установки, применяется для удобства отслеживания исключений в Sentry по конкретным установкам **Базис.WorkPlace**, может содержать английские буквы и цифры, тире, подчеркивание.
- ***vms_api_url*** — адрес пользовательского интерфейса (WEB UI) **Базис.vControl**.
- ***vms_user*** — имя пользователя в **Базис.vControl**, под которым **Базис.WorkPlace** будет подключаться к API **Базис.vControl**. Является отдельной технической учетной записью, занесенной в исключения политики паролей.
- ***vms_passwd*** — пароль пользователя, созданного при установке **Базис.vControl** (параметр **Пароль**).
- ***vms_tls_verification —*** проверять сертификат при подключении к API **Базис.vControl**. Если **Базис.vControl** используется с корректным сертификатом, необходимо использовать значение ***true***, если сертификат самоподписанный или не доверенный, значение должно быть ***false***.
- ***embedded_pgsql*** — производить ли установку локальной версии PostgreSQL на сервер, где будет установлен **Бэкенд Базис.WorkPlace.** При значении ***false*** система будет использовать параметры для подключения к внешней PostgreSQL. При значении ***true*** будет произведена локальная установка PostgreSQL из подключенного репозитория, а параметры ***pgsql_bind_port*** и ***pgsql_bind_ip*** будут

игнорироваться (прослушивается 127.0.0.1:5432). При установке в режиме отказоустойчивости поддерживает использование только внешней базы, параметр должен быть в ***false***. В случае использования внешнего сервера PostgreSQL базу создавать не нужно, при развертывании это будет сделано автоматически. Учетная запись для подключения к серверу должна обладать правами на создание базы.

Примечание

Максимальное количество одновременных подключений к БД (параметр ***max_connections*** в PostgreSQL) рассчитывается как:

120 * (кол-во Бэкенд-серверов) * (кол-во CPU на Бэкенд-сервере – 2)

где 120 — лимит подключений к БД на один процесс **Менеджера диспетчеров подключений.**

Итоговое значение не может быть больше 1500: в случае его превышения автоматически уменьшаются лимиты подключений к БД на один процесс Менеджера диспетчера подключений во время установки.

- ***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 (***embeded_pgsql: true***), и для использования внешнего сервера PostgreSQL так, как в систему ставится клиент PostgreSQL. По умолчанию ставится:

- Для Astra Linux: Postgres 9.6 из установочного диска ОС.
- Для Альт 8.1: 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.

- ***use_pgbouncer*** — использовать pgbouncer для доступа к postgresql. В этом режиме на каждый бэкенд будет установлен pgbouncer, и 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 Workplace 1500) будут равномерно распределены по каждому pgbouncery на каждом бэкенде (при трех бэкендах получаем 1500/3, т.е. по 500 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.

> **Примечание**
>
> Пример получения содержимого переменной pgbouncer_auth_scram_secret для пользователя 'ПОЛЬЗОВАТЕЛЬ' из базы на сервере postgresq. Запускается из подсистемной учетной записи postgres:
>
> ```
> psql -Atq -d postgres -c "SELECT passwd FROM pg_shadow
> where usename='ПОЛЬЗОВАТЕЛЬ';"
> ```

- ***ntp_servers*** — список NTP-серверов, необязательный параметр. Включает синхронизацию времени на всех серверах (**Бэкенд Базис.WorkPlace** и **Диспетчеров подключений**) с заданными NTP-серверами с использованием ntpd/chronyd.

> **Осторожно**
>
> Если параметр ***ntp_servers*** не указан, то системный администратор должен сам настроить NTP и обеспечить синхронизацию времени между всеми компонентами системы.

- ***logs*** — секция настройки параметров ротации лог-файлов;
- ***log_path*** — параметр устанавливает общий путь для хранения всех логов;
- ***logs.backend.save_last_days*** — количество дней, втечение которого хранятся
- лог-файлы **Бэкенда Базис.WorkPlace/Менеджера диспетчеров подключений**. Ротация лог-файлов происходит каждый день, каждый предыдущий день архивируется. Лог-файлы старше указанного количества дней удаляются из файловой системы.
- ***logs.broker.save_last_days*** — количество дней, в течении которого хранятся лог-файлы **Диспетчера подключений**. Ротация лог-файлов происходит каждый день, каждый предыдущий день архивируется. Лог-файлы старше указанного количества дней удаляются из файловой системы;
- ***clickhouse_ip*** — адрес, значение которого зависит от типа развертывания **Базис.vControl**:

  - в HA режиме это VIP адрес ClickHouse **Базис.vControl** (параметр ***vips.clickhouse*** в **Базис.vControl**);
  - в non-HA режиме это адрес сервера **Бэкенда Базис.vControl**.

- ***clickhouse_secure*** — использование шифрованного соединения tls/ssl для взаимодействия с компонентами ClickHouse.

  По умолчанию: false.

- ***clickhouse_tls_verification*** — проверка сертификата, предоставляемого третьей стороной, при подключении к внешнему кластеру Clickhouse. Предполагается, что необходимый корневой сертификат уже установлен в операционной системе в хранилище сертификатов по умолчанию. Актуально при clickhouse_secure: true.

  По умолчанию: false.

> **Примечание**
>
> ВАЖНО настроить соответствующий порт для ssl/tls, по умолчанию 9440.

- ***clickhouse_cluster_name* —** имя ClickHouse кластера, в котором нужно создавать реплицированные таблицы.

  По умолчанию: vcontrol.

- ***ha_deploy*** — установка в режиме отказоустойчивости, при установке в HA-конфигурации должно быть в ***true***;
- ***redis_on_backend*** — Redis-кластер будет располагаться на серверах **Бэкенда Базис.WorkPlace**, при этом файл ***redis-hosts*** игнорируется, и установка идет на серверы из файла ***backends-hosts***;
- ***redis_pass*** — пароль доступа к Redis.

> **Примечание**
>
> Пароль, указанный в качестве значения параметра ***redis_pass***, используется так же для аутентификации в ***redis-sentinel***.

- ***vm_agents_bind_host*** — IP-адрес, используемый для связи с ВС Агентами.

Примечание

Данный параметр является опциональным при установке **Бэкенда Базис.WorkPlace**, но является обязательным, если требуется подключение функциональности для работы с физическими ПК в **Базис.WorkPlace**.

Если на **Бэкенде** всего один IP-интерфейс, то будет использоваться заданное в параметре значение, либо будет прописан адрес, через который идет шлюз по умолчанию (default gw) на системе. Если значение не указано, а IP-интерфейсов на **Бэкенде** несколько, то при установке возникнет ошибка.

Параметр также может быть задан на конкретный **Бэкенд** через конфигурационный файл ***backends-hosts***.

- ***broker_cert*** — опциональный параметр; путь к сертификату для **Диспетчера подключений** в pem формате. Может быть задано на конкретный **Диспетчер подключений** в ***broker-hosts***;
- ***broker_key*** — опциональный параметр; путь к секретному ключу (rsa/gost) сертификата для **Диспетчера подключений** в pem формате. Может быть задано на конкретный **Диспетчер подключений** в ***broker-hosts***.

Совет

Через ***broker-hosts*** можно переопределить параметры ***broker_cert*** и ***broker_key*** на конкретный **Диспетчер подключений**. Пример:

```
node1 ansible_user=root ansible_host=192.168.0.18
ansible_ssh_private_key_file='/tmp/key'
broker_in_ip_for_client=192.168.0.18
broker_out_ip_to_vm=192.168.0.18
broker_out_ip_to_backend=192.168.0.18
broker_cert=/tmp/broker2.crt
broker_key=/tmp/broker2.key
```

Если для конкретного **Диспетчера подключений** или в ***vdi-config*** параметры ***broker_cert*** и ***broker_key*** не определены, то генерируется один самоподписанный сертификат для всех **Диспетчеров подключений**, для которых эти параметры не определены.

Если параметры ***broker_cert*** и ***broker_key*** определены в ***vdi-config*** или на хост в ***broker-hosts***, то используются сертификат и ключ из них.

- ***broker_cert_key_type*** — опциональный параметр; тип ключа для подписи сертификата: rsa или gost. Параметр нужен только для генерации самоподписанного сертификата, если явно передан сертификат в ***broker_cert***, то его тип определится автоматически.
- ***broker_cert_key_bit*** — опциональный параметр; битность ключа для подписи сертификата при генерации самоподписанного сертификата:
  - ***broker_cert_key_bit.rsa*** — для rsa ключа;
  - ***broker_cert_key_bit.gost*** — для gost ключа.
- ***keepalived_on_backend*** — необязательный параметр, отвечает за установку сервиса keepalived на хостах Бэкенда.

  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 протокола VRRP для доступа к хостам **Бэкенда Базис.WorkPlace**:
  - ***vips.backend.vip*** — виртуальный IP-адрес для **Бэкенда Базис.WorkPlace**, который будет перемещаться, если хост выйдет из строя;
  - ***vips.backend.vrouter_id*** — идентификационный номер VRRP-роутера, который должен задаваться целым числом от 0 до 255 и быть уникальным в рамках L2-сети.
- ***snmp_agent_deploy*** — для установки SNMP Агента при развертывании **Бэкенда Базис.WorkPlace** параметр должен иметь значение ***true***, в противном случае – ***false***.

> **Примечание**
>
> Чтобы при развертывании **Бэкендов Базис.WorkPlace** одновременно была выполнена установка их SNMP Агентов, сконфигурируйте параметры в файле ***vdi-config***, как описано в разделе Установка SNMP Агента.

> **Примечание**
>
> Файл конфигурации имеет YAML-формат, правила описания параметров представлены в разделе Правила редактирования конфигурационных файлов.

Шаги для установки **Сервера развертывания:**

1. При необходимости, поправьте параметры в ***vdi-config***, как указано выше.
2. Если произошла смена IP адреса **Сервера развертывания**, то перед развертыванием **Бэкендов** необходимо на хостах **Бэкендов** выполнить:

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

3. Установите **Сервер развертывания** следующей командой с указанием пути к файлу с парольной фразой в обязательном параметре ***-v***:

> **Примечание**
>
> Файл с парольной фразой — это текстовый файл, в котором открытым текстом записывается парольная фраза.

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

> **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».

По итогам выполнения команды **Сервер развертывания** будет установлен на текущий сервер.

Пример успешного завершения операции развертывания **Сервера развертывания Базис.WorkPlace** (рисунок 3.33):

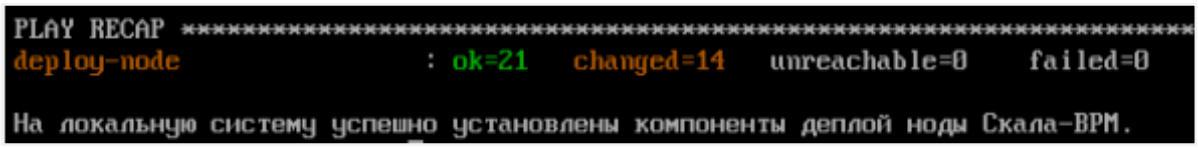

Рисунок 3.33 Пример успешного развертывания Сервера развертывания Базис.WorkPlace

3.4.4 Установка кластера Redis

Пример конфигурационного файла для установки кластера Redis содержится в файле ***redis-hosts-example*** архива ***vdi-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=123.123.123.125
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.WorkPlace** 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.WorkPlace** (параметры ***redis_on_backend: true*** в конфигурационном файле ***vdi-config***), то верно следующее:

- Redis-кластер будет располагаться на серверах **Бэкенда Базис.WorkPlace**;
- 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-vdi.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 3.34):

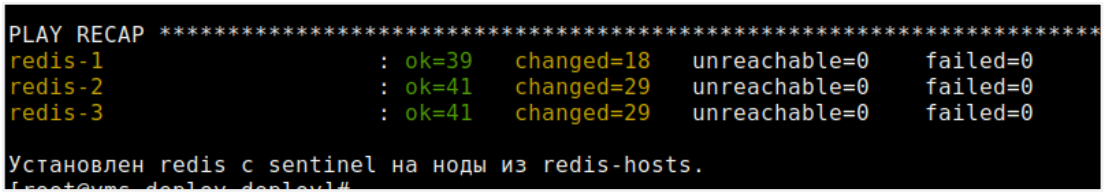

Рисунок 3.34 Сообщение при успешной установке Redis-кластера

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

3.4.5 Установка нескольких серверов Бэкенда Базис.WorkPlace

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

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

```
[vdi-backends]
backend-1 ansible_user=root ansible_host=123.123.123.123
ansible_ssh_pass='AnsiblePassword' bm_bind_host='192.168.0.1'
backend-2 ansible_user=root ansible_host=123.123.123.124
ansible_ssh_pass='AnsiblePassword' bm_bind_host='192.168.0.1'
backend-3 ansible_user=root ansible_host=123.123.123.125
ansible_ssh_pass='AnsiblePassword' bm_bind_host='192.168.0.1'
```

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.
- ***bm_bind_host*** (необязательный параметр) — IP-адрес, который будет использоваться **Менеджером диспетчеров подключений** для запросов от **Диспетчеров подключений**, других **Менеджеров диспетчеров подключений** и **API-бэкендов**.

- **bm_per_host_count** (необязательный параметр) — количество **Менеджеров диспетчеров подключений**, которые будут запущены на хосте.

Примечание

Если необходимо изменить какой-либо внутренний параметр **Базис.WorkPlace**, который не содержится в ***vdi-config***, то его необходимо прописать в файл переопределений ***backend-overrides***. Файл имеет YAML-формат, правила описания параметров представлены в разделе Правила редактирования конфигурационных файлов. Все, что было переопределено в ***backend-overrides,*** добавится в ***/etc/vdi.yaml***. Переопределять можно все параметры, которые описаны в документации. Прописывать нужно в том виде, как они прописаны в соответствующих конфигурационных файлах в RPM.

Примечание

Напрямую править конфигурационные файлы в ***/etc/vdi*.yaml*** или в составе RPM нельзя, они будут перезаписаны при следующем обновлении. Если необходимо внести дополнительные параметры в конфигурацию после того, как **Бэкенд Базис.WorkPlace** был установлен, нужно внести эти параметры в backend-overrides и переустановить **Бэкенд Базис.WorkPlace**. Для обнуления ранее прописанных переопределений нужно выполнить переустановку **Бэкенда Базис.WorkPlace** с пустым ***backend-overrides***.

Шаги для установки **Бэкендов Базис.WorkPlace**:

1. При необходимости, поправьте параметры в ***backends-hosts*** как указано выше.
2. Установите **Бэкенды**, выполнив следующую команду:

```
./deploy.sh -b -a environment-vdi.tgz -w vdi-agent-updates.tar.gz
```

> **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.WorkPlace**. При успешной установке будет выведено соответствующее сообщение с версиями установленных RPM-пакетов с компонентами (рисунок 3.35):

```
PLAY RECAP *********************************************************************
backend-1                  : ok=78   changed=23   unreachable=0    failed=0
backend-2                  : ok=72   changed=21   unreachable=0    failed=0
backend-3                  : ok=72   changed=21   unreachable=0    failed=0

Скала-Р BPM успешно установлен.
Версии установленных компонетов:
vdi-broker:
  version:1.16.2 build:34 Пт 15 июн 2018 14:56:38
vdi-backend:
  version:1.16.2 build:35 Пт 15 июн 2018 14:57:32
vdi-playbooks:
  version:1.16.2 build:30 Пт 15 июн 2018 14:57:10
```

Рисунок 3.35 Сообщение при успешной установке Базис.WorkPlace

В случае возникновения ошибок они будут выведены на консоль, дополнительно их можно просмотреть в лог-файле установки ***/opt/vdi-playbooks/logs/ansible.log***.

3.4.6 Установка диспетчеров подключений

> **Осторожно**
>
> При установке **Диспетчеров подключений** на Альт 9 должны быть подключены официальные репозитории для этой ОС из интернета.

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

В файле ***broker-hosts*** описываются серверы, на которые будет установлены **Диспетчеры подключений** и параметры SSH-подключения к ним д ля автоматической установки **Диспетчеров** через Ansible. Например:

```
[vdi-brokers]
broker_name1 ansible_user=root ansible_host=123.123.123.123
ansible_ssh_private_key_file='/tmp/key'
broker_in_ip_for_client=123.123.123.123
broker_out_ip_to_vm=123.123.123.123
broker_out_ip_to_backend=123.123.123.123
broker_name2 ansible_user=root ansible_host=123.123.123.175
ansible_ssh_pass='AnsiblePassword'
broker_in_ip_for_client=123.123.123.125
broker_out_ip_to_vm=123.123.123.125
broker_out_ip_to_backend=123.123.123.125
```

Описание параметров:

- ***broker_name*** — имя сервера.
- ***ansible_user*** — имя пользователя целевого сервера (где будет развернут **Диспетчер**) с правами root.
- ***ansible_host*** — IP-адрес целевого сервера (где будет развернут **Диспетчер**).
- ***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.
- ***broker_in_ip_for_client*** **—** IP-адрес, к которому будут подключаться **Клиенты Базис.WorkPlace**.
- ***broker_out_ip_to_vm*** **—** IP-адрес, с которого **Диспетчер подключений** подключается к виртуальным машинам рабочих столов.
- ***broker_out_ip_to_backend*** **—** IP-адрес, с которого **Диспетчер подключений** соединяется с **Менеджером диспетчеров подключений**.
- ***default_broker_manager*** (необязательный параметр) — IP-адрес и порт основного **Менеджера диспетчеров подключений** в составе **Бэкенда Базис.WorkPlace**, к которому подключается **Диспетчер подключений** и получает список всех зарегистрированных **Менеджеров диспетчеров подключений** (discovery). Изменяйте его только если вы хорошо понимаете, зачем это необходимо.
- ***preferred_managers*** (необязательный параметр) — список IP-адресов и портов дополнительных предпочтительных **Менеджеров диспетчеров подключений**. Изменяйте его только если вы хорошо понимаете, зачем это необходимо.
- ***connect_to_discovered_managers*** (необязательный параметр) — означает, что **Диспетчер подключений** будет подключаться к **Менеджерам диспетчеров подключений**, которые были обнаружены в ходе процедуры обнаружения (discovery) и получены от основного **Менеджера диспетчеров подключений** (***default_broker_manager***) либо от дополнительных (***preferred_managers***). В такой

конфигурации при отключении основного и всех дополнительных менеджеров **Диспетчер подключений** будет подключен к резервным, соответственно останется работоспособным. Изменяйте этот параметр только если вы хорошо понимаете, зачем это необходимо.

Примечание

Если необходимо изменить какой-либо внутренний параметр **Базис.WorkPlace Диспетчер подключений**, который не содержится в ***vdi-config***, то необходимо прописать в файл переопределений ***broker-overrides***. Файл имеет YAML-формат, правила описания параметров представлены в разделе Правила редактирования конфигурационных файлов. Все, что переопределено в ***broker-overrides***, добавится в ***/etc/vdi-broker.yaml***. Переопределять можно все параметры, которые описаны в документации. Прописывать их нужно в том виде, как они прописаны в соответствующих конфигурационных файлах в RPM.

Примечание

Напрямую править конфигурационные файлы в ***/etc/vdi-broker-*.yaml*** или в составе RPM нельзя; они будут перезаписаны при следующем обновлении. Если необходимо внести дополнительные параметры в конфигурацию после того как **Диспетчеры подключений** были установлены, нужно внести параметры в ***broker-overrides*** и переустановить **Диспетчеры подключений**. Для обнуления ранее прописанных переопределений нужно выполнить переустановку **Диспетчеров подключений** с пустым ***broker-overrides***.

Рекомендуется, чтобы файл ***broker-hosts*** со списком диспетчеров подключений содержал те же имена серверов, что и реальные имена хостов и названия серверов, которые будут использованы для добавления в **Базис.WorkPlace** через **Фронтенд Базис.vControl**.

Шаги для установки Сервера развертывания:

1. При необходимости, поправьте параметры в ***broker-hosts***, как указано выше.
2. Установите **Диспетчеры подключений**, выполнив следующую команду:

```
./deploy.sh -e -a environment-vdi.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».

В случае если требуется включить возможность скачивания дистрибутивов **Клиента Базис.WorkPlace** через браузер с **Диспетчера подключений**, то в команде через параметр ***-c*** укажите файл, содержащий набор пакетов **Клиента Базис.WorkPlace** для всех поддерживаемых платформ:

```
./deploy.sh -e -a environment-vdi.tgz -c vdi-client.tar.gz
```

Критерием удачной установки диспетчеров подключения является сообщение (рисунок 3.32):

```
PLAY RECAP *********************************************************************
backend                    : ok=1    changed=0    unreachable=0    failed=0
node1                      : ok=45   changed=20   unreachable=0    failed=0

Диспетчер подключений Скала-Р BPM успешно установлен.
Версии установленных компонетов:
vdi-broker:
  version:1.16.2 build:35 Пт 15 июн 2018 15:21:43
[root@dev-deploy-vdi-backend deploy]#
```

Рисунок 3.32 Сообщение об успешной установке диспетчеров подключения

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

Если в процессе работы **Диспетчера подключений Базис.WorkPlace** потребуется перезапустить его службы, это можно сделать следующей командой:

```
systemctl restart vdi-broker
```

3. Добавьте все установленные **Диспетчеры подключений** в инфраструктуру **Базис.WorkPlace** через **Фронтенд Базис.WorkPlace** в разделе **Диспетчеры подключений**. Имя **Диспетчера подключений** должно совпадать с hostname **Диспетчера подключений** для успешной связи компонентов решения (***hostname -f***). Подробнее добавление **Диспетчера подключений** описано в **Руководстве администратора Базис.WorkPlace**. Этот шаг возможен только после активации Фронтенда Базис.WorkPlace, см. соответствующий раздел.

3.4.7 Подготовка Базис.vControl для работы с Базис.WorkPlace

Решения **Базис.vControl** и **Базис.WorkPlace** обладают общим интерфейсом (Web UI). Чтобы включить в **Базис.vControl** пользовательский интерфейс **Базис.WorkPlace**, необходимо после развертывания **Базис.WorkPlace** провести повторное развертывание **Бэкенда Базис.vControl** с дополнительными параметрами в конфигурационном файле ***vms-config***:

```
vdi_enable: true
vdi_api:
  - 'http://123.123.123.109'
  - 'http://123.123.123.110'
  - 'http://123.123.123.111'
vdi_redis_pass: 'RedisPassword'
vdi_redis_hosts:
  - 'http://123.123.123.100'
  - 'http://123.123.123.9'
  - 'http://123.123.123.98'
```

где:

- ***vdi_enable*** – включение поддержки **Базис.WorkPlace.**
- ***vdi_api*** — список IP-адресов **Бэкенда/ов Базис.WorkPlace.**
- ***vdi_redis_pass*** - Пароль для доступа к Redis Базис.WorkPlace (параметр ***redis_pass*** в Базис.WorkPlace).
- **vdi_redis_host** - список IP-адресов серверов, на которых установлен Redis для Базис.WorkPlace, в случае если при установке ВРМ использовался параметр ***redis_on_backend: true***, то данный список аналогичен списку IP-адресов ВРМ **Бэкенда/ов Базис.WorkPlace.**

Потери данных системы при повторном развертывании **Бэкенда Базис.vControl** не произойдет, однако следует проводить такое обновление в периоды обслуживания.

За инструкциями по переустановке **Бэкенда Базис.vControl** обратитесь в документ **«Руководство по установке Базис.vControl»**.

3.5 Общая установка и настройка системы

3.5.1 Установка Агента Базис.WorkPlace

Установка Агента описана в документе «Базис.WorkPlace. Руководство администратора».

3.5.2 Настройка Базис.WorkPlace для работы

После того как были установлены и настроены **Бэкенд Базис.WorkPlace, Диспетчеры подключений**, а также **Фронтенд Базис.WorkPlace* (в составе**Базис.vControl**), появляется возможность подключиться к веб-интерфейсу для продолжения настройки решения.

3.5.3 Вход в веб-интерфейс Базис.vControl

Для начала работы Администратор должен выполнить вход на странице **Базис.vControl** в браузере (рисунок 3.33). Для этого Администратор должен ввести логин и пароль и нажать кнопку **Войти**. Чтобы система запомнила авторизацию пользователя, необходимо поставить галочку для опции *Запомнить меня*.

Примечание

Время хранения авторизационной сессии на портале настраивается в соответствии с документацией **Базис.vControl**.

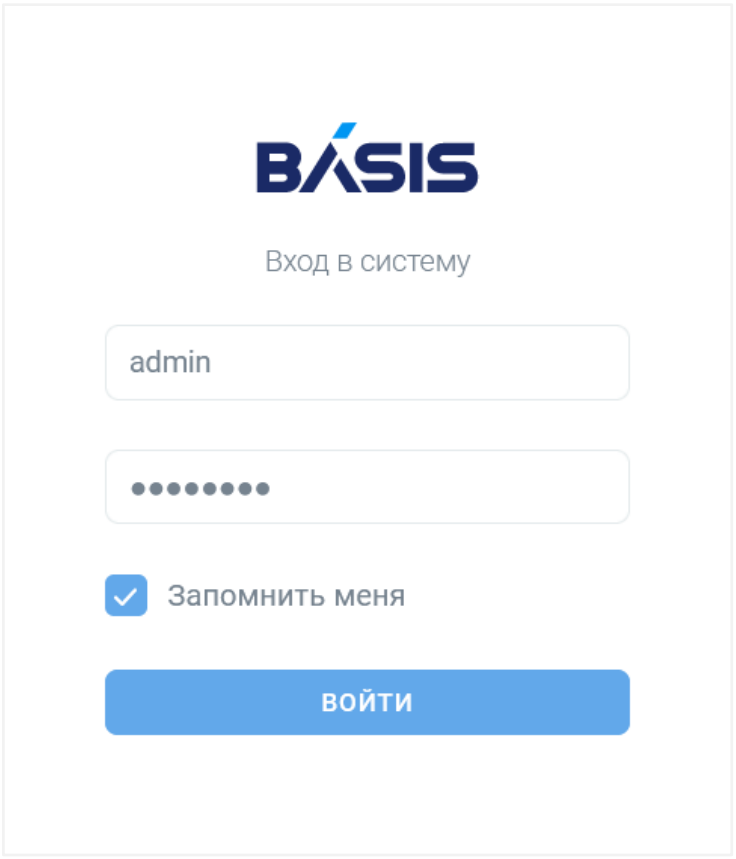

Рисунок 3.33 Форма входа в систему

Администратор **Базис.vControl** может предоставлять другим администраторам права и привилегии определенного уровня (описано в **Руководстве администратора Базис.WorkPlace**) для управления инфраструктурой **Базис.WorkPlace**.

Интерфейс **Базис.WorkPlace** (рисунок 3.34) предоставляет интуитивно понятную систему навигации, с помощью которой Администратор может быстро выполнять различные задачи.

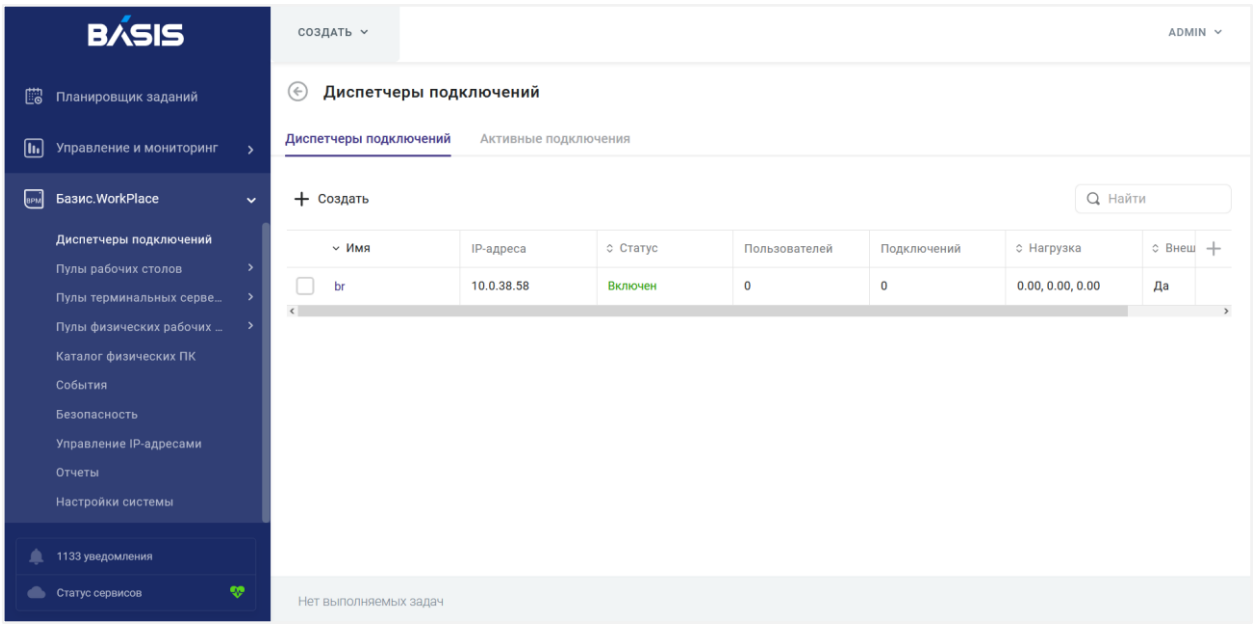

Рисунок 3.34 Пользовательский интерфейс Базис.WorkPlace

3.5.4 Подключение к Диспетчеру подключений

Подключение **Диспетчера подключений** к инфраструктуре решения **Базис.WorkPlace** описано в документе **Базис.WorkPlace. Руководство администратора.**

Примечание

После подключения **Диспетчера подключений** его следует перезагрузить, чтобы успешно инициализировать в **Бэкенде Базис.WorkPlace.**

3.5.5 Подключение к домену

Базис.WorkPlace может использовать в качестве каталога учетных записей внешнюю систему.

Способ настройки подключения к внешнему каталогу учетных записей подробно изложен в документе **Базис.WorkPlace. Руководство администратора**.

3.5.6 Настройка безопасного соединения между компонентами решения

3.5.6.1 Настройка безопасного соединения между Бэкендом Базис.WorkPlace и базой данных

Защищенное взаимодействие **Бэкенда Базис.WorkPlace** с базой данных PostgreSQL не предусмотрено. Необходимо самостоятельно обеспечить безопасность каналов связи между бэкендом систем и БД.

3.5.6.2 Настройка безопасного соединения между Бэкендом Базис.WorkPlace и Active Directory/LDAP

Допускается использование подключения к MS Active Directory и LDAP с использованием безопасного протокола LDAPS. Для этого необходимо указать SSL-порт в коннекторе к AD и указать данный параметр в конфигурационном файле **Бэкенда Базис.WorkPlace**.

Примечание

Сертификат, используемый при работе с LDAPS, дополнительно не проверяется и используется только для шифрования передаваемых данных.

В случае подключения нескольких независимых каталогов указание SSL-порта в коннекторе к AD и внесение данного параметра в конфигурационном файле осуществляется для каждого каталога.

3.5.6.3 Настройка безопасного соединения между Бэкендом Базис.WorkPlace и Диспетчером подключений

Настройка безопасного соединения между **Бэкендом Базис.WorkPlace** и **Диспетчером подключений** не предусмотрена, однако есть возможность организовать изоляцию передаваемых данных, если организовать взаимодействие через выделенную сеть. Для этого необходимо создать дополнительную сеть, которая будет доступна для **Диспетчера подключений** и **Бэкенда Базис.WorkPlace**.

3.5.6.4 Настройка безопасного соединения между Диспетчером подключений и Клиентом Базис.WorkPlace

Соединение между **Диспетчером подключений** и клиентским приложением производится при помощи TLS. По умолчанию используется шифрование RSA с длиной ключа 1024 бит, но опционально можно подключить свои ключи и сертификаты, сгенерированные по стандарту ГОСТ (как в клиенте, так и в диспетчере подключений).

В **Базис.WorkPlace** реализована процедура автоматического прекращения текущей сессии пользователя BPM для предотвращения получения злоумышленником доступа к рабочему столу в период физического отсутствия пользователя BPM у устройства доступа. Разрыв соединения происходит после превышения таймаута неактивности

пользователя. Значение таймаута задается администратором в параметре ***broker_manager.vdi_client.inactive_timeout***. Параметр может быть изменен либо в веб-интерфейсе **Базис.WorkPlace** в разделе *Настройки системы → Клиенты BPM*, либо в файле переопределений ***backend-overrides*** с последующей переустановкой **Менеджера диспетчеров подключений**.

```
broker_manager:
  # Клиенты BPM
  vdi_client:
    # Таймаут неактивности Клиента Базис.WorkPlace, по прошествии
которого он должен отключиться от Диспетчера подключения.
    inactive_timeout: 300
```

4. ОБНОВЛЕНИЕ БАЗИС.WORKPLACE

Обновление компонентов **Базис.WorkPlace** производится тем же способом, что и установка. При обновлении решения в НА-режиме производятся действия, аналогичные установке всех компонентов решения с сохранением конфигурационных файлов предыдущего развертывания. При этом, если в примечаниях к новой версии решения не оговорено иного, обновление кластера Redis не производится.

4.1 Обновление сервера развертывания

Перед обновлением необходимо сравнить текущие конфигурационные файлы и примеры, при обнаружении новых параметров следует добавить их в текущий конфигурационный файл.

Обновление **Сервера развертывания** необходимо только в случае использования **Базис.WorkPlace** в отказоустойчивом варианте. Обновление происходит через установку новой версии из ***vdi-deploy-X.tgz*** поверх старой версии с сохранением всех конфигурационных файлов (***vdi-config, *-hosts, *-overrides***). В процессе обновления система не должна использоваться.

4.2 Обновление Бэкенда Базис.WorkPlace

Перед обновлением необходимо сравнить текущие конфигурационные файлы и примеры, при обнаружении новых параметров следует добавить их в текущий конфигурационный файл.

Обновление происходит через установку новой версии из ***vdi-deploy-X.tgz*** поверх старой версии с сохранением всех конфигурационных файлов (***vdi-config, *-hosts, *-overrides***). В процессе обновления система не должна использоваться (см. **Базис.vControl. Руководство администратора**). В случае, если необходимо использовать дополнительные параметры конфигурационного файла **Бэкенда Базис.WorkPlace**, эти параметры следует вносить в файл ***backend-overrides*** комплекта установки. Это обеспечит сохранение параметров при переустановке и обновлении решения.

4.3 Обновление Диспетчера подключений Базис.WorkPlace

Перед обновлением необходимо сравнить текущие конфигурационные файлы и примеры, при обнаружении новых параметров следует добавить их в текущий конфигурационный файл.

Обновление происходит через установку новой версии из ***vdi-deploy-X.tgz*** поверх старой версии с сохранением всех конфигурационных файлов (***vdi-config, *-hosts, *-overrides***).

При обновлении система не должна использоваться (см. **Базис.vControl. Руководство администратора**). В случае если необходимо использовать дополнительные параметры конфигурационного файла диспетчера подключений **Базис.WorkPlace**, эти параметры следует вносить в файл ***broker-overrides***. Это обеспечит сохранение параметров при переустановке и обновлении решения.

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.

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.

external_virtualization - параметр конфигурационного файла vms-config, отвечающий за использование ClickHouse как внешнего сервиса, выставление этого параметра в значение true означает использование внешнего кластера ClickHouse.

4.4 Обновление Клиента Базис.WorkPlace

4.4.1 Windows

Обновление **Клиента Базис.WorkPlace** производится аналогично его установке. Никаких дополнительных действий при обновлении приложения не требуется. Обновление приложения может быть произведено внешними средствами автоматизации.

4.4.2 Linux

Обновление Клиента Базис.WorkPlace производится аналогично его установке. Никаких дополнительных действий при обновлении приложения не требуется.

4.5 Обновление Агента Базис.WorkPlace

Пакеты обновления **Агентов Базис.WorkPlace** выдаются вместе с релизом в файле ***vdi-agent-updates.tar.gz***. Чтобы они попали на **Бэкенд BPM** хоста нужно скрипту установки ***deploy.sh*** передать файл через флаг ***-w***. В параметре ***-v*** указывается путь к файлу с парольной фразой, он является обязательным при развертывании **Бэкенда BPM** в обычном режиме.

```
./deploy.sh -b -a environment-vdi.tgz -w vdi-agent-updates.tar.gz
./deploy.sh -s -a environment-vdi.tgz -w vdi-agent-updates.tar.gz -v
/path/to/vault-password-file
```

Осторожно

Параметр ***-w*** является обязательным для скрипта установки, если он запускается для развертывания **Бэкендов BPM** с флагом ***-s*** (обычный режим) или ***-b*** (HA-режим).

Установка **Бэкенда Базис.WorkPlace** в не-HA режиме 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 обновление выполняется от непривилегированного пользователя, которому доступно sudo без пароля. Если обновление идет при прямом доступе в консоль (не через ssh), то во время логина пользователя ***integrity level*** должен быть выбран «63».

5. ПРИЛОЖЕНИЕ

5.1 Поддержка зашифрованных параметров в конфигурации Базис.WorkPlace

Базис.WorkPlace поддерживает шифрование данных подключения и паролей, которые хранятся на хостах в конфигурационных файлах системы. К этим данным относятся:

- пароли для подключения к серверу Redis;
- пароли для подключения к базе данных;
- пароли 'ldap_settings'.

Шифрование данных настраивается при установке компонентов системы и выполняется с помощью механизмов Ansible Vault. На этом этапе 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.WorkPlace** производить из-под отдельной учетной записи с необходимыми правами администратора.
- Конфигурационные параметры 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***. Установка компонентов системы подробно описана в разделах Установка Бэкенда Базис.WorkPlace (не-НА режим) и Установка Сервера развертывания (НА режим).

Примечание

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

5.1.1 Смена парольной фразы

Осторожно

Парольную фразу можно менять только в рамках одной и той же версии системы **Базис.WorkPlace**. 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***:

- Для переразвертывания **Бэкендов Базис.WorkPlace** в не-HA режиме следует выполнить команду:

```
./deploy.sh -s -a environment-vdi.tgz -w vdi-agent-updates.tar.gz
-v /path/to/vault-password-file
```

Осторожно

Установка **Бэкенда Базис.WorkPlace** 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 HA режиме следует сначала обновить парольную фразу на **Сервере развертывания**, а потом обновить **Бэкенды Базис.WorkPlace**:

```
./deploy.sh -i -a environment-vdi.tgz -v /path/to/vault-password-
file
./deploy.sh -b -a environment-vdi.tgz -w vdi-agent-updates.tar.gz
```

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».

5.2 Использование Syslog

5.2.1 Включение встроенного Syslog-сервера на 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 recieved with -r.
#
# See syslogd(8) for more details.
SYSLOGD_OPTIONS='-u syslogd -j /var/resolv -r'
```

2. Перезапустите syslogd:

```
systemctl restart syslogd
```

5.2.2 Включение встроенного Syslog-сервера на 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
```

5.2.3 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 *Базис.WorkPlace → События → Журнал операций* и *Базис.WorkPlace → События → Журнал аудита*, выполните следующие шаги:

1. В боковом меню перейдите в раздел *Базис.WorkPlace → Настройки системы*.
2. Найдите секцию *Отправка нотификаций*.
3. Укажите в параметрах значения хоста и порта syslog-сервера:
   - **broker_manager.periodic.send_events_notifications.syslog_settings.host** — хост syslog-сервера для событий;
   - **broker_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 **broker_manager.periodic.send_events_notifications.period** и по умолчанию равен 5 минутам.

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

- **broker_manager.periodic.send_events_notifications.events_per_message** - количество обрабатываемых за раз событий.
- **broker_manager.periodic.send_events_notifications.syslog_settings.vendor** - значение поля vendor для отправляемых событий.
- **broker_manager.periodic.send_events_notifications.syslog_settings.product** - значение поля product для отправляемых событий.
- **broker_manager.periodic.send_events_notifications.syslog_settings.cef_version** - значение поля cef_version для отправляемых событий.

- **broker_manager.periodic.send_events_notifications.syslog_settings.preferred_language** - язык для событий.
- **broker_manager.periodic.send_events_notifications.max_event_age** - события старше, чем это количество секунд, не будут обрабатываться.

Внутренние события и сообщения **Бэкенда Базис.WorkPlace** и **Диспетчеров подключений Базис.WorkPlace** 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 *Базис.WorkPlace → 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.WorkPlace**, 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.

5.2.4 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 первоначальной установке или решении каких-то сложных технических проблем.

Для изменения уровня логирования необходимо добавить в файл конфигурации ***vdi-config*** параметр:

```
log_level: DEBUG
```

5.3 Справочник по параметрам конфигурации системы

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

- Указать новые значения параметров в разделе *Настройки системы*.
- Вручную внести изменения в файлы конфигурации ***vdi-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.

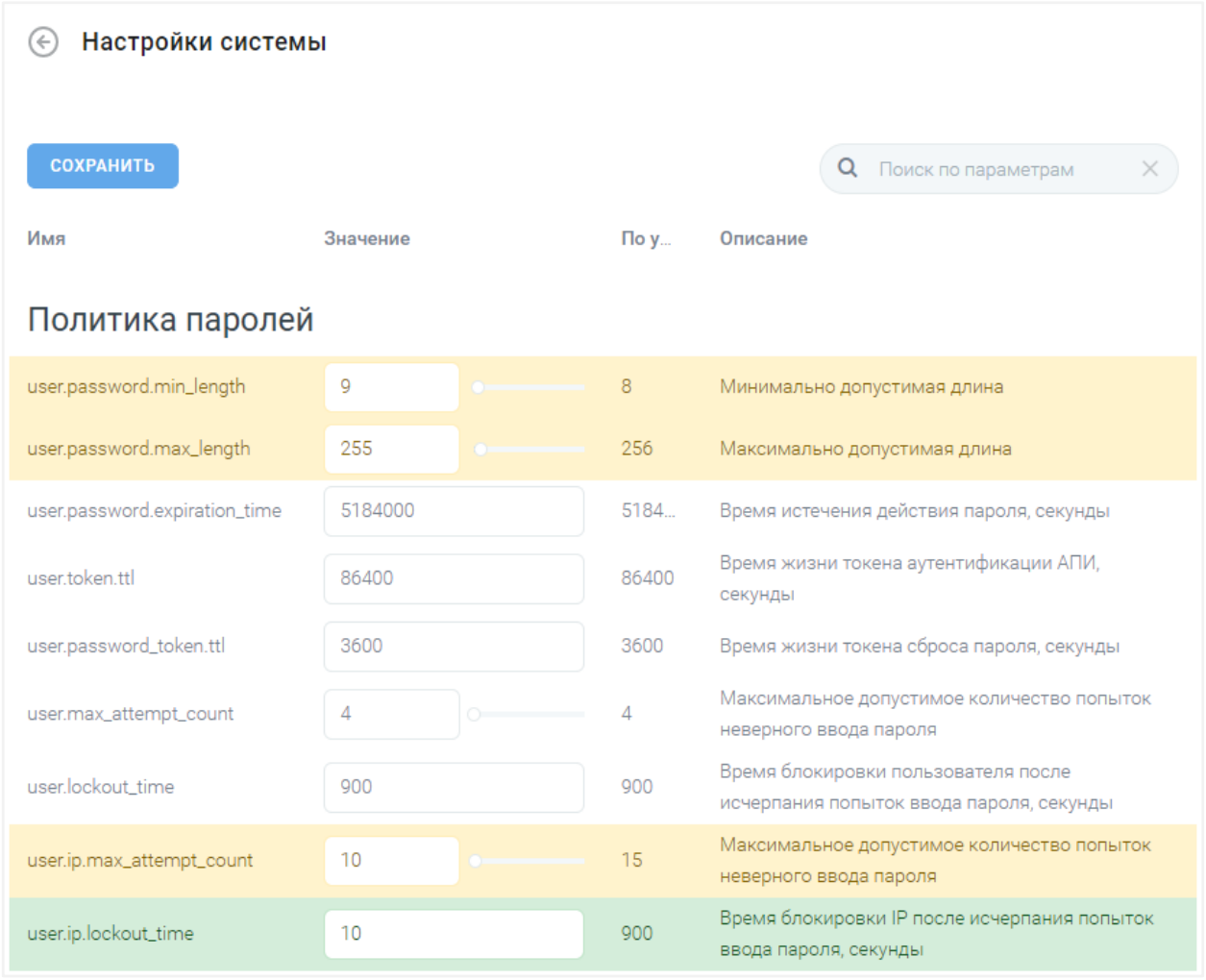

Рисунок 5.1 Общий вид раздела «Настройки системы»

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

- **Имя** — наименование параметра в рамках **Базис.WorkPlace**.
- **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 **Диспетчеров подключений**, то эти изменения отправляются на все диспетчеры подключений и записываются в файле ***/etc/vdi-broker-from-db.yaml***.
- Сервисы **Бэкенда Базис.WorkPlace** 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:

- **vdi-config** — основной файл для настройки конфигурации **Базис.WorkPlace**.
- **backend-overrides** — файл для переопределения значений дополнительных параметров системы, не содержащихся в ***vdi-config***. Переопределять можно все параметры из описанных ниже разделов.

Примечание

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

5.3.1 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 ***broker_manager.periodic.export_db_logs.enabled***:

```
broker_manager:
  periodic:
    export_db_logs:
      enabled: true
```

5.3.2 Описание параметров конфигурации для Бэкенда Базис.WorkPlace

Совет

Правила описания параметров в YAML-формате представлены в разделе Правила редактирования конфигурационных файлов.

Примечание

Полный список параметров с описанием представлен в разделе *Базис.WorkPlace → Настройки системы*.

5.3.3 Описание параметров конфигурации для Диспетчера подключений Базис.WorkPlace

Совет

Правила описания параметров в YAML-формате представлены в разделе Правила редактирования конфигурационных файлов.

Примечание

Полный список параметров с описанием представлен в разделе *Базис.WorkPlace → Настройки системы*.

5.4 Сценарии использования API Базис.WorkPlace

5.4.1 Мониторинг API-бэкенда внешней системой мониторинга

Для проверки API-бэкенда можно послать GET HTTP-запрос на сервер бэкенда, например:

```
http://123.123.123.123/vdi/api/0/health?check_local_broker_manager=true
```

Если HTTP-сервис не отвечает или возвращает ошибку, это означает, что нарушена работоспособность системы. Дополнительно можно разбирать вывод запроса. Запрос возвращает JSON-документ вида:

```
{"all_ok": true, "health": {"db_write": true, "broker_manager": true,
"conf": true, "db_read": true, "redis_read": true, "redis_write":
true}}
```

- ***all_ok*** — общее состояние системы в целом (возвращается false, когда в одном из компонентов системы есть проблемы);
- секция ***health*** — состояние каждого из компонентов системы:
  - ***db_write*** — системной учетной записи доступна БД на запись;
  - ***db_read*** — системной учетной записи доступна БД на чтение;
  - ***broker_manager*** — состояние Менеджера диспетчеров подключений;
  - ***conf*** — конфигурационный файл не содержит ошибок;
  - ***redis_read*** — системной учетной записи доступен Redis на чтение;
  - ***redis_write*** — системной учетной записи доступен Redis на запись.

5.4.2 Получение статуса компонентов Базис.WorkPlace

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

```
http://172.29.225.109/vdi/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 авторизированного запроса возвращается ответ в статусе 200, содержащий JSON-документ вида:

```
{
  "is_cached": true,
  "timestamp": 1575623385.608229,
  "status": {
    "backends": [
      {
        "address": "1.1.1.1",
        "alive": true
      },
      {
        "address": "2.2.2.2",
        "alive": true
      }
```

```
    ],
    "managers": [
      {
        "address": "1.1.1.1:5501",
        "alive": true
      },
      {
        "address": "2.2.2.2:5502",
        "alive": true
      }
    ],
    "redis": [
      {
        "host": "localhost",
        "port": 6379,
        "is_master": true,
        "subjective_alive": true,
        "objective_alive": true,
        "role_reported": "master"
      }
    ],
    "sentinel": [
      {
        "host": "localhost",
        "port": 26379,
        "is_master": true,
        "subjective_alive": true,
        "objective_alive": true,
        "role_reported": "master"
      }
    ],
    "db": {
      "address": "localhost:5432",
      "read": true,
      "write": true
    },
    "memdb": {
      "address": "localhost:6379",
      "read": true,
      "write": 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.WorkPlace**:
  - **address** — IP-адрес.
  - **alive** — статус работоспособности: true — активен, false — сбой.
- секция ***managers*** — данные о состоянии **Менеджеров Диспетчеров подключений Базис.WorkPlace**:
  - **address** — IP-адрес.
  - **alive** — статус работоспособности: true — активен, 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 ***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 ***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.

5.4.3 Получение статистики активности использования Базис.WorkPlace

Для получения статистики активности по **Диспетчерам подключений**, пулам и пользователям **Базис.WorkPlace** можно послать GET HTTP-запрос следующего вида:

```
http://123.123.123.123/vdi/api/0/load_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 авторизированного запроса возвращается ответ в статусе 200, содержащий JSON-документ вида:


```
{
  "is_cached": false,
  "timestamp": 1575623385.608229,
  "load_status": {
    "brokers": [
        {
            "addresses": [
                {
                    "ipv4": "123.123.123.59",
                    "types": [
                        "external",
                        "internal",
                        "backend"
                    ]
                }
            ],
            "alive": true,
            "connections_count": 0,
            "name": "broker2",
            "users_count": 0
        }
    ],
    "hosts": [
      {
        "connections_count": 2,
        "desktops_count": 5,
        "desktops_error_count": 1,
        "desktops_other_count": 1,
        "desktops_preparing_count": 2,
        "desktops_ready_count": 1,
        "name": "node_name"
      },
```

```
      {
        "connections_count": 0,
        "desktops_count": 1,
        "desktops_error_count": 0,
        "desktops_other_count": 1,
        "desktops_preparing_count": 0,
        "desktops_ready_count": 0,
        "name": "node_name2"
      }
    ],
    "pools": [
      {
        "connections_count": 1,
        "desktops_count": 5,
        "desktops_error_count": 1,
        "desktops_other_count": 2,
        "desktops_preparing_count": 1,
        "desktops_ready_count": 1,
        "hosts": [
          {
            "connections_count": 1,
            "desktops_count": 4,
            "desktops_error_count": 1,
            "desktops_other_count": 1,
            "desktops_preparing_count": 1,
            "desktops_ready_count": 1,
            "name": "node_name"
          },
          {
            "connections_count": 0,
            "desktops_count": 1,
            "desktops_error_count": 0,
            "desktops_other_count": 1,
            "desktops_preparing_count": 0,
            "desktops_ready_count": 0,
            "name": "node_name2"
          }
        ],
        "name": "pool1"
      },
      {
        "connections_count": 1,
        "desktops_count": 1,
        "desktops_error_count": 0,
        "desktops_other_count": 0,
        "desktops_preparing_count": 1,
        "desktops_ready_count": 0,
```

```
        "hosts": [
          {
            "connections_count": 1,
            "desktops_count": 1,
            "desktops_error_count": 0,
            "desktops_other_count": 0,
            "desktops_preparing_count": 1,
            "desktops_ready_count": 0,
            "name": "node_name"
          }
        ],
        "name": "pool2"
      }
    ],
    "totals": {
      "connections_count": 2,
      "desktops_count": 6,
      "desktops_error_count": 1,
      "desktops_other_count": 2,
      "desktops_preparing_count": 2,
      "desktops_ready_count": 1,
      "users_count": 1
    }
  }
}
```


- ***is_cached*** — флаг, означающий что ответ взят из кэша.
- ***timestamp*** — время, когда был сделан оригинальный ответ (POSIX-время).
- секция ***brokers*** — статистика **Диспетчеров подключений**:
  - **addresses** — секция с информацией по IP-адресу и его типу.
  - **alive** — статус работоспособности: true — активен, false — сбой.
  - **connections_count** — количество подключений к рабочим столам.
  - **name** — название **Диспетчера подключений**.
  - **users_count** — количество пользователей, подключенных к **Диспетчеру подключений**.
- секция ***hosts*** — статистика по хостам:
  - **name** — название хоста.
  - **connections_count** — количество соединений с хостом.
  - **desktops_count** — общее количество рабочих столов на хосте.
  - **desktops_ready_count** — количество рабочих столов на хосте в статусе «Готов».
  - **desktops_error_count** — количество рабочих столов на хосте в статусе «Сбой».

- **desktops_preparing_count** — количество рабочих столов на хосте в статусе «Подготовка».
- **desktops_other_count** — количество рабочих столов на хосте в прочих статусах.

- секция ***pools*** — статистика по пулам:
  - **name** — название пула.
  - **connections_count** — количество соединений в рамках пула.
  - **desktops_count** — общее количество рабочих столов в рамках пула.
  - **desktops_ready_count** — количество рабочих столов в рамках пула в статусе «Готов».
  - **desktops_error_count** — количество рабочих столов в рамках пула в статусе «Сбой».
  - **desktops_preparing_count** — количество рабочих столов в рамках пула в статусе «Подготовка».
  - **desktops_other_count** — количество рабочих столов в рамках пула в прочих статусах.
- секция ***totals*** — общая статистика в рамках **Базис.WorkPlace**:
  - **connections_count** — общее количество соединений.
  - **desktops_count** — общее количество рабочих столов.
  - **desktops_ready_count** — общее количество рабочих столов в статусе «Готов».
  - **desktops_error_count** — общее количество рабочих столов в статусе «Сбой».
  - **desktops_preparing_count** — общее количество рабочих столов в статусе «Подготовка».
  - **desktops_other_count** — общее количество рабочих столов в прочих статусах.
  - **users_count** — общее количество пользователей **Базис.WorkPlace**.

5.5 Установка SNMP Агента

SNMP Агент устанавливается на **Бэкенде Базис.WorkPlace**. В случае отказоустойчивой конфигурации, когда инсталляция **Базис.WorkPlace** включает несколько **Бэкендов**, на каждом из них устанавливается свой SNMP Агент. При этом используется VRRP протокол и для обращения к **Бэкенду Базис.WorkPlace** настраивается виртуальный IP-адрес (Virtual IP). На рисунке 5.2 в качестве иллюстрации показана схема обмена данными между SNMP Агентом **Базис.WorkPlace** и широко распространенной системой мониторинга Zabbix.

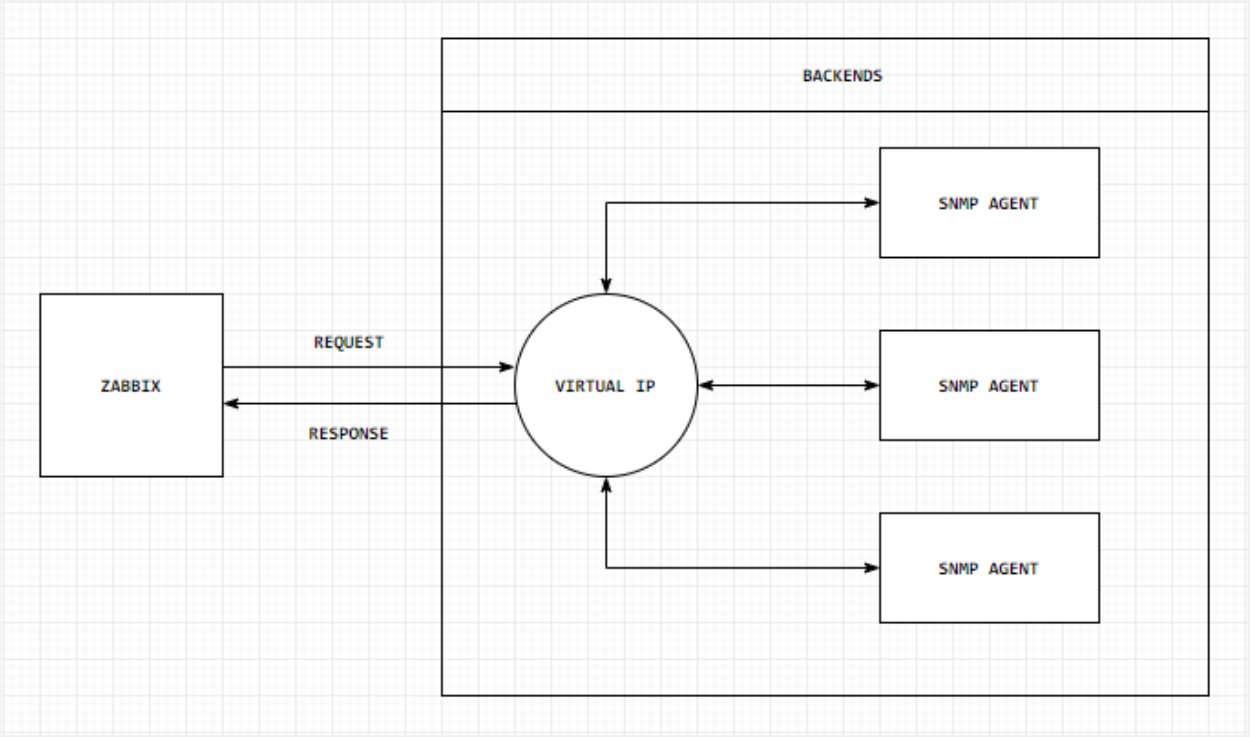

Рисунок 5.2 Схема обмена данными между SNMP Агентом Базис.WorkPlace и внешней системой мониторинга

Примечание

По умолчанию SNMP Агент занимает локальный порт 7161. При установке SNMP Агента автоматически настраивается правило ***iptables***, которое перенаправляет запросы к порту 161 виртуального IP-адреса **Бэкенда Базис.WorkPlace** на локальный порт 7161. Данное правило автоматически применяется при запуске SNMP Агента и удаляется при его остановке.

Чтобы установка SNMP Агента была автоматически выполнена во время разворачивания **Бэкенда Базис.WorkPlace**, в конфигурационный файл ***vdi-config*** необходимо включить следующие строки:

```
# Установка SNMP-агента и keepalived
snmp_agent_deploy: true
vips:
  backend:
    # Виртуальный IP-адрес для Бэкенда Базис.WorkPlace, который будет
перемещаться, если хост выйдет из строя.
```

```
    vip: '192.168.0.111'
    # vrrp router id, должен быть уникален в рамках L2-сети, должно
быть целым числом от 0 до 255.
    vrouter_id: '111'
```

5.6 Установка гостевых утилит в Linux ВМ для рабочего стола

Для работы Агента Базис.WorkPlace достаточно использовать **qemu-agent**, входящий в комплект системы. Утилита устанавливается в системе следующим образом:

```
apt-get install qemu-guest-agent
systemctl start qemu-guest-agent
systemctl enable qemu-guest-agent
```

Если вы хотите использовать гостевые утилиты из состава платформы, то после их установки нужно удалить пакет prl_nettool:

```
apt-get remove prl_nettool
```

5.7 Инструкция по настройке смены пароля при использовании OpenLDAP

5.7.1 Создание файла krb5.conf

Создайте файл ***/etc/krb5.conf*** на всех **Менеджерах диспетчеров подключений** (в случае HA-установки) следующего вида:

```
[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
  ticket_lifetime = 24h
  renew_lifetime = 7d
```

```
  forwardable = true
  rdns = false
  default_realm = SK.LOCAL
  default_ccache_name = KEYRING:persistent:%{uid}

[realms]
  SK.LOCAL = {
    kdc = 123.123.123.123
    admin_server = 123.123.123.123
    default_domain = sk.local
  }

[domain_realm]
  .sk.local = SK.LOCAL
  sk.local = SK.LOCAL
```

В файле выполните следующие замены:

- **SK.LOCAL** — замените на имя вашего домена в соответствии с регистром.
- **kdc** и **admin_server** — укажите в этих параметрах соответствующие имена серверов.

При подключении в системе нескольких независимых доменов в конфигурационном файле krb5.conf в секциях [realms] и [domain_realm] должны быть прописаны параметры для каждого домена.

5.7.2 Пример конфигурационного файла krb5.conf в системе с несколькими независимыми доменами

```
[logging]
  default = FILE:/var/log/krb5libs.log
  kdc = FILE:/var/log/krb5kdc.log
  admin_server = FILE:/var/log/kadmind.log

[libdefaults]
  dns_lookup_kdc = true
  dns_lookup_realm = false
  dns_canonicalize_hostname = false
  ticket_lifetime = 24h
  renew_lifetime = 1d
  forwardable = true
  rdns = false
  default_realm = QA2.ORG
  default_ccache_name = KEYRING:persistent:%{uid}
```

```
[realms]
  SK.LOCAL = {
    kdc = ad.sk.local
    default_domain = SK.LOCAL
    admin_server = ad.sk.local
  }
  QA2.ORG = {
    kdc = qadc2.qa2.org
    default_domain = QA2.ORG
    admin_server = qadc2.qa2.org
  }
  QA3.ORG = {
    kdc = qadc3.qa3.org
    default_domain = QA3.ORG
    admin_server = qadc3.qa3.org
  }
  FREEIPA.LOCAL = {
    kdc = dc01.freeipa.local
    admin_server = dc01.freeipa.local
    default_domain = FREEIPA.LOCAL
  }
  VDI.LAN = {
    kdc = server.vdi.lan
    admin_server = server.vdi.lan
    default_domain = VDI.LAN
  }
  ALDPRO.TEST = {
    kdc = dc.aldpro.test
    admin_server = dc.aldpro.test
    default_domain = ALDPRO.TEST
  }

[domain_realm]
  .sk.local = SK.LOCAL
  sk.local = SK.LOCAL
  .qadc2.qa2.org = QA2.ORG
  qadc2.qa2.org = QA2.ORG
  .qadc3.qa3.org = QA3.ORG
  qadc3.qa3.org = QA3.ORG
  .dc01.freeipa.local = FREEIPA.LOCAL
  dc01.freeipa.local = FREEIPA.LOCAL
  .vdi.lan = VDI.LAN
  server.vdi.lan = VDI.LAN
  .aldpro.test = ALDPRO.TEST
  dc.aldpro.test = ALDPRO.TEST
```

5.7.3 Обновление конфигурационного файла backend-overrides

На сервере развертывания в конфигурационный файл ***backend-overrides*** добавьте параметры настройки для доступа к Kerberos через kadmin:

```
broker_manager:
  kerberos:
    #: Имя учетной записи с правом смены пароля у других принципалов
    admin_principal: kadmin/admin
    #: Пароль от учетной записи с правом смены пароля у других
принципалов
    admin_principal_password: 'AdminPassword'
    #: Путь до исполняемого файла kadmin
    kadmin_bin: kadmin
```

В файле замените **AdminPassword** на соответствующий пароль, который будет применен на ***kadmin/admin***. После этого переустановите все **Бэкенды Базис.WorkPlace**.

Совет

Пароль на ***kadmin/admin*** на OpenLDAP сервере можно поменять командой:

```
kadmin.local -q 'cpw -pw AdminPassword kadmin/admin'
```

В параметре ***-pw*** передайте нужный пароль.

5.7.4 Запуск kadmin

На OpenLDAP сервере должен быть запущен и добавлен в автозагрузку сервис ***kadmin***. При использовании ***systemd*** это можно выполнить следующим образом:

```
systemctl enable slapd kadmin krb5kdc
systemctl start slapd kadmin krb5kdc
```

5.7.5 Проверка выполненных настроек

Для проверки корректности настроек запустите на **Менеджере диспетчеров подключений** следующую команду, заменив **AdminPassword** на пароль для ***kadmin/admin*** (пароль должен быть в кавычках):

```
kadmin -p kadmin/admin -w 'AdminPassword' -q 'list_principals'
```

Если настройки были выполнены правильно, то команда выдаст список principal. Если в результате возвращается ошибка, отличная от некорректного пароля, то на OpenLDAP сервере нужно:

- Проверить, что все службы запущены:

```
systemctl status slapd kadmin krb5kdc
```

- Проверить, что слушают заданные порты:

```
netstat -ltupn|egrep 'slap|krb|kadm'
```

Примечание

Пример портов, которые должны прослушиваться на OpenLDAP сервере:

```
netstat -ltupn|egrep 'slap|krb|kadm'
tcp 0 0 0.0.0.0:88 0.0.0.0:* LISTEN 4629/krb5kdc
tcp 0 0 0.0.0.0:636 0.0.0.0:* LISTEN 4552/slapd
tcp 0 0 0.0.0.0:389 0.0.0.0:* LISTEN 4552/slapd
tcp 0 0 0.0.0.0:749 0.0.0.0:* LISTEN 4567/kadmind
tcp 0 0 0.0.0.0:464 0.0.0.0:* LISTEN 4567/kadmind
udp 0 0 0.0.0.0:88 0.0.0.0:* 4629/krb5kdc
udp 0 0 0.0.0.0:464 0.0.0.0:* 4567/kadmind
udp 0 0 0.0.0.0:750 0.0.0.0:* 4629/krb5kdc
```

Аналогично с **Менеджера диспетчеров подключений** должен быть доступ к OpenLDAP серверу по портам из примера выше.

Совет

Для отладки на **Бэкендах Базис.WorkPlace** можно запускать kadmin следующим образом:

```
KRB5_TRACE=/dev/stdout kadmin -p kadmin/admin -w test -q
'getprinc krbtest1'
```

5.8 Поддерживаемые версии PostgreSQL

Примечание

Для open source версий PostgreSQL (9.5 и 9.6) в случае установки в non-HA режиме подразумевается, что пакеты берутся из репозитория дистрибутива Linux, на который ставится продукт.

Продукт	Версия	ОС и тип развертывания
Postgres Pro 9.6	Enterprise	Альт 8 СП: HA, non-HA Альт 8: HA, non-HA Astra Linux Special Edition 1.7
Postgres Pro 9.6	Standard	Альт 8 СП: HA, non-HA Альт 8: HA, non-HA Astra Linux Special Edition 1.7
Postgres Pro 9.6	Standard Certified	Альт 8 СП: HA Альт 8: HA Astra Linux Special Edition 1.7

Продукт	Версия	ОС и тип развертывания
Postgres Pro 10	Enterprise	Альт 8 СП: HA Альт 8: HA Astra Linux Special Edition 1.7
Postgres Pro 10	Enterprise Certified	Альт 8 СП: HA Альт 8: HA Astra Linux Special Edition 1.7
Postgres Pro 10	Standard	Альт 8 СП: HA Альт 8: HA Astra Linux Special Edition 1.7
Postgres Pro 10	Standard Certified	Альт 8 СП: HA Альт 8: HA Astra Linux Special Edition 1.7
Postgres Pro 11	Enterprise	Альт 8 СП: HA Альт 8: HA Astra Linux Special Edition 1.7
Postgres Pro 11	Standard	Альт 8 СП: HA Альт 8: HA Astra Linux Смоленск 1.6: HA Astra Linux Орел 2.12: HA
Postgres Pro 11	Standard Certified	Альт 8 СП: HA Альт 8: HA Astra Linux Special Edition 1.7

Продукт	Версия	ОС и тип развертывания
Jatoba		Альт 8 СП: HA Альт 8: HA Astra Linux Special Edition 1.7
PostgreSQL 9.5 (Open Source)		Альт 8 СП: HA, non-HA Альт 8: HA, non-HA
PostgreSQL 9.6 (Open Source)		Альт 8: HA, non-HA Astra Linux Special Edition 1.7