



Почтовая система RuPost

Руководство по установке и конфигурированию

© 2021-2023, ООО «РуПост» (RuPost, LLC.). Все права защищены.

РуПост, RuPost, WorksPad, логотип WorksPad являются торговыми марками или зарегистрированными торговыми марками РуПост (RuPost, LLC.) в США, России и других странах.

Названия прочих компаний и продуктов, упомянутые здесь, могут являться товарными знаками соответствующих компаний.

Продукты сторонних фирм упоминаются исключительно в информационных целях и конфигурирования зависимостей RuPost. Компания РуПост не несет ответственности за эксплуатационные качества и использование этих продуктов. Все договоренности, соглашения или гарантийные обязательства, при наличии таковых, заключаются непосредственно между поставщиком и потенциальными пользователями. При составлении данного руководства были предприняты все усилия для обеспечения достоверности и точности информации. Данное руководство является предметом изменений в соответствии с динамикой развития продукта и может не содержать наиболее последних версий копий экранов, имен параметров и других характеристик продукта. РуПост не несет ответственности за опечатки или описки.

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

Оглавление

1. Обзор системы	5
1.1. Функциональные возможности RuPost	5
1.2. Архитектура и компоненты сервера RuPost	6
1.3. Отказоустойчивый кластер RuPost	9
2. Подготовка к установке RuPost.....	12
2.1. Системные требования	12
2.2. Операционная система	13
2.3. Синхронизация времени.....	13
2.4. Службы каталогов LDAP.....	14
2.4.1. Служебная учётная запись	14
2.4.2. Интеграция с ALD Pro	14
2.4.3. Подготовка FreeIPA	14
2.4.4. Подготовка Microsoft Active Directory	15
2.5. Система управления базами данных	16
2.6. Служба кэширования объектов в оперативной памяти Memcached	17
2.7. Подключение сетевых каталогов файловой системы NFSv4	17
2.8. Настройки DNS	18
3. Установка RuPost.....	20
2.9. Установка системы.....	20
2.10. Обновление системы.....	20
2.11. Конфигуратор RuPost.....	21
2.11.1. Командный интерфейс конфигуратора rupost-wizard (CLI).....	24
2.12. Подготовка системы к реальной эксплуатации (меры информационной безопасности)	25
2.12.1. Генерация устойчивого уникального ключа Диффи-Хеллман.....	25
2.12.2. Использование валидных корпоративных сертификатов.....	25
2.13. Действия после установки и настройка системы.....	27
2.14. Удаление RuPost из операционной системы	28
2.15. Основные пути и файлы системы	28
Приложение 1. Функциональное взаимодействие RuPost с подключенными доменами LDAP.....	30
1. Права доступа к атрибутам у служебной учётной записи RuPost	30
1.1 . FreeIPA.....	30
1.2 . ALD Pro	30

1.3 . Active Directory	31
2. Функциональное использование объектных классов и атрибутов LDAP.....	32
2.1 . Классы	32
2.2 . Ключевые атрибуты	32
2.15.1. FreeIPA атрибуты для глобальной адресной книги	33
2.15.2. ALD Pro	33
2.15.3. Active Directory	34
Приложение 2. Сетевые настройки (порты).....	35

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)
- Группы рассылки
- 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, P7)
- 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.

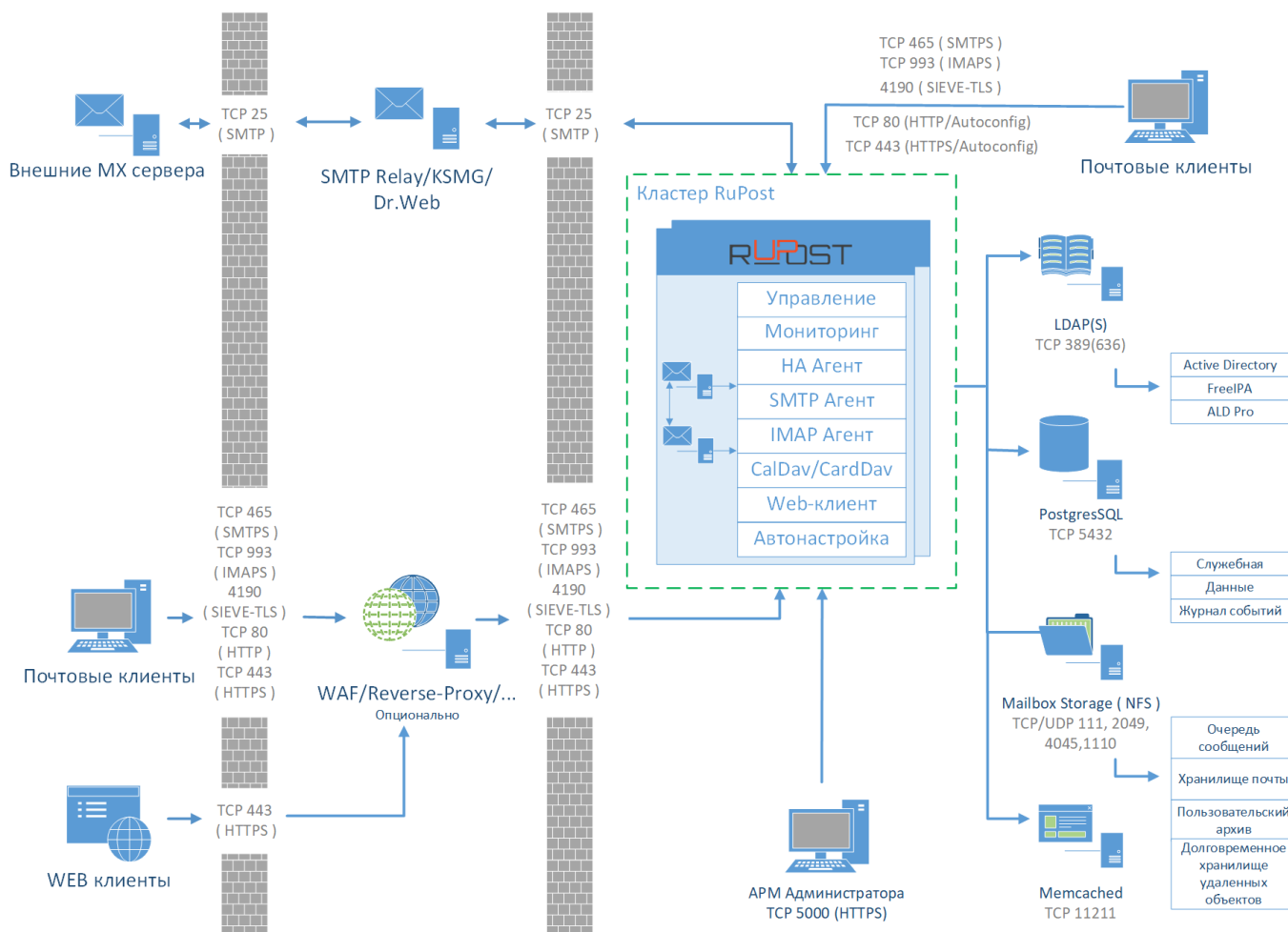
1.2. Архитектура и компоненты сервера RuPost

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 (APM 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;
 - переадресация сетевых соединений на внутренний веб-сервер доступа Nginx, терминирующий доступ к агентам SMTP и IMAP и серверу CalDav/CardDav.

- **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 CalDAV и CardDAV.
 - **Web-клиент корпоративной почты – SOGo.** Доступен во всех актуальных версиях современных браузеров.
 - **Web-сервер доступа (терминирующий обратный прокси-сервер) – Nginx.** Работает по протоколам TCP, HTTP(S), proxy-protocol. Сервис выполняет следующие функции:
 - 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.
 - **Компонент кеширования в оперативной памяти – Memcached.** Работает по протоколам TCP и UDP. Выполняет функцию кеширования 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.

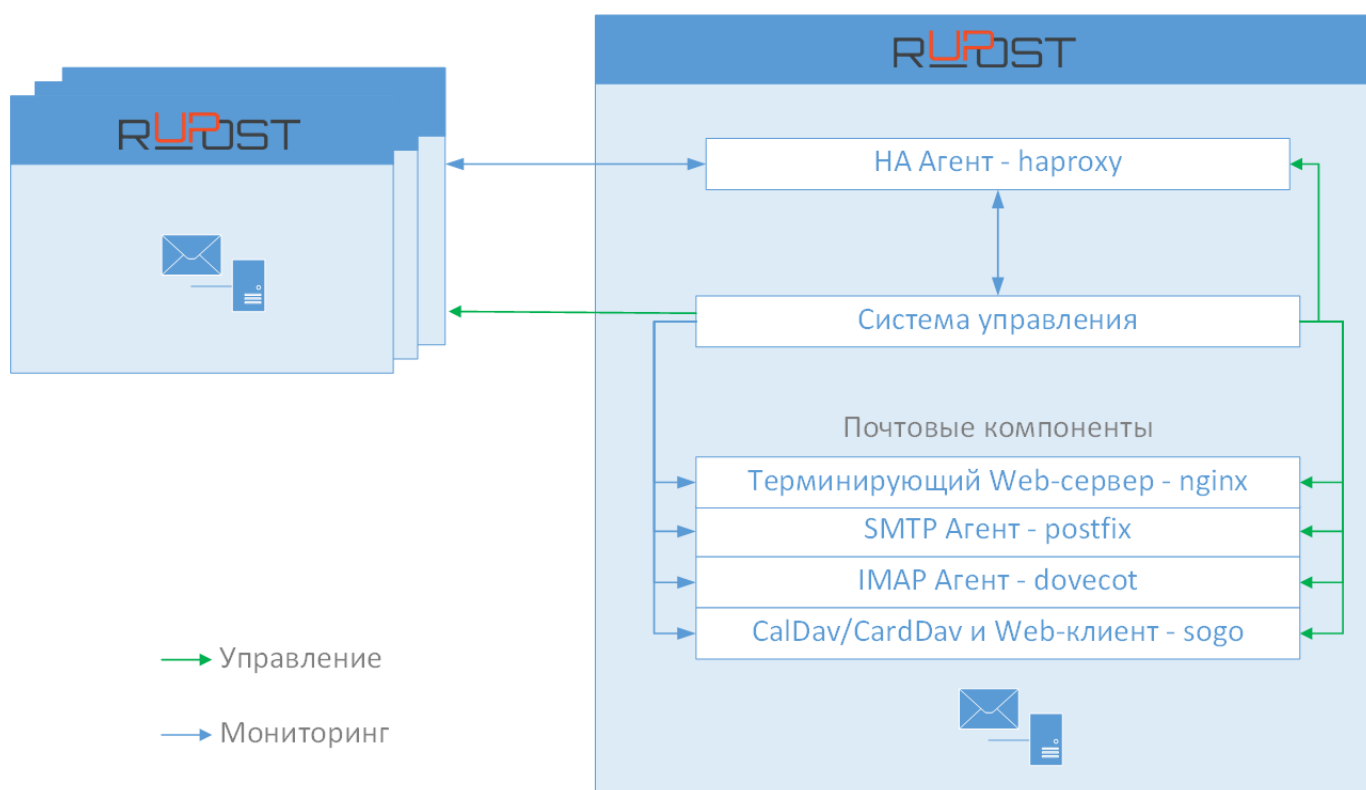
При **развертывании конфигурации** на базе выбранного шаблона система управления RuPost генерирует все необходимые конфигурационные файлы для компонентов системы.

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 функционируют 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:

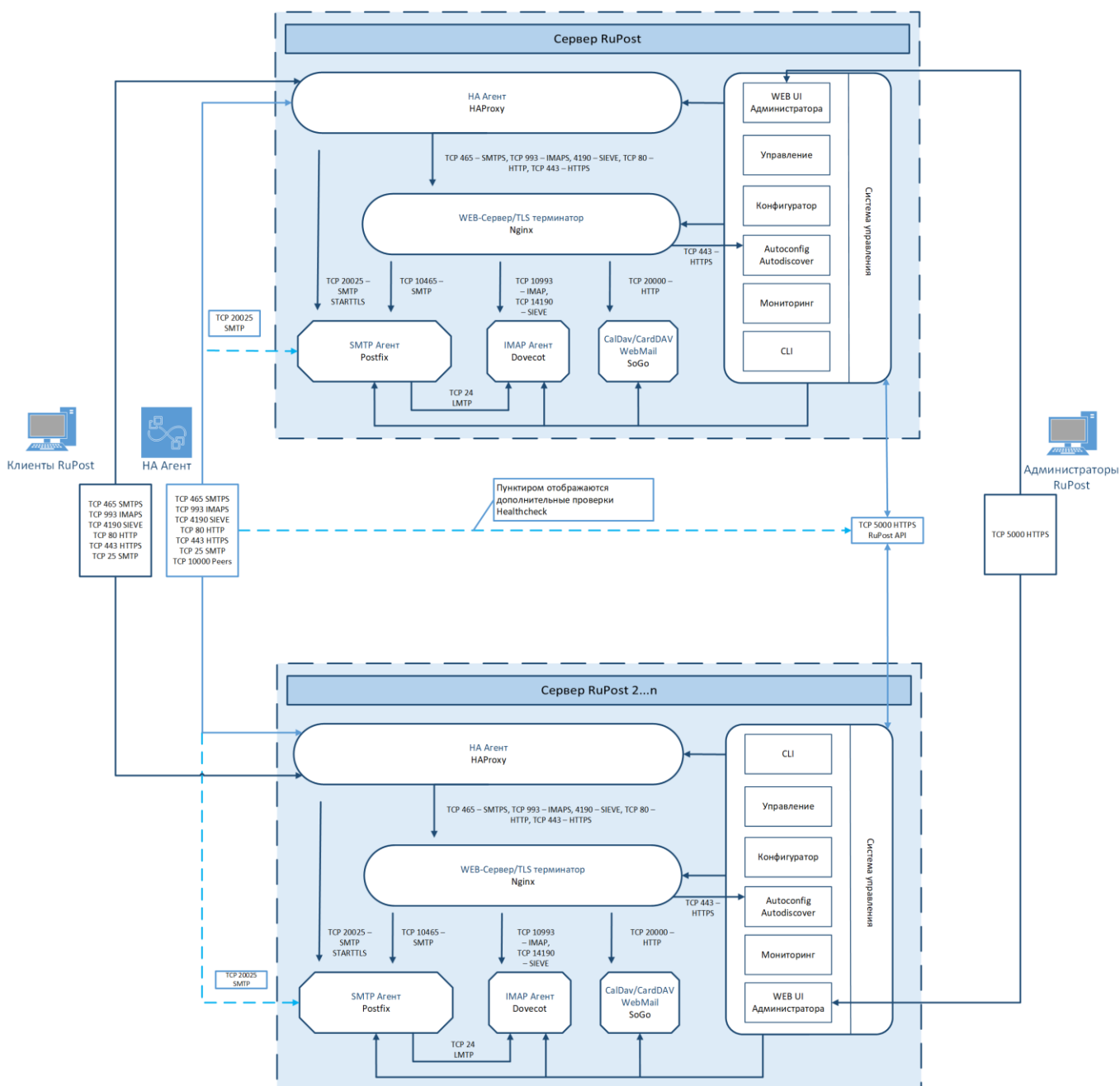


Схема взаимодействия компонентов и узлов кластера

При подключении клиентов к системе IP-адрес клиента привязывается к соответствующему узлу системы, на который он был распределен. Если в течение 30 минут после последнего обращения от клиента с соответствующим IP не поступает запросов, его адрес удаляется из таблицы привязки и может быть обслужен другим узлом. Если в пределах 60 минутного лимита по тем или иным причинам клиент попадает на другой узел кластера, то он будет автоматически перенаправлен на тот узел, к которому привязан его IP. 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 на другой доступный штатно функционирующий узел кластера.

Такая высокая доступность (высокий уровень отказоустойчивости) кластера RuPost достигается за счет постоянной синхронизации таблиц соответствия клиентов (stick table) на HA Агентах системы – HAProxy. Таким образом, для автоматизации балансировки нагрузки необходимо использовать те инструменты, которые обеспечивают прозрачность передачи исходного IP адреса клиента (Originating IP).

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

- Round Robin DNS с использованием А записи, указывающей на набор IP адресов узлов кластера
- Direct Routing
- TPROXY

Поддержка proxy protocol системой RuPost планируется в следующих обновлениях – соответственно, не рекомендуется использовать внешний HAProxy или другие балансировщики, распределяющие нагрузку на узлы системы по протоколу proxy.

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 «сервисы» можно устанавливать локально на этот же узел, где разворачивается RuPost.

2.2. Операционная система

Версия RuPost 2.0.1 поддерживает ОС **Astra Linux Special Edition (ALSE) 1.7** – 1.7.1, 1.7.2, 1.7.3 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-2.0.1-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
```

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, радиосигналы, 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 имеющих 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 файрвола 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. 2. 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 дополнительной настройки атрибутов для работы с RuPost (версии ALD Pro 1.2.x и выше).

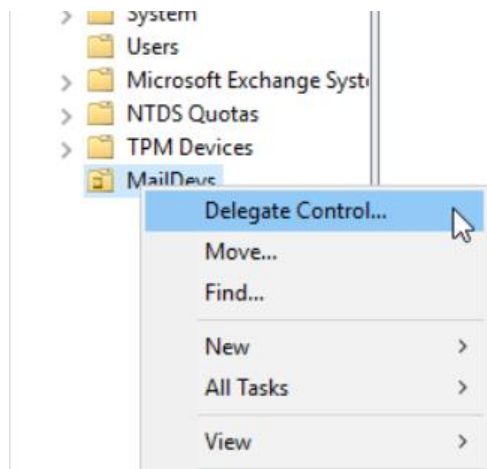
Для работы RuPost необходимо в ALD Pro завести служебную учётную запись.

2.4.3. Подготовка FreeIPA

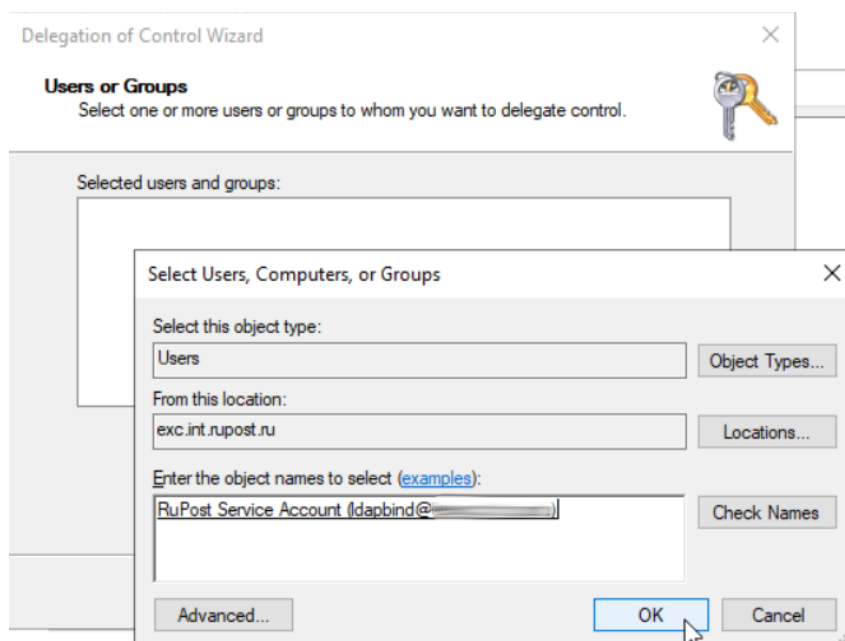
Для подготовки FreeIPA на мастер контроллере домена требуется выполнить bash сценарий, поставляемый вендором по соответствующему запросу.

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

Delegation of Control Wizard ×

Tasks to Delegate
You can select common tasks or customize your own. 

Delegate the following common tasks:

Create, delete, and manage user accounts

Reset user passwords and force password change at next logon

Read all user information

Create, delete and manage groups

Modify the membership of a group

Manage Group Policy links

Generate Resultant Set of Policy (Planning)

Create a custom task to delegate

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 configurator, который будет описан в разделе 2.4.

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>;
```


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.

Размер выделяемой памяти рассчитывается по формуле:

Требуемая память = 512k * (количество доменов LDAP) + (10k * 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 Memcached:

```
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.

2.8. Настройки DNS

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

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

- **А запись** - набор SMTP серверов узлов системы для получения почты или сервер в отдельности. Для кластера запись должна состоять из нескольких IP адресов узлов системы.
- **CNAME к А 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)

Для общедоступного (публичного) DNS:

- **А запись** - набор серверов RuPost для получения почты или релей-сервера, за которым находятся серверы RuPost. Запись может состоять из нескольких внешних IP адресов.
- **PTR** - провайдер на IP адрес, от которого набор узлов RuPost выполняет отправку сообщений, должен создать запись равную вашему SMTP EHLO (указывается в Общих настройках - Имя узла почтовой системы)

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 **каждого** почтового домена в обоих вариантах DNS ожидаются ниже указанные 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) со значением: `v=spf1 mx ~all`

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.`

3. Установка RuPost

2.9. 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 команду установки с правами суперпользователя – см. статью базы знаний Astra Linux <https://wiki.astralinux.ru/pages/viewpage.action?pageId=144311245>).

```
N: Загрузка выполняется от лица суперпользователя без ограничений песочницы, так как файл </home/administrator/Demo/rupost-1.1.0-alsa-amd64.deb> недоступен для пользователя <_apt>. - pkgAcquire::Run (13: Отказано в гостине)
administrator@mail01:~/Demo$
```

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.

2.10. Обновление системы

Внимание!

При обновлении системы с предыдущей версии требуется:

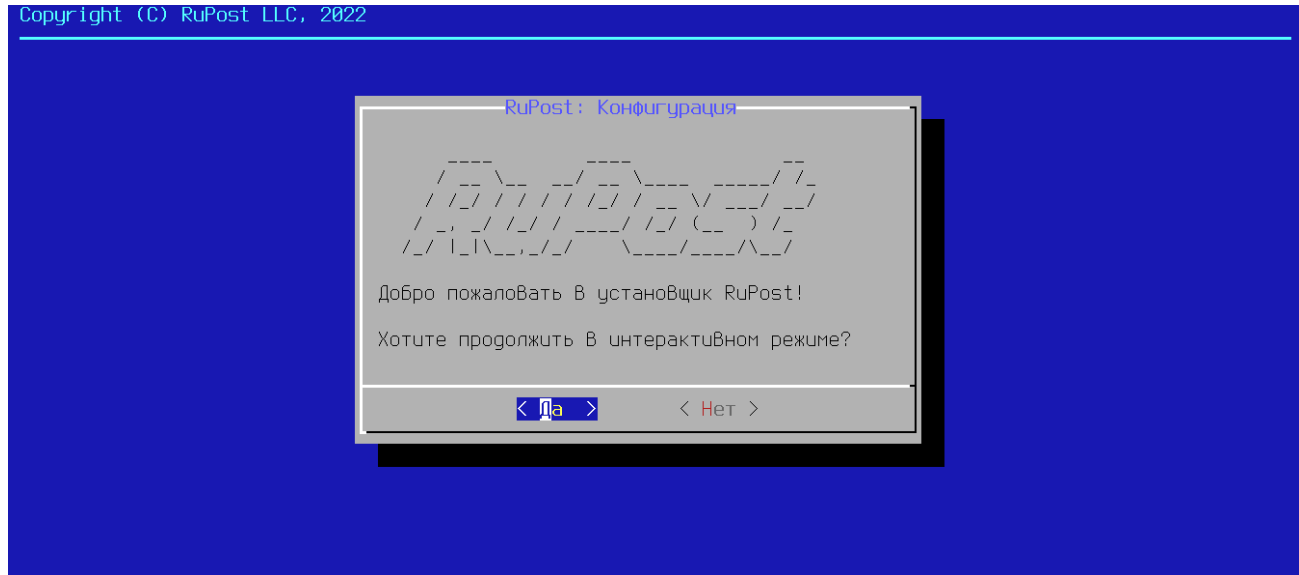
1. перед обновлением выполнить резервное копирование узла, на котором развернут(ы) RuPost;
2. установить .deb пакет новой версии на все узлы системы;
3. выполнить запуск конфигуратора `rupost-wizard` на всех узлах системы (в диалоговом или командном режиме);
4. повторно развернуть активную конфигурацию 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.

2.11. Конфигуратор RuPost

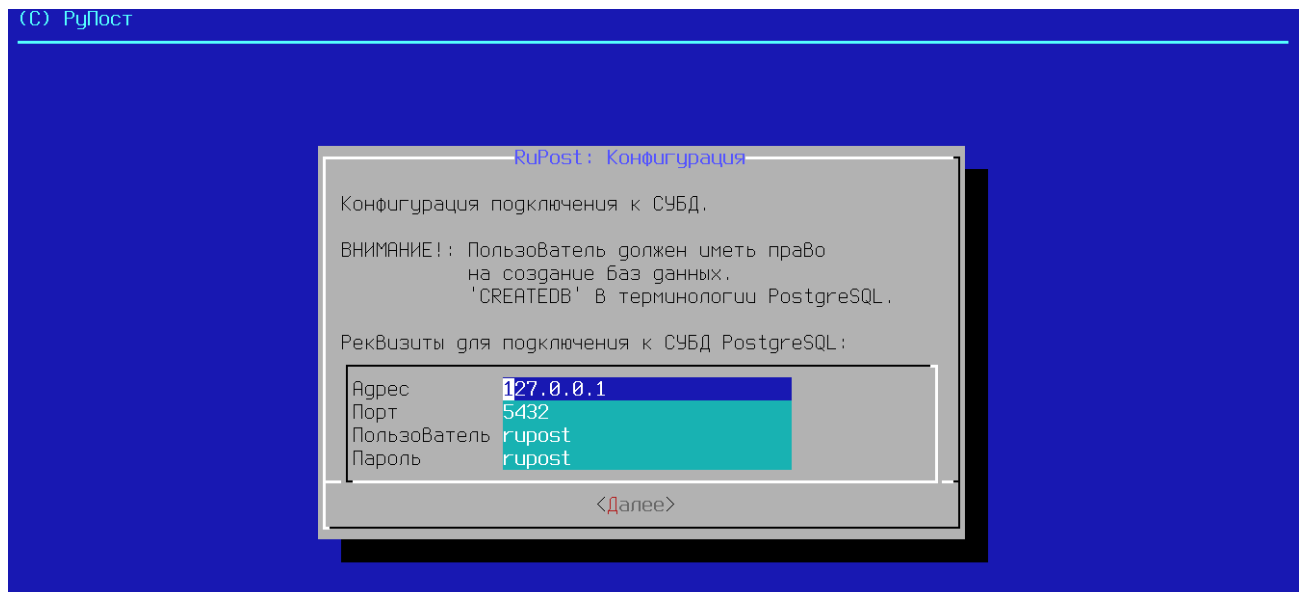
После выполнения команды установки (в том числе при обновлении с предыдущей версии RuPost) необходимо запустить интерактивный конфигуратор. Для этого используется команда:

```
sudo rupost-wizard
```



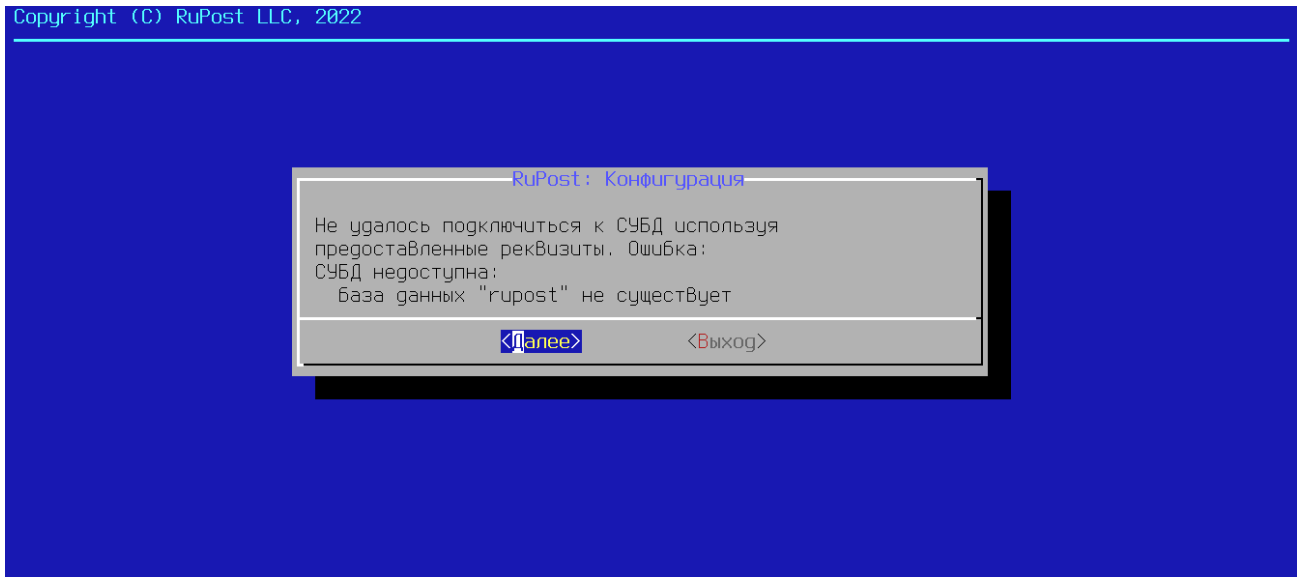
При нажатии кнопки “Нет” интерактивная конфигурация будет прервана.

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

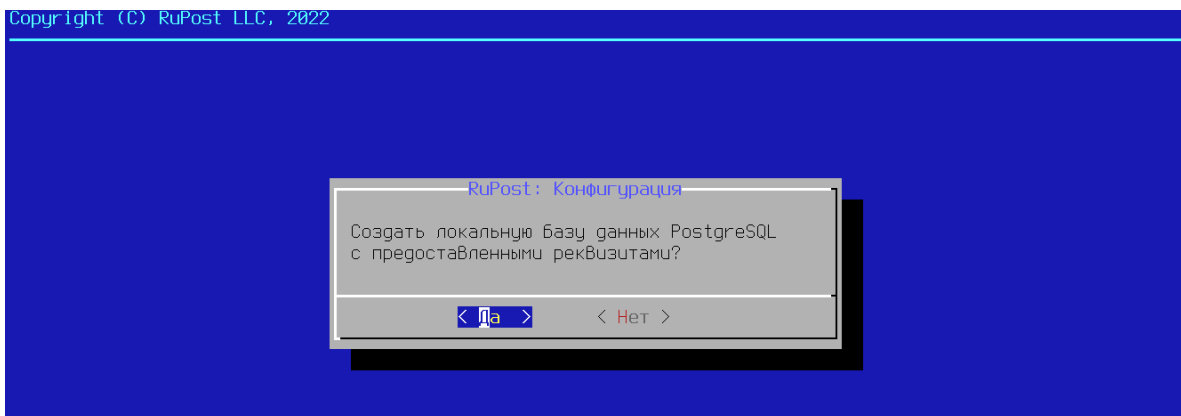


После ввода данных для подключения к СУБД и последующего выбора “Далее” будет выполнена попытка подключения к СУБД с использованием предоставленных реквизитов. В случае успеха будет выполнен переход к завершающему шагу.

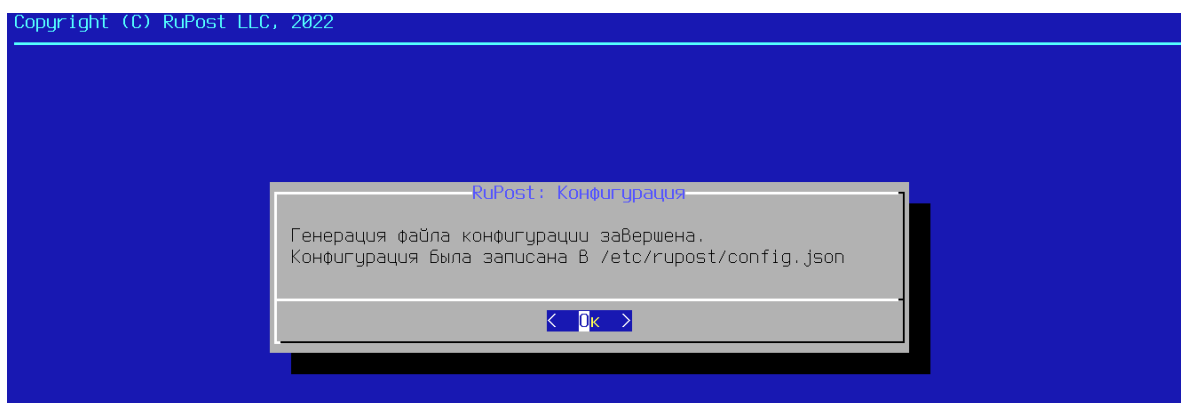
В случае, если интерактивному конфигуратору не удалось подтвердить корректность предоставленных реквизитов для подключения к СУБД, пользователю будет выведена ошибка, произошедшая во время попытки подключения:



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



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:

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

Внимание!

Совокупность представленных ниже мер требуется для снижения рисков информационной безопасности.

2.12.1. 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!

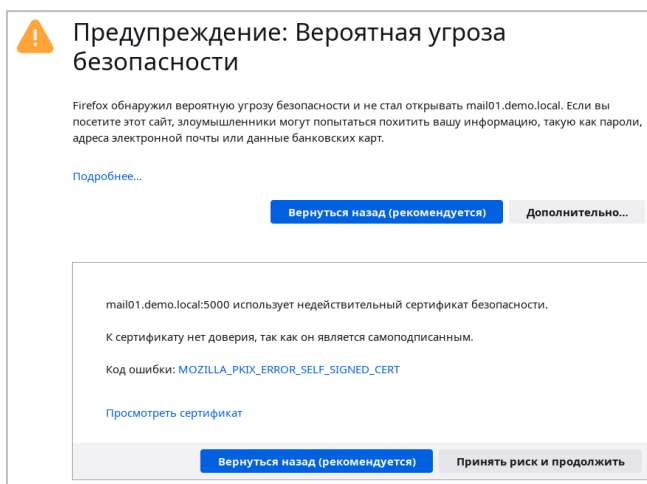
После обновления ключа необходимо повторно развернуть активную конфигурацию.

2.12.2. 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.



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.

2.13. 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.

2.14. 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”*).

2.15. 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 `SOG` 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 1.3.6.1.4.1.57980.3.1.2.1);
- 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.

2.15.1. 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

2.15.2. 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

2.15.3. 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 Rupos 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