Почтовая система RuPost

Руководство по установке и конфигурированию

Версия 2.2.0 – Июль 2023

Официальный веб-сайт: http://www.rupost.ru .

Оглавление

1. Обзор системы

RuPost – почтовая система, предназначенная для предприятий любого масштаба – от небольших организаций до корпораций. RuPost устанавливается в корпоративной сети предприятия и работает на платформе Astra Linux.

1.1. Функциональные возможности RuPost

RuPost включает следующую функциональность:

- Панель управления почтовой системой, доступная через современные web-браузеры
- Командный интерфейс управления (CLI)
- Электронная почта (протоколы SMTP и IMAP)
- Календари (протокол CalDav)
- Задачи (протокол CalDav)
- Контакты (протокол CardDav)
- Корпоративная адресная книга (на базе LDAP)
- Списки рассылки (статические и динамические)
- Ресурсы календаря
- Интеграция с корпоративными службами каталогов Active Directory, FreeIPA, ALDPro
- Интеграция со средствами ИБ по протоколу Milter (антивирусная/антиспам/антималваре защита, DLP) – включая интеграцию “из коробки” с Kaspersky Security (KLMS, KSMG) и Dr.Web
- Использование СУБД PostgreSQL/Postgres Pro
- Встроенный Web-клиент
- Поддержка настольных почтовых клиентских приложений
    - Модуль расширения Microsoft Outlook с поддержкой календарей, контактов, задач и адресных книг RuPost по протоколам CalDav и CardDav
    - Evolution и его расширенная версия для Astra Linux
    - Thunderbird и настольные почтовые клиенты на его основе (например, МойОфис, Р7)
- Поддержка безопасного мобильного доступа с использованием WorksPad (отдельный продукт, интегрируемый с RuPost, включая специальную поддержку пуш-уведомлений)
- Средства миграции почтовых ящиков, календарей и контактов с Microsoft Exchange, с возможностью сосуществования почтовых систем RuPost и Exchange в одном почтовом домене на период миграции.

Система RuPost развертывается в корпоративной сети предприятия (on-prem) и может управлять почтовыми ящиками только для пользователей зарегистрированных в системе доменов LDAP. Регистрация доменов LDAP производится в Панели управления RuPost. Администраторами системы могут выступать только пользователи LDAP, а также локальный администратор ОС для конфигураций на одном узле.

RuPost поставляется в двух редакциях:

- Стандартная – Standard
- Корпоративная – Enterprise

Корпоративная редакция (Enterprise) отличается расширенными функциональными возможностями и может устанавливаться в отказоустойчивой (кластерной) конфигурации.

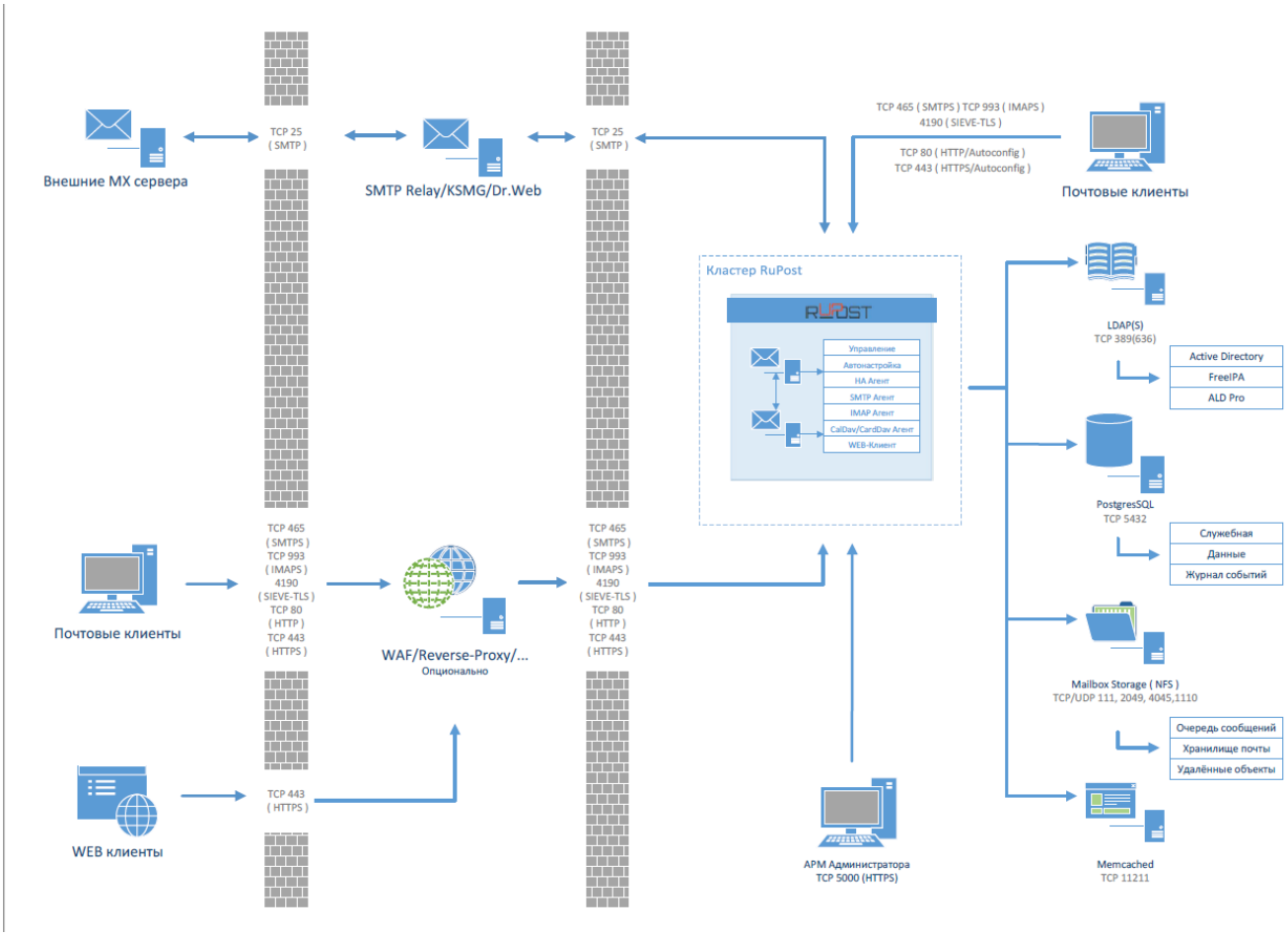
1.2. Архитектура и компоненты сервера RuPost

Сервер RuPost включает в себя систему управления, средства мониторинга, интегрированный набор почтовых компонентов для работы по протоколам SMTP/IMAP/CalDAV/CardDAV, вспомогательные сервисы, веб-клиент и средства автонастройки клиентских приложений, предназначенные для организации электронной почты корпоративного класса.

Сервер RuPost может функционировать как на одном узле, так и в кластере из множества узлов.

Кластер RuPost предназначен для обеспечения высокой доступности почтовой системы. Кластер функционирует в режиме Active-Active, где все экземпляры системы равнозначны и динамически перераспределяют нагрузку между собой. Каждый узел системы в кластере обладает всеми функциями управления и даже при полном выводе из эксплуатации узла или выходе из строя любого из его компонент продолжит функционировать пока в системе есть хоть один функционирующий узел. Сбои отдельных компонентов обнаруживаются автоматически и соответствующие узлы также автоматически выводятся из эксплуатации, при этом кластер продолжает функционировать.

Конфигурационные параметры системы хранятся в единой БД и совместно используются всеми экземплярами – узлами системы.



Внутренние компоненты сервера RuPost:

- **Система управления** RuPost – ядро системы, обеспечивающее функции управления, мониторинга и автонастройки, инструментарий командной строки и визуальную Панель управления системой (АРМ Администратора):
    - управление и применения типовых шаблонов конфигураций к почтовым компонентам;
    - настройка, конфигурирование, мониторинг, диагностика и управление поведением системы и ее почтовых компонентов через специально разработанные адаптеры почтовых компонентов;
    - подключение пользователей и управление почтовыми адресами и ящиками;
    - управление квотами и другими параметрами пользовательских ящиков;
    - управление администраторами системы RuPost;
    - управление обслуживаемыми почтовыми доменами;
    - подключение к службам каталогов Active Directory и другими LDAP;
    - автоматическое формирование и обновление корпоративной адресной книги (Global Address List, GAL) на базе информации из подключенных служб каталогов;
    - кластеризация узлов для обеспечения отказоустойчивости и высокой доступности системы;
    - проверка работоспособности и целостности системы со встроенным мониторингом и самодиагностикой узлов системы, и её компонентов на каждом узле;
    - журналирование операций;
    - графическая **Панель управления** RuPost, доступная из браузера;
    - командный интерфейс управления (CLI)/

- **HA Агент (High Availability Agent)** – **HAProxy**, агент обеспечения высокой доступности системы, работающий по протоколам TCP, HTTP(S). Выполняет следующие функции:
    - дублирующее отслеживание состояния Системой управления и других HA Агентов системы;
    - внутренняя балансировка сетевых запросов от пользователей;
    - проксирование и терминирование соединений к почтовым компонентам по протоколам IMAP и SMTP;
    - безопасный доступ клиентских приложений к почтовым ящикам;
    - безопасный доступ к web-клиенту с использованием SSL/TLS.

- **SMTP Агент – Postfix**. Компонент пересылки писем (Mail Transfer Agent, MTA), работающий по протоколам TCP, SMTP, LMTP, STARTTLS, TLS, SASL, LDAP, Milter. Номера занимаемых портов зависят от типа конфигурации. Основными задачами данного сервиса являются:
    - получение писем от сторонних почтовых серверов;
    - отправка писем пользователей сторонним почтовым серверам;
    - передача полученных писем компоненту обработки писем MDA Dovecot по протоколу LMTP для дальнейшего сохранения в пользовательских почтовых ящиках и/или отправки конечным адресатам;
    - получение пользовательских писем от Mail User Agent (MUA) для последующей пересылки сторонним почтовым серверам или пользователям своего домена;
    - интеграция со средствами безопасности (например, Kaspersky Security) для фильтрации входящей и исходящей почты и соединений по протоколу Milter.

- **IMAP Агент – Dovecot.** Компонент обработки писем (Mail Delivery Agent, MDA), работающий по протоколам TCP, IMAP, LMTP, STARTTLS, TLS, SASL, LDAP. Номера занимаемых портов зависят от типа конфигурации. Компонент выполняет следующие функции:
    - предоставление доступа пользователям к личным почтовым ящикам посредством клиентских приложений;
    - осуществление квотирования ресурсов пользовательских ящиков;
    - выполнение функции авторизации клиентов;
    - хранение и управление письмами;
    - обработка пользовательских и глобальных сценариев, написанных на языке Sieve;
    - предоставление средств удалённого изменения пользовательских Sieve сценариев.

- **CalDAV/CardDAV компонент для календарей и контактов – SOGo**. Отвечает за хранение и удалённый доступ к корпоративным и пользовательским календарям, задачам, контактам и корпоративной адресной книге. Работает по протоколам по протоколам CalDAV и CardDAV.

- **Web-клиент корпоративной почты – SOGo**. Доступен во всех актуальных версиях современных браузеров.
- **Web-сервер – Nginx. Обеспечивает работу web-клиента почты.**
- **Компонент кеширования в оперативной памяти – Memcached.** Работает по протоколам TCP и UDP. Выполняет функцию кэширования и синхронизации части пользовательских данных, для увеличения быстродействия доступа к календарям, контактам и web-клиенту.

Управление всеми компонентами системы осуществляется через специализированные адаптеры, обеспечивающие интегрированность и целостность конфигураций RuPost.

Концепция управления RuPost строится на использовании **шаблонов конфигураций**, разрабатываемых на основе заранее созданных и проверенных типовых конфигураций интегрированных компонентов. Шаблоны конфигураций описываются на языке YAML, в котором отражаются основные параметры компонентов RuPost. RuPost предоставляет **библиотеку шаблонов конфигураций**, на основе которых развертываются конкретные конфигурации.

Шаблоны конфигураций бывают двух типов:

- **Встроенные (builtin)** – поставляются в составе RuPost
- **Специализированные (custom)** – разрабатываются в рамках проектов внедрения RuPost для учета особенностей требований конкретной организации и ее корпоративного ИТ и ИБ ландшафта. Такие шаблоны поддерживаются только в старших редакциях продукта RuPost и не поддерживаются в RuPost Standard. Специализированные шаблоны конфигураций могут быть загружены в библиотеку шаблонов с использованием соответствующих инструментов RuPost. Структура шаблонов конфигураций описана в отдельном “*Руководстве по шаблонам конфигураций*” RuPost.

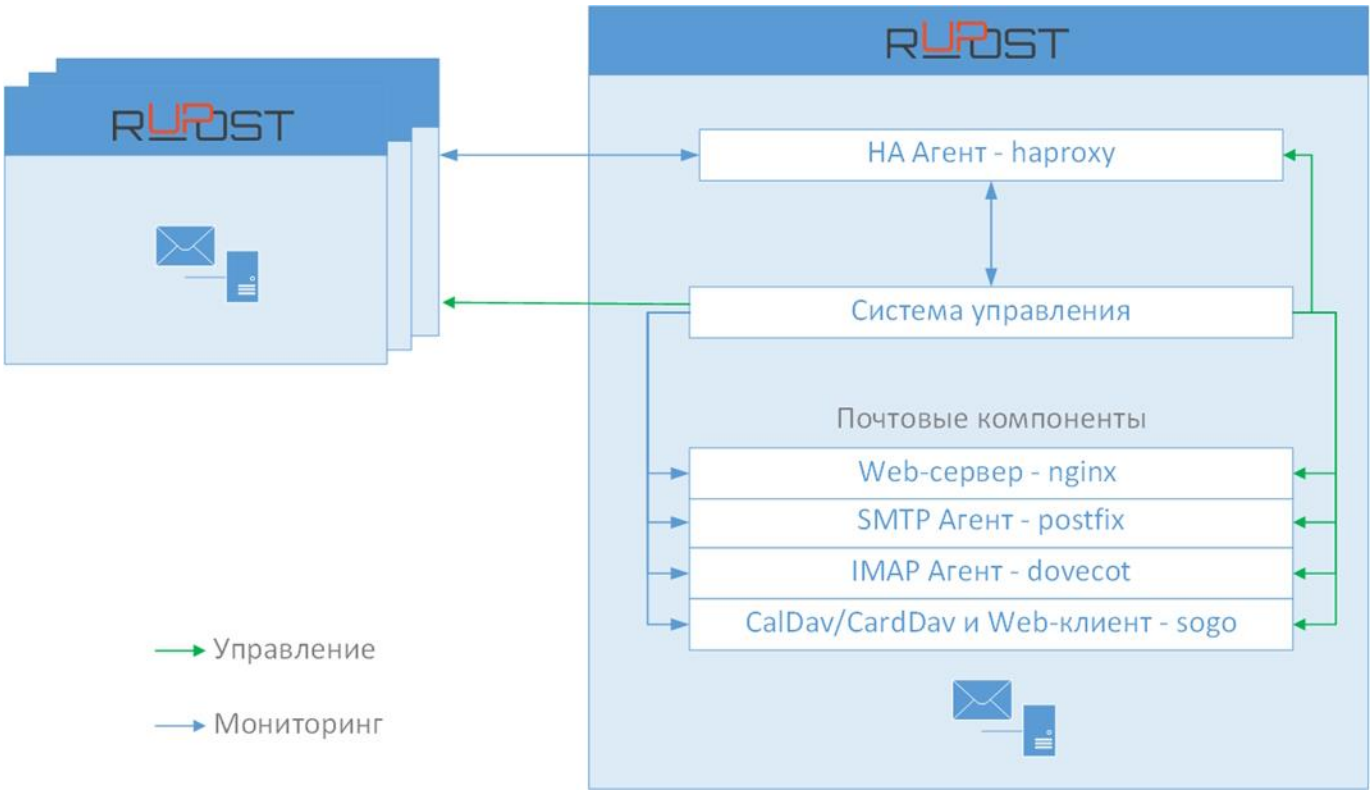
При **развертывании конфигурации** на базе выбранного шаблона система управления RuPost генерирует все необходимые конфигурационные файлы для компонентов системы.

1.3. Отказоустойчивый кластер RuPost

Кластер системы включает **узлы** кластера, на каждом из которых установлен **экземпляр** системы. Все экземпляры системы равнозначны и включают:

- Систему управления с входящей в нее Панелью управления
- HA Агент, обеспечивающий коммуникации с другими HA Агентами и перенаправление полезного трафика на почтовые компоненты
- Почтовые компоненты, к которым относятся:
    - терминирующий Web-сервер – nginx
    - SMTP Агент – postfix
    - IMAP Агент – dovecot
    - CalDav/CardDav сервер с входящим в него почтовым Web-клиентом системы – sogo

Узел доступен для управления и мониторинга, когда на нем функционируют как минимум Система управления и HA Агент.



Экземпляр системы **введен в эксплуатацию**, то есть является функционирующим элементов кластера, при двух условиях:

- для всех компонентов успешно развернута активная конфигурация системы
- все компоненты запущены и функционирую штатно

Все почтовые компоненты (вместе с терминирующим их Web-сервером) работают как единое целое - в режиме синхронизации. То есть при остановке любого из этих компонентов останавливаются они все, причем вне зависимости от того останавливаются они явно администратором или останавливается какой-либо компонент при наличии тех или иных сбоев. Такое поведение почтовых компонентов обеспечивается Системой управления.

Отказоустойчивая архитектура RuPost позволяет обеспечить постепенное масштабирование системы от одного узла до необходимого числа узлов кластера с автоматическим применением одной и той же активной конфигурации RuPost без необходимости индивидуального изменения конфигураций узлов. Число узлов кластера архитектурно неограниченно.

При планировании развертывания системы администратор должен руководствоваться *следующей схемой взаимодействия компонентов и узлов кластера*, обеспечивая открытие необходимых сетевых портов:

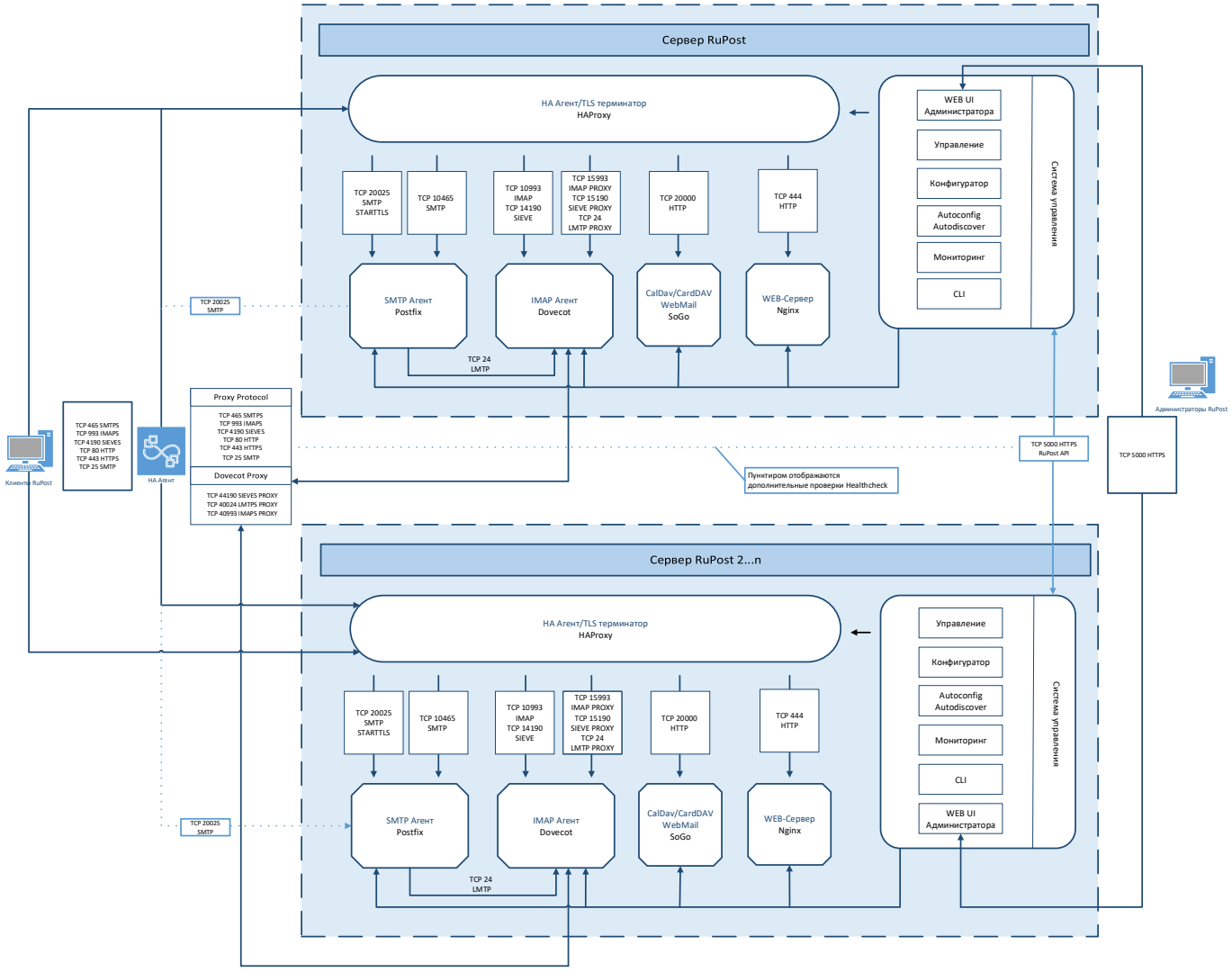


Схема взаимодействия компонентов и узлов кластера

Если клиент при подключении попал на узел, чей экземпляр выведен из эксплуатации – клиент будет перенаправлен на другой узел. В случае идентификации отказа почтовых компонентов любого узла кластера, ассоциированные с ним почтовые очереди автоматически эвакуируются ну другой доступный штатно функционирующий узел кластера.

Такая высокая доступность (высокий уровень отказоустойчивости) кластера RuPost достигается за счет постоянных проверок работоспособности почтовых сервисов не только средствами сервиса RuPost, но и средствами HAProxy.

Балансировка нагрузки между узлами системы в кластере RuPost может осуществляться с использованием следующих методов:

- Round Robin DNS с использованием A записи, указывающей на набор IP адресов узлов кластера
- Direct Routing
- TPROXY
- Сетевой балансировки с использованием PROXY protocol (v2)

Внимание!
Балансировка TCP трафика на портах 25, 80, 443, 465, 993, 4190 должна выполняться на транспортном уровне алгоритмом Round Robin.

Внимание!

1. При развертывании кластера рекомендуется вначале развернуть один узел системы, настроить необходимые параметры системы, развернуть на этом узле требуемую конфигурацию и убедиться в работоспособности настроек инфраструктуры и системы, а также доступность системы из клиентских почтовых приложений.

2. Только после успешного развертывания одного узла стоит переходить к развертыванию и включению в кластер других узлов системы, к которым автоматически будет применяться активная конфигурация по мере их включения в кластер.

Такой подход позволяет сразу убедиться в корректной организации и настройке инфраструктурного ландшафта, необходимого для работы RuPost.

2. Подготовка к установке RuPost

2.1. Системные требования

В качестве платформы для системы **RuPost** может использоваться как физическое аппаратное обеспечение или “*bare metal*”, так и виртуальная машина с поддержкой операционных систем семейства **GNU/Linux**.

Для корректного функционирования системы каждый из узлов должен удовлетворять следующим системным требованиям:

Компонент	Требования
Центральное процессорное устройство (CPU)	Не менее 2-х ядер с частотой от 2-х ГГц
Оперативное запоминающее устройство (RAM)	Не менее 2-х ГБ

Требования к оперативной памяти, числу ядер и производительности процессора зависят от числа подключенных пользователей и обслуживаемых почтовых ящиков исходя из нагрузки на узел RuPost:

Число пользователей / почтовых ящиков	Параметры vCPU / vRAM
1000	Не менее 2 vCPU / 2 Гб vRAM
2000	Не менее 2 vCPU / 4 Гб vRAM
10 000	Не менее 4 vCPU / 4 Гб vRAM
15 000	Не менее 6 vCPU / 10 Гб vRAM
20 000	Не менее 8 vCPU / 12 Гб vRAM

В случае развертывания системы на одном узле с локальной базой данных и локальным сервисом Memcached требуется дополнительно не менее 2 Гб vRAM (рекомендуется 4 Гб).

Внимание!

При использовании кластерного развёртывания системы или при одноузловой схеме и количестве почтовых ящиков более 100 необходимо устанавливать PostgreSQL и Memcached только на выделенных для них отдельных узлах. При одноузловом развёртывании с менее 100 пользователей PostgreSQL и Memcached можно устанавливать локально на этот же узел, где развертывается RuPost.

2.2. Операционная система

Версия RuPost 2.2.0 поддерживает ОС **Astra Linux Special Edition (ALSE) 1.7** – 1.7.1, 1.7.2, 1.7.3, 1.7.4 и их оперативные обновления.

Для соответствующих основных версий Astra Linux необходимо использовать предназначенные для них дистрибутивы - установочные пакеты:

Операционная система	Установочный пакет RuPost
Astra Linux Special Edition 1.7.*	rupost-2.2.0-alse-amd64.deb

При установке **Astra Linux** необходимо выбрать следующие опции:

- На этапе *Установка базовой системы* выбрать ядро:
  - linux-5.10-generic или выше
- Указать при установке и/или установить из репозитория следующее ПО:
  - Средства удалённого доступа SSH (обязательно)
  - Базовые средства (опционально)
  - Рабочий стол Fly (опционально)
  - Средства работы в Интернет (опционально)
  - СУБД PostgreSQL (в случае использования локальной базы данных)

Перед установкой RuPost должен быть подключен расширенный репозиторий Astra Linux. При установке RuPost из данного репозитория будут установлены дополнительные пакеты:

```
autotools-dev gobjc liblasso3 libobjc4 libxmlsec1-openssl libxmlsec1 lua-json lua-lpeg
```

Внимание!

При необходимости добавления сервера RuPost в домен, нужно сначала установить RuPost, а потом добавлять сервер в домен.

2.3. Синхронизация времени

Внимание!

Для корректной работы, физические серверы или виртуальные машины, на которых развернуты узлы RuPost и сопутствующие сервисы – (база данных, служба каталогов, сервис кеширования в памяти, сетевое файловое хранилище) **должны быть синхронизированы по времени с допуском, не превышающим одну секунду**.

Невыполнение данного требования приведет к неопределенным ошибкам функционирования системы (например, #50026), нарушению связанности кластера и целостности конфигурационных и пользовательских данных!

Также при расхождении времени на узлах не будет работать применение конфигурации к узлам кластера.

Данное требование может быть реализовано путем синхронизации времени с ближайшим расположенным, в рамках инфраструктуры, сервисом синхронизации времени на базе протоколов Network Time Protocol(NTP), Simple Network Time Protocol(SNTP) или аппаратными решениями, предоставляющие сервисы точного времени, которые используют спутниковую навигацию, данные сотовых сетей, радио-сигналы, атомные часы и тому подобное.

2.4. Службы каталогов LDAP

Почтовая система RuPost использует домены LDAP для авторизации пользователей. Одновременно к системе RuPost может быть подключено несколько независимых доменов LDAP. Завести почтовые ящики можно только для имеющихся активных учётных записей в службе каталогов.

Контроллер службы каталогов должен поддерживать один из способов подключения:

- протокол LDAPv3 без шифрования;
- протокол LDAPv3 с шифрованием TLS.

Добавляемый домен LDAP должен состоять в контексте имён указанных при добавлении контроллеров домена.

Правила сетевых маршрутов (route) и межсетевого экрана (firewall) должны разрешать прямое подключение всех узлов кластера RuPost к указываемым при настройке контроллерам домена на соответствующие порты (обычно 389 для протокола LDAP без шифрования и 636 для TLS LDAPS сессий).

Если контроллеры домена указываются с помощью имён, а не IP адресов, такие имена должны разрешаться в DNS или быть прописаны в файле hosts на всех узлах кластера RuPost.

В настоящее время система RuPost поддерживает следующие службы каталогов по протоколу LDAP:

- ALD Pro
- FreeIPA
- Microsoft Active Directory

2.4.1. Служебная учётная запись

RuPost для управления учётными записями пользователей в службе каталогов использует служебную учётную запись (сервисного пользователя). Администратор RuPost должен получить уникальные имена (DN) и пароли соответствующих сервисных аккаунтов во всех подключаемых к RuPost доменах до их подключения к RuPost. Права доступа к атрибутам и функциональное использование LDAP со стороны служебной учётной записи RuPost описано в “Приложении 1” данного Руководства.

2.4.2. Интеграция с ALD Pro

ALD Pro не требует расширения схемы домена для работы с RuPost (версии ALD Pro 1.3.x и выше).

Для интеграции с RuPost в ALD Pro необходимо завести служебную учетную запись. Для этого на контролере домена ALD Pro (права суперпользователя необязательны) получите Kerberos билет администратора домена. Это можно сделать, выполнив команду и введя пароль администратора:

```
kinit admin
```

После этого для просмотра имеющихся сервисных учётных записей системы RuPost исполните команду:

```
python3 /opt/rbta/ad/mgmtportal/api/core/manage.py rupostadmin find
```

Если в выводе записи отсутствуют, или необходима новая, для служебной записи **ldapbind** с паролем **12345678** команда будет иметь следующий вид:

```
python3 /opt/rbta/ad/mgmtportal/api/core/manage.py rupostadmin add --uid ldapbind --
password 12345678
```

В RuPost такая сервисная запись должна применяться с её полным уникальным именем (Distinguished Name, DN). Такое имя соответствует схеме:

```
uid={служебная запись RuPost},cn=sysaccounts,cn=etc,{RDN LDAP домена в 'DC' формате}
```

Так для служебной записи **ldapbind** в домене **org.example.com** уникальное имя будет следующим:

```
uid=ldapbind,cn=sysaccounts,cn=etc,dc=org,dc=example,dc=com
```

Утилита **rupostadmin** поддерживает и другие команды управления сервисными учётными записями RuPost.

Общая схема работы с утилитой:

```
python3 /opt/rbta/ad/mgmtportal/api/core/manage.py rupostadmin command
```

Первый позиционный аргумент определяет действие:

`info` **- справка; не требует дополнительных аргументов.**

rupostadmin info

`find` **- список существующих УЗ RuPost; не требует дополнительных аргументов.**

rupostadmin find

`add` **- создание новой УЗ RuPost; требует аргументы "Имя УЗ" и "Пароль УЗ".**

rupostadmin add -u user -p password

`passwd` **- изменение пароля существующей УЗ RuPost; требует "Имя УЗ" и "Пароль УЗ".**

rupostadmin passwd -u user -p password

`del` **- удаление существующей УЗ RuPost; требует один или несколько аргументов "Имя УЗ".**

rupostadmin passwd -u user

rupostadmin passwd -u user1 -u user2 -u user3

Именные аргументы:

`-u [UID], --uid [UID]` **Имя УЗ RuPost: не может быть пустым или "new", может содержать цифры, латиницу в нижнем регистре и символы "-", "_", "$", "."**

`-p [PASSWORD], --password [PASSWORD]` **Пароль УЗ RuPost: может быть от 7 до 255 символов,**

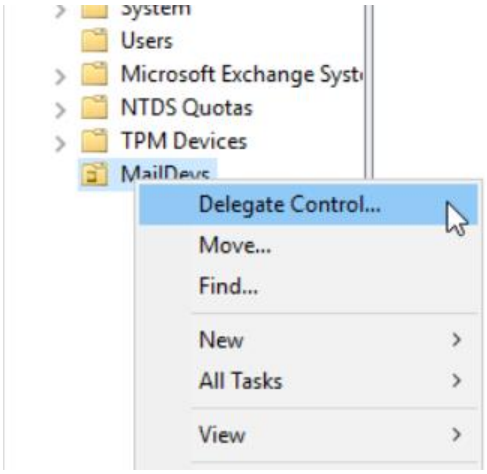
	не может начинаться или заканчиваться пробелом, не может содержать символы "`", "~", "{", "}", "'", '"'

2.4.3. Подготовка FreeIPA

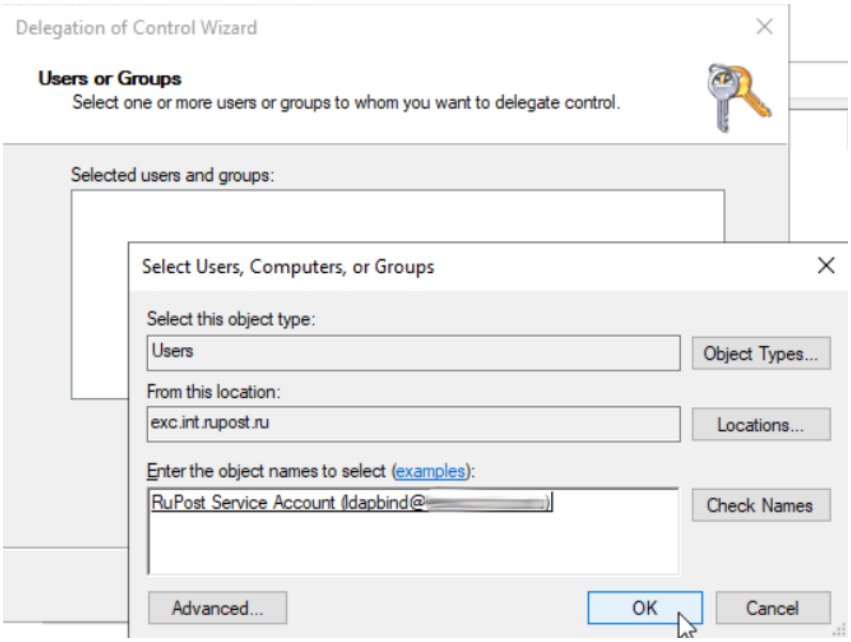
Для подготовки FreeIPA на мастер контроллере домена требуется выполнить bash сценарий, поставляемый вендором по соответствующему запросу.

2.4.4. Подготовка Microsoft Active Directory

После заведения в службе каталогов сервисной учётной записи, посредством которой RuPost будет управлять пользовательскими атрибутами своих клиентов, необходимо делегировать упомянутой учётной записи соответствующие права. Для этого выберите в службе каталогов подразделение, которое выделено для обслуживания в RuPost, и в контекстном меню выберите Delegate Control...

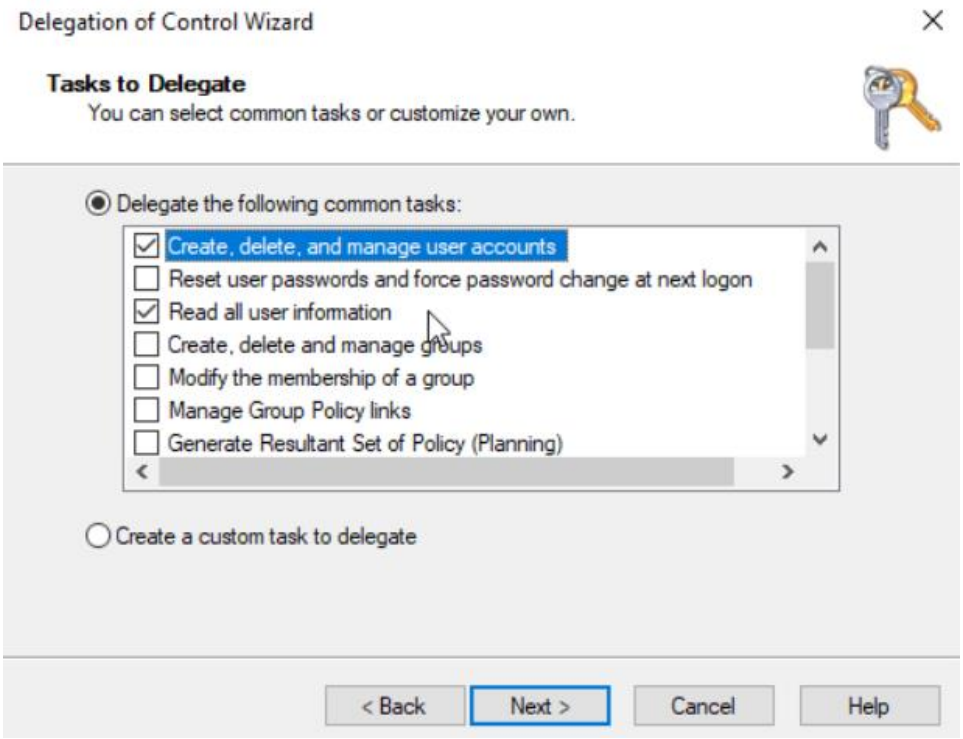


Далее необходимо добавить сервисную учётную запись RuPost для расширения прав.



После этого выберете в списке:

- Create, delete, and manage user accounts
- Read all user information



Сохраните выбранные привилегии. Теперь служебная учётная запись RuPost будет обладать достаточными правами для управления пользовательскими атрибутами в выбранном подразделении.

2.5. Система управления базами данных

Поддерживаемые СУБД:

- PostgreSQL версии не ниже 9.6, **рекомендуется версия 13**.

По умолчанию для конфигурации на одном узле предлагается использовать СУБД PostgreSQL, выполняющуюся на самом узле RuPost. В этом случае необходимые базы данных будут созданы автоматически во время установки через интерактивный конфигуратор, который будет описан в разделе 2.4.

Внимание!

Пароли от баз данных хранятся в открытом виде в конфигурационных файлах системы, поэтому необходимо предпринять организационно-технические меры нацеленные на ограничение и мониторинг действий круга лиц имеющих доступ к этим файлам как на просмотр так и на редактирование - для этого рекомендуется использовать встроенные механизмы ОС AstraLinux.

В случае, если требуется подключение к серверу баз данных, развёрнутому в инфраструктуре организации, то необходимо до начала установки RuPost выполнить следующие шаги:

1) создать специальную роль с параметрами
   `NOSUPERUSER NOCREATEROLE CREATEDB LOGIN ENCRYPTED PASSWORD;`
2) создать пустые базы данных с именами “`rupost`”, “`rupost_data`” и “`rupost_logs`”:

```
CREATE ROLE <ИМЯ_РОЛИ> WITH NOSUPERUSER CREATEDB NOCREATEROLE LOGIN ENCRYPTED PASS-
WORD '<ПАРОЛЬ>';
CREATE DATABASE rupost WITH ENCODING 'UTF8' OWNER <ИМЯ_РОЛИ>;
CREATE DATABASE rupost_data WITH ENCODING 'UTF8' OWNER <ИМЯ_РОЛИ>;
CREATE DATABASE rupost_logs WITH ENCODING 'UTF8' OWNER <ИМЯ_РОЛИ>;
```

Рекомендуемые параметры настройки СУБД Postgresql для оптимального быстродействия (файл postgresql.conf):

```
shared_buffers = 256MB

temp_buffers = 256MB

work_mem = 128MB

effective_io_concurrency = 1

max_worker_processes = 64

wal_buffers = 16MB

wal_writer_delay = 2000ms

wal_sync_method = open_sync

synchronous_commit = off

max_wal_size = 256MB
```

2.6. Служба кэширования объектов в оперативной памяти Memcached

Поддерживается служба Memcached версии не ниже 1.4.33.

При кластерной конфигурации или при одноузловой схеме развёртывания системы и количестве почтовых ящиков более 100 необходимо устанавливать Memcached только на выделенный узел.

Внимание!

В памяти сервиса Memcached хранятся пары логин/пароль от базы данных, и хеш паролей пользователей от ldap, которые можно получить, используя команды telnet или netcat.

В случае кластерной конфигурации, необходимо ограничить подключения к сервису всем, кроме узлов RuPost с помощью сетевых средств защиты (например, межсетевого экрана).

При установке RuPost на одном узле, служба Memcached обслуживает только локальные подключения, но нужно обеспечить установку корректных прав доступа для пользователей, имеющих доступ к узлу.

Размер выделяемой памяти рассчитывается по формуле:

```
Требуемая память (килобайт) = 512 * (количество доменов LDAP) + (10 * количество пользователей)
```

Требуемая память указывается в **Мб** конфигурационном файле `/etc/memcached.conf`.

```
# set ram size to 8MBytes to 256MBytes

CACHESIZE="4096"
```

Указать требуемую память можно также через командный интерфейс Memcahed:

```
memcached -m 3072
```

Ключ -m задает значение объема памяти в Мб.

Например:

```
-m 64
```

означает 64 Мб.

После внесения изменений нужно выполнить перезапуск сервиса memcached командой:

```
service memcached restart
```

2.7. Подключение сетевых каталогов файловой системы NFSv4

Для подключения сетевого файлового хранилища и каталога почтовых очередей необходимо экспортировать сетевые каталоги NFSv4 со следующими настройками:

- Для всех подключаемых каталогов (почтовых очередей, хранилища почтовых ящиков, пользовательских архивов и управления записями “record storage”) необходимо активировать параметры **rw, sync, no_subtree_check, no_root_squash** (как правило, в файле /etc/exports).

Также для каждого подключаемого сетевого каталога, например, `/srv/nfs/MailStorage`, на стороне сервера NFS необходимо назначить **UID:GID** равные **420:420** соответственно. Сделать это можно, по аналогии выполнив команду на сервере NFS для всех подключаемых каталогов:

```
sudo chown 420:420 -R /srv/nfs/MailStorage
```

Внимание!

Простое копирование каталогов и содержимого NFS между хранилищами без корректного контроля прав и параметров приведет к неработоспособности системы.

Пример экспорта каталогов конфигурации NFS:

```
/srv/nfs/MailQueues 10.154.22.0/24(rw,sync,no_subtree_check,no_root_squash)
/srv/nfs/MailStorage 10.154.22.0/24(rw,sync,no_subtree_check,no_root_squash)
/srv/nfs/MailArchive 10.154.22.0/24(rw,sync,no_subtree_check,no_root_squash)
/srv/nfs/MailRecord 10.154.22.0/24(rw,sync,no_subtree_check,no_root_squash)
```

*[где 10.154.22.0/24 — пример подсети, в которой расположены узлы RuPost]

Внимание!

Для корректной работы, необходимо убедиться, что на сервере NFS и всех клиентах NFS время синхронизировано.

Если внутренние часы узлов отличаются друг от друга более чем на одну секунду и несколько клиентов одновременно обращаются к одному и тому же почтовому ящику, в работе сервисов могут появляться критические ошибки.

2.7.1. Рекомендации по настройке сетевого файлового хранилища на примере NFS сервера, входящего в состав ОС Astra Linux 1.7

В примере рассматривается конфигурация, рассчитанная для обслуживания до 20000 почтовых ящиков, при среднестатистической ежедневной нагрузке 80% на чтение и 20% на запись. При указанной нагрузке к системным требованиям к серверу относятся:

- 4 ядра CPU;
- 4 GB оперативной памяти;
- Дисковая подсистема в 250 IOPS на 10000 активных соединений.

При этой конфигурации в файле ***/etc/default/nfs-kernel-server*** рекомендуется выставить параметр ***RPCNFSDCOUNT***, отвечающий за количество обработчиков соединений, равным произведению ***32*** на количество процессорных ядер, т.е. для текущего примера:

```
# Number of servers to start up
RPCNFSDCOUNT=128
```

Также для приведённых далее параметров ядра Linux следует выставить значения буферов в соотношении 1 MiB на каждый 1 GB оперативной памяти:

```
net.core.wmem_max = 4194304
net.core.rmem_max = 4194304
net.core.wmem_default = 4194304
net.core.rmem_default = 4194304
```

При более чем четырёх узлах в кластере RuPost рекомендуется выделить для сервера NFS одно процессорное ядро и 1 GB оперативной памяти для обслуживания каждого дополнительно узла; таким образом для шести узлов RuPost требуется 6 CPU/6GB RAM.

В связи с тем, что задержки и производительность NFS связанны с индивидуальной нагрузкой и активностями той или иной организации, рекомендуется вносить коррективы в настройки и используемое

оборудование при столкновении с недостаточной производительностью NFS сервера, а также вести мониторинг следующих параметров:

- Производительность дисковой системы ввода/вывода такими инструментами как iostat. При 100% утилизации мощности системы хранения данных принимать шаги по увеличению IOPS.
- Загрузка процессоров. При чрезмерной загрузке увеличивать количество ядер, объём доступной памяти, вносить изменения в системные настройки согласно рекомендациям, описанным выше.
- Утилизация пропускной способности сетевых соединений. В том числе, задействуя инструменты nfsstat на предмет увеличивающегося количества ретрансмит-пакетов. При обнаружении указанной проблемы увеличивать полосу пропускания сетевого трафика и вносить коррективы в MTU и настройки Jumbo Frames, если это возможно для топологии сетевых коммуникаций.

2.8. Настройки DNS

Для обмена письмами в сети интернет необходимо зарегистрировать RuPost на серверах DNS.

В корпоративном DNS для отправки и получения писем с внутрикорпоративных клиентов и SMTP серверов требуется настроить:

- **A запись** для имени хоста почтовой системы (заполняется в общих настройках под заголовком «Имя узла почтовой системы в DNS MX записи»), указывающую на локальный IP адрес узла RuPost или в кластерной конфигурации — внутренние адресы балансиров почтовой системы. В случае использования конфигурации с релей-сервером, за которым находятся серверы RuPost, в этой записи указывается IP адрес и имя хоста релей-сервера.

- **CNAME к A записи,** указанной выше. В случае указания конкретного сервера, можно задать приоритет обращения через Weight. Запись может состоять из нескольких адресов.

- Наличие **PTR записи** внутри сети зависит от Ваших корпоративных политик для других SMTP серверов, сосуществующих в организации. Например, используемых как open-relay для принтеров/МФУ и других систем.

- **Тип TXT (SPF)** со значением: v=spf1 a -all (опционально, внутри обычно не используется).

Возможно использование Split-DNS, если данный DNS сервер публично является authoritative для почтового домена, либо корректно настроена DNS-пересылка. Уточняйте возможность у Вашего провайдера услуги.

Для общедоступного (публичного) DNS:

- **A запись** для имени хоста почтовой системы (заполняется в общих настройках под заголовком «Имя узла почтовой системы в DNS MX записи»), указывающую на IP адресы шлюзов или балансиров почтовой системы, если они имеют публичные IP адресы. В случае использования конфигурации с релей-сервером, за которым находятся серверы RuPost, в этой записи указывается IP адрес и имя хоста релей-сервера.

- **PTR запись** для публичного IP адреса шлюза, с адреса которого набор узлов RuPost выполняет отправку сообщений. Должна указывать на имя хоста, соответствующее вашему SMTP EHLO (указывается в общих настройках под заголовком «Имя узла почтовой системы в DNS MX записи»). В случае применения конфигурации с релей-сервером, через который серверы RuPost выполняют отправку сообщений, в этой записи указывается SMTP EHLO релей-сервера.

Для **каждого** почтового домена в обоих вариантах DNS ожидаются нижеуказанные записи.

- Тип **MX**, в которой указывается приоритет (вес) и имя хоста почтовой системы или релей сервера. Для всех обслуживаемых доменов упомянутое имя одинаково. Пример:

```
domain.ru. MX 10 mail.domain.ru.
```

- Тип **TXT** (SPF). В случае, когда публичный IP адрес шлюза, с адреса которого набор узлов RuPost выполняет отправку сообщений, *совпадает* с IP адресом **A записи** для имени хоста почтовой системы, значение будет следующим:

  v=spf1 mx ~all

- Однако, если набор узлов RuPost выполняет отправку сообщений с других публичных IP адресов, все они должны быть указаны в директиве **ip4**. Например, если отправка писем из системы RuPost может осуществляться от IP адреса **A** записи, указанной в **MX** записи почтового домена, а также от IP адресов *10.20.30.41*, *10.20.30.42*, то **SPF** запись будет иметь следующее значение:

  *v=spf1 mx ip4:*10.20.30.41 *ip4:*10.20.30.42 *~all*

- В случае применения конфигурации с релей-сервером, в **SPF** должны быть указаны IP адресы релей-серверов.

- Для каждого домена организации, с которых НЕ планируется рассылка писем, следует создать SPF или TXT запись со значением: ***v=spf1 -all***. В этом случае письма злоумышленников, пытающихся отправить от таких необслуживаемых почтовым сервером доменов, будут идентифицированы как нарушающие доверие большинством корректно настроенных почтовых систем получателей.

- Для автонастройки клиентских приложений (Evolution, Thunderbird и построенные на них клиенты) тип **CNAME** для домена следующего уровня по формуле:
  autoconfig.<почтовый-домен>.
  указывающая на имя хоста почтовой системы. Пример:

```
autoconfig.domain.ru. CNAME mail.domain.ru.
```

- Для автонастройки клиента Outlook с плагином RuPost тип **CNAME** для домена следующего уровня по формуле:
  autodiscover.<почтовый-домен>.
  указывающая на имя хоста почтовой системы. Пример:

```
autodiscover.domain.ru. CNAME mail.domain.ru.
```

- Для доступа клиентских приложений к контактам и корпоративным адресным книгам тип **SRV** для домена следующего уровня по формуле:

  _carddavs._tcp.<почтовый-домен>.

  указывающая вес, приоритет, 443 порт и имя хоста почтовой системы. Пример:

  ```
  _carddavs._tcp.domain.ru. SRV 0 1 443 mail.domain.ru.
  ```

- Для доступа клиентских приложений к календарям и задачам тип **SRV** для домена следующего уровня по формуле:

  _caldavs._tcp.<почтовый-домен>.

  указывающая вес, приоритет, 443 порт и имя хоста почтовой системы. Пример:

  ```
  _caldavs._tcp.domain.ru. SRV 0 1 443 mail.domain.ru.
  ```

Проверка DNS записей для входящих подключений

Обратите внимание, что для корректной обработки **PTR** записей почтовых серверов, от которых RuPost получает письма, балансиры почтовой системы должны передавать соответствующие заголовки узлам RuPost, используя **Proxy Protocol**. Для работы протокола необходимо в общих настройках почтовой системы, на вкладке «*Кластер*», указать в поле «*IP адреса внешних proxy*» все IP балансиров почтовой системы, использующих **Proxy Protocol**. Данная информация актуальна для корпоративной редакции (Enterprise).

3. Установка RuPost

3.1. Установка системы

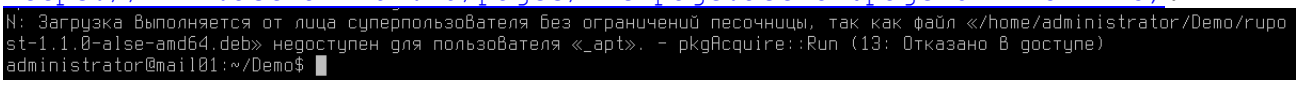
Для установки из deb-пакета необходимо выполнить следующую команду:

```
sudo apt install <путь к deb-пакету>
```

или

```
sudo dpkg -i <путь к deb-пакету>
```

В конце установки может отображаться предупреждение о том, что программа установки, не имея нужных прав доступа к текущему каталогу, вынуждена была получить привилегии root для выполнения установки. Установка при этом завершается успешно, и предупреждение можно игнорировать (т.к. связана с выполнением команды установки с правами суперпользователя – см. статью базы знаний Astra Linux https://wiki.astralinux.ru/pages/viewpage.action?pageId=144311245) .



Использование привилегий root необходимы системе RuPost для автоматического создания специальных системных пользователей и групп, применяемых для запуска и функционирования компонентов и служб RuPost.

Внимание!

Программа RuPost при установке заводит сервисную учетную запись `rupost` для работы приложения. Запрещено самостоятельно создавать пользователя `rupost` администраторам системы.

После установки системы необходимо запустить интерактивный конфигуратор RuPost (см. ниже), который помогает администратору указать стартовые параметры системы, позволяющие после этого начать использовать визуальную Панель управления и командный интерфейс CLI для дальнейшей настройки и управления системой.

3.2. Обновление системы

Внимание!

При обновлении системы с предыдущей версии требуется:

1. перед обновлением выполнить резервное копирование узла, на котором развернут(ы) RuPost;

2. установить .deb пакет новой версии на все узлы системы;

3. выполнить запуск конфигуратора rupost-wizard на всех узлах системы (в диалоговом или командном режиме);

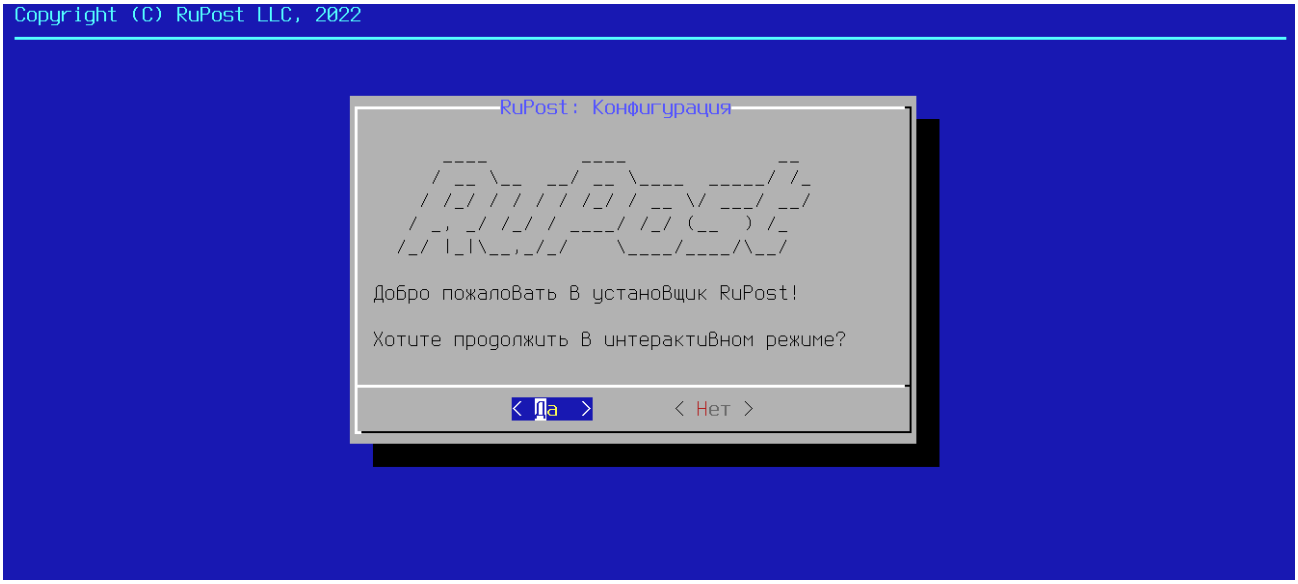
4. повторно развернуть активную конфигурацию с использованием обновленной версии необходимого шаблона конфигураций.

При обновлении системы нет необходимости останавливать процессы RuPost – они будут автоматически остановлены после обновления с сохранением всех конфигурационных параметров.

3.3. Конфигуратор RuPost

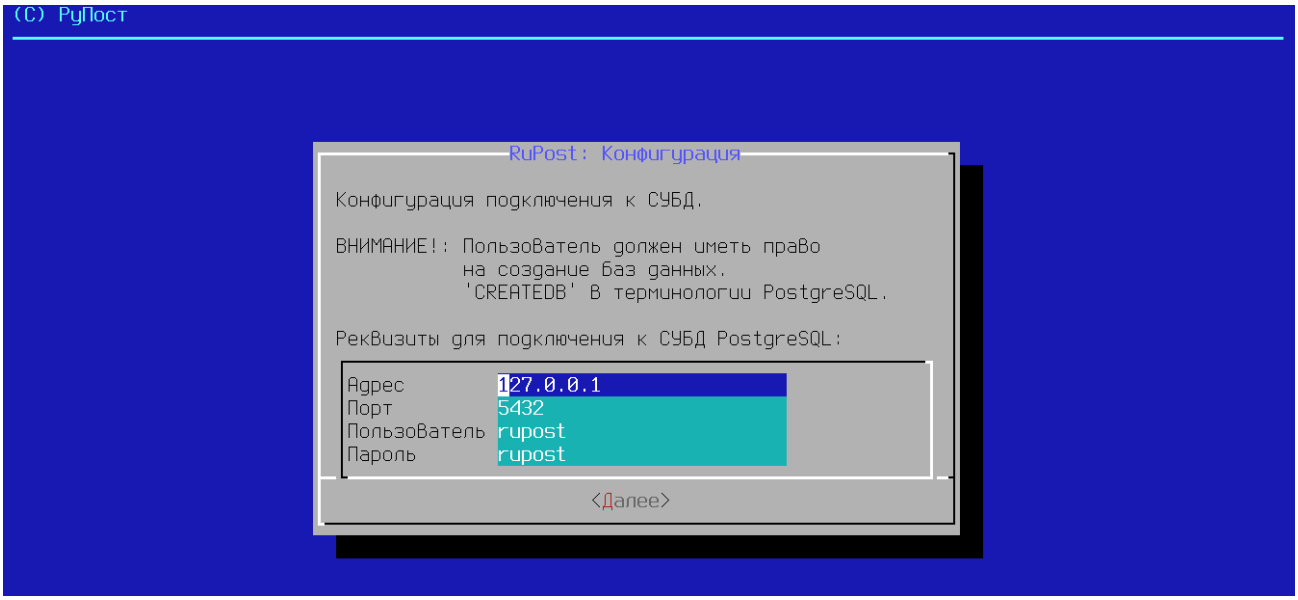
После выполнения команды установки (в том числе при обновлении с предыдущей версии RuPost) необходимо запустить интерактивный конфигуратор. Для этого используется команда:

```
sudo rupost-wizard
```



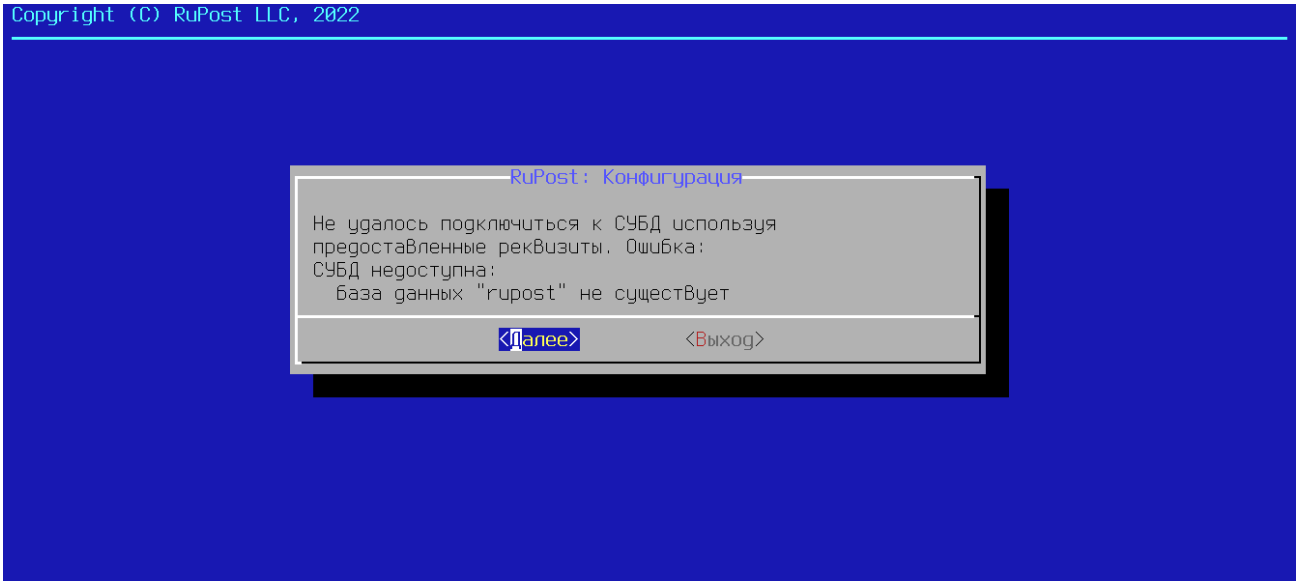
При нажатии кнопки “Нет” интерактивная конфигурация будет прервана.

Далее интерактивный конфигуратор запросит у пользователя данные для подключения к СУБД PostgreSQL:

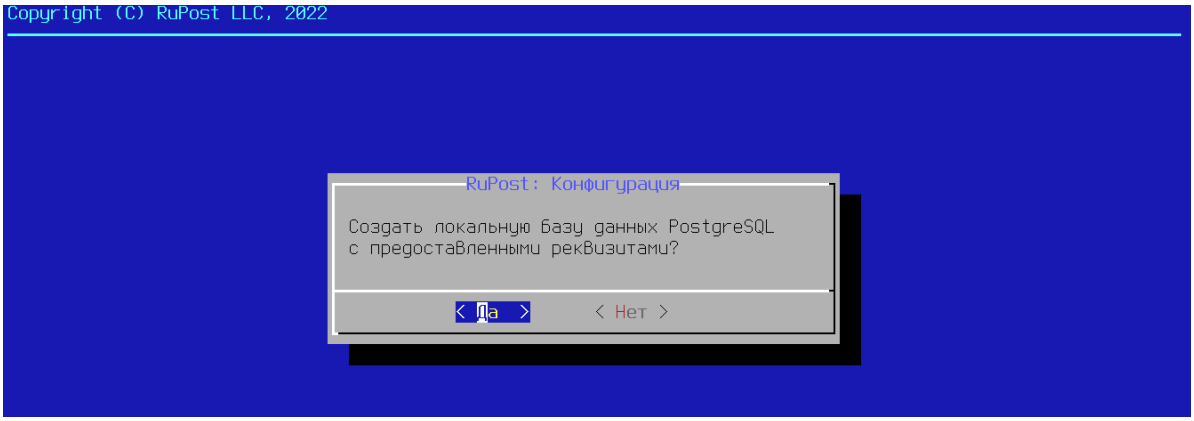


После ввода данных для подключения к СУБД и последующего выбора “Далее” будет выполнена попытка подключения к СУБД с использованием предоставленных реквизитов. В случае успеха будет выполнен переход к завершающему шагу.

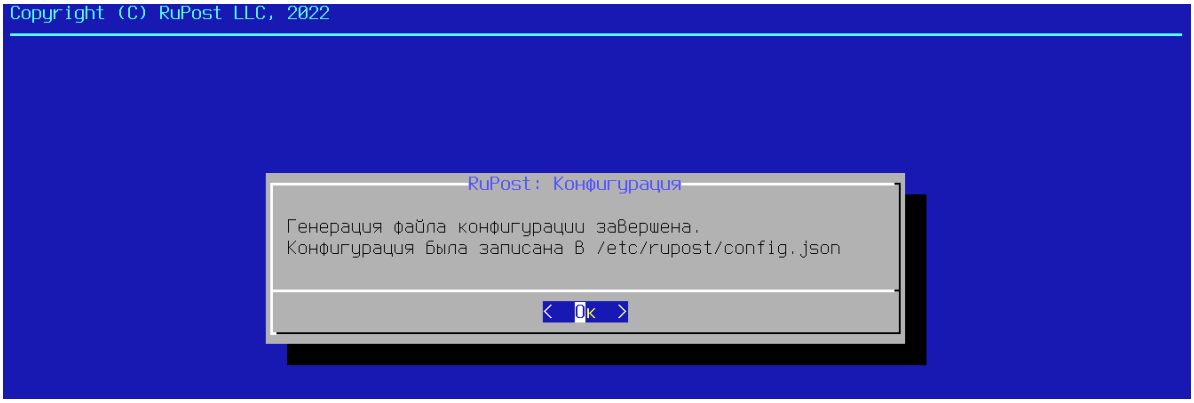
В случае, если интерактивному конфигуратору не удалось подтвердить корректность предоставленных реквизитов для подключения к СУБД, пользователю будет выведена ошибка, произошедшая во время попытки подключения:



Если СУБД установлена локально, то пользователю будет предложено произвести автоматическое создание пользователя и базы данных в СУБД с предоставленными ранее реквизитами посредством интерактивного конфигуратора:



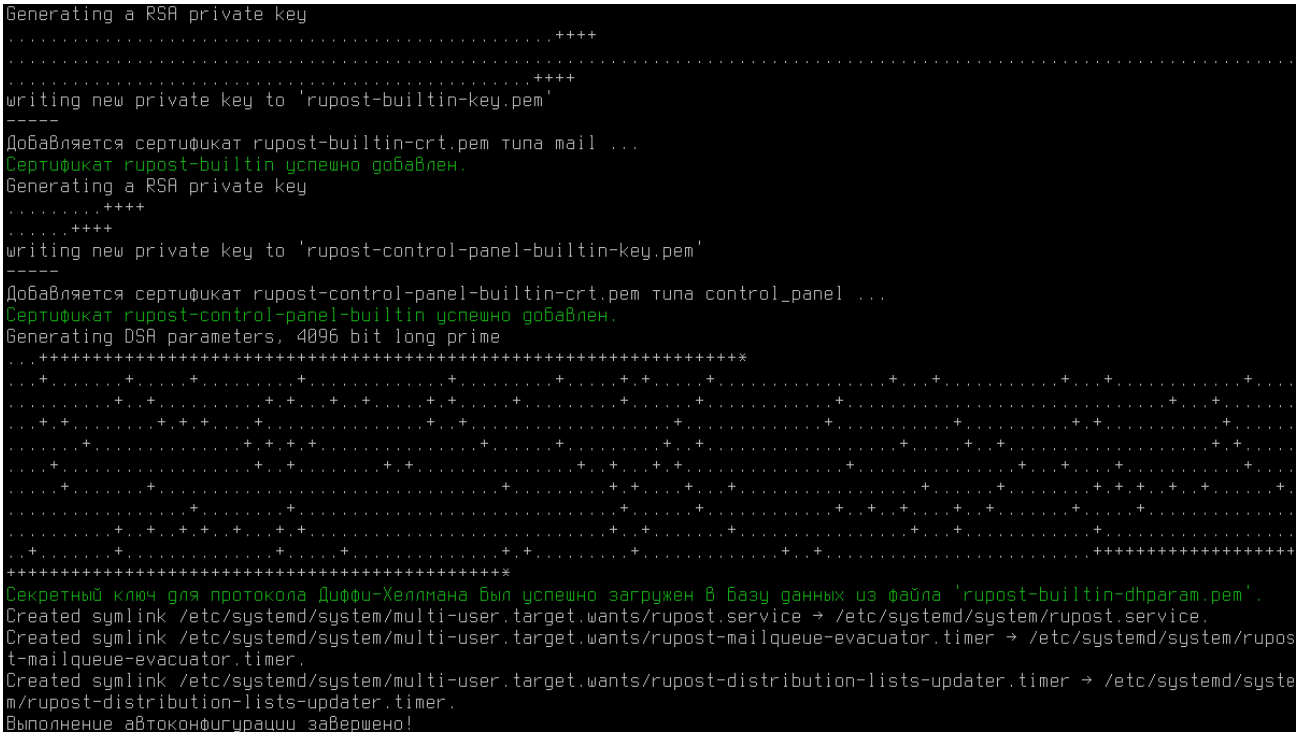
На завершающем этапе будет выполнена запись конфигурационного файла системы RuPost:



В процессе автоконфигурации производятся следующие действия, результат которых выводится в консоль:

1. Создается/мигрируется структура баз данных, необходимых для работы RuPost.
2. Загружаются стандартные (встроенные) шаблоны конфигураций почтовых компонентов.
3. Генерируется уникальный самоподписанный SSL сертификат RuPost (rupost-builtin), необходимый для подключения клиентских приложений по SSL/TLS (например, Thunderbird).
4. Генерируется уникальный самоподписанный SSL сертификат (rupost-control-panel-builtin) для доступа к Панели управления RuPost по https.
5. Генерируется секретный ключ для протокола Диффи-Хеллмана (файл 'rupost-builtin-dhparam.pem', автоматически загружаемый в конфигурационную базу данных системы).
6. Регистрируется таймер отслеживания состояния узлов системы в кластерной конфигурации для эвакуации очереди сообщений сбойного узла на рабочий узел кластера.
7. Регистрируется таймер обновления внутренних списков рассылки на основе LDAP-фильтров.
8. Регистрируются другие внутренние службы и таймеры (при наличии необходимости).

По окончании выполнения автоконфигурации администратор увидит следующий вывод в консоль:



3.3.1. Командный интерфейс конфигуратора rupost-wizard (CLI)

Командный интерфейс конфигуратора rupost-wizard предназначен для решения задач автоматизации развертывания экземпляров RuPost (настройка подключения к СУБД, определение администратора по-умолчанию и т.п.), управление которыми в дальнейшем осуществляется через Панель управления в браузере.

Флаги вызова `rupost-wizard`:

`--help` вывести данное сообщение и выйти
`--silent` провести автоконфигурацию в "тихом" режиме, без использования графического конфигуратора

Аргументы, используемые при флаге --silent:
`--db-host HOST` (или `-h HOST`), где HOST = адрес для подключения к СУБД
`--db-port PORT` (или `-p PORT`), где PORT = порт для подключения к СУБД
`--db-name NAME` (или `-n NAME`), где NAME = имя базы данных RuPost (rupost)
`--data-db-name NAME` (или `-d NAME`), где NAME = имя базы пользовательских данных (rupost_data)
`--logs-db-name NAME` (или `-l NAME`), где NAME = имя базы данных журналов (rupost_logs)
`--db-user USERNAME` (или `-u USERNAME`), где NAME = имя пользователя для подключения к СУБД
`--db-password PASSWORD`, где PASSWORD = пароль для подключения к СУБД (может быть передан и через переменную окружения `RUPOST_INSTALLER_DB_PASSWORD`).Пароль должен быть заключен в одинарные кавычки.

Пример вызова:

```
rupost-wizard --silent --db-host 127.0.0.1 --db-port 5432 --db-user rupost --
db-password 'rupost' --db-name rupost --data-db-name rupost_data --logs-db-
name rupost_logs
```

3.4. Подготовка системы к реальной эксплуатации (меры информационной безопасности)

Внимание!

Совокупность представленных ниже мер требуется для снижения рисков информационной безопасности.

3.4.1. Генерация устойчивого уникального ключа Диффи-Хеллман.

Данное действие необходимо для обеспечения прямой секретности SSL-соединений (Forward Secrecy). Генерируемый ключ не должен использоваться для получения каких-либо дополнительных ключей.

```
openssl dhparam -out rupost-builtin-dhparam.pem 4096
```

Добавление производится вызовом командного интерфейса RuPost CLI:

```
rupost dhparam import /путь/rupost-builtin-dhparam.pem
```

Достаточно сделать это один раз, так как в конфигурационной базе данных RuPost хранится только один экземпляр ключа, и он автоматически распространяется на все узлы системы при развёртывании конфигурации.

Внимание!

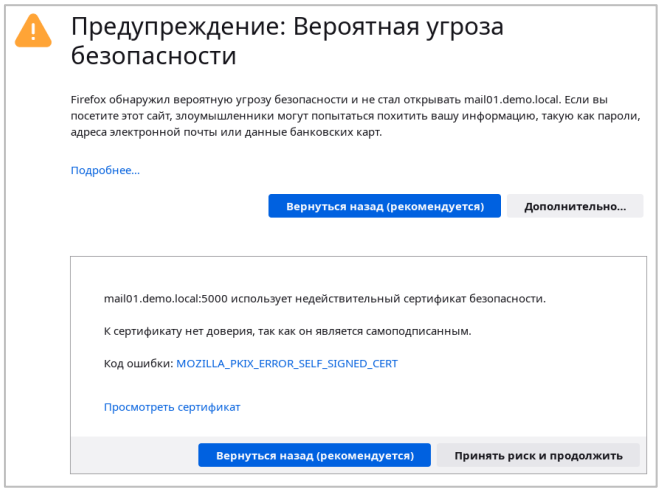
После обновления ключа необходимо повторно развернуть активную конфигурацию.

3.4.2. Использование валидных корпоративных сертификатов.

Внимание!

Генерируемые самоподписанные сертификаты требуют для реальной эксплуатации замены на действительные (валидные) сертификаты с использованием корпоративного Удостоверяющего Центра (УЦ – CA, Certificate Authority).

При продолжении использования самоподписанных сертификатов вы будете получать ошибки. Например, при входе в Панель администратора вы увидите предупреждение о вероятной угрозе безопасности.



Поддерживаемые типы сертификатов:

- mail - SSL сертификат почтового сервера RuPost
- control_panel - SSL сертификат панели управления

Для добавления собственных сертификатов, используемых при подключении клиентских приложений, необходимо выполнить команду:

```
rupost cert add "mail_cert" \
    --login mailadmin \
    --cert-type mail \
    --cert-path certs/rupost-mail.crt \
    --key-path certs/rupost-mail.key
```

где:

- `mail_cert` - имя сертификата которое будет отображаться в БД
- `mailadmin` - имя администратора от имени которого происходит загрузка
- `mail` - тип сертификата
- `certs/rupost-mail.crt` - путь до сертификата
- `certs/rupost-mail.key` - путь до ключа

Добавление сертификата для Панели управления аналогично процессу добавления сертификата для клиентских приложений. Ключевым отличием является то, что используется другой тип:

```
rupost cert add "control_panel_cert" \
    --login mailadmin \
    --cert-type control_panel \
    --cert-path certs/rupost-control-panel.crt \
    --key-path certs/rupost-control-panel.key
```

Внимание!

При добавлении сертификата с типом "control_panel" он не будет применен до принудительной перезагрузки сервиса rupost. В случае кластера это необходимо сделать на всех узлах системы.

Обновление системы с использованием интерактивного конфигуратора останавливает все компоненты системы на выбранном узле. После обновления требуется переразвернуть конфигурацию почтовых служб RuPost с использованием обновленной версии необходимого шаблона конфигураций. При запуске конфигуратора сохраняются параметры системы - общие настройки, зарегистрированные службы каталогов, почтовые домены, почтовые ящики и т.п.

3.5. Действия после установки и настройка системы

Дальнейшая настройка и управление RuPost осуществляется через командный интерфейс или в графической **Панели управления** RuPost, описанным в *Руководстве администратора*.

Панель управления доступна из web-браузера по имени или адресу узла RuPost по порту 5000, например локально (находясь на выбранном узле):

```
https://localhost:5000
```

или по имени хоста почтовой системы:

```
https://mail01.demo.local:5000
```

Список доступных команд RuPost CLI можно получить, выполнив команду

```
sudo rupost
```

или

```
sudo rupost --help
```

```
administrator@mail01:~/Demo$ sudo rupost
[sudo] пароль для administrator:
Usage: rupost [OPTIONS] COMMAND [ARGS]...

  RuPost CLI

Options:
  --help  Show this message and exit.

Commands:
  about               Выводит краткую сводку о приложении
  add-license         Добавляет файл лицензии из каталога или напрямую
  admins              Группа команд для управления администраторами
  cert                Группа команд для управления сертификатами
  components          Управляет почтовыми компонентами
  db                  Управляет базой данных
  distribution-lists  Группа команд для управления почтовыми рассылками
  impersonation       Группа команд для управления аккаунтами имперсонации
  ldap-filters        Группа команд для управления фильтрами LDAP.
  licenses            Управление лицензиями.
  mailboxes           Управляет почтовыми ящиками
  mailqueues          Управление почтовыми очередями.
  push                Группа команд для управления push уведомлениями.
  resources           Группа команд для управления ресурсами календаря
  run                 Запускает приложение
  template            Управляет шаблонами конфигураций
```

Внимание!

Часть функций RuPost доступна только через командный интерфейс CLI или Панель управления.

3.6. Удаление RuPost из операционной системы

Для удаления RuPost выполните команду

```
sudo apt remove rupost
```

Внимание!

Почтовые ящики, размещенные в файловой системе, не удаляются. Файл лицензии не удаляется. Файл конфигурации config.json экземпляра (узла) RuPost удаляется (см. *“Руководство администратора RuPost”*).

3.7. Основные пути и файлы системы

Ключевые файлы и директории, необходимые администратору системы:

Путь	Описание
/usr/bin/rupost	Главный исполняемый файл RuPost
/usr/bin/rupost-wizard	Интерактивный конфигуратор
/etc/rupost	Директория с файлом настроек config.json и файлом лицензии редакции Standard
/etc/systemd/system/rupost*.service /etc/systemd/system/rupost*.timer	Службы RuPost (unit-файлы): /etc/systemd/system/rupost.service /etc/systemd/system/rupost-distribution-lists-updater.service /etc/systemd/system/rupost-distribution-lists-updater.timer /etc/systemd/system/rupost-mailqueue-evacuator.service /etc/systemd/system/rupost-mailqueue-evacuator.timer /etc/systemd/system/rupost-scheduler.service
/var/log/rupost/monitor.log	Файл журнала RuPost
/usr/lib/rupost	Каталог с репозиторием, автогенерируемым самоподписанным сертификатом и вспомогательными программами и библиотеками, необходимыми для корректного функционирования RuPost

Системные журналы компонентов системы:

- Объединённый лог dovecot и postfix располагается по пути `/var/log/mail.log`. Он удобен для того, чтобы отслеживать факт отправки/получения писем и взаимодействие этих двух ключевых почтовых компонентов.
- Отдельно лог dovecot можно вывести в stdout командой `journalctl -u dovecot` либо сохранить во временный файл `journalctl -u dovecot > /tmp/dovecot.log`.
- Лог встроенного web-клиента и сервера календарей и контактов почтового компонента SOGo располагается по пути `/var/log/sogo/sogo.log`.
- Лог прокси-сервера Nginx с информацией по доступу к ресурсам пишется в файл `/var/log/nginx/access.log`, а сообщения об ошибках в работе того же компонента можно получить в файле `/var/log/nginx/error.log`.
- Лог компонента HAProxy доступен в файле `/var/log/haproxy.log`.

Дополнительные файлы:

Для корректной поддержки масштабируемости серверов RuPost система автоматически добавляет исключения для сервиса `dovecot.service` с целью снятия ограничений на число подключений к серверу. Для этого создается файл `/etc/systemd/system/dovecot.service.d/override.conf` и в нем автоматически устанавливаются следующие параметры сервиса:

- `LimitNOFILE=1048576`
- `LimitNPROC=4194304`

Приложение 1. Функциональное взаимодействие RuPost с подключенными доменами LDAP

1. Права доступа к атрибутам у служебной учётной записи RuPost

1.1 . FreeIPA

Служебная учётная запись должна обладать следующими правами на атрибуты пользователей RuPost.

Имя attributeTypes	Требуемые права
cn	чтение, поиск, сравнение
givenName	чтение, поиск, сравнение
l	чтение, поиск, сравнение
mail	чтение, запись, добавление, удаление, поиск, сравнение
mobile	чтение, поиск, сравнение
sn	чтение, поиск, сравнение
st	чтение, поиск, сравнение
street	чтение, поиск, сравнение
title	чтение, поиск, сравнение
employeeNumber	чтение, поиск, сравнение
employeeType	чтение, поиск, сравнение
facsimileTelephoneNumber	чтение, поиск, сравнение
ou	чтение, поиск, сравнение
pager	чтение, поиск, сравнение
proxyAddresses	чтение, запись, добавление, удаление, поиск, сравнение
objectClass	чтение, запись, поиск, сравнение
uid	чтение, поиск, сравнение
ipaUniqueID	чтение, поиск, сравнение

1.2 . ALD Pro

Служебная учётная запись должна обладать следующими правами на атрибуты пользователей RuPost.

Имя attributeTypes	Требуемые права

cn	чтение, поиск, сравнение
givenName	чтение, поиск, сравнение
l	чтение, поиск, сравнение
mail	чтение, запись, добавление, удаление, поиск, сравнение
mobile	чтение, поиск, сравнение
sn	чтение, поиск, сравнение
st	чтение, поиск, сравнение
street	чтение, поиск, сравнение
title	чтение, поиск, сравнение
c	чтение, поиск, сравнение
employeeNumber	чтение, поиск, сравнение
proxyAddresses	чтение, запись, добавление, удаление, поиск, сравнение
rbtadp	чтение, поиск, сравнение
rbtamiddlename	чтение, поиск, сравнение
telephoneNumber	чтение, поиск, сравнение
objectClass	чтение, запись, поиск, сравнение
uid	чтение, поиск, сравнение
ipaUniqueID	чтение, поиск, сравнение

1.3 . Active Directory

Служебная учётная запись должна обладать следующими правами на атрибуты пользователей RuPost.

Имя attributeTypes	**Требуемые права**
cn	чтение, поиск, сравнение
givenName	чтение, поиск, сравнение
l	чтение, поиск, сравнение
mail	чтение, запись, добавление, удаление, поиск, сравнение
mobile	чтение, поиск, сравнение
sn	чтение, поиск, сравнение
st	чтение, поиск, сравнение
street	чтение, поиск, сравнение

title	чтение, поиск, сравнение
company	чтение, поиск, сравнение
department	чтение, поиск, сравнение
facsimileTelephoneNumber	чтение, поиск, сравнение
homePhone	чтение, поиск, сравнение
pager	чтение, поиск, сравнение
proxyAddresses	чтение, запись, добавление, удаление, поиск, сравнение
objectClass	чтение, запись, поиск, сравнение
sAMAccountName	чтение, поиск, сравнение
objectGUID	чтение, поиск, сравнение

2. Функциональное использование объектных классов и атрибутов LDAP

2.1 . Классы

В службах каталогов FreeIPA и ALD Pro (актуально для версии 1.1.1) все пользователи должны обладать объектным классом *ruPostMailAccount* (OID 1.3.6.1.4.1.57980.3.1.1.1). Данный класс выполняет две роли:

- позволяет учётным записям наследовать атрибут *proxyAddresses* (OID 1.3.6.1.4.1.57980.3.1.2.2);
- применяется в фильтрах привилегий и разрешений, которые накладываются на сервисную учётную запись RuPost в службе каталогов.

Для службы каталогов Active Directory расширять схему указанным классом и дополнительными атрибутами не требуется.

2.2 . Ключевые атрибуты

Ключевыми атрибутами учётных записей LDAP у пользователей RuPost являются:

- «mail»: в этот атрибут при заведении пользователя записывается первичный почтовый псевдоним пользователя. На этот атрибут опирается процедура аутентификации пользователя компонентами RuPost.

  Внимание! Любое изменение и правка указанного атрибута для существующего в системе RuPost пользователя приведёт к неработоспособности связанного с ним почтового аккаунта! Этим атрибутом должна управлять только система RuPost.

- «proxyAddresses»: в этот атрибут записывается первичный почтовый псевдоним пользователя, а также его дополнительные псевдонимы в синтаксисе аналогичном для одноимённого атрибута в Active Directory. Запись в этот атрибут системой RuPost осуществляется только при заведении для

учётной записи LDAP почтового ящика. В дальнейшем целостность этого атрибута не проверяется, а также он не участвует в mail flow и других критично важных функциях почтовой системы. Основная задача атрибута состоит в сообщении внешним системам всех почтовых псевдонимов пользователя.

- «objectGUID/ipaUniqueID (в зависимости от службы каталогов)»: RuPost опирается на данный атрибут для контроля актуальности ФИО, логина, подразделения и др. пользовательской информации.
- «uid/sAMAccountName (в зависимости от службы каталогов)»: логин учётной записи. Применяется для поиска учётных записей, автоматического формирования имени первичного почтового псевдонима нового ящика, в процессе миграции ящиков из системы электронной почты Microsoft Exchange в RuPost.

Указанные далее атрибуты используются для формирования глобальной адресной книги (GAL), автоматически подключаемой всем пользователям почтовой системы RuPost.

3.7.1. FreeIPA атрибуты для глобальной адресной книги

Имя attributeTypes	**Функциональное назначение**
cn	Полное имя
givenName	Имя
l	Город
mail	Первичный адрес электронной почты
mobile	Мобильный телефон
sn	Фамилия
st	Регион
street	Улица
title	Должность
employeeNumber	Дополнительный номер
employeeType	Роль
facsimileTelephoneNumber	Факс
ou	Департамент
pager	Пейджер
proxyAddresses	Электронная почта

3.7.2. ALD Pro

Имя attributeTypes	**Функциональное назначение**
cn	Полное имя
givenName	Имя

l	Город
mail	Первичный адрес электронной почты
mobile	Мобильный телефон
sn	Фамилия
st	Регион
street	Улица
title	Должность
c	Страна
employeeNumber	Дополнительный номер
proxyAddresses	Электронная почта
rbtadp	Департамент
rbtamiddlename	Отчество
telephoneNumber	Рабочий телефон

3.7.3. Active Directory

Имя attributeTypes	**Функциональное назначение**
cn	Полное имя
givenName	Имя
l	Город
mail	Первичный адрес электронной почты
mobile	Мобильный телефон
sn	Фамилия
st	Регион
street	Улица
title	Должность
company	Компания
department	Департамент
facsimileTelephoneNumber	Факс
homePhone	Домашний телефон
pager	Пейджер
proxyAddresses	Электронная почта

Приложение 2. Сетевые настройки (порты)

На узле с установленным ПО Rupost должны быть открыты следующие входящие порты:

Порт	Протокол	Источник	Описание
tcp/25	SMTP (STARTTLS)	Интернет, интранет	Входящий почтовый трафик от других серверов (и/или от Relay сервера)
tcp/465	SMTPS	Интернет, интранет	SMTPS (SMTP Secure) Входящий почтовый трафик от клиентов
tcp/993	IMAPS	Интернет, интранет	IMAPS (IMAP Secure) доступ к электронной почте.
tcp/4190	SIEVE-TLS	Интернет, интранет	работа с пользовательскими фильтрами
tcp/80	HTTP	Интернет, интранет	301 код возврата (Moved Permanently) на 443 порт HTTPS, незащищенный Autodiscovery
tcp/443	HTTPS	Интернет, интранет	WEB клиенты, защищенный Autodiscover
tcp/5000	HTTP	Интранет	Панель управления RuPost
tcp/10000	TCP	Интранет	Связь между узлами кластера
tcp/20025	SMTP	Интранет	дополнительные проверки Healthcheck в кластере