Почтовая система RuPost

Руководство администратора

RU.47022019.10001-01 92 01

Версия 4.3.4 – Ноябрь 2026

© 2021-2026, ООО «РуПост». Все права защищены.

РуПост, RuPost, WorksPad, логотип WorksPad являются торговыми марками или зарегистрированными торговыми марками ООО РуПост в 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.

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

Оглавление

1. Концепция управления системой 9
2. Графическая Панель управления 11
2.1. Вход в Панель управления системы 11
2.1.1. Учетная запись встроенного администратора системы 11
2.1.2. Разграничение полномочий администраторов 11
2.1.3. Администраторы системы с аутентификацией в LDAP 13
1.1.3.1. Автоматическое добавление администраторов по фильтрам LDAP 16
1.1.3.2. Автоматическое назначение ролей администраторов по фильтрам LDAP 16
2.2. Домашняя страница Панели управления -“Мониторинг” (Dashboard) 18
2.2.1. Мониторинг инфраструктуры 23
2.2.2. Интеграция с Zabbix 28
2.3. Пошаговая "Быстрая настройка" в Панели управления 30
2.4. Управление лицензиями 31
2.4.1. Управление лицензиями через командный интерфейс CLI 31
2.4.2. Управление лицензиями в Панели управления 31
2.4.3. Лицензии для образовательных учреждений 31
2.5. Управление сертификатами 33
2.6. Общие настройки системы 33
2.6.1. Общие настройки – rupost-cs (Memcached) 34
2.6.2. Общие настройки - почта 36
2.6.3. Общие настройки - кластер 38
2.6.4. Общие настройки – число обработчиков web клиента 38
2.6.5. Общие настройки - отправка с разрешенных IP адресов без авторизации 38
2.6.6. Общие настройки - максимальное число получателей 39
2.6.7. Общие настройки - максимальная частота отправки писем (rate limit) 39
2.6.8. Общие настройки - максимальный размер письма 40
2.6.9. Возможность отключения сервиса postscreen 40
2.7. Подключение служб каталогов LDAP 41
2.8. Настройка почтовых доменов 44
2.9. Развертывание конфигураций 47
2.9.1. Библиотека шаблонов конфигураций 47
2.9.2. Создание конфигурации 50

© 2021-2026 РуПост

2.9.3. История конфигураций 53
2.9.4. Активная конфигурация 54
2.10. Мониторинг системы, управление и самодиагностика компонентов 55
2.10.1. Общие принципы 55
2.10.2. Контроль работы почтовых компонентов (Healthcheck) 55
2.10.3. Управление и мониторинг работы кластера 56
2.10.4. Пул соединений к базе данных 63
2.10.5. Работа с компонентами и узлами через командный интерфейс CLI 66
2.11. Пространства хранения, Группы ящиков и Хранилища 67
2.11.1. Управление Группами почтовых ящиков 70
2.11.2. Управление Пространствами хранения и Хранилищами 71
2.11.3. Периодическая очистка хранилища записей (RecordStorage) 74
2.11.4. Возможность перезапуска репликации холодной (backup) реплики 75
2.11.5. Настройка времени запуска холодной (backup) реплики 75
2.11.6. Работа хранилища при монтировании на части узлов кластера 76
2.11.7. Оптимизация алгоритма репликации хранилищ 77
2.11.8. Статус синхронизации реплики 79
2.11.9. Перенос почты в архив в соответствии с политикой архивации 79
2.12. Моментальные снимки состояния 83
2.13. Интеграция с СХД / SDS 85
2.14. Управление почтовыми ящиками 92
2.14.1. Создание почтовых ящиков 94
2.14.2. Управление почтовыми ящиками – CLI 97
2.14.3. Конструктор шаблонов почтовых адресов для импорта 98
2.14.4. Фильтры ящиков 99
2.14.5. Поиск почтовых ящиков 101
2.14.6. Групповые политики 101
2.14.7. Периодическая очистка папок “Удалённые” и “Спам” 104
2.14.8. Управление почтовым ящиком пользователя 105
2.14.9. Замена “владельца” почтового ящика 107
2.14.10. Переименования “владельца” почтового ящика (смена фамилии и почтового адреса) 108
2.14.11. Перенос почтового ящика в другое пространство хранения 109
2.14.12. Синхронизация с LDAP 113

© 2021-2026 РуПост

2.14.13. Перенос почтового ящика из одного каталога LDAP в другой при синхронизации 114
2.14.14. Динамические общие почтовые ящики 115
2.14.15. Отображение списка общих почтовых ящиков, к которым предоставлен доступ 117
2.15. Учетная запись имперсонации 119
2.16. Автоматическая обработка входящих сообщений, содержащих календарные события 120
2.17. Ресурсы календаря 121
2.17.1. Управление ресурсами календаря в Панели управления 122
2.17.2. Управление ресурсами календаря через командный интерфейс CLI 123
2.18. Списки рассылки 125
2.18.1. Оптимизация механизма рассылок 125
2.18.2. Фильтры LDAP 127
2.18.3. Динамические списки рассылки 129
2.18.4. Статические списки рассылки 129
2.18.5. Управление списками рассылки через командный интерфейс CLI 129
2.18.6. Управление списками рассылки в Панели управления 129
2.19. Правила обработки почты (ограничения) 134
2.20. Транспортные правила 137
2.20.1. Структура транспортных правил 137
2.20.2. Набор условий 139
2.20.3. Набор действий 140
2.20.4. Примеры транспортных правил 140
2.20.5. Создание транспортного правила 141
2.20.6. Проверка набора транспортных правил 144
2.20.7. Миграция почтовых правил 145
2.21. Поддержка SPF 147
2.22. Управление автоответами 148
2.23. Групповая политика – автоподпись 149
2.24. Трассировка писем 153
2.24.1. Трассировка писем – CLI 153
2.25. Аудит действий администратора – команда CLI audit 155
2.26. Просмотр логов почтовых компонентов в Панели управления 156
2.27. Единый лог для всех почтовых компонентов – команда CLI logs 158
2.28. Сбор и экспорт характеристик системы и лог файлов – команда CLI report 158

© 2021-2026 РуПост

2.29. Поддержка SOSReport ... 159
2.30. Глобальные правила фильтрации почты на сервере ... 159
2.31. Блокировка доступа в web клиент LDAP пользователей при отсутствии ящиков ... 160
2.32. Групповая политика - ограничение доступа к почтовым ящикам по протоколам POP3 / IMAP ... 160
2.33. Управление возможностью предоставления доступа к своему почтовому ящику всем пользователям ... 160
2.34. Система уведомлений администратора ... 161
2.35. Предупреждения пользователей об исчерпании квоты на место в почтовом ящике ... 162
2.36. Аудит действий пользователя в ящике ... 162
2.37. Поиск и удаление писем ... 163
2.37.1. Выгрузка найденных писем в формате eml ... 165
2.37.2. Отзыв писем ... 166
2.38. Управление push-уведомлениями – команда CLI push ... 167
2.39. Панель управления инструмента миграции с Microsoft Exchange ... 167
2.39.1. Отсутствие дублирования сообщений при миграции с Microsoft Exchange ... 169
2.40. Информация о версии системы ... 169
3. Работа с системой резервного копирования (СРК) ... 170
3.1. Основные сценарии работы с СРК ... 171
3.2. Восстановление данных пользователей на сервере RuPost ... 172
3.2.1. Создание «холодной реплики» ... 173
3.2.2. Восстановление из «холодной реплики» ... 176
4. Структуры хранения данных ... 188
4.1. Почтовые ящики ... 188
4.2. Базы данных RuPost ... 189
4.2.1. Смена пароля доступа к базе данных ... 190
5. Глобальная адресная книга (GAL) ... 192
5.1. Атрибуты, используемые для формирования глобальной адресной книги (GAL) ... 194
5.1.1. FreeIPA ... 194
5.1.2. ALD Pro ... 195
5.1.3. Active Directory ... 195
5.1.4. Редактор атрибутов адресной книги ... 196
6. Геокластер ... 198

© 2021-2026 РуПост

6.1. Введение ... 198
6.2. Создание Геокластера ... 199
6.3. Средства обеспечения надежности Геокластера ... 201
6.4. Глобальные настройки Геокластера ... 204
6.4.1. Геокластер - редактор глобальных настроек ... 205
6.5. Маршрутизация почты между сайтами ... 207
6.6. Перенос почтового ящика между сайтами ... 208
6.7. Списки рассылок и общие ящики ... 210
6.8. Ограничения в работе Геокластера ... 211
6.9. Геокластер – резервный сайт ... 211
6.9.1. Создание резервного сайта ... 213
6.9.2. Назначение резервного сайта ... 214
6.9.3. Репликация баз данных на резервный сайт ... 215
6.9.4. Конфигурирование резервного сайта ... 216
6.9.5. Репликация почтовых данных на резервный сайт ... 217
6.9.6. Переключение на резервный сайт ... 218
6.9.7. Отключение резервного сайта ... 220
6.10. Геокластер – трассировка писем ... 222
6.11. Геокластер – отзыв писем ... 222
6.12. Геокластер – поиск и выгрузка найденных писем ... 222
6.13. Геокластер – лицензирование ... 222
7. Клиентские приложения ... 224
7.1. Встроенный web-клиент ... 224
7.1.1. Настройка “Возможность предоставлять совместный доступ” ... 225
7.1.2. Уведомление о прочтении ... 226
7.1.3. Вложения в календарные события ... 226
7.1.4. Пересылка приглашения на событие ... 228
7.1.5. Поддержка аутентификации Kerberos и OpenID Connect для веб-клиента ... 229
7.1.6. Аутентификация пользователей веб-клиента по протоколу Kerberos ... 231
7.2. Совместимые настольные почтовые клиенты ... 234
7.2.1. Клиенты на базе Thunderbird ... 234
7.2.2. Evolution ... 234
7.2.3. Microsoft Outlook ... 234

© 2021-2026 РуПост

7.3. Настольный клиент Desktop X 235
7.4. Мобильный клиент WorksPad 236
7.4.1. Создание ключа для интеграции с WorksPad сервером 237
8. Дополнительные комментарии 239
9. Приложение 1 – Шаблон “Интеграция RuPost с внешним релей сервером” 240
9.1. Сценарии использования 240
9.2. Требования к инфраструктуре 240
9.3. Подключение шаблона 240
10. Приложение 2 – Шаблон “Интеграция RuPost с Microsoft Exchange” 242
10.1. Сценарии использования 242
10.2. Требования к инфраструктуре 243
10.3. Подключение шаблона 243
11. Приложение 3 – Шаблоны интеграции с Kaspersky и Dr. Web 245
11.1. Сценарии использования 245
11.2. Требования к инфраструктуре 245
11.3. Подключение шаблона 245
12. Приложение 4 – Пример скриптов интеграции с СХД для работы с SDS Linstor 247
13. Приложение 5 – Настройка инфраструктуры Kerberos 251
13.1. Регистрация сервисов (SPN) 251
13.2. Настройка для Microsoft Active Directory 251
13.3. Настройка для Samba DC 252
13.4. Настройка для ALD.PRO и FreeIPA 253
13.5. Проверка созданного keytab-файла 254
13.6. Настройка браузеров через Групповые политики домена 254
13.7. Настройка браузеров для компьютеров вне домена 262

© 2021-2026 РуПост

Внимание!

Начиная с версии 3.0 изменена структура документации. В связи с тем, что количество команд CLI постоянно увеличивается, в состав документации добавлен отдельный документ - “Справочное руководство по командной строке”. Соответственно, разделы “Руководства администратора”, относящиеся к описанию команд CLI, перенесены в новый документ.

1. Концепция управления системой

Концепция управления RuPost строится на использовании **шаблонов конфигураций**, разрабатываемых на основе заранее созданных и проверенных типовых конфигураций различных компонентов почтовой системы разного уровня сложности.

Шаблоны конфигураций описываются на языке YAML, в котором отражаются основные конфигурационные параметры внутренних 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 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 инструменты RuPost. Структура шаблонов конфигураций описана в отдельном “*Руководстве по разработке шаблонов конфигураций*” RuPost.

Для расширения функциональных возможностей RuPost в одноузловой конфигурации, начиная с версии 3.2.0, разрешено использование custom шаблонов конфигураций с лицензией Standard.

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

Шаблоны конфигураций по своей природе являются параметризированными:

- При развертывании конфигурации всегда используются общесистемные параметры настроек RuPost, которые задаются с использованием визуальной **Панели управления RuPost**:
  - Общие настройки – например, пути хранения почтовых ящиков и др.
  - Домены AD/LDAP
  - Почтовые домены

- Шаблон конфигурации может включать набор дополнительных параметров, требуемых для развертывания рабочей конфигурации. Эти параметры запрашиваются у администратора системы через автоматически создаваемый пользовательский интерфейс форм и после

заполнения соответствующих значений применяются для конкретной конфигурации в процессе ее развертывания. Например, шаблон конфигурации может требовать данные (хост, порт) для подключения к корпоративной антивирусной системе.

Внимание! Изменения значений параметров настроек RuPost требует явного (ручного – через Панель управления) повторного развертывания конфигурации для применения новых настроек ко всем компонентам системы.

После обновления системы с предыдущей версии также требуется повторное развертывание конфигурации для генерации новых конфигурационных файлов почтовых компонентов.

© 2021-2026 РуПост

2. Графическая Панель управления

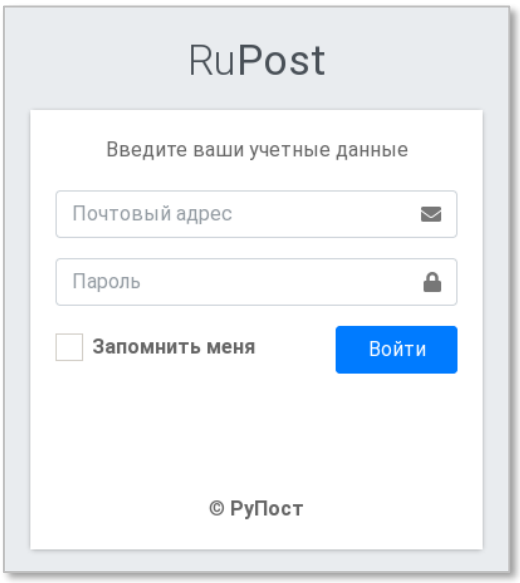
2.1. Вход в Панель управления системы

После установки rupost и загрузки лицензии вход в Панель управления осуществляется в браузере по адресу **`https://<имя хоста RuPost>:5000`** . Откроется окно входа в Панель управления, где необходимо ввести логин и пароль системного администратора RuPost.

2.1.1. Учетная запись встроенного администратора системы

Встроенный (“локальный”) системный администратор RuPost по умолчанию:

- Логин: **mailadmin**
- Пароль: **rupost**



Отключение встроенной учетной записи системного администратора возможно с использованием командного интерфейса.

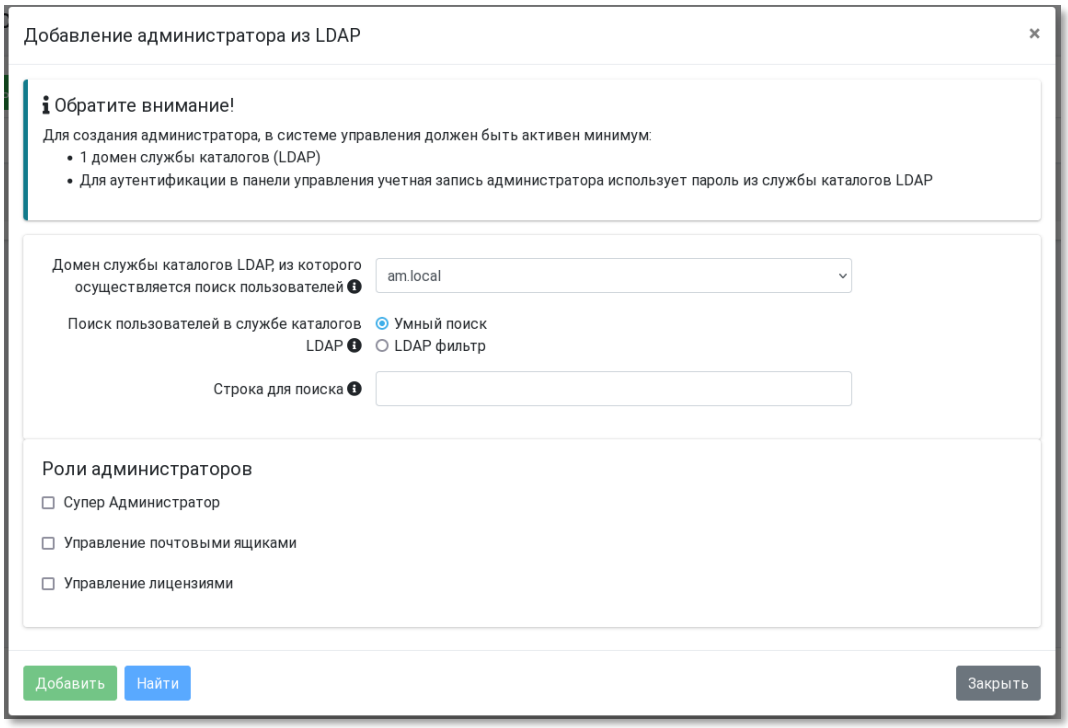
2.1.2. Разграничение полномочий администраторов

В версии 2.5.0 добавлен контроль доступа администраторов системы к функциям управления RuPost на основе разграничения полномочий администраторов.

Полномочие – это именованная совокупность разрешений на доступ к функциям управления, которые получает администратор.

Разрешение – это элемент контроля доступа к функциональности RuPost. Создание и редактирование полномочий заключается в выборе набора разрешений. Некоторые разрешения являются минимально необходимыми для входа в Панель управления, поэтому их нельзя отключить при создании/редактировании полномочий.

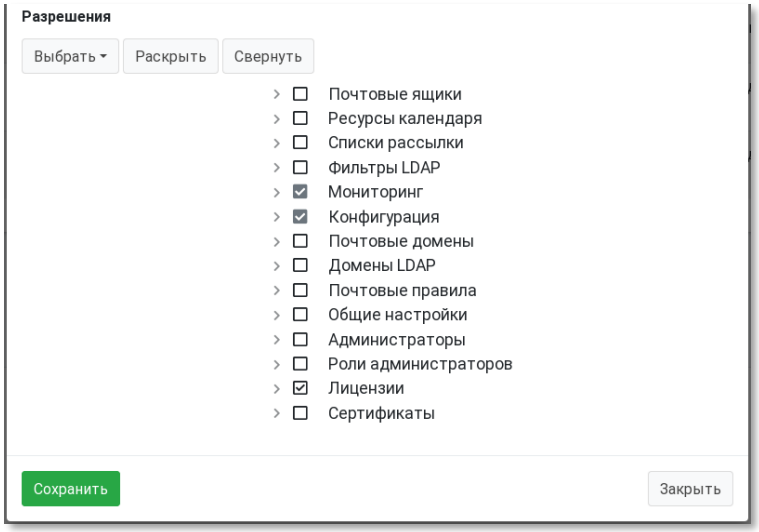
При регистрации нового администратора теперь необходимо назначить ему одну или несколько полномочий.



Управление полномочиями доступно через командный интерфейс CLI и визуальную Панель управления RuPost.

Синтаксис команды и примеры управления полномочиями из командной строки приведены в разделе **«rupost admins группа команд для управления администраторами»** Справочного руководство по командной строке.

Полномочие можно создать и отредактировать через Панель управления:



При установке RuPost создаются следующие полномочия:

- Супер Администратор
- Управление почтовыми ящиками

- Управление лицензиями

Встроенные полномочия ничем не отличаются от обычных полномочий – они могут изменены или удалены.

Полномочие “Супер Администратор” имеет возможность полного доступа к системе, включая создание администраторов и управление полномочиями администраторов. Как и другие полномочия, она может быть удалена – в этом случае, ни один администратор не будет иметь полномочия полного доступа к системе. После удаления, при необходимости, полномочие “Супер Администратор” может быть восстановлена с помощью команды CLI.

Синтаксис команды и примеры управления полномочиями из командной строки приведены в разделе **«rupost admins группа команд для управления администраторами»** Справочного руководство по командной строке.

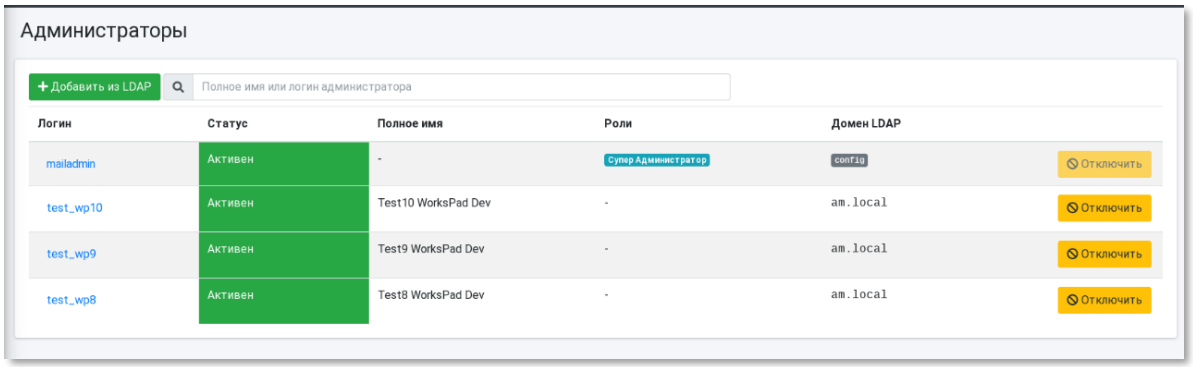
Полномочие, которое, в данный момент, назначена какому-либо администратору, не может быть удалено.

2.1.3. Администраторы системы с аутентификацией в LDAP

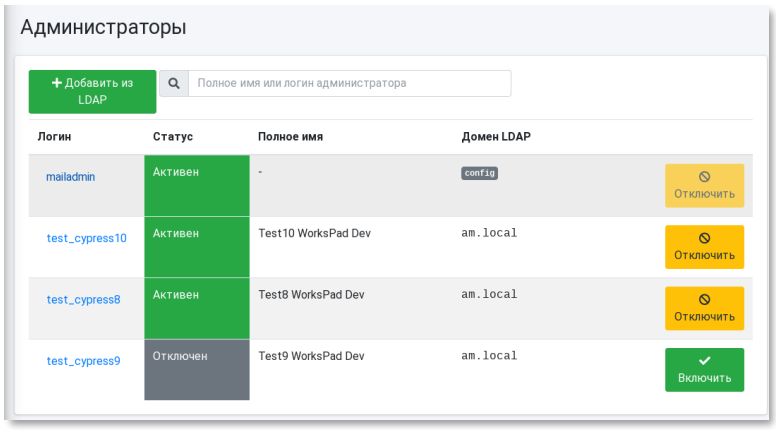
Управлять администраторами системы можно как с помощью Панели управления, так и через командный интерфейс CLI.

2.1.3.1. *Управление администраторами системы в Панели управления*

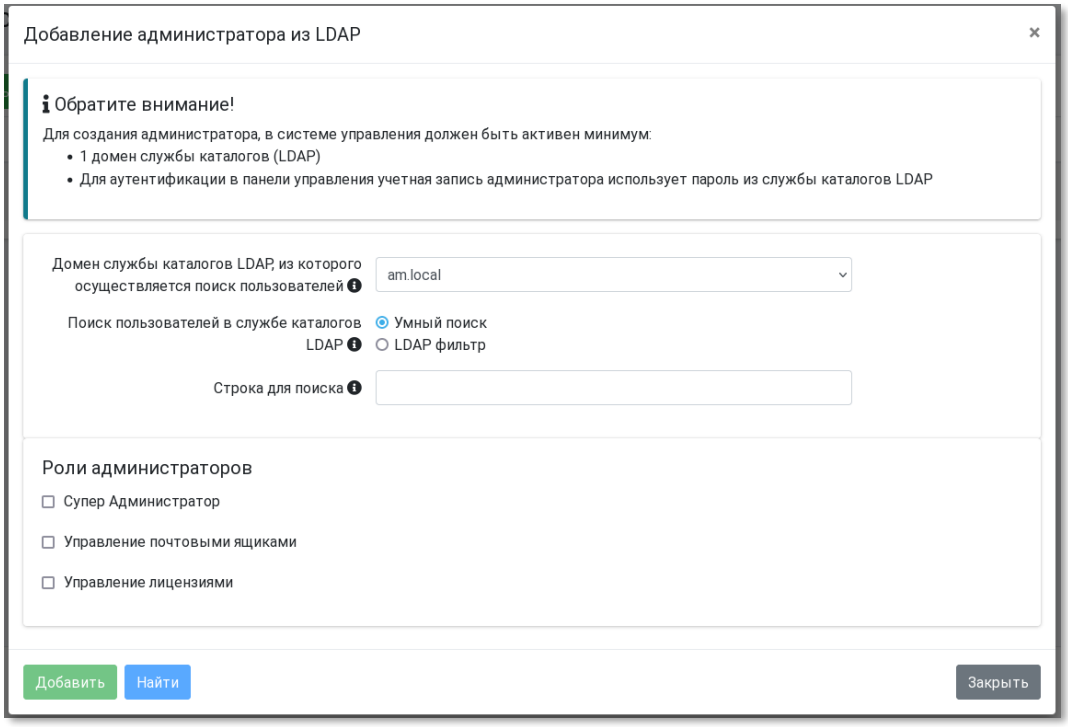
Для управления администраторами в Панели управления нужно в меню выбрать пункт “Администраторы”:



Будет показан полный список администраторов RuPost, включая встроенного локального администратора. При необходимости, любого администратора (включая локального) можно отключить, нажав на желтую кнопку в соответствующей строке таблицы.

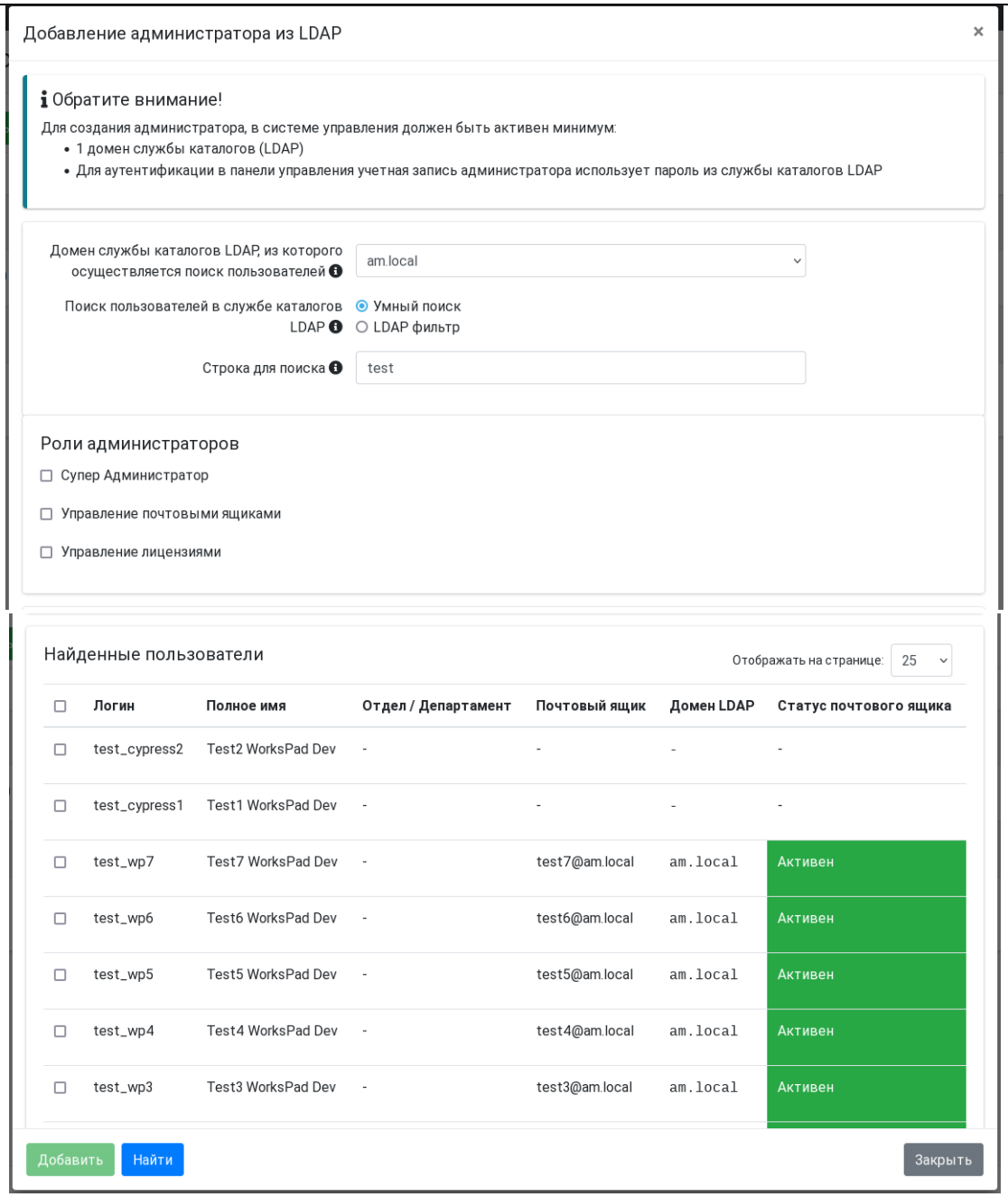


Выбор пользователя из LDAP для последующего добавления в качестве администратора осуществляется по кнопке ”Добавить из LDAP”.



Поиск может быть осуществлен либо по вхождению строки для поиска в любой из параметров пользователя (“Умный поиск”) либо посредством задания LDAP фильтра.

После того, как искомый пользователь найден, для добавления в список администраторов нужно отметить его в первой колонке таблицы и нажать кнопку “Добавить”.



Обратите внимание – в колонке “Статус почтового ящика” показывается статус почтового ящика пользователя. Для тех пользователей, у которых нет почтового ящика в RuPost, будет указано “Отсутствует”. Наличие почтового ящика в RuPost не является необходимым условием для администратора - администратором системы может быть и пользователь, у которого нет почтового ящика в RuPost.

2.1.3.2. *Управление администраторами системы через командный интерфейс CLI*

Командный интерфейс (CLI) для управления администраторами системы с аутентификацией в LDAP доступен при обращении к основной программе rupost. Администратор назначается по его логину, т.е. `userPrincipalName` или `sAMAccountName` в AD, во всех остальных случаях `uid`. В текущей

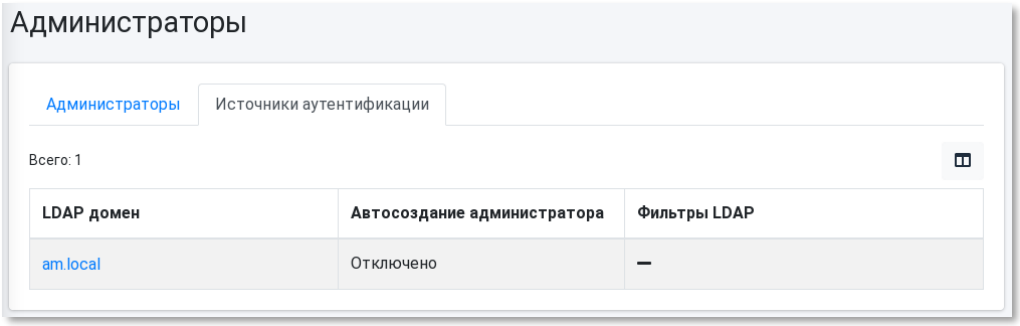
реализации не может быть разных администраторов с одинаковыми логинами из разных служб каталогов.

Синтаксис команды и примеры управления полномочиями из командной строки приведены в разделе **«rupost admins группа команд для управления администраторами»** Справочного руководство по командной строке.

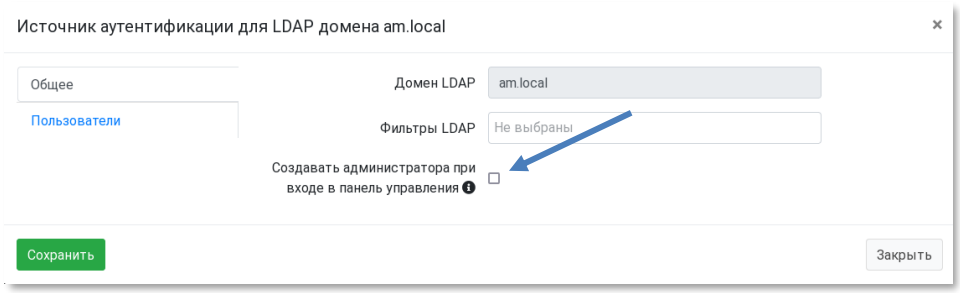
1.1.3.1. Автоматическое добавление администраторов по фильтрам LDAP

В версии 4.3.4 добавлена возможность автоматического создания учетных записей администраторов в момент входа в панель управления RuPost.

Для конфигурирования автоматического создания администраторов, на странице “Администраторы” перейдите на вкладку “Источники аутентификации”.



Для каждого LDAP домена можно выбрать фильтры LDAP, которые будут являться источником записей аутентификации для администраторов, а также разрешить автоматическое создание учетной записи администратора при входе в Панель управления.

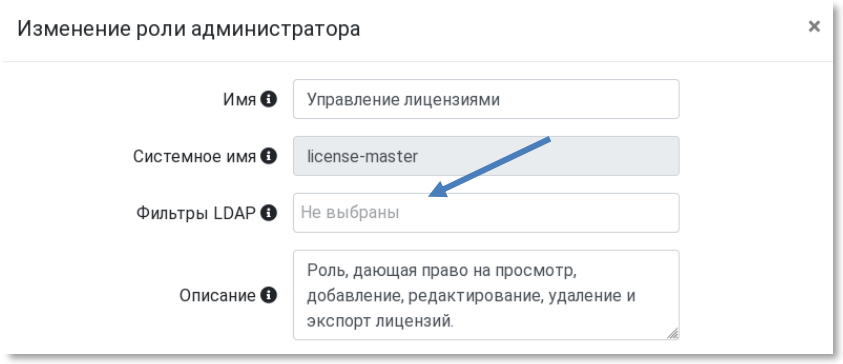


На вкладке “Пользователи” можно просмотреть список пользователей, из выбранных фильтров LDAP.

1.1.3.2. Автоматическое назначение ролей администраторов по фильтрам LDAP

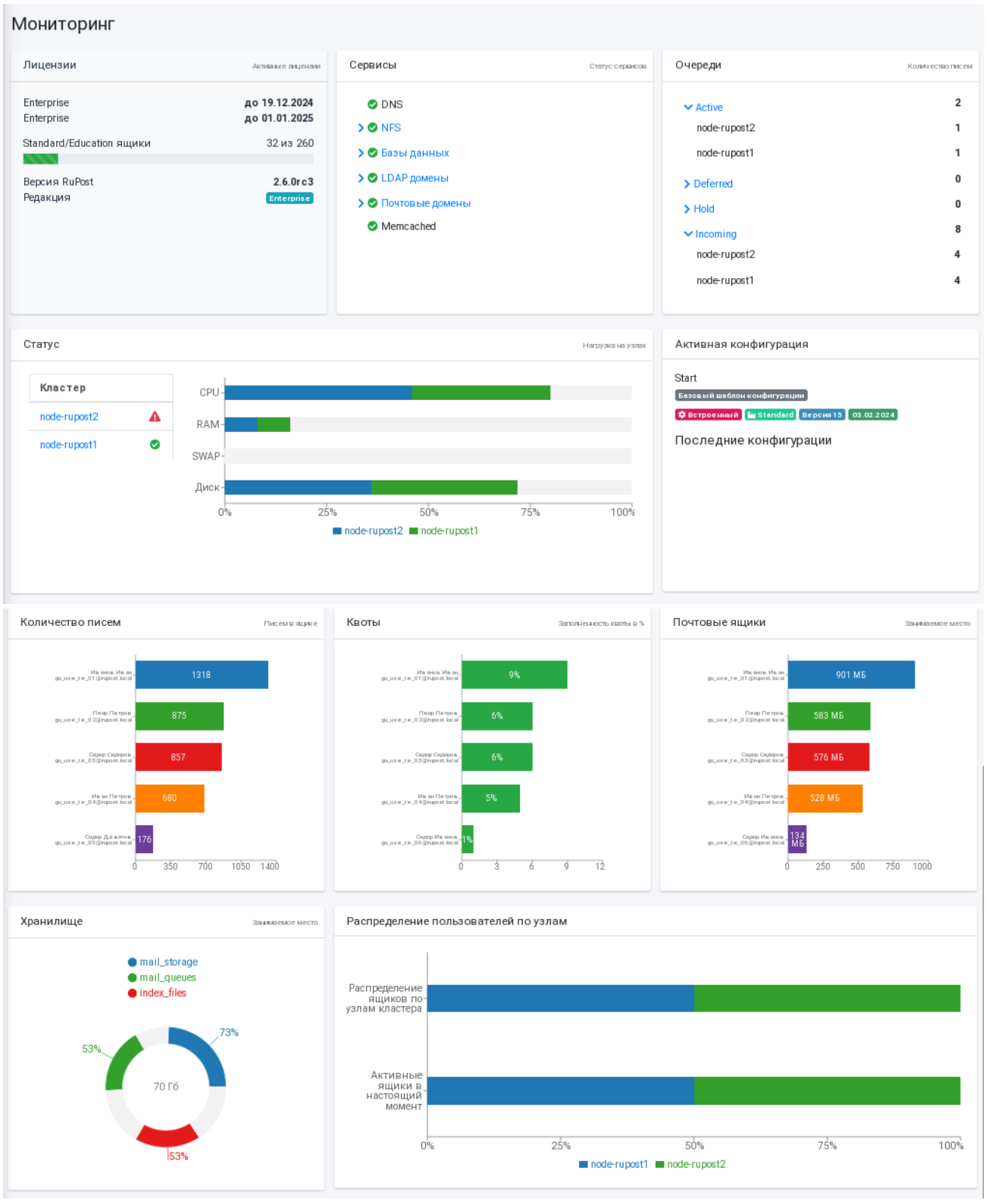
В версии 4.3.4 добавлена возможность автоматического назначения ролей администраторам по фильтрам LDAP.

Для конфигурирования автоматического назначения ролей администраторам, выберите нужную роль (страница “Роли”, окно “Изменение роли администратора”) и затем выберите фильтры LDAP, определяющие учетные записи администраторов, которым будет автоматически назначена данная роль.


Изменение роли администратора
Имя
Управление лицензиями
Системное имя
license-master
Фильтры LDAP
Не выбраны
Описание
Роль, дающая право на просмотр, добавление, редактирование, удаление и экспорт лицензий.

2.2. Домашняя страница Панели управления -“Мониторинг” (Dashboard)

В версии 2.6 добавлена новая страница “Мониторинг”, отображающая информацию о текущем состоянии инфраструктуры и работе экземпляров RuPost.



На странице представлена следующая информация (карточки):

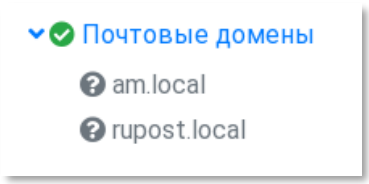
1. **Лицензии** – редакция и количество использованных и доступных лицензий, а также дата окончания действия лицензии. Индикатор процента использованных лицензий имеет следующую цветовую кодировку:
   - Зеленый – при значении до 80%
   - Жёлтый – от 80% до 90%
   - Красный – 90% и выше.
2. **Сервисы** – статус инфраструктурных сервисов:
   - DNS
   - NFS
   - Базы данных
   - LDAP домены
   - Почтовые домены
   - Memcached

   Иконки статусов сервисов имеет следующую цветовую кодировку:

   Сервис работает, ошибок нет.

   Есть ошибки в работе сервиса.

В версии 4.3.4 изменена логика работы индикатора результатов проверки записей DNS (страница “Мониторинг”). Если в свойствах почтового домена настройка "Проверка корректности DNS записей" отключена, то соответствующая проверка не производится и, в этом случае, индикатор имеет серый цвет.



3. **Очереди** – количество сообщений в очередях postfix:
   - Active
   - Deferred
   - Hold
   - Incoming
4. **Статус** – текущие параметры узлов RuPost – для каждого узла:
   - IP адрес
   - UUID экземпляра RuPost
   - CPU
   - RAM
   - SWAP
   - Диск

   Если RuPost работает в кластере, то первая закладка отображает совмещенные параметры всех узлов кластера, остальные – индивидуальные показатели каждого узла.

Иконки статуса узлов на вкладках:

- Статус экземпляра “Активен” и загруженность всех параметров узла менее 80%
- Статус экземпляра ”Активен” и загруженность любого параметра узла более 80%, но менее 90%
- Статус экземпляра ”Активен ” и загруженность любого параметра узла более 90%
- Статус экземпляра ”Заблокирован” или ”Удален”
- Статус экземпляра ”Выведен из эксплуатации”

Диаграмма использования ресурсов узла имеет следующую цветовую кодировку:

- Зеленый - от 0% до 80%
- Жёлтый - от 80% до 90%
- Красный - от 90% до 100%

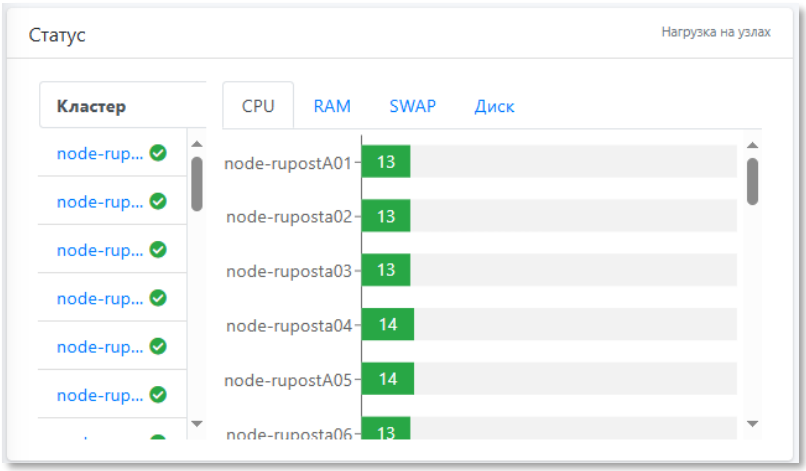
5. **Активная конфигурация** – информация о текущем развернутом шаблоне конфигурации и история конфигураций с указанием даты развертывания;
6. **Количество писем** – топ-5 почтовых ящиков по количеству писем;
7. **Квоты** - топ-5 почтовых ящиков по проценту использования квоты на размер почтового ящика;
8. **Почтовые ящики** - топ-5 почтовых ящиков по размеру почтового ящика;
9. **Хранилище** – информация об NFS, используемых в RuPost
10. **Распределение пользователей по экземплярам** - % подключений IMAP пользователей к экземплярам кластера. Карточка не отображается для не кластерной конфигурации.

Периодичность обновления информации:

- Очереди, нагрузка узлов, распределение пользователей, хранилище NFS - интервал 30 секунд
- Квоты, занятость ящиков - интервал 60 секунд
- Лицензии, конфигурации, статус сервисов (LDAP, почтовые домены, DB) - интервал 5 минут

В версии 3.1.0 на странице Мониторинг улучшено отображение общей информации о кластере – теперь на карточке “Статус” администратор имеет возможность выбрать тип отображаемой информации:

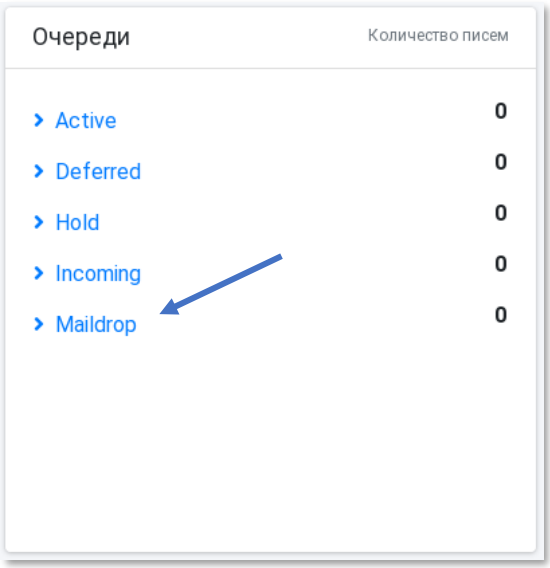
- CPU
- RAM
- SWAP
- Диск



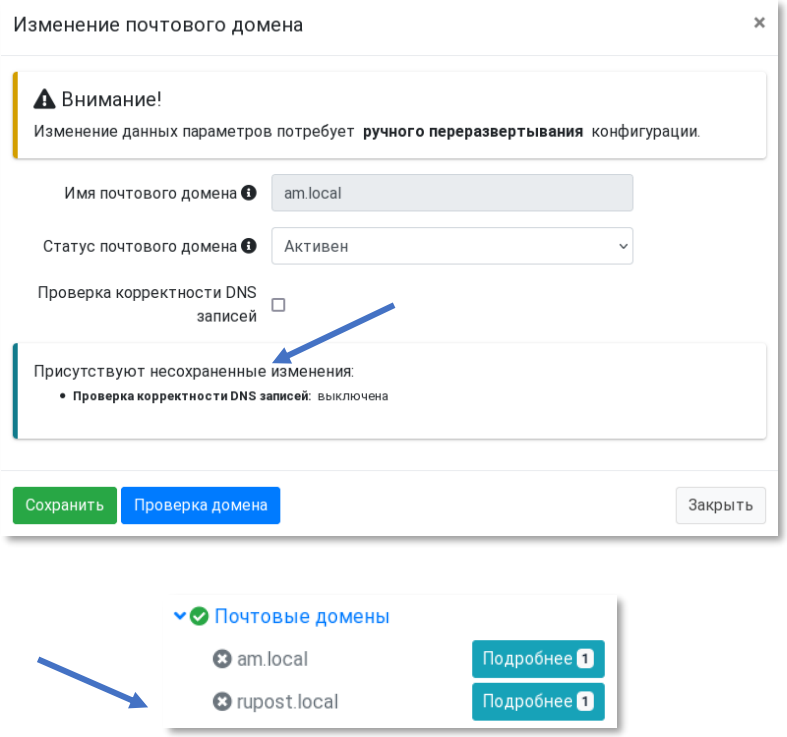
Карточка отображает информацию одного типа, но для всех узлов кластера, что позволяет легко сравнивать нагрузку на различные узлы кластера между собой.

В версии 3.4.0, так как аппаратная часть узла тоже принадлежит к инфраструктуре, поэтому блок информации о состоянии узлов перемещен со страницы “Почтовая система” на страницу “Мониторинг инфраструктуры”.

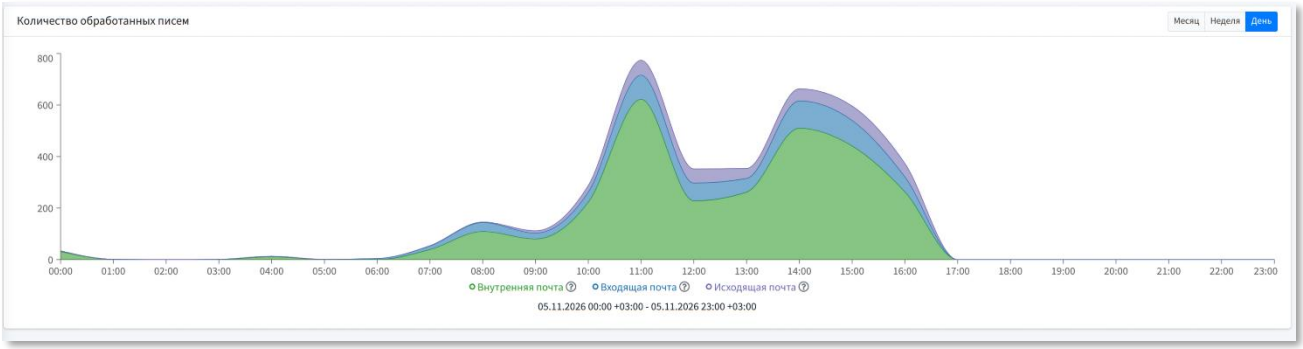
В версии 4.1.0 на страницу “Мониторинг” -> “Почтовая система” добавлена статистика по очереди maildrop.



В версии 4.1.0 изменена логика отображения результатов проверки корректности записей DNS. Если в настройках DNS установлен переключатель “Не проверять корректность DNS записей”, то индикатор результатов проверки DNS для почтовых доменов будет отображаться серым цветом.



В версии 4.3.4 на страницу “Мониторинг” добавлено отображение количества обрабатываемых писем за период времени.



Переключатель на графике позволяет выбрать период отображения информации:

- **День** – данные за текущие 24 часа с начала суток.
- **Неделя** – данные за прошлую неделю, включая текущий день.
- **Месяц** – данные за прошлый месяц, включая текущий день.

Цвет данных отражает различные типы доставок сообщений:

- **Внутренняя почта** – и отправитель и получатель находятся в обслуживаемых почтовых доменах.
- **Исходящая почта**– отправитель из обслуживаемого почтового домена, а получатель – внешний.

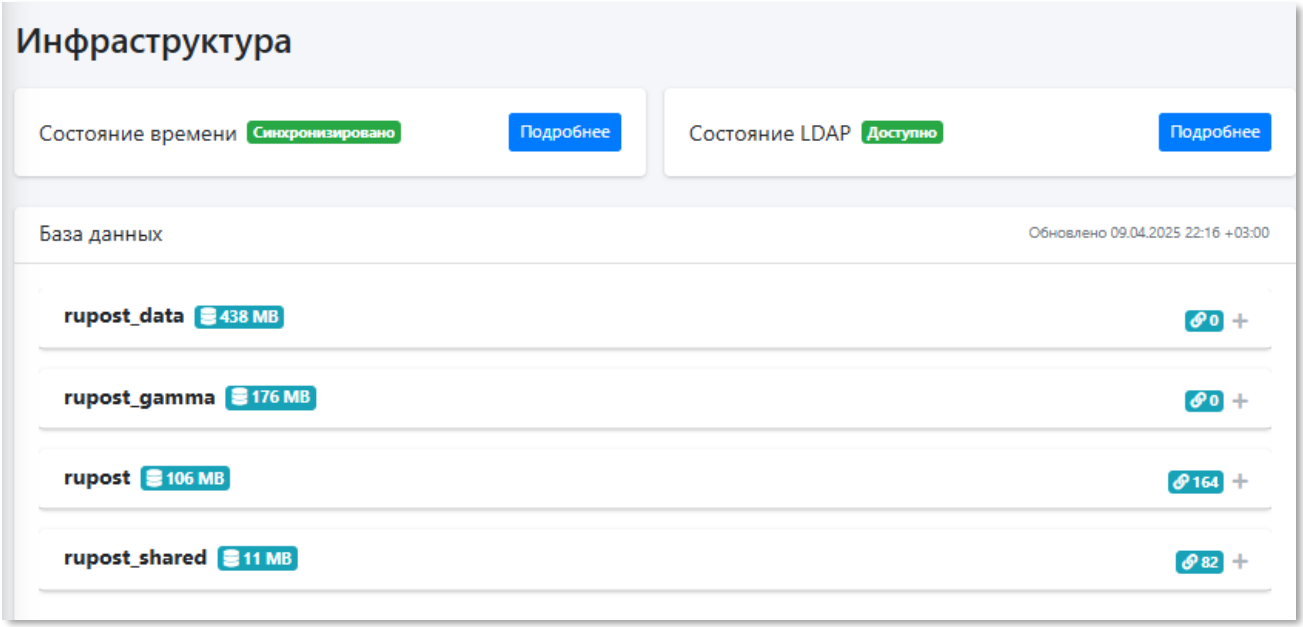
- **Входящая почта** – получатель из обслуживаемого почтового домена, а отправитель – внешний.

2.2.1. Мониторинг инфраструктуры

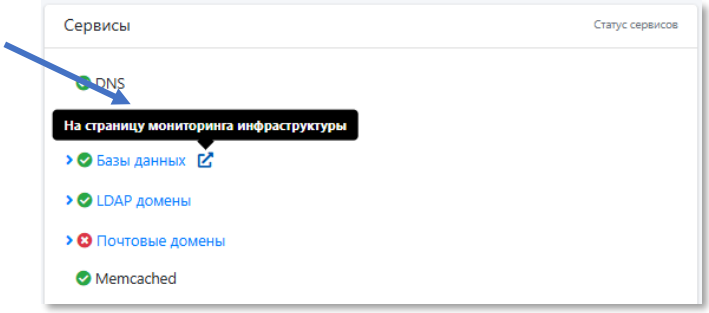
В версии 3.3.0 расширены возможности RuPost по мониторингу состояния инфраструктуры. Добавлен мониторинг следующих элементов инфраструктуры:

- База данных (включая кластер Patroni)
- Подключение и состояние серверов LDAP
- Наличие изменений ключевых атрибутов в LDAP
- Синхронизация времени на узлах кластера

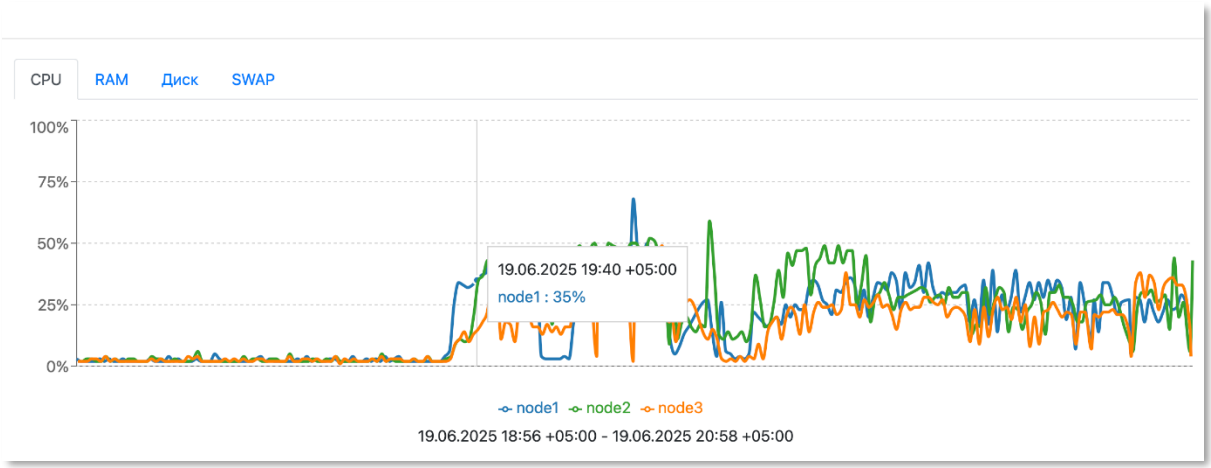
Все данные, поступающие от подсистемы мониторинга инфраструктуры, отображаются в Панели управления на странице **Мониторинг -> Инфраструктура** и записываются в специализированный лог файл – **infrastructure.log**.



Для получения дополнительной информации по статусу баз данных и серверам LDAP, на страницу “Мониторинг” -> “Почтовая система” добавлены ссылки быстрых переходов на страницу “Инфраструктура”.

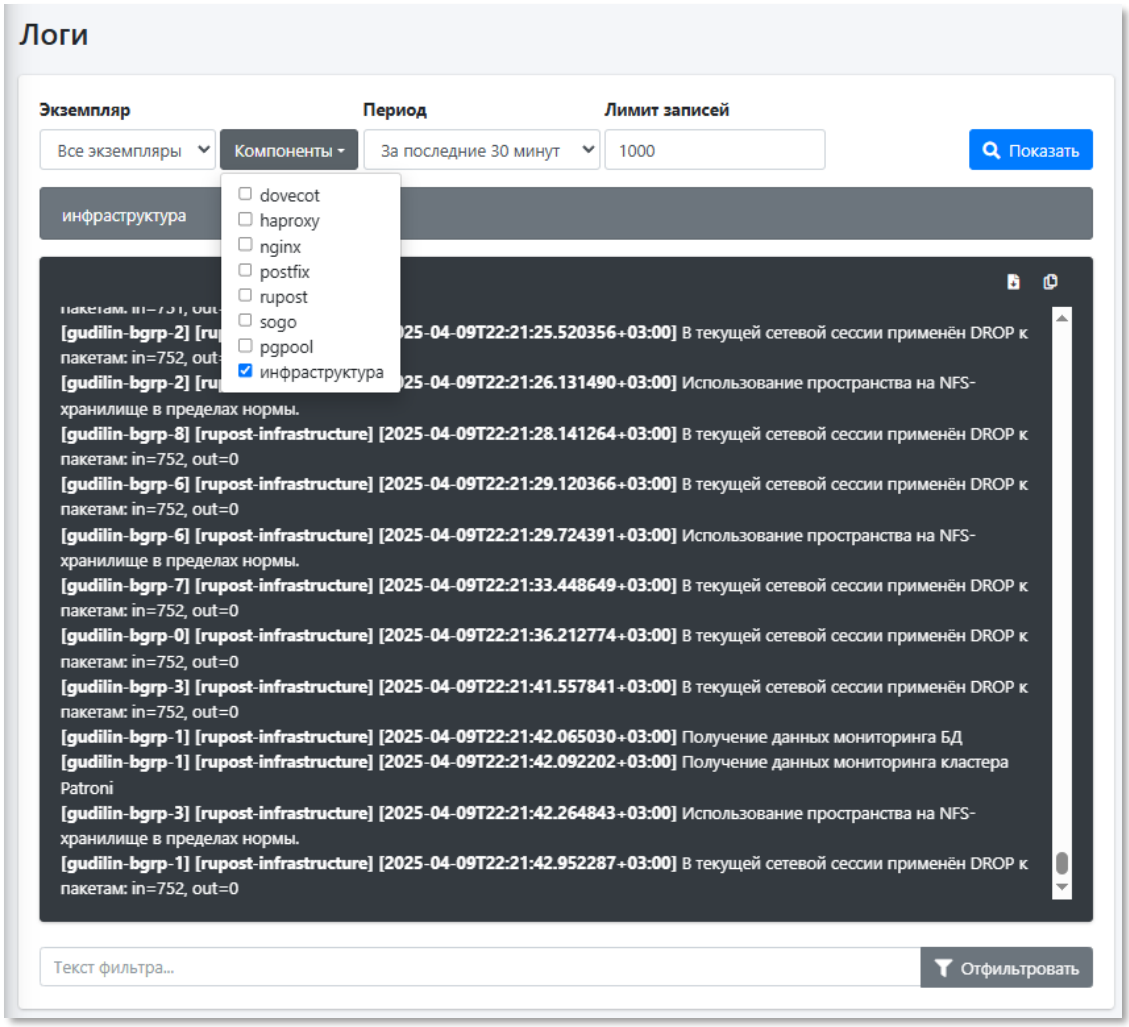


В версии 3.4.0 расширен мониторинг состояния инфраструктуры – добавлена возможность просмотра истории изменения параметров узлов кластера.



Диапазон времени отображения событий по горизонтальной оси указан в нижней части диаграммы.

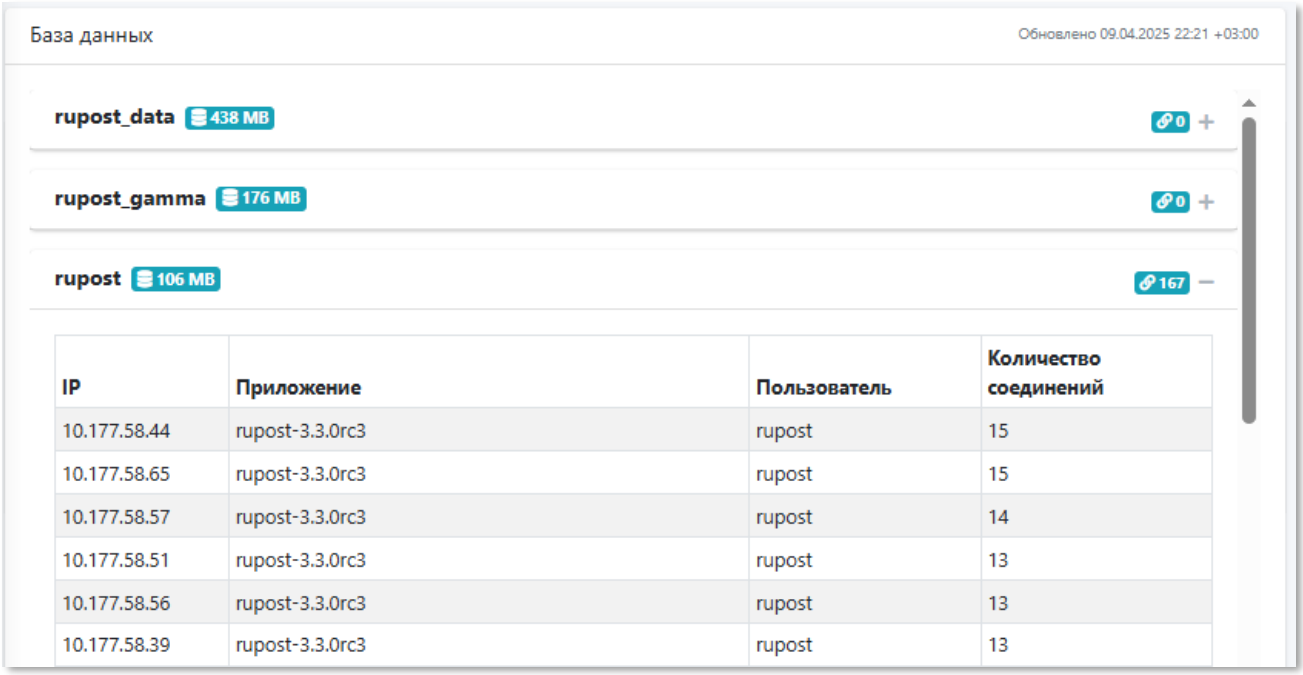
Журнал инфраструктуры доступен для просмотра на странице “Логи”.



2.2.1.1. *Мониторинг базы данных*

В версии 3.3.0 добавлен мониторинг состояния баз данных. На странице “Мониторинг” -> “Инфраструктура” в разделе “База данных” отображается следующая информация:

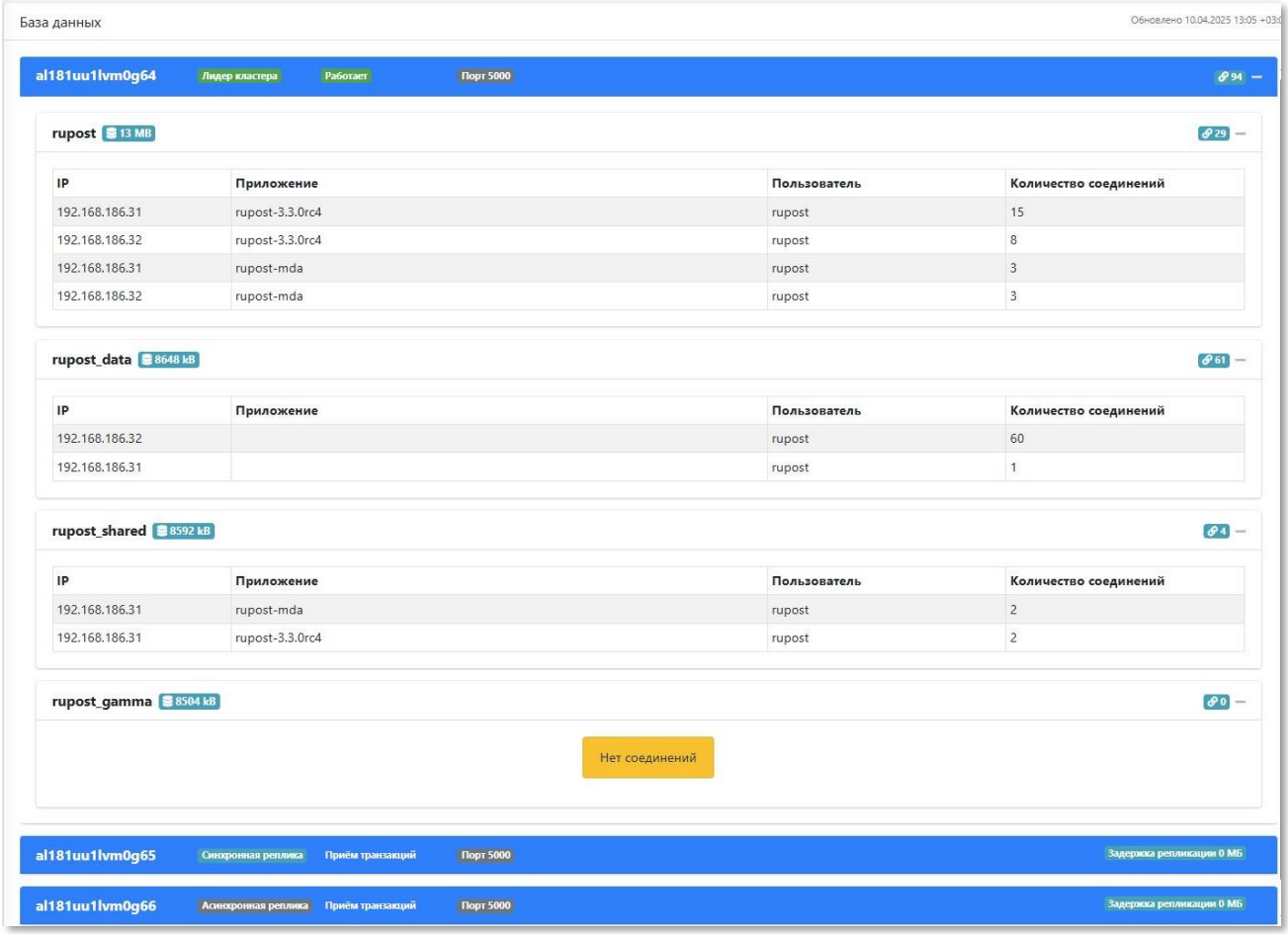
- Название базы данных
- Размер базы данных
- Информация о текущих подключениях (IP адрес, Приложение, Пользователь, Количество соединений)



IP	Приложение	Пользователь	Количество соединений
10.177.58.44	rupost-3.3.0rc3	rupost	15
10.177.58.65	rupost-3.3.0rc3	rupost	15
10.177.58.57	rupost-3.3.0rc3	rupost	14
10.177.58.51	rupost-3.3.0rc3	rupost	13
10.177.58.56	rupost-3.3.0rc3	rupost	13
10.177.58.39	rupost-3.3.0rc3	rupost	13

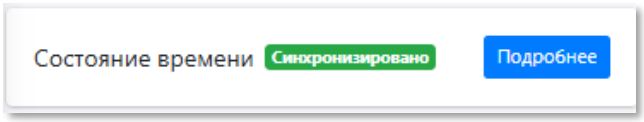
При использовании кластера Patroni, дополнительно отображаются следующие параметры:

- Идентификатор узла
- Роль узла в кластере Patroni (Лидер кластера, Синхронная реплика, Асинхронная реплика)
- Текущий статус
- Порт подключения



2.2.1.2. *Мониторинг синхронизации времени*

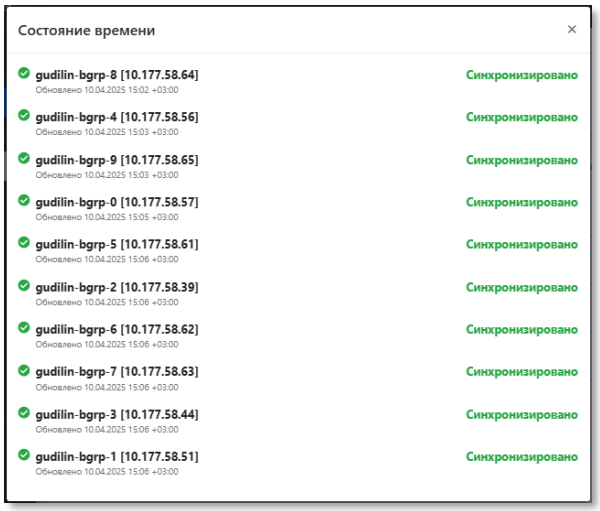
В версии 3.3.0 добавлен контроль за состоянием синхронизации времени на всех узлах кластера и сервера базы данных RuPost. Информация о состоянии синхронизации времени отображается на странице “Мониторинг” -> “Инфраструктура” в разделе “Состояние времени”.



Предупреждение в Панели управления о том, что время не синхронизировано, отображается при наличии разницы во времени между узлами кластера и/или сервера баз данных более 1 секунды.

Состояние “Устаревшие данные синхронизации” означает, что, в данный момент, на странице отображается информация о синхронизации времени, собранная более 30 секунд назад – рекомендуется обновить страницу.

При нажатии на кнопку “Подробнее” отображается статус синхронизации времени на всех узлах кластера.

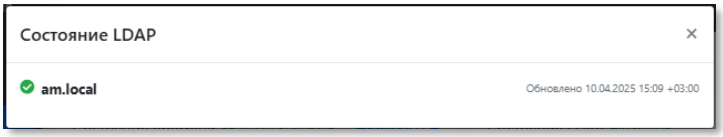


2.2.1.3. *Мониторинг серверов LDAP*

В версии 3.3.0 добавлен постоянный мониторинг наличия подключений и работы всех серверов LDAP, используемых RuPost. Информация о состоянии серверов LDAP отображается на странице “Мониторинг” -> “Инфраструктура” в разделе “Состояние LDAP”.



При нажатии на кнопку “Подробнее” отображается статус по каждому из используемых серверов LDAP.

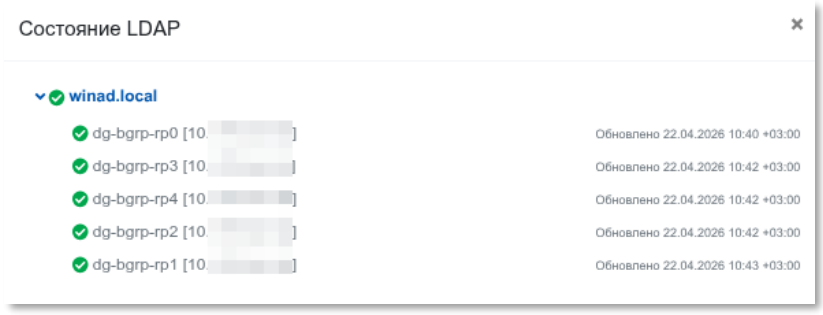


При обнаружении сбоя в работе серверов LDAP, производится запись в infrastructure.log и отображается предупреждение для администратора в Панели управления.

В версии 4.2.0 расширена диагностика подключений к серверам LDAP – теперь подключение к LDAP серверам проверяется на каждом из узлов кластера.

На странице “Мониторинг” индикатор наличия подключения к домену LDAP имеет следующую цветовую кодировку:

- *Красный* – подключение к серверам LDAP отсутствует на всех узлах кластера.
- *Желтый* – подключение к серверам LDAP отсутствует на части узлов кластера.
- *Зеленый* – подключение к серверам LDAP осуществляется на всех узлах кластера.



2.2.2. Интеграция с Zabbix

В версии 4.0 добавлена интеграция с сервером мониторинга информационных систем Zabbix.

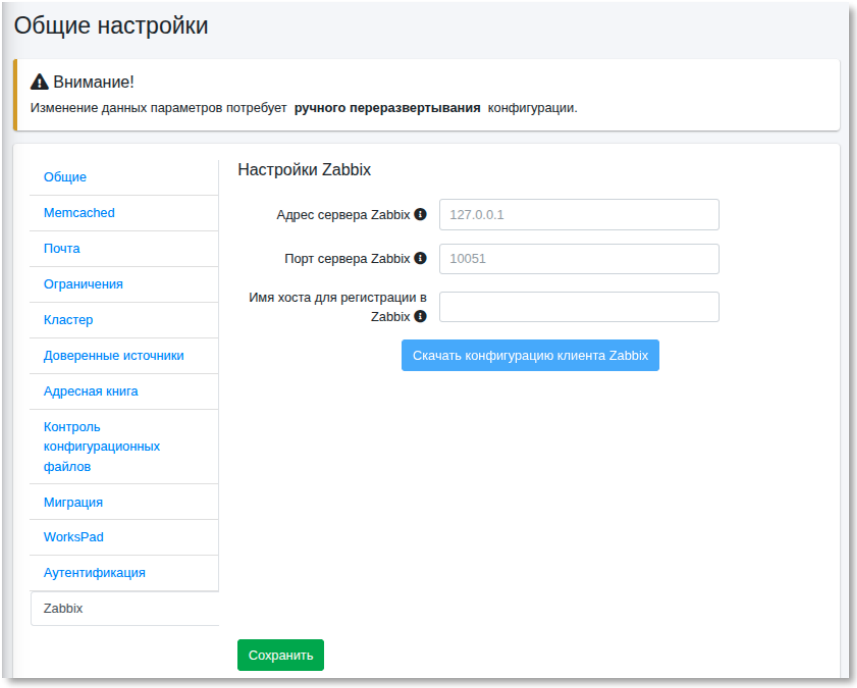
Интеграция с Zabbix позволяет администраторам информационных систем:

- Осуществлять мониторинг текущих параметров работы кластера RuPost и просматривать историю их изменения в удобном специализированном пользовательском интерфейсе.
- Настраивать оповещения о выходе параметров RuPost за пределы установленных норм.

Интеграция с Zabbix реализована посредством отправки данных с кластера RuPost на сервер Zabbix.

Для того, чтобы подключить RuPost к серверу Zabbix, в окне “Общие настройки” на закладке “Zabbix” необходимо ввести:

- Адрес сервера Zabbix.
- Порт сервера Zabbix.
- Имя хоста для регистрации в Zabbix – название, которое будет использовано Zabbix при отображении полученных данных.



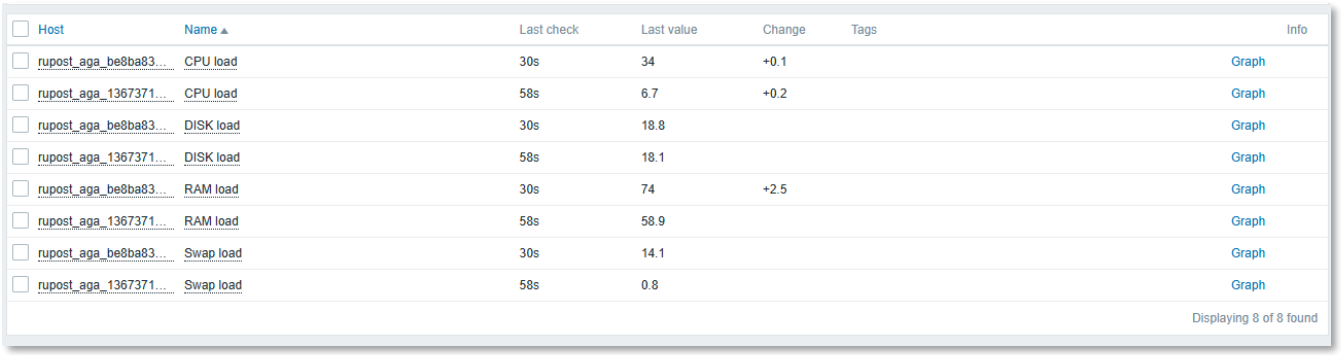
После заполнения полей настроек, по кнопке “Скачать конфигурацию клиента Zabbix” получаем конфигурационный файл, определяющий экземпляры RuPost как источники данных для Zabbix. Полученный файл необходимо загрузить в Zabbix.

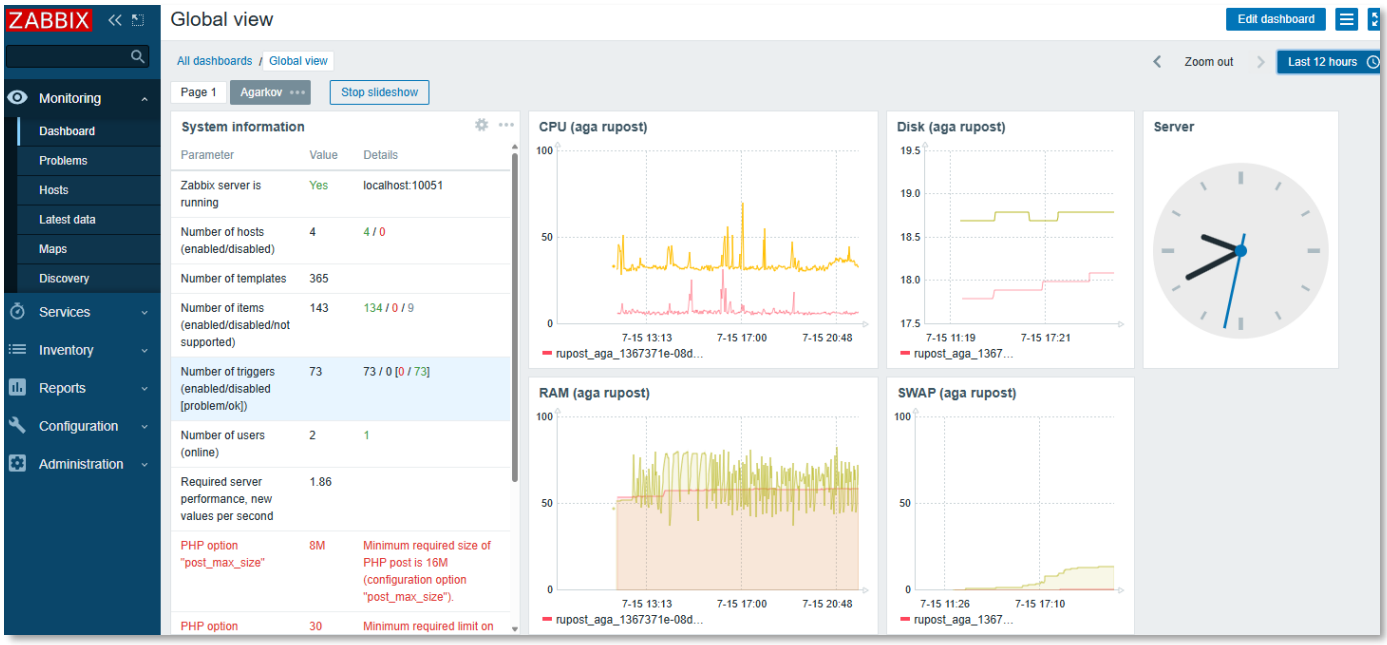
Для добавления источника данных RuPost в Zabbix нужно:

1. Выбрать пункт меню “Configuration” -> “Hosts”.
2. Нажать на кнопку “Import”.
3. Выбрать файл конфигурации Zabbix, ранее полученный из RuPost.

Настройка подключения источника данных RuPost в Zabbix завершена.

При успешном подключении RuPost к Zabbix, в списке “Hosts” появятся названия экземпляров RuPost и можно увидеть, переданные из RuPost данные.





В данный момент RuPost передает в Zabbix следующие данные – по каждому узлу кластера:

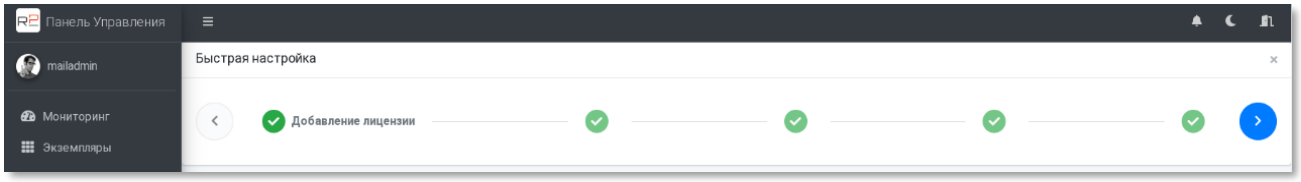
- CPU- нагрузка на процессор (%).
- DISK free space – размер свободного пространства на диске (%).

- RAM load - загрузка оперативной памяти (%).
- SWAP load - загрузка SWAP на диске (%).

Данные обновляются раз в 60 секунд.

2.3. Пошаговая "Быстрая настройка" в Панели управления

В версии 2.7.0 для повышения удобства и скорости ввода в эксплуатацию сервера RuPost после первоначальной установки в Панель управления RuPost добавлена панель “Быстрая настройка”.



Панель “Быстрая настройка” обеспечивает пошаговую навигацию по отдельным страницам Панели управления RuPost и содержит минимально необходимый набор действий для того, чтобы обеспечить работу сервера электронной почты:

- Добавление лицензии
- Добавление имени узла
- Добавление LDAP домена
- Добавление почтового домена
- Развёртывание конфигурации

После завершения первоначальной настройки панель “Быстрая настройка” автоматически скрывается, но, при необходимости, ее можно включить по кнопке, находящейся под главным меню Панели управления.

2.4. Управление лицензиями

2.4.1. Управление лицензиями через командный интерфейс CLI

Внимание!

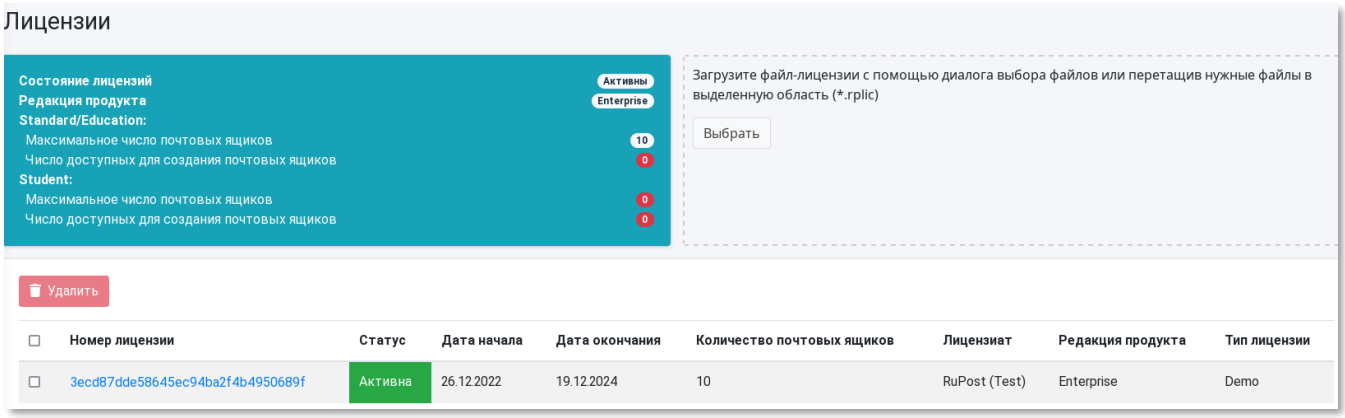
Использование системы RuPost невозможно без добавления электронной лицензии.

Для управления лицензиями предусмотрена группа команд licenses. Соответственно, продолжить настройку RuPost администратор системы может при наличии индивидуального файла лицензии. Службы RuPost стартуют автоматически после добавления файла лицензии.

Синтаксис команды и примеры управления лицензиями из командной строки приведены в разделе **«rupost licenses группа команд для управления лицензиями»** Справочного руководство по командной строке.

2.4.2. Управление лицензиями в Панели управления

Панель управления RuPost содержит специальную страницу для управления файлами лицензий.



2.4.3. Лицензии для образовательных учреждений

В версии 2.5.4 добавлена поддержка лицензий следующих редакций:

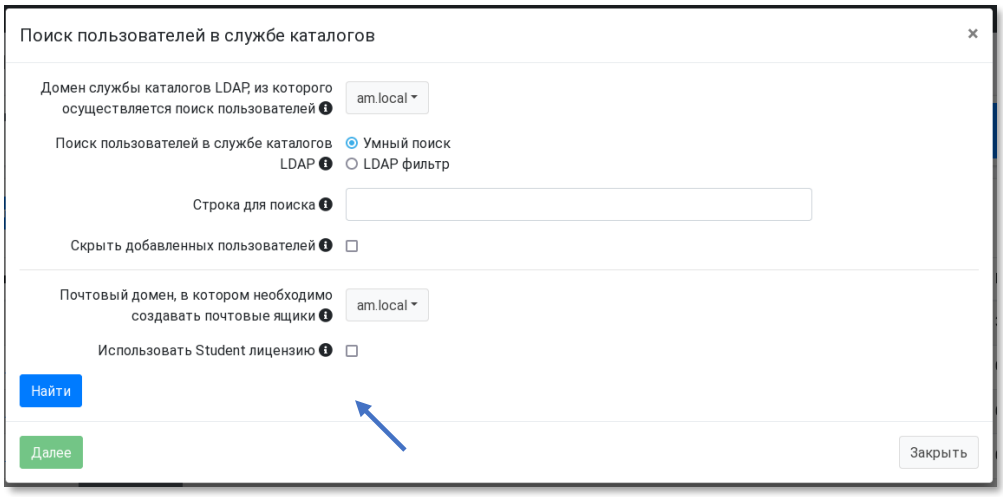
- Standard Education
- Enterprise Education
- Enterprise Education Upgrade
- Standard Student
- Enterprise Student
- Enterprise Student Upgrade

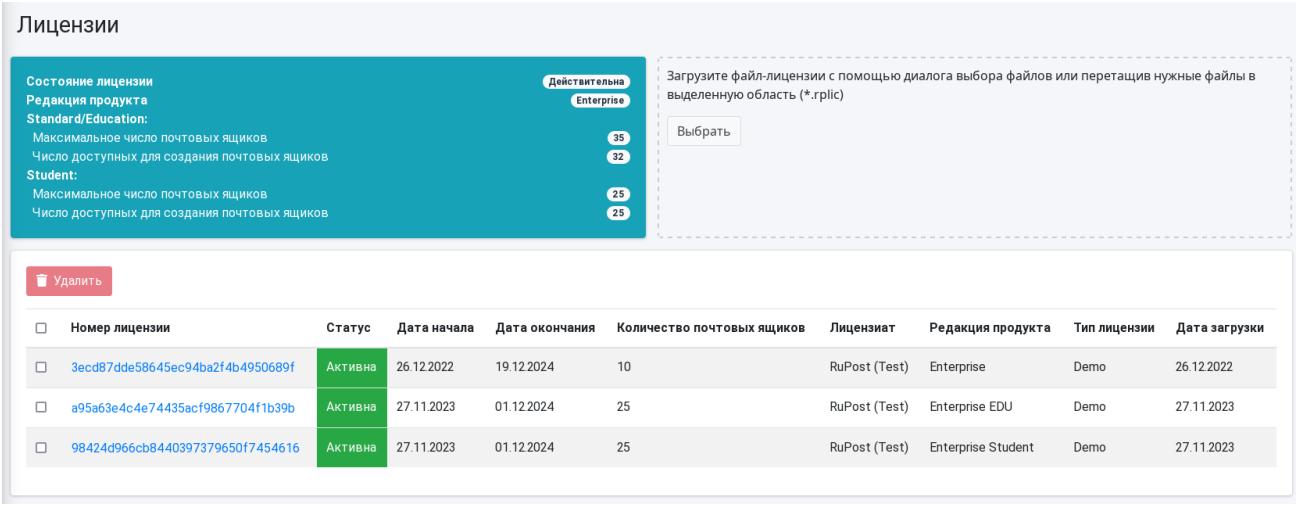
При добавлении почтовых ящиков, необходимо выбрать тип лицензии.

Лицензии “Student” имеют ограничение – почтовые ящики с такими лицензиями не могут отправлять почту на внешние адреса.

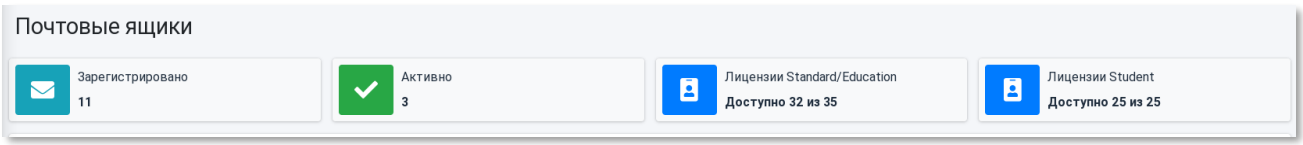
Внимание!

Пользователям со студенческими лицензиями заблокирована отправка писем на внешние адреса, но, если у них есть разрешение писать на списки рассылки, которые содержат внешних получателей, то эти письма дойдут до соответствующих внешних получателей.



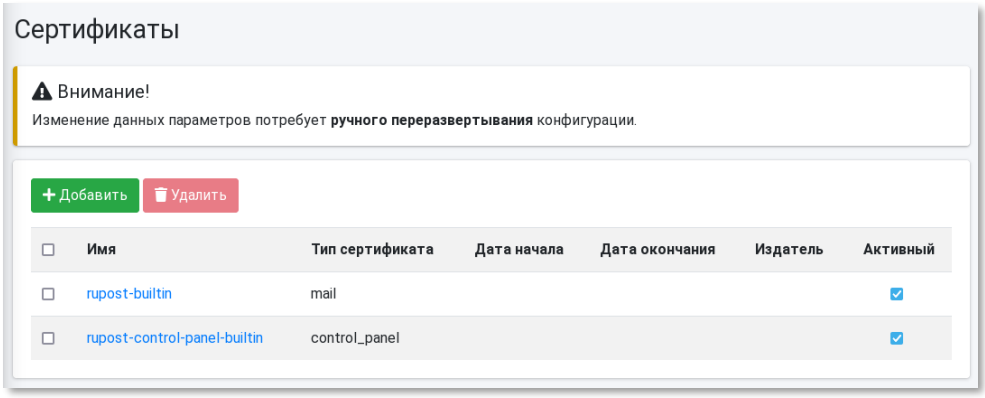


Для удобства контроля за количеством Student лицензий, на страницу “Почтовые ящики” добавлен счетчик лицензий редакции Student.



2.5. Управление сертификатами

В версии 2.6.0 добавлена возможность управлять сертификатами в Панели управления на странице “Сертификаты” (пункт главного меню “Настройки” -> “Сертификаты”).



Внимание!

При создании ключей необходимо выполнить следующие требования:
для алгоритма шифрования RSA, рекомендуемая длина ключа должна составлять не менее 2048 бит;
для алгоритма шифрования на основе эллиптических кривых ECDSA - длина ключа не менее 256 бит;

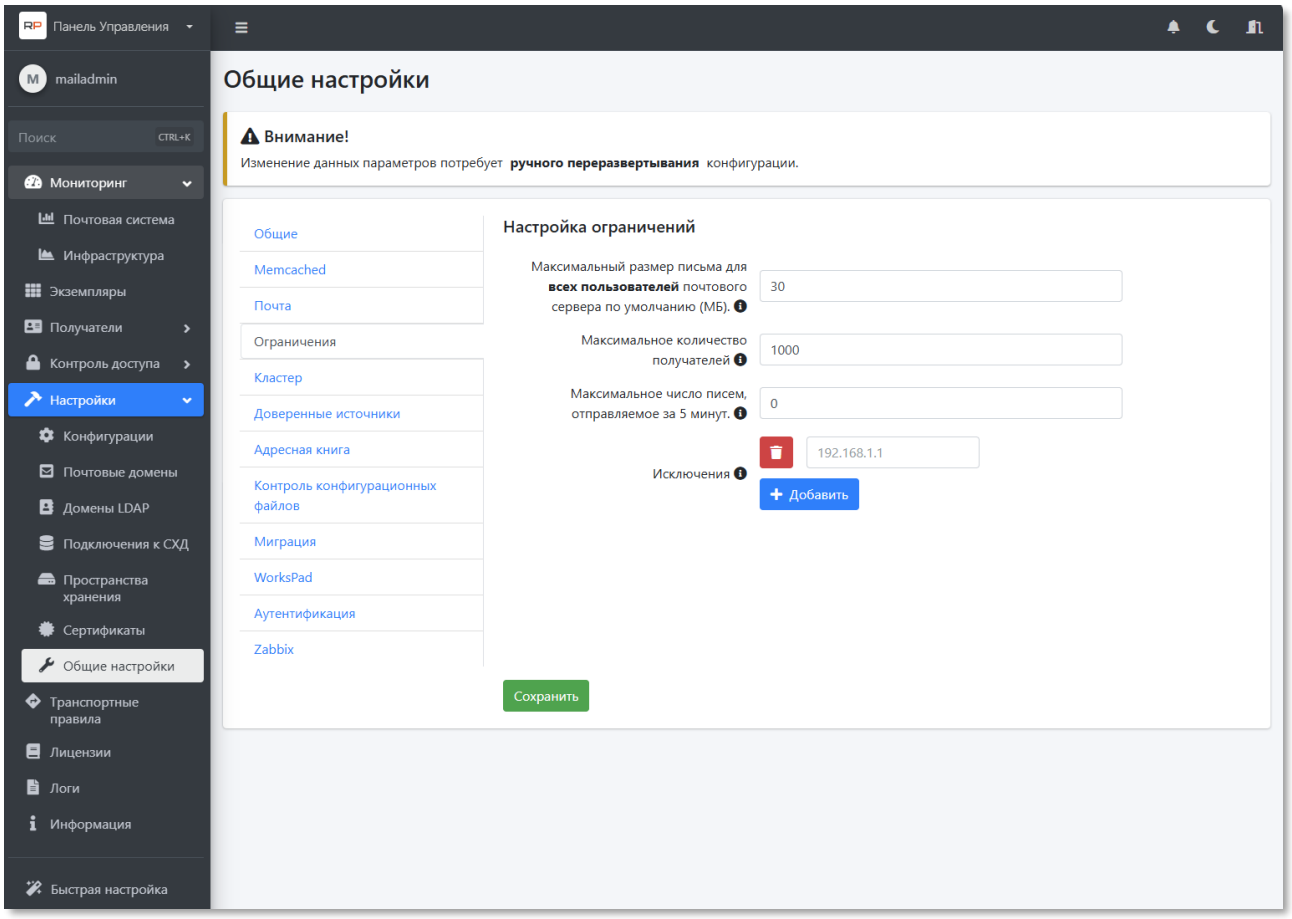
Внимание!

После установки новых сертификатов старые сертификаты в каталоге `/etc/ssl/certs`не удаляются, их можно удалить вручную.

2.6. Общие настройки системы

Общие настройки системы определяют глобальные параметры функционирования системы, определяемые администратором системы:

- Имя хоста почтовой системы, отражаемое в MX-записи DNS.
- Поддержка автонастройки клиентов (autodiscovery/autoconfig).
- Максимальный размер письма для всех пользователей (вкладка «Ограничения»).
- Адрес почтового ящика администратора системы, на который могут приходить сообщения-“отбои” в случае невозможности доставки отправляемых писем.
- Адрес почтового ящика системы защиты от утечек данных (DLP – Data Leak Prevention), который автоматически будет прописываться в BCC для всех отправляемых писем.



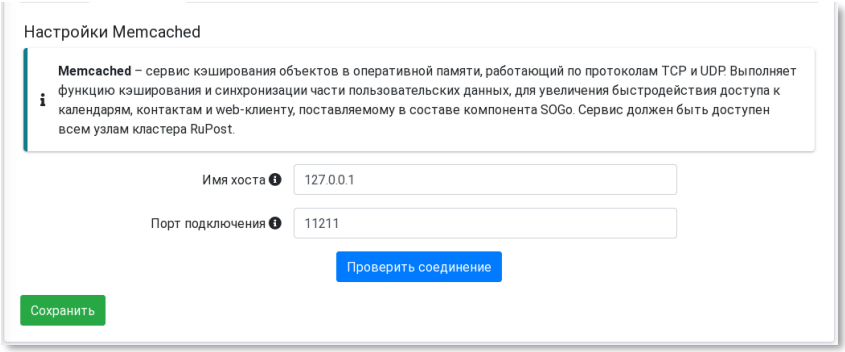
Внимание!

По умолчанию имя хоста почтовой системы не задано! Необходимо задать имя почтового сервера, указываемое для подключения клиентских приложений.

2.6.1. Общие настройки – rupost-cs (Memcached)

Также, общие настройки включают и параметры сервиса Memcached для кеширования данных (вкладка Memcached). На этой вкладке указывается адрес и порт сервиса кеширования данных **Memcached** в оперативной памяти.

В версии 2.5.0 добавлена возможность проверки подключения к сервису Memcached:

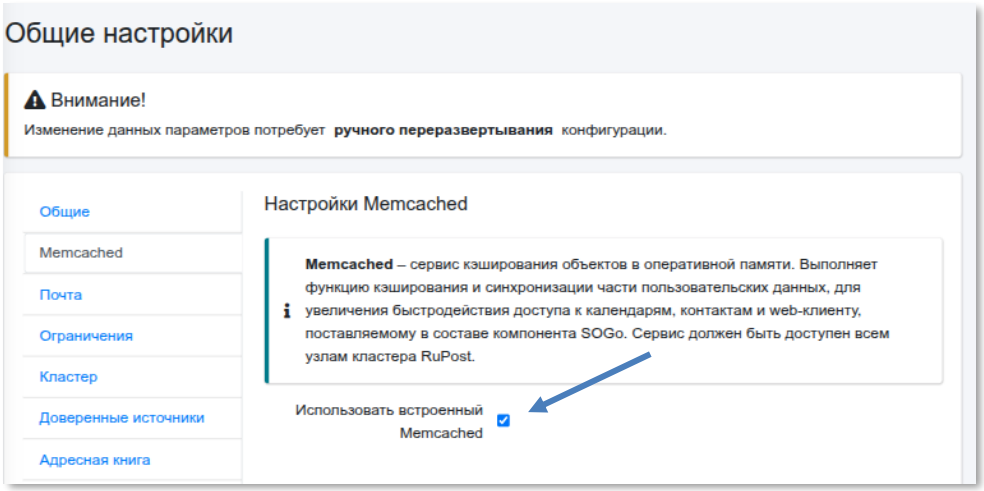


Если Memcached установлен на выделенный сервер, то в поле “Имя хоста” необходимо указывать A запись его расположения в DNS.

В версии 4.2.0 устранена необходимость развертывания отдельного сервера *rupost-cs* (Memcached) для кластера RuPost – в качестве общего может использоваться *rupost-cs*, установленный на одном из узлов кластера RuPost.

Узел, на котором будет использоваться *rupost-cs* в качестве общего ресурса, выбирается случайным образом из работающих узлов кластера. При выходе из строя данного узла, перенастройка на другой узел произойдет автоматически.

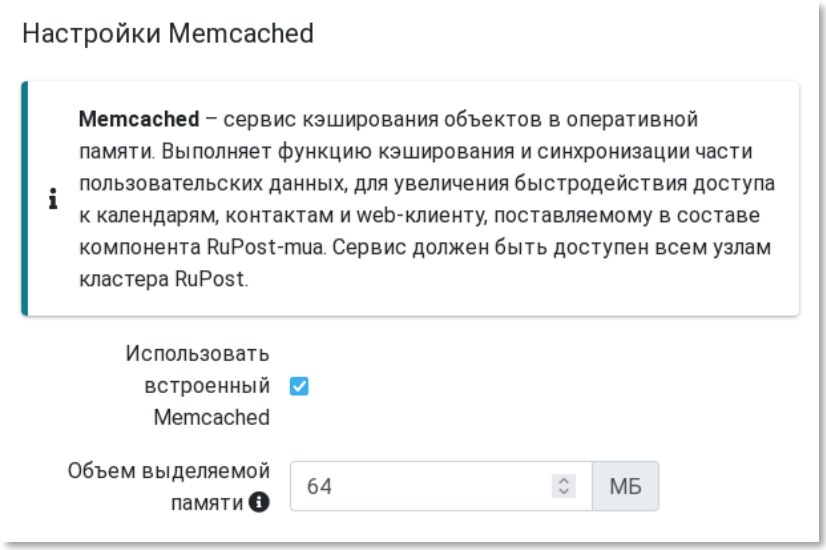
Для управления конфигурацией *rupost-cs*, используйте переключатель “Использовать встроенный Memcached” (страница “Общие настройки”, вкладка “Memcached”).



Если у вас уже есть кластер RuPost с выделенным сервером Memcached, то для перехода на использование находящегося на узлах кластера *rupost-cs*, необходимо установить переключатель «Использовать встроенный Memcached» и *переразвернуть конфигурацию.*

В версии 4.3.4 добавлена возможность настраивать размер используемой памяти для встроенного компонента Memcached.

Размер памяти, используемый компонентом Memcached для кеширования данных, определяется параметром “Объем выделяемой памяти” (вкладка “Memcached” на странице “Общие настройки”). Минимально необходимый размер памяти – 64 МБ.

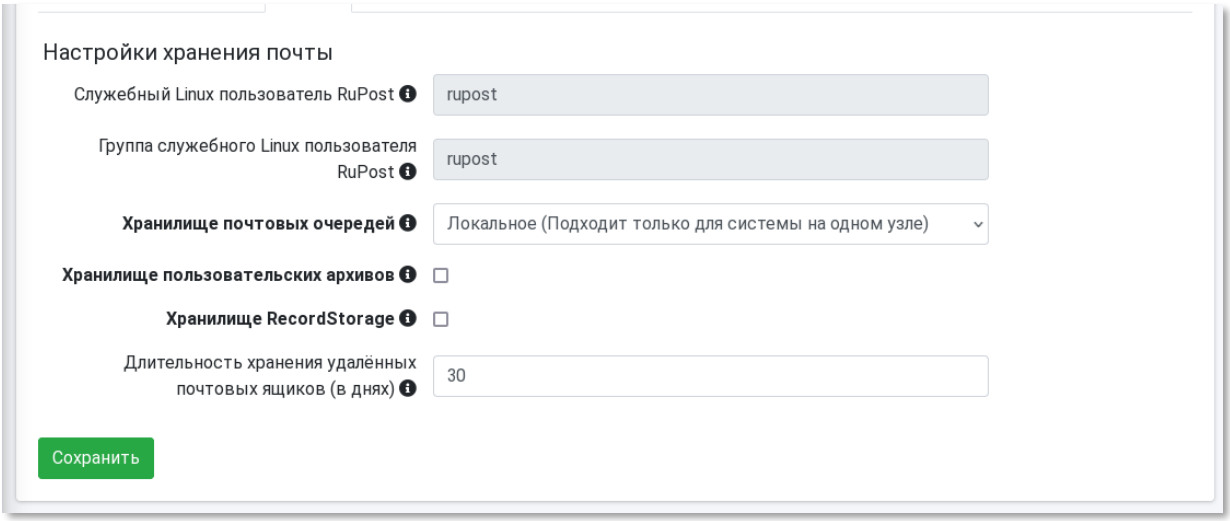


2.6.2. Общие настройки - почта

Важным разделом общих настроек RuPost являются **настройки хранения почты.**

Изменения в версии 3.0

В версии 3.0 изменена структура хранения почты (см. раздел “Группы ящиков, Пространства хранения и Хранилища”) и, соответственно, внесены изменения в настройки на вкладке “Почта” страницы “Общие настройки”.
Так как настройка индивидуальных точек монтирования для хранения почты является частью настроек отдельного Хранилища, то этой вкладке осталась только настройка точки монтирования для очередей (так как она единая для всего кластера RuPost).
Опция включения/отключения Архивов и Record Storage, также, не содержит настройки точки монтирования и является единой для всего кластера RuPost. При включении Архивов и/или Record Storage соответствующая точка монтирования должна быть настроена у всех Хранилищ, кроме Backup.



- **Хранилище почтовых очередей**, в которое попадают все отправляемые письма для дальнейшей обработки и пересылки на другие почтовые серверы.
- **Хранилище пользовательских архивов**, в случае включения - доступны пользователям для переноса писем и восстановления с использованием клиентских приложений, где архивы выглядят как специализированные папки “Архивы”. По умолчанию - выключено.
- **Хранилище RecordStorage** – предназначено для ведения дубликатов всех удаляемых писем пользователей, недоступных в почтовом ящике и архиве пользователя, что может требоваться регуляторами и/или внутренними регламентами организации в рамках осуществления процедур Управления записями (англ. Records Management) для управления документами организации с момента их создания до окончательного уничтожения. Эти данные, в отличие от архивов - недоступны пользователям. По умолчанию - выключено.

RuPost поддерживает:

- локальное хранение – т.е. на том же узле, где развернута система;
- сетевое хранение – на ресурсах NFS.

По умолчанию, при развертывании на одном узле, почтовые ящики и очереди сообщений хранятся локально, а пользовательские архивы и хранилища RecordStorage - выключены.

Рекомендации: Практика эффективного использования инфраструктурных ресурсов для функционирования почтовой системы организации предполагает размещение пользовательских архивов и RecordStorage на менее производительных системах хранения, в отличие от почтовых ящиков и очередей сообщений, обычно требующих высокоскоростного доступа (обычно на системах хранения с SSD).

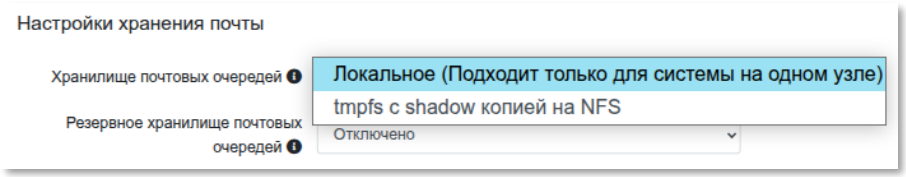
Параметры организации подключения сетевых каталогов файловой системы NFSv4 описано в “*Руководстве по установке и конфигурированию*” RuPost.

В версии 4.2.0 оптимизирована работа компонента *rupost-mta* (Postfix).

Почтовые очереди *incoming*, *active* и *deferred* перенесены в оперативную память, что существенно ускорило обработку почты и снизило нагрузку на дисковую подсистему или NFS.

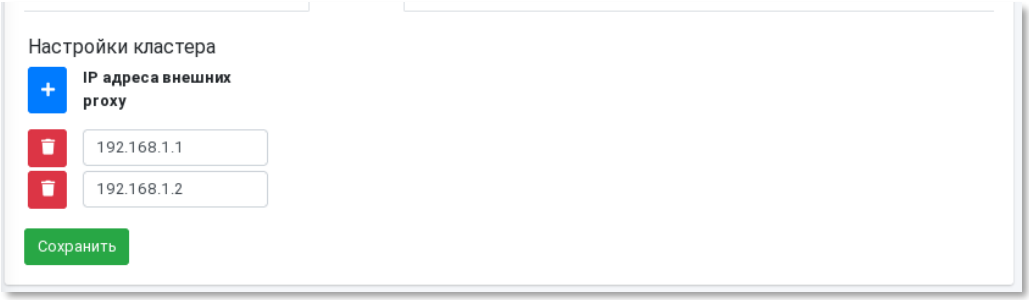
Для того, чтобы при выходе из строя узла кластера исключить потерю почты, находящейся в почтовых очередях, резервная (shadow) копия сохраняется на NFS в каталоге *shadow*, который находится там же, где и находились почтовые очереди до версии 4.2.0. С учетом этого изменения, были, также, внесены изменения в механизм эвакуации почты при выходе узла кластера из строя.

Для одноузловой конфигурации, где для хранения почты используется локальный диск, перенос очередей в оперативную память не применяется.



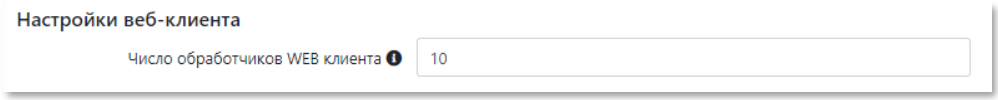
2.6.3. Общие настройки - кластер

В том случае, когда RuPost работает через внешние прокси сервера или балансировщики нагрузки, поддерживающие PROXY протокол, на закладке “Кластер” необходимо указать перечень внешних прокси серверов и балансировщиков – указываются IP адрес или подсеть всех внешних серверов.



2.6.4. Общие настройки – число обработчиков web клиента

В версии 3.1.0 в Панели управления добавлен новый параметр, управляющий количеством обработчиков web клиента для компонента SOGo (“Общие настройки” -> “Почта” -> ”Настройка веб клиента”).

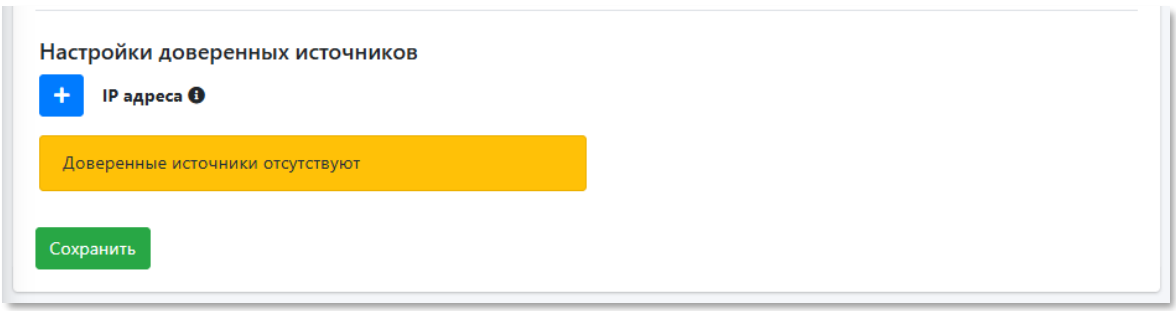


Сбалансированное число обработчиков зависит как от соотношения числа пользователей настольных клиентов и web-интерфейса, так и общего количества клиентских подключений. При росте числа пользователей web клиента, может потребоваться увеличение значения этого параметра. Устанавливать значение **менее 20** не рекомендуется даже в том случае, когда web-клиент не используется.

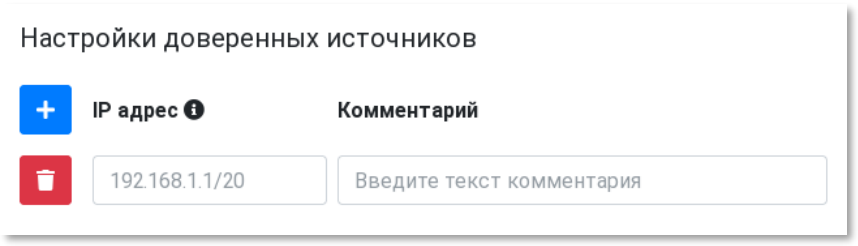
Так как этот параметр теперь добавлен как общесистемная настройка, то из встроенных шаблонов удалён раздел “Настройка WEB клиента”.

2.6.5. Общие настройки - отправка с разрешенных IP адресов без авторизации

В версии 3.2.0 добавлена возможность отправки почты без авторизации из доверенных источников (только на порт 25). Указать перечень доверенных IP адресов можно на закладке “Доверенные источники” страницы “Общие настройки”.

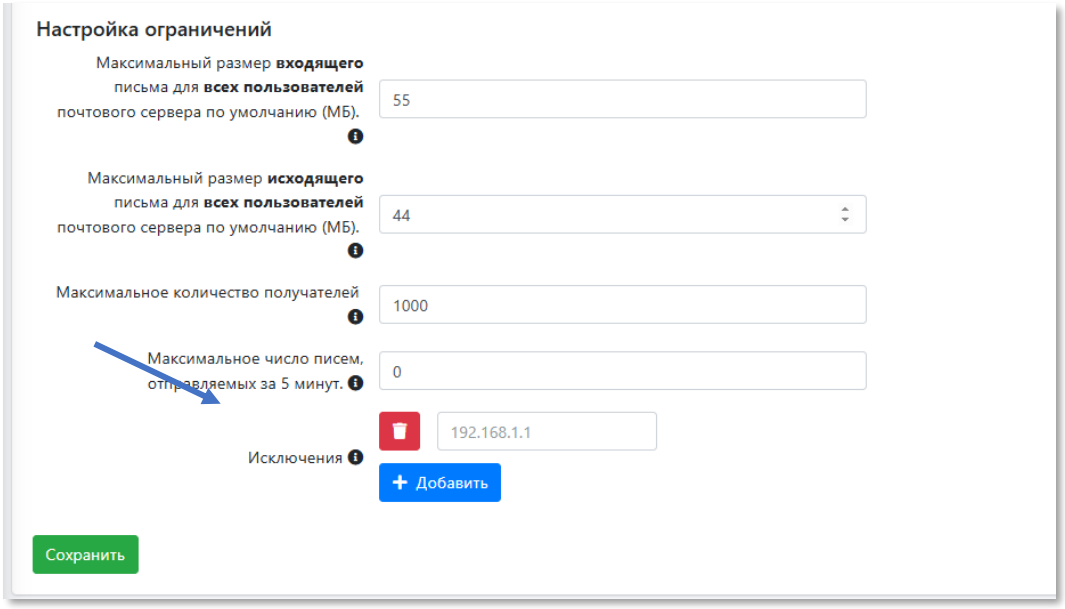


В версии 4.3.4 при создании записи о доверенном источнике (вкладка “Доверенные источники” на странице “Общие настройки”) кроме ввода IP адреса появилась возможность добавить комментарий – например, указать наименование или номер устройства и причину его добавления в доверенные источники.



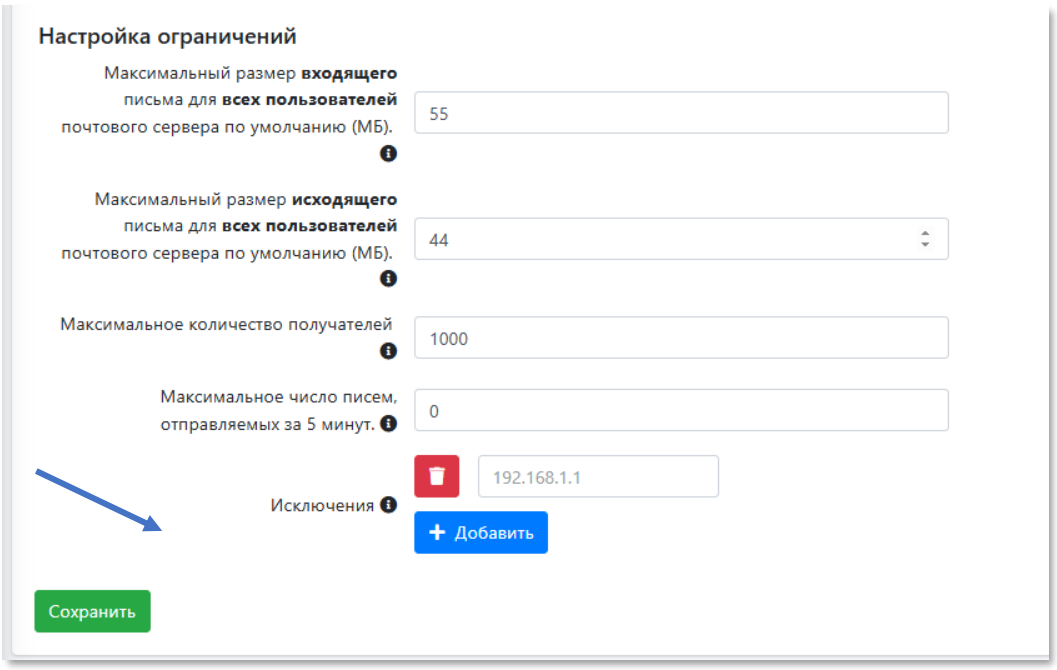
2.6.6. Общие настройки - максимальное число получателей

В версии 3.2.0 добавлена возможность указать максимально возможное число получателей для одного отправляемого письма. Этот параметр указывается на закладке “Ограничения” страницы “Общие настройки”.



2.6.7. Общие настройки - максимальная частота отправки писем (rate limit)

В версии 3.2.0 добавлена возможность управлять максимальной частотой отправки писем – параметр “Максимальное число писем, отправляемое за 5 минут” находится на закладке “Ограничения” страницы “Общие настройки”.



Если нужно разрешить отдельным отправителям превышать указанное ограничение, то их IP адреса нужно добавить в список “Исключения”.

2.6.8. Общие настройки - максимальный размер письма

В версии 4.0 изменено управление максимальным допустимым размером обрабатываемых писем.

Теперь нельзя указать различные значения для размера входящих и исходящих писем – указывается только одно значение. Соответственно, было проведено обновление Панели управления:

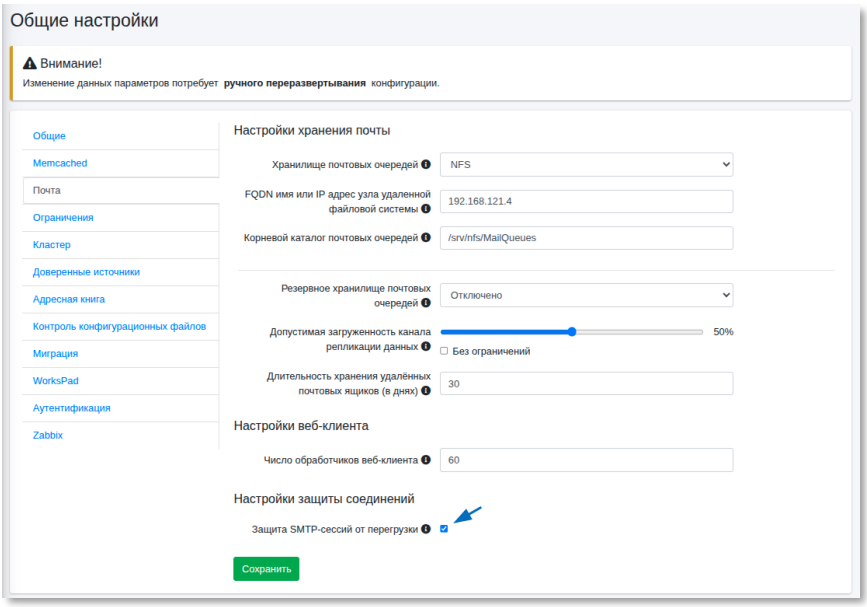
- В окне “Общие настройки” на закладке “Почта” указывается только одно значение – “Максимальный размер письма почтового сервера по умолчанию (МБ)”.
- В Групповых политиках название столбца “Максимальный размер входящего письма (МБ)” изменено на “Максимальный размер письма (МБ)”.

2.6.9. Возможность отключения сервиса postscreen

В версии 4.0 добавлена возможность отключения сервиса MTA postscreen.

Сервис MTA postscreen добавляет к обработчику SMTP протокола дополнительную защиту от перегрузки его сервисов, которые обычно происходят из-за попыток рассылки спам-писем. Слишком частые подключения по SMTP от отдельных серверов являются одним из признаков, по которым postscreen определяет паразитный почтовый траффик. Для обращений с этих серверов, postscreen добавляет интервал ожидания сессии, тем самым, снижая нагрузку на почтовую систему и обеспечивая приоритетную доставку почты с других серверов. Однако, в конфигурациях, когда входящая почта сначала проходит через почтовый шлюз, а затем передается на MTA, защитой от подобных атак уже занимается вышестоящий шлюз, обычно это антивирус. Поэтому, в таком случае, службу postscreen желательно отключать.

Отключить службу postscreen можно в Панели управления (окно “Общие настройки”, закладка “Настройки хранения почты”) переключателем “Защита SMTP сессий от перегрузки”.



2.7. Подключение служб каталогов LDAP

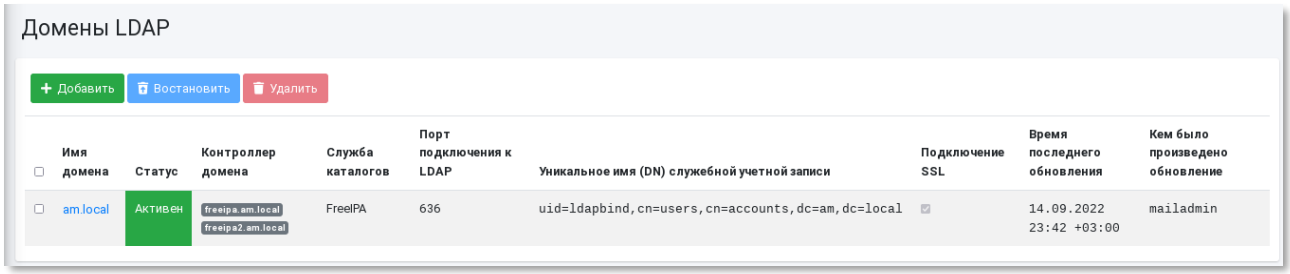
RuPost обеспечивает одновременную работу с несколькими службами каталогов.

Поддерживаемые службы каталогов:

- Microsoft Active Directory
- FreeIPA
- ALD Pro Группы “Астра”
- Samba DC

В версии 4.0 добавлена поддержка нового типа каталога LDAP – “Аванпост”. Наличие поддержки LDAP домена “Аванпост” позволяет использовать RuPost совместно с системой аутентификации и управления доступом компании “Аванпост”.

Почтовые ящики в RuPost могут создаваться только для пользователей тех служб каталогов, которые зарегистрированы в системе LDAP. Соответствующая служба каталогов используется для аутентификации в LDAP пользователя при любой операции работы с почтовым ящиков (отправка, получение, архивирование писем, работа с календарями, контактами и адресной книгой). Также на базе зарегистрированных в системе служб каталогов (должны находится в статусе Активен) строится корпоративная адресная книга, которая автоматически доступна пользователям системы.

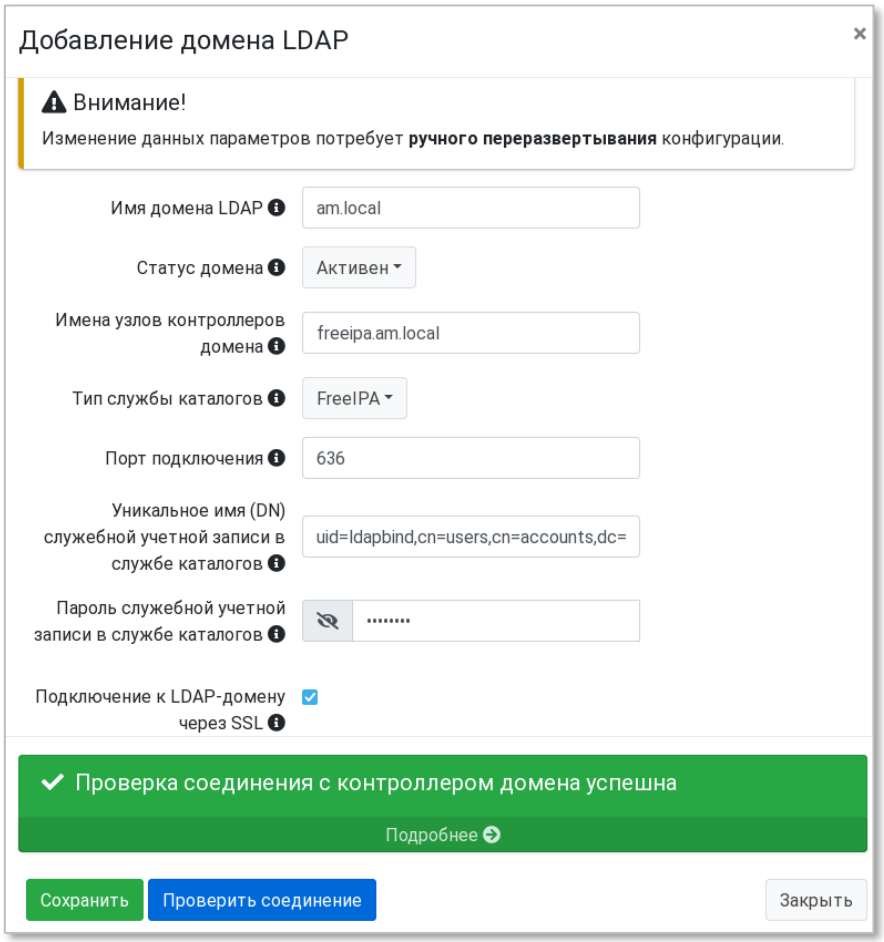


Для чтения информации из служб каталогов система RuPost обращается к соответствующей службе каталогов через специализированную учетную запись bind, составное уникальное имя которой – DN (Distinguished Name) необходимо указывать при регистрации службы каталогов в системе. Обычно запись DN представляется в следующем виде:

`uid=ldapbind,cn=users,cn=accounts,dc=<основная часть домена>,dc=<домен верхнего уровня>`

Статус домена LDAP может принимать значения:

- Активен – может использоваться
- Отключен – не используется
- Удален – удален, возможно восстановление

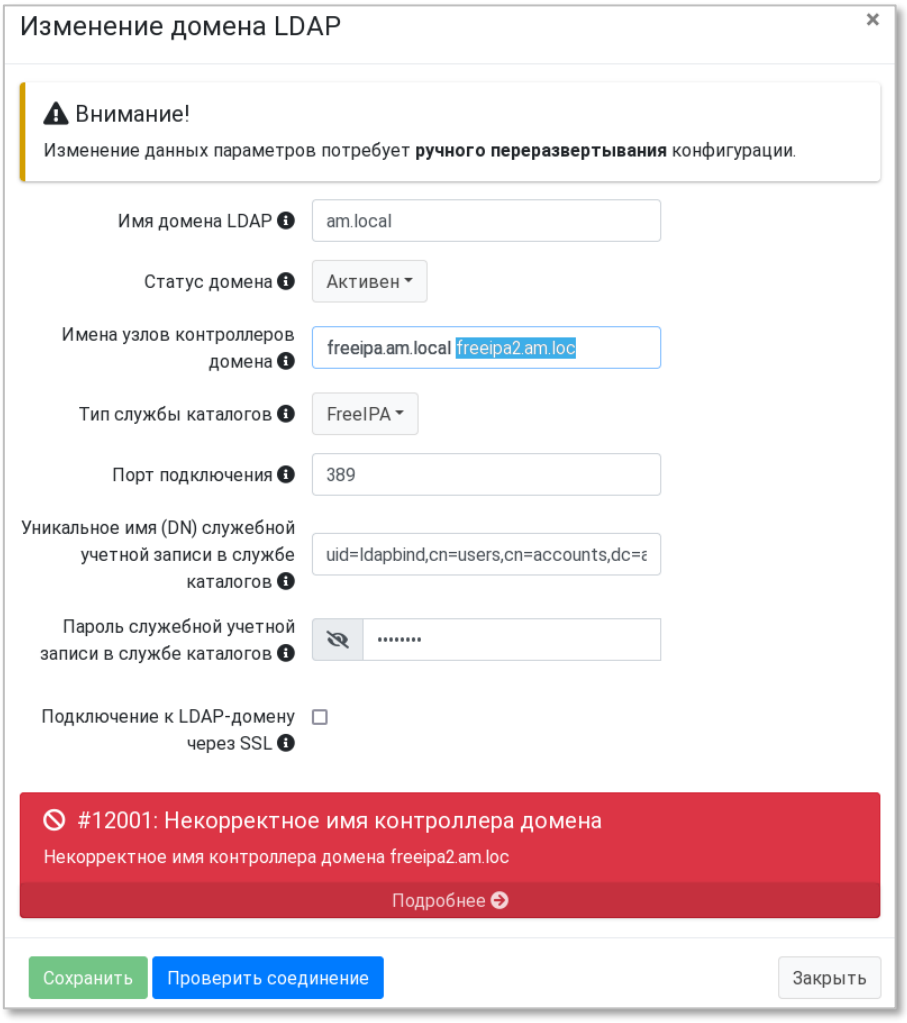


Внимание! Изменение списка используемых служб каталогов, как и любого отдельного параметра записи о службе каталогов, включая ее статус, требует явного повторного развертывания конфигурации для обновления информации об используемых службах каталогов в конфигурационных параметрах системы и ее компонентов.

Внимание! При установке подключения к LDAP по SSL (т.е. LDAPS) проверьте порт подключения! В типовых конфигурациях необходимо изменить порт по умолчанию 389 без SSL на 636 при использовании SSL.

Изменение параметров домена осуществляется выбором имени домена в списке.

В случае недоступности любого из указанных контроллеров домена в информации об ошибке будет указано имя недоступного контроллера домена.



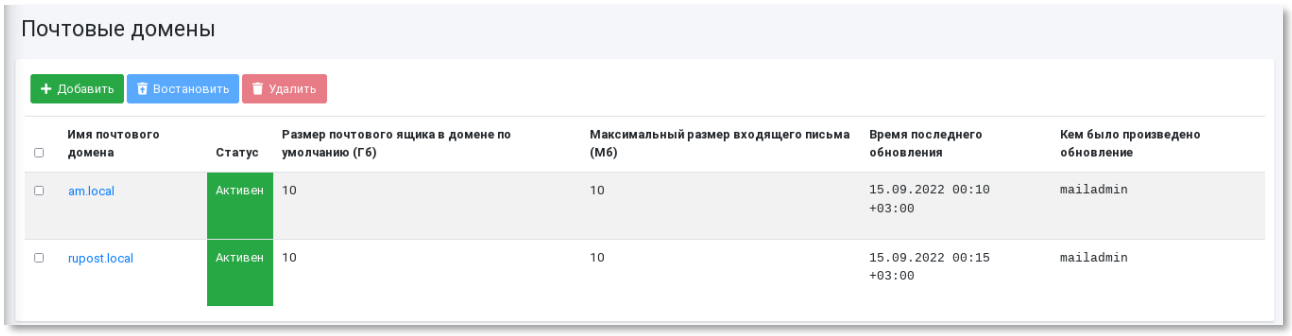
В версии 4.0 добавлена поддержка доменов верхнего уровня (TLD - Top Level Domain) для названий LDAP доменов. Наименование LDAP домена может состоять из одного слова без точки – например “mycompany”.

Внимание!

Так как RuPost синхронизирует данные почтовых ящиков с данными в LDAP каталогах, то после внесения изменений в настройки LDAP каталогов и при наличии большого количества почтовых ящиков синхронизация может проходить в течение нескольких минут.

2.8. Настройка почтовых доменов

Все используемые почтовые домены должны быть зарегистрированы в системе.



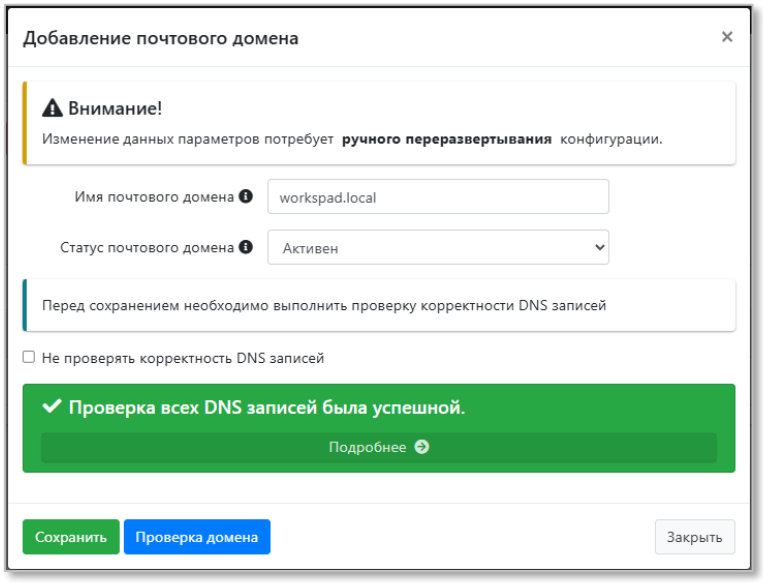
RuPost поддерживает возможность одновременной работы с несколькими почтовыми доменами. При этом почтовые домены не связаны с доменами LDAP – одни и те же почтовые домены могут использоваться для организации почтовых ящиков пользователей из разных служб каталогов.

Для используемых почтовых доменов на используемых в организации серверах DNS должны быть заведены соответствующие записи, параметры которых представлены в “*Руководстве по установке и конфигурированию*” RuPost.

Статус почтового домена может принимать значения:

- **Активен** – может использоваться:
- **Отключен** – не используется;
- **Удален** – удален, возможно восстановление.

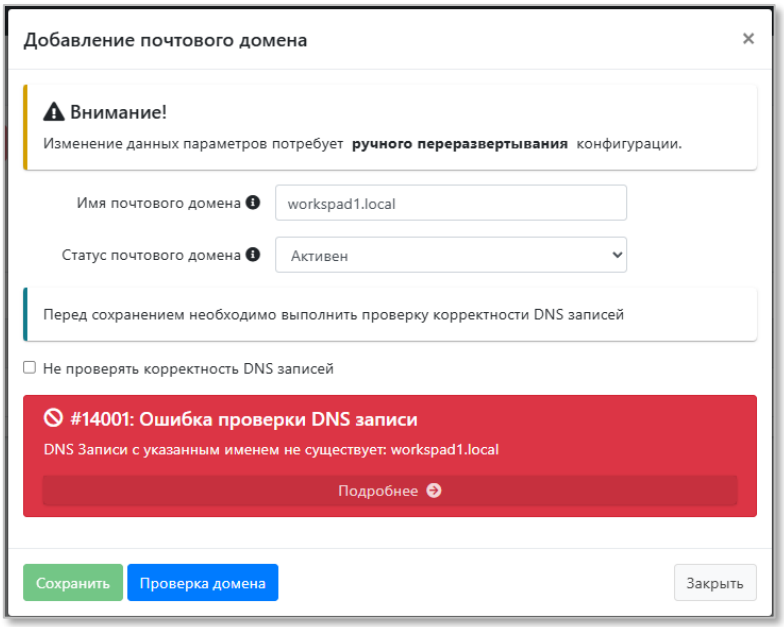
Начиная с версии 3.1.0 квоты на почтовые ящики определяются Политиками квотирования.



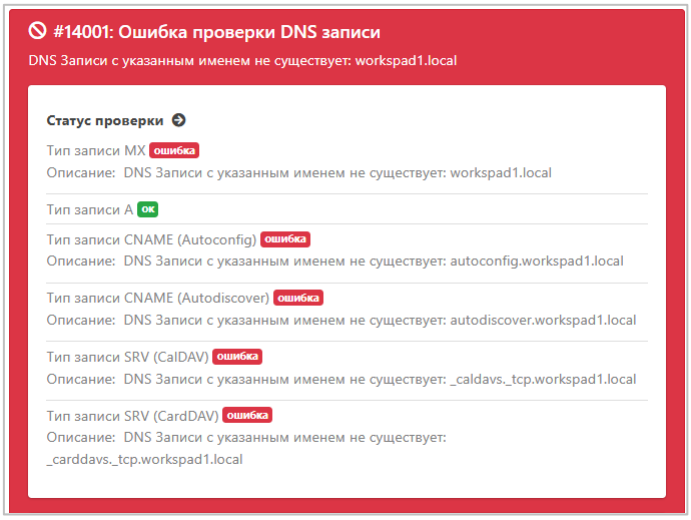
Проверка соединения для выбранного почтового домена может осуществляться только при наличии соответствующих записей в DNS. Для заведения почтовых доменов до или без внесенных A- и MX-записей в DNS (например, для доменов-псевдонимов) необходимо перед сохранением информации о почтовом домене отметить опцию “Не требовать проверки соединения”.

Внимание!
Изменение списка используемых почтовых доменов, как и любого отдельного параметра записи о почтовом домене, включая его статус, требует явного - ручного развертывания конфигурации с использованием Панели управления RuPost.

В случае отсутствия необходимых записей или наличия ошибок в записях, при проверке соединения с DNS будет отображена ошибка с показом первой отсутствующей или неверной записи.



В свою очередь, при выборе ссылки “Подробнее” (в области отображения ошибки под ее текстом) будут отображены все найденные ошибки.



В версии 4.0 добавлена поддержка почтовых доменов, у которых наименование домена первого уровня состоит из одной буквы. Например “mycompany.r”.

2.9. Развертывание конфигураций

Внимание!

Развертывание конфигурации RuPost должно производиться только после задания параметров общих настроек системы, регистрации доменов LDAP и определения почтовых доменов.

Перед развертыванием конфигурации проверьте настройки и доступность требуемых инфраструктурных сервисов.

Развертывание конфигурации производится на базе выбора необходимого шаблона конфигурации из доступных шаблонов библиотеки конфигураций.

Страница Конфигурация в Панели управления RuPost содержит виджеты:

- Библиотека шаблонов конфигураций для выбора необходимого шаблона
- Историю успешно развернутых конфигураций, позволяющую повторно развернуть заданную конфигурацию с применением новых общесистемных параметров, списка актуальных активных доменов LDAP и почтовых доменов

2.9.1. Библиотека шаблонов конфигураций

Внимание!

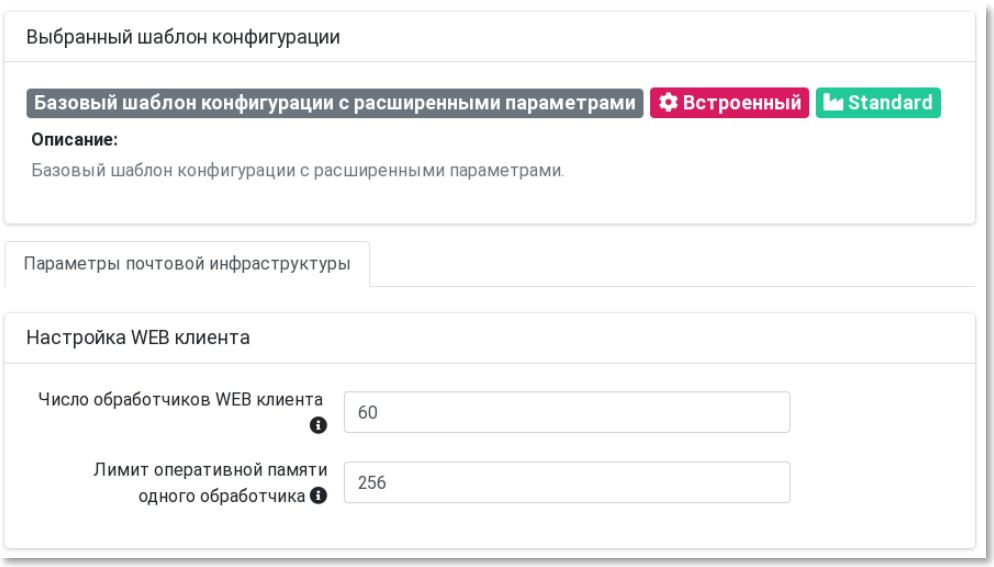
RuPost начиная с версии 2.0.3 не поддерживает шаблоны с версией схемы ниже 4.

Библиотека шаблонов RuPost включает встроенные (builtin) шаблоны конфигураций:

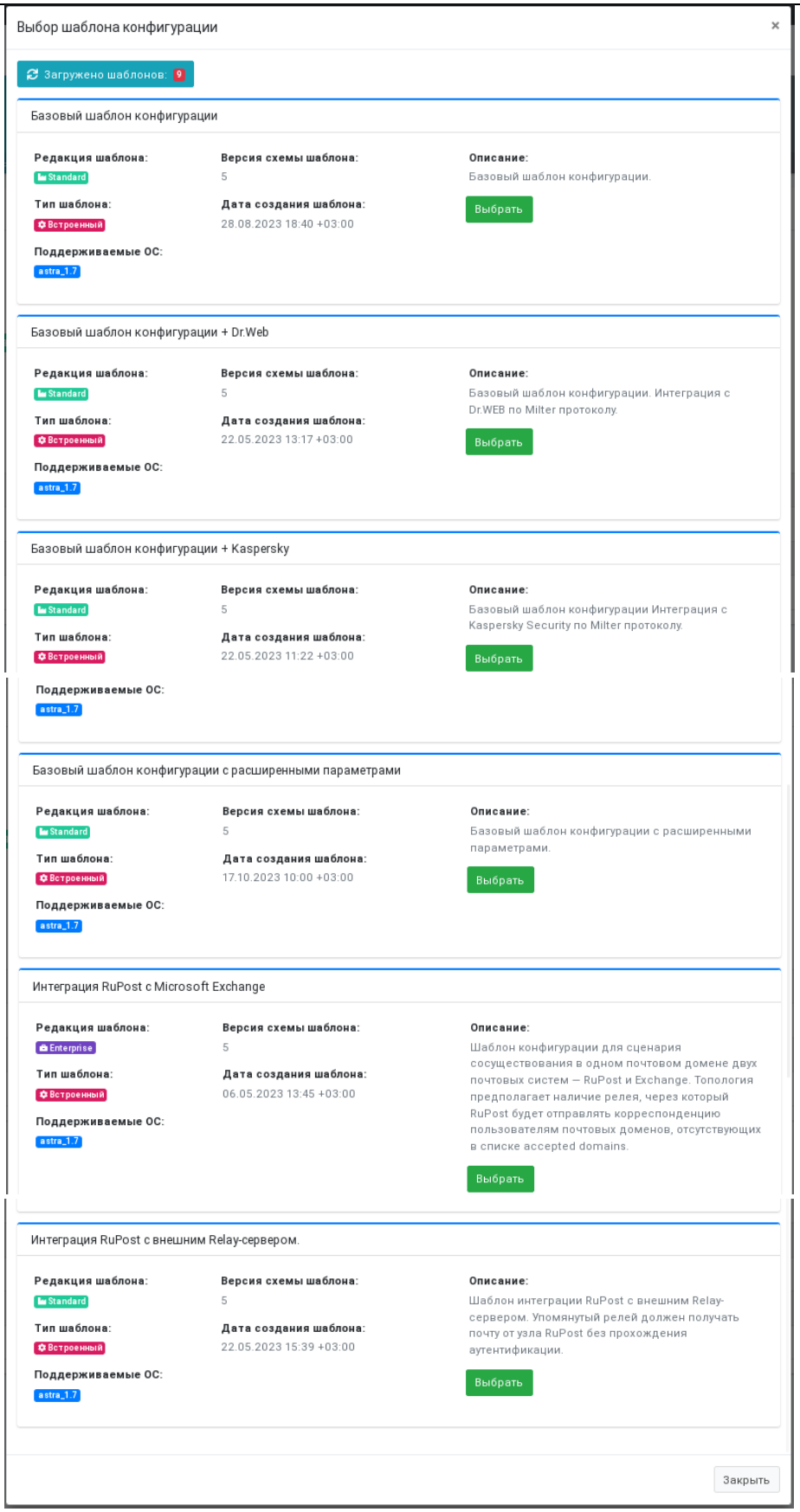
- **Базовый шаблон конфигурации** – для развертывания конфигурации на одном узле и в кластере.
- **Базовый шаблон конфигурации с расширенными параметрами –** применяется при наличии большого числа пользователей, использующих веб-клиент.
- **Интеграция RuPost с внешним релей сервером** – применяется при работе сервера RuPost через внешний релей сервер. Требует ввода дополнительных параметров конфигурации для взаимодействия с релеем. Подробное описание шаблона приведено в Приложении 1.
- **Базовый шаблон конфигурации + Kaspersky** – шаблон конфигурации со встроенной интеграцией с системами защиты почты Kaspersky Security for Linux Mail Server (KLMS) и Kaspersky Security Mail Gateway (KSMG) по протоколу Milter. Требует ввода дополнительных параметров конфигурации – имени хоста и порта подключения к соответствующей системе защиты.
- **Базовый шаблон конфигурации + Dr.Web** - шаблон конфигурации со встроенной интеграцией защиты почты Dr.Web по протоколу Milter. Требует ввода дополнительных параметров конфигурации – имени хоста и порта подключения к соответствующей системе защиты.
- **Интеграция RuPost с Microsoft Exchange** – шаблон конфигурации для сосуществования RuPost и Microsoft Exchange. Шаблон применяется для сосуществования сервера RuPost и Microsoft Exchange в рамках одного почтового домена. Подробное описание шаблона

приведено в Приложении 2. **Этот шаблон может быть применен только в редакции Enterprise.**

В версии 2.5.0 для более точного учета нагрузки при использовании web клиентов, добавлен новый шаблон конфигурации “Базовый шаблон конфигурации с расширенными параметрами”, а также добавлены дополнительные параметры настройки во все шаблоны, кроме шаблона “Базовый шаблон конфигурации”. Секция “Настройки Web клиента” содержит два параметра:



Значения этих параметров зависят от планируемой нагрузки на экземпляр RuPost – более подробно см. Приложение 1 “Руководство по установке и конфигурированию”.


Выбор шаблона конфигурации
Загружено шаблонов: 9
Базовый шаблон конфигурации
Редакция шаблона:
Standard
Версия схемы шаблона:
5
Описание:
Базовый шаблон конфигурации.
Тип шаблона:
Встроенный
Дата создания шаблона:
28.08.2023 18:40 +03:00
Выбрать
Поддерживаемые ОС:
astra_1.7
Базовый шаблон конфигурации + Dr.Web
Редакция шаблона:
Standard
Версия схемы шаблона:
5
Описание:
Базовый шаблон конфигурации. Интеграция с Dr.WEB по Milter протоколу.
Тип шаблона:
Встроенный
Дата создания шаблона:
22.05.2023 13:17 +03:00
Выбрать
Поддерживаемые ОС:
astra_1.7
Базовый шаблон конфигурации + Kaspersky
Редакция шаблона:
Standard
Версия схемы шаблона:
5
Описание:
Базовый шаблон конфигурации Интеграция с Kaspersky Security по Milter протоколу.
Тип шаблона:
Встроенный
Дата создания шаблона:
22.05.2023 11:22 +03:00
Выбрать
Поддерживаемые ОС:
astra_1.7
Базовый шаблон конфигурации с расширенными параметрами
Редакция шаблона:
Standard
Версия схемы шаблона:
5
Описание:
Базовый шаблон конфигурации с расширенными параметрами.
Тип шаблона:
Встроенный
Дата создания шаблона:
17.10.2023 10:00 +03:00
Выбрать
Поддерживаемые ОС:
astra_1.7
Интеграция RuPost с Microsoft Exchange
Редакция шаблона:
Enterprise
Версия схемы шаблона:
5
Описание:
Шаблон конфигурации для сценария сосуществования в одном почтовом домене двух почтовых систем — RuPost и Exchange. Топология предполагает наличие релея, через который RuPost будет отправлять корреспонденцию пользователям почтовых доменов, отсутствующих в списке accepted domains.
Тип шаблона:
Встроенный
Дата создания шаблона:
06.05.2023 13:45 +03:00
Выбрать
Поддерживаемые ОС:
astra_1.7
Интеграция RuPost с внешним Relay-сервером.
Редакция шаблона:
Standard
Версия схемы шаблона:
5
Описание:
Шаблон интеграции RuPost с внешним Relay-сервером. Упомянутый релей должен получать почту от узла RuPost без прохождения аутентификации.
Тип шаблона:
Встроенный
Дата создания шаблона:
22.05.2023 15:39 +03:00
Выбрать
Поддерживаемые ОС:
astra_1.7
Закрыть

При наличии лицензии редакции Enterprise возможно применение собственных – “пользовательских” (custom) шаблонов конфигураций. Для загрузки и удаления таких шаблонов в библиотеку шаблонов необходимо использовать командный интерфейс CLI.

Синтаксис команды и примеры управления шаблонами из командной строки приведены в разделе **«rupost template группа команд для управления шаблонами конфигураций»** Справочного руководство по командной строке.

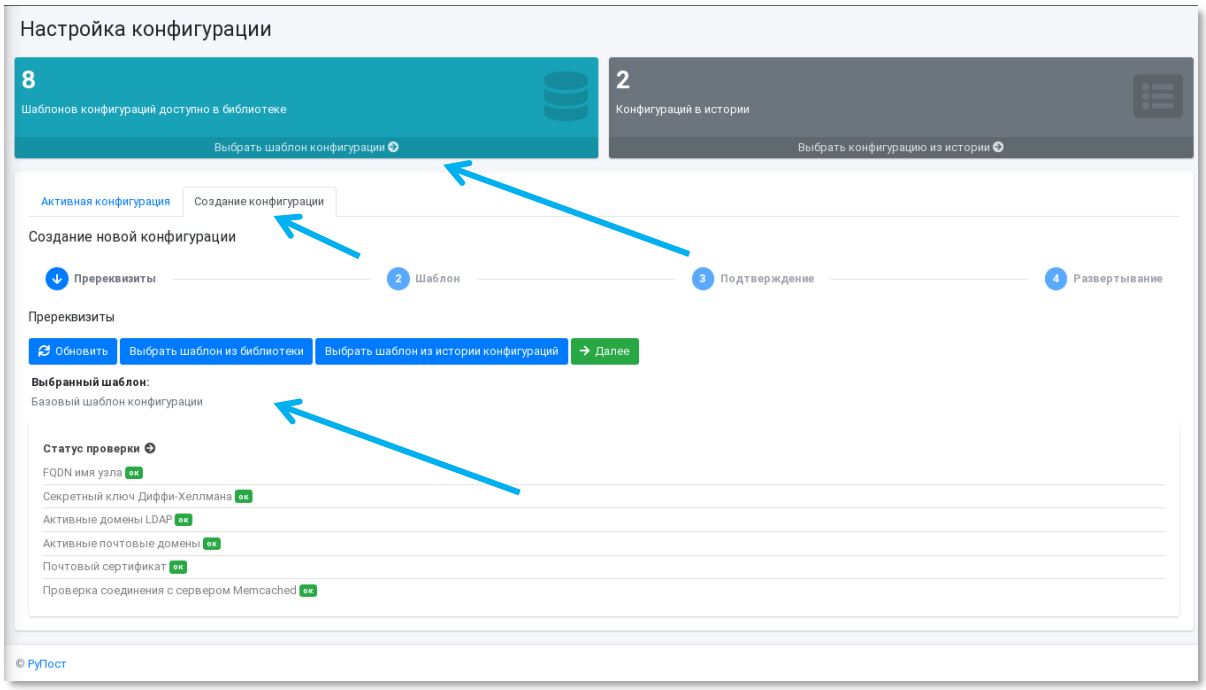
После выбора соответствующего шаблона конфигурации и указания дополнительных параметров конфигурации, в случае такой необходимости, администратор системы может развернуть новую конфигурацию, обратившись к пошаговому визарду на вкладке “Создание конфигурации”.

На странице представлены две вкладки:

- **Активная конфигурация**, отображающая текущую конфигурацию, сохраненную в базе данных;
- **Создание конфигурации** – пошаговый визард развертывания конфигурации с проверкой необходимых для развертывания параметров/

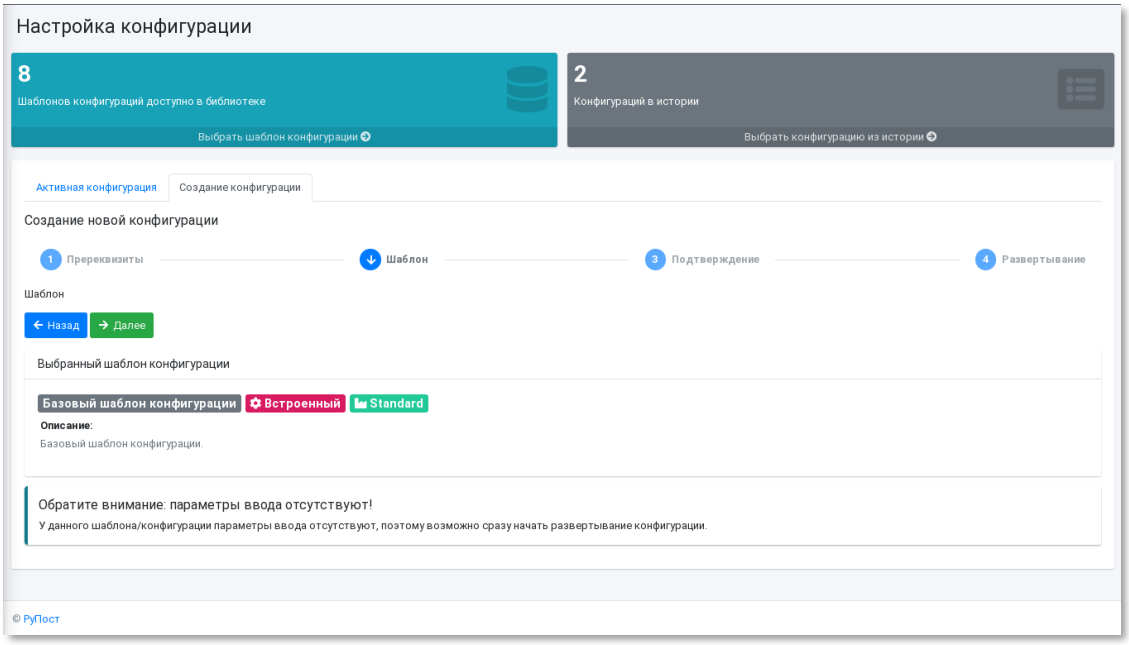
2.9.2. Создание конфигурации

Для создания конфигурации требуется выбрать необходимый шаблон из библиотеки доступных шаблонов конфигураций. К библиотеке шаблонов можно обратиться из виджета Шаблоны конфигураций или непосредственно на вкладке Создание конфигурации.

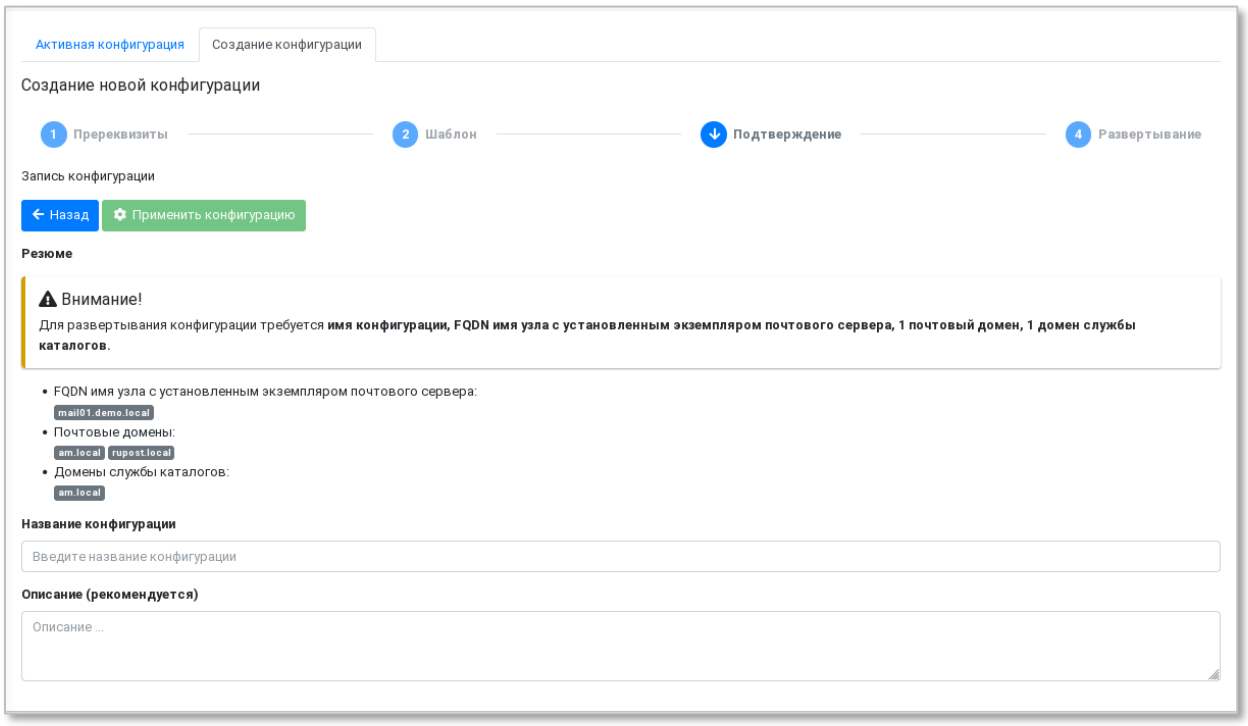


При открытии вкладки Создание конфигурации автоматически запускается первый шаг – Пререквизиты, на котором проверяются необходимые для развертывания параметры.

Также на данной вкладке возможен выбор необходимой конфигурации из истории успешных конфигураций, например, для повторного развертывания текущей (“активной”) конфигурации после обновления системы (это необходимо в связи с необходимостью перегенерации конфигурационных файлов почтовых компонентов системы, работающих с обновленной структурой баз данных RuPost).

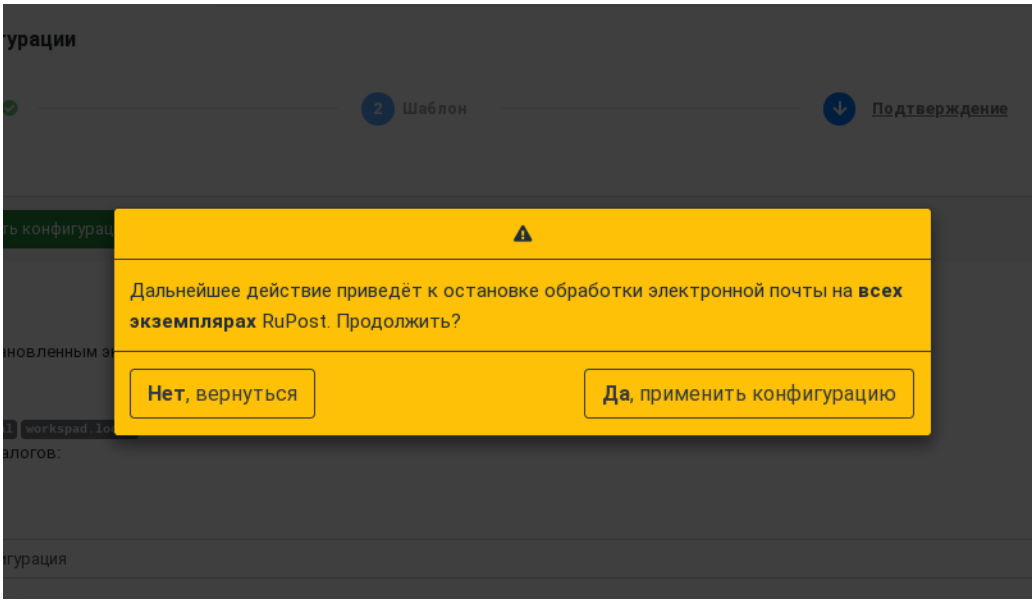


После нажатия кнопки “Далее” администратору системы предлагается задать название конфигурации и составить Описание.

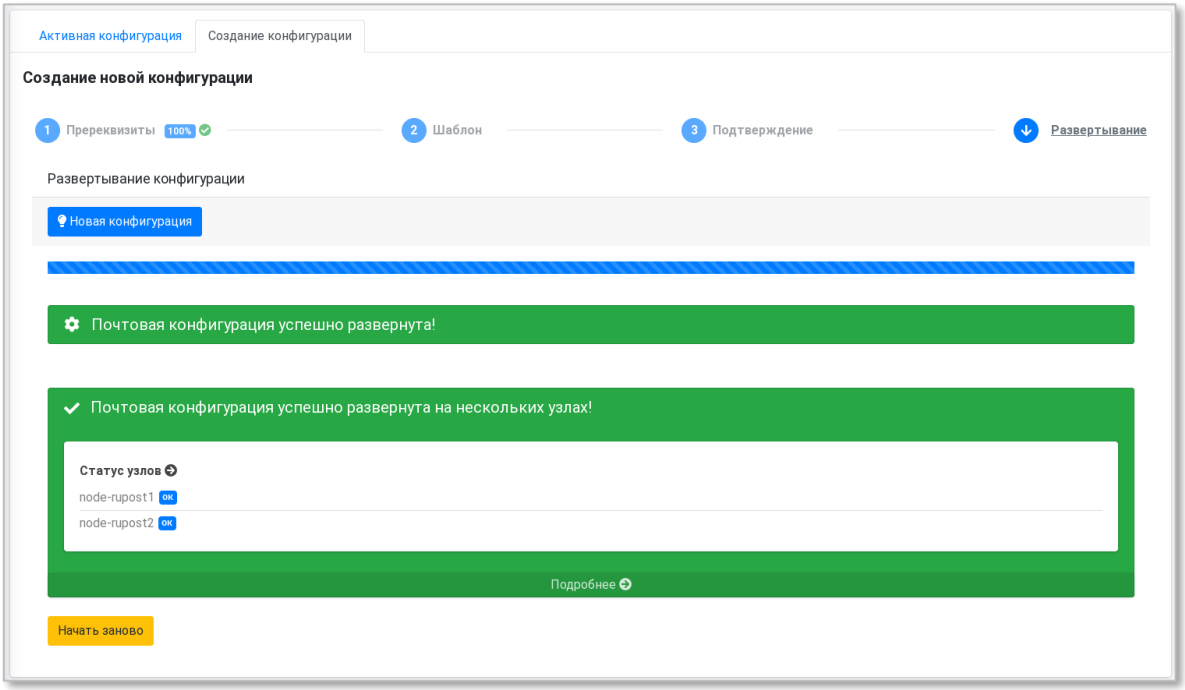


При этом администратору доступна информация о применяемых ключевых параметрах конфигурации – имени почтового узла, почтовых доменах и доменах службы каталогов.

Применение конфигурации приведет к остановке обработки электронной почты на время развертывания конфигурации перезапуска компонентов всех экземпляров систем. Администратор предупреждается о временной недоступности системы при развертывании конфигурации.



При успешном развертывании конфигурации администратор системы видит подтверждение, и полученная конфигурация попадает в историю конфигураций в качестве активной. Если развертывание происходит в кластере, то на финальной странице администратор может увидеть статус развертывания конфигурации на отдельных узлах системы, нажав кнопку “Подробнее” в сообщении о развертывании на нескольких узлах.

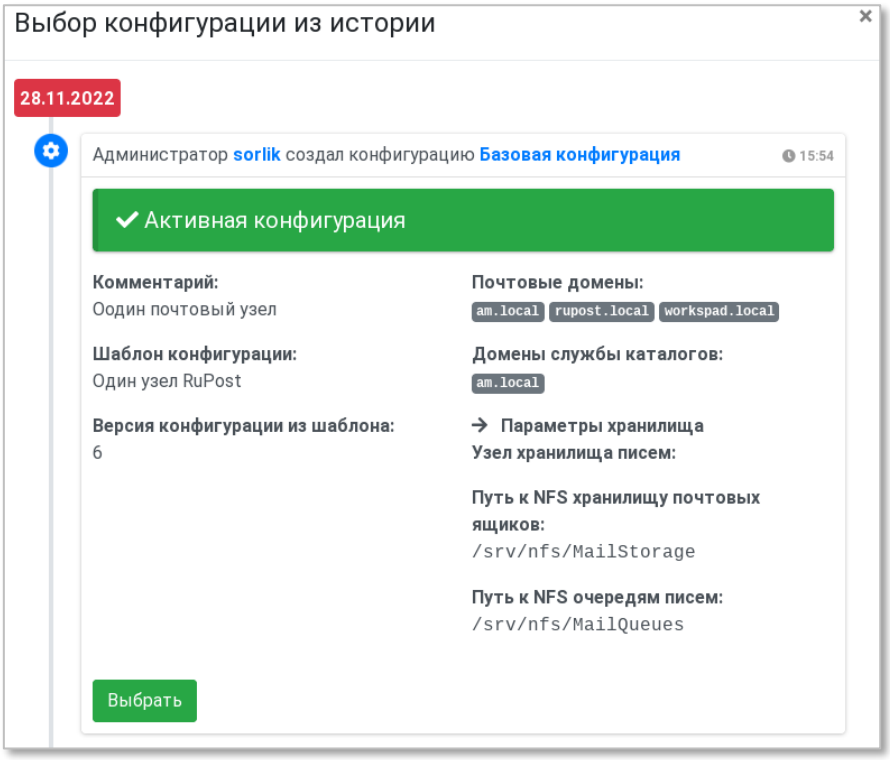


Развертывание новой конфигурации охватывает все узлы кластера, включая выведенные из эксплуатации узлы для поддержания целостности конфигурации кластера. Такие узлы также автоматически запускаются при успешном развертывании конфигурации.

На финальной странице статуса развертывания можно также заново запустить процесс создания новой конфигурации, при наличии такой необходимости.

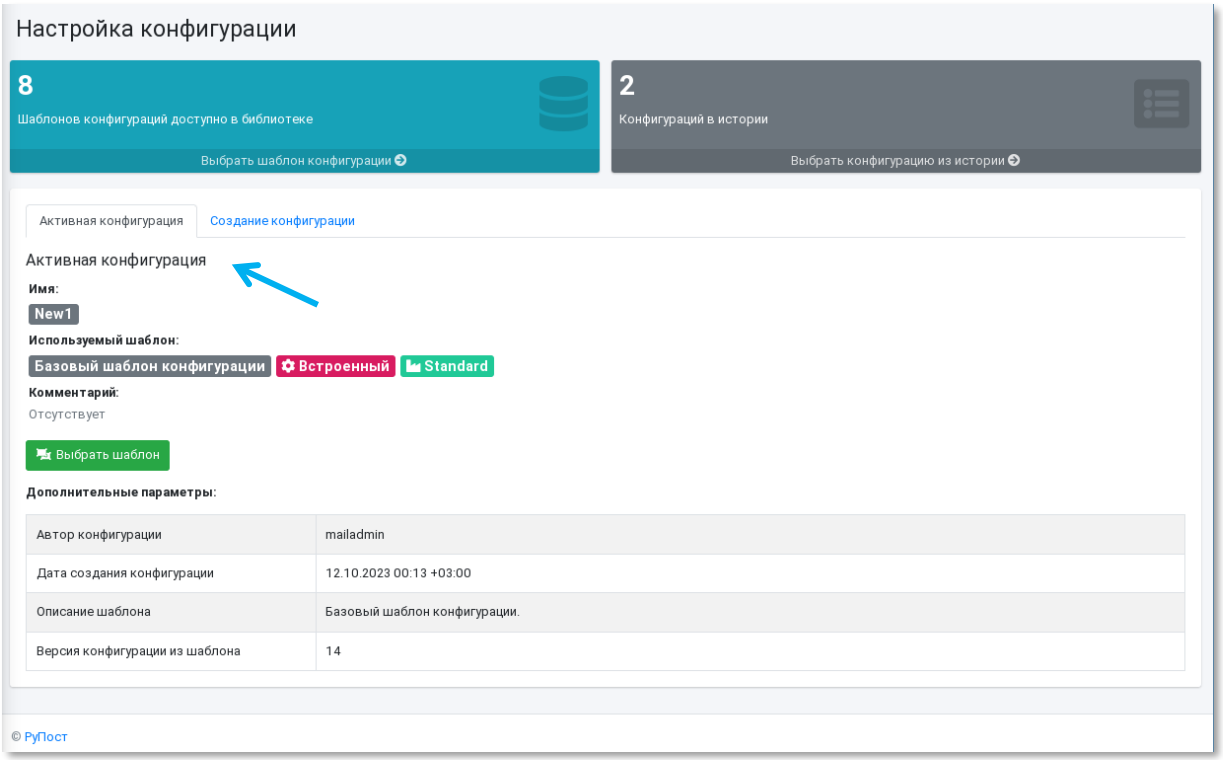
2.9.3. История конфигураций

История конфигураций позволяет не только просматривать успешные конфигурации, но и восстанавливать необходимую конфигурацию уже в контексте новых общесистемных параметров RuPost. В истории сохраняется также информация о том администраторе, который разворачивал конфигурацию.



2.9.4. Активная конфигурация

Активная конфигурация отображается как в истории конфигураций, так и на вкладке Активная конфигурация. Данная вкладка выбрана по умолчанию при переходе на страницу конфигурации.



2.10. Мониторинг системы, управление и самодиагностика компонентов

2.10.1. Общие принципы

RuPost включает внутренние механизмы проверки самодиагностики (HealthCheck) и обеспечивает встроенные базовые визуальные средства мониторинга системы и ее ключевых компонентов.

2.10.2. Контроль работы почтовых компонентов (Healthcheck)

В версии 2.7.0 для повышения надежности работы RuPost внесены изменения в схему работы процедур контроля работы почтовых компонентов (**healthcheck**). Система обеспечения надежности состоит из двух “контуров” постоянного мониторинга работы кластера RuPost:

- **Внешний** – обеспечивает проверку доступности портов почтовых компонентов данного узла, а также доступность служебного порта (32000) компонента HAProxy всех других узлов кластера. Проверка производится средствами HAProxy раз в 3 секунды. При обнаружении сбоя:
    a. запросы на подключение к сбойному узлу перенаправляются на другие узлы кластера;
    b. алгоритм балансировки IMAP подключений перераспределяет клиентов по другим узлам в соответствии с профилем нагрузки.
- **Внутренний** – обеспечивает проверку статусов работы почтовых компонентов данного узла и наличие ошибок в логах. При этом проверяются все компоненты узла кластера, включая HAProxy. Проверка производится раз в 30 секунд. При обнаружении сбоя в работе почтовых компонентов, делается три попытки перезагрузки с проверкой статусов. Если работоспособность после перезагрузок не восстановилась, то экземпляр выводится из эксплуатации.

В версии 2.7.0 добавлен автоматический перезапуск экземпляра RuPost после обнаружения сбоя в работе почтовых компонентов и автоматический старт RuPost при старте узла.

В случае обнаружения сбоя, делается три попытки перезапуска. После каждой попытки процедура **healthcheck** проверяет статус всех почтовых компонентов и, если функционирование восстановлено, то экземпляр больше не перезапускается. Если же после трех попыток перезапуска функциональность почтовых компонентов восстановить не удалось, то экземпляр выводится из эксплуатации. Все попытки перезарузки, как и финальный результат, записываются в лог-файл.

При старте узла происходит автоматический ввод в эксплуатацию сервера RuPost. При наличии мастер-конфигурации, при вводе в эксплуатацию происходит развертывание мастер-конфигурации на данном экземпляре RuPost.

В версии 4.3.4 добавлена CLI команда, позволяющая настроить периодичность и время выполнения ребалансировки пользователей по узлам кластера.

Для определения порядка работы процедуры ребалансировки пользователей, можно использовать CLI команду:

```
rupost set-kick-interval [--time] [--interval]
```

имеющую параметры:

- `--time` – время выполнения ребалансировки в формате hh:mm.
- `--interval` – интервал выполнения ребалансировки в днях.

Примеры:

```
rupost set-kick-interval --time 10:00 --interval 5
```

Устанавливает время ребалансировки (сброса IMAP-сессий) на 10 часов утра, интревал - каждые 5 дней.

```
rupost set-kick-interval --time 02:00
```

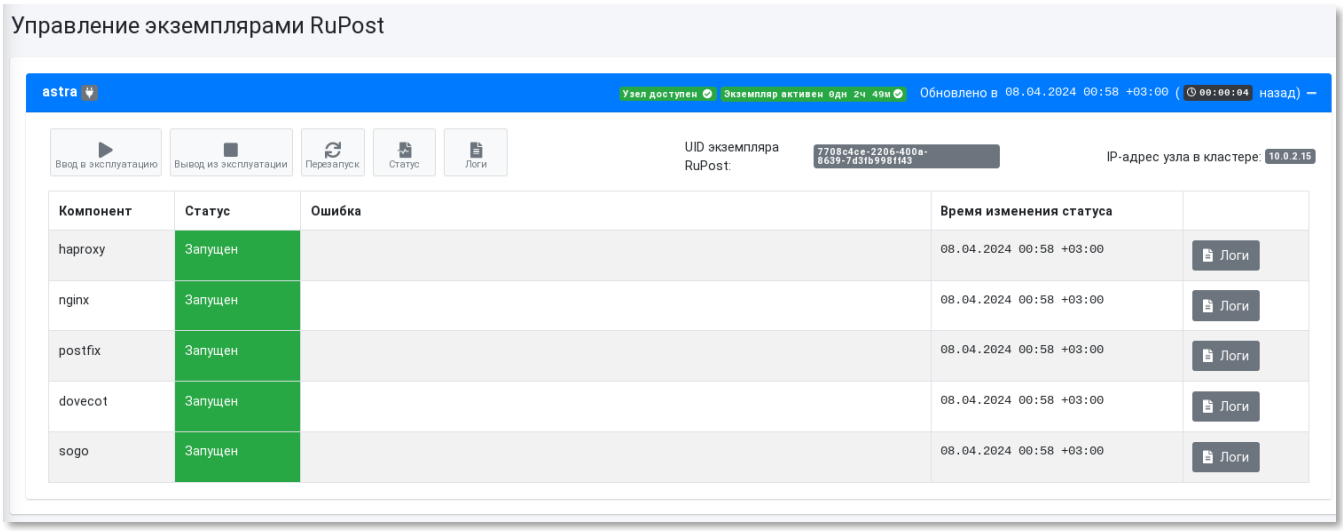
Установить время ребалансировки на 2 часа ночи, без изменения ранее установленного интервала.



Полный синтаксис команд и примеры их использования приведены в документе “Справочное руководство по командной строке”.

2.10.3. Управление и мониторинг работы кластера

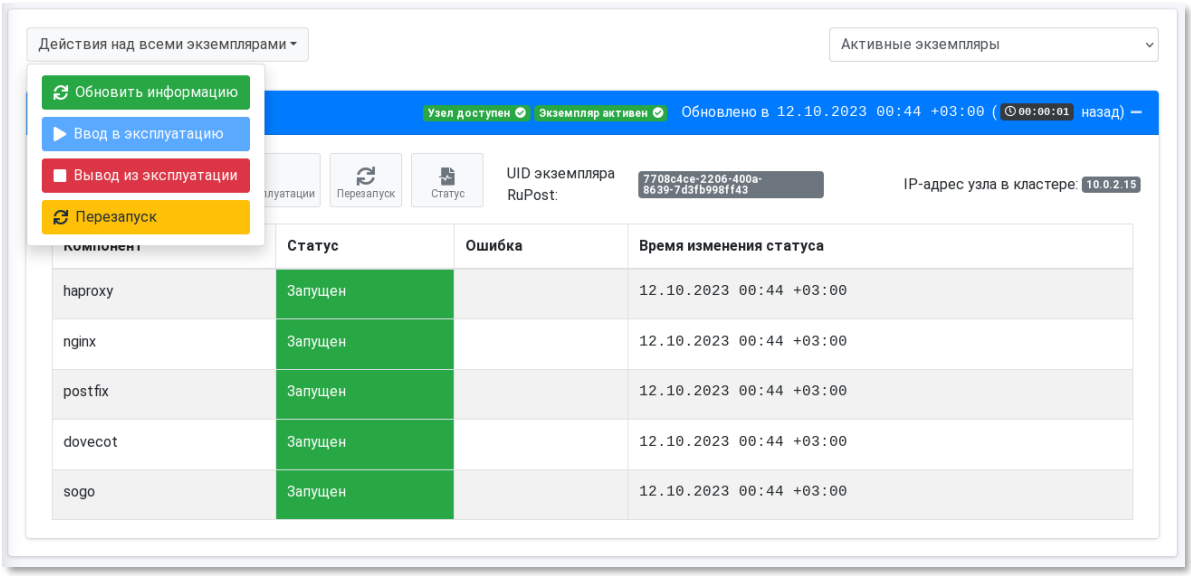
Страница “Экземпляры” позволяет отслеживать состояние всех узлов кластерных конфигураций RuPost (для старших редакций продукта).



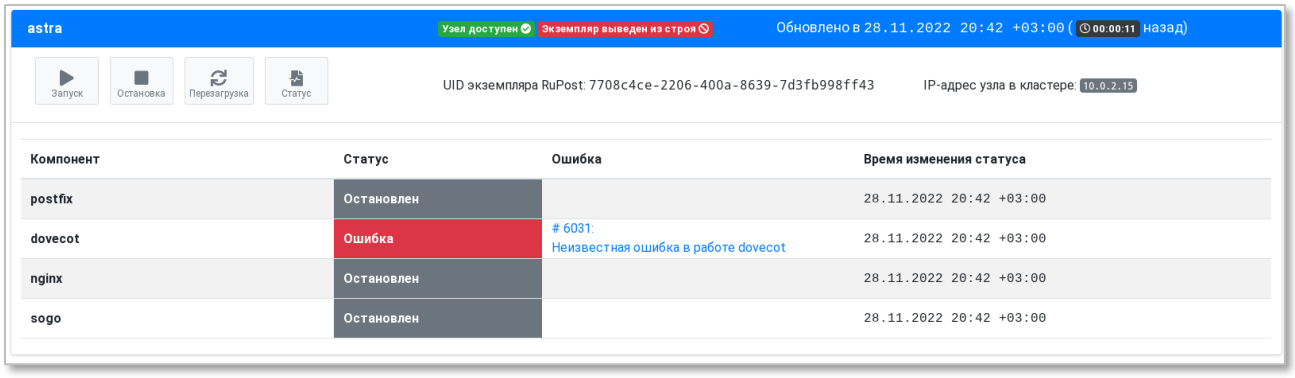
На странице управления экземплярами RuPost представлены инструменты остановки, запуска и перезапуска узлов, а также получения актуального статуса узла, который снимается автоматически при переходе на страницу мониторинга и может быть обновлен автоматически при перезагрузке страницы или выборе кнопки Статус.

Для удобства управления кластерной конфигурацией, на странице “Экземпляры” добавлены следующие функции:

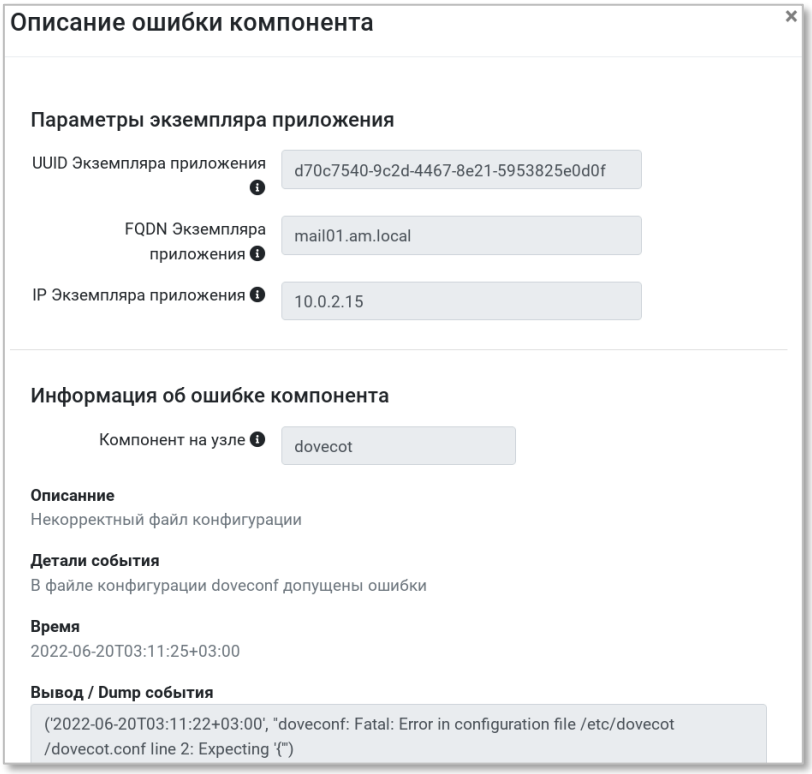
- Возможность выполнения операций над экземпляром RuPost без ожидания завершения предыдущей операции над другим экземпляром RuPost;
- Возможность выполнения операций “Вывод из эксплуатации” и “Ввод в эксплуатацию” для всех экземпляров одновременно;
- Фильтрация отображаемых экземпляров RuPost по статусам.



Каждый узел RuPost со всеми своими компонентами рассматривается как единое целое – все компоненты интегрированы между собой и их связь полностью управляется системой RuPost. В случае возникновения проблем на уровне того или иного компонента для обеспечения целостности системы автоматически отключает другие компоненты на узле (например, нерегламентированные некорректные изменения конфигурации отдельного компонента в обход системы управления).



При этом, панель управления позволяет получить всю диагностическую информацию из индивидуального журнала соответствующего компонента, который считывается системой управления RuPost. Для получения детальной информации об ошибке достаточно нажать на код и краткое описание ошибки.



Для устранения такого рода ошибки достаточно развернуть новую или последнюю успешную конфигурацию из истории конфигураций.

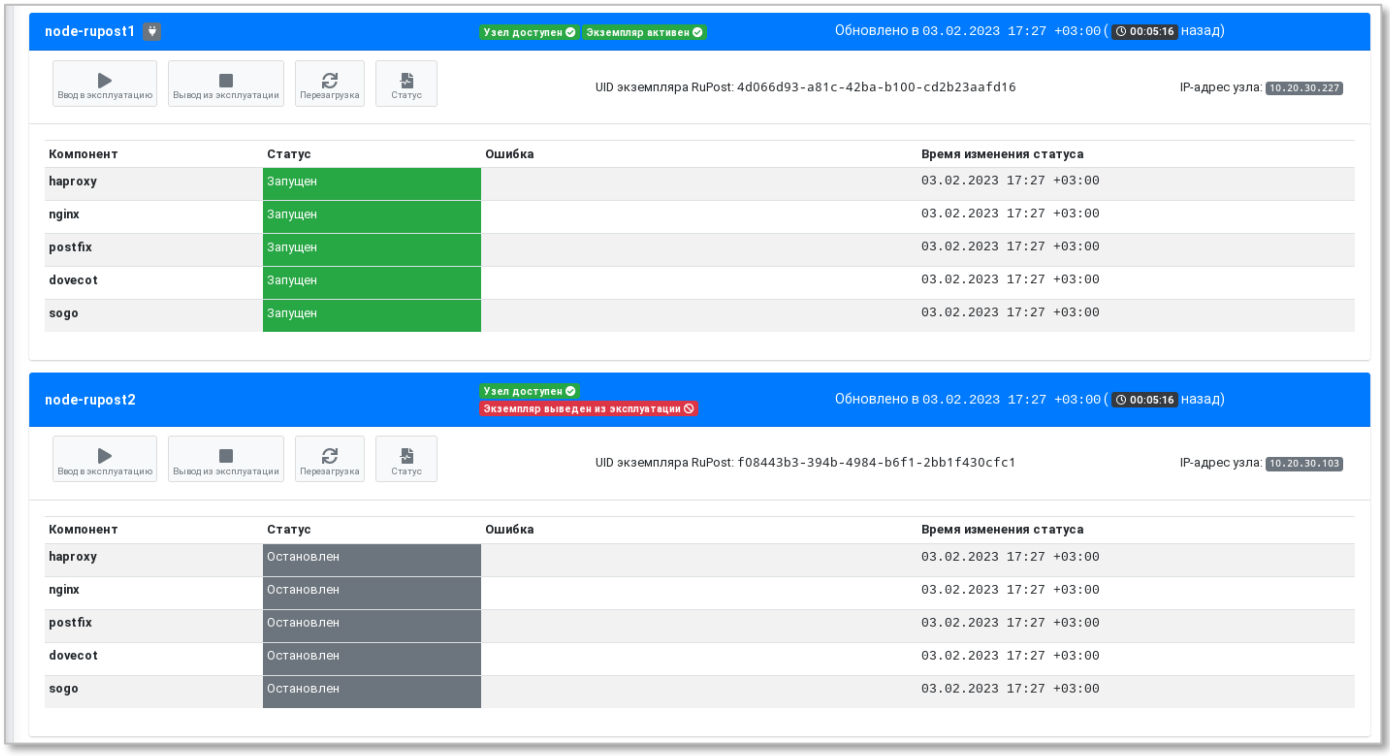
Внимание!

При развертывании кластера рекомендуется вначале установить только один узел системы, настроить необходимые параметры и развернуть на этом узле требуемую конфигурацию. Только убедившись в работоспособности выбранных инфраструктурных настроек и параметров системы приступайте к развертыванию и добавлению в кластер новых узлов системы.

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

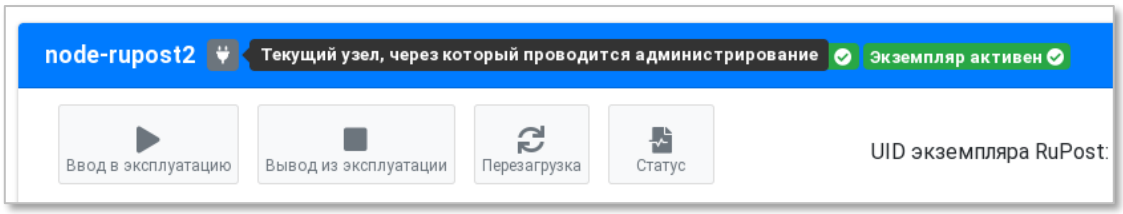
Добавление очередного узла в кластер состоит из двух шагов:

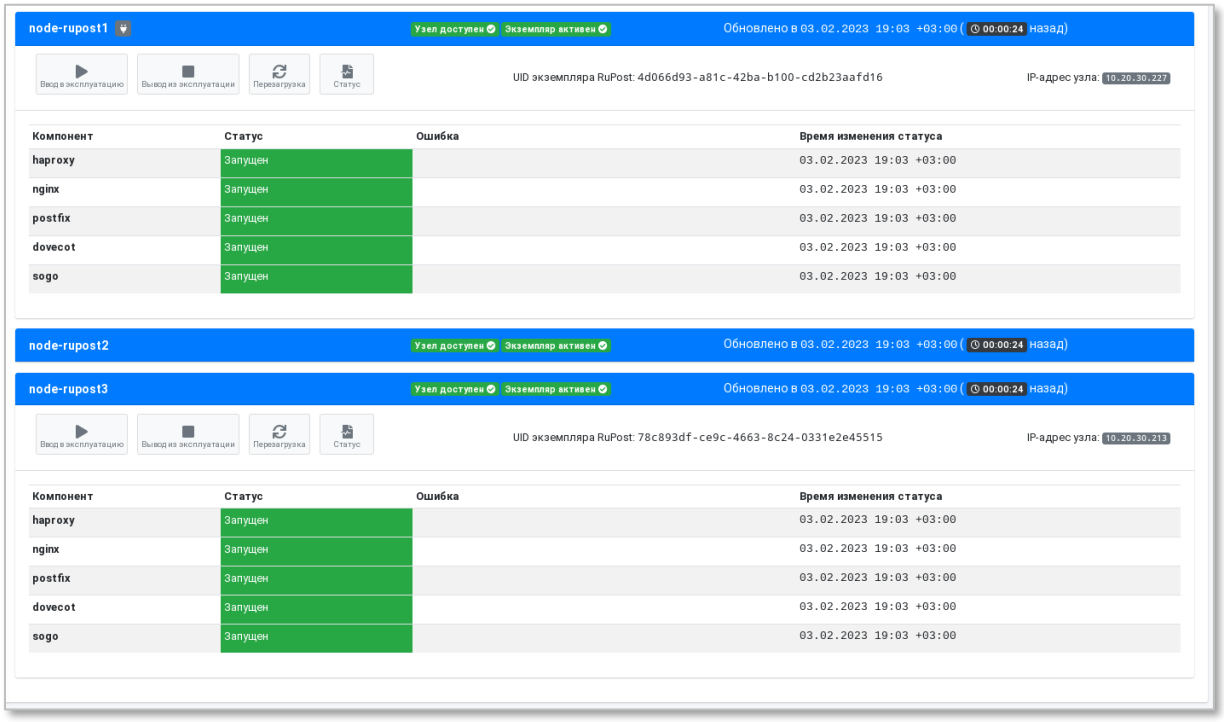
1. RuPost устанавливается на дополнительный узел мастером установки RuPost в интерактивном или командном режиме. В результате установки соответствующий экземпляр настроен на работу с общей базой данных, где хранятся все конфигурационные настройки. При этом сам экземпляр (“узел кластера”) автоматически не запускается.



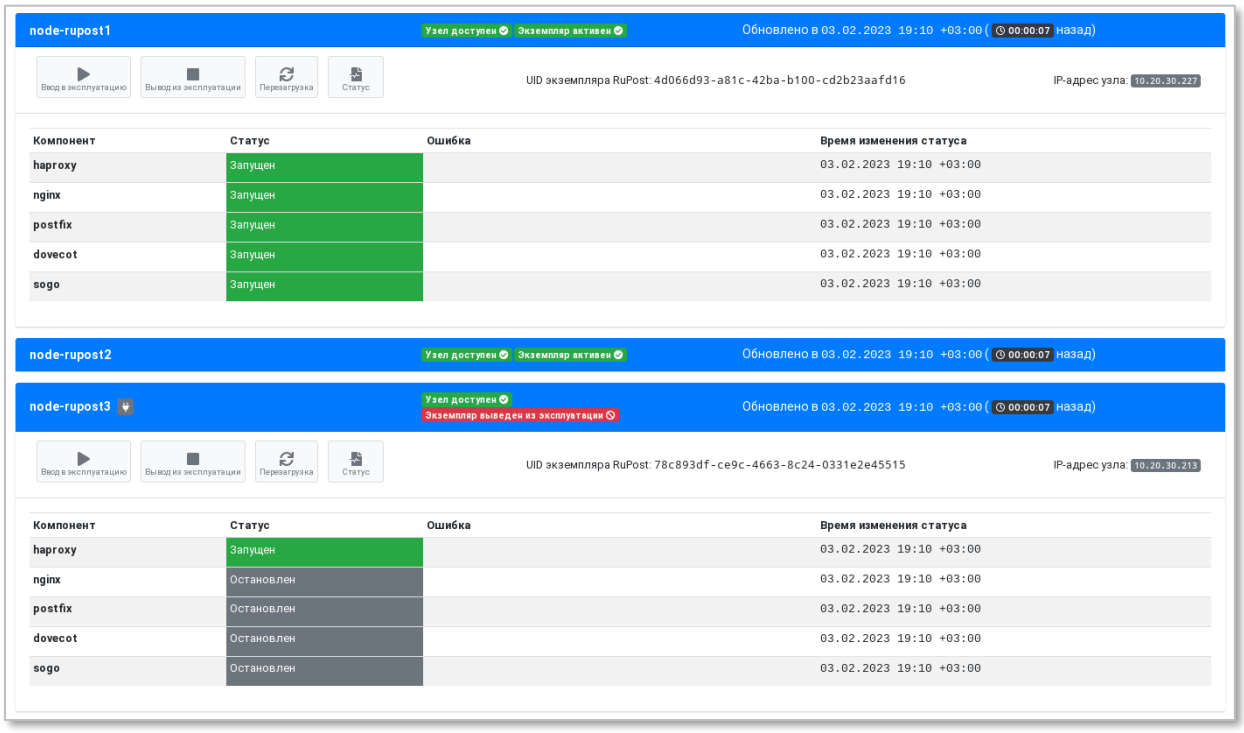
2. Администратор должен явно добавить экземпляр в кластер, нажав кнопку “Ввести в эксплуатацию” для необходимого узла в списке узлов на странице Мониторинг. При таком добавлении для экземпляра системы будет применена активная конфигурация, экземпляр будет запущен и на всех экземплярах системы будут обновлены настройки внутренних механизмов отказоустойчивости и мониторинга.

В пользовательском интерфейсе страницы мониторинга для удобства можно “сворачивать” те или иные узлы, нажимая на заголовок узла с именем экземпляра. А иконка “электрическая вилка” показывает через какой узел ведется работа в Панели управления в данный момент.

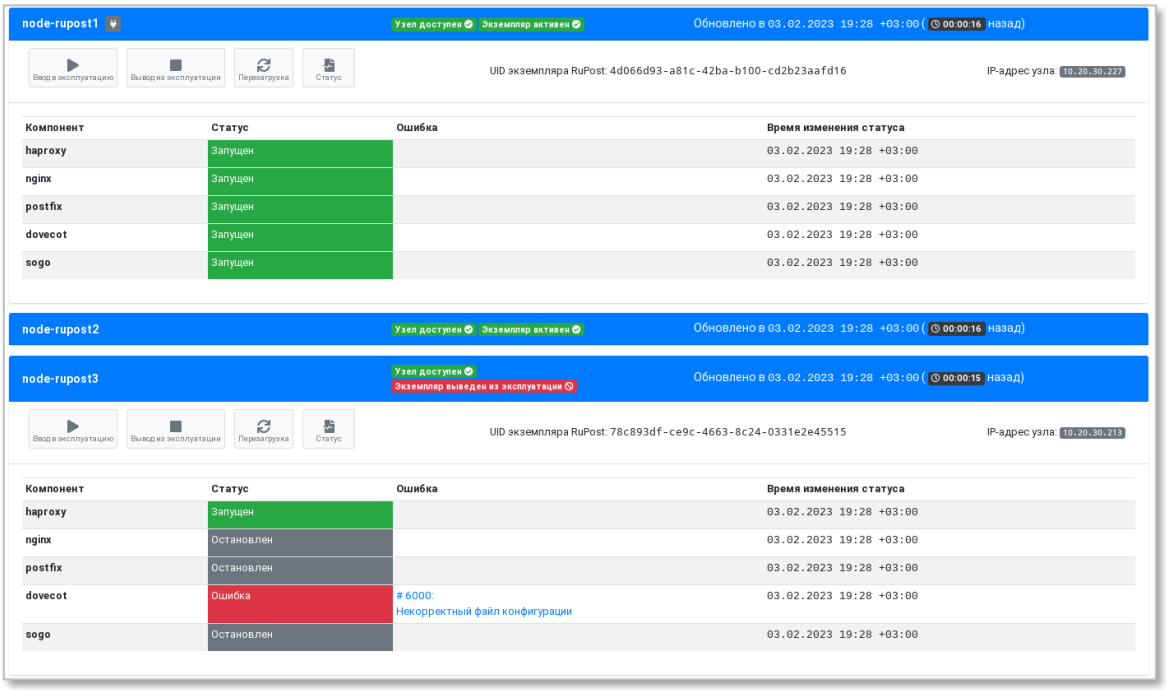




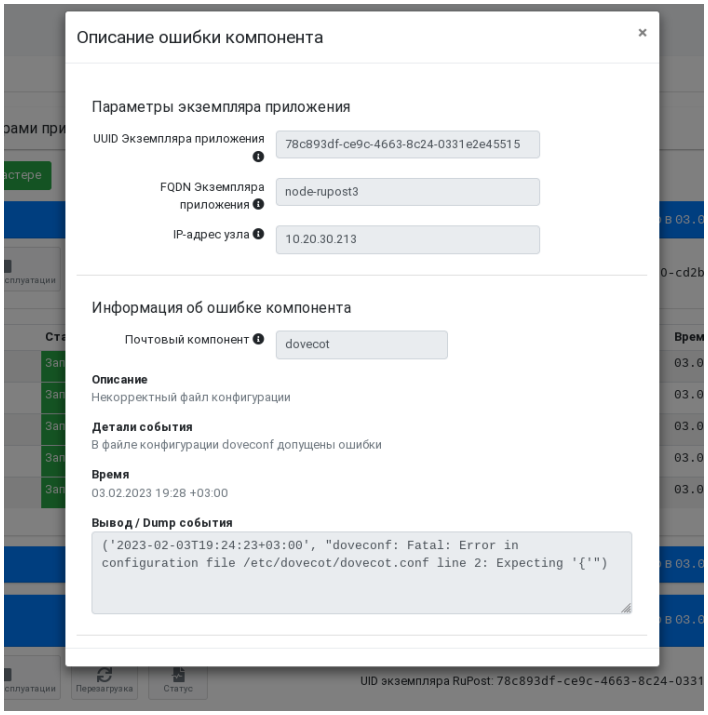
При выводе экземпляра из эксплуатации (как штатном, так и автоматически в результате возможных сбоев в том или ином почтовом компоненте системы) останавливаются только почтовые компоненты (postfix, dovecot, sogo) и web-сервер (nginx). Основной управляющий процесс RuPost и агент высокой доступности (HAProxy) не останавливаются, а статус узла обновляется во всех узлах системы как “выведенный из эксплуатации”.



При обнаружении сбоев почтовых компонентов экземпляра системы в кластере при старте/рестарте или в процессе работы – все почтовые компоненты останавливаются, узел остается доступным для мониторинга и управления, неотправленные почтовые сообщения из очереди сообщений автоматически эвакуируются на другой экземпляр системы, сбойный экземпляр выводится из эксплуатации, а информация об этом сохраняется в единой базе данных кластера.



Детальная информация об ошибке доступна при нажатии на сообщение об ошибке в списке компонентов.

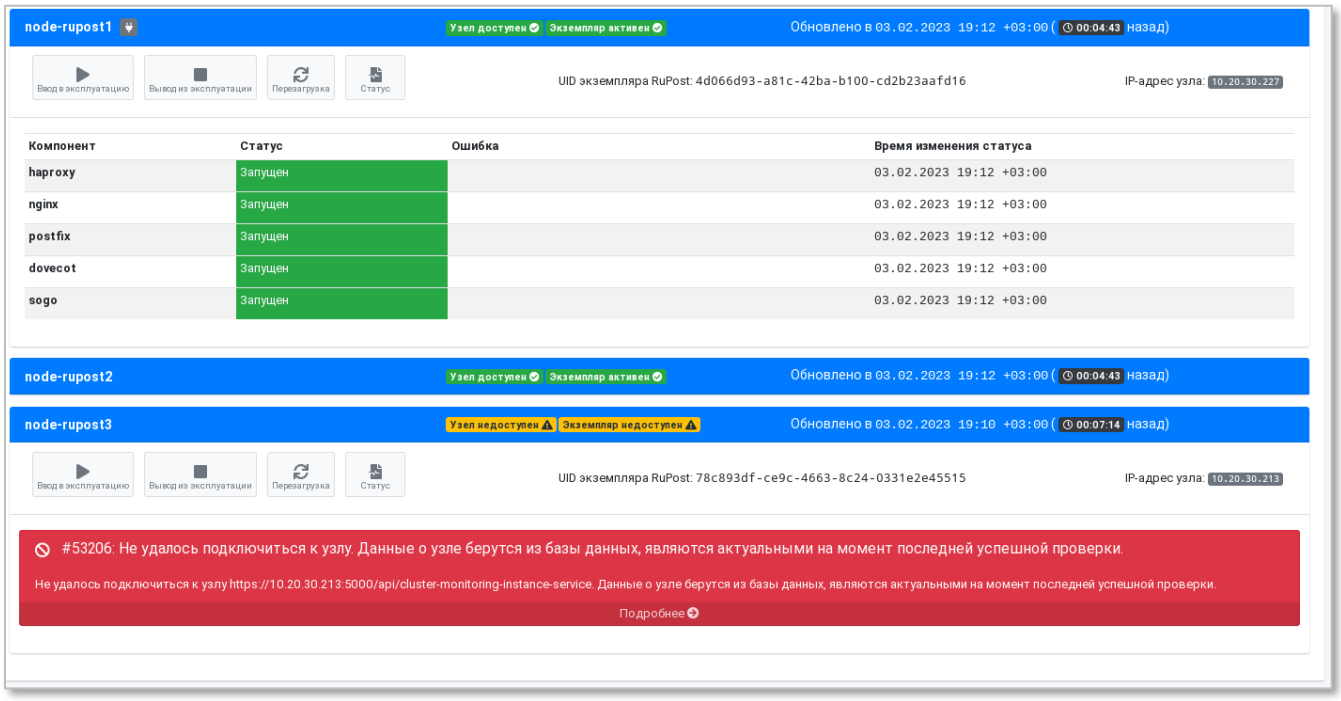


Данный вывод статуса HAProxy на узле демонстрирует самодиагностику объединённых в кластер узлов системы – на текущем узле почтовые компоненты остановлены, а автоматическая диагностика других экземпляров показывает их доступность и штатное функционирование. Конкретные детали можно запросить напрямую у узлов также на уровне системных команд.

```
root@node-rupost3:/etc/dovecot# systemctl status haproxy
• haproxy.service - HAProxy Load Balancer
   Loaded: loaded (/lib/systemd/system/haproxy.service; disabled; vendor preset: enabled)
   Active: active (running) since Fri 2023-02-03 20:23:05 MSK; 4s ago
     Docs: man:haproxy(1)
           file:/usr/share/doc/haproxy/configuration.txt.gz
  Process: 11006 ExecStartPre=/usr/sbin/haproxy -Ws -f $CONFIG -c -q $EXTRAOPTS (code=exited, status=0/SUCCESS)
 Main PID: 11008 (haproxy)
    Tasks: 3 (limit: 4596)
   Memory: 138.8M
   CGroup: /system.slice/haproxy.service
           ├─11008 /usr/sbin/haproxy -Ws -f /etc/haproxy/haproxy.cfg -p /run/haproxy.pid -S /run/haproxy-master.sock
           └─11010 /usr/sbin/haproxy -Ws -f /etc/haproxy/haproxy.cfg -p /run/haproxy.pid -S /run/haproxy-master.sock

фев 03 20:23:05 node-rupost3 haproxy[11010]: Server autoconfig/rupost78c893df-ce9c-4663-8c24-0331e2e45515 is DOWN via self-healthcheck/rupost78c893df-ce9c-4663-8c2
фев 03 20:23:05 node-rupost3 haproxy[11010]: Server sieve/rupost78c893df-ce9c-4663-8c24-0331e2e45515 is DOWN via self-healthcheck/rupost78c893df-ce9c-4663-8c24-033
фев 03 20:23:05 node-rupost3 haproxy[11010]: Server imap_mua/rupost78c893df-ce9c-4663-8c24-0331e2e45515 is DOWN via self-healthcheck/rupost78c893df-ce9c-4663-8c24-
фев 03 20:23:05 node-rupost3 haproxy[11010]: Server smtp_mua/rupost78c893df-ce9c-4663-8c24-0331e2e45515 is DOWN via self-healthcheck/rupost78c893df-ce9c-4663-8c24-
фев 03 20:23:05 node-rupost3 haproxy[11010]: Server smtp_mx/rupost78c893df-ce9c-4663-8c24-0331e2e45515 is DOWN via self-healthcheck/rupost78c893df-ce9c-4663-8c24-0
фев 03 20:23:06 node-rupost3 haproxy[11010]: 10.20.30.1:38738 [03/Feb/2023:20:23:06.014] smtp_mx smtp_mx/rupost4d066d93-a81c-42ba-b100-cd2b23aafd16 1/0/5 54 -- 1/1
фев 03 20:23:08 node-rupost3 haproxy[11008]: [WARNING]  (11010) : Health check for server cluster-healthcheck/rupost4d066d93-a81c-42ba-b100-cd2b23aafd16 succeeded,
фев 03 20:23:08 node-rupost3 haproxy[11010]: Health check for server cluster-healthcheck/rupost4d066d93-a81c-42ba-b100-cd2b23aafd16 succeeded, reason: Layer7 check
фев 03 20:23:09 node-rupost3 haproxy[11008]: [WARNING]  (11010) : Health check for server cluster-healthcheck/rupostf08443b3-394b-4984-b6f1-2bb1f430cfc1 succeeded,
фев 03 20:23:09 node-rupost3 haproxy[11010]: Health check for server cluster-healthcheck/rupostf08443b3-394b-4984-b6f1-2bb1f430cfc1 succeeded, reason: Layer7 check
```

При обнаружении сбоя отдельных почтовых компонентов рекомендуется повторно развернуть активную конфигурацию, выбрав ее из истории успешных конфигураций. При этом конфигурация будет развернута на всех экземплярах/всех узлах системы в кластерной конфигурации.

В случае остановки или сбоев в управляющем процессе RuPost узел и экземпляр в кластере помечаются как недоступные другими экземплярами системы, неотправленные почтовые сообщения из очереди сообщений автоматически эвакуируются на другой экземпляр системы, а информация об этом сохраняется в единой базе данных кластера.

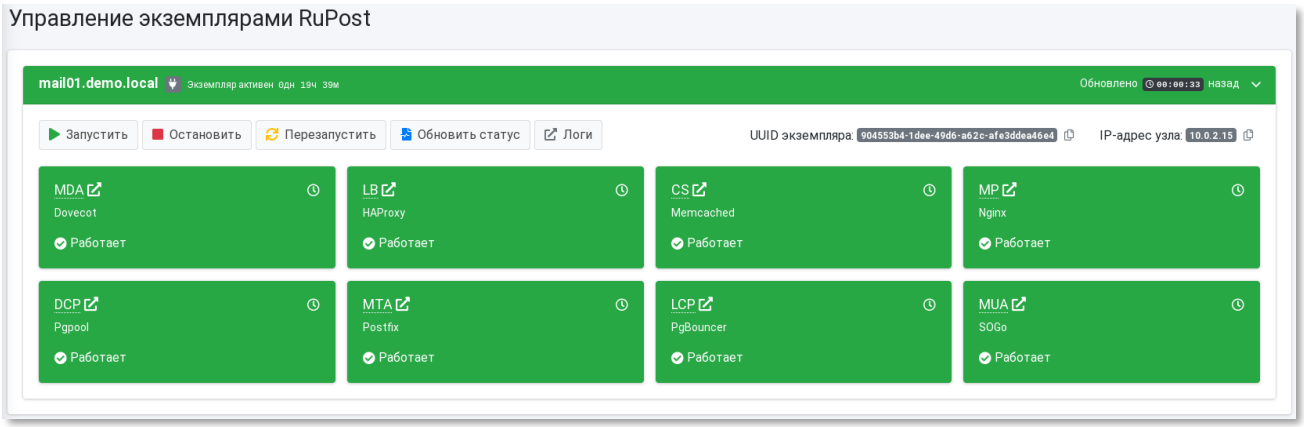


В версии 4.3.4 обновлен внешний вид страницы “Экземпляры”.

Расширен набор отображаемых компонентов – добавлены:

- **rupost-cs** (Memcached),
- **rupost-dcp** (PGPool),
- **rupost-lcp** (PGBouncer).

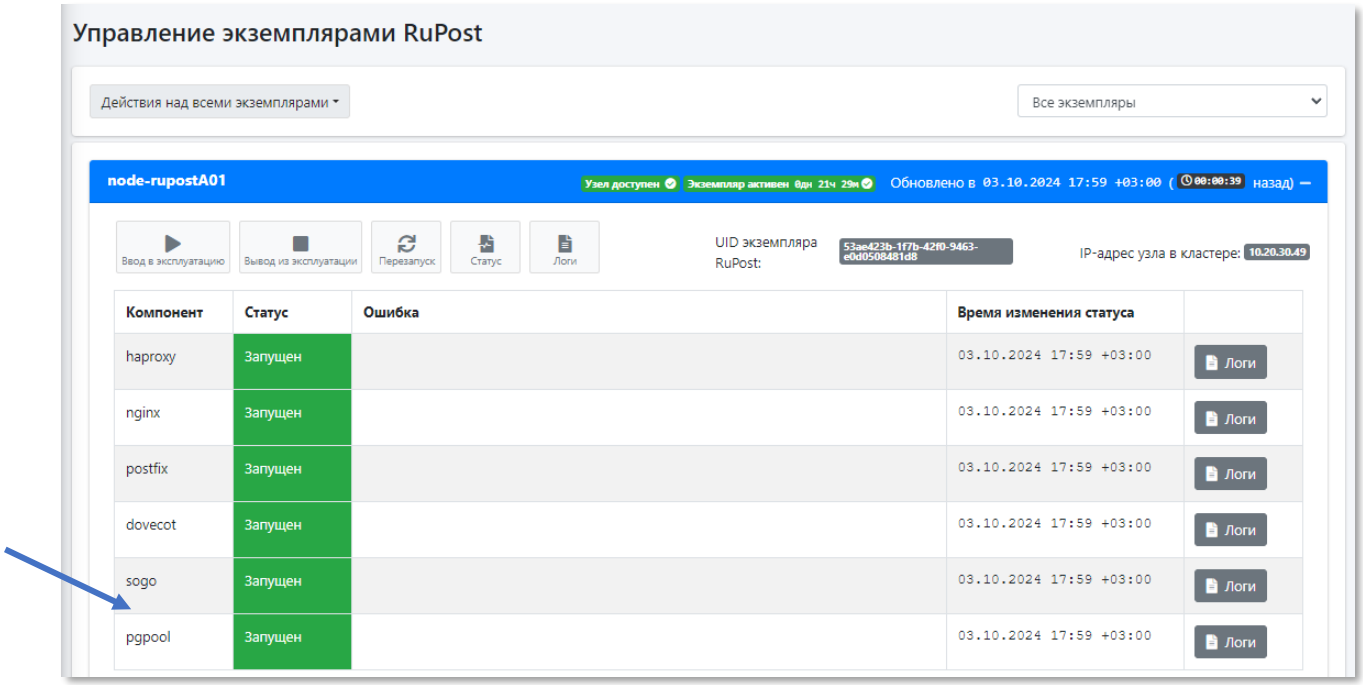
А также изменено расположение индикаторов статусов компонентов.



2.10.4. Пул соединений к базе данных

В версии 3.1.0 в состав компонентов RuPost добавлен компонент pgpool, обеспечивающий управление пулом соединений к базе данных и кеширование результатов запросов SoGo при работе с глобальной адресной книгой

Статус компонента pgpool отображается на странице “Экземпляры”:



В версии 4.3.4 в RuPost добавлен компонент rupost-lcp (PGBouncer).

Этот компонент используется для всех подключений почтовых компонентов к базе данных (кроме подключений rupost-mua к корпоративной адресной книге) и, таким образом, существенно снижает требования к серверу баз данных по максимально необходимому числу одновременных подключений.

2.10.4.1. *Контроль целостности конфигурационных файлов почтовых компонент*

В версии RuPost 2.2.1 добавлена возможность контроля нерегламентированного изменения конфигурационных файлов почтовых компонентов.

Конфигурационные файлы почтовых компонентов генерируются системой при развертывании конфигурации. Если пользователь с правами локального администратора системы (суперпользователя) изменяет конфигурационные файлы в обход штатных средств RuPost (панели управления или командного интерфейса), то это может привести к нарушению работоспособности системы. Постоянный контроль целостности конфигурационных файлов почтовых компонент позволяет администратору системы быть уверенным, что никакие изменения не были внесены в конфигурационные файлы через прямое редактирование файлов.

Контроль включает в себя два этапа:

1. Обнаружение изменений файла;
2. Корректирующие действия в соответствии с заданной стратегией реагирования.

Обнаружение изменений производится за счет постоянного мониторинга следующих каталогов/файлов:

- Каталог `/etc/postfix/ - *.cf` и файлы без расширения. Например, `main.cf` или `pgsql_alias_maps`;
- Каталог `/etc/dovecot - *.conf` и `*.conf.ext`. Например, `dovecot.conf` или `dovecot-acl.conf.ext`;
- Каталог `/etc/sogo - *.conf`. Например, `sogo.conf`;
- Каталог `/etc/default/ - *.conf` и `*.conf.ext`;
- Файл `/etc/default/sogo`;
- Каталог `/etc/nginx/ - *.conf`. Например, `nginx.conf`;
- Каталог `/etc/haproxy/ - *.cfg`. Например, `haproxy.cfg`.

В версии 4.3.4 следующие компоненты были перенесены в папку `/opt/rupost` в подпапки:

- **rupost-mua** (SOGo) – подпапка `mua`,
- **rupost-lcp** (PGBouncer) – подпапка `lcp`,
- **rupost-mp** (NGinx) – подпапка `mp`.

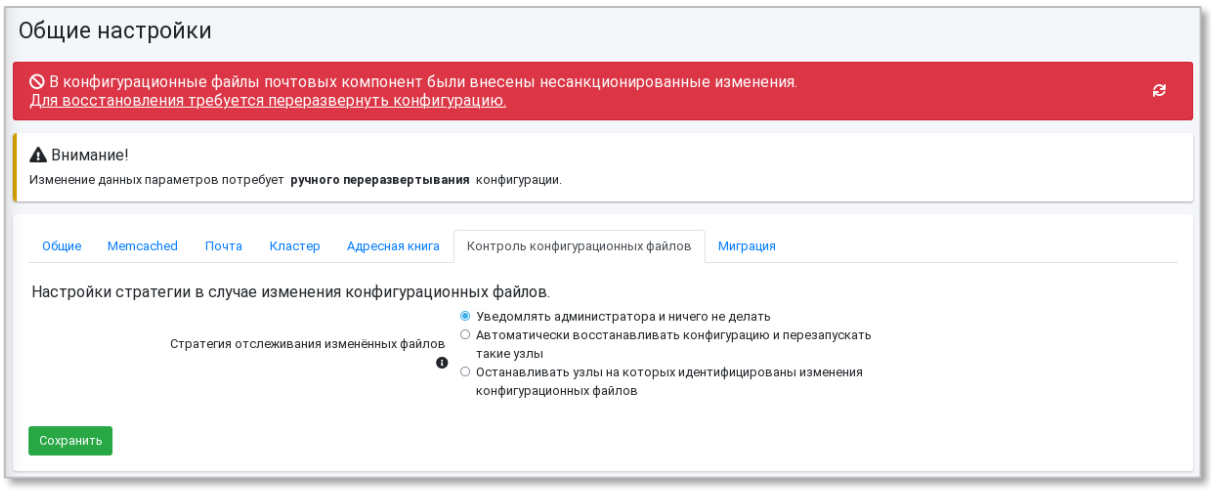
Соответственно, изменены пути мониторинга каталогов/файлов:

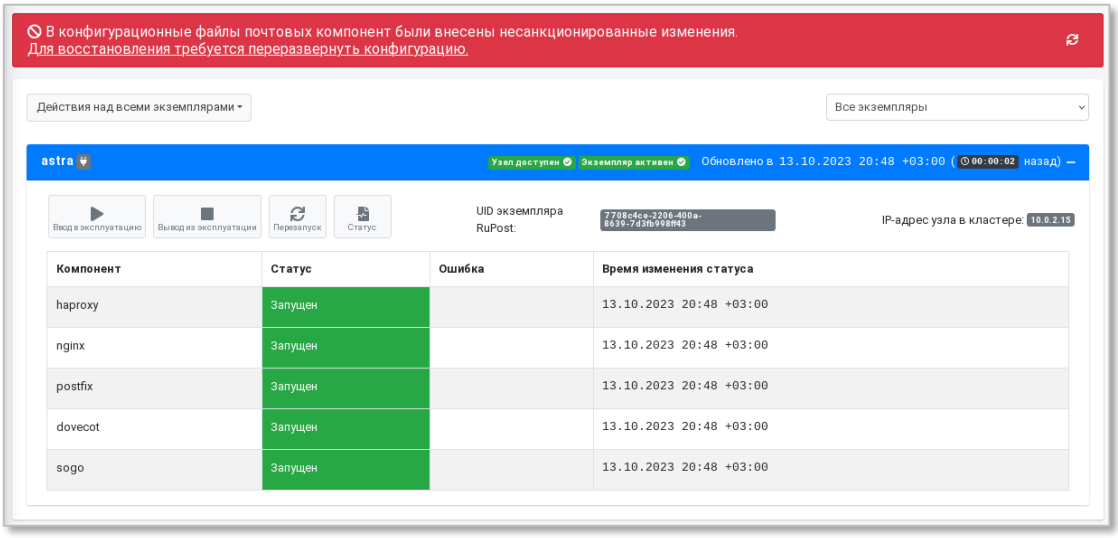
- Каталог `/etc/postfix/` - *.cf и файлы без расширения. Например, `main.cf` или `pgsql_alias_maps`;

- Каталог `/etc/dovecot/` - *.conf и *.conf.ext. Например, `dovecot.conf` или `dovecot-acl.conf.ext`;
- Каталог `/opt/rupost/mua/default` - файл, параметры конфигурации Sogo;
- Каталог `/opt/rupost/mua/` - *.conf. Например, `sogo.conf`;
- Файл `/opt/rupost/mp/nginx.conf`;
- Каталог `/opt/rupost/mp/conf.d`;
- Каталог `/etc/haproxy/` - *.cfg. Например, `haproxy.cfg`.
- Каталог `/opt/rupost/lcp/` - *.ini. Например, `pgbouncer.ini`;
- Каталог `/etc/pgpool2/` - *.conf. Например, `pgpool.conf`;

Для определения корректирующих действий после обнаружении изменений в разделе (вкладке) “Контроль конфигурационных файлов” страницы “Общие настройки” Панели управления можно определить стратегию реагирования на нерегламентированные изменения:

- **Оповещение** – опция *“Уведомлять администратора и ничего не делать”*. Система записывает в лог и визуально оповещает администратора о том, что внесены изменения в файл, но не предпринимает никаких дальнейших действий;
- **Восстановление файлов** – опция *“автоматически восстанавливать конфигурацию и перезапускать такие узлы”*. При обнаружении изменений в одном из файлов, система автоматически переразворачивает текущую почтовую конфигурацию, тем самым перезаписывая измененные файлы и перезапускает экземпляр.
- **Остановка узла** – опция *“Останавливать узлы на которых идентифицированы изменения конфигурационных файлов”*. Система останавливает экземпляр, на котором обнаружены изменения, записывает в лог информацию о событии и визуально оповещает администратора о том, что обнаружены изменения в конфигурационном файле и экземпляр остановлен;





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 связности кластера и целостности конфигурационных и пользовательских данных!

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

2.10.5. Работа с компонентами и узлами через командный интерфейс CLI

Командный интерфейс RuPost CLI предоставляет базовые средства получения статуса, перезапуска и остановки почтовых компонентов на конкретном узле или на всех узлах системы. В случае указания команды без дополнительных параметров работа будет вестись с тем экземпляром RuPost, который запущен на узле, где выполняется команда. Например, при отсутствии параметров при подключении к узлу в кластере доступны операции над компонентами данного узла. В случае использования соответствующих параметров можно оперировать разными узлами. Активный узел нельзя удалить - если необходимо удалить узел, то необходимо его сначала вывести из эксплуатации.

Внимание!

При применении команды `instances delete` **узел будет удален полностью, без возможности последующего восстановления.**

Синтаксис команды и примеры управления компонентами и узлами из командной строки приведены в разделе **«rupost components группа команд для управления почтовыми компонентами»** Справочного руководство по командной строке.

2.11. Пространства хранения, Группы ящиков и Хранилища

Для обеспечения сценариев высокой доступности RuPost, в версии 3.0 добавлены новые средства управления хранением почты – **Пространство хранения** (MailSpace), **Группа ящиков** (MailBox Group) и **Хранилище** (MailStore).

Пространство хранения (MailSpace) - совокупность нескольких хранилищ почты (MailStore), связанных правилами репликации. Минимально необходимо наличие хотя бы одного хранилища почты. Хранилища почты делятся по типам - одно из них является мастером (активное, обслуживает почту в данный момент), несколько хранилищ могут быть ведомыми (slave, "горячие" реплики мастер-хранилища) и, кроме того, может быть одно резервное (Backup, "холодная" реплика) хранилище. Состояние всех slave и backup хранилищ почты постоянно синхронизируется посредством периодической односторонней репликации в направлении мастер -> slave / backup. Slave хранилища почты считаются "горячими", т.е. при сбое на мастер-хранилище возможно переключение на slave.

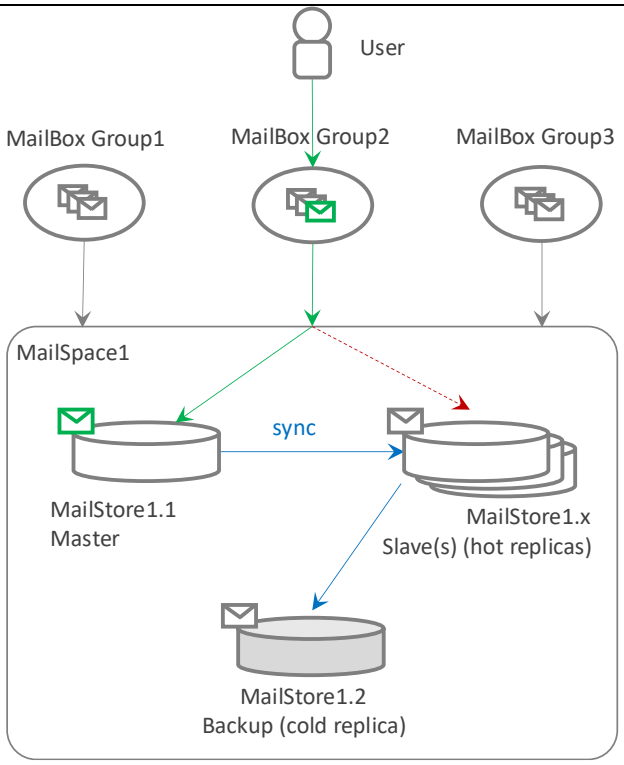
Группа ящиков (MailBox Group) - это набор почтовых ящиков, обслуживаемых одним Пространством хранения (MailSpace). Все ящики, входящие в одну Группу ящиков (MailBox Group) расположены в том Пространстве хранения (MailSpace), которое указано в свойствах этой Группы ящиков. Одно Пространство хранения может быть использовано для хранения нескольких Групп ящиков. Каждый Почтовый ящик (MailBox) принадлежит только одной Группе ящиков.

Хранилище почты (MailStore) - набор точек монтирования. Минимально необходимо наличие одной точки монтирования для хранения почтовых файлов в формате Maildir. В том случае, когда в Общих настройках системы установлено, что должны использоваться Архивы и/или Record Storage, то в свойствах хранилища должны быть указаны точки монтирования для Архивов и.или Record Storage соответственно. Точки монтирования являются уникальными для всех master и slave хранилищ всех Пространств хранения. Уникальность отслеживается по полному пути - адрес NFS сервера + имя папки.

Одним из параметров Slave хранилища является “Вес”. Этот параметр задает приоритет обработки Slave хранилищ – чем выше “вес” хранилища, тем больший приоритет оно имеет. Например, для того, чтобы снизить нагрузку на master хранилище, репликация на Backup хранилище производится со Slave хранилища, имеющего минимальный “вес”. Все Slave хранилища должны иметь отличающиеся значения свойства “вес”.

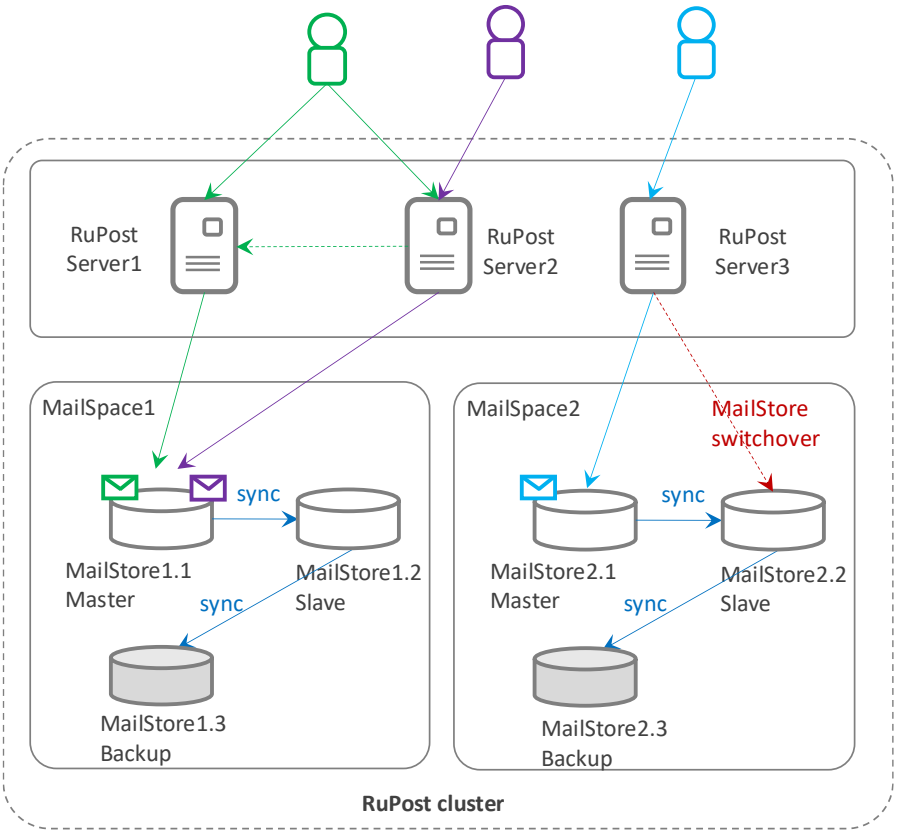
Резервное хранилище (Backup, "холодная" реплика). В пространство хранения может быть добавлено Backup-хранилище ("холодная" реплика), которое используется как источник данных для Системы резервного копирования (СРК). Периодичность синхронизации Backup-хранилища, в общем случае, имеет гораздо больший интервал (т.е. больше "отстает" от мастер-хранилища) чем у slave-хранилищ ("горячих" реплик). Backup-хранилище не может быть назначено мастером, т.е. на него нельзя переключить обслуживание почты.

Логические связи между сущностями, которыми оперирует новое поколение RuPost 3, отражены на диаграмме:



Настройка Групп почтовых ящиков, Пространств хранения и Хранилищ осуществляется как из Панели управления RuPost так и с помощью командного интерфейса (CLI).

Общая логика коммуникаций в кластере RuPost 3.0 представлена на диаграмме:



Уникальным преимуществом представленной архитектуры RuPost является возможность работы разных пользователей с почтовыми ящиками, размещенными в одном пространстве хранения, через разные узлы почтового кластера RuPost (серверы RuPost). Такой подход существенно повышает надежность работы кластера в целом и качественно оптимизирует нагрузку на отдельные серверы обработки почты в кластере – что повышает эффективность использования инфраструктурных ресурсов и производительность почтовой системы.

Ниже представлен рекомендуемый пример организации структуры каталогов для пространства хранения.

Мастер-хранилище почты MailStore (каталог **master**), "горячая" реплика мастер-хранилища (каталог **replica**) и "холодная" реплика мастер-хранилища для системы резервного копирования (каталог **backup**). Каталоги **queuesprim** и **queuessec** используются для почтовых очередей**.** В каталог **archives** перемещаются сообщения электронной почты, предназначенные для длительного хранения. В каталог **recordstorage** перемещаются удаленные пользователем почтовые сообщения.

```
/srv/
└── nfs
    └── strg
        ├── backup
        │   ├── archives
        │   ├── mail
        │   └── recordstorage
        ├── master
        │   ├── archives
        │   ├── mail
        │   └── recordstorage
        ├── queuesprim
        ├── queuessec
        └── replica
            ├── archives
            ├── mail
            └── recordstorage
```

Внимание!

При первичном создании хранилищ с назначением «Архив» и скрытой копии «RecordStorage» тип хранилища следует оставить slave. Перед созданием выполняется проверка и, в случае отсутствия хранилища с данным назначением и типом «мастер», вновь создаваемому хранилищу будет назначен тип «мастер».

Внимание!

В версии RuPost 4.0.0 мастер хранилище, архив и скрытая копия RecordStorage реализованы в виде отдельных самостоятельных хранилищ, раздел 2.8.1 «Рекомендации по настройке сетевых файловых хранилищ».

Внимание!

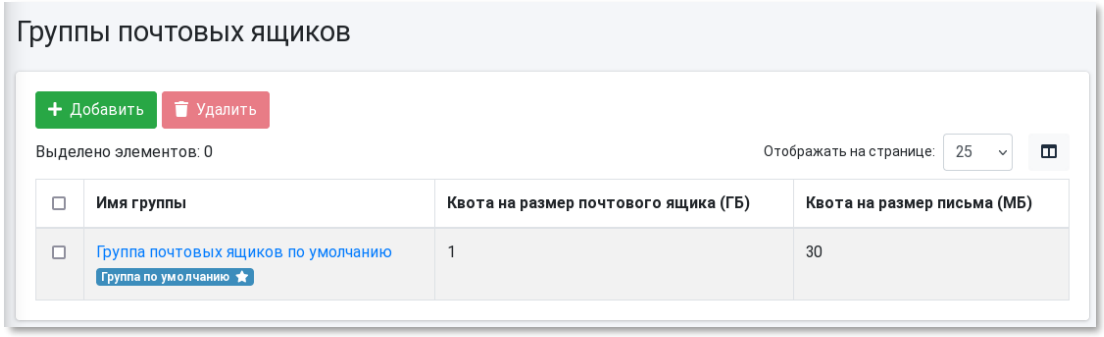
При выполнении удаления хранилища из графического интерфейса администратора RuPost происходит только размонтирование точки хранения.

Данные почтовых ящиков, структура каталогов MailDir не удаляются!

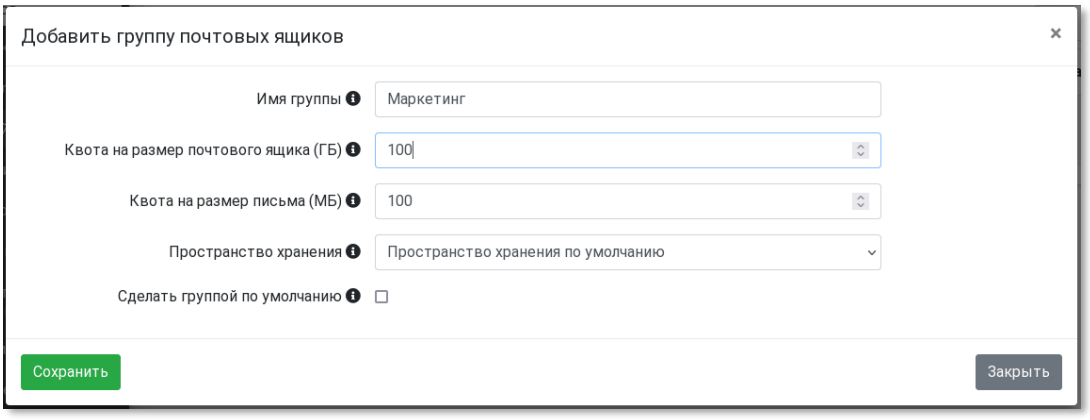
Для полного удаления данных необходимо вручную удалить их в соответствующем каталоге точки монтирования NFS.

2.11.1. Управление Группами почтовых ящиков

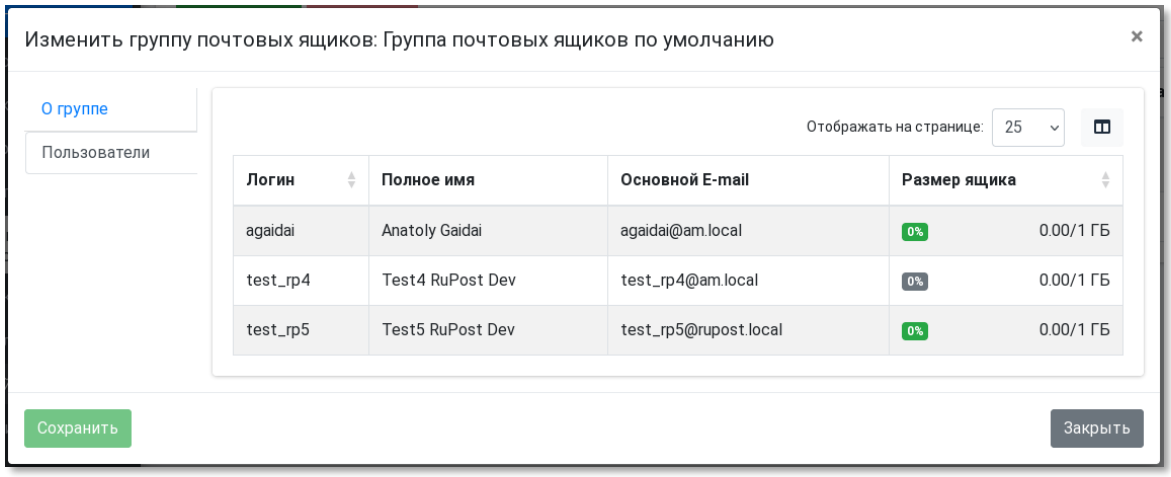
Список всех Групп ящиков с указанием квот на размер почтового ящика и размер письма отображается на странице “Группы почтовых ящиков”:



Добавления Группы ящиков осуществляется по кнопке “Добавить”:



Окно свойств Группы ящиков позволяет задать значения квот, которые будут использованы как значения по умолчанию для добавляемых в Группу почтовых ящиков. Здесь же выбирается в каком Пространстве хранения будут храниться почтовые ящики, входящие в эту группу.
Список ящиков, которые находятся в Группе, показан на закладке “Пользователи”:

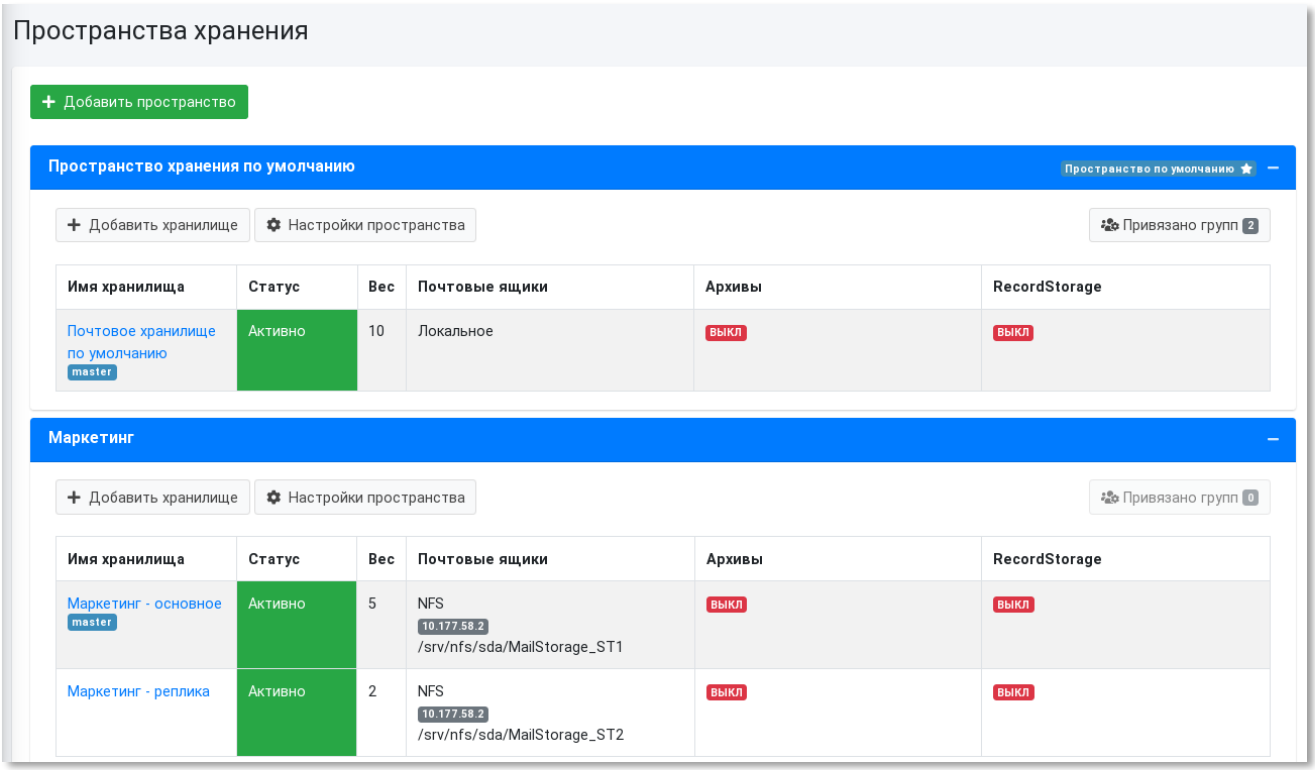


Управление правами доступа к странице “Группы почтовых ящиков” производится через редактирование разрешений полномочий администраторов.

Изменения в версии 3.1
Обратите внимание – в связи с добавлением Групповых политик квотирования, в версии 3.1 изменена структура управления квотами. Квоты на размер ящика и размер входящего письма теперь задаются в свойствах Групповых политик квотирования, а не в свойствах Группы ящиков.

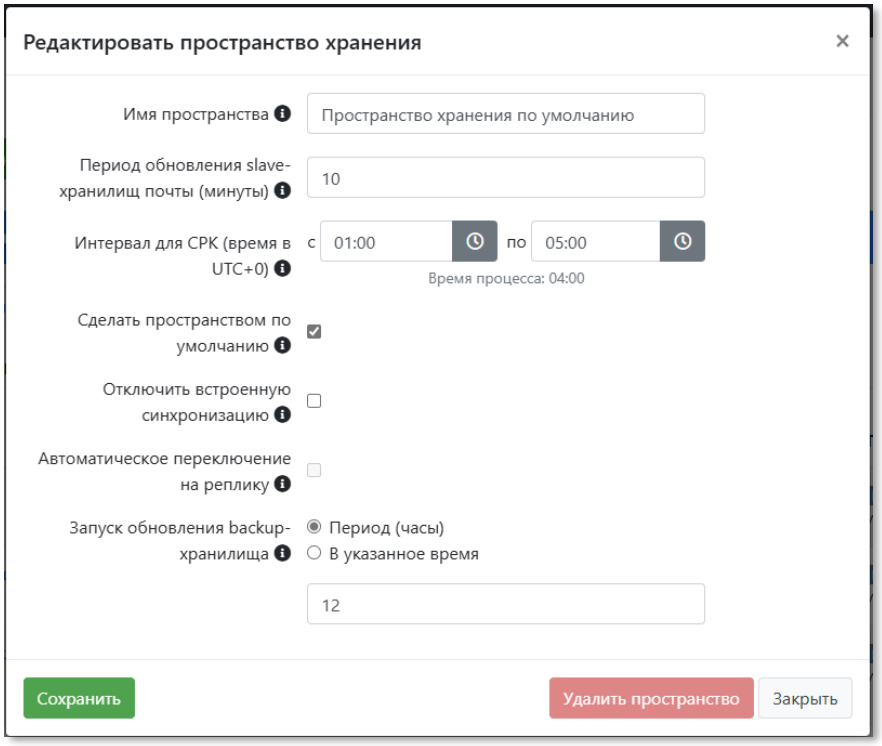
2.11.2. Управление Пространствами хранения и Хранилищами

На странице “Пространства хранения” осуществляется управление не только собственно Пространствами хранения, но и Хранилищами, входящими в каждое Пространство хранения.



В таблице отображаются все Пространства хранения и их Хранилища. По каждому Хранилищу отображается его статус, точки монтирования, а также индикатор, показывающий является ли данное Хранилище основным (master) в Пространстве хранения.

Добавить новое Пространство хранения можно по кнопке “Добавить Пространство”, а отредактировать его свойства можно по кнопке “Настройки Пространства”.



В окне свойств, кроме названия Пространства, указываются параметры, управляющие репликацией “горячих” и “холодной” реплик.

Начиная с версии 4.0.0 добавлена возможность указания времени начала создания «холодной реплики. Если требуется запустить обновления backup хранилища в реальном времени немедленно, то к текущему времени необходимо добавить 12 минут.

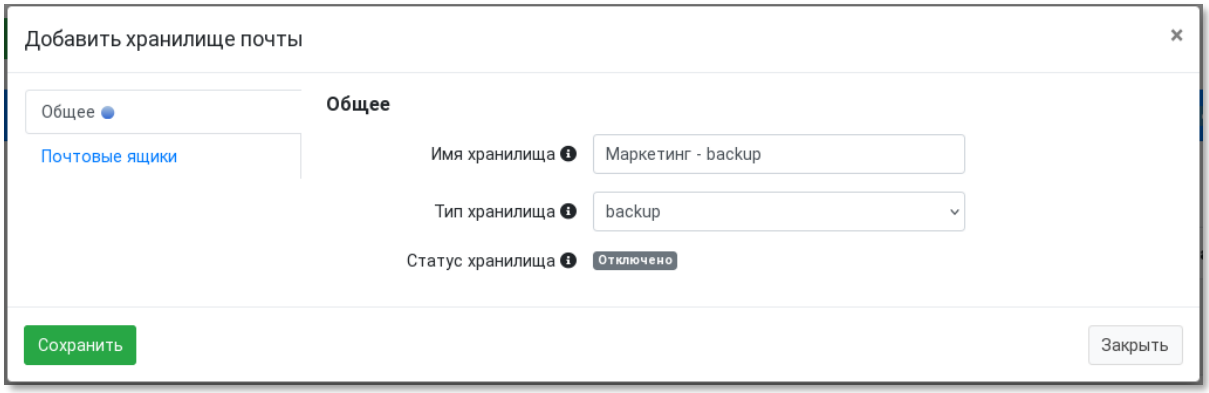
Внимание!

При добавлении в пространство хранения хранилища с типом slave немедленно начнётся полная репликация данных из хранилища типа master! В связи с этим, внимательно планируйте время подключения дополнительного хранилища, избегая наиболее нагруженных часов дня.

Однако, при включенной настройке пространства «Включить внешнюю синхронизацию» репликация между хранилищами встроенными средствами RuPost не выполняется, в связи с чем, добавление нового хранилища не приведёт к возможной перегрузке канала доступа к подключаемым удалённым файловым системам.

Опция “Использовать внешнюю репликацию” применяется в ситуации, когда репликация данных между master и slave осуществляется средствами СХД и, соответственно, репликация RuPost, в данной конфигурации, не применяется.

Добавление нового Хранилища в Пространство хранения осуществляется по кнопке “Добавить хранилище”.



В окне свойств Хранилища указывается его тип – Slave или Backup – а также набор точек монтирования (с учетом опций “Архивы” и “Record Storage” в “Общих настройках”).

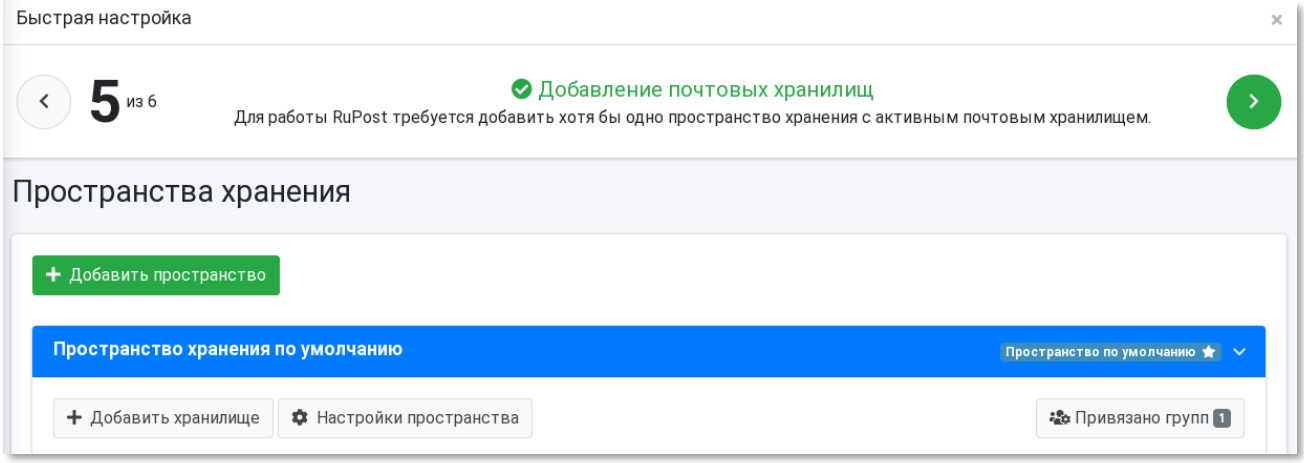
После добавления нового хранилища, так как его точки подключения еще не смонтированы, отображается статус “Подключение”.

Хранилище становится активным (статус “Активно”) только тогда, когда все его точки монтирования успешно смонтированы хотя бы на одном активном узле кластера RuPost. Каждый узел RuPost осуществляет периодическую проверку всех точек монтирования и, если хранилище не смонтировано, хотя бы на одном узле, то Хранилищу устанавливается статус “Ошибка”. Этот же сервис монтирует точки подключения новых Хранилищ.

При необходимости (например, для проведения профилактических работ), Хранилище можно отключить по кнопке “Отключить хранилище”. Основное (master) Хранилище отключить нельзя, сначала нужно назначить основным другое Slave хранилище. Это можно сделать по кнопке “Сделать мастером”. Управление правами доступа к странице “Пространства хранения” производится через редактирование разрешений полномочий администраторов.

2.11.2.1. *Быстрая настройка – выбор типа хранилища*

В версии 4.1.0 автоматическое добавление локального хранилища “по умолчанию” заменено на добавление хранилища нужного типа на шаге “быстрой настройки”.



Таким образом, администратор имеет возможность, при необходимости, сконфигурировать хранилища NFS без промежуточного удаления локального хранилища, созданного при установке.

2.11.2.2. *Удаление пространства хранения*

При возникновении необходимости удаление пространства хранения вместе с его хранилищем может быть выполнено из графического интерфейса администратора RuPost.

Внимание!

Для удаления пространство хранения, необходимо, что бы с ним не было связанных групп почтовых ящиков.

2.11.3. Периодическая очистка хранилища записей (RecordStorage)

В версии 4.1.0 добавлена возможность удаления старых записей из хранилища записей (RecordStorage).

Удаление писем из хранилища записей производится один раз в сутки (в 02:15). После установки версии 4.1.0, по умолчанию, очистка хранилища записей отключена.

Для включения очистки хранилища записей, необходимо с помощью команды CLI настроить интервал времени очистки (в месяцах – от 1 до 36).

Например, для очистки записей старше 12-ти месяцев:

```
sudo rupost group-policy set-clean-records --aging-period 12
```

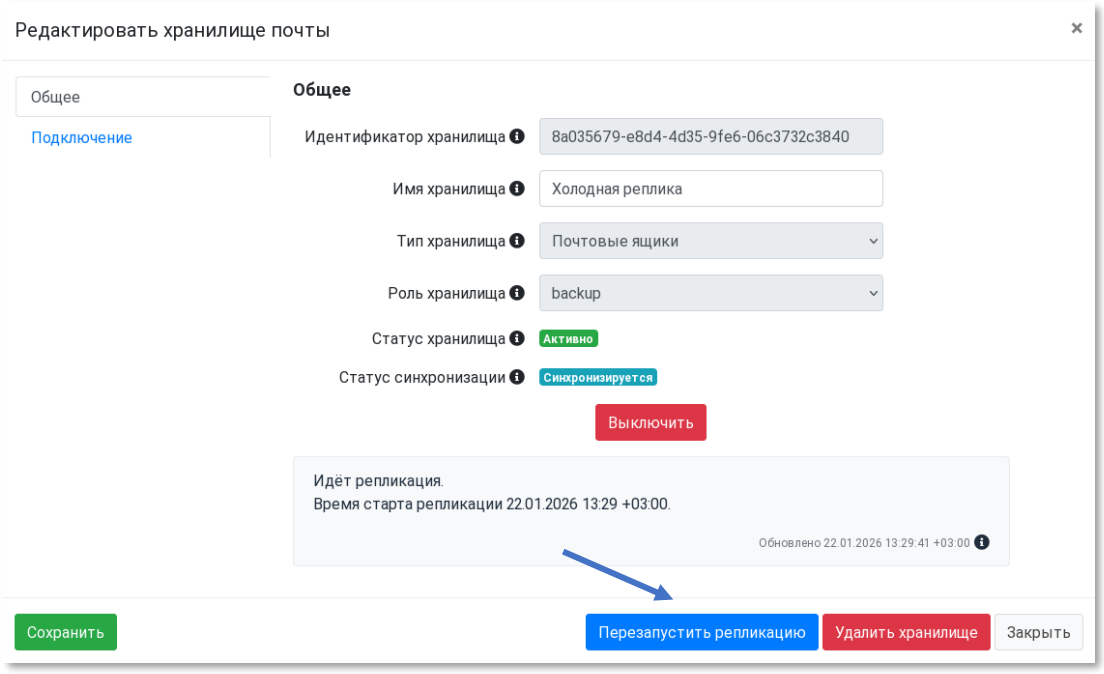
Полный синтаксис команд и примеры их использования приведены в разделе **«rupost group-policy – Группа команд для работы с групповыми политиками»** Справочного руководство по командной строке.

Записи, имеющие время создания, отстоящее от текущей даты на время большее выбранного интервала, будут удалены.

2.11.4. Возможность перезапуска репликации холодной (backup) реплики

В версии 4.1.0 добавлена возможность перезапуска репликации реплики backup.

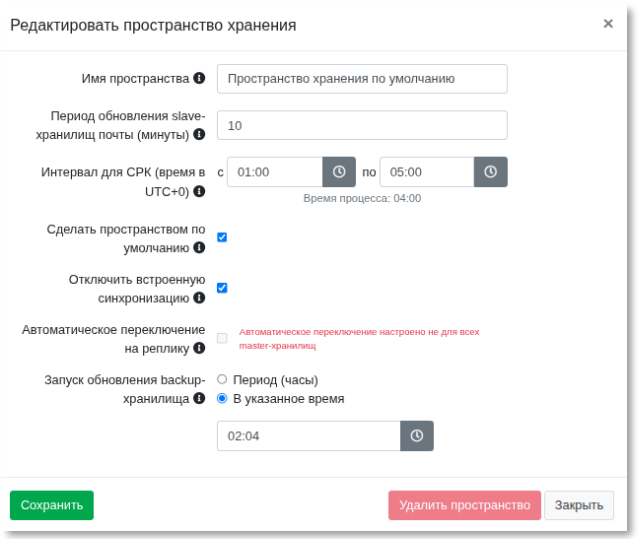
Для того, чтобы перезапустить репликацию, нужно в окне свойств соответствующего хранилища нажать кнопку “Перезапустить репликацию”.



2.11.5. Настройка времени запуска холодной (backup) реплики

В версии 4.0 добавлена возможность установить время создания “холодной” реплики.

Для того, чтобы указать время суток, когда должно начинаться копирование данных на “холодную” реплику, в окне “Пространства хранения” откройте свойства нужного хранилища и выберите период или укажите время.



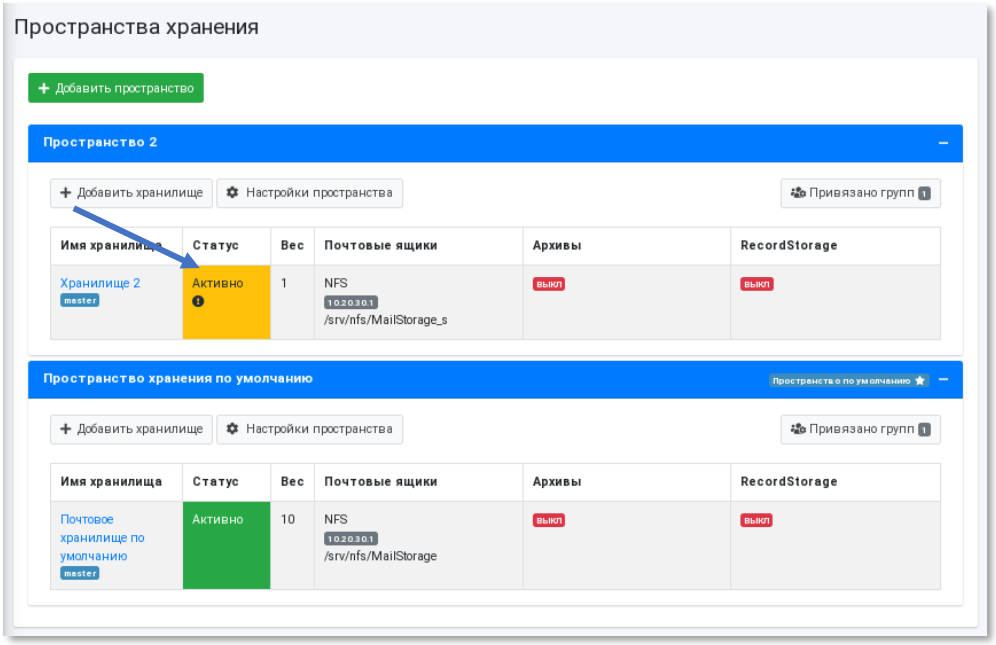
Если указано конкретное время, то репликация будет запускаться только один раз в сутки в указанное время.

2.11.6. Работа хранилища при монтировании на части узлов кластера

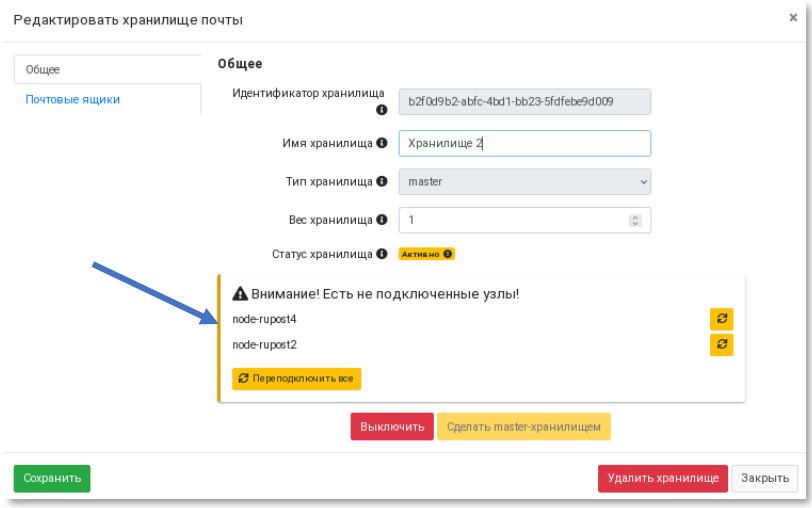
В версии 3.1.0 для повышения отказоустойчивости кластера RuPost расширены возможности подключения хранилищ (MailStore) к узлам кластера – хранилище продолжает работу, даже если оно не доступно на части узлов кластера.

Индикатор статуса хранилища имеет следующие значения:

- Хранилище подключается;
- Хранилище подключено к части узлов кластера (минимум – один узел);
- Хранилище подключено ко всем узлам кластера;
- Хранилище отключено - не подключено ни к одному узлу кластера.

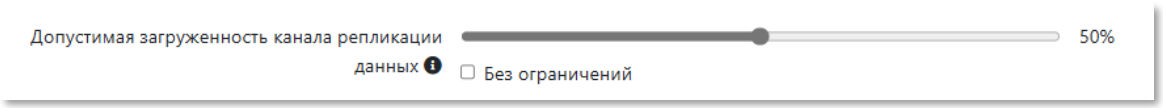


Очевидно, что максимальная эффективность использования хранилища достигается тогда, когда оно подключено ко всем узлам кластера – поэтому, для того чтобы администратор мог определить на каких узлах кластера не удалось подключить хранилище, при клике на статус хранилища отображается список узлов, к которым данное хранилище не подключено.



2.11.7. Оптимизация алгоритма репликации хранилищ

В версии 3.1.0 существенно оптимизирован алгоритм репликации между основным хранилищем и горячими репликами, что позволило снизить нагрузку на NFS и сократить время синхронизации реплик. Кроме того, для обеспечения устойчивой работы почтовых компонентов во время интенсивной репликации (например, при подключении нового дополнительного хранилища), на cпраницу “Общие настройки” (закладка “Почта”) добавлена настройка ширины канала NFS, которую может использовать процесс репликации.



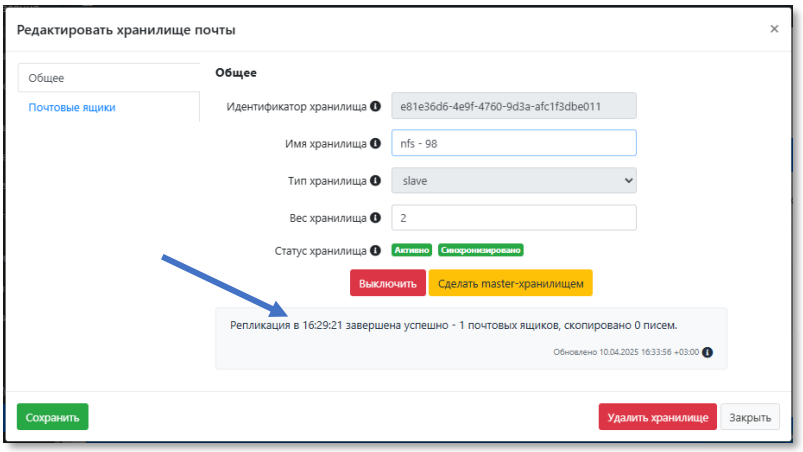
При выборе опции “Без ограничений” система автоматически подстраивается под максимально возможную, в данный момент, скорость передачи данных.

В версии 3.3.0 переработан механизм репликации данных. Новый механизм обеспечивает гораздо большую производительность обработки данных за счет использования нескольких потоков копирования на каждом узле кластера.

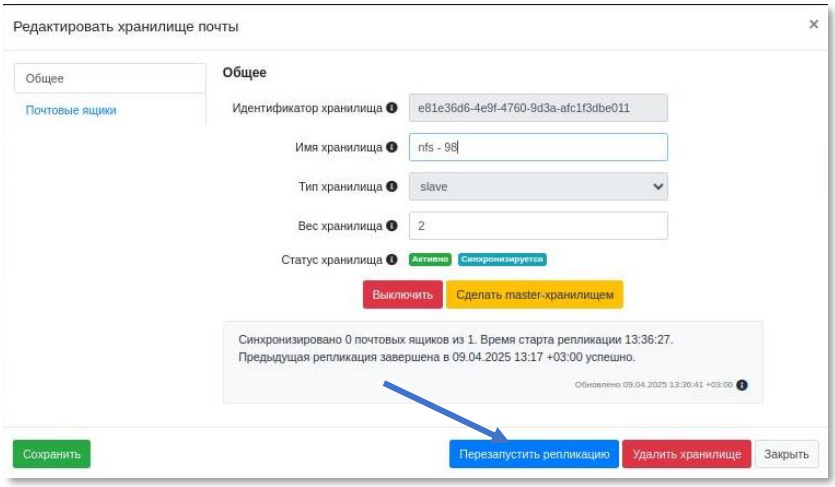
Внимание!

Реализация функциональности быстрой репликации носит экспериментальный характер и работает с ограничениями.
В этой версии, быстрая репликация работает **только** для “горячих” реплик - копирование данных на “холодную” реплику и перенос почтовых ящиков между группами / пространствами хранения осуществляется “старым’ механизмом.

В окне свойств хранилища, которое является “горячей” репликой, внесены изменения в отображение текущего статуса процесса репликации – в ходе репликации отображается количество обработанных почтовых ящиков, а также время последней успешно завершенной репликации.



В случае, если репликация завершилась с ошибкой, есть возможность запуска репликации по команде администратора – это можно сделать с помощью кнопки “Перезапуск репликации”.



В версии 3.4.0 оптимизирован механизм копирования почтовых данных при следующих сценариях:

- Копирование данных с “горячей” реплики на “холодную”
- Перенос почтовых ящиков в другое Пространство хранения
- Перенос Группы ящиков в другое Пространство хранения.

Так как перенос Группы ящиков в другое Пространство хранения может занимать существенное время, этот механизм был модифицирован - теперь такая операция осуществляется как последовательный перенос отдельных почтовых ящиков Группы.

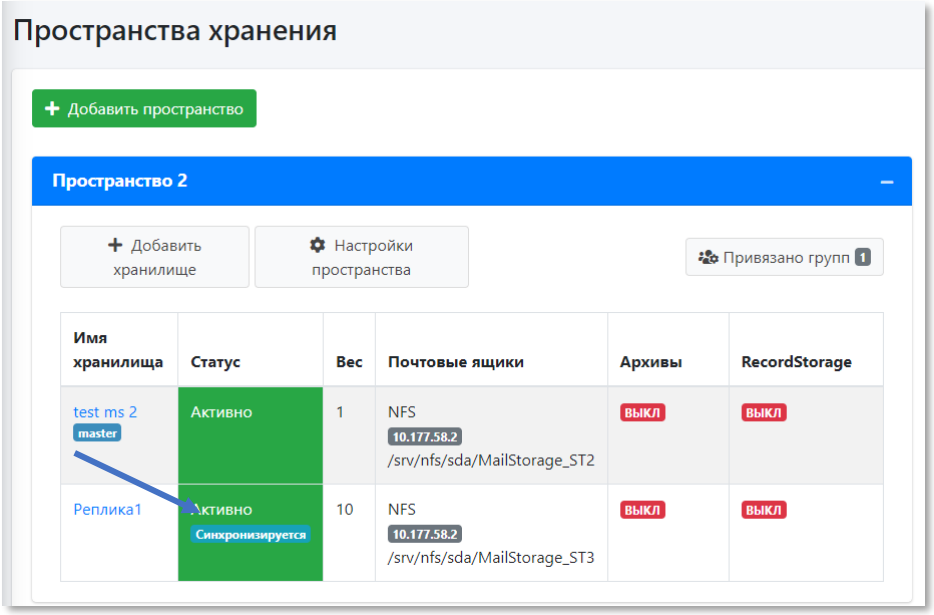
В версии 4.3.4 для оптимизации репликационной нагрузки на мастер-хранилище, внесены изменения в схему репликации данных при наличии нескольких “горячих” реплик.

Репликация для “горячих” реплик проводится в два этапа:

1. Данные с мастер-хранилища реплицируются на первую “горячую” реплику (имеющую наибольший вес).
2. Данные с первой “горячей” реплики реплицируются на остальные “горячие" реплики.

2.11.8. Статус синхронизации реплики

В версии 3.1.0 добавлена расширенная информация о состоянии репликации почтовых хранилищ (MailStore).



Цветовой индикатор статуса репликации может иметь следующие значения:

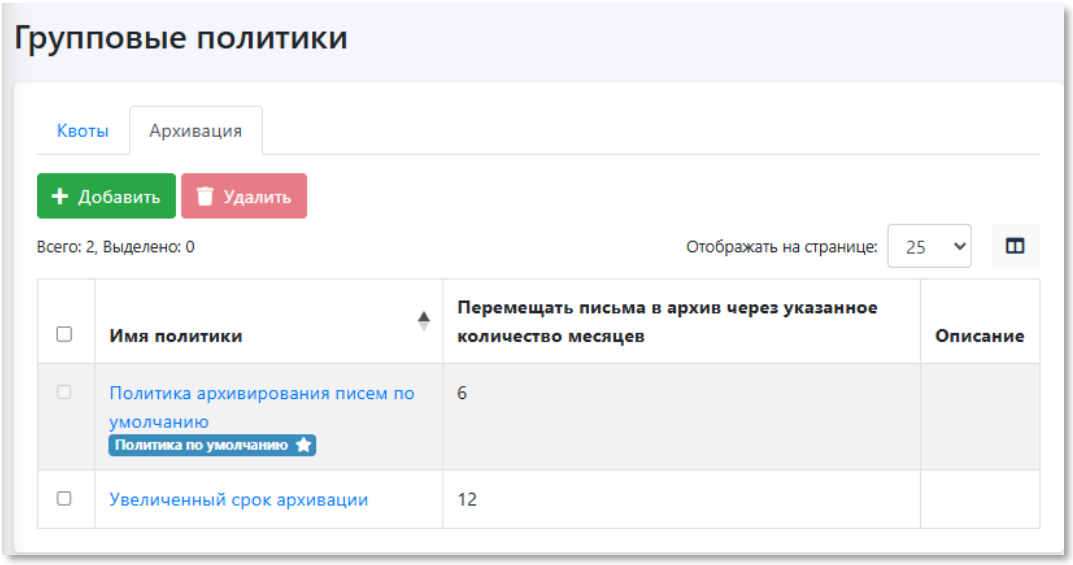
- Синхронизировано
- Ошибка синхронизации
- Синхронизируется
- Ожидает синхронизации

2.11.9. Перенос почты в архив в соответствии с политикой архивации

В версии 3.2.0 добавлено автоматическое архивирование почты – перенос писем, которые созданы ранее выбранного интервала архивации, в папку Архив.

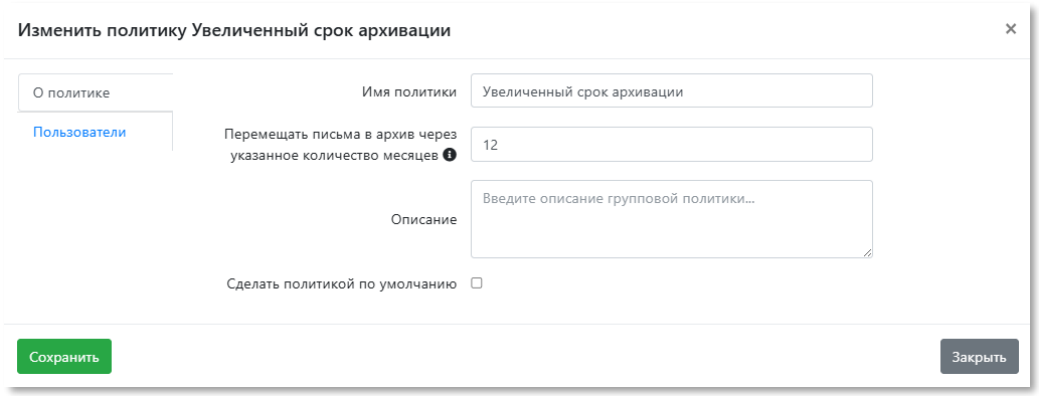
Процесс архивирования почты запускается ежедневно в 2 часа ночи.

Настройка интервала архивации осуществляется с помощью Политик архивации, задаваемых на закладке “Архивация” страницы “Групповые политики”.

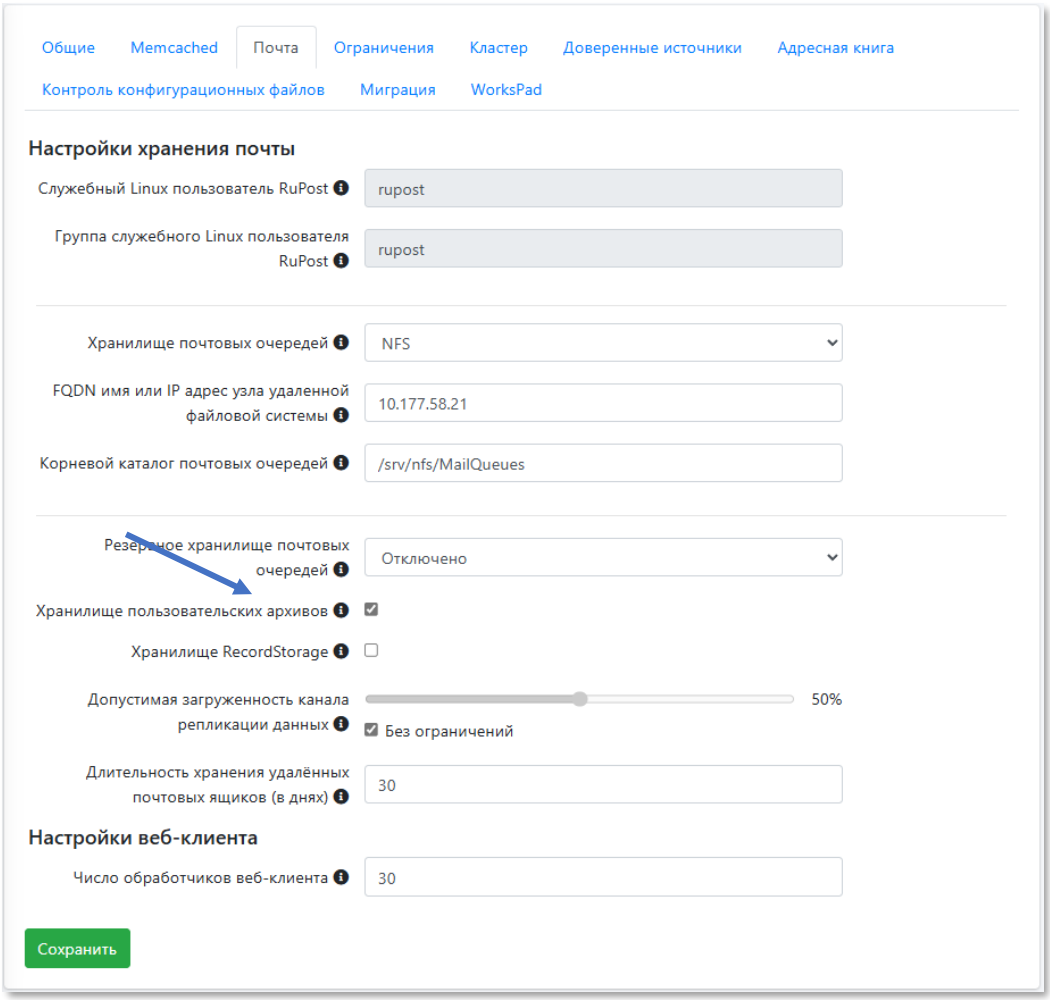


При создании почтового ящика к нему применяется политика “по умолчанию”.

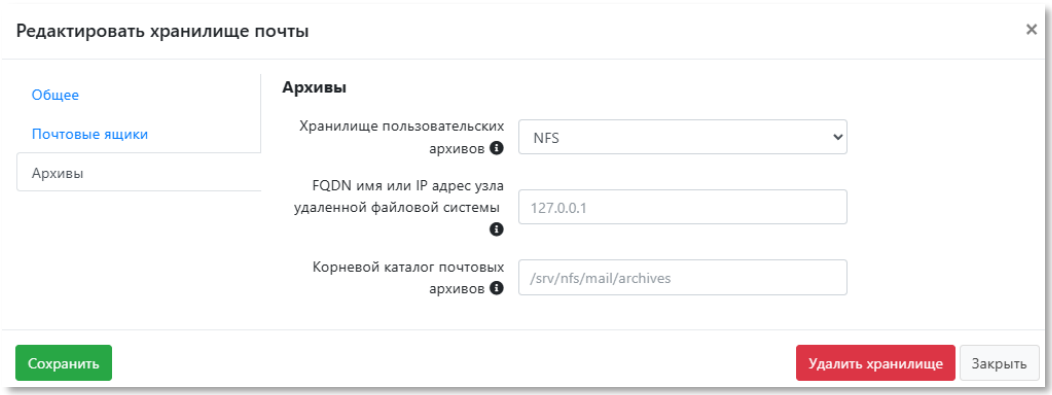
Если есть необходимость для различных групп пользователей определить свой интервал архивирования, отличающийся от Политики “по умолчанию”, то нужно создать еще одну Политику архивирования и применить ее к выбранным почтовым ящикам.



Для того, чтобы архивирование почты работало, необходимо на закладке “Почта” страницы “ Общие настройки” включить “Хранилище пользовательских архивов”.



После чего, в свойствах хранилища указать адрес NFS сервера и путь, по которому будут храниться пользовательский архив почты.



В версии 3.2.1 добавлена автоматическая архивация папки “Отправленные” (Sent). Правила архивации для папки Sent те же, что и для папки Inbox.

Соответственно, изменена структура папок в разделе “Архивы” – добавлены подпапки “Inbox” и “Sent”.

В версии 4.1.0 изменен порядок папок, которые формируются в пользовательских архивах.

Папки по месяцам не создаются, а папки по годам перенесены на уровень выше – т.е. архивные папки имеют следующую структуру:

Архивы / [год] / Inbox, Sent

В версии 4.2.0 реализовано архивирование с сохранением структуры папок почтового ящика пользователя.

Рекомендуется

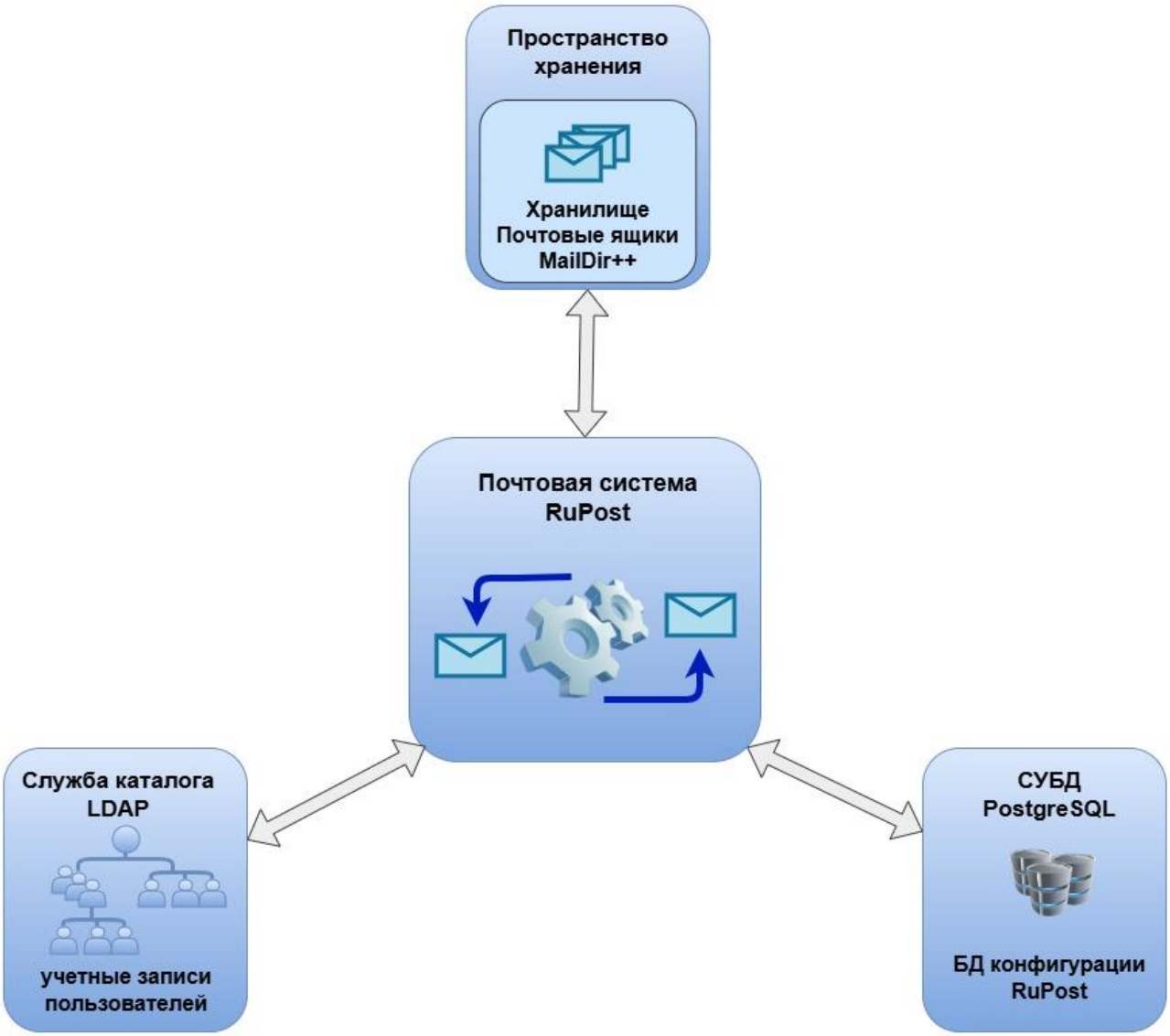
Для того, чтобы обновить пользовательские архивы в соответствии с новой схемой, добавлена специальная команда CLI:

```
rupost mailbox update-archive-emails-folders
```

Рекомендуется выполнить данную команду сразу же после обновления с версии 4.0.1 или более ранней.

2.12. Моментальные снимки состояния

Современные файловые системы и системы виртуализации предоставляют возможность создания моментальных снимков состояния файловой структуры и виртуальных машин, не требующие остановки работы с ними. В процессе выполнения данной функции происходит кратковременное прекращение операций ввода/вывода и записи данных на файловую систему. В сложных и много узловых кластерных системах, одной из которых является RuPost, это может привести к непредсказуемому поведению различных сервисов и сбою их работы.



Внимание!

Критическими источниками данных для RuPost являются базы данных, Пространство хранения с Хранилищами и сервис службы каталогов LDAP с данными пользователей RuPost.

Работа почтовой системы RuPost при отсутствии одного или нескольких этих источников невозможна!

Рекомендуется перед выполнением моментальных снимков узла RuPost выводить узел из эксплуатации, а наилучшим решением для виртуального узла будет его выключение, перед созданием снимка, с последующим включением. Эта рекомендация распространяется как на сервер управления базами данных PostgreSQL, с базой RuPost, так и на сервис сетевой файлового доступа NFS с Пространствами хранения и Хранилищами RuPost.

При необходимости снятия снимков всех узлов много узловой конфигурации RuPost до их выполнения рекомендуется последовательное выключение сначала всех узлов RuPost, затем узлов сервера управления базами данных и сервиса сетевой файлового доступа NFS. Включение узлов производится в обратном порядке.

Внимание!

Моментальные снимки состояния не являются резервными копиями и не могут быть использованы вместо них!

Моментальные снимки состояния

Моментальные снимки состояния привязаны к конкретной виртуальной машине, не могут быть применены на другой, перемещены и использованы в другой системе виртуализации или применены к реальному (аппаратному) компьютеру.

Резервная копия

Резервная копия может быть перемещена и использована для восстановления между различными система виртуализации, а также на (аппаратном) компьютере.

Для обеспечения сохранности данных рекомендуется регулярное создание резервных копий Пространств хранения с Хранилищами, баз данных и сервиса службы каталогов LDAP с данными пользователей RuPost.

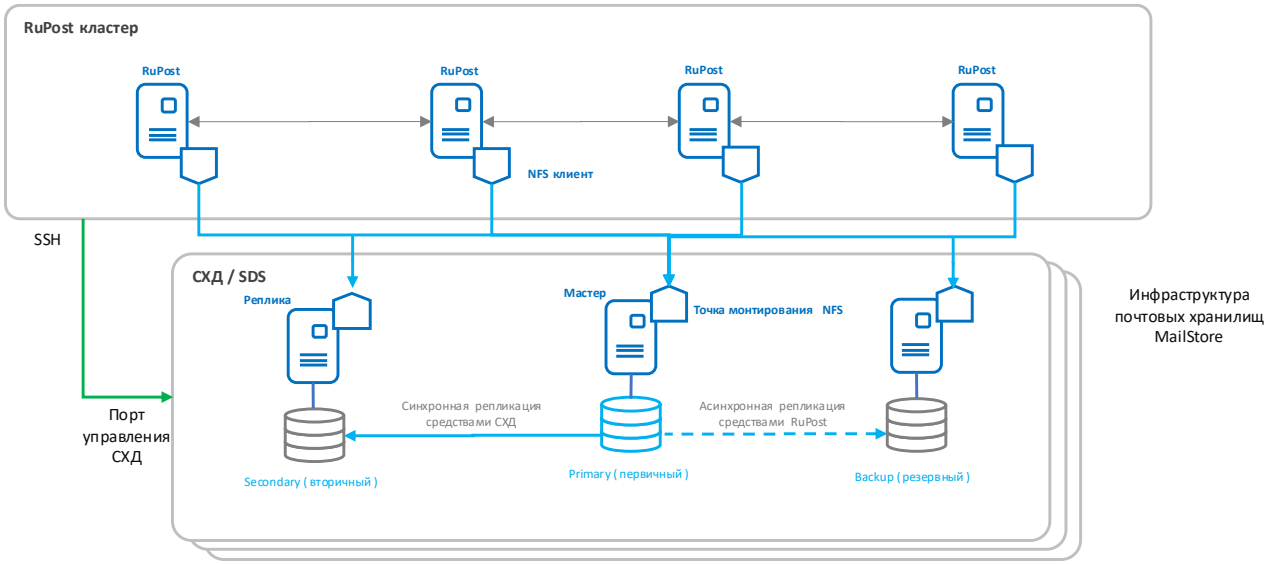
© 2021-2026 РуПост

2.13. Интеграция с СХД / SDS

В версии 3.4.0 добавлена возможность интеграции RuPost с внешними системами хранения данных - СХД (*Система Хранения Данных*) или SDS (*Software Defined Storage*). Теперь администратор почтовой системы имеет возможность осуществлять управление системой хранения данных, к которой подключен RuPost. Наличие такого механизма позволяет осуществлять ряд операций с данными, хранящимися в СХД, непосредственно средствами СХД. Это имеет существенное значение в случае больших объемов данных – например, копирование данных из одного хранилища в другое, синхронизация хранилищ и т.д. Кроме того, механизм интеграции с СХД решает и задачу передачи знаний – от администратора СХД, знающего тонкости работы с конкретной СХД к администратору почтовой системы, управляющего хранением почтовых данных для решения задач электронной почты.

Ядром подсистемы интеграции с СХД является модуль хранения и управления наборами команд СХД (скриптами). С его помощью администратор СХД может сконфигурировать ряд скриптов для выполнения действий с хранилищами.

В терминах RuPost, каждый набор команд управляет данными отдельного Хранилища, определяемого в Пространстве хранения. В случае использования СХД, для хранения почтовых данных (MailDir), каждому хранилищу RuPost соответствует хранилище на уровне СХД, которое опубликовано по протоколу NFS.



Для упрощения управления СХД администратором RuPost, скрипты разделены на три сценария работы системы электронной почты, которые требуют наиболее интенсивной работы с почтовыми данными:

1. **Первоначальная репликация данных с мастера на реплику**. Применяется в том случае, когда на исходном хранилище (мастере) уже есть большое количество почтовых данных и нам нужно создать новую реплику. В этом случае, копирование данных средствами СХД может оказаться быстрее, чем встроенный в RuPost механизм репликации. Для привязки хранилища СХД к хранилищу RuPost хранилище СХД должно быть опубликовано через NFS.

Предлагаемая структура скрипта:

- Создание хранилища СХД для реплики
- Копирование данных с мастер-хранилища на реплику
- Публикация реплики через NFS.

Ожидаемый результат работы скрипта:

- Наличие реплики, опубликованной через NFS

Действия RuPost после выполнения скрипта:

- Проверка работоспособности точки монтирования NFS и установка соответствующего статуса реплики

2. **Непрерывная синхронизация реплики и мастера**. Этот сценарий применяется в том случае, когда необходимо обеспечить постоянную синхронизацию мастера и реплики. Использование средств СХД для решения этой задачи позволяет осуществить *синхронную* репликацию - в отличие от встроенного механизма репликации RuPost, который обеспечивает *асинхронную* репликацию. Обратите внимание – часто, при осуществлении такой синхронизации на блочном уровне СХД, хранилище не доступно. Для того, чтобы в нужный момент сделать его доступным и опубликовать через NFS должен быть подготовлен скрипт 3.

   Предлагаемая структура скрипта:

   - Запуск синхронной репликации данных с мастер-хранилища на реплику.

   Ожидаемый результат работы скрипта:

   - Идет синхронная репликация с мастера на эту реплику

   Действия RuPost после выполнения скрипта:

   - Нет

3. **Смена мастера: отключение синхронизации, публикация хранилища в NFS и назначение реплики мастером**. Этот сценарий применяется в том случае, когда необходимо назначить синхронизирующуюся реплику мастером, но, из-за того, что, в данный момент, выполняется синхронная репликация (запущенная скриптом 2), реплика заблокирована на уровне СХД и, соответственно, не опубликована через NFS.

   Предлагаемая структура скрипта:

   - Остановка синхронной репликации с мастер-хранилища на реплику
   - Публикация реплики через NFS.

   Ожидаемый результат работы скрипта:

   - Наличие реплики, опубликованной через NFS

   Действия RuPost после выполнения скрипта:

   - Проверка работоспособности точки монтирования NFS и назначение этой реплики мастером

Внимание!

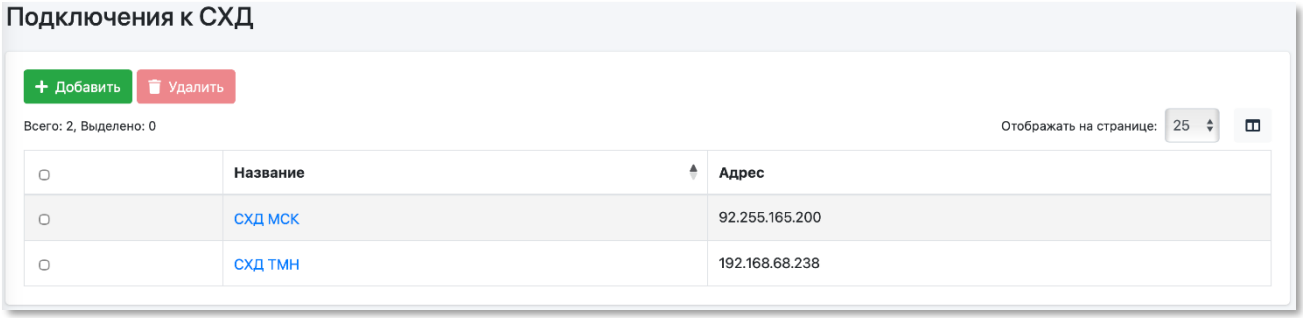
- В данный момент, передача параметров NFS из хранилища RuPost в скрипт СХД не осуществляется, поэтому, обратите внимание на совпадение параметров NFS хранилища RuPost и соответствующего ему хранилища в СХД.
- Не обязательно создавать скрипт под каждый сценарий, можно определить только некоторые.

© 2021-2026 РуПост

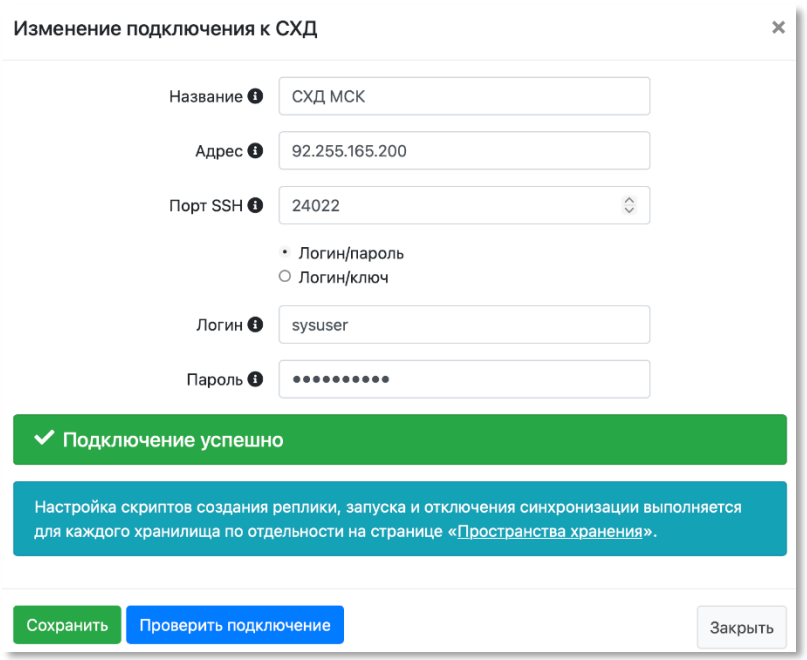
Большинство команд СХД не являются блокирующими, т.е. команда только запускает соответствующий процесс внутри СХД и возвращает управление. В этом случае для того, чтобы получить результат (или текущий статус) выполнения команд, для каждого набора команд предусмотрен дополнительный скрипт - “Скрипт проверки статуса”.

Перед началом конфигурирования скриптов управления СХД, необходимо обеспечить возможность подключения RuPost к СХД по протоколу SSH - так как RuPost использует этот протокол для отправки команд в СХД. Доступ к СХД по SSH должен быть открыт для всех узлов кластера RuPost.

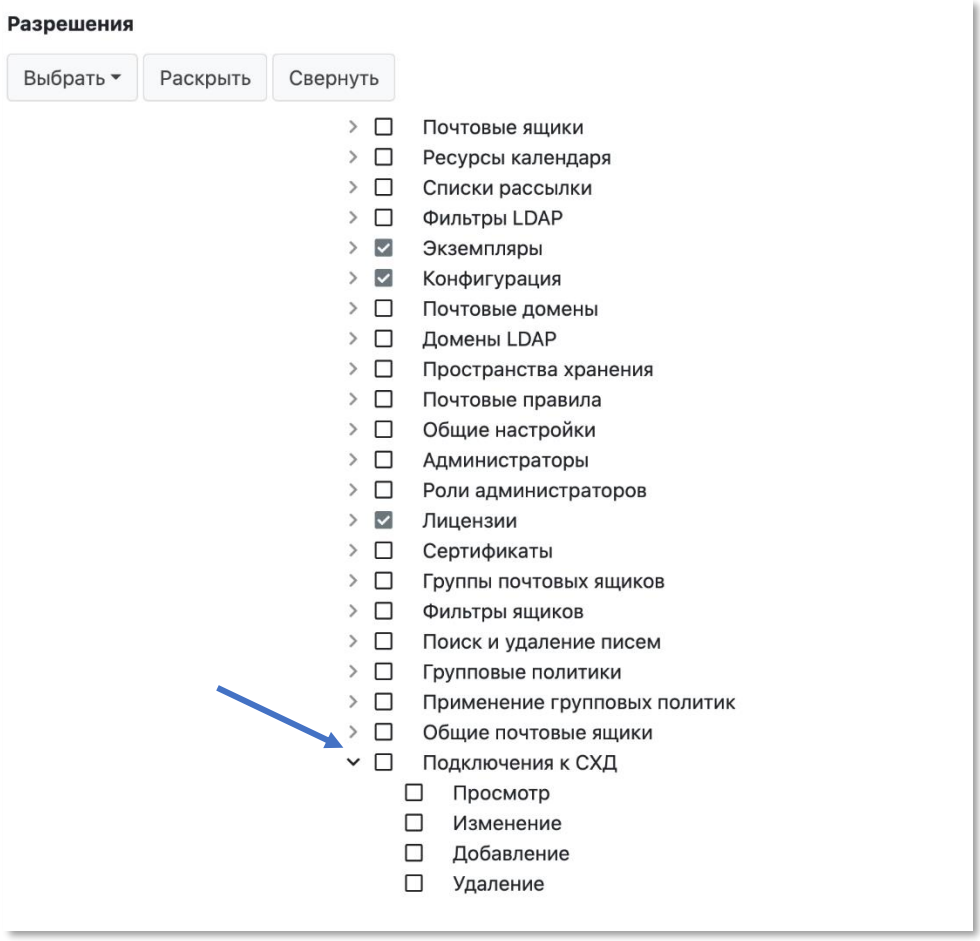
Управление подключениями к внешним системам хранения данных осуществляется в Панели управления на странице “Подключения к СХД”.



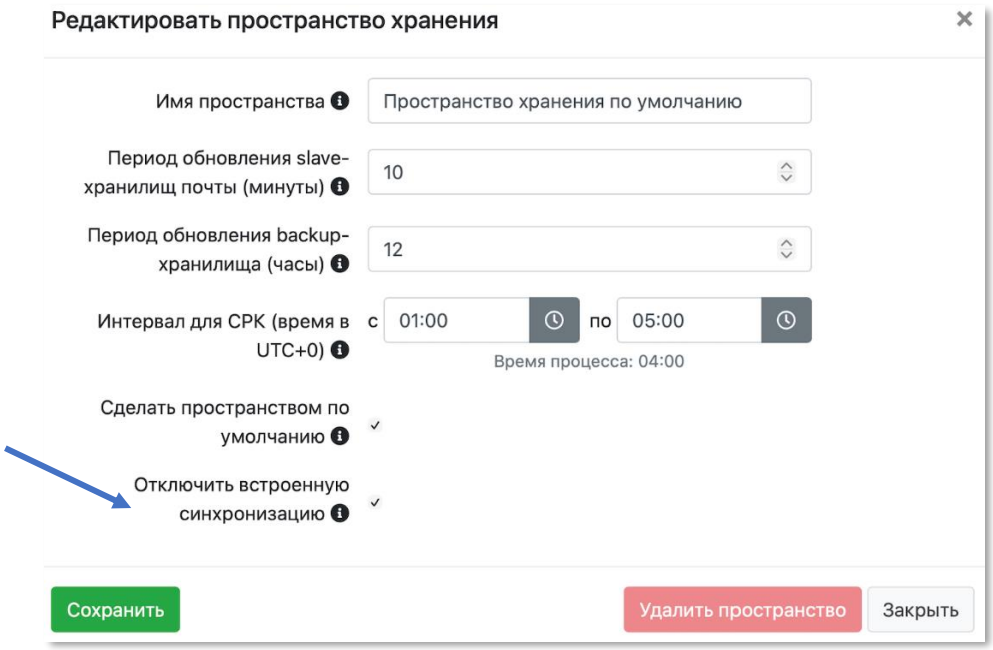
Для создания подключения, нажмите на кнопку “Добавить” и укажите параметры подключения по SSH - IP-адрес СХД и логин / пароль (или логин / ключ). Проверить корректность введенных данных можно по кнопке “Проверить подключение”.



Права доступа администраторов к управлению подключениями к СХД задаются для ролей администраторов на странице “Разрешения”.



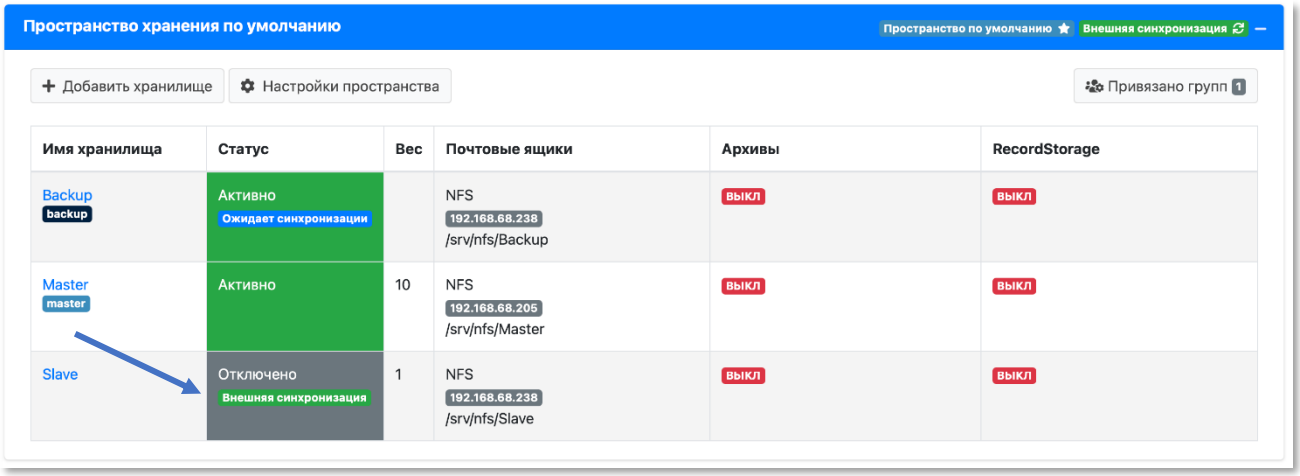
Режим интеграции с СХД включается на уровне Пространства хранения. Для включения этого режима, необходимо отключить встроенную репликацию в свойствах выбранного Пространства хранения.



После этого, у Пространства хранения появится статус “Внешняя синхронизация”.

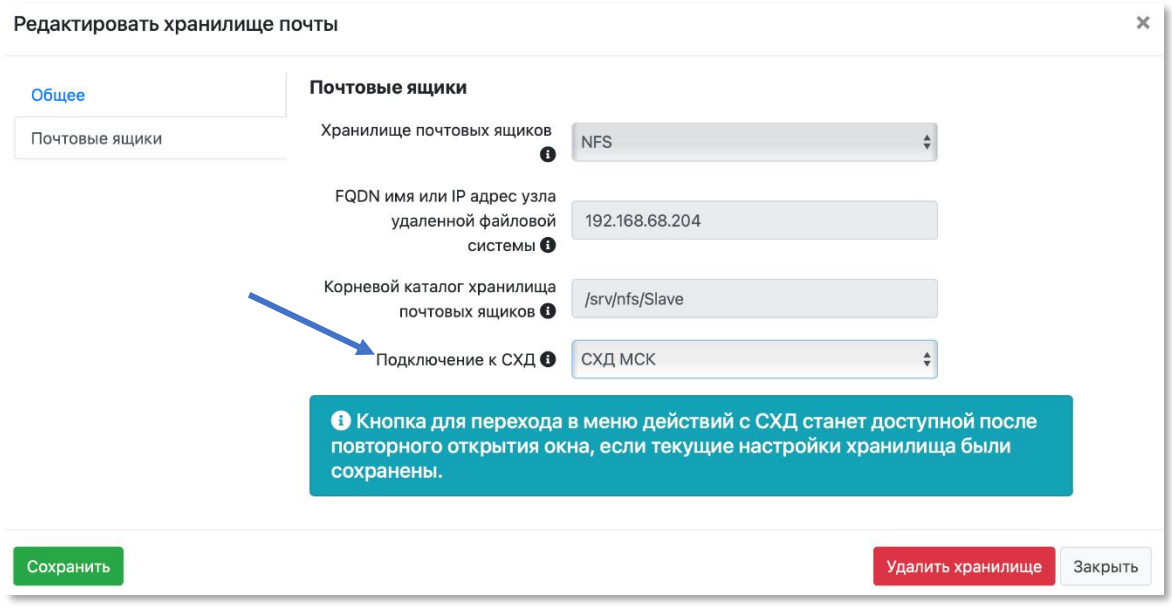


Хранилища-реплики при включенном режиме интеграции с СХД, также имеют новый статус синхронизации – “Внешняя синхронизация”.

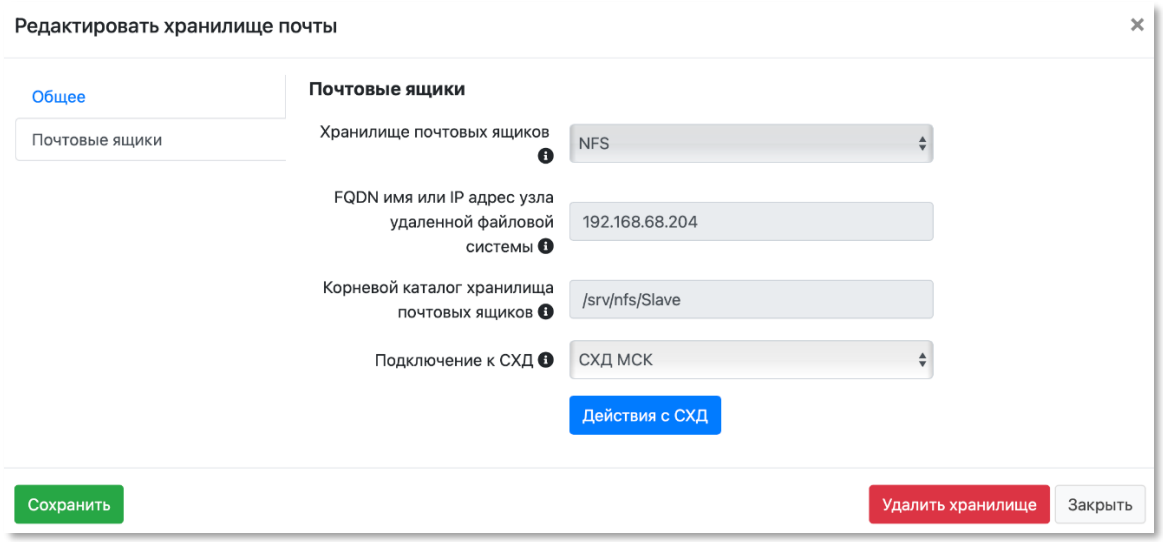


В режиме, когда встроенная репликация отключена, точка монтирования NFS, указанная в свойствах вновь созданного хранилища-реплики, может быть не активной до выполнения соответствующего скрипта. Поэтому, в этом случае, чтобы исключить проверки точки монтирования NFS, хранилище создается в статусе “Отключено”.

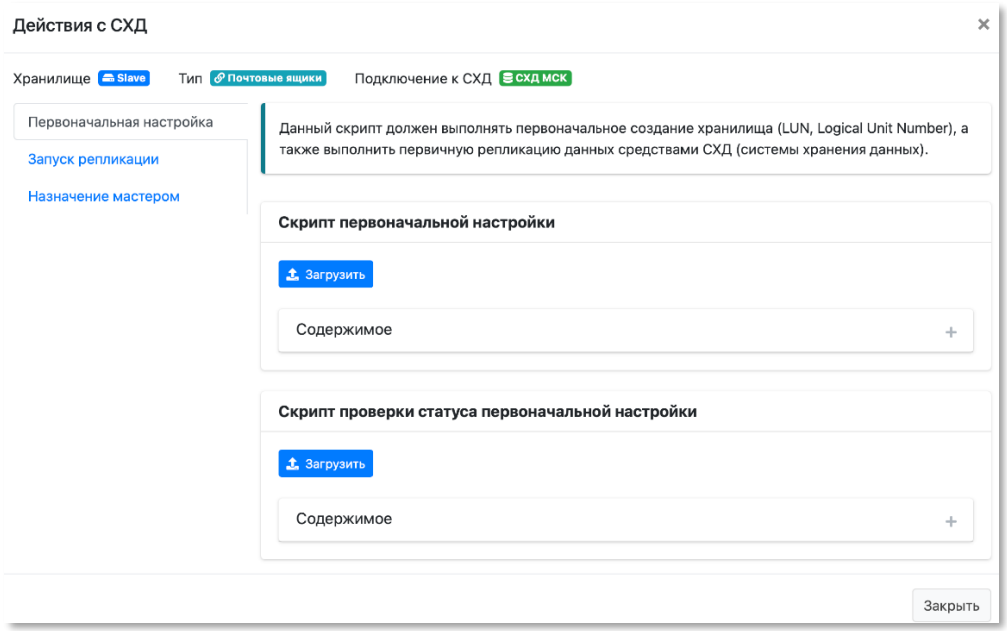
Для конфигурирования набора команд, необходимо в свойствах хранилища выбрать ранее созданное подключение к СХД.



Переход на страницу конфигурирования и выполнения скриптов осуществляется по кнопке “Действия с СХД”.



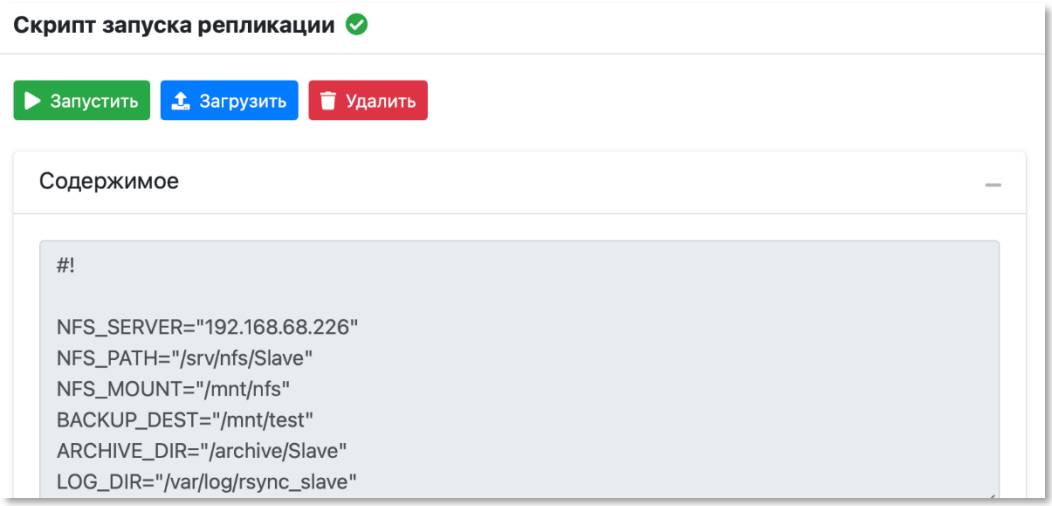
На странице “Действия с СХД” выбор необходимого сценария осуществляется на соответствующих вкладках.



Наименования вкладок соответствуют вышеописанным сценариям:

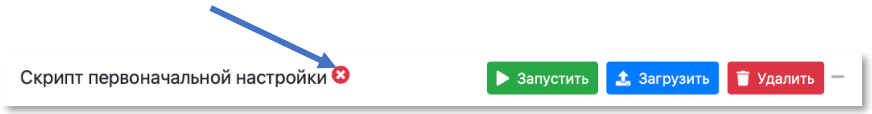
- **Первоначальная настройка** – первоначальная репликация данных с мастера на реплику
- **Запуск репликации** – непрерывная синхронизация реплики и мастера
- **Назначение мастером** - прекращение синхронизации, публикация хранилища в NFS и назначение реплики мастером.

Скрипт, предварительно подготовленный администратором СХД, должен быть загружен из файла администратором RuPost по кнопке “Загрузить”.

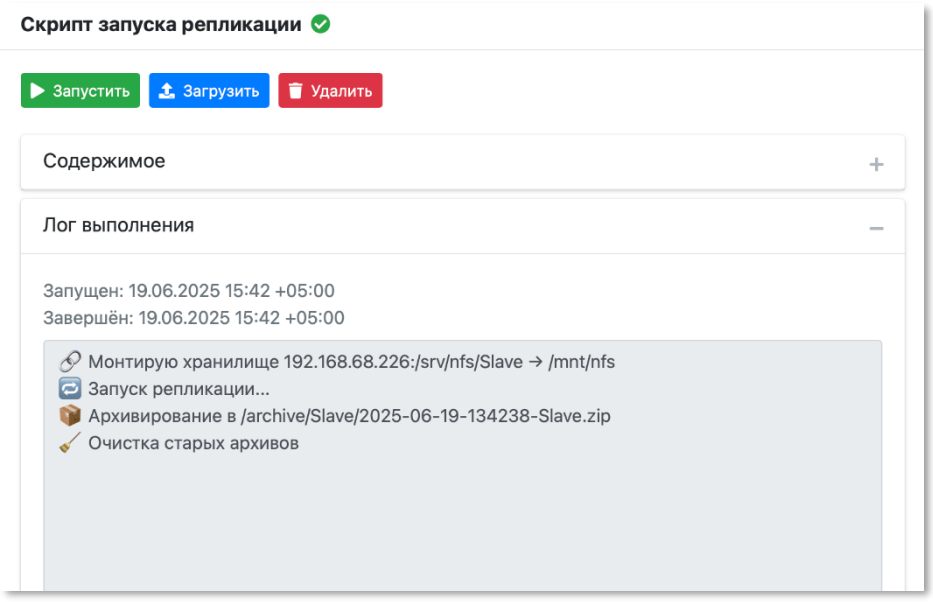


Для выполнения набора команд нажмите на кнопку “Запустить”.

После запуска команды на выполнение у наименования скрипта появится индикатор, показывающий, выполняется ли в данный момент этот скрипт. По окончанию выполнения, индикатор покажет, была ли операция успешной (зеленый) или завершилась с ошибкой (красный).



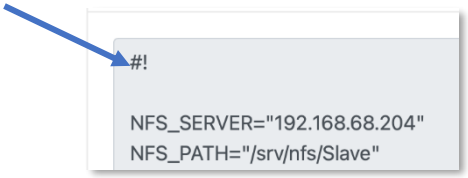
При выполнении набора команд вся информация, которая поступает от СХД по стандартным каналам stdout / stderr, отображается в окне лога выполнения.



RuPost поддерживает два режима выполнения команд:

- **Построчно** – текст рассматривается как набор команд, где каждая строка содержит отдельную команду СХД. Команды выполняются последовательно, по одной, с выводом результата после каждой команды.
- **Файл** – весь текст рассматривается как одна команда, даже если содержит несколько строк. Соответственно, выполняется за один вызов СХД, т.е. весь текст отправляется в СХД одной командой.

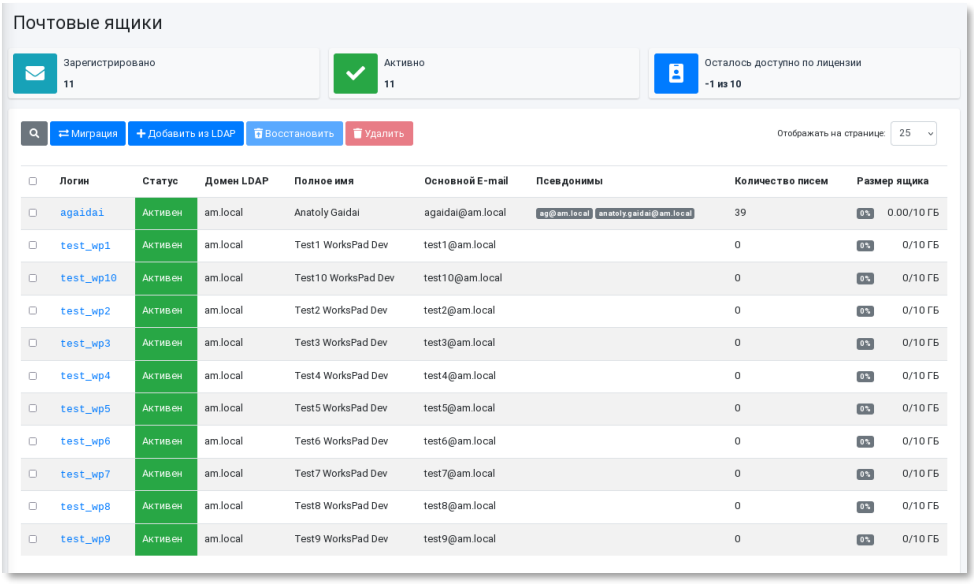
Индикатором того, что необходимо применить режим “Файл”, является наличие символов шебанг (символов “#!”) в начале первой строки скрипта.



Пример скриптов для работы с SDS Linstor приведен в Приложении 4.

2.14. Управление почтовыми ящиками

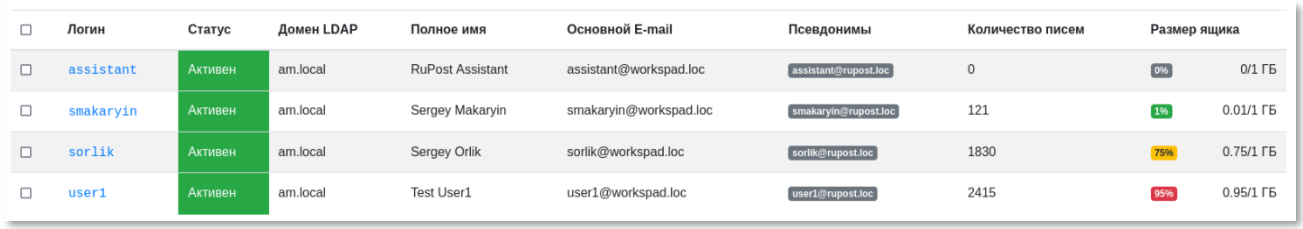
Страница управления почтовыми ящиками обеспечивает весь жизненный цикл почтовых ящиков, от заведения их в системе, поиска среди заведенных ящиков, изменения параметров, вплоть до вывода из эксплуатации (пометки как удаленных) и восстановления удаленных ящиков в течение периода удержания (retention), определяемого на странице общих настроек.



В версии 2.5.0 на страницу “Почтовые ящики” добавлена информация о количестве писем в ящике, а также о занимаемом объеме и проценте использования квоты. Актуальные значения счетчиков появляются либо после переиндексации, либо после первого подключения пользователя к своему почтовому ящику.

Значение цветового индикатора “%” использования квоты поля “Размер ящика’:

- Серый - квота на ящик не установлена или не использована (**0%**);
- Зеленый – квота использована менее, чем на **75%**;
- Желтый - квота использована на **75%** и более;
- Красный – квота использована на **95%** и более.

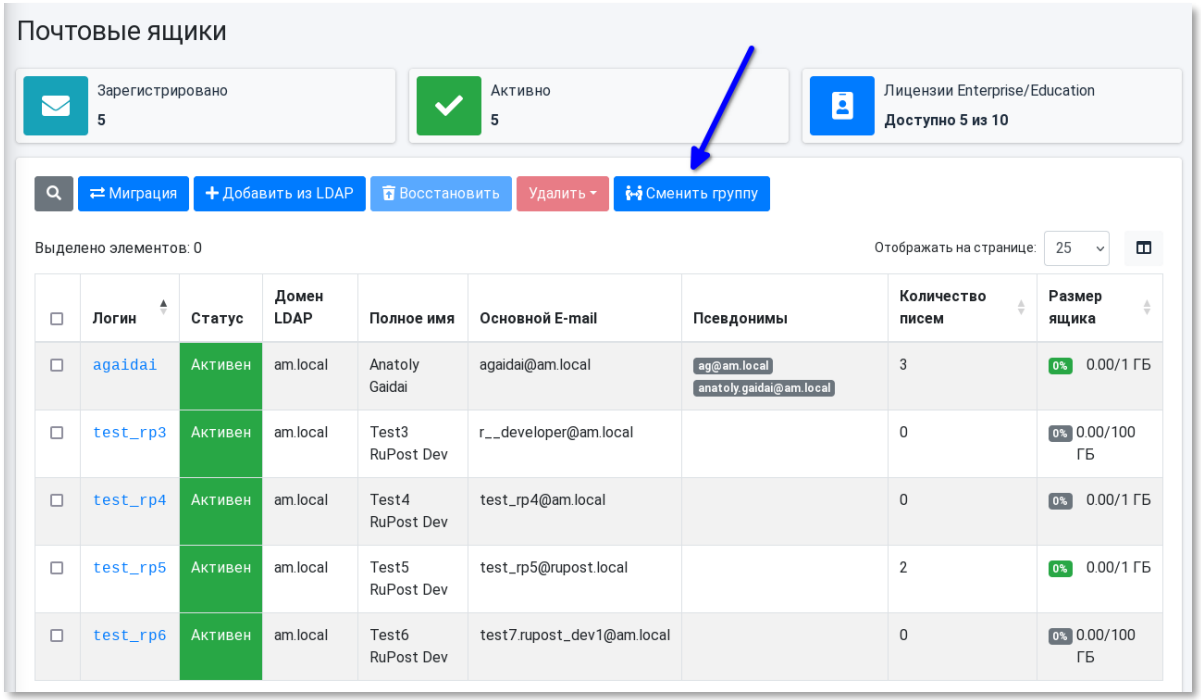


Логин	Статус	Домен LDAP	Полное имя	Основной E-mail	Псевдонимы	Количество писем	Размер ящика
assistant	Активен	am.local	RuPost Assistant	assistant@workspad.loc	assistant@rupost.loc	0	0% 0/1 ГБ
smakaryin	Активен	am.local	Sergey Makaryin	smakaryin@workspad.loc	smakaryin@rupost.loc	121	1% 0.01/1 ГБ
sorlik	Активен	am.local	Sergey Orlik	sorlik@workspad.loc	sorlik@rupost.loc	1830	75% 0.75/1 ГБ
user1	Активен	am.local	Test User1	user1@workspad.loc	user1@rupost.loc	2415	95% 0.95/1 ГБ

В версии 2.6.0 на странице “Почтовые ящики” добавлена возможность сортировки почтовых ящиков в таблице по столбцам:

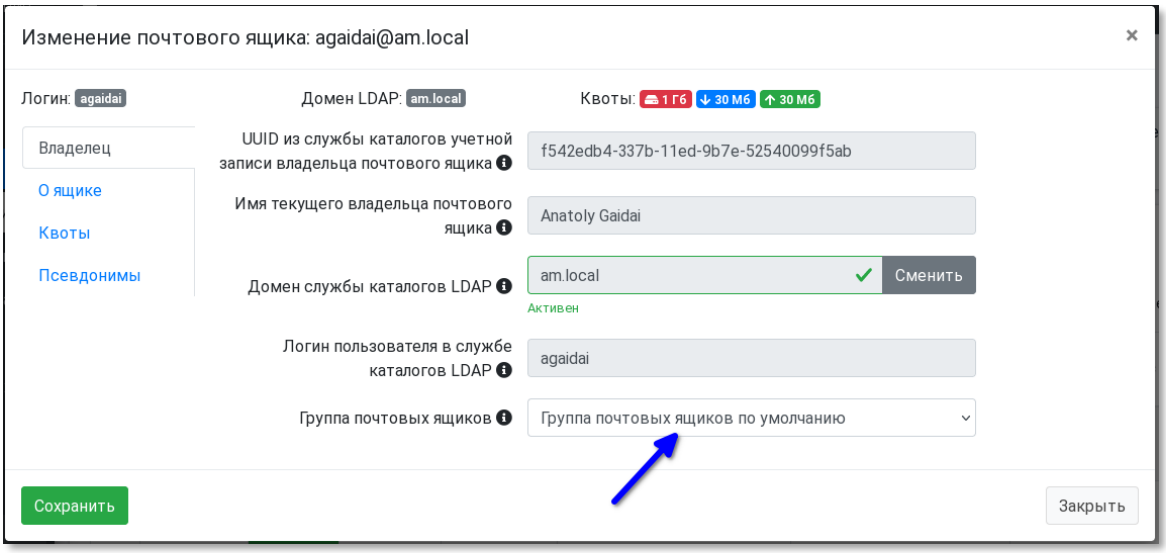
- Логин
- Количество писем
- Размер ящика

В версии 3.0 на странице “Почтовые ящики” добавлены возможности управлять размещением Почтовых ящиков в Группах ящиков:



Логин	Статус	Домен LDAP	Полное имя	Основной E-mail	Псевдонимы	Количество писем	Размер ящика
agaidai	Активен	am.local	Anatoly Gaidai	agaidai@am.local	ag@am.local anatoly.gaidai@am.local	3	0% 0.00/1 ГБ
test_rp3	Активен	am.local	Test3 RuPost Dev	r__developer@am.local		0	0% 0.00/100 ГБ
test_rp4	Активен	am.local	Test4 RuPost Dev	test_rp4@am.local		0	0% 0.00/1 ГБ
test_rp5	Активен	am.local	Test5 RuPost Dev	test_rp5@rupost.local		2	0% 0.00/1 ГБ
test_rp6	Активен	am.local	Test6 RuPost Dev	test7.rupost_dev1@am.local		0	0% 0.00/100 ГБ

В панель управления на списке ящиков добавлена кнопка “Сменить группу” – с ее помощью можно переместить один или несколько почтовых ящиков в другую Группу ящиков.
Выбор Группы для конкретного почтового ящика, также, может быть сделан через окно свойств почтового ящика.



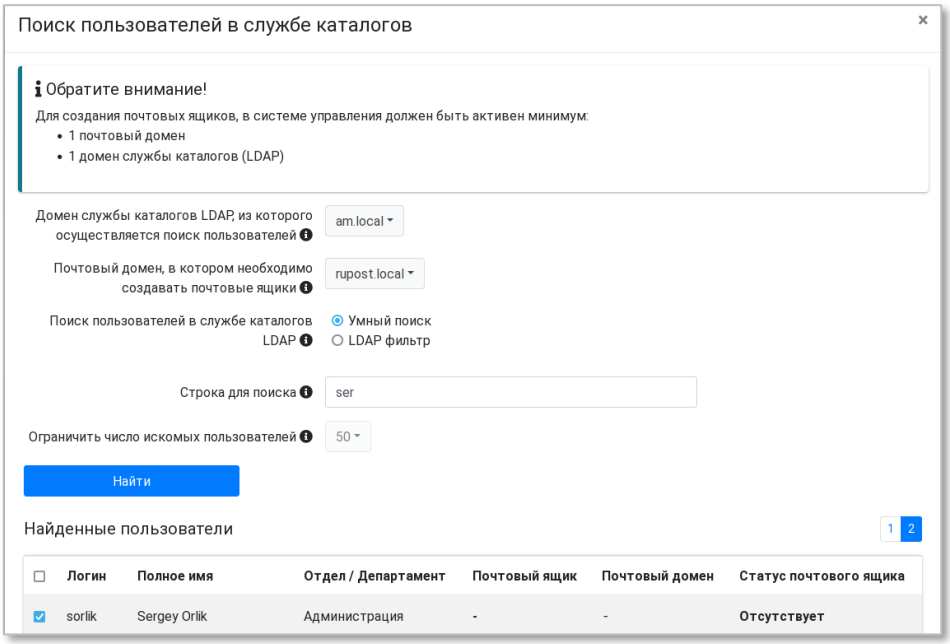
В версии 4.2.0 расширено отображение списка почтовых ящиков. На странице “Почтовые ящики” теперь отображаются не только почтовые ящики пользователей, но и Общие ящики.

2.14.1. Создание почтовых ящиков

Внимание!

Атрибут principalName у учетных записей LDAP MS должен иметь уникальное значение, иначе перестает работать импорт\создание почтовых ящиков и авторизация (keycloak\kerberos).
Для ALD Pro LDAP название атрибута: krbprincipalname.

Добавление индивидуального почтового ящика или множества почтовых ящиков осуществляется в специальном диалоге добавления на основании критериев поиска пользователей в домене LDAP (текст в имени, фамилии, группе пользователей, должности или на основании LDAP-фильтра).



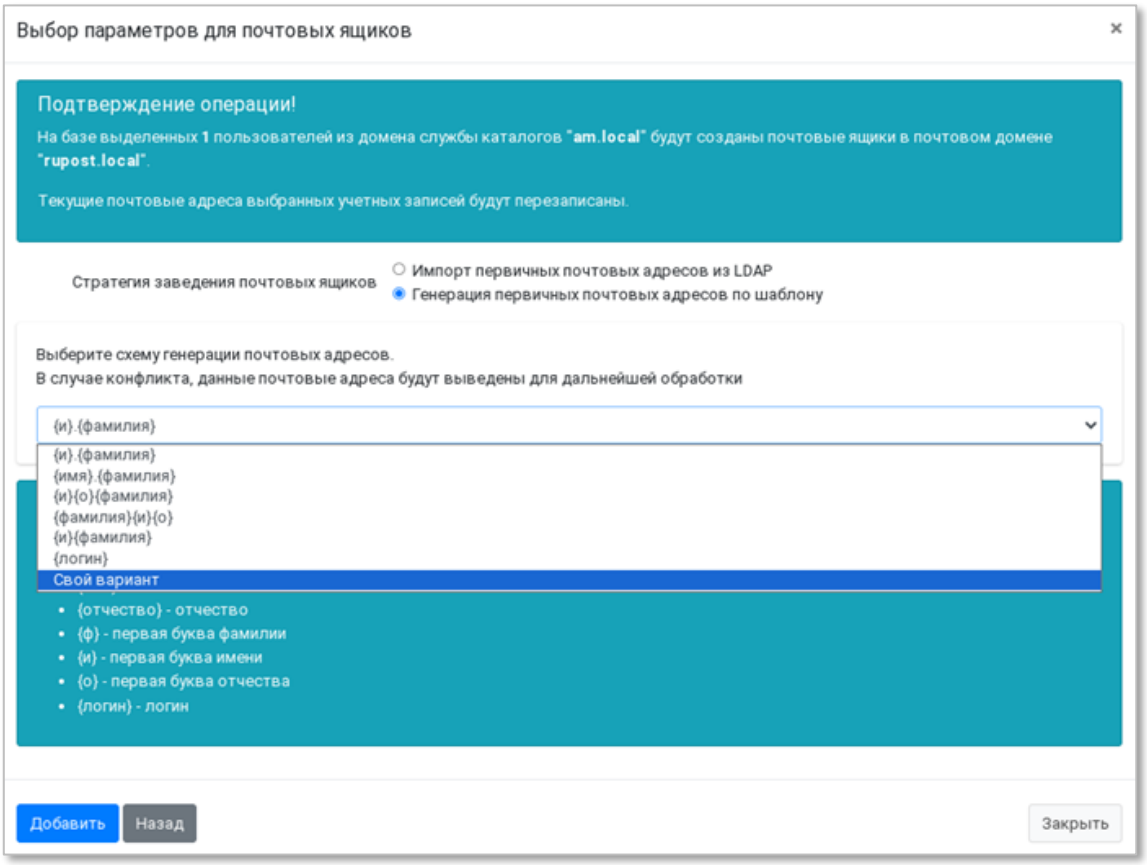
Возможен одинарный и множественный выбор пользователей, для которых необходимо завести почтовые ящики. При нахождении более 5 пользователей автоматически включается постраничное представление (справа вверху над таблицей со списком пользователей).

Для всех найденных пользователей отображается информация о наличии ящика в системе RuPost.

После выбора пользователей, для которых необходимо создать почтовые ящики, требуется выбрать режим заведения первичных почтовых адресов (primary email), используемых в том числе для подключения клиентских приложений и входа в веб-клиент RuPost.

Таких режима два:

- Первичные почтовые адреса берутся из службы каталогов LDAP без изменений.
- Первичные почтовые адреса генерируются на основе выбираемой схемы формирования адреса.



Доступны наиболее распространенные шаблоны именования почтовых адресов. Список шаблонов генерации имен почтовых ящиков до @{почтовый домен} - результат показан на примере пользователя Иван Иванов):

- Схема: `{и}.{фамилия}`
  Описание: {первая буква имени}.{фамилия} Ivan Ivanovich Ivanov -> i.ivanov
- Схема: `{имя}.{фамилия}`

Описание: {имя}.{фамилия} Ivan Ivanovich Ivanov -> ivan.ivanov

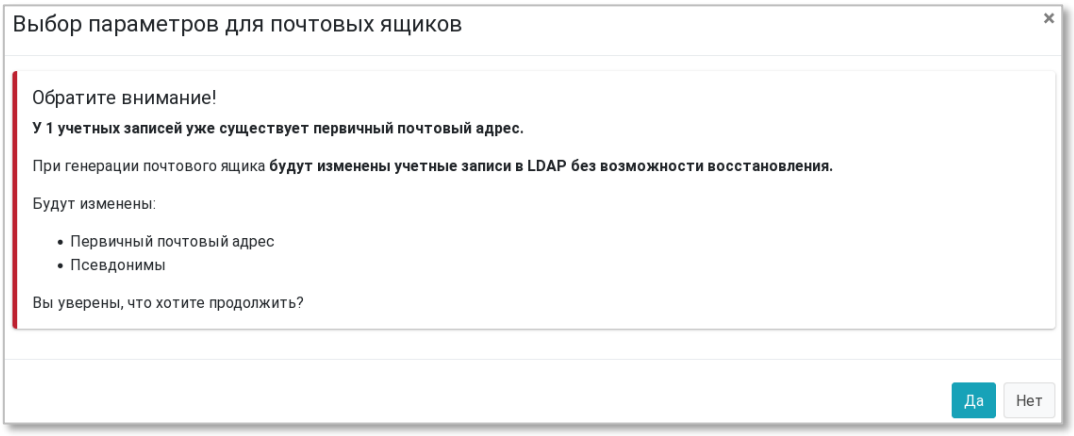
- Схема: `{и}{о}{фамилия}`
  Описание: {первая буква имени}{первая буква отчества}{фамилия} Ivan Ivanovich Ivanov -> iiivanov
- Схема: `{фамилия}{и}{о}`
  Описание: {фамилия}{первая буква имени}{первая буква отчества} Ivan Ivanovich Ivanov -> ivanovii
- Схема: `{и}{фамилия}`
  Описание: {первая буква имени}{фамилия} Ivan Ivanovich Ivanov -> iivanov
- Схема: `{логин}`
  Описание: логин пользователя, указанный в службе каталогов:
  - В случае Microsoft AD это атрибут sAMAccountName;
  - В случае FreeIPA и ALDpro это атрибут uid.

При добавлении нового почтового ящика, в случае наличия совпадений в имени автоматически генерируемого почтового ящика (например, если пользователь имеет совпадающую фамилию и начинающееся с той же буквы имя) администратору будет предложено разрешить конфликт вручную, указав другое имя почтового ящика.

Внимание!

Имя основного почтового ящика в сочетании с паролем пользователя из службы каталогов используется в качестве логина для доступа из клиентских приложений. При выборе первого режима, у пользователя в LDAP записи должен быть заполнен атрибут “proxyAddresses” значением “SMTP:<почтовый адрес пользователя>”.

При любом режиме заведения почтовых ящиков из службы каталогов считываются почтовые псевдонимы (алиасы) и, при наличии соответствующего зарегистрированного в системе почтового домена, добавляются также и почтовые псевдонимы. Результат создания почтовых ящиков записывается в базу данных RuPost и почтовые адреса пользователей обновляются в их службах каталогов.



2.14.2. Управление почтовыми ящиками – CLI

В версии 3.2.0 добавлена группа команд CLI для управления почтовыми ящиками – mailbox.

Команды mailbox позволяют делать следующие операции с почтовыми ящиками:

- Создавать
- Удалять
- Изменять свойства
- Получать список
- Восстанавливать ранее удаленный, если не истек срок до полного удаления
- Архивировать письма в соответствии с выбранной политикой архивации

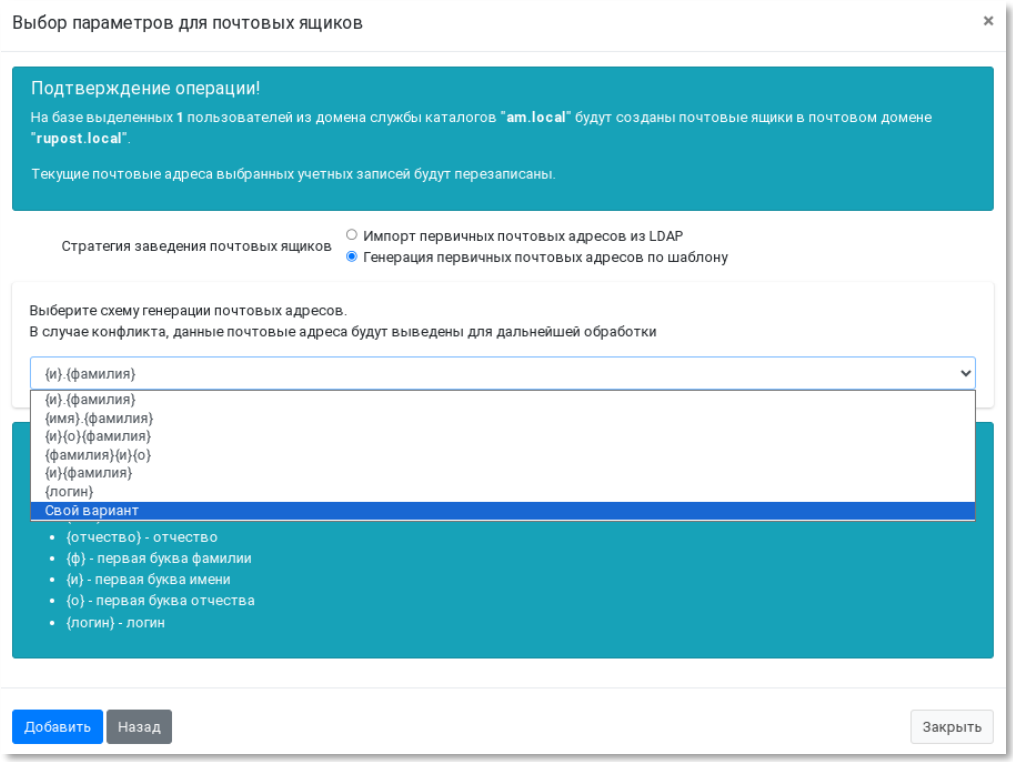


Синтаксис команд командной строки группы mailbox из приведены в разделе **«rupost mailbox»** Справочного руководство по командной строке.

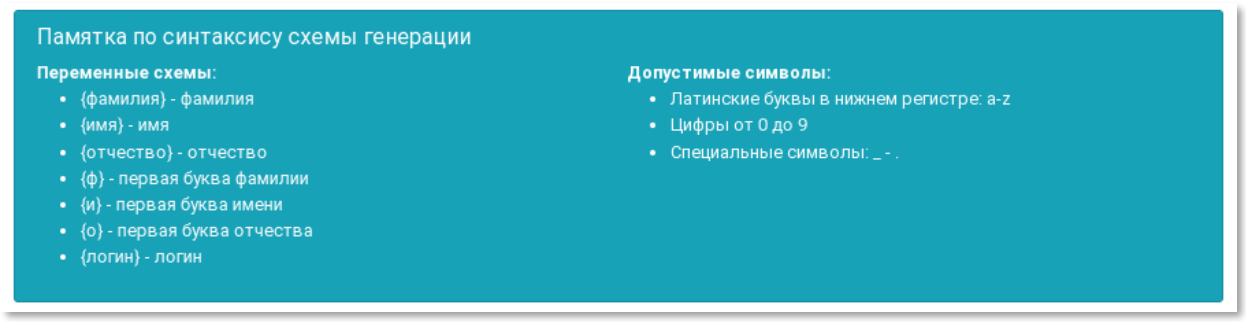
```
# rupost mailbox list --search "a"

  ID ящика:                    03116632-a6e9-4683-8b02-fcdba5495db7
  Первичный почтовый адрес:    valera@rupost.local
  Статус:                      active
  LDAP домен:                  exch2016.local
  UUID LDAP пользователя:      0647f2c1-eb45-40b8-8500-da6924abac7e
  ID почтовый группы:          c3b059f3-d474-44b9-85ba-6ce7a7b08e79
  Размер почтового ящика:      1.0 GiB
  Максимальный размер письма:  30.0 MiB

  ID ящика:                    99a03c7d-4d16-4354-b70b-e08b77cf49a0
  Первичный почтовый адрес:    aga_20@am.local
  Статус:                      active
  LDAP домен:                  am.local
  UUID LDAP пользователя:      046833a8-acbf-11ef-956e-525400689e97
  ID почтовый группы:          c3b059f3-d474-44b9-85ba-6ce7a7b08e79
  Размер почтового ящика:      1.0 GiB
  Максимальный размер письма:  30.0 MiB

  ID ящика:                    71eda7da-cfa9-4741-93df-e3804042133e
  Первичный почтовый адрес:    a_dev@am.local
  Статус:                      active
  LDAP домен:                  am.local
  UUID LDAP пользователя:      15956f02-6679-11ee-849d-52540099f5ab
  ID почтовый группы:          c3b059f3-d474-44b9-85ba-6ce7a7b08e79
  Размер почтового ящика:      1.0 GiB
  Максимальный размер письма:  30.0 MiB
```

2.14.3. Конструктор шаблонов почтовых адресов для импорта

В версии 2.7.0 добавлена возможность создания собственного шаблона почтового адреса, который может быть использован при создании почтовых ящиков.



Набор атрибутов LDAP, которые могут быть использованы при создании имени пользователя для почтового адреса:



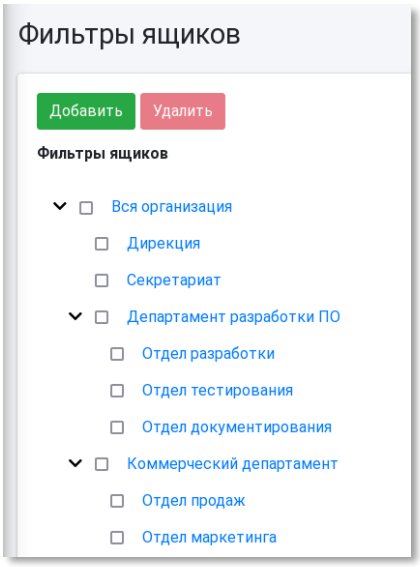
Например, для того, чтобы для пользователя Петр Иванов использовать адрес p_ivanov@domain.ru нужно задать следующий шаблон:

```
{и}_{фамилия}
```

2.14.4. Фильтры ящиков

В версии 3.1.0 добавлен новый механизм управления большим количеством почтовых ящиков – “Фильтры ящиков”, позволяющий системному администратору быстро формировать подмножества ящиков для проведения любых групповых операций над совокупностью выбранных (отфильтрованных) ящиков.

Вызов страницы “Фильтры ящиков” находится в главном меню в разделе “Получатели”:



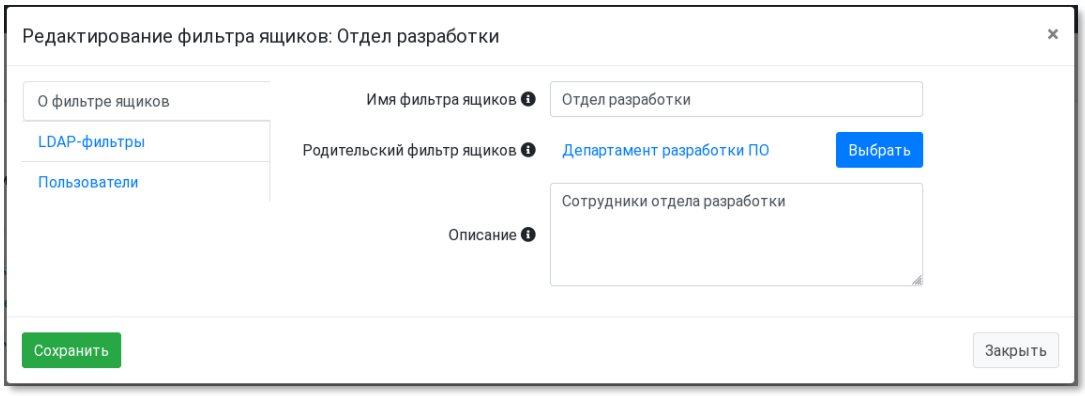
Фильтр ящиков – настраиваемый администратором иерархический фильтр, применяемый для формирования необходимого набора почтовых ящиков. Примером подобной иерархической структуры, состоящей из групп пользователей, является многоуровневая организационная структура – например:

```
Организация -> Департамент -> Отдел -> Сотрудник
```

Соответственно, если администратор настроил структуру фильтров ящиков отражающую структуру организации, то, при необходимости, например, перенести все ящики сотрудников какого-либо подразделения в отдельное хранилище, администратору достаточно будет применить соответствующий фильтр и список всех почтовых ящиков сотрудников этого подразделения будет сформирован.

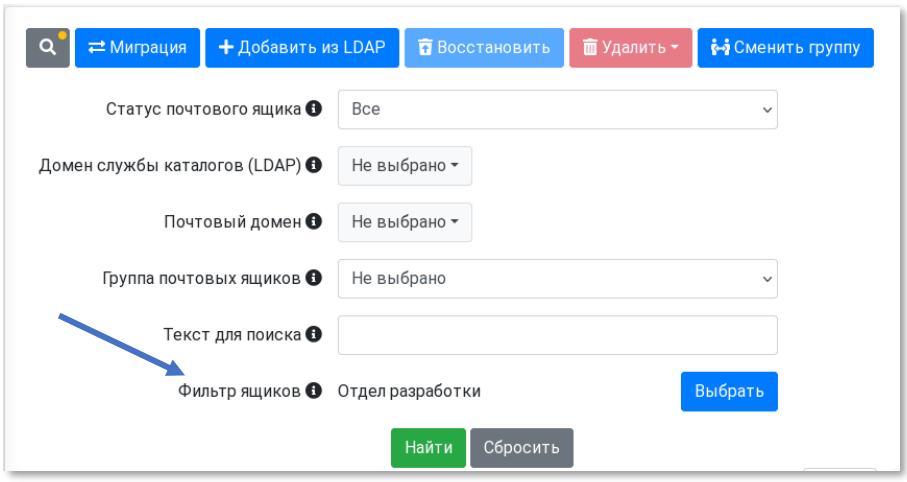
В Фильтрах ящиков иерархия работает естественным образом – список ящиков, возвращаемый фильтром верхнего уровня, включает в себя все списки, возвращаемые “вложенными” фильтрами.

Для создания фильтра ящиков на странице “Фильтры ящиков” нажмите кнопку “Добавить”, для редактирования – нажмите на нужный фильтр:

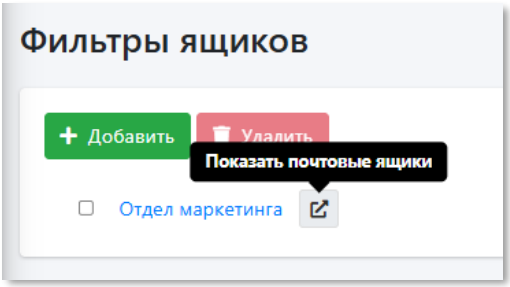


При формировании структуры фильтра ящиков, в качестве источников могут быть использованы LDAP-фильтры и статические списки пользователей/почтовых ящиков. Так как иерархия задается в структуре фильтров ящиков, то LDAP фильтр должен возвращать подмножество записей (почтовых ящиков) только для одного фильтра ящиков, а не для всей иерархии, включающей “вложенные” фильтры.

Для формирования списка почтовых ящиков с применением Фильтра ящиков, на странице “Почтовые ящики’ нажмите кнопку “Поиск” и затем, в открывшейся панели, выберите нужный Фильтр ящиков.

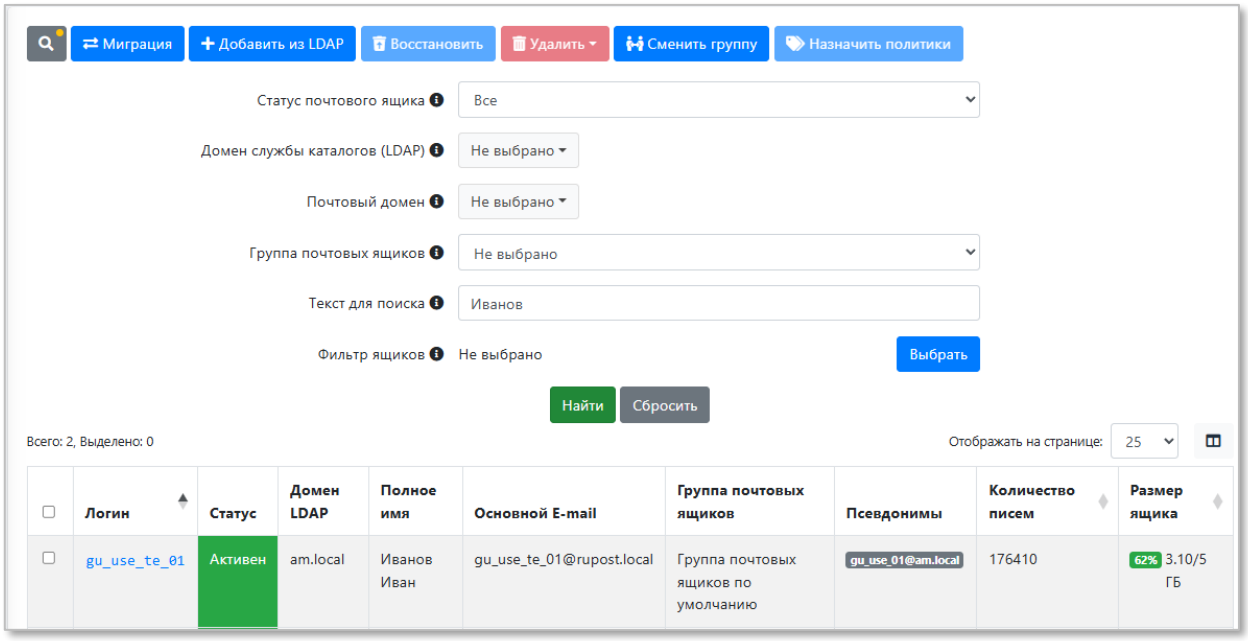


В версии 3.2.0 добавлена возможность отфильтровать список почтовых ящиков по выбранному Фильтру ящиков – для этого необходимо навести указатель мыши на выбранный Фильтр и нажать на появившуюся кнопку.



2.14.5. Поиск почтовых ящиков

Средства поиска (кнопка с иконкой “лупа” в панели кнопок операций на странице управления почтовыми ящиками) предоставляют широкий спектр условий поиска/фильтрации почтовых ящиков среди уже заведенных. Как и при заведении и просмотре списка почтовых ящиков для результатов поиска доступны групповые операции.



RuPost предоставляет средства управления индивидуальным почтовым ящиком, доступным при клике на логине необходимого пользователя в списке почтовых ящиков.

2.14.6. Групповые политики

Для повышения удобства управления настройками больших наборов почтовых ящиков, в версии 3.1.0 добавлено понятие “Групповые политики”. Групповая политика – это специальная группа почтовых ящиков и набор значений параметров почтовых ящиков, который применяется ко всем почтовым ящикам, входящим в эту группу. При применении политики к конкретному почтовому ящику (добавлении ящика в группу), почтовому ящику автоматически присваивается набор значений параметров / свойств, задаваемый этой политикой. Например, Групповая политика квотирования задает квоту на размер почтового ящика - соответственно, при применении этой политики к какому-либо почтовому ящику у него будет установлено новое значение квоты, заданное в этой Групповой политике.

Для изменения параметров у каждого ящика в группе, администратору нет необходимости изменять индивидуальные свойства каждого почтового ящика, достаточно изменить параметры на уровне политики.

Все Групповые политики одного типа имеют одинаковый набор параметров, но могут иметь различные значения этих параметров. Для каждого типа, одна из политик является политикой по умолчанию. Для определения нескольких возможных вариантов значений параметров

администратор может создать несколько Групповых политик с различными названиями и различными значениями параметров.
Рассмотрим, как это работает на примере Групповых политик квотирования. Все Групповые политики квотирования имеют два параметра:

- Максимальный размер входящего письма;
- Максимальный размер почтового ящика.

Пусть политика квотирования “По умолчанию” будет иметь следующие значения параметров:

- Максимальный размер входящего письма = **3 MB**;
- Максимальный размер почтового ящика = **1 GB**.

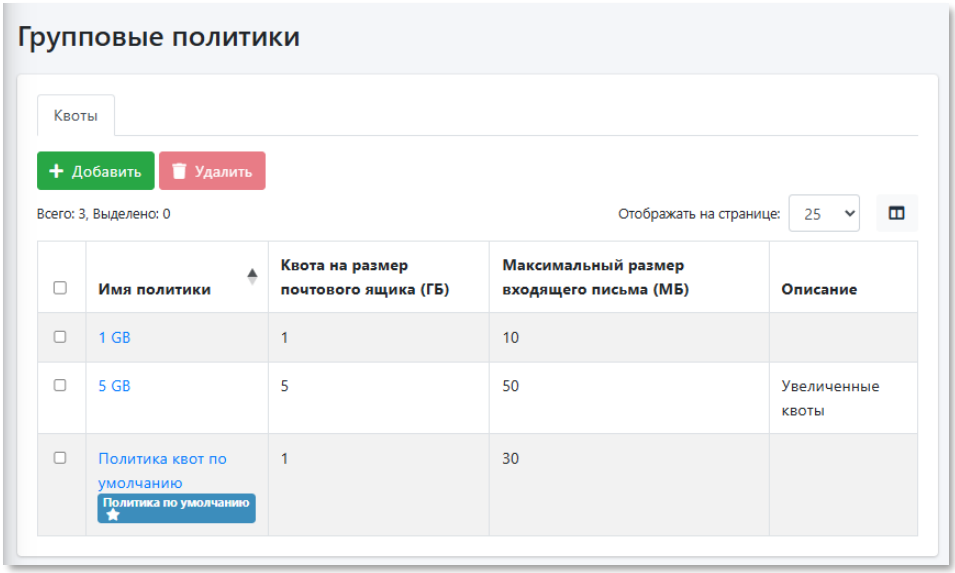
Если для части почтовых ящиков необходимо задать увеличенный размер квот, то нужно определить еще одну политику квотирования, например “Увеличенные квоты”, со значениями:

- Максимальный размер входящего письма = **5 MB**;
- Максимальный размер почтового ящика = **2 GB**.

Применяя к набору почтовых ящиков одну либо другую политику, администратор изменяет значения квот сразу у всех выбранных ящиков.

Политика “по умолчанию” автоматически применяется ко всем создаваемым почтовым ящикам.

Вызов страницы “Групповые политики” находится в главном меню в разделе “Получатели”:



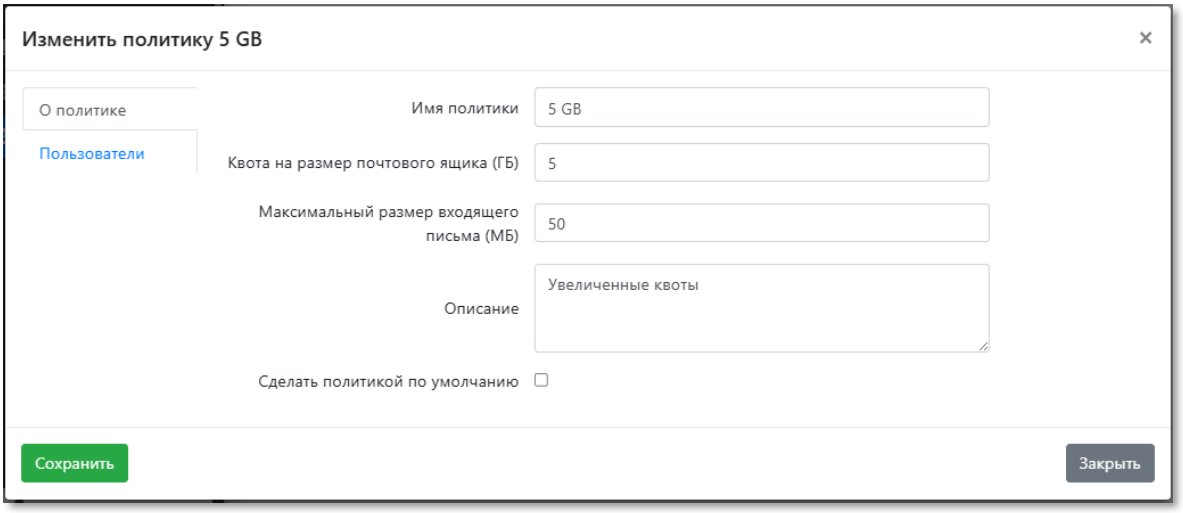
2.14.6.1. *Групповые политики – квотирование*

В версии 3.1.0 реализована Групповая политика квотирования, задающая два параметра:

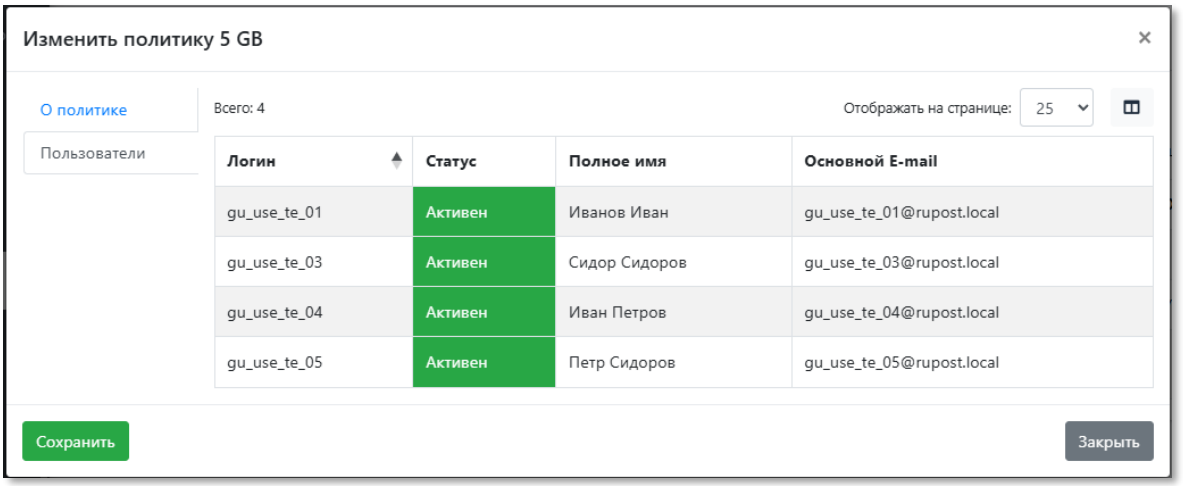
- Максимальный размер входящего письма;
- Максимальный размер почтового ящика.

В версии 4.0 добавлена возможность указывать размер квоты на размер почтового ящика, используя дробные значения.

Для добавления новой политики нажмите кнопку “Добавить”, для редактирования – нажмите на название выбранной политики.

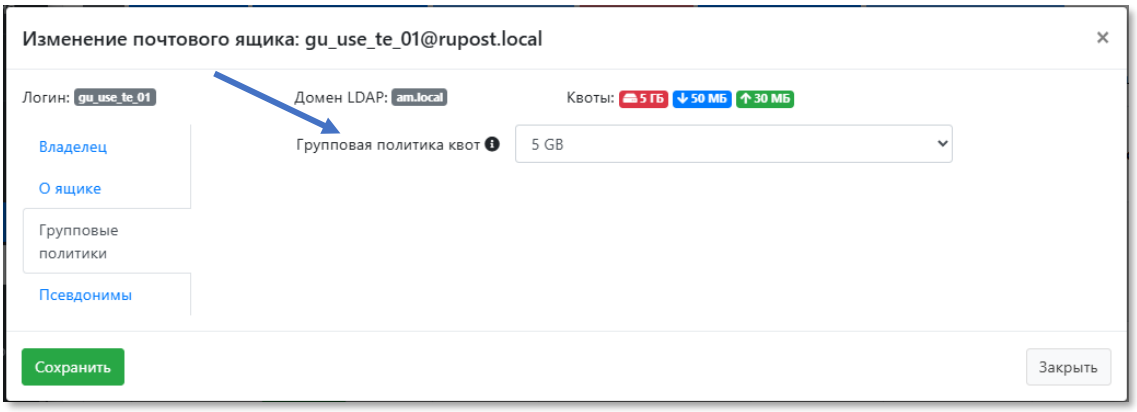


Список почтовых ящиков, к которым применена политика, можно просмотреть на закладке “Почтовые ящики”.

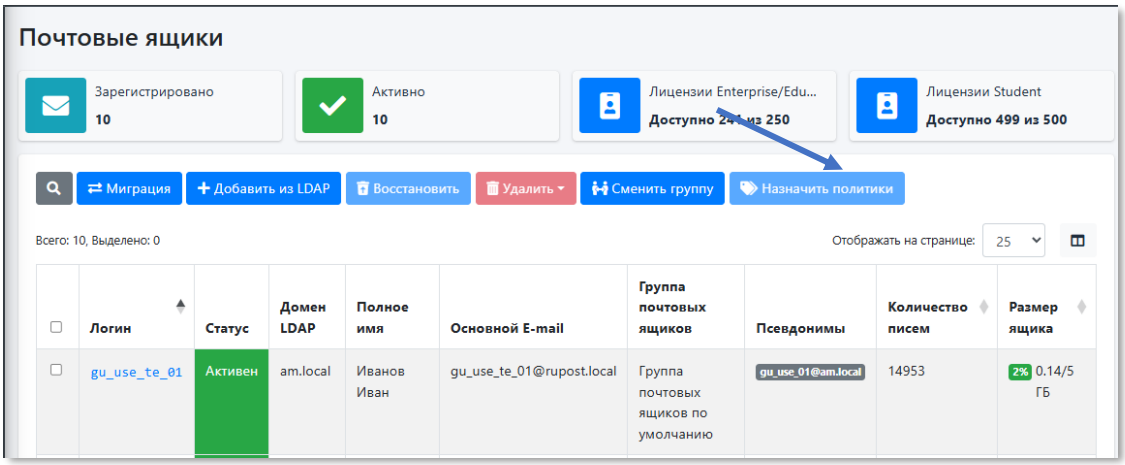


Для удаления политики, отметьте ее в списке политик и нажмите кнопку “Удалить”. Если в данный момент есть почтовые ящики, к которым применена эта политика, то, перед ее удалением, к этим ящикам нужно применить другую политику.

Применить политику к отдельному почтовому ящику можно в диалоговом окне свойств ящика



Применить политику к набору ящиков можно на странице “Почтовые ящики”, использовав групповую операцию “Назначить политики”.



2.14.7. Периодическая очистка папок “Удалённые” и “Спам”

В версии 4.1.0 добавлена периодическая очистка папок “Удаленные” и “Спам”.

Удаление писем из указанных папок производится один раз в сутки (в 02:15). После установки версии 4.1.0, по умолчанию, очистка этих папок отключена.

Для включения очистки выбранной папки, необходимо с помощью команды CLI настроить интервал времени очистки (в месяцах – от 1 до 36) для соответствующей папки.

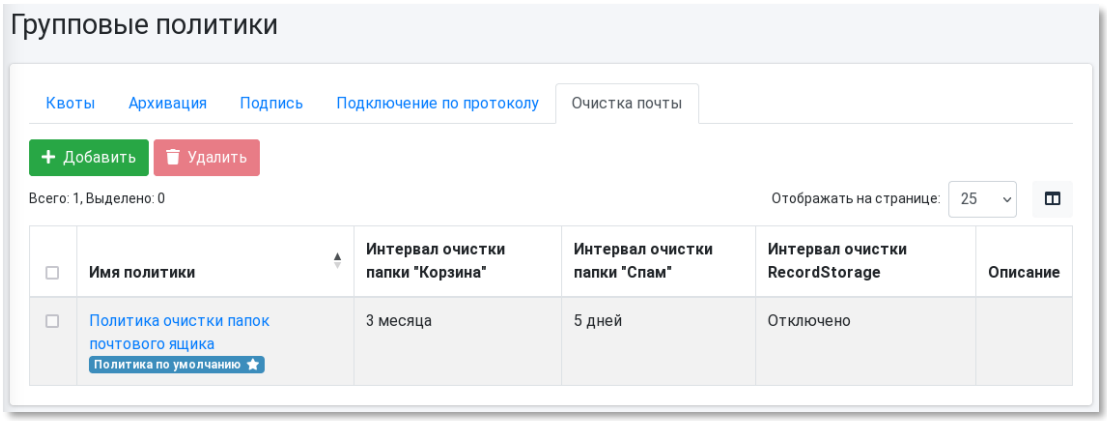
Например, для очистки папки “Спам” от писем, старше 3-х месяцев:

```
sudo rupost group-policy set-clean-spam --aging-period 3
```

Полный синтаксис команд и примеры их использования приведены в разделе **«rupost group-policy – Группа команд для работы с групповыми политиками»** Справочного руководство по командной строке.

Письма, находящиеся в этих папках и имеющие время создания, отстоящее от текущей даты на время большее выбранного интервала, будут удалены.

В версии 4.3.4 добавлена возможность задавать политики очистки почтового ящика в Панели управления.

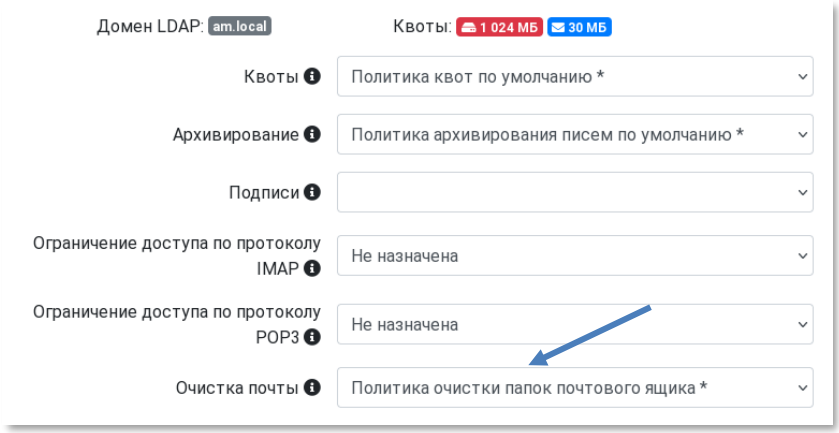


В политике можно указать интервала очистки следующих папок:

- Корзина.
- Спам.
- Записи (Record Storage).

Интервал можно задавать в днях, месяцах и годах.

Политику очистки можно назначить почтовому ящику также, как и другие политики.



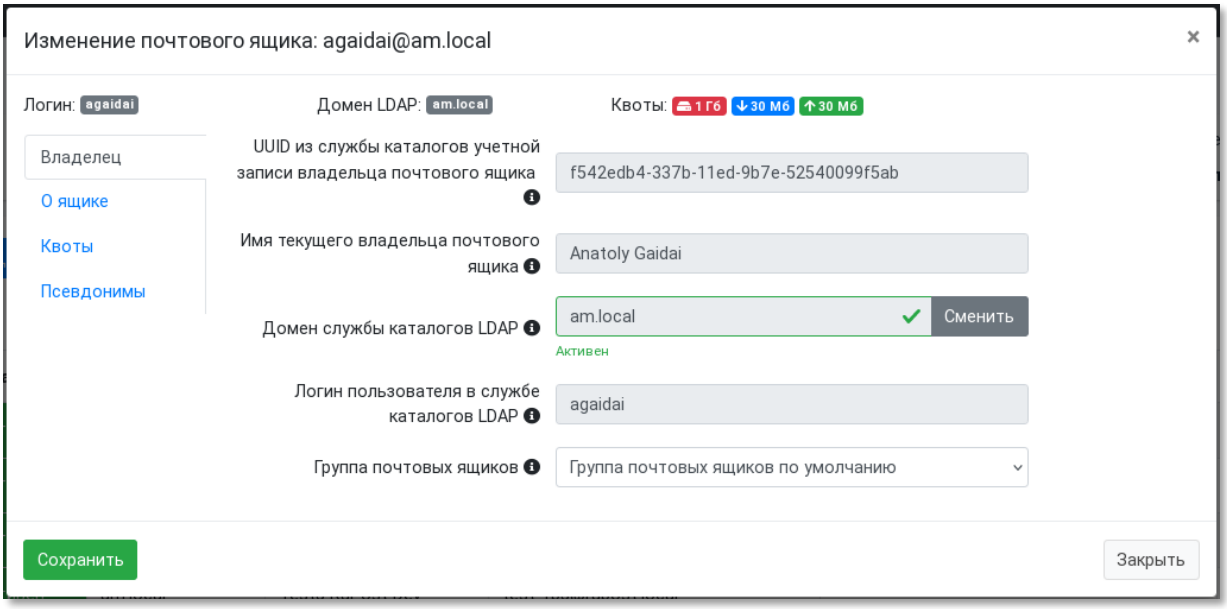
В ходе очистки, в соответствии с назначенной политикой, письма, находящиеся в указанной папке и имеющие дату получения ранее указанного интервала, будут удалены.

Процедура очистки работает один раз в сутки (в 02:15) - сначала произойдет архивирование и, после его окончания, произойдет очистка.

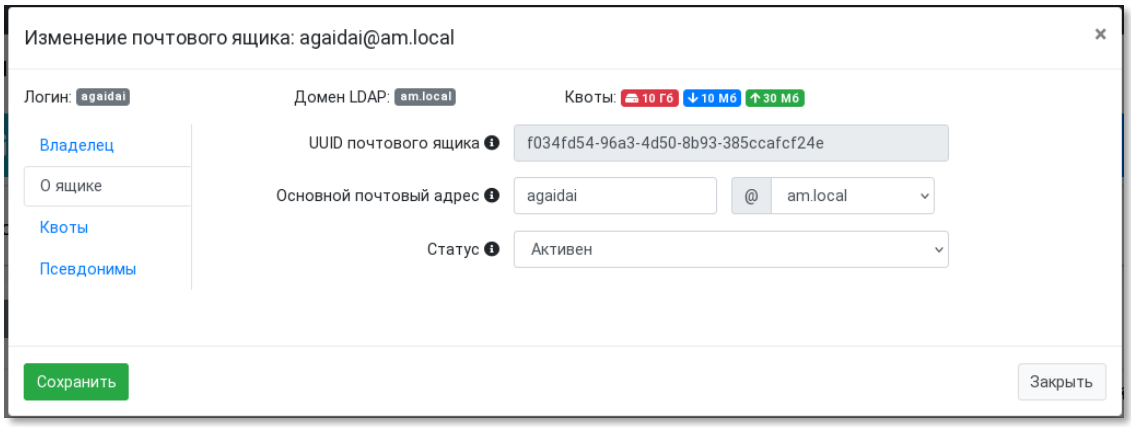
2.14.8. Управление почтовым ящиком пользователя

Диалог управления почтовым ящиком включает в себя информацию об учетной записи владельца ящика в корпоративной службе каталогов и возможности изменения основного e-mail.

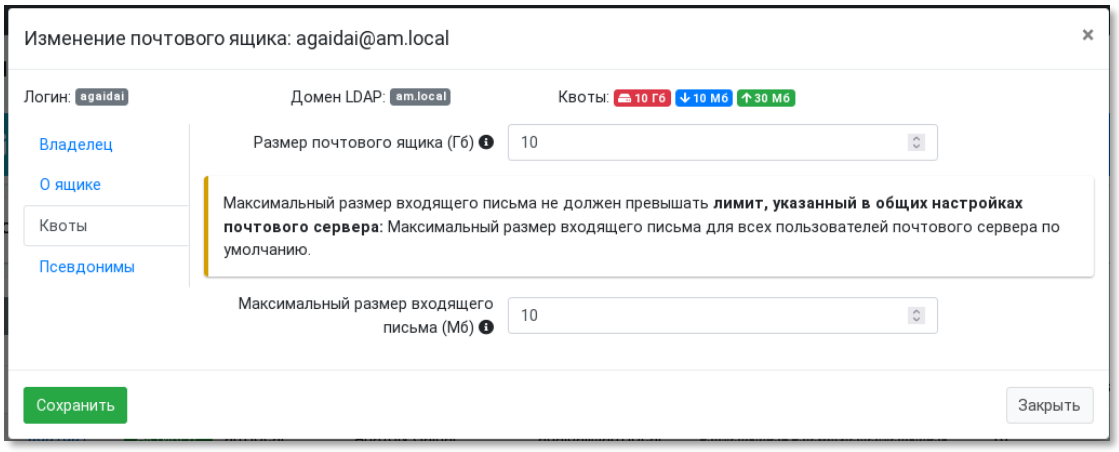
Вкладка диалога управления почтовым ящиком “Владелец” включает в себя информацию об учетной записи владельца ящика в корпоративной службе каталогов, включающая LDAP UUID – уникальный идентификатор пользователя в службе каталогов, которому принадлежит почтовый ящик.



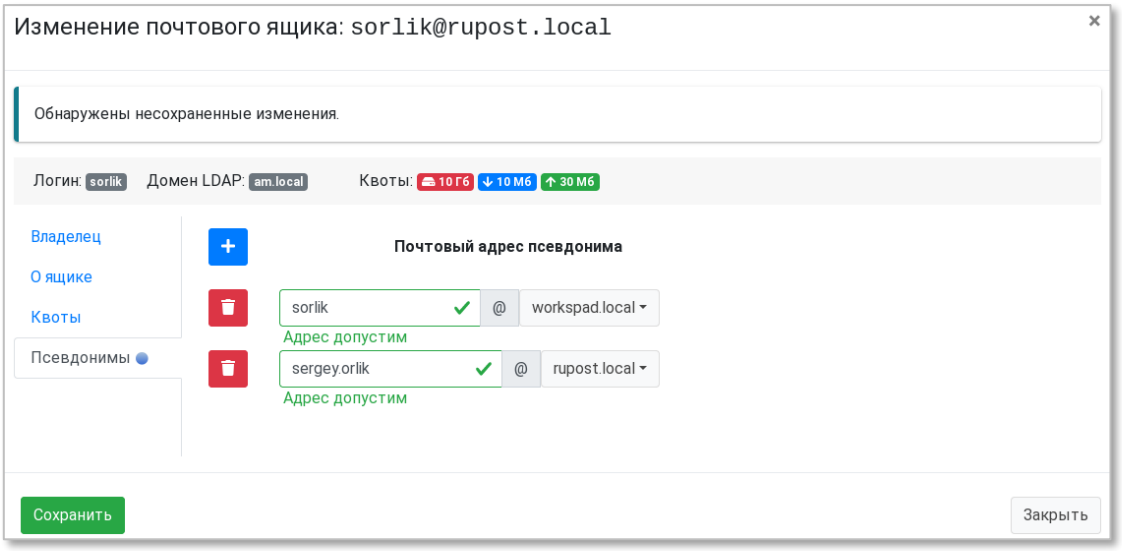
Вкладка диалога управления почтовым ящиком “О ящике” отражает информацию об уникальном идентификаторе UUID ящика, основной e-mail и статус почтового ящика.



Для выбранного почтового ящика на вкладке “Квоты” возможно индивидуальное задание максимального размера ящика и входящего письма, которые по умолчанию определяются на уровне почтового домена, используемого для основного e-mail.

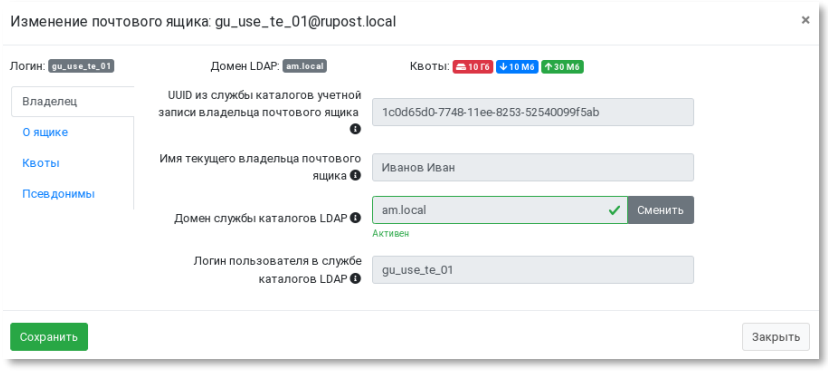


Вкладка “Псевдонимы” позволяет задать дополнительные почтовые адреса – алиасы. Редактор псевдонимов проверяет допустимость почтовых адресов-псевдонимов.



2.14.9. Замена “владельца” почтового ящика

В версии 2.7.0 добавлена возможность смены пользователя LDAP для выбранного почтового ящика. Для того, чтобы сменить пользователя, нужно в свойствах почтового ящика выбрать другого пользователя из списка пользователей LDAP нажав на кнопку “Сменить”.

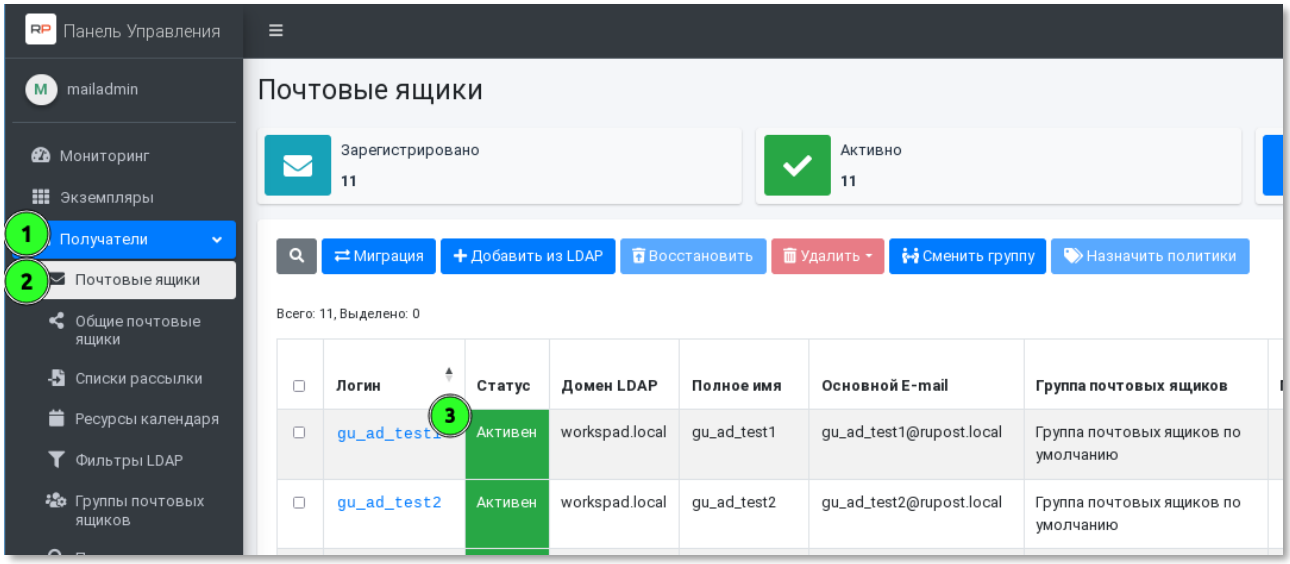


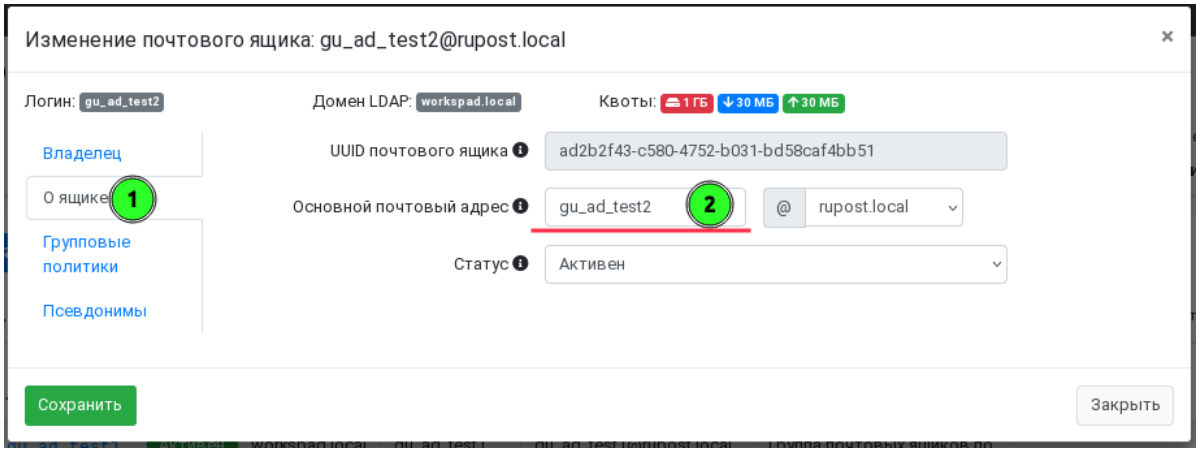
Пользователей можно выбирать как из текущей службы каталогов, так и из другого домена LDAP. Список пользователей содержит только пользователей (записи LDAP) у которых нет почтового ящика. Новый “владелец” ящика получает все текущие почтовые атрибуты ящика (основной адрес электронной почты и псевдонимы). Соответственно, у предыдущего “владельца” эти атрибуты очищаются.

2.14.10. Переименования “владельца” почтового ящика (смена фамилии и почтового адреса)

При переименовании пользователя в LDAP связанной, например, со сменой фамилии или действиями со сменой учетных данных (имя пользователя, логин т.п.) которые влекут за собой смену e-mail адреса необходимо придерживаться следующего порядка действий:

- Переименовать пользователя средствами LDAP без изменения почтового адреса.
- На одном из узлов кластера выполнить синхронизацию LDAP каталога (команда CLI rupost ldap sync).
- В свойствах переименовываемой учетной записи на закладке "О ящике" сменить почтовый адрес.





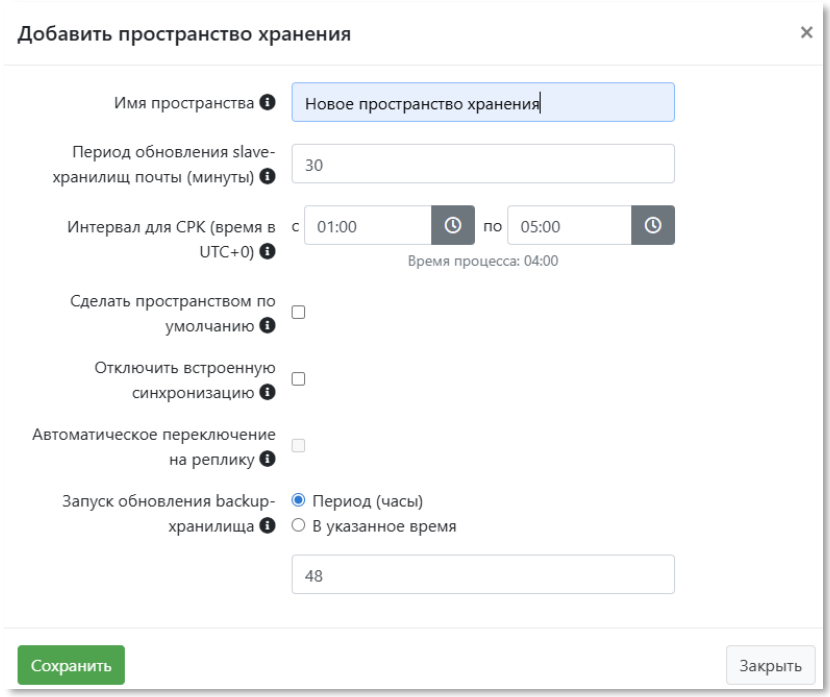
2.14.11. Перенос почтового ящика в другое пространство хранения

Внимание!

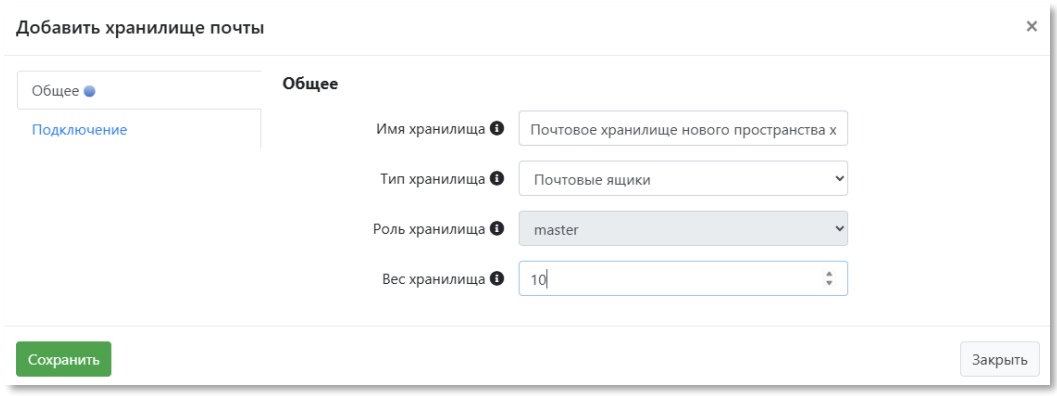
При изменении группы для почтового ящика на время переноса почтовый ящик будет недоступен.

Необходимые условия:

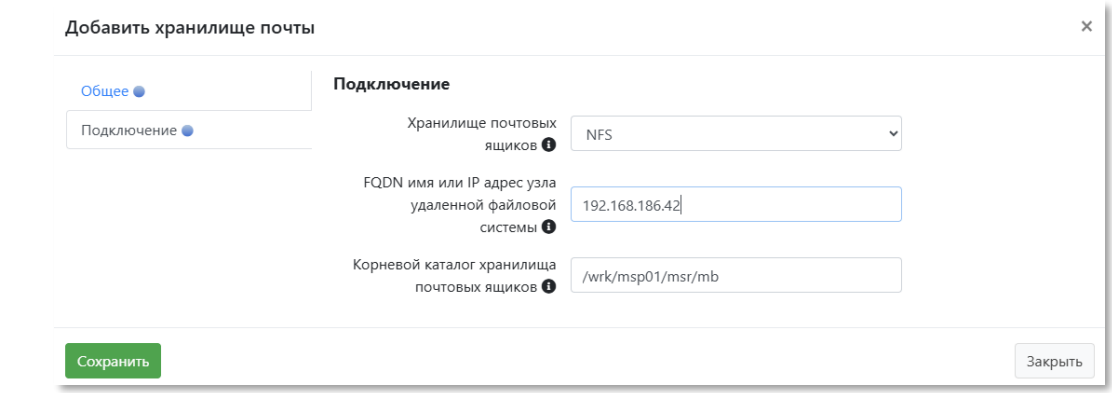
- **создано новое пространство хранения**
  открыть «Настройки» -> «Пространства хранения» -> «Добавить пространство»

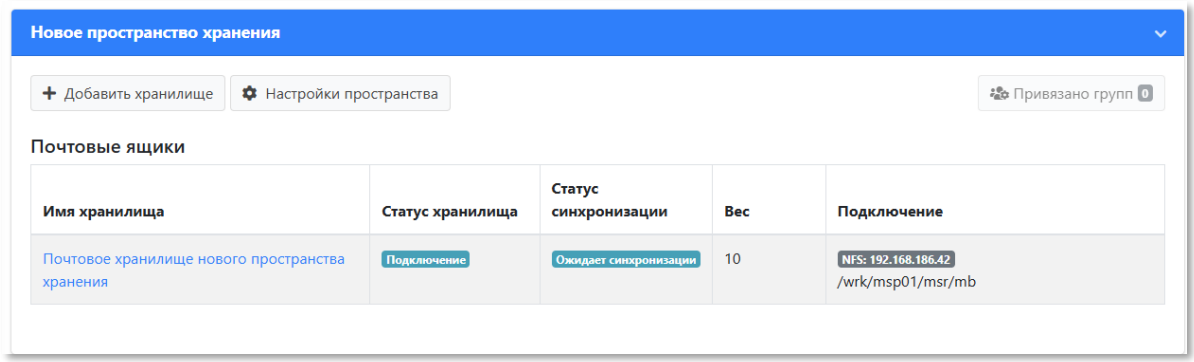


- **создано хотя бы одно хранилище в новом пространстве хранения**
  «Добавить хранилище» указать название, тип, вес

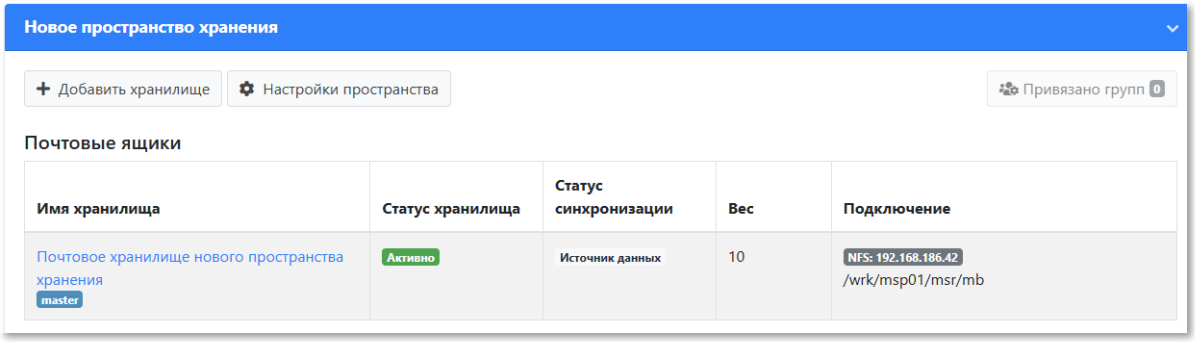


  добавить информацию о подключении хранилища

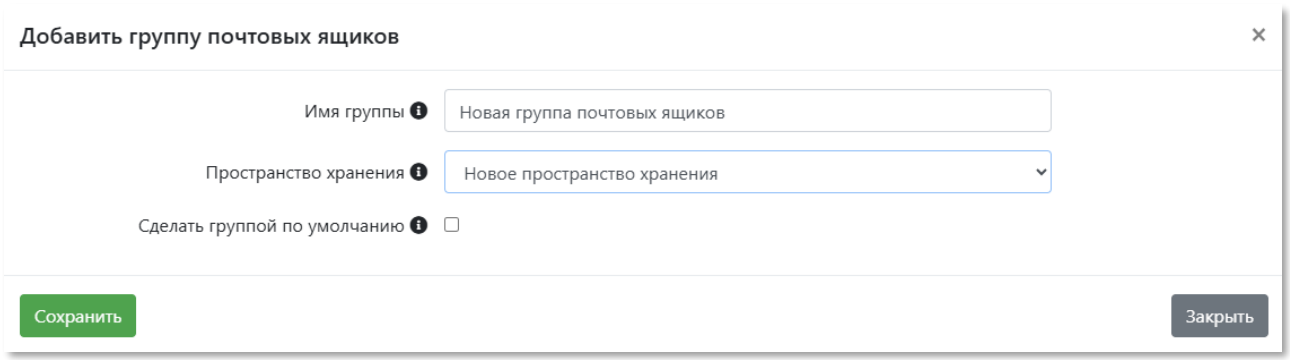




Убедиться, что статус нового хранилища «Активно»

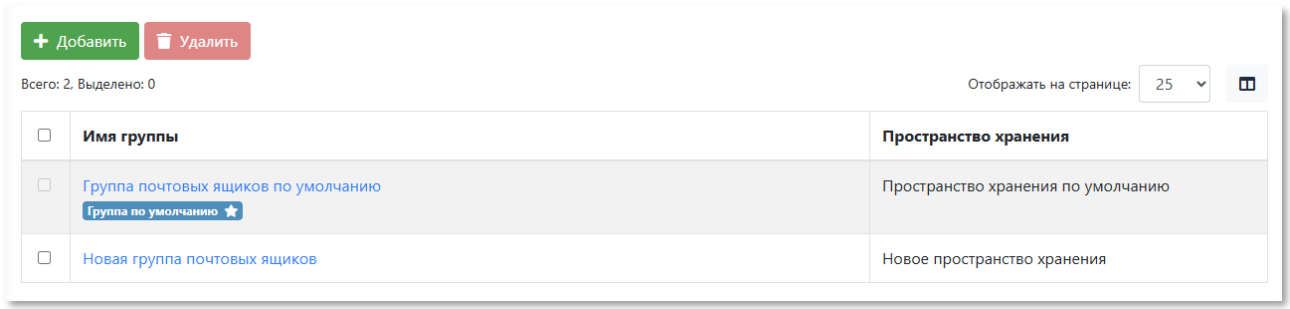


- **создана новая почтовая группа**
  «Получатели» -> «Группы почтовых ящиков» -> «Добавить»



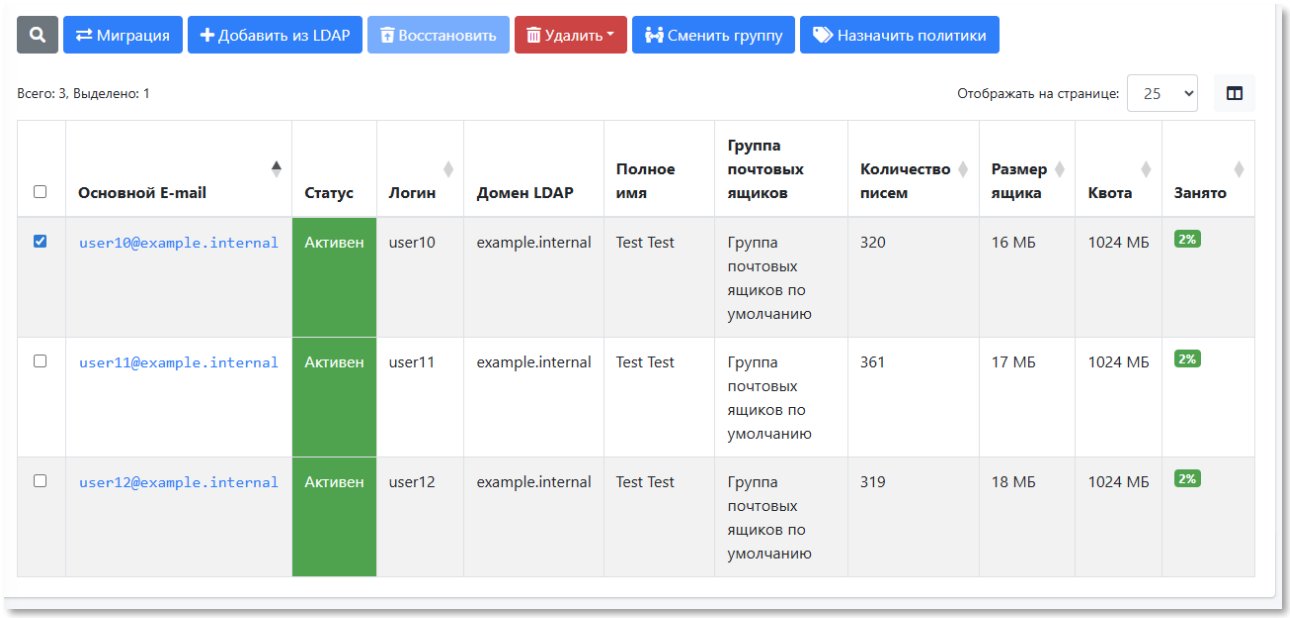
указать название группы и новое пространство хранения

- **новая почтовая группа привязана к новому пространству хранения**

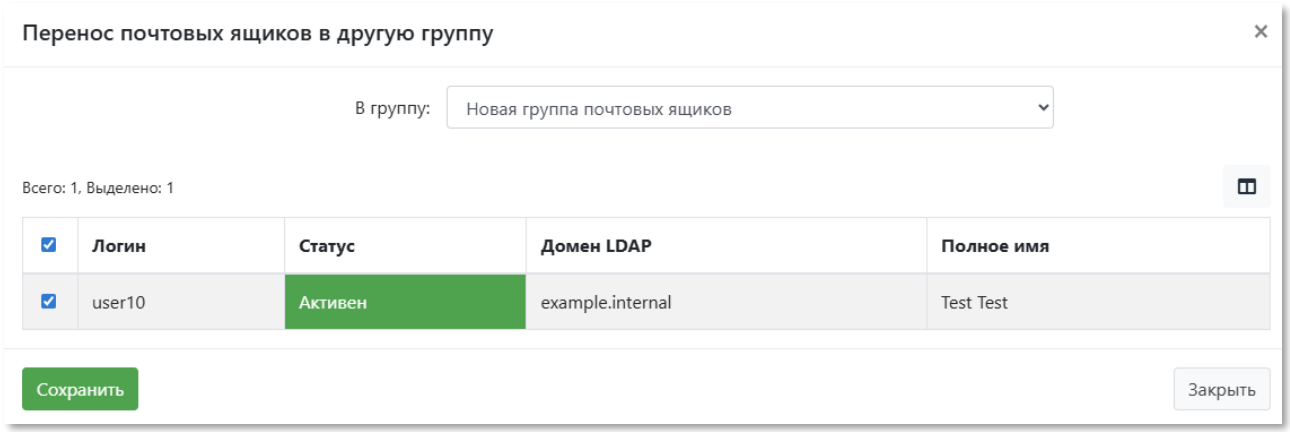


Для переноса почтового ящика в другое пространство хранения необходимо выполнить следующие действия:

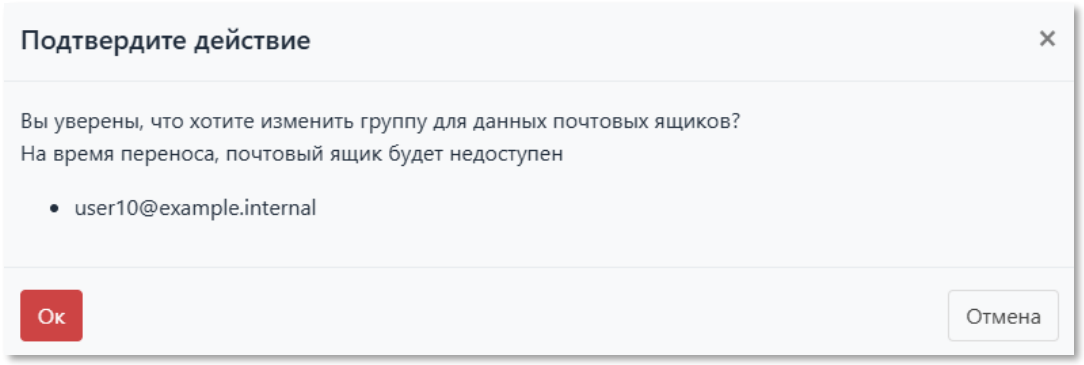
- **выбрать ящик для переноса в новое пространство хранения**
  «Получатели» » -> «Почтовые ящики» выделить ящик для переноса



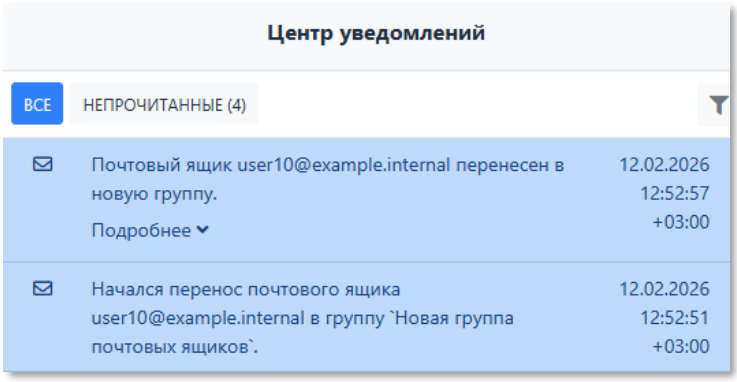
- **выполнить перенос ящика в новое пространство хранения**
  «Сменить группу» для выбранного ящика на новую и выбрать «Сохранить»



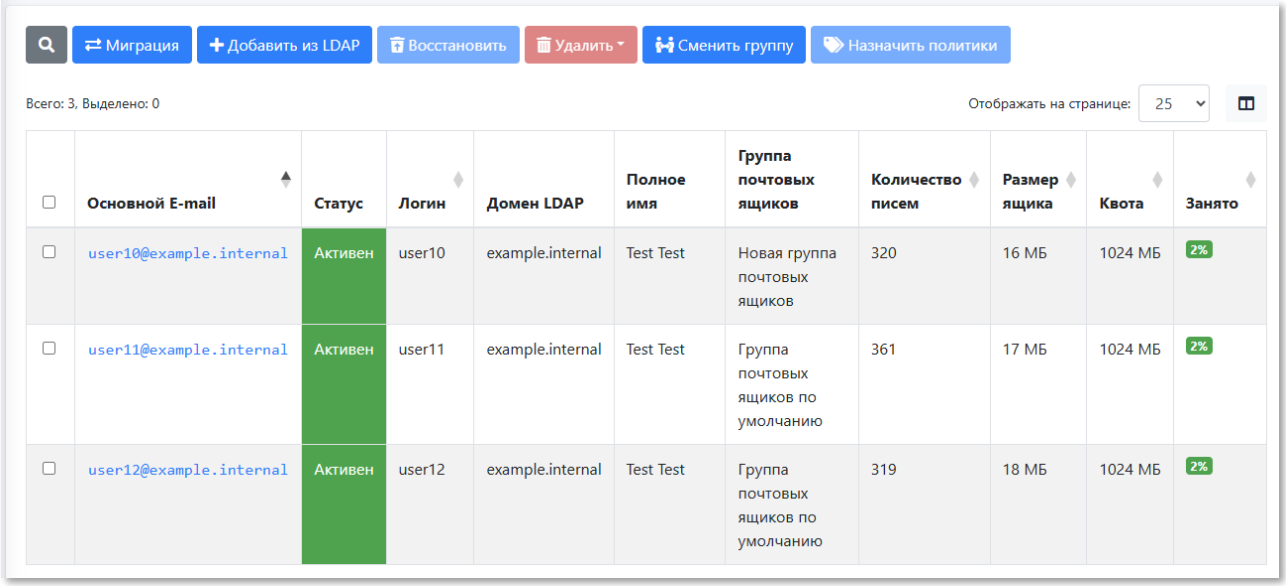
подтвердить выполнения действия



дождаться завершения переноса ящика, соответствующие сообщения будут отображаться в центре уведомлений



почтовый ящик успешно перенесен в новое пространство хранения



2.14.12. Синхронизация с LDAP

В версии RuPost 2.2.1 добавлена синхронизация данных почтовых ящиков с LDAP. Синхронизация выполняется автоматически каждые 6 часов. При необходимости оперативной синхронизации с LDAP можно воспользоваться командой CLI.



Синтаксис команды и примеры управления синхронизацией с LDAP из командной строки приведены в разделе **«rupost ldap группа команд для управления взаимодействия с LDAP»** Справочного руководство по командной строке.

В версию 4.1.0 добавлена команда CLI по управлению периодом синхронизации с LDAP.

Пример команды для установки интервала синхронизации LDAP равного 6-ти часам:

```
sudo rupost ldap-sync-settings-interval set 6
```



Полный синтаксис команд и примеры их использования приведены в разделе **«rupost ldap-sync-settings-interval – Настройка интервала времени синхронизации с LDAP»** Справочного руководство по командной строке.

2.14.12.1. *Мониторинг изменений атрибутов LDAP*

В версии 3.3.0 добавлен мониторинг наличия изменений в ключевых атрибутах учетной записи пользователей в LDAP. Проверка проводится при каждом выполнении синхронизации учетных записей с LDAP (LDAP sync).

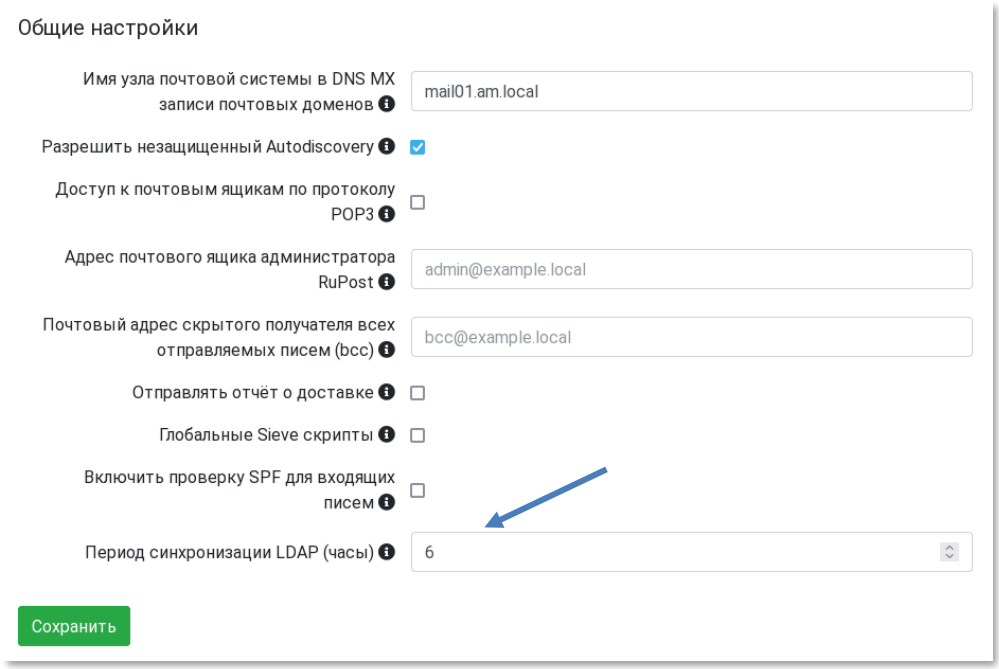
Контролируются следующие атрибуты и статусы записей LDAP:

- Удаление записи
- Статус блокировки записи
- Значение атрибута mail
- Записи в атрибуте proxyAddresses

При обнаружении изменений в LDAP, внесенных внешними системами, об этом делается запись в infrastructure.log.

В версии 4.3.4 добавлена возможность управлять периодом синхронизации данных с LDAP в Панели управления.

Для того, чтобы задать интервал синхронизации с LDAP серверами, необходимо открыть вкладку “Общие” на странице “Общие настройки”.



2.14.12.2. *Работа с LDAP в режиме “только чтение”*

В версии 3.3.0 обеспечивается работа RuPost с LDAP серверами в режиме “только чтение” – т.е. когда сервисная учетная запись, под которой RuPost подключается к серверу LDAP, не имеет прав на внесение изменений. Соответственно, в этом режиме, RuPost не имеет возможности изменять значения атрибутов LDAP, поэтому все необходимые изменения должны делаться при помощи внешних инструментов.

Например, перед добавлением нового почтового ящика, в LDAP должен быть занесен первичный почтовый адрес – как в атрибут mail, так и в атрибут proxyAddresses (строка, начинающаяся на “SMTP:”).

2.14.13. Перенос почтового ящика из одного каталога LDAP в другой при синхронизации

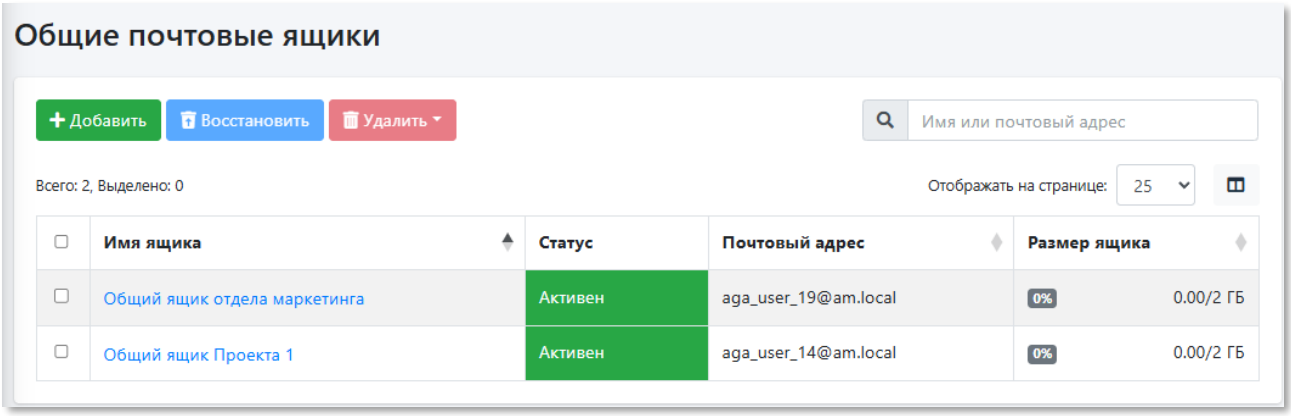
В версии 2.7.0 в процедуру синхронизации с LDAP добавлена возможность автоматической перепривязки почтового ящика к другому пользователю LDAP с совпадающим основным адресом электронной почты. Это позволяет осуществить быстрое переключение почтовых ящиков, обслуживаемых одним каталогом LDAP в другой – например, из Microsoft AD в ALD Pro. Для этого нужно в целевом LDAP каталоге создать записи о пользователях с сохранением основного адреса электронной почты, заблокировать эти же записи в исходном каталоге и запустить синхронизацию с LDAP.



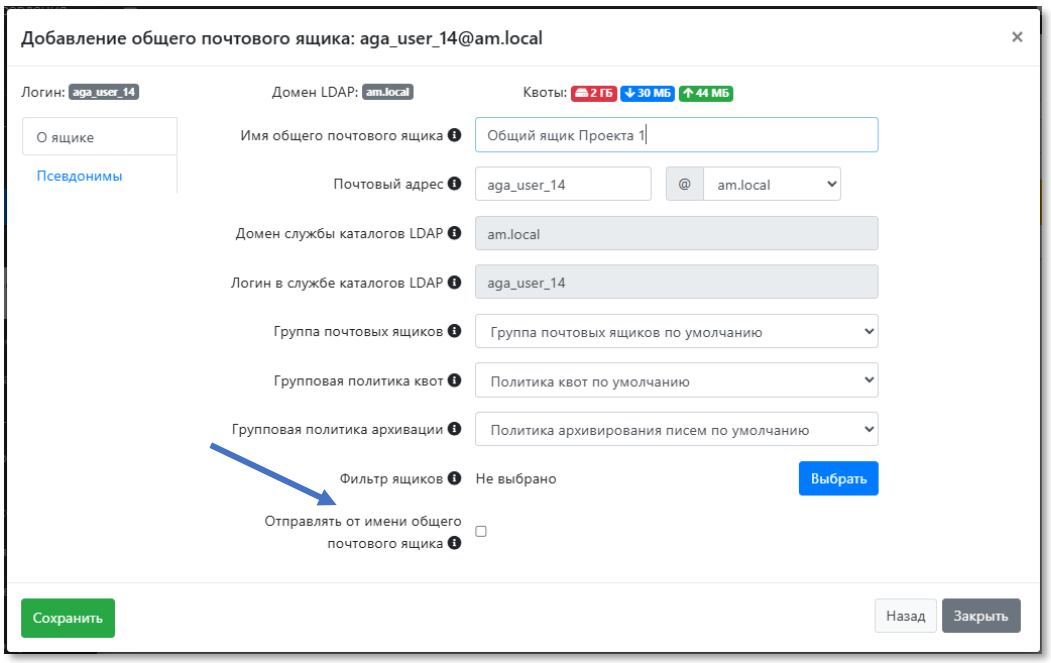
Синтаксис команды и примеры управления синхронизацией с LDAP из командной строки приведены в разделе **«rupost ldap группа команд для управления взаимодействия с LDAP»** Справочного руководство по командной строке.

2.14.14. Динамические общие почтовые ящики

В версии 3.2.0 добавлено управление Общими ящиками.



Общий ящик – это полнофункциональный почтовый ящик, к которому при помощи Панели управления предоставляется доступ для группы пользователей. Администратор имеет возможность управлять составом группы пользователей с помощью соответствующего Фильтра ящиков.

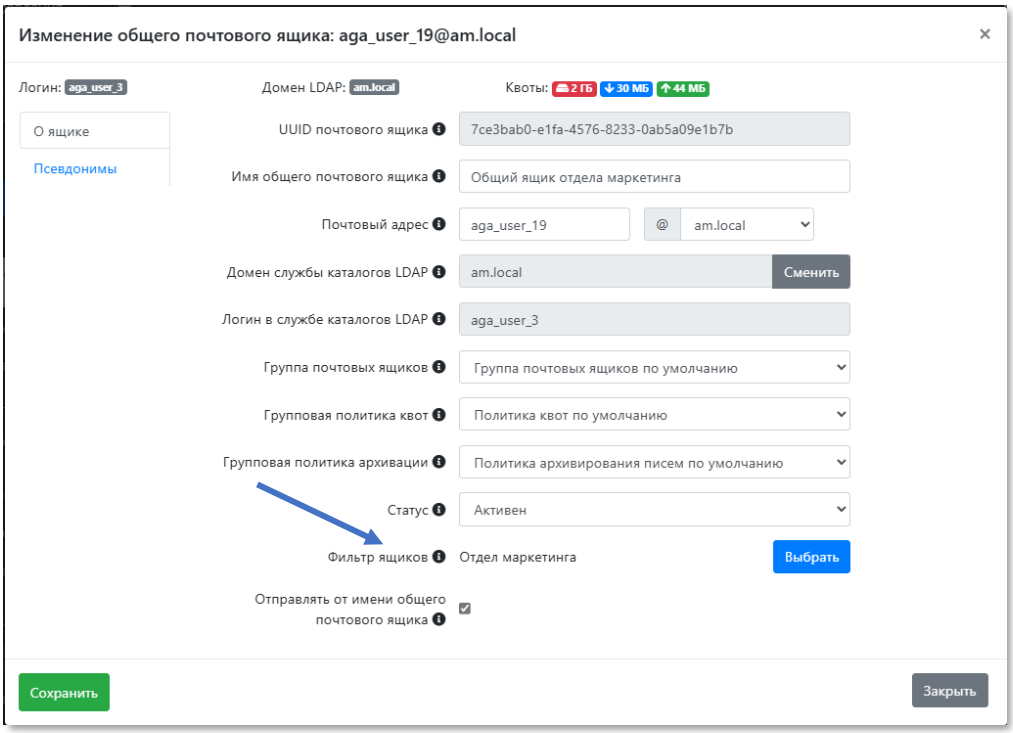


Пользователи Общего ящика имеют права “полный доступ” – т.е. могут создавать и удалять папки и письма, а также пользоваться календарем и адресной книгой.

Если включена настройка “Отправлять от имени общего почтового ящика”, то пользователи могут отправлять почту от имени Общего ящика. При отправке от имени Общего ящика, отправленное письмо будет скопировано в папку “Отправленные” Общего ящика.

Общие ящики, управляемые с помощью Фильтра ящиков, являются “динамическими” (по аналогии со списками рассылки) – так как, если Фильтр ящиков включает в себя один или несколько LDAP

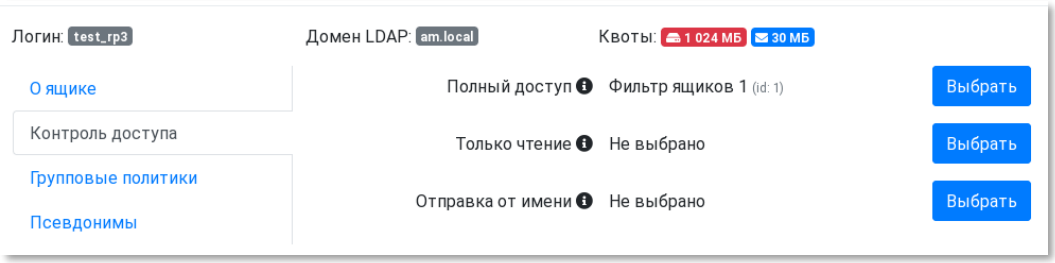
фильтров, то группа пользователей, которым предоставлены права на Общий ящик, будет периодически обновляться (период обновления – 6 часов).



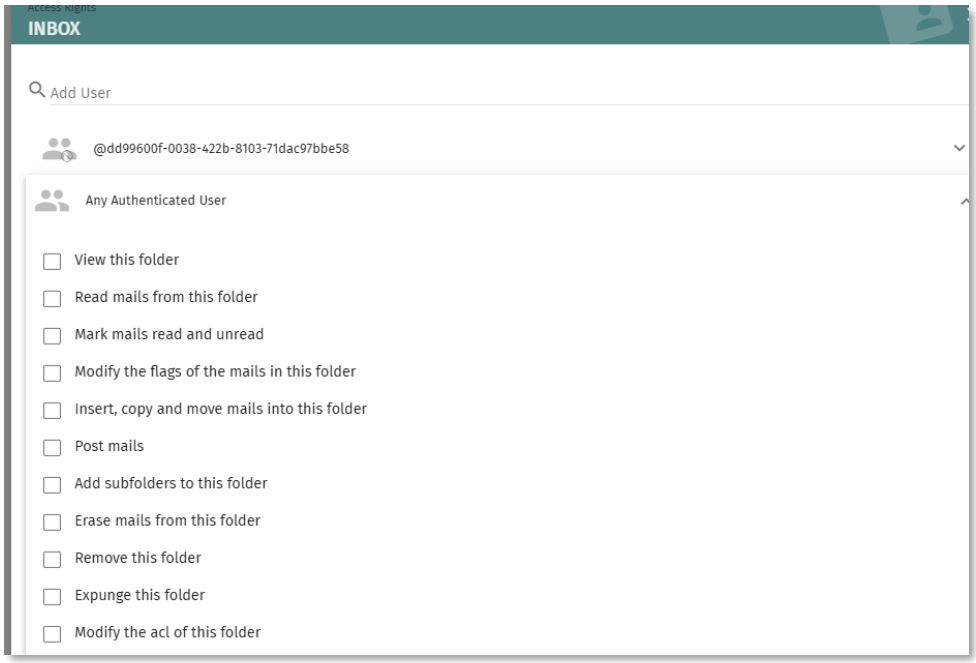
В версии 4.3.4 расширены возможности по управлению доступом к общим почтовым ящикам.

Доступ управляется при помощи фильтров ящиков в трех категориях:

- **Полный доступ** – пользователи, прошедшие через фильтр, получают права полного доступа к почте, календарям и адресным книгам общего ящика.
- **Доступ на чтение** - пользователи, прошедшие через фильтр, получают доступ только на чтение. Полный доступ имеет приоритет, поэтому, если пользователь получает права и на чтение и полный доступ, то итоговый его доступ – полный.
- **Отправка от имени** - пользователи, прошедшие через фильтр, получают право отправки писем от имени общего ящика.



При необходимости передать управление Общим ящиком выделенному пользователю (например, если Общий ящик создан для какого-либо проекта и управлять доступом к нему должен руководитель этого проекта) можно создать Общий ящик **без указания Фильтра ящиков**. В этом случае, управлять правами доступа можно с помощью веб-клиента, от имени владельца этого ящика. Например, ниже приведен набор прав, которыми можно управлять для папки “Inbox”.



Внимание!

Если в свойствах Общего ящика указан Фильтр ящиков, то права, выданные пользователям при помощи веб-клиента, будут перезаписаны системой.

В версии 3.3.0 добавлена поддержка инструмента миграции из Microsoft Exchange в части переноса Общих ящиков.

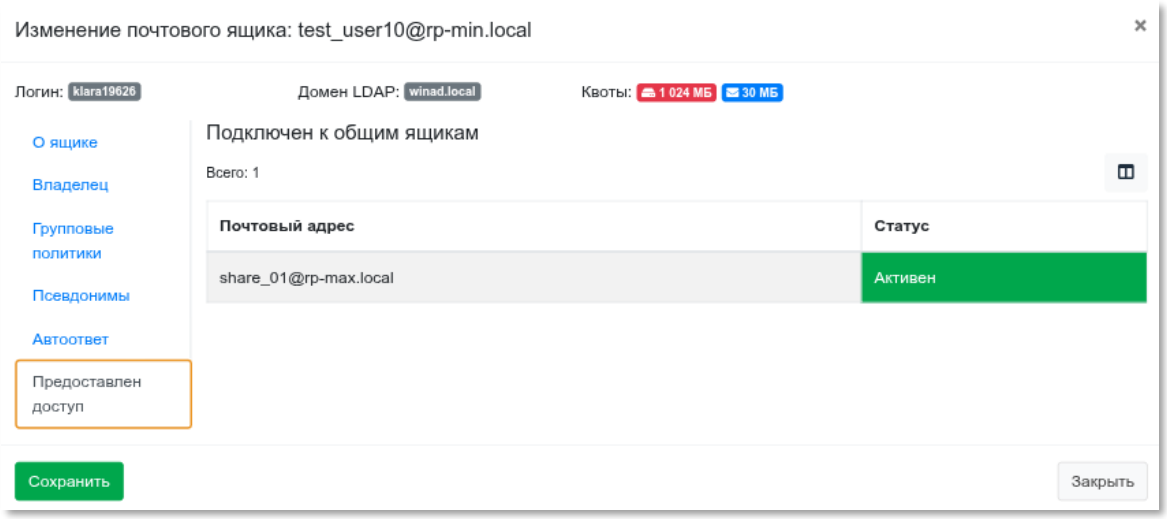
Для миграции Общего почтового ящика необходимо:

1. Перед началом работы по миграции Общего ящика, необходимо для выбранного ящика в Active Directory задать пароль доступа и снять флаг ACCOUNTDISABLE в атрибуте UserAccountControl.
2. Добавить в RuPost посредствам CLI или Панели управления Общий почтовый ящик и ящики владельцев в статусе «Миграция».
3. В инструменте миграции добавить в очередь на миграцию ящики владельцев и Общий почтовый ящик.
4. Произвести миграцию этих ящиков.
5. В Панели управления RuPost создать фильтр ящиков, включающих ящики владельцев - для доступа к Общему почтовому ящику.
6. В свойствах Общего ящика добавить фильтр ящиков, созданный на предыдущем шаге.

2.14.15. Отображение списка общих почтовых ящиков, к которым предоставлен доступ

В версии 4.2.0 добавлена возможность просмотреть список общих почтовых ящиков, к которым есть доступ у данного пользователя (ящика).

Для того, чтобы просмотреть список общих почтовых ящиков, к которым имеется доступ, нужно в окне “Свойства ящика” перейти на вкладку “Предоставлен доступ”.


Изменение почтового ящика: test_user10@rp-min.local
Логин: klara19626
Домен LDAP: winad.local
Квоты: 1 024 МБ 30 МБ
О ящике
Владелец
Групповые политики
Псевдонимы
Автоответ
Предоставлен доступ
Подключен к общим ящикам
Всего: 1
Почтовый адрес
Статус
share_01@rp-max.local
Активен
Сохранить
Закрыть

2.15. Учетная запись имперсонации

Внимание!

УЗ имперсонации не тратит лицензию и не учитывается при подсчёте почтовых ящиков.

Начиная с версии 2.2.3 в команду управления учетной записью имперсонации **impersonation set** внесены следующие изменения:

- Удален параметр primary_email – теперь учетная запись имперсонации задается с помощью ключа **-u / --user**.
- Добавлен обязательный параметр **-u / --user** – при активации учетной записи имперсонации нужно указать логин этой учетной записи.
- Запрос пароля происходит после ввода команды, пароль при вводе маскируется символами * и не запоминается в истории команд.
- Добавлен не обязательный параметр **-c / --calendar** – этот параметр должен быть установлен для автоматической обработки входящих почтовых сообщений, содержащих календарные события.
- Добавлен ключ **–f / --force** для принудительного назначения аккаунта имперсонации, при этом игнорируется любая предыдущая запись.

Внимание!

Убедитесь, что срок действия пароля учетной записи имперсонации не закончился и, в случае изменения ее пароля, своевременно обновляйте эти данные при помощи RuPost CLI для исключения нарушений в работе RuPost.

Внимание!

После присвоения аккаунта имперсонации требуется переразвернуть конфигурацию.



Синтаксис команды и примеры управления учетной записью имперсонации из командной строки приведены в разделе **«rupost impersonation группа команд для управления аккаунтом имперсонации»** Справочного руководство по командной строке.

2.16. Автоматическая обработка входящих сообщений, содержащих календарные события

В версии 2.2.3 добавлена автоматическая обработка входящих сообщений с календарными событиями, полученных от внешних адресатов. При получении такого сообщения (например, приглашения на собрание, обновление или отмена ранее созданной встречи), RuPost анализирует календарное событие и создает его или обновляет статус этого события в календаре пользователя. Таким образом, календарное событие отображается в календаре пользователя даже если он, пока что, не принял приглашения.

Обработка происходит в момент прихода письма в почтовый ящик пользователя, поэтому письма с календарными событиями, полученные пользователями до включения автоматической обработки остаются не обработанными и, соответственно, календарные события в календарь добавлены не будут.

Включение данной функциональности производится с помощью ключа **-c / --calendar** команды CLI **impersonation set**:

```
rupost impersonation set -u [УЗ имперсонации] -p [пароль УЗ имперсонации] -c
```

Внимание!

Если автоматическая обработка входящих событий не будет включена, то календарные события не будут отображаться в календарях пользователей автоматически!

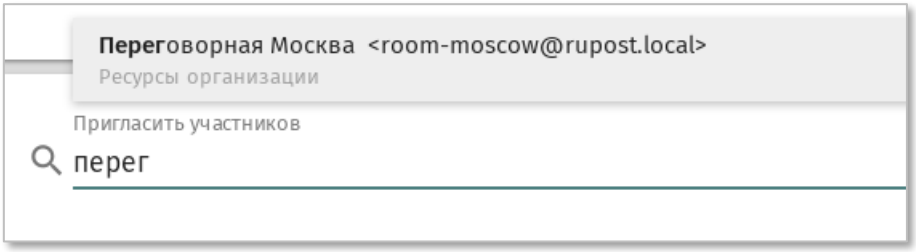
Приглашения и обновления календарных событий, полученные до включения данной функциональности, не будут обработаны.

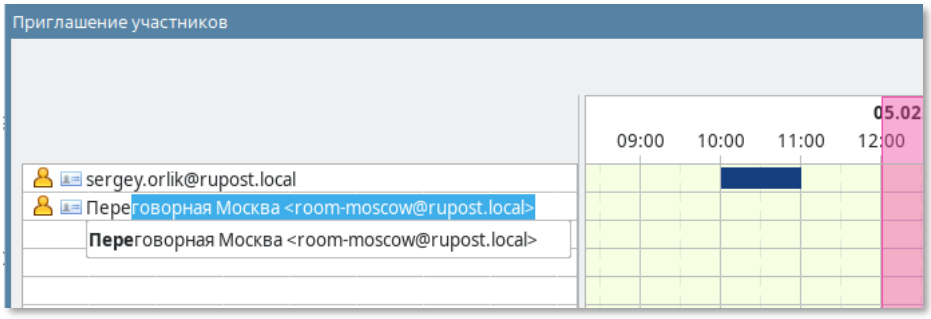
В версии 4.3.4 расширена функциональность автоматического добавления событий в календарь при получении внешних приглашений (отправленных из необслуживаемых почтовых доменов), отправленных на псевдонимы.

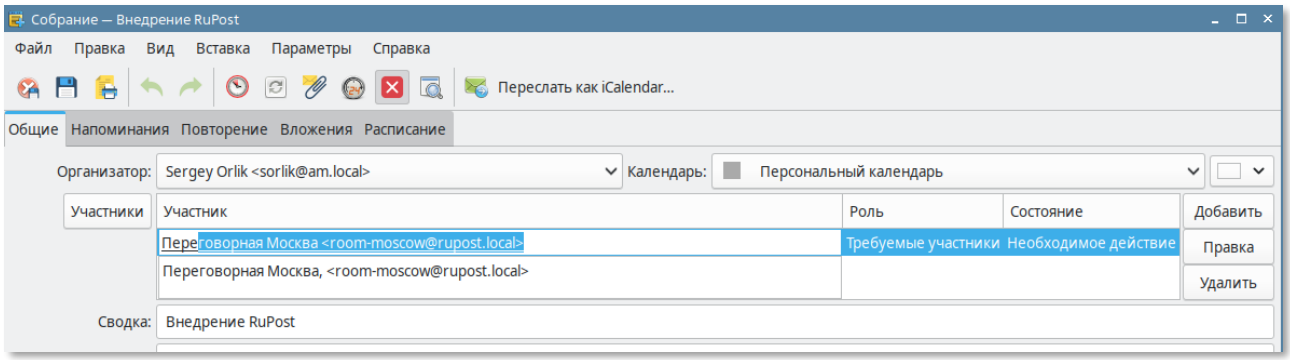
2.17. Ресурсы календаря

В понимании системы Ресурсы — это пользователи почтовой системы, которые автоматически отвечают на приглашения участвовать в событиях.

Ресурсы доступны при заведении календарных событий в клиентских приложениях при выборе участников, наравне с обычными пользователями. Все ресурсы, заводимые в системе, доступны в дополнительной адресной книге “Ресурсы организации”, автоматически создаваемой RuPost. Ниже приведены примеры отображения подсказок выбора ресурсов из дополнительной адресной книги в Web-клиенте, Thunderbird и Evolution.







Управление ресурсами календаря реализовано в виде набора команд CLI.

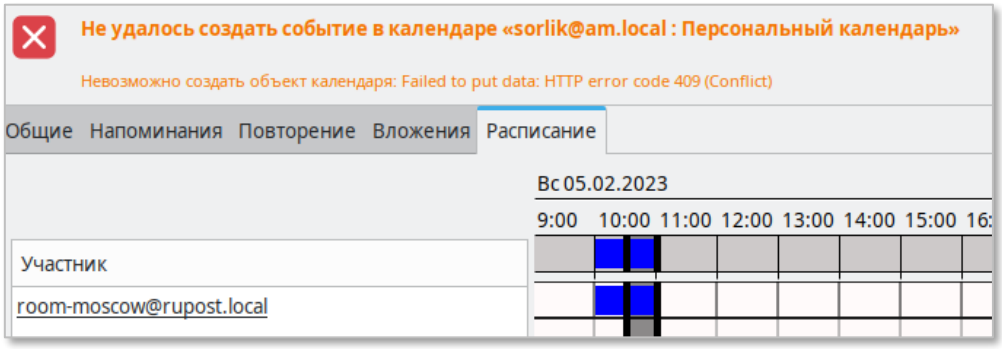
Объектами ресурсов могут быть сущности трёх видов:

- `location` — комната или помещение.
- group — группа, может быть востребована для некоторых сценариев.
- thing — предмет, например, проектор.

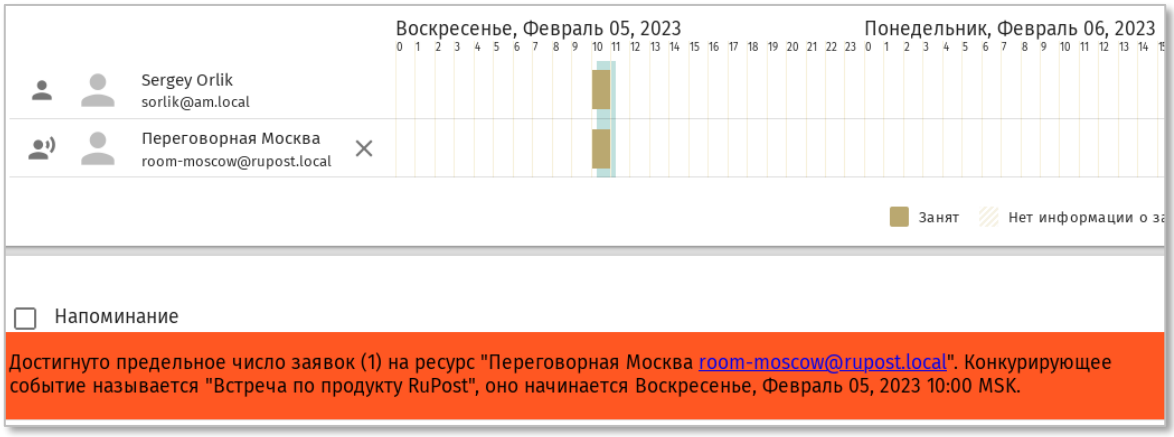
Система поддерживает три стратегии автоматического ответа на приглашения:

- `ones` — в один промежуток времени ресурс может стать участником только одного события, остальные заказы отклоняются (наиболее подходящий сценарий для комнат).
- `nolimit` — без ограничений, т.е. отвечает на события в параллельное время столько раз, сколько его закажут (например, подходит для бронирования участия в рабочих группах).
- `nolimit_busy`— выводится предупреждение при попытке забронировать параллельно в одно время, но событие всё равно создаётся.

При попытке бронирования уже занятого ресурса в стратегии `ones` будет невозможно создать событие с использованием данного ресурса.

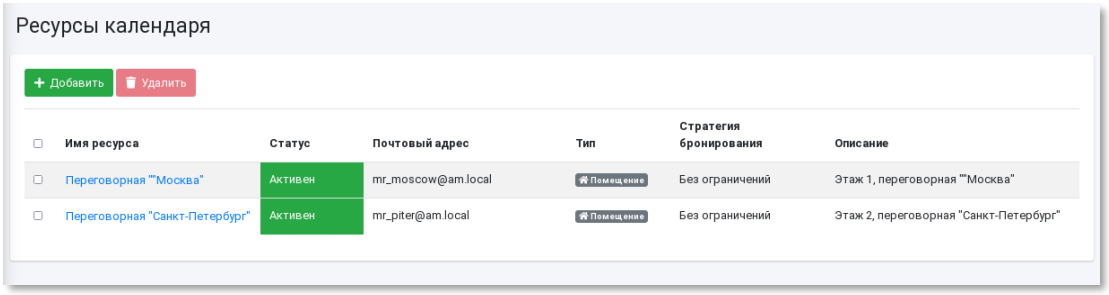


В web-клиенте будет выведена не только занятость ресурса, но и предупреждение о невозможности бронирования.



2.17.1. Управление ресурсами календаря в Панели управления

Для управления Ресурсами календаря в Панели управления выберите в меню “Ресурсы календаря” – будет показан список ресурсов, обслуживаемых RuPost.

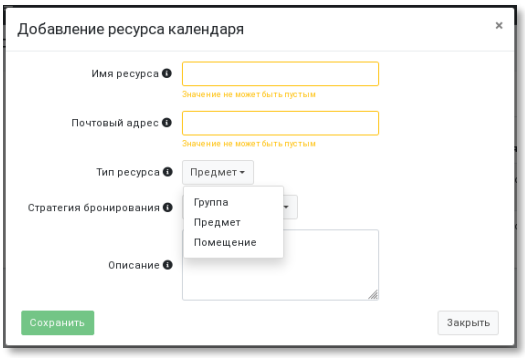


Кроме атрибутов ресурса, описанных выше (правка которых доступна через диалоговое окно свойств), в таблице есть колонка “Статус”, показывающая статус почтового домена, в котором зарегистрирован адрес данного ресурса.

Отредактировать ресурс можно нажав на ссылку в колонке “Имя ресурса”.

Для удаления ресурса отметьте нужный ресурс в левой колонке таблицы и нажмите кнопку “Удалить”.

Для добавления нового ресурса, нажмите кнопку “Добавить” и введите информацию в диалог свойств ресурса.



2.17.2. Управление ресурсами календаря через командный интерфейс CLI

Для управления ресурсами используется группа команд `resources`, которая выводит таблицу заведённых в настоящее время ресурсов. Например:

Имя ресурса	Почтовый адрес	Тип	Стратегия бронирования	Описание	Статус
Переговорная «Волгоград»	room_volgograd@rupost.ru	Помещение	Одно событие в одно время	Переговорная «Волгоград» расположена в каб. 511 главного корпуса	Активен

Если почтовый домен недоступен (отключен, удалён), в выводится статус «Почтовый домен недоступен», не обращая внимание на статус самого ресурса. В ином случае выводится статус ресурса: активен, выключен, удалён.



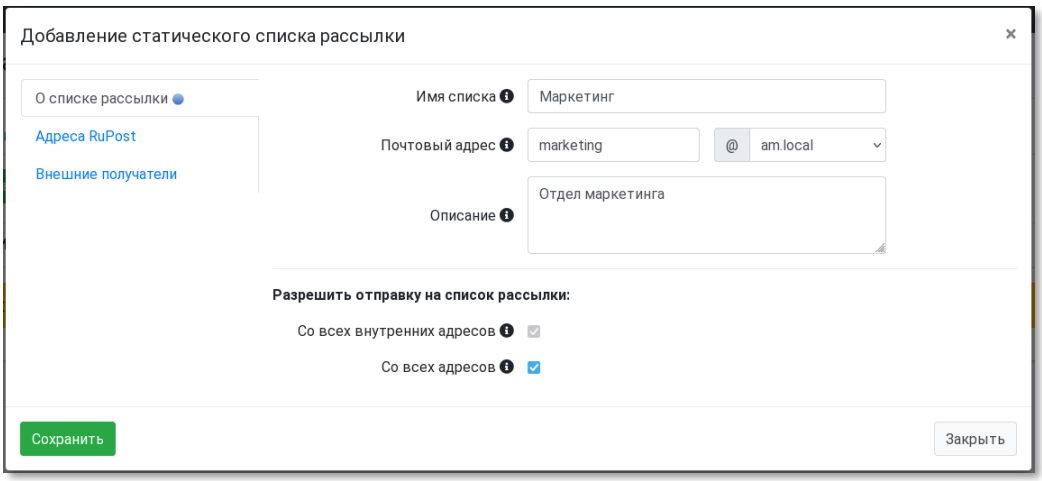
Синтаксис команды и примеры управления ресурсами календаря из командной строки приведены в разделе **«rupost resources группа команд для управления ресурсами календаря»** Справочного руководство по командной строке.

2.18. Списки рассылки

Списки рассылки – это сервис RuPost, позволяющий организовать рассылку писем по группе получателей. В RuPost реализованы и статические и динамические списки рассылки. Кроме того, для каждого списка рассылки, есть возможность задавать не только группу получателей, но и группу пользователей RuPost, которые имеют право проводить рассылку писем с помощью этого списка рассылки.

В версии 2.6.0:

- Добавлены опции, позволяющие разрешить отправку писем на Список рассылки как от всех внутренних адресов (переключатель “Со всех внутренних адресов”) так и от внешних (переключатель “Со всех адресов”). Разрешение отправки с внешних адресов автоматически разрешает отправку со всех внутренних.
- Разделено управление Отправителями и Получателями – теперь Отправитель не обязательно должен находиться в списке Получателей. Отправитель получит письмо только если его добавить в список получателей.
- Также внесены изменения в алгоритм конфигурирования почтовых компонентов после создания либо внесения изменений в Список рассылки – теперь развертывание конфигурации не требуется и соответственно, управление Списками рассылки происходит практически без остановки обработки почты.



2.18.1. Оптимизация механизма рассылок

В версии 4.2.0 добавлен специализированный сервис обслуживания рассылок.

При рассылке, доставка писем в почтовые ящики пользователей кластера RuPost осуществляется новым сервисом без использования почтовых компонентов *rupost-mta* и *rupost-mda*, что существенно снижает нагрузку на почтовую систему в целом и, таким образом, обеспечивает высокое быстродействие. Кроме того, новый сервис обеспечивает дедупликацию – т.е. при доставке рассылок через этот сервис, используемый размер места на диске чуть больше размера одного письма на каждое хранилище.

Внимание!

Реализация сервиса рассылок носит экспериментальный характер и работает со следующими ограничениями – при доставке письма:

- **не учитываются квоты** на размер почтовых ящиков, т.е. письмо будет доставлено даже если почтовый ящик переполнен;

- **не выполняются Sieve** скрипты.

При получении письма, отправленного на список рассылки, *rupost-mta* пересылает это письмо сервису рассылок, который доставляет письмо каждому адресату непосредственно в его почтовый ящик.

Если в момент обработки рассылки часть Хранилищ, содержащих почтовые ящики адресатов, не доступна, то доставка писем для этих адресатов будет осуществлена посредством SMTP.

Если же адресатами рассылки являются пользователи, почтовые ящики которых находятся на нескольких сайтах Геокластера, то, сначала, межсайтовая доставка письма производится существующим механизмом (по SMTP/SMTPS), а затем, сервис обслуживания рассылок на каждом сайте осуществляет доставку письма в почтовые ящики пользователей этого сайта.

Так как, в данный момент, сервис работает в экспериментальном режиме, то он отключен по умолчанию. Включить специализированный сервис рассылок можно командой CLI:

```
rupost dlservice on
```

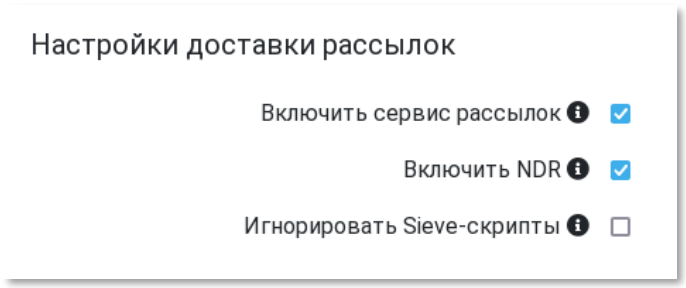
Для переключения в стандартный режим доставки рассылок используйте команду CLI:

```
rupost dlservice off
```

После выполнения этой команды, необходимо переразвернуть конфигурацию.

2.18.1.1. *Настройки для сервиса рассылок в Панели управления*

В версии 4.3.4 на страницу “Общие настройки” добавлена вкладка “Доставка рассылок”.



Настройки сервиса рассылок следующие:

- **Включить сервис рассылок** – при включении, для доставки рассылок будет использован специализированный сервис рассылок. В противном случае, для доставки рассылок будет использоваться тот же механизм, что и для обычной почтовой доставки.

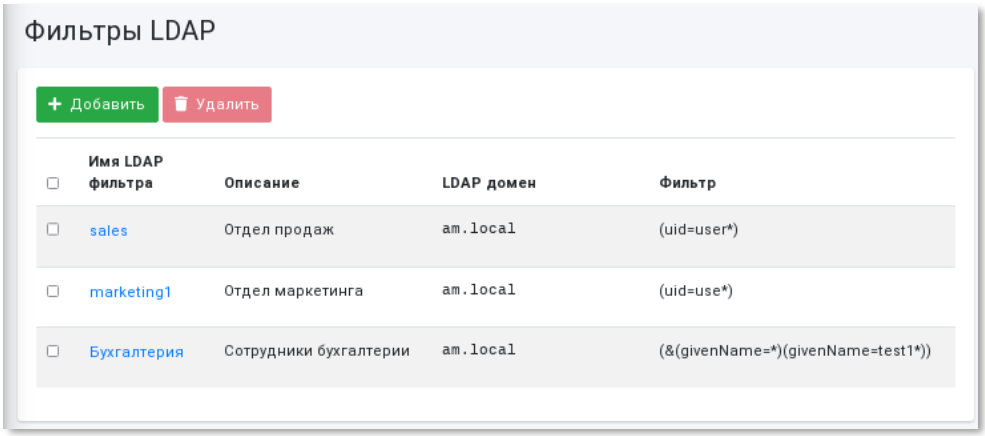
- **Включить NDR** – отправлять ли отчет о доставке отправителю рассылки.
- **Игнорировать Sieve-скрипты** – при включении, доставка рассылки будет осуществляться напрямую в папку “Входящие” почтовых ящиков на MailDir, что существенно ускоряет доставку всем адресатам, не приводит к повышению нагрузки на почтовую систему и обладает еще одним преимуществом – автоматической дедупликацией. Так как доставка осуществляется непосредственно в хранилище, то Sieve скрипты выполнены не будут. Если же этот переключатель отключен, то доставка писем будет осуществляться по LMTP протоколу с выполнением Sieve-скриптов.

2.18.2. Фильтры LDAP

Для создания динамических списков рассылки вначале необходимо определить для них фильтры LDAP, по которым в список рассылки будут включаться пользователи (список автоматически обновляется каждые 6 часов).

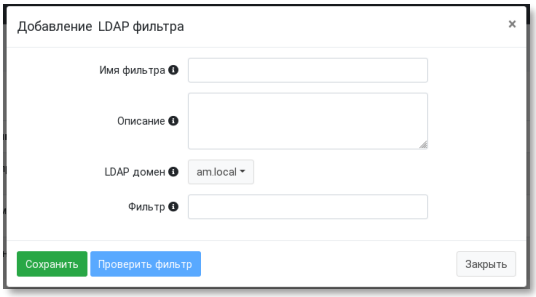
Настраивать фильтры LDAP можно как с помощью Панели управления, так и через командный интерфейс CLI.

Работа с фильтрами LDAP в Панели управления осуществляется на специальной странице “Фильтры LDAP” содержащей список всех ранее созданных фильтров.



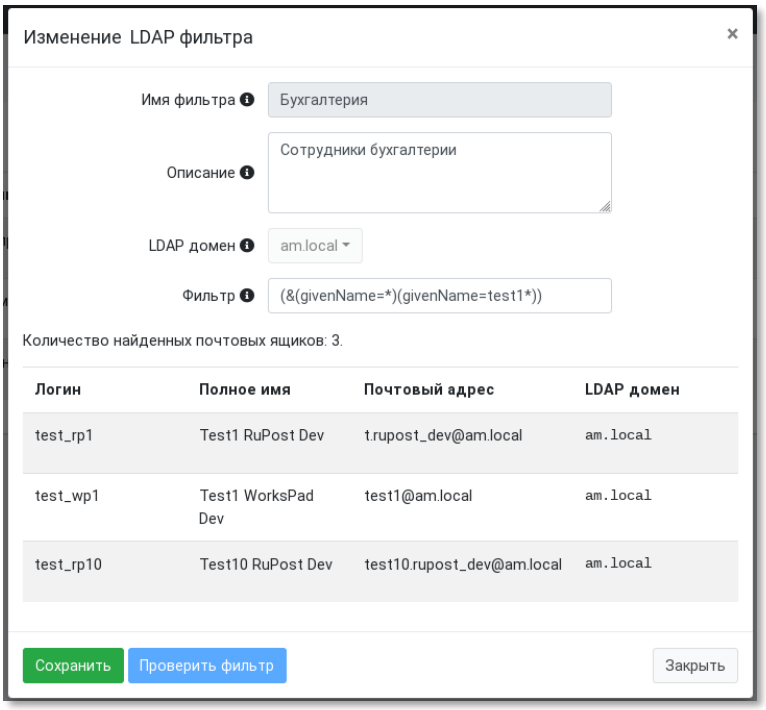
Для удаления фильтров нужно отметить один или несколько в первом столбце и нажать кнопку “Удалить”. Система не даст удалить те фильтры, которые в данный момент используются для формирования динамических списков рассылки.

Для добавления нового фильтра LDAP нажмите на кнопку “Добавить”:

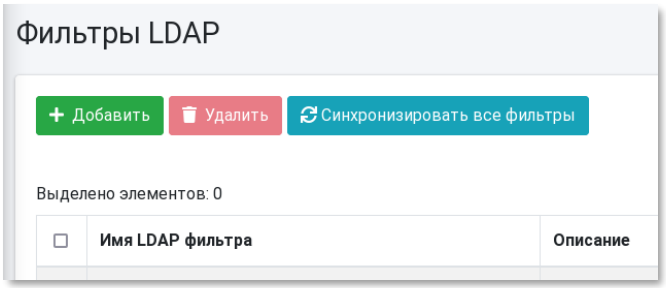


В поле “Фильтр” указывается строка, определяющая фильтр LDAP по которому будет идти поиск записей в выбранном домене LDAP. Обратите внимание, что поиск производится только по записям существующих почтовых ящиков RuPost. Проверить работу заданного фильтра можно, нажав на кнопку “Проверить фильтр” – будет показано количество найденных записей и несколько первых записей в таблице.

При изменении свойств LDAP фильтра результаты фильтрации обновляются автоматически:



В версии 2.6.0 на странице “Фильтры LDAP” появилась возможность синхронизировать все фильтры LDAP, использующиеся в динамических списках рассылки и почтовых правилах, со службами каталогов по кнопке “Синхронизировать все фильтры”.



Синтаксис команды и примеры управления LDAP фильтрами из командной строки приведены в разделе **«rupost ldap-filters группа команд для управления фильтрами LDAP»** Справочного руководство по командной строке.

Фильтры имеют единственную зависимость — LDAP домен, для которого они создаются. Отключение/удаление LDAP домена приведет к отключению зависящих от него LDAP фильтров.

2.18.3. Динамические списки рассылки

Динамические группы или списки рассылки отличаются автоматическим сбором и обновлением списков отправителей и получателей в зависимости от назначенного для них фильтра LDAP. Для каждой группы указывается как список получателей, так и список почтовых ящиков, которым разрешено отправлять на указанную группу.

2.18.4. Статические списки рассылки

Статические списки рассылки, в отличие от динамических, задаются с помощью перечней адресов как для отправителей, так и для получателей. Для того, чтобы обновить список получателей, либо отправителей необходимо вручную отредактировать соответствующий список с помощью веб-интерфейса, либо через CLI. Для каждого списка рассылки указывается как список получателей, так и список почтовых ящиков, которым разрешено отправлять на указанный список. Отправителями могут быть только пользователи RuPost. Отправители автоматически становятся получателями, независимо от явно указанного отдельного списка получателей.

Еще одним существенным отличием статических списков рассылки от динамических является возможность добавлять в качестве получателей **внешние адреса** (не обслуживаемые RuPost).

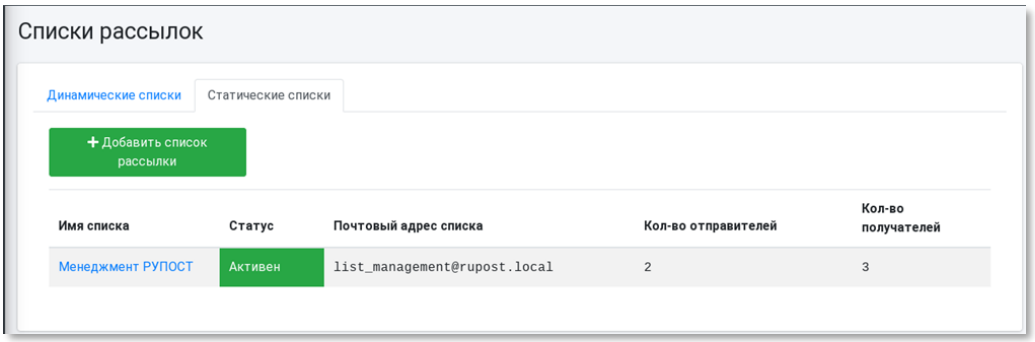
2.18.5. Управление списками рассылки через командный интерфейс CLI



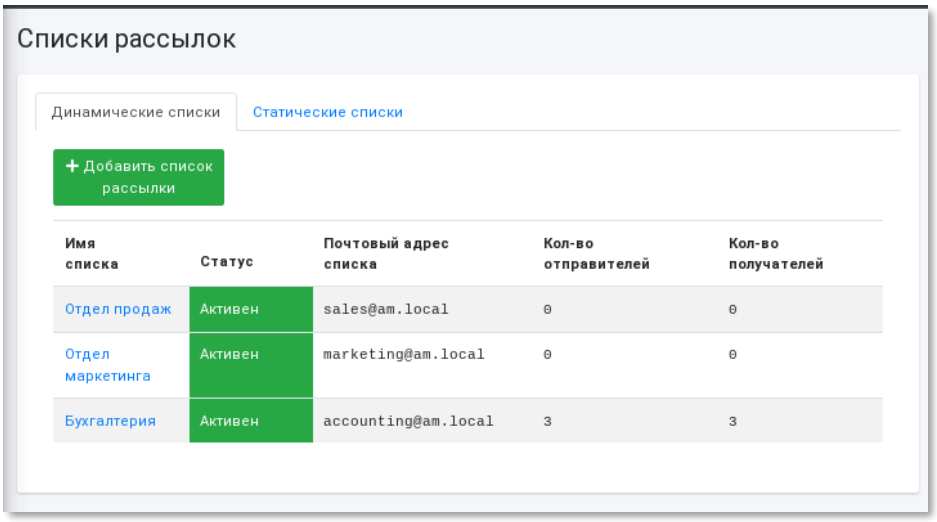
Синтаксис команды и примеры управления списками рассылки из командной строки приведены в разделе **«rupost distribution-lists группа команд для управления почтовыми списками рассылки»** Справочного руководство по командной строке.

2.18.6. Управление списками рассылки в Панели управления

Для управления списками рассылки в Панели управления нужно выбрать из меню пункт “Списки рассылок”:



Работа с динамическими и статическими списками рассылки разделена на две закладки в соответствии с типом списков рассылки. Рассмотрим работу с динамическими списками рассылки:

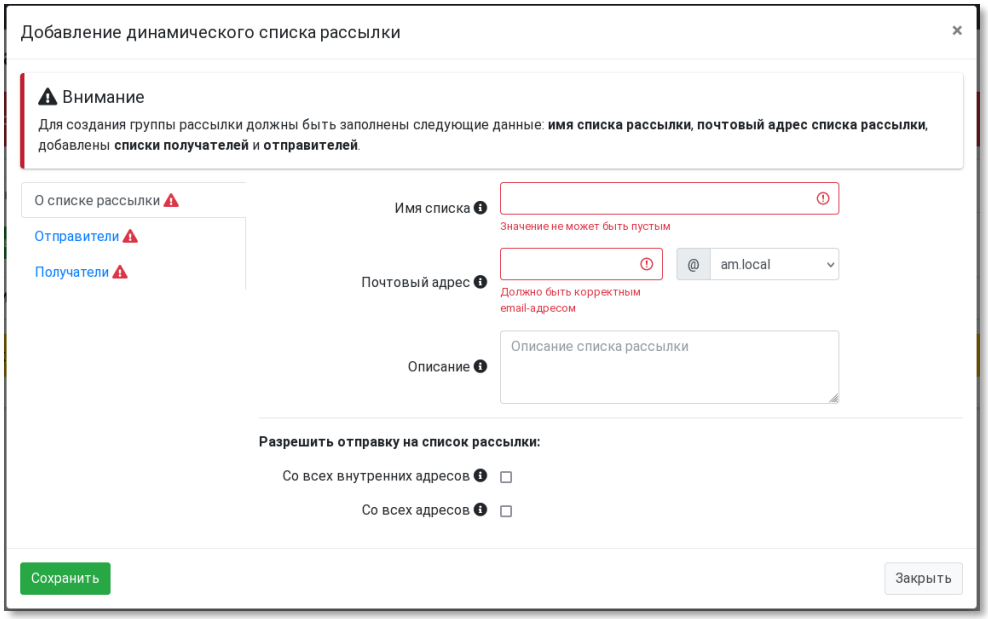


В таблице динамических списков рассылки кроме имени списка и почтового адреса показываются также:

- **Статус** – статус почтового домена в котором зарегистрирован адрес списка рассылки.
- **Кол-во отправителей** – количество пользователей RuPost, выбранных с помощью LDAP фильтров, которые имеют право отправлять письма на эту группу рассылки.
- **Кол-во получателей** - количество пользователей RuPost, выбранных с помощью LDAP фильтров, которые являются получателями рассылок.

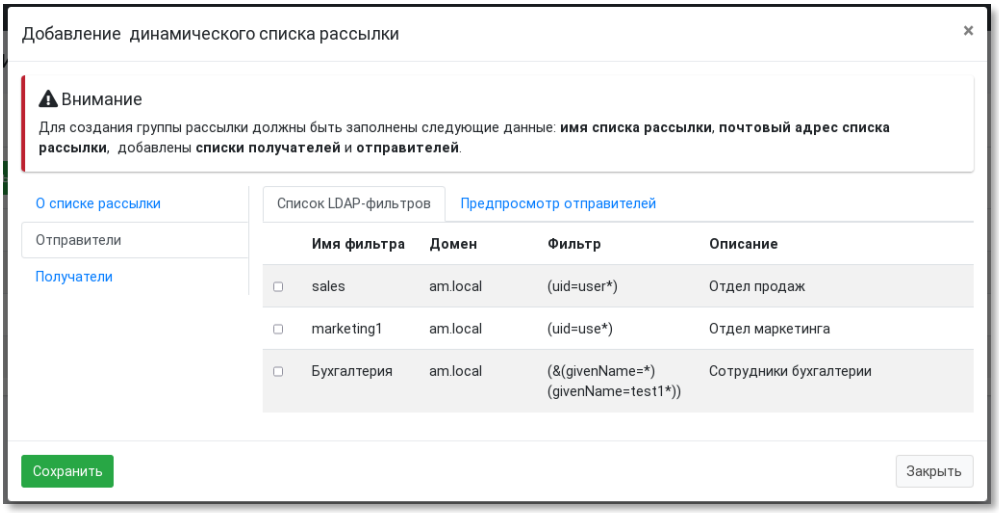
Для редактирования или удаления списка рассылки перейдите по ссылке в колонке “Имя списка”.

Для добавления динамического списка рассылки нажмите кнопку “Добавить список рассылки” и введите параметры создаваемого списка рассылки.



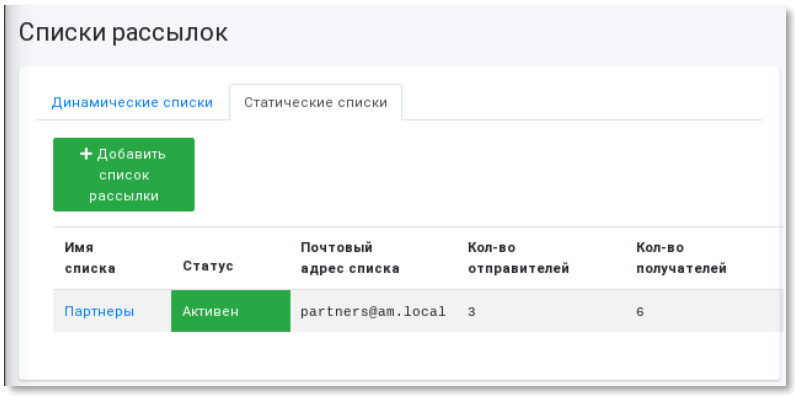
Обязательные для заполнения поля выделены красным цветом.

На закладках “Отправители” и “Получатели” необходимо выбрать один или несколько LDAP фильтров, с помощью которых будет сформирована соответствующая группа пользователей.



Результаты работы выбранных фильтров можно просмотреть на закладке “Предпросмотр отправителей” или “Предпросмотр получателей” соответственно.

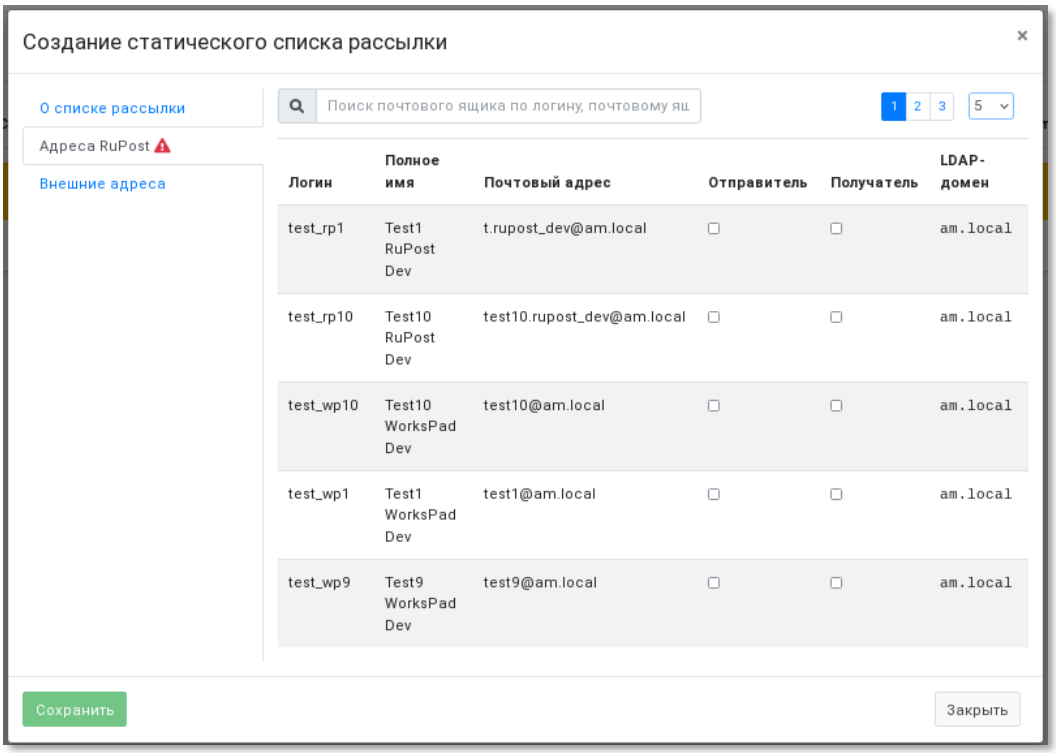
Рассмотрим работу со статическими списками рассылки.



На закладке “Статические списки” по каждому списку рассылки показана следующая информация:

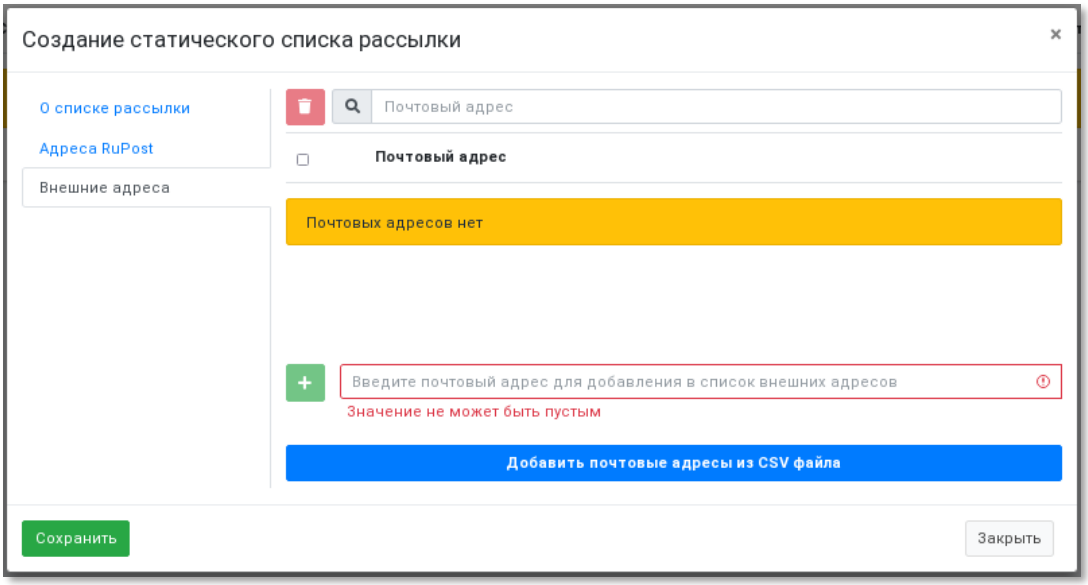
- **Статус** – статус почтового домена, в котором зарегистрирован адрес списка рассылки.
- **Кол-во отправителей** – количество пользователей RuPost, которые имеют право отправлять письма на эту группу рассылки.
- **Кол-во получателей** - количество адресатов (как пользователей RuPost так и внешних адресатов), которые являются получателями рассылок.

Для редактирования или удаления списка рассылки перейдите по ссылке в колонке “Имя списка”. Для добавления статического списка рассылки нажмите кнопку “Добавить список рассылки” и введите параметры создаваемого списка рассылки.



Диалог создания статического списка рассылки содержит закладки:

- **О списке рассылки** – имя списка, его почтовый адрес и описание.
- **Адреса RuPost** – пользователи RuPost, которые могут являться как отправителями, так и получателями.
- **Внешние адреса** – почтовые адреса внешних получателей, не являющимися пользователями RuPost.



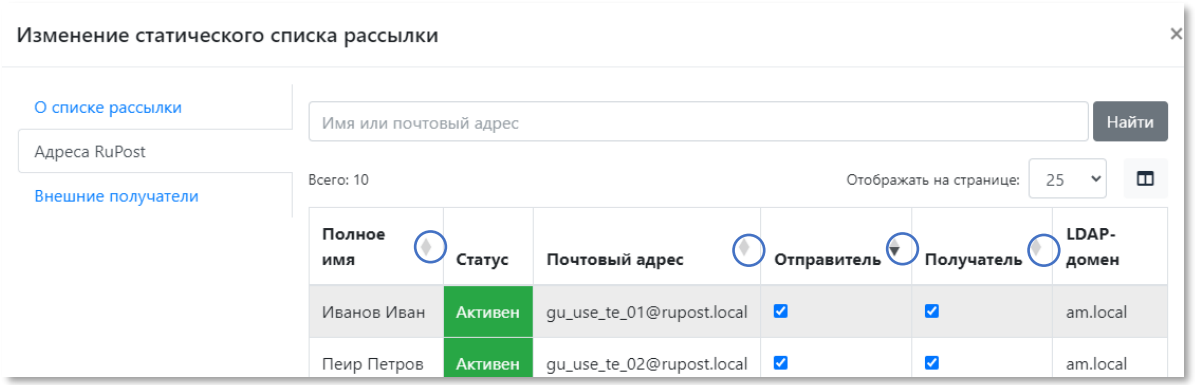
На закладке “Внешние адреса” показан список внешних адресатов, в который можно добавить адрес либо вручную по кнопке “+”, либо из CSV файла по кнопке “Добавить почтовые адреса из CSV файла”.

Формат CSV файла для импорта – перечень почтовых адресов, один адрес в каждой строке. Например:

```
EmailAddress;distinguishedName;sAMAccountName
test_rp1@am.local;uid=test_rp1,cn=users,cn=accounts,dc=am,dc=local;test_rp1
test_rp2@am.local;uid=test_rp2,cn=users,cn=accounts,dc=am,dc=local;test_rp2
```

Обязательным столбцом является `EmailAddress`. Все остальные столбцы являются опциональными.

В версии 3.1.0 при показе списка почтовых ящиков, входящих в статический список рассылки, добавлена сортировка по полям “Отправитель”, “Получатель”, “Полное имя” и “Почтовый адрес”.



2.19. Правила обработки почты (ограничения)

Внимание!

Информация в этом разделе является актуальной вплоть до версии 4.1.1.

В версии 4.2 **Почтовые правила перенесены в Транспортные правила** (см. раздел 2.20).

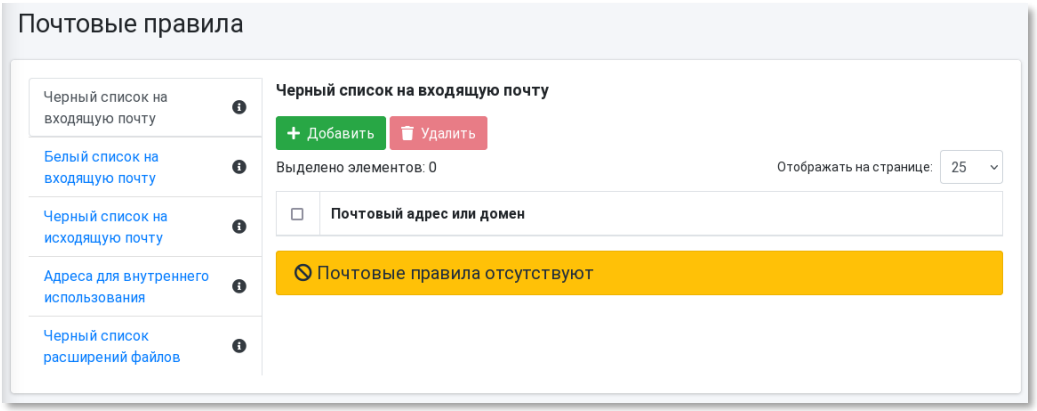
Поддерживаются следующие правила обработки почты (ограничения):

- **“Черный список на входящую почту”** – почта от указанных доменов и/или адресов не принимается;
- **“Белый список на входящую почту”** – почта от указанных доменов и адресов принимается. Это правило имеет более высокий приоритет, чем “черный” список – таки образом, можно, например, обеспечить прием почтовых сообщений с одного адреса в домене при том, что прием почты будет заблокирован для всех остальных адресов этого домена.
- **“Черный список на исходящую почту”** – запрет отправки на указанные домены и/или адреса.
- **“Адреса для внутреннего использования”** – запрет приема почты с внешних адресов.
- **“Черный список расширений файлов”** – запрет входящей почты, содержащей указанные типы вложений.
- **“Запрет отправки на внешние адреса”** – запрет исходящей почты.

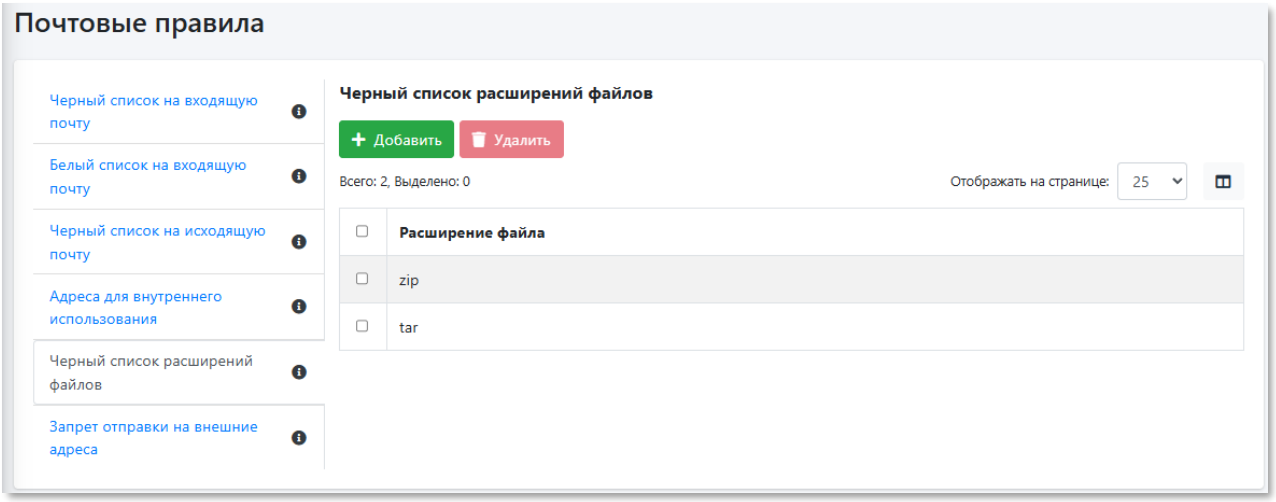
Внимание!

Если адрес находится в черном списке на исходящую почту, и он же добавлен в список рассылки, то, при отправке писем на этот список рассылки, письма будут доставлены соответствующим внешним получателям.

Управление почтовыми правилами находится на странице “Контроль доступа” -> “Почтовые правила”:

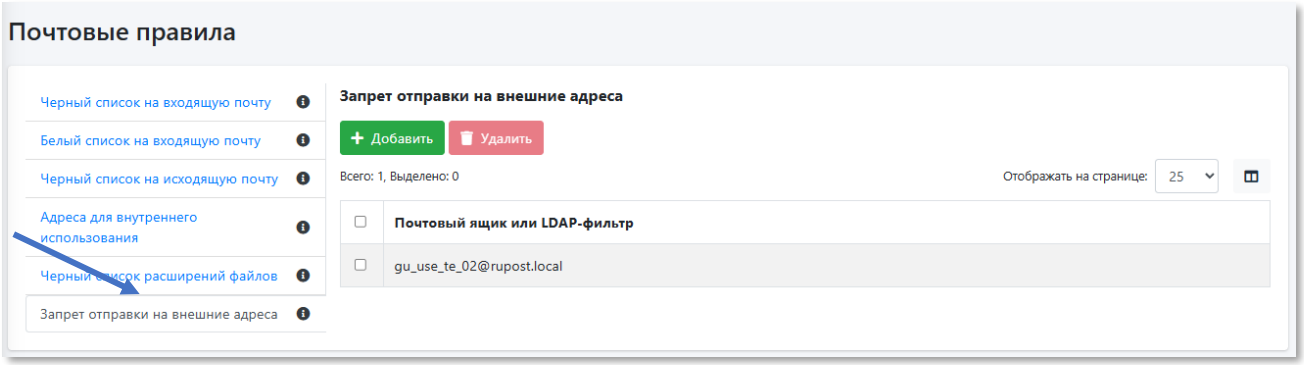


В версии 2.5.0 добавлено почтовое правило, позволяющее запретить получение сообщений, содержащих вложения с определенными расширениями файлов.



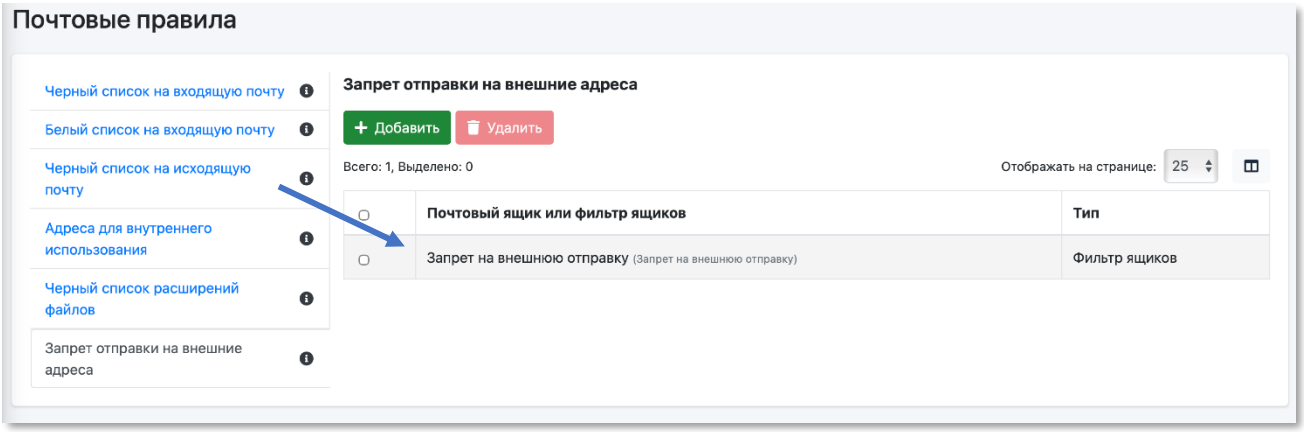
В версии 2.5.0 для почтового правила “Адреса для внутреннего использования” добавлена возможность задавать список почтовых адресов не только статически (выбором из списка вручную), но и динамически - при помощи выбора LDAP фильтра, который возвращает список почтовых ящиков, к которым будет применено данное правило.

В версии 3.1.0 добавлено почтовое правило “Запрет отправки на внешние адреса”.



Пользователи, к которым применено данное правило, имеют возможность отправлять почтовые сообщения только на адреса обслуживаемых почтовых доменов и, соответственно, не могут отправлять почту за пределы организации.

В версии 3.4.0 в настройку почтового правила “Запрет отправки на внешние адреса” добавлена возможность задавать список ящиков, к которому применимо данное правило, с помощью выбора Фильтра ящиков.



Необходимый фильтр ящиков предварительно настраивается на странице панели управления “Получатели“ -> “Фильтры ящиков”.

Синтаксис команды и примеры управления почтовыми правилами из командной строки приведены в разделе **«rupost restrictions группа команд для управления почтовыми ограничениями»** Справочного руководство по командной строке.

2.20. Транспортные правила

В версии 4.2.0 добавлена возможность обработки почтовых сообщений при помощи Транспортных правил (аналог *Mail Flow Rules* в Microsoft Exchange).

Транспортные правила предоставляют возможность администратору системы гибко конфигурировать поведение системы при обработке почтовых сообщений (например, запретить доставку сообщений, которые содержат определенные типы вложений, либо ограничить отправку сообщений “наружу” для группы пользователей).

Транспортное правило - правило, которое задает выполнение определенных действий для обрабатываемого почтового сообщения при выполнении набора условий.

Набор транспортных правил - список из нескольких Транспортных правил, которые применяются к почтовым сообщениям. По умолчанию, к каждому сообщению применяются все правила из набора. Правила применяются последовательно, одно за другим, порядок применения правил задается порядком следования правил в наборе. Если в списке правил есть действие, подразумевающее, что нужно прекратить дальнейшую обработку (либо это в нем явно указано), то на этом правиле обработка списка правил для текущего почтового сообщения завершается и, соответственно, правила, следующие в списке за текущим правилом, не выполняются.

Функциональность Транспортных правил реализуется с помощью протокола Milter.

2.20.1. Структура транспортных правил

Каждое транспортное правило состоит из:

- **условий** - в совокупности определяют, должны ли выполниться действия, заданные в правиле, для обрабатываемого сообщения;
- **исключений** - в совокупности определяют, нужно ли исключить обрабатываемое сообщение - не выполнять действия в текущем правиле;
- **действий** - что делать с сообщением, если условие выполнено;
- **статуса правила** - Включено / Отключено.

Условия транспортного правила

В правиле может быть указано несколько условий. Если условий несколько, то они объединяются логической операцией И (AND). Т.е. для того, чтобы действия, указанные в правиле, выполнились, необходимо, чтобы все условия были выполнены. Если же требуется, чтобы условия были объединены по логическому ИЛИ (OR), то необходимо создать несколько отдельных правил. При обработке сообщения, каждое условие и исключение проверяется и возвращает логическое значение - TRUE/FALSE. Если все условия вернули TRUE и все исключения вернули FALSE, то заданные в правиле действия - выполняются. Условие является обязательным элементом - в правиле должно быть, хотя бы, одно условие.

© 2021-2026 РуПост

В том случае, когда значения полей сообщения получены из SMTP сессии (например, MAIL FROM, RCPT TO), а не из заголовков самого письма, мы используем термин **Конверт** (Envelope), как рекомендовано в RFC 5321.

Пример набора условий:

- Если поле "Конверт" → "Получатель" содержит "*@astralinux.ru"
- Если поле "Конверт" → "Отправитель" содержит "*@workspad.com"
- Если сообщение имеет вложение с расширением zip

Исключения транспортного правила

В правиле может быть указано несколько исключений. Если исключений несколько, то они объединяются логической операцией ИЛИ (OR). При обработке сообщения, каждое исключение проверяется и возвращает логическое значение - TRUE/FALSE. Исключения имеют приоритет над Условиями - условия почтового правила проверяются, только если все исключения вернули FALSE. Исключения не являются обязательными – правило может не иметь исключений.

Действия транспортного правила

В правиле может быть указано несколько действий, которые будут выполнены над обрабатываемым почтовым сообщением, при выполнении условий. Есть специальное (управляющее потоком правил) действие – *Не выполнять остальные правила*. Если в списке действий выполняемого правила есть это действие, то проверки остальных правил (следующих за текущим) не выполняются.

Например, для сообщений от условного чёрного списка может быть задан такой набор действий:

- Написать отправителю письмо с предупреждением о нахождении в чёрном списке.
- Переслать его письмо на SMTP-шлюз антивируса.
- Прекратить дальнейшую обработку правил.

Статусы транспортного правила

Если почтовое правило используется в данный момент, то оно имеет статус “Включено”. Администратор имеет возможность временно отключить отдельное правило, для этого, необходимо изменить статус выбранного правила на “Отключено”. При создании правила, оно, по умолчанию, имеет статус “Отключено”.

Для тестирования правил войдите в режим группового редактирования транспортных правил. Для этого нажмите на кнопку «Групповое редактирование». В этом режиме можно изменить порядок исполнения правил простым перетаскиванием элементов между позициями в списке. Также в появившееся поле ввода «Тестовое письмо» можно вставить исходный текст предполагаемого письма и узнать, какие именно правила отработают нажатием на кнопку «Тестировать».

Встроенные транспортные правила (например, правило доставки почты между сайтами Геокластера) управляются RuPost, не могут быть изменены администратором и, соответственно, не отображаются в Панели управления.

2.20.2. Набор условий

Набор доступных для использования условий будет постепенно пополняться, но на момент выхода версии 4.2.0 реализованы следующие условия:

1. *Конверт → Отправитель / Получатель*

- *Содержит* - хотя бы одно из перечисленных значений [строка1, строка 2, ...] встречается среди значений поля.
- *Входит в LDAP-фильтр* - хотя бы одно из перечисленных значений поля встречается среди списка ящиков LDAP-фильтра.
- *Входит в фильтр ящиков* - хотя бы одно из перечисленных значений поля встречается среди списка фильтра ящиков.
- *Входит в обслуживаемые домены* - хотя бы один из почтовых адресов поля имеет домен, обслуживаемый текущей почтовой системой.
- *Не входит в обслуживаемые домены* - хотя бы один из почтовых адресов поля имеет домен, не обслуживаемый текущей почтовой системой.

2. *Расширение вложения* - хотя бы одно из приложений письма имеет расширение из приведённого списка [строка1, строка2, ...]

Если поле “Получатель” содержит несколько адресов, то условие будет считаться выполненным, если оно верно, хотя бы, для одного из адресов.

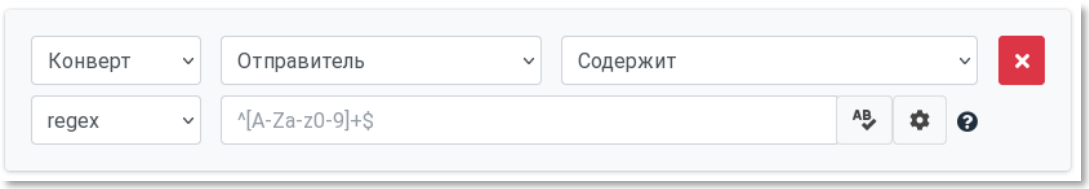
В версии 4.3.4 расширены возможности транспортных правил – добавлен ряд новых условий.

Добавлены следующие условия:

- **Наличие вложения** – “Вложение”-“Присутствует”.
- **Размер вложения** – “Вложение”-“Размер больше или равен”-[размер в МБ]
- **Размер письма** – “Конверт”-“Размер больше или равен”-[размер в МБ].
- **IP-адрес отправителя** – “Конверт”-“Отправитель”-“IP адрес соответствует”-[IP адрес/маска].
- **Отправитель содержит** – “Конверт”-“Отправитель”-“Содержит”-“glob”/”regex”-[текст].
- **Получатель содержит** – “Конверт”-”Получатель”-“Содержит”-“glob”/”regex”-[текст].

Для условий “Отправитель содержит” или “Получатель содержит” возможны два варианта задания параметров для сравнения:

- **Glob** - варианты перечисляются через запятую.
- **Regex** – вводится регулярное выражение (синтаксис модуля Python). Дополнительные опции – “Игнорировать регистр” и “Многострочный режим”. Есть, также, проверка синтаксиса регулярного выражения.



2.20.3. Набор действий

Набор доступных для использования действий будет постепенно пополняться, но на момент выхода версии 4.2.0 реализованы следующие действия:

1. *Удалить письмо*
3. *Сообщение отправителю [текст сообщения]*
4. *Переслать письмо* - переслать письмо на указанный SMTP или LMTP сервер.

Если в транспортном правиле будут одновременно использованы действия и «Удалить письмо» и «Переслать письмо», то выполняется только пересылка на указанный сервер, а удаление письма не выполняется.

2.20.4. Примеры транспортных правил

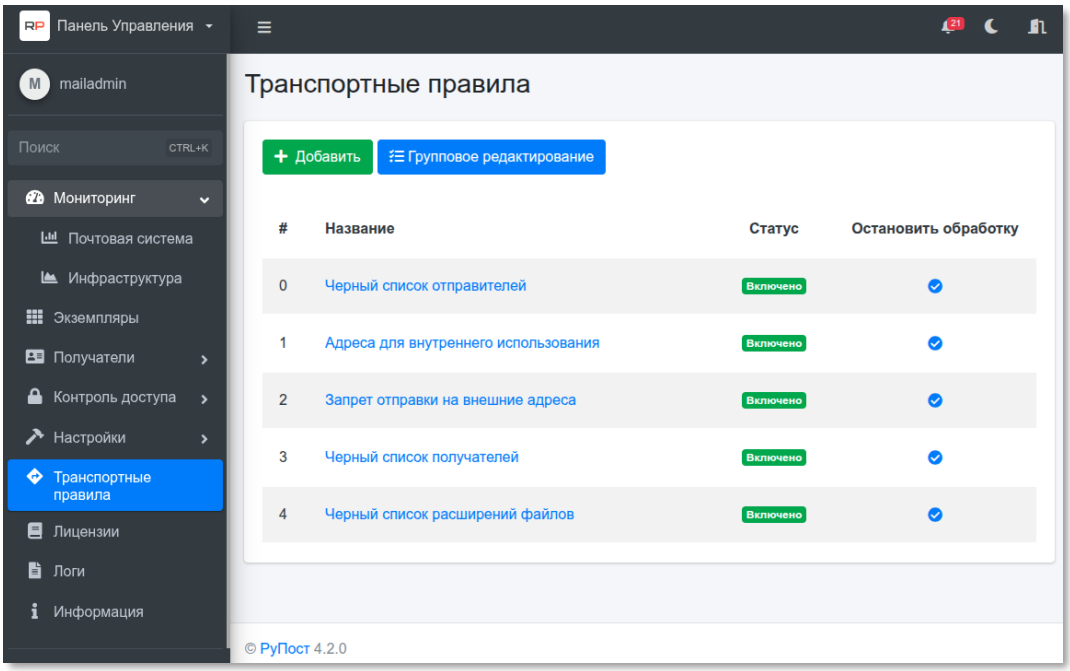
В таблице приведены примеры транспортных правил.

Название	Условия	Исключения	Действия	Прекратить дальнейшую обработку правил
Черный список на входящую почту	Поле **Отправитель** Содержит: {*@domain.ru, aaa@domain1.ru...}		Удалить письмо	☑
Черный список на исходящую почту	1. Поле **Отправитель** Входит в обслуживаемые домены 2. Поле **Получатель** Содержит: {*@domain.ru, aaa@domain1.ru, ...}	Поле **Отправитель** Содержит {bbb@domain.ru, ...}	1. Удалить письмо 2. Сообщение отправителю [Письмо не доставлено]	☑
Адреса для внутреннего использования	Поле **Получатель** Содержит: {aaa@domain.ru, ...}	Поле **Отправитель** Входит в обслуживаемые домены	Удалить письмо	☑
Адреса для внутреннего использования по LDAP-фильтрам	Поле **Получатель** Входит в LDAP-фильтр: {ldap_f1, ...}	Поле **Отправитель** Входит в обслуживаемые домены	Удалить письмо	☑

Адреса для внутреннего использования по LDAP-фильтрам	Поле **Получатель** Входит в LDAP-фильтр: {ldap_f1, ...}	Поле **Отправитель** Входит в обслуживаемые домены	Удалить письмо	☑
Запрет отправки на внешние адреса	1. Поле **Отправитель** содержит: {aaa@domain.ru, ...} 2. Поле **Получатель** Не входит в обслуживаемые домены		Удалить письмо	☑
Запрет отправки на внешние адреса по LDAP-фильтрам	1. Поле **Отправитель** Входит в LDAP-фильтр: {ldap_f1, ...} 2. Поле **Получатель** Не входит в обслуживаемые домены		Удалить письмо	☑
Транспортное правило	Поле **Получатель** Содержит: {*@domain.ru, ...}	Поле **Получатель** Входит в обслуживаемые домены	Переслать письмо на: **FQDN/IP**	☑
Запрет вложений	Расширение вложения: {zip, tar, ...}	Поле **Отправитель** Входит в обслуживаемые домены	Удалить письмо	☑

2.20.5. Создание транспортного правила

Для просмотра списка транспортных правил, а также для создания нового правила, перейдите на страницу “Транспортные правила” (Главное меню, пункт “Транспортные правила”).

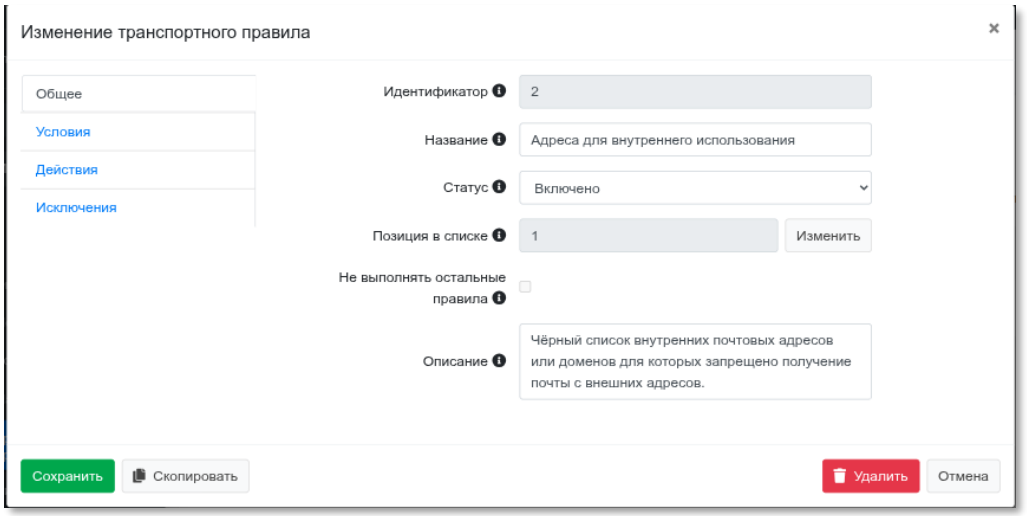


На странице отображается список Транспортных правил с их статусами. Номер правила задает порядок выполнения правил.

Для добавления нового правила есть две возможности:

- На странице “Транспортные правила” - с помощью кнопки “Добавить”.
- В окне свойств Транспортного правила - с помощью кнопки “Скопировать”. Этот вариант удобен для случая, когда нужно создать правило, похожее на одно из тех, что уже находятся в списке.

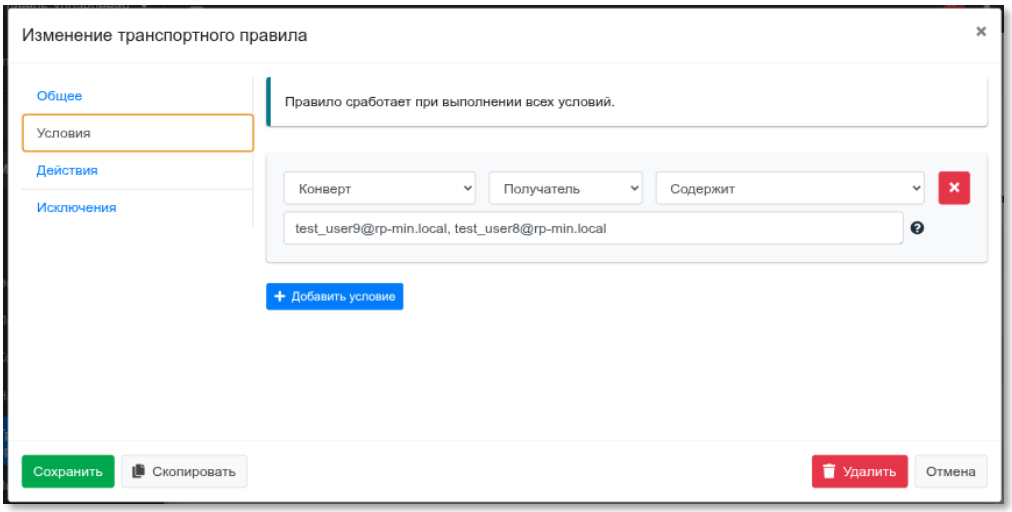
Для редактирования уже существующего правила, нажмите на его название, откроется окно свойств Транспортного правила.



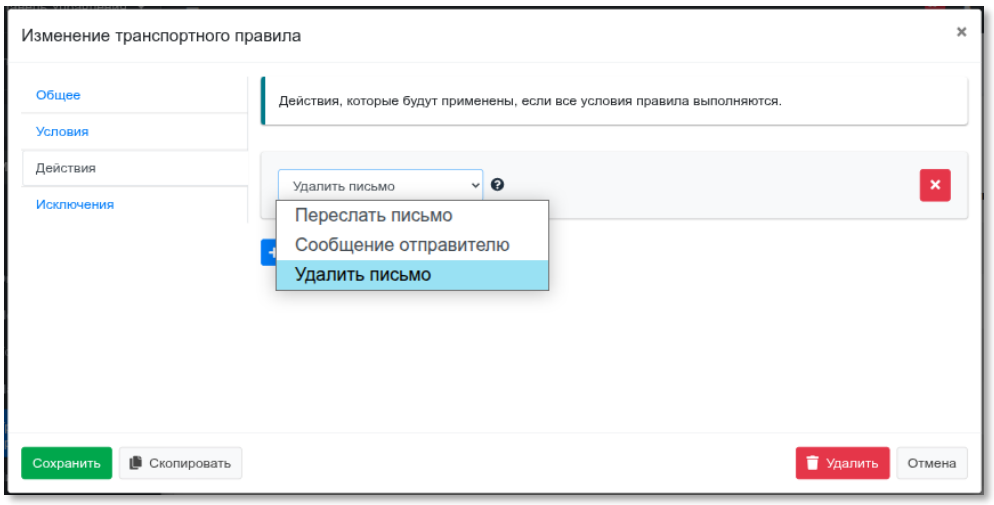
Так как функциональность добавляемого правила зависит от порядка следования правил, то обратите внимание на то, что изменить порядок следования правил можно двумя способами:

- В окне свойств правила изменить значение поля “Позиция в списке” – при нажатии на кнопку “Изменить” можно выбрать, после какого (или перед каким) правила будет добавлено данное правило.
- В списке правил в режиме группового редактирования – перетаскиванием правил в списке.

При добавлении правила, необходимо указать его Условия и Действия (Исключения – не обязательны). Для добавления нового Условия, нажмите на кнопку “Добавить условие” в Списке условий, выберите необходимое условие из выпадающего списка и задайте значения.



Также, при добавлении правила, нужно выбрать действия, которые будут произведены над сообщением, если условия будут выполнены. Для выбора действий, нажмите кнопку “Добавить действие” в Списке действий и выберите нужное действие из выпадающего списка.



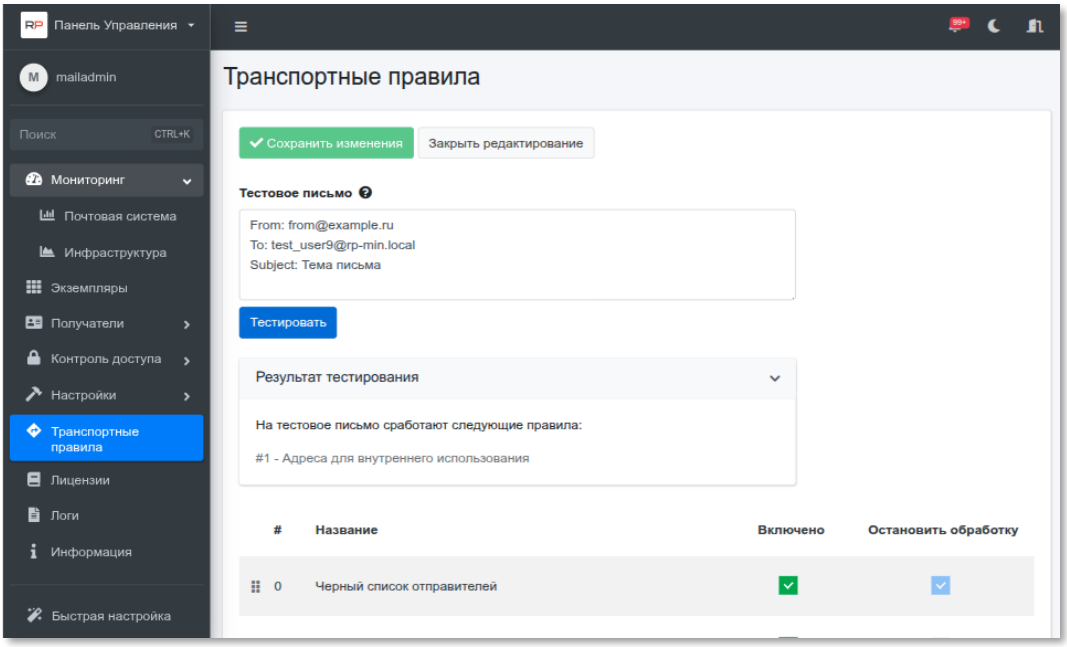
После завершения редактирования свойств Транспортного правила, нажмите на кнопку “Сохранить” – добавленное правило появится в списке правил.

Для удаления Транспортного правила, выберите нужное правило, откройте окно его свойств, и затем нажмите на кнопку “Удалить.”

2.20.6. Проверка набора транспортных правил

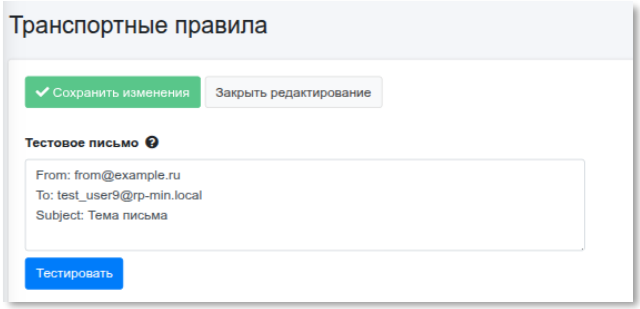
Так как Транспортные правила непосредственно влияют на доставку почты, то высок риск нарушить работу почтовой системы, если при конфигурировании Транспортных правил были допущены ошибки. Поэтому, в RuPost добавлен режим проверки Транспортных правил. При создании нового правила, либо при изменении параметров существующего, перед внесением изменений в обработку потока почтовых сообщений, можно проверить работу набора правил, переключившись в режим проверки.

Для перехода в режим проверки нужно нажать «Групповое редактирование».



Любые правки, которые вносятся в Транспортные правила в этом режиме, не затрагивают текущий, работающий в данный момент, набор Транспортных правил.

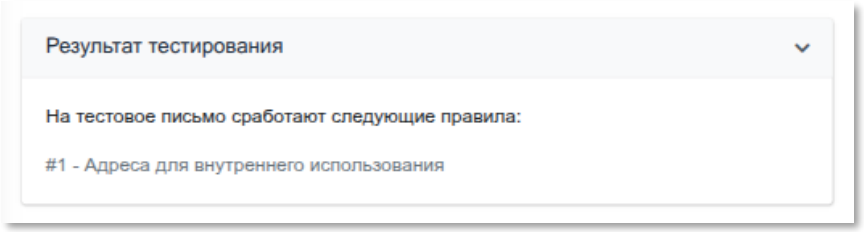
Проверить работу Транспортных правил можно с помощью текстового поля “Тестовое письмо”. Введите необходимые для проверки значения полей **Конверта** (Envelope) письма (например, From и To).



Значения полей почтового сообщения вносятся по схеме:

[заголовок сообщения]:[значение поля]

После ввода всех необходимых полей тестового сообщения, можно осуществить проверку работы набора правил, нажав на кнопку “Тестировать”. Правила будут срабатывать точно так же, как если бы сервер RuPost получил данное тестовое письмо.



Проверку можно проводить многократно, изменяя содержимое поля “Тестовое письмо”, либо включая/отключая отдельные правила.

По окончании отладки набора правил, результат можно сохранить, нажав на кнопку “Сохранить изменения”.

Чтобы выйти из режима проверки правил без сохранения внесенных изменений, нажмите кнопку “Отмена”.

2.20.7. Миграция почтовых правил

Внимание!

Так как Транспортные правила обеспечивают, в том числе, и всю функциональность Почтовых правил, то, при установке версии 4.2.0 **Почтовые правила будут перенесены в Транспортные правила**.

Соответственно, следующие CLI команды по управлению почтовыми правилами отключены и будут удалены в следующей версии:

- *rupost restrictions list*
- *rupost restrictions add*
- *rupost restrictions remove*

Если использовались Почтовые правила, то, при установке версии 4.2.0, они будут преобразованы в Транспортные. В таблице приводится информация о том, как каждое Почтовое правило реализовано с помощью одного или нескольких Транспортных правил.

Почтовое правило	**Транспортное правило**	
	Название	**Описание**
Чёрный и Белый список на входящую почту	Черный список отправителей	Чёрный список внешних почтовых адресов или доменов для входящей почты. Белый список внешних почтовых адресов или доменов для входящей почты прописан в исключениях
Черный список расширений файлов	Черный список расширений файлов	Черный список расширений файлов
Черный список на исходящую почту	Черный список получателей	Чёрный список внешних почтовых адресов или доменов для исходящей почты
Запрет получения почты с внешних адресов	Адреса для внутреннего использования	Чёрный список внутренних почтовых адресов или доменов, для которых запрещено получение почты с внешних адресов
	Адреса для внутреннего использования (LDAP фильтр - {название фильтра})	Чёрный список внутренних почтовых адресов, входящих в фильтр, для которых запрещено получение почты с внешних адресов
Запрет отправки на внешние адреса	Запрет отправки на внешние адреса	Чёрный список внутренних почтовых адресов или доменов, для которых запрещена отправка почты на внешние адреса
	Запрет отправки на внешние адреса (LDAP фильтр - {название фильтра})	Чёрный список внутренних почтовых адресов, входящих в фильтр, для которых запрещена отправка почты на внешние адреса
	internal-list (почтовый фильтр - {название фильтра})	Чёрный список внутренних почтовых адресов, входящих в фильтр, для которых запрещена отправка почты на внешние адреса

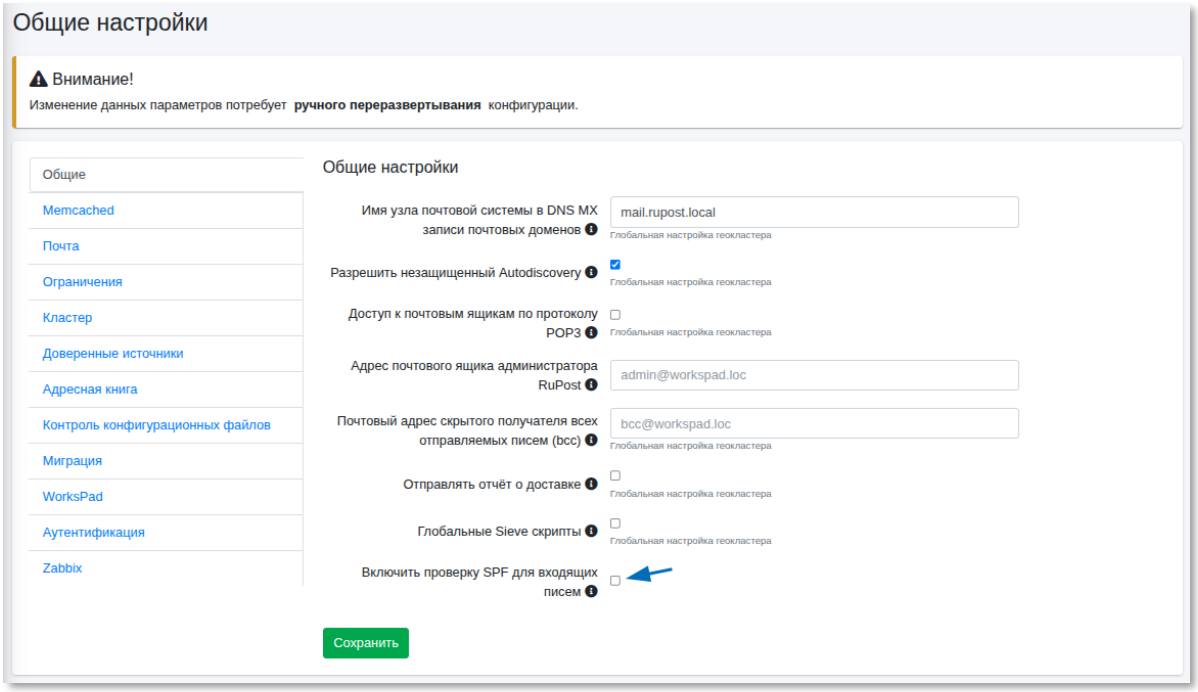
© 2021-2026 РуПост

2.21. Поддержка SPF

В версии 4.0 добавлена проверка корректности DNS записи SPF.

Обработка SPF записи позволяет удостовериться, что сервер-отправитель имеет право отправлять электронную почту от имени почтового домена, указанного в заголовке письма.

Проверка SPF включается в окне “Общие настройки” на закладке “Почта” переключателем “Включить проверку SPF для входящих писем”.



При включенной проверке SPF, в каждое письмо добавляется заголовок `Received-SPF` (такой же, как и в Microsoft Exchange). Его значения следующие:

- `none` - В DNS нет SPF-записи для данного домена.
- `pass` - Сервер отправителя авторизован для отправки почты.
- `fail` - Сервер отправителя не авторизован для отправки почты.
- `neutral` - SPF-запись не указывает явно на авторизацию сервера отправителя.
- `softfail` - Вероятно, сервер отправителя не авторизован.
- `temperror` - Ошибка при проверке SPF из-за временной проблемы.
- `permerror` - Ошибка при проверке SPF из-за ошибки в SPF-записи.

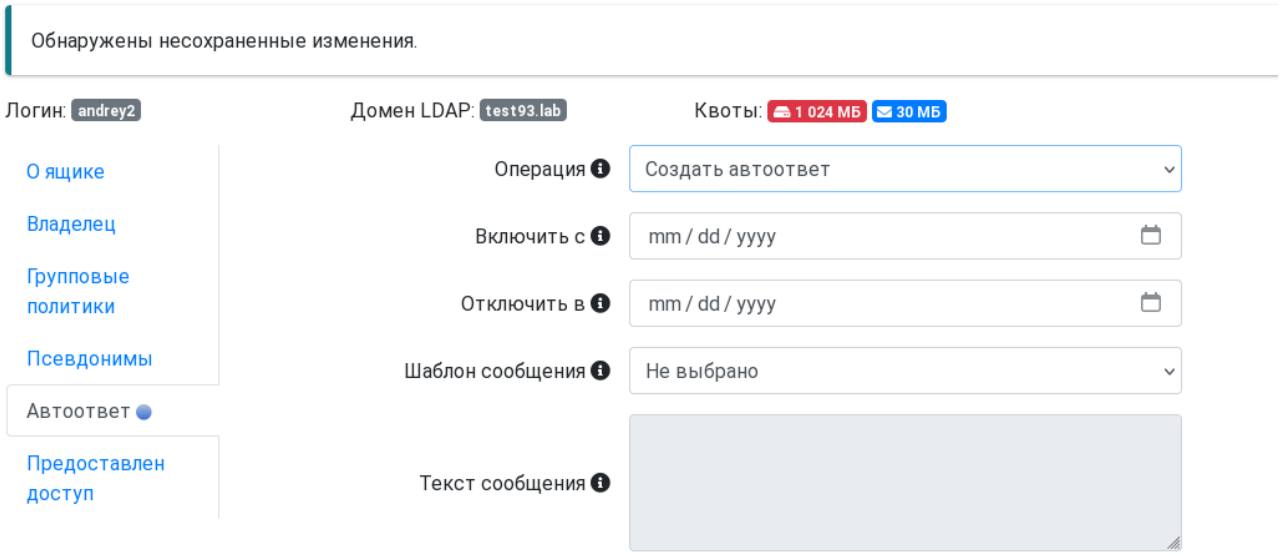
При результатах проверки `fail` и `softfail` в начало темы письма (Subject) добавляется надпись [НЕДОСТОВЕРНЫЙ ОТПРАВИТЕЛЬ].

2.22. Управление автоответами

В версии 4.0 в Панели управления добавлена возможность управления автоответами пользователей.

Автоответ представляет собой автоматически созданное письмо, которое будет отправлено в ответ при получении любого письма адресатом, для которого включён автоответ.

Для создания шаблона автоответа, в Панели управления выберите меню Получатели -> Почтовые ящики. Найдите интересующий и войдите в режим редактирования почтового ящика. Далее на закладке Автоответ выберете операцию “Создать / заменить автоответ”:



Для создания нового автоответа, заполните поле “Текст сообщения” и укажите интервал действия автоответа (поля “Включить с” и “Отключить в”).

При формировании автоооответа может быть использован один из встроенных шаблонов:

- Отпуск
- Командировка
- Болезнь
- Увольнение

При выборе шаблона, происходит подстановка соответствующего текста, который, затем, можно отредактировать.

Для удаления автоответа, выберите операцию “Удалить автоответ”.

После завершения установки автоответа, рекомендуем проверить корректность формирования автоответа для выбранного пользователя. Это можно сделать, отправив на адрес пользователя любое тестовое письмо – в ответ должен прийти выбранный ранее автоответ.

2.23. Групповая политика – автоподпись

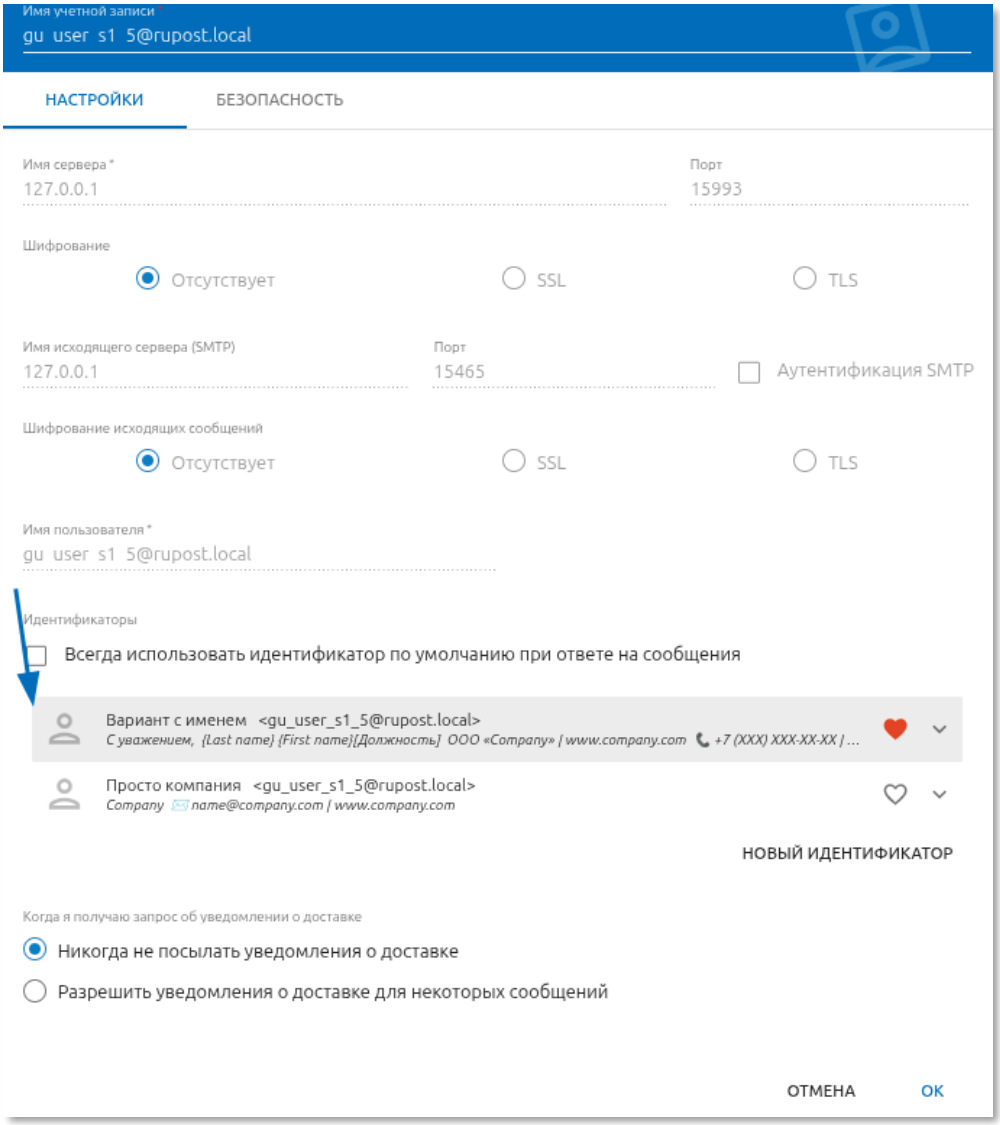
Внимание!

Для поддержки функциональности автоподписи, необходимо включить учетную запись имперсонации.

В версии 4.0 добавлена возможность задавать автоподпись для различных категорий пользователей.

Автоподпись – это часть письма, которая будет подставляться автоматически при создании нового письма пользователем.

Автоподпись конфигурируется в веб-клиенте, в настройках учетной записи имперсонации. Если необходимо создать несколько вариантов подписи (для различных групп пользователей), то создайте нужное количество профилей в учетной записи имперсонации и настройте подпись для каждого профиля.



Для персонализации автоподписи используйте шаблоны полей данных, в которых есть возможность указать требуемый атрибут адресной книги. Во время установки автоподписи для конкретного пользователя, будет осуществлена замена шаблона поля данных на данные из адресной книги для данного пользователя.

Шаблоны полей данных имеют следующий формат:

$$<“наименование атрибута адресной книги”>

Например, для того, чтобы в подпись автоответа были добавлены фамилия и имя адресата, необходимо использовать два шаблона, разделенные пробелом:

$$givenname $$sn

Пример:
С уважением,
$$givenname $$sn
$$title

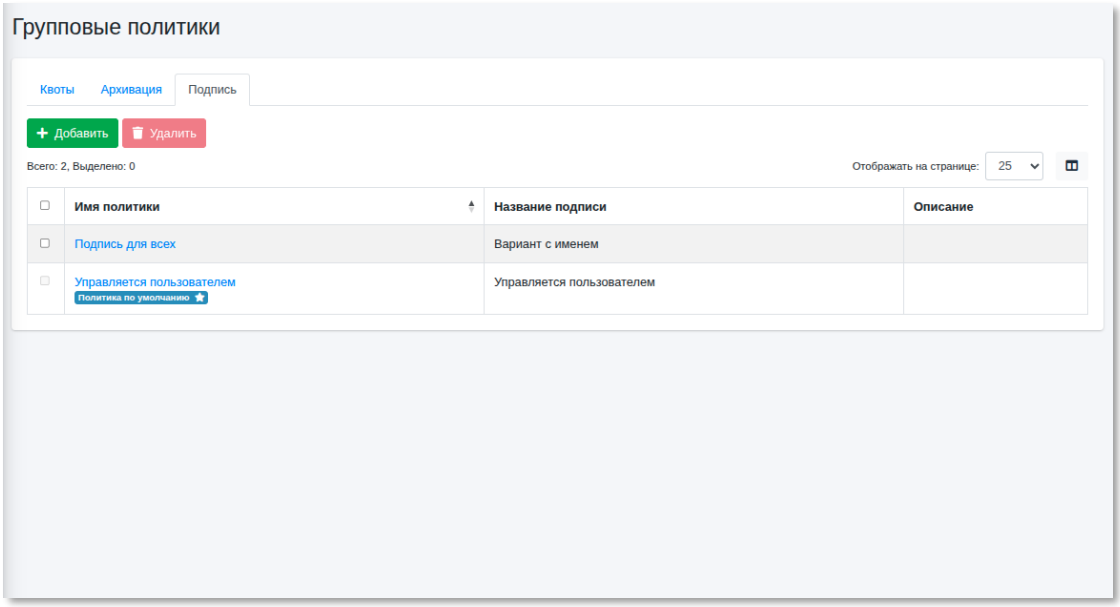
ООО «Company» | www.company.com
+7 (XXX) XXX-XX-XX $$primary_mail
[Россия, Москва, Светлый переулок 13]

В качестве атрибута адресной книги могут быть указаны:

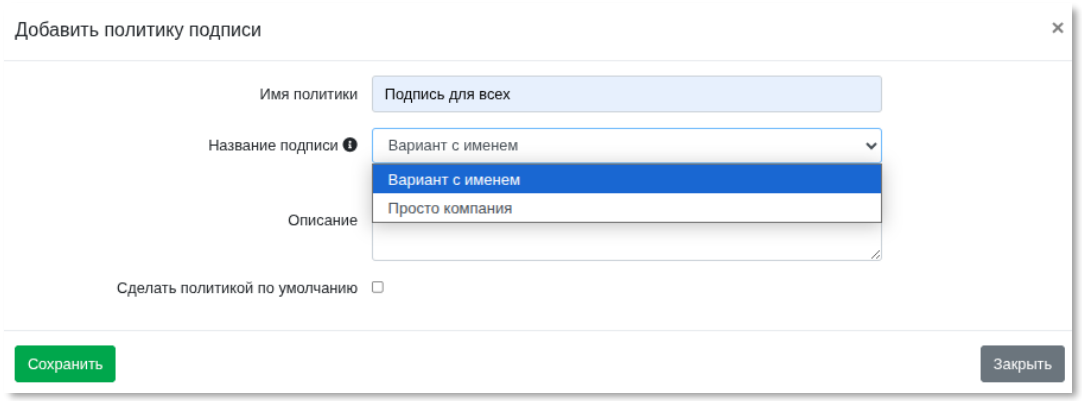
- primary_mail
- aliases
- cn
- givenname
- sn
- nsaimid
- nickname
- title
- ou
- o
- telephonenumber
- homephone
- mobile
- fax
- pager
- street
- l
- st
- c
- postalcode

- workurl
- secondemail
- homestreet
- homelocalityname
- homestate
- homecountryname
- homepostalcode
- homeurl
- description

После того, как все автоподписи в веб-клиенте сконфигурированы, для назначения подписей пользователям, в меню Панели управления выберите пункт “Получатели” -> “Групповые политики” и перейдите на закладку “Подпись”.



Создайте новую Групповую политику, из выпадающего списка выберите нужную подпись и добавьте в группу пользователей, которым должна быть назначена эта подпись.



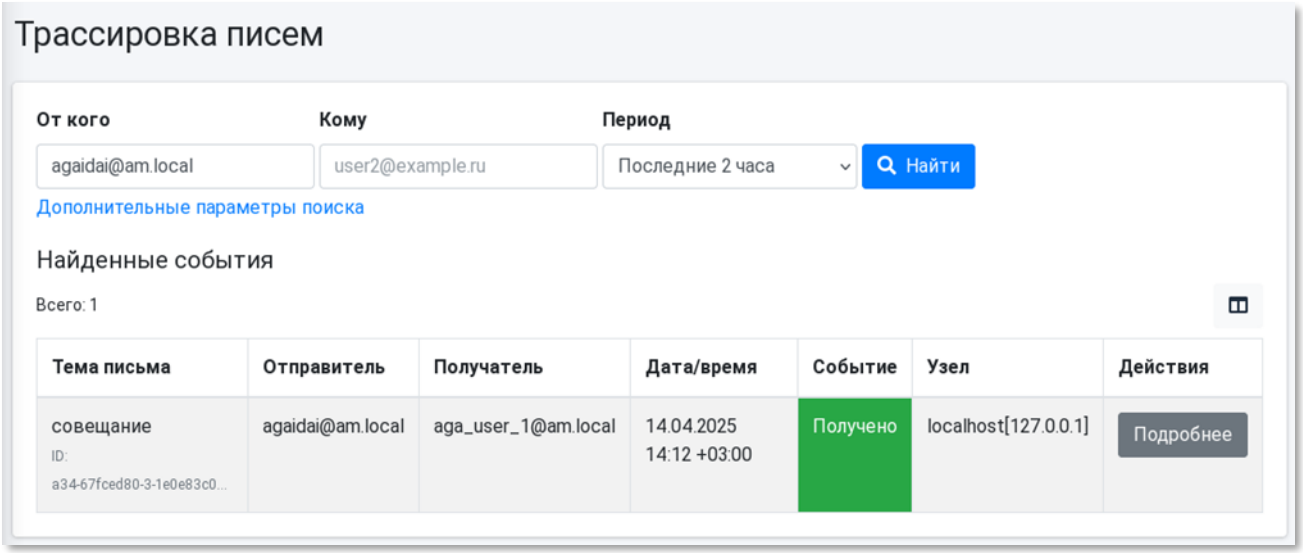
В версии 4.1.0 внесены изменения в механизм автоматического добавления корпоративной подписи к создаваемому пользователем с помощью веб-клиента rupost-mua письму.

Подпись, заданная администратором для пользователей в Групповой политике подписи, будет подставлена в создаваемое с помощью веб-клиента rupost-mua письмо даже если пользователь выбрал в настройках веб-клиента другую подпись для применения по умолчанию. Однако, в окне редактирования письма, пользователь имеет возможность затем изменить подпись, выбрав одну из тех, которые он сконфигурировал в настройках веб-клиента rupost-mua.

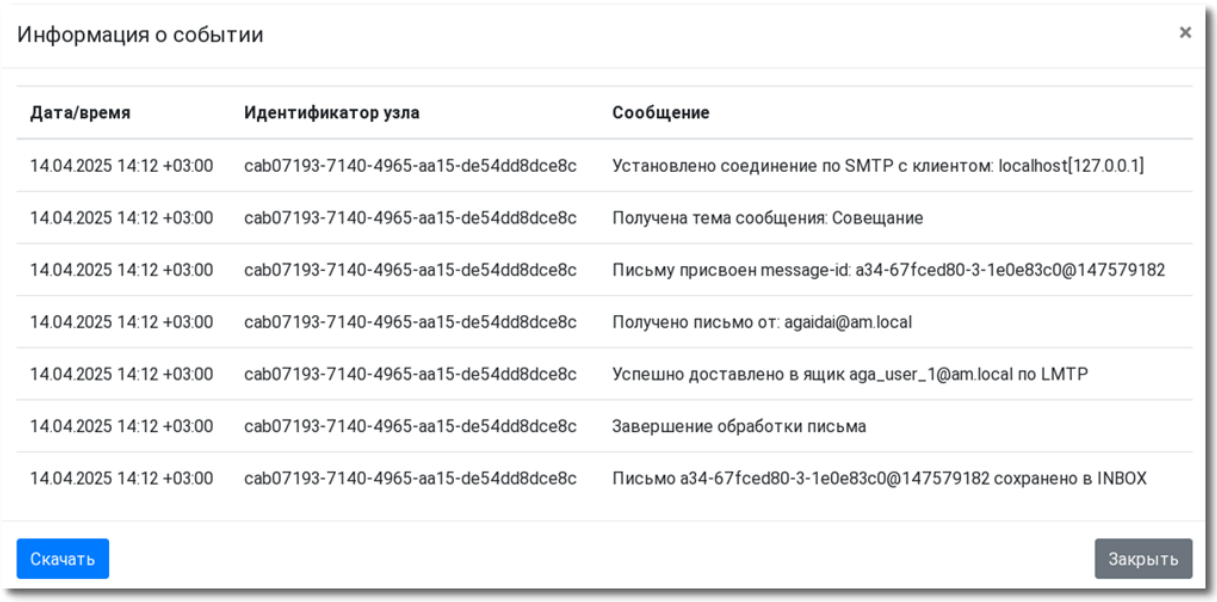
© 2021-2026 РуПост

2.24. Трассировка писем

В версии 3.3.0 в Панель управления добавлена страница “Трассировка писем” (“Получатели” -> “Трассировка писем”), которая позволяет получить информацию о том, как обрабатывалось выбранное письмо кластером RuPost.



При нажатии на кнопку “Подробнее”, для выбранного письма выводится полная информация о последовательности шагов его обработки внутри RuPost.



2.24.1. Трассировка писем – CLI

В версии 3.2.0 добавлена команда CLI для трассировки писем mail-trace, позволяющая получить информацию о статусе письма имея информацию о том, от кого, кому и когда было отправлено это письмо.

Синтаксис команды и примеры трассировки писем из командной строки приведены в разделе **«rupost mail-trace»** Справочного руководство по командной строке.

```
# rupost mail-trace
Выполняется анализ логов, подождите...

 Поседний статус:          Получено
 От:                       "office@am.local"
 Кому:                     "iivanov@zm.local"
 Время:                    2024-11-22T07:48:28
 IP адрес клиента:         127.0.0.1
 Имя клиента:              "localhost"
 Идентификатор сообщения: "bd266-67400d00-21-31c7d880@92960938"
```

2.25. Аудит действий администратора – команда CLI audit

В версии 2.5.0 добавлена регистрация всех действий администраторов, выполняемых как с использованием Панели управления, так и с помощью командного интерфейса CLI. Получить лог файл, содержащий перечень действий выбранного администратора можно через команду CLI.

В версии 3.3.0 в записи событий аудита добавлена поясняющая информация о событии – исполнитель / администратор и расширенное наименование действия. Если действие было связано с изменением настроек RuPost, то будут, также, выведены значения изменяемых параметров – как до внесения изменений, так и после.

Для просмотра событий аудита необходимо выполнить команду CLI *rupost audit*.

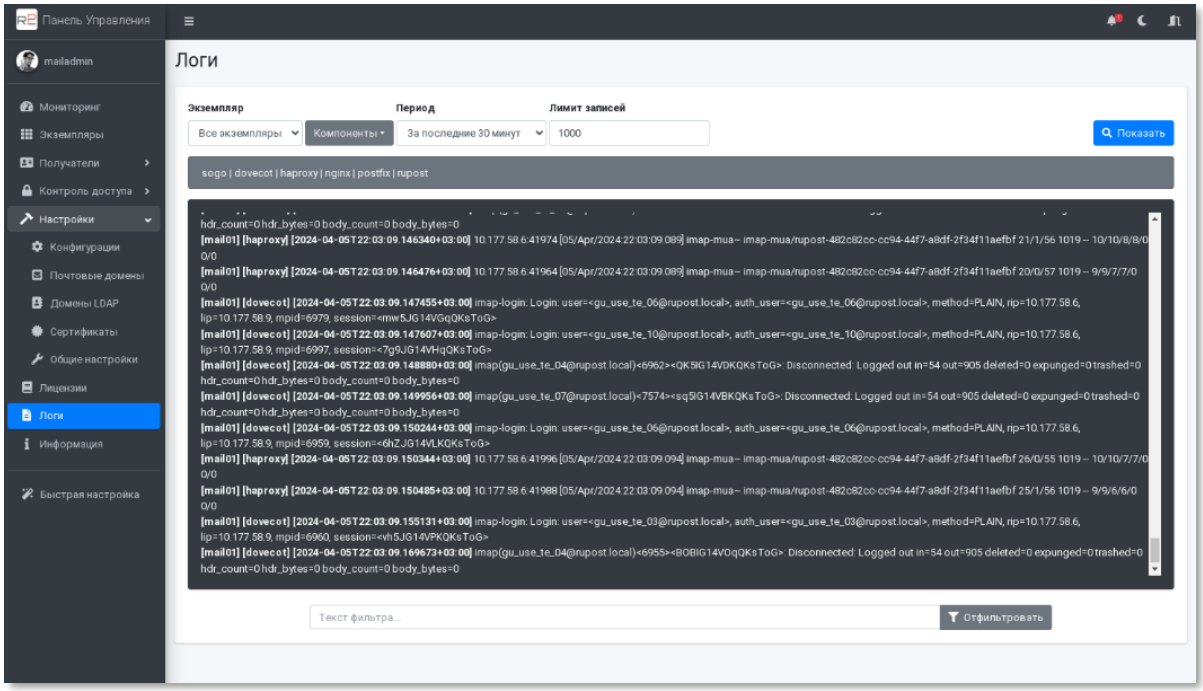
```
aadmin@mail01:~$ sudo rupost audit
2025-04-10T18:48:01+03:00 -  - cab..e8c - False - GET /services/healthcheck -
2025-04-10T18:48:32+03:00 -  - cab..e8c - False - GET /services/healthcheck -
2025-04-10T18:49:02+03:00 -  - cab..e8c - False - GET /services/healthcheck -
2025-04-10T18:49:32+03:00 -  - cab..e8c - False - GET /services/healthcheck -
2025-04-10T18:50:02+03:00 -  - cab..e8c - False - GET /services/healthcheck -
2025-04-10T18:50:32+03:00 -  - cab..e8c - False - GET /services/healthcheck -
2025-04-10T18:51:02+03:00 -  - cab..e8c - False - GET /services/healthcheck -
2025-04-10T18:51:32+03:00 -  - cab..e8c - False - GET /services/healthcheck -
2025-04-10T18:52:02+03:00 -  - cab..e8c - False - GET /services/healthcheck -
2025-04-10T18:52:32+03:00 -  - cab..e8c - False - GET /services/healthcheck -
2025-04-10T18:52:57+03:00 - mailadmin - cab..e8c - True - Попытка Входа В панель управления. -
2025-04-10T18:53:02+03:00 - mailadmin - cab..e8c - False - Получение активной конфигурации. -
2025-04-10T18:53:02+03:00 -  - cab..e8c - False - GET /services/healthcheck -
2025-04-10T18:53:02+03:00 - mailadmin - cab..e8c - False - Получение активной конфигурации. -
2025-04-10T18:53:02+03:00 - mailadmin - cab..e8c - False - Получение истории конфигураций. -
2025-04-10T18:53:02+03:00 - mailadmin - cab..e8c - False - Получение списка LDAP доменов. - {"list_pa
2025-04-10T18:53:02+03:00 - mailadmin - cab..e8c - False - Получение списка почтовых доменов. - {"lis
2025-04-10T18:53:02+03:00 - mailadmin - cab..e8c - False - Получение активной конфигурации. -
2025-04-10T18:53:02+03:00 - mailadmin - cab..e8c - False - Поиск почтовых ящиков. - {"list_params": {
 null}
2025-04-10T18:53:03+03:00 - mailadmin - cab..e8c - False - Поиск почтовых ящиков. - {"list_params": {
": null}
2025-04-10T18:53:03+03:00 - mailadmin - cab..e8c - False - Поиск почтовых ящиков. - {"list_params": {
pe": null}
2025-04-10T18:53:03+03:00 - mailadmin - cab..e8c - False - Получение списка LDAP доменов. - {"list_pa
2025-04-10T18:53:03+03:00 - mailadmin - cab..e8c - False - Возвращает данные из кеша со всех экземпля
```



Синтаксис команды и примеры управления аудитом действий администратора из командной строки приведены в разделе **«rupost audit вывод журнала активности администраторов»** Справочного руководство по командной строке.

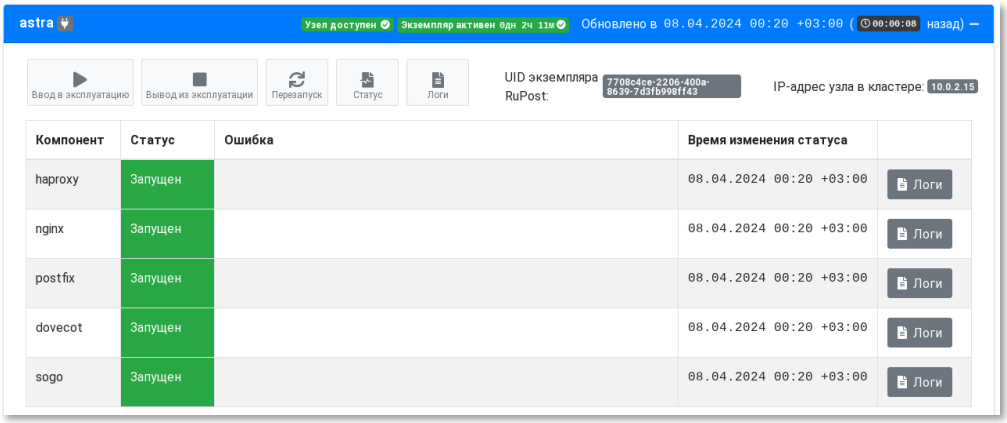
2.26. Просмотр логов почтовых компонентов в Панели управления

В версии 2.7.0 добавлена возможность просматривать логи почтовых компонентов на странице “Логи” в Панели управления.



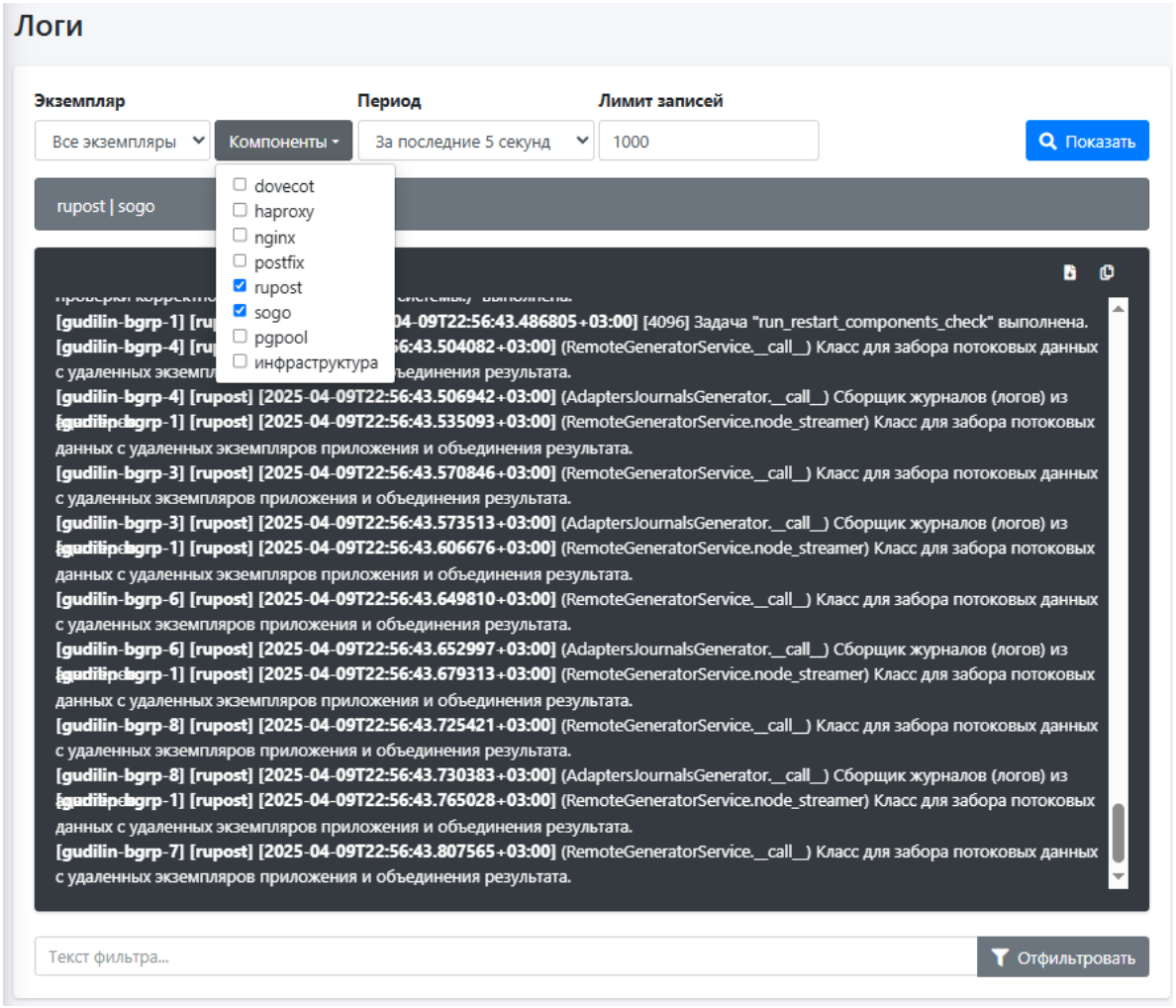
На странице “Логи” есть возможность просматривать объединенный лог всех почтовых компонентов, находящихся на различных узлах кластера либо же выбрать только некоторые узлы и компоненты. В нижней части страницы расположено текстовое поле, позволяющее осуществлять поиск введенной строки в отображаемых логах. При нажатии на кнопку “Отфильтровать” отображаются только те записи логов, в которых найдена введенная строка.

Для оперативной диагностики сбоев в работе почтовых компонентов или экземпляров RuPost вызов страницы “Логи” добавлен на все элементы страницы “Экземпляры”. При нажатии на кнопку “Логи” происходит перенаправление на страницу “Логи” с уже преднастроенным фильтром, соответствующим выбранному элементу.



В версии 3.3.0 реализован сбор со всех узлов кластера и вывод на страницу “Логи” Панели управления следующих журналов работы RuPost:

- Monitor.log (компонент RuPost)
- Rupost-scheduler (компонент RuPost)
- Rupost-queue (компонент RuPost)
- Sogo.log



2.27. Единый лог для всех почтовых компонентов – команда CLI logs

В версии 2.5.0 добавлена возможность просмотра логов всех почтовых компонентов (в кластере – со всех почтовых компонентов текущего экземпляра RuPost) в виде единого лога, синхронизированного по времени событий. Таким образом, стало гораздо удобнее диагностировать работу сервисов RuPost в случае, когда, например, обработка почтового сообщения обеспечивается взаимодействием нескольких почтовых компонент.

В версии 2.6.0:

- Реализован сбор информации со всех экземпляров RuPost – в кластерной конфигурации достаточно подключиться только к одному экземпляру RuPost и получить логи всех почтовых компонентов со всех экземпляров.
- Добавлена опция components, позволяющая указать логи каких почтовых компонентов необходимо отображать.



Синтаксис команды и примеры управления логом всех почтовых компонентов из командной строки приведены в разделе **«rupost logs вывод журнала всех почтовых компонентов»** Справочного руководство по командной строке.

2.28. Сбор и экспорт характеристик системы и лог файлов – команда CLI report

В версии 2.5.0 добавлена возможность получить информацию о системе (в кластере – с одного узла), а также все логи работы почтовых компонентов в виде одного архива. При этом формируется zip файл, содержащий следующий перечень файлов:

- app-report.txt
- hardware-report.txt
- postgres-report.txt
- licenses-report.txt
- monitor.log
- postfix.log
- dovecot.log
- nginx.log
- sogo.log
- haproxy.log

В версии 2.6.0 в команду CLI report добавлена возможность задавать диапазон времени для собираемых лог-файлов.



Синтаксис команды и примеры управления сбором и экспортом характеристик системы и лог файлов из командной строки приведены в разделе **«rupost report сбор всей информации о работе экземпляра системы»** Справочного руководство по командной строке.

2.29. Поддержка SOSReport

В версии 2.5.0 добавлена поддержка выгрузки системной информации и лог файлов через сервис SOSReport. Через этот сервис может быть получена та же информация, что и через команду CLI.

Синтаксис команды и примеры управления выгрузкой системной информации и лог файлов из командной строки приведены в разделе **«sos report поддержка выгрузки системной информации и лог файлов»** Справочного руководство по командной строке.

2.30. Глобальные правила фильтрации почты на сервере

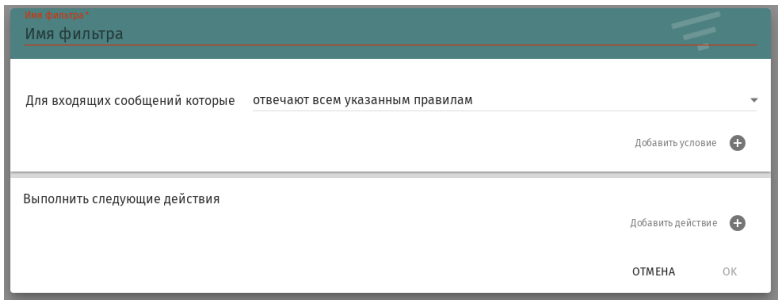
В версии 2.5.0 добавлена возможность фильтрации почтовых сообщений на сервере при помощи Sieve скриптов.
Для работы с серверными фильтрами необходимо:

1. Активировать учетную запись имперсонации и включить использование глобальных правил фильтрации командой CLI.

Синтаксис команды и примеры управления глобальными sieve скриптами из командной строки приведены в разделе **«rupost sieve группа команд для настройки работы с глобальными Sieve скриптами»** Справочного руководство по командной строке.

После этого повторно развернуть почтовую конфигурацию.

2. Войти в веб-клиент RuPost, используя учетную запись имперсонации. Для создания нового фильтра почтовых сообщений, перейдите в “Настройки” -> “Почта” -> вкладка “Фильтры” -> “Создать фильтр”.



Как видите, процесс создания/редактирования серверных правил фильтрации сообщений ничем не отличается от создания клиентских фильтров, но фильтры, созданные под учетной записью имперсонации, становятся серверными фильтрами для всех экземпляров RuPost.
При наличии и клиентских и серверных скриптов Sieve, сначала будут выполнены серверные скрипты, затем клиентские.

Внимание!

В версии 4.2.0 при использовании sieve-правила, которое в себе содержит “Послать сообщение об отказе”, оповещение об отказе доставлено не будет.

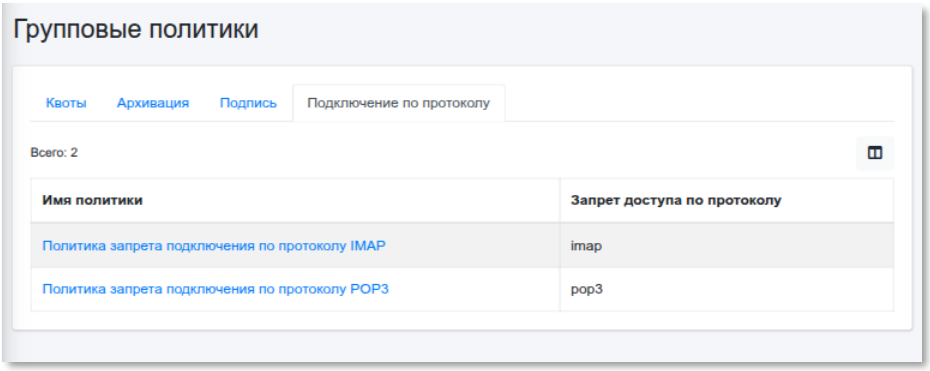
2.31. Блокировка доступа в web клиент LDAP пользователей при отсутствии ящиков

В версии 3.1.0 добавлена проверка наличия почтового ящика у пользователя при попытке получить доступ к календарям и адресным книгам.

2.32. Групповая политика - ограничение доступа к почтовым ящикам по протоколам POP3 / IMAP

В версии 4.2.0 добавлена возможность отключения доступа клиентских приложений к RuPost по протоколам IMAP и POP3 для групп пользователей.

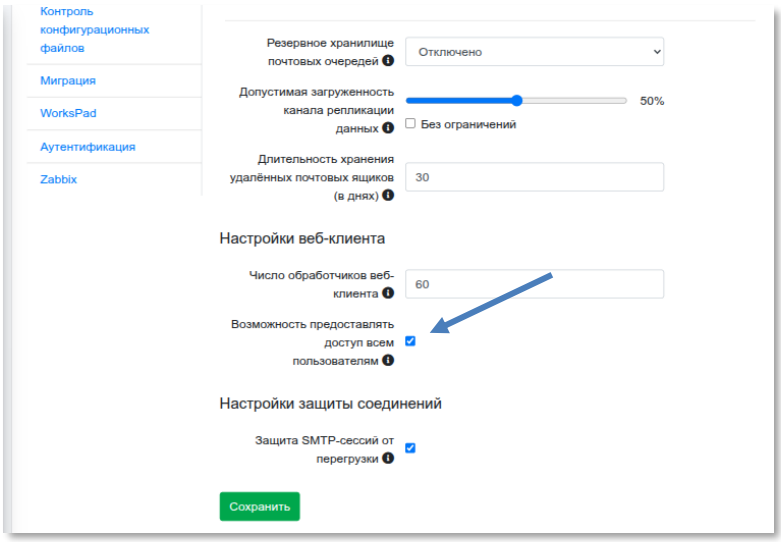
Для управления доступом клиентских приложений, которые используют протоколы IMAP и POP3, добавлены соответствующие Групповые политики. По умолчанию, всем пользователям доступ по IMAP и POP3 разрешен. Для того, чтобы для отдельных пользователей отключить возможность использования протоколов IMAP и POP3, необходимо им назначить соответствующую Групповую политику (страница “Групповые политики”, вкладка “Подключение по протоколу”).



2.33. Управление возможностью предоставления доступа к своему почтовому ящику всем пользователям

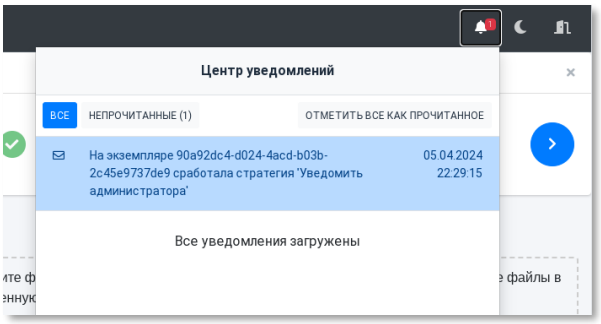
В версии 4.2.0 добавлено управление возможностью предоставления доступа пользователем к своему почтовому ящику всем пользователям.

Для отключения возможности предоставления доступа пользователем к своему почтовому ящику всем пользователям, нужно в “Общих настройках” снять переключатель “Возможность предоставления доступа всем пользователям” (страница “Общие настройки”, вкладка “Почта”).



2.34. Система уведомлений администратора

В версии 2.7.0 в Панель управления RuPost добавлена Система уведомлений администратора.

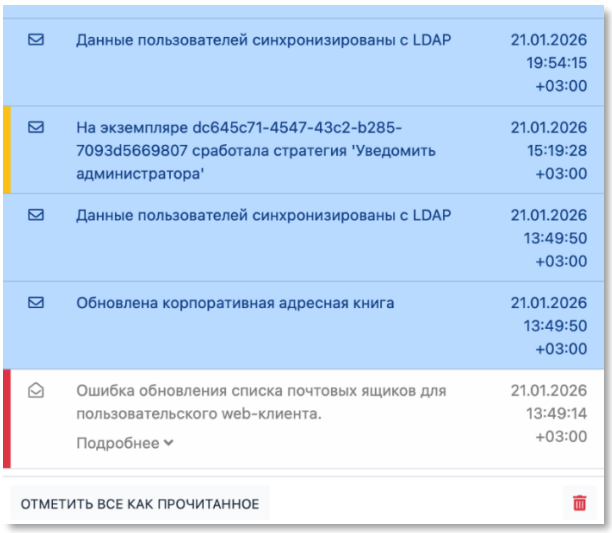


Система уведомлений позволяет серверу RuPost отправлять сообщения администраторам в случаях, требующих внимания администратора или информирующих администратора о событиях, которые произошли во время его отсутствия. Например, о срабатывании стратегии контроля целостности конфигурационных файлов либо о завершении длительных фоновых процессов. При появлении новых сообщений, в верхней части Панели управления отображается соответствующий индикатор. Каждое сообщение имеет статус “прочитано / не прочитано” и есть возможность отметить все сообщения как прочтенные.

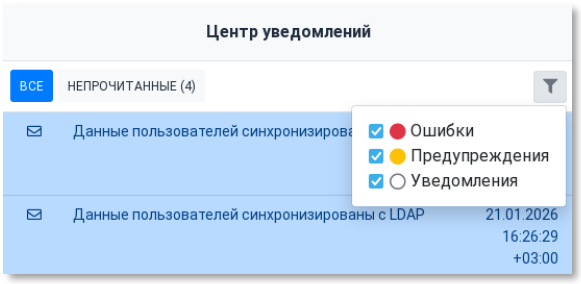
В версии 4.1.0 добавлено цветовое выделение ошибок и предупреждений в окне “Уведомления”.

Уведомление имеют один из следующих типов:

- **Уведомление** – информационное сообщение, цветом не выделяется.
- **Предупреждение** – сообщение о том, что есть не критичное отклонение от нормального функционирования системы, выделяется жёлтым цветом.
- **Ошибка** – сообщение об ошибке, выделяется красным цветом.



Кроме того, администратор имеет возможность отфильтровать уведомления по типу, например, отображать только ошибки.



2.35. Предупреждения пользователей об исчерпании квоты на место в почтовом ящике

В версии 2.7.0 добавлена возможность оповещения пользователей о различных уровнях использовании квоты на место в почтовом ящике. При использовании квоты на 70%, 80% и 95% пользователь получает соответствующее письмо-оповещение.

В версии 4.1.0 изменена схема проверки квоты на размер ящика.

При получении письма, проверка квоты производится не на компоненте *rupost-mta*, а на компоненте *rupost-mda*, перед сохранением письма в почтовый ящик.

Это позволяет улучшить работу списков рассылки – те пользователи, у которых нет превышения квоты, получат сообщение, отправленное на список рассылки, даже если среди адресатов списка рассылки есть те, у которых квота превышена.

2.36. Аудит действий пользователя в ящике

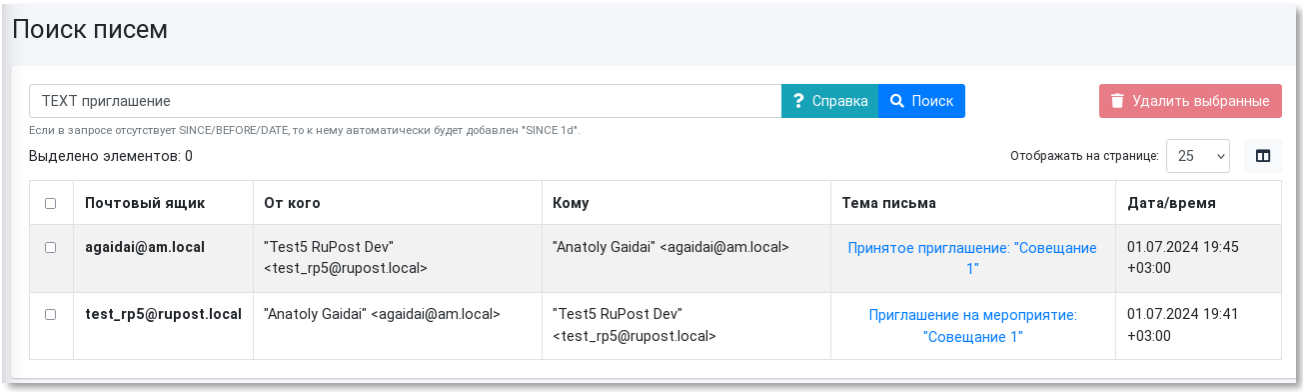
В версии 2.7.0 добавлена возможность отслеживания действий, которые пользователь совершает в своем почтовом ящике, например, удаление письма, переименование папки и пр. Управление этой функцией осуществляется при помощи команды CLI.

Синтаксис команды и примеры управления логированием действий почтовых ящиков из командной строки приведены в разделе **«rupost user-audit для управления логированием действий почтовых ящиков»** Справочного руководство по командной строке.

При включении логирования можно указать перечень почтовых ящиков, действия в которых необходимо отслеживать. Также, можно выбрать, какие действия пользователя нужно регистрировать. Лог действий пользователя записывается в файл /var/log/mail.log .

2.37. Поиск и удаление писем

В версии 3.0 добавлена возможность поиска и удаления нежелательной почты в почтовых ящиках пользователей в Панели управления RuPost (пункт меню “Получатели”->“Поиск писем”).



Для поиска писем введите критерий поиска с указанием команд фильтрации почты (синтаксис команд - см. внизу). Справочник по командам также доступен на странице при нажатии на кнопку “Справка”.

Результат поиска отображается в таблице – в качестве идентификатора почтового ящика (столбец “Почтовый ящик”), в котором найдено письмо, используется первичный почтовый адрес.

Для просмотра содержимого письма, нажмите на ссылку в столбце “Тема письма”.

Для удаления писем, отметьте их в левом столбце таблицы результатов поиска и нажмите на кнопку “Удалить выбранные”.

Управление правами доступа к странице “Поиск писем” производится через редактирование разрешений полномочий администраторов.

Команды поиска писем

ALL – ищет все письма;
ANSWERED - письма с установленным флагом IMAP "Answered";
BCC *строка* - письма, которые содержат указанную строку в поле BCC структуры IMAP письма;
BEFORE *дата* - письма с внутренней датой до указанной даты;
BODY *строка* - письма, которые содержат указанную строку в теле письма;
CC *строка* - письма, которые содержат указанную строку в поле CC структуры IMAP письма;
DELETED - письма с установленным флагом IMAP "Deleted";
DRAFT - письма с установленным флагом IMAP "Draft";

FLAGGED - письма с установленным флагом IMAP "Flagged";
FROM *строка* - письма, которые содержат указанную строку в поле FROM структуры IMAP письма;
HEADER *поле строка* - письма, которые имеют указанное поле заголовка, если передана пустая строка. Или письма, для которых указанное поле заголовка содержит заданную строку;
KEYWORD *ключевое слово* - письма с установленным флагом для переданного ключевого слова IMAP (например $Forwarded);
LARGER *размер* - письма, которые больше указанного размера;
MAILBOX *имя* - письма в почтовом ящике с указанным именем;
NEW - письма, с установленным флагом IMAP "Recent", но с неустановленным флагом IMAP "Seen";
NOT *ключ поиска* - письма, где поиск не соответствует указанному ключу поиска или его значению;
OLD - письма, у которых не установлен флаг IMAP "Recent";
ON *дата* - письма, внутренняя дата которых соответствует указанной дате;
ключ поиска **OR** *ключ поиска* - письма, для которых совпадает один из ключей поиска, указанных до и после OR;
RECENT - письма с установленным флагом IMAP "Recent";
SAVEDBEFORE *дата* - письма, которые были сохранены до указанной даты;
SAVEDON *дата* - письма, дата сохранения которых соответствует указанной дате;
SAVEDSINCE *дата* - письма, которые были сохранены после указанной даты;
SEEN - письма с установленным флагом IMAP "Seen";
SENTBEFORE *дата* - письма с заголовком Date до указанной даты;
SENTON *дата* - письма с заголовком Date соответствующим указанной дате;
SENTSINCE *дата* - письма с заголовком Date после указанной даты;
SINCE *дата* - письма, внутренняя дата которых находится в пределах или после указанной даты;
SMALLER *размер* - письма, которые меньше указанного размера;
SUBJECT *строка* - письма, которые содержат указанную строку в поле SUBJECT структуры IMAP письма;
TEXT *строка* - письма, которые содержат указанную строку в заголовках или теле письма;
TO *строка* - письма, которые содержат указанную строку в поле TO структуры IMAP письма;
UNANSWERED - письма с не установленным флагом IMAP "Answered";
UNDELETED - письма с не установленным флагом IMAP "Deleted";
UNDRAFT - письма с не установленным флагом IMAP "Draft";
UNFLAGGED - письма с не установленным флагом IMAP "Flagged";
UNKEYWORD *ключевое слово* - письма, для которых не установлен флаг передаваемого ключевого слова IMAP;
UNSEEN - письма с не установленным флагом IMAP "Seen";

Спецификация дат

dd-mon-yyyy - формат даты IMAP4rev1 по умолчанию.
day - день месяца: 1-31.
month - сокращённое название месяца: Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, Oct, Nov или Dec.
year - четыре цифры года, например 2024.
dd-mon-yyyy hh:mm:ss [+-]zzzz - форматы даты/времени IMAP4rev1 по умолчанию. См. dd-mon-yyyy выше для формата даты.
Для формата времени:
hh - часы
mm - минуты
ss - секунды
[+-]zzzz - часовой пояс в формате hhmm, например +0530, -0700

Interval - комбинация положительного целого числа и единицы времени. Доступные единицы времени:

weeks - аббревиатура: w
days - аббревиатура: d
hours - аббревиатура: h
mins - аббревиатура: m
secs - аббревиатура: s

Временная метка Unix - временная метка Unix, состоящая из 10 цифр, представляющая количество секунд с 1 января 1970, 00:00:00 UTC. Например “13 апреля 2007” будет отображено как 1176418800.
YYYY-MM-DD - расширенный формат даты ISO-8601. Например “13 апреля 2007” будет отображено как 2007-04-13.

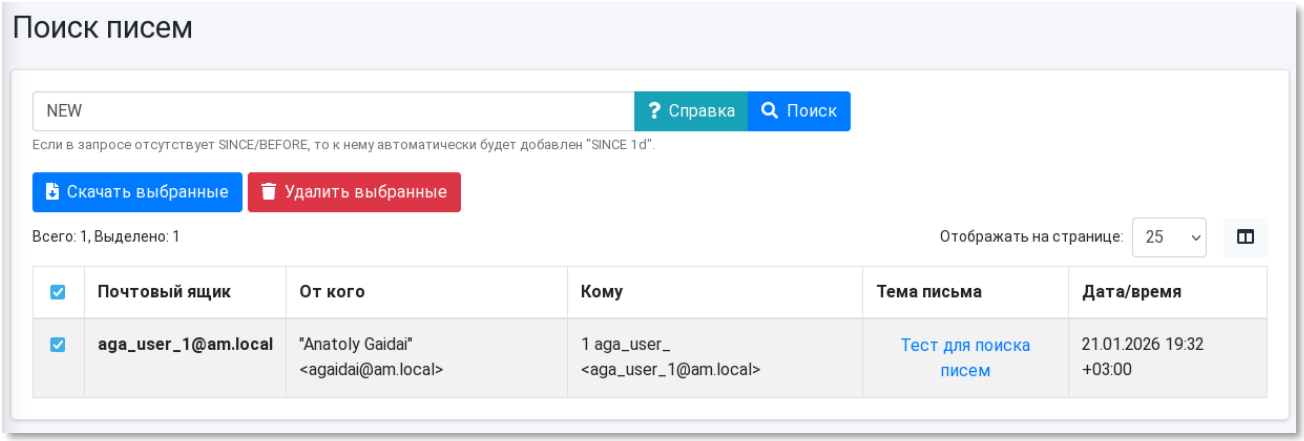
Спецификация размеров

Размер - размер письма в B (байтах), k (килобайтах), M (мегабайтах), G (гигабайтах) или T (терабайтах). Для соответствия письмам более чем 1 мегабайт, вы можете указать, например: более 1M или более 1024k.

В версии 3.2.0 добавлена возможность сохранения найденного письма в файл на странице “Поиск писем”. Для того, чтобы сохранить письмо, откройте выбранное письмо и нажмите на кнопку “Скачать” – файл с текстом письма будет сохранен в папку “Загрузки” вашего браузера. Файл имеет текстовый формат, сохраняется только текст письма. Если в письме есть вложения, то они не сохраняются.

2.37.1. Выгрузка найденных писем в формате eml

В версии 4.1.0 добавлена возможность сохранения найденных писем в формате eml.



Для того, чтобы сохранить письмо, находящееся в списке результатов поиска, в формате eml, нужно на странице “Поиск писем” выбрать нужное письмо, перейти по ссылке в колонке “Тема письма” – откроется окно просмотра письма.



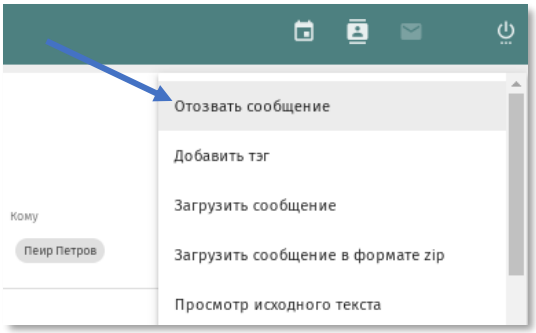
Для сохранения письма в формате eml, нажмите кнопку “Скачать как eml” – будет сформирован и загружен файл eml, содержащий просматриваемое письмо. Обратите внимание, что если в письме есть вложения, то они также будут добавлены в eml-файл.

2.37.2. Отзыв писем

Внимание!

Отзыв сообщений работает только для почтовых ящиков, обслуживаемых RuPost – письмо, отправленное на внешний адрес, не может быть отозвано.

В версии 3.1.0 реализован механизм отзыва писем. Если пользователь отправил письмо по ошибке и хотел бы его удалить из почтовых ящиков получателей, то, для этого, он может воспользоваться новым пунктом меню веб клиента RuPost “Отозвать сообщение”.



Отзыв писем осуществляется за счет обработки сообщений в специальном служебном почтовом ящике, имеющем адрес recall@rupost.corp. После обработки сообщения (запроса на удаление письма) пользователю придет письмо с результатами попытки удаления сообщения из всех почтовых ящиков, где оно было найдено.

Статус прочтения письма (прочитано / нет) не влияет на возможность удаления письма из ящика получателя.

Для отзыва письма пользователем в веб-клиенте RuPost, нужно:

1. перейти в папку “Отправленные”;

2. открыть письмо, которое нужно отозвать;
3. нажать на “…” и в выпадающем меню выбрать пункт “Отозвать сообщение” – будет подготовлена форма отправки письма для отзыва;
4. убедиться, что отображается нужное письмо и нажать кнопку “Отправить”.

В версии 3.2.0 для ускорения выполнения Отзыва писем при больших объемах почтовых ящиков внесены следующие изменения в механизм поиска писем для удаления:

- Поиск осуществляется не по всем почтовым ящикам, а только по почтовым ящикам адресатов – т.е. указанным в полях “Кому”, “Копия” и “Скрытая копия”.
- Таймаут при поиске письма увеличен до 5 минут.

2.38. Управление push-уведомлениями – команда CLI push

При получении нового письма, пользователь может получать уведомление об этом на мобильном устройстве с помощью push-уведомлений. Управление push-уведомлениями осуществляется с помощью CLI.

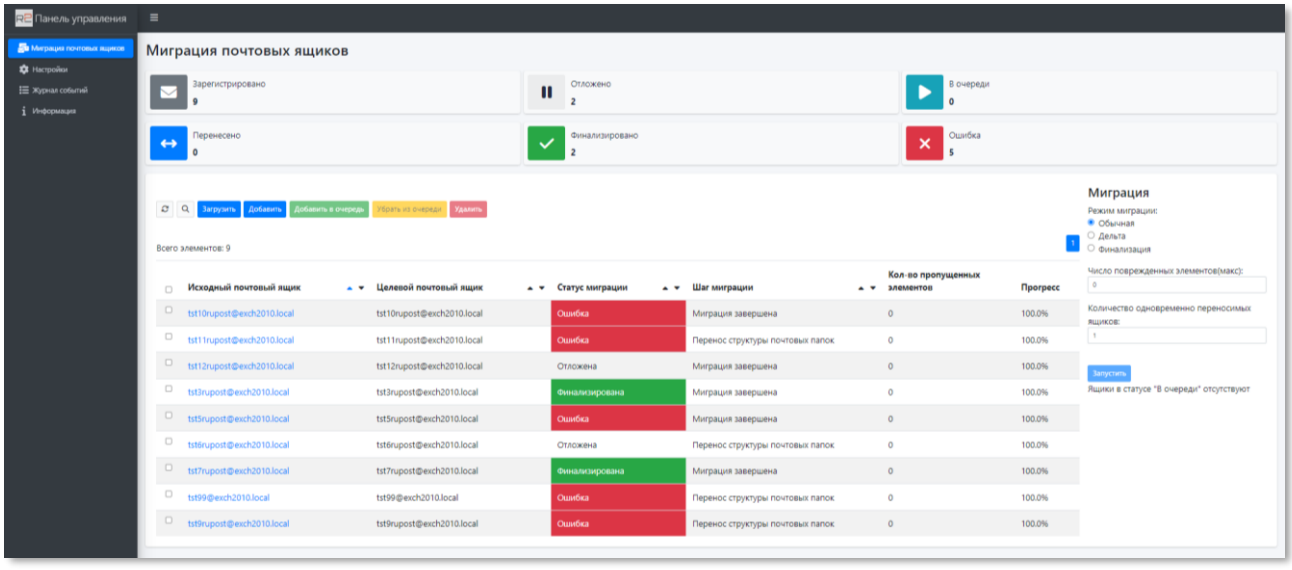
Синтаксис команды и примеры управления push уведомлениями из командной строки приведены в разделе **«rupost push группа команд для управления push уведомлениями»** Справочного руководство по командной строке.

2.39. Панель управления инструмента миграции с Microsoft Exchange

Внимание!

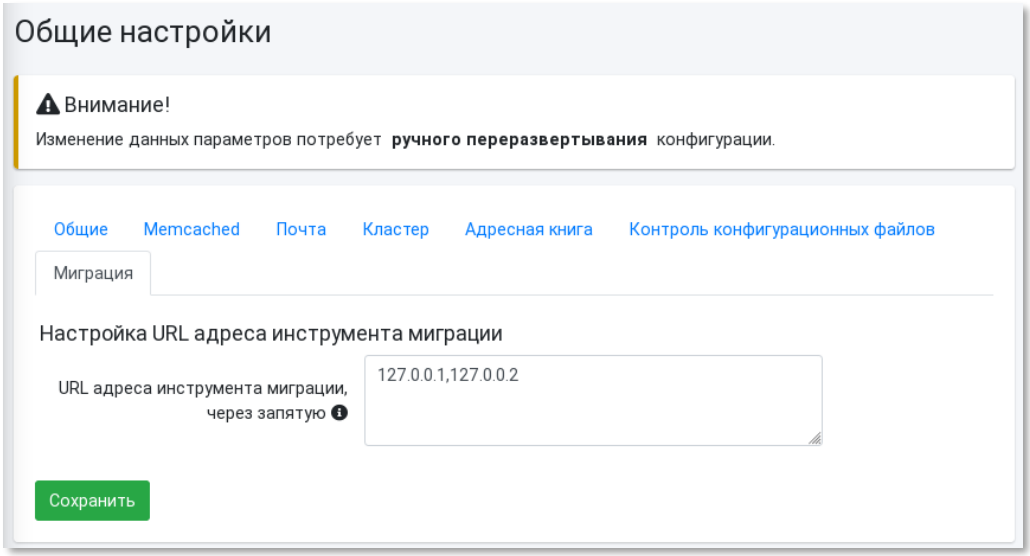
Версия инструмента миграции должна быть не ниже 2.5.0.

В версии 2.5.0 в инструмент миграции добавлен веб-интерфейс - Панель управления инструмента миграции, которая позволяет визуально конфигурировать, запускать и контролировать процесс миграции почтовых ящиков, календарей и адресных книг из Microsoft Exchange в RuPost.

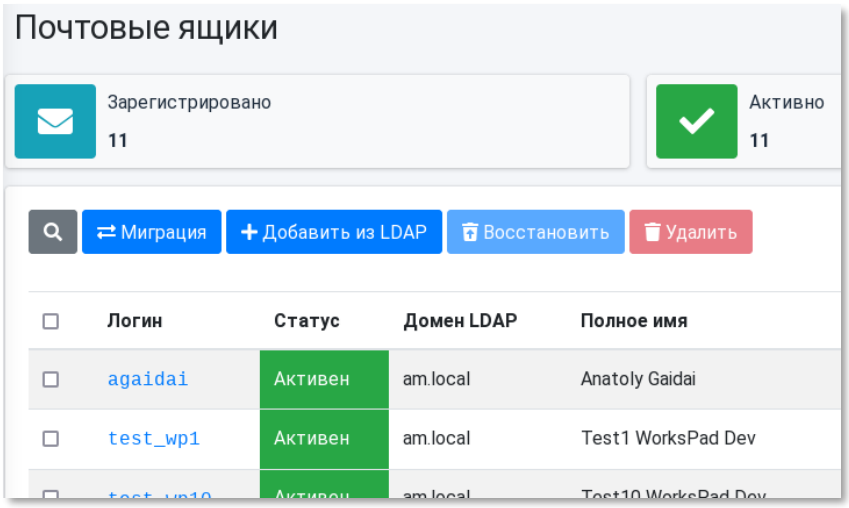


Для вызова инструмента миграции из Панели управления RuPost необходимо задать URL Панели управления инструмента миграции на странице “Общие настройки” -> вкладка “Миграция”.

В версии 3.0 добавлена возможность аутентификации в LDAP администратора через RuPost при запуске Инструмента миграции. Все экземпляры Инструмента миграции должны быть зарегистрированы через “Общие настройки” RuPost (закладка “Миграция”). В поле “URL адреса инструмента миграции” можно добавить FQDN серверов, где установлен Инструмент миграции (разделитель – запятая).



После задания этого параметра, Панель управления инструмента миграции может быть вызвана по кнопке “Миграция” на странице “Почтовые ящики”.



Если зарегистрировано несколько Инструментов миграции, то на странице “Почтовые ящики” по кнопке “Миграция” будет вызван первый из списка.

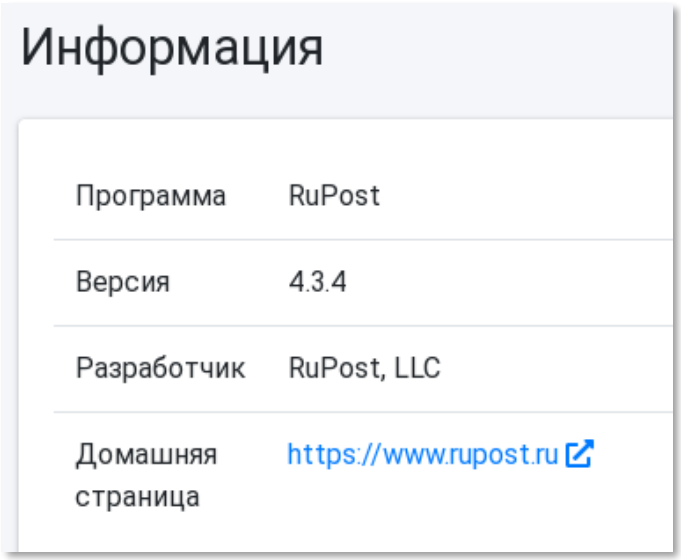
2.39.1. Отсутствие дублирования сообщений при миграции с Microsoft Exchange

В версии 2.7.0 добавлен статус почтового ящика “Миграция”. Ящик, имеющий этот статус, доступен для подключения по протоколу IMAP, но не получает почту по SMTP/LMTP. При использовании сценария сосуществования RuPost-Exchange (когда сервер Exchange является релеем для RuPost) это помогает избежать дублирования сообщений в мигрируемом ящике. Во время миграции с Microsoft Exchange на RuPost пользователь продолжает пользоваться своим почтовым ящиком на сервере Exchnage, но имеет возможность подключиться и к своему ящику на сервере RuPost для мониторинга процесса переноса почты.

Инструмент миграции RuPost управляет установкой и снятием статуса “Миграция”, так что по окончании процесса миграции почтовый ящик автоматически получает статус “Активен”.

2.40. Информация о версии системы

Страница “Информация” в Панели управления содержит данные об используемой версии (сборке) RuPost.



Командный интерфейс CLI для показа информации о системе позволяет получить не только информацию о версии RuPost но еще и информацию о лицензии.

Для поддержки сценариев автоматизированного развертывания RuPost, в версии 2.6.0 в команду CLI about добавлена возможность управления набором выводимой информации.

Синтаксис команды и примеры управления выводом краткой справки о приложении из командной строки приведены в разделе **«rupost about вывод краткой справки о приложении»** Справочного руководство по командной строке.

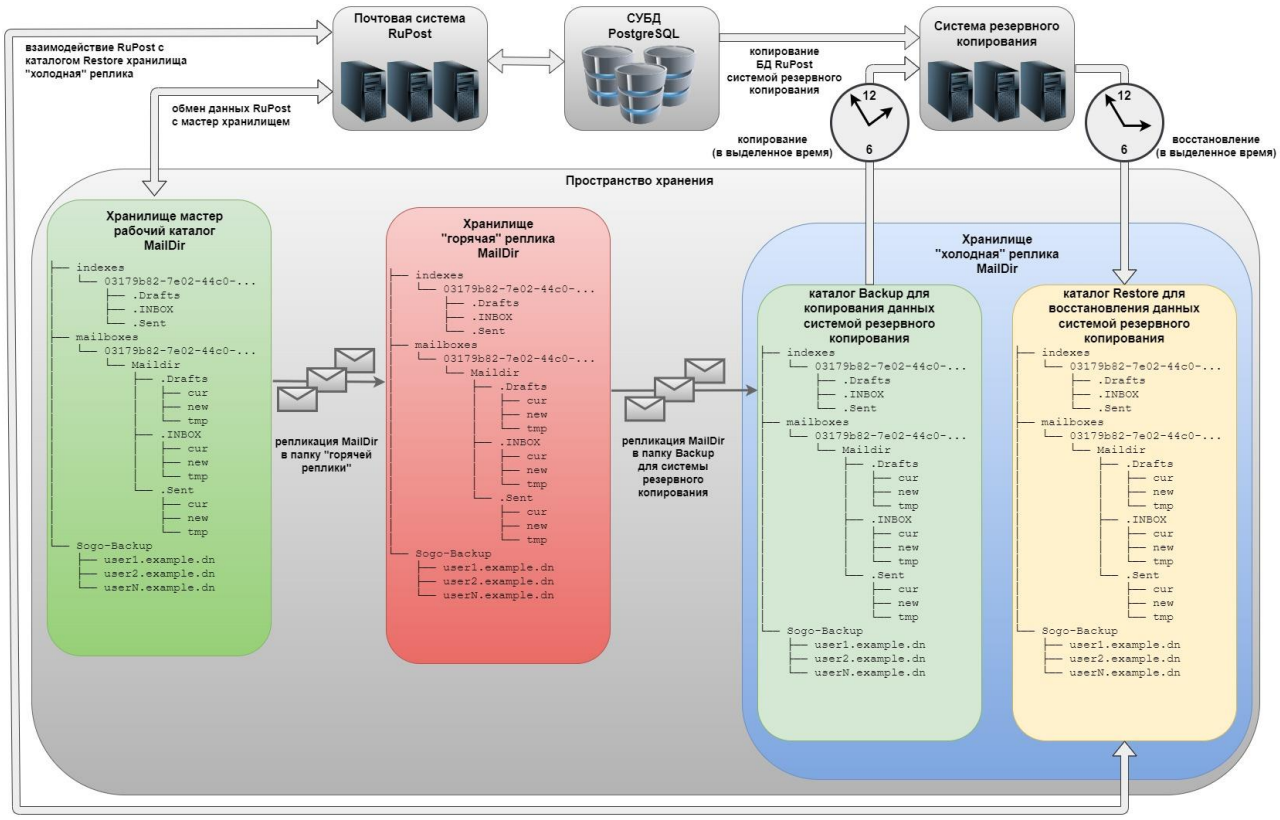
3. Работа с системой резервного копирования (СРК)

Начиная с версии 3.2.0 поддерживается интеграция с СРК RuBackup версии 2.4 и выше.

В версии 3.0 добавлена поддержка работы с Системой резервного копирования (СРК) – как в части поддержки резервного копирования почтовых ящиков, календарей и контактов пользователей, так и в части восстановления этих данных из СРК.

Для того, чтобы в процессе работы СРК совместно с RuPost не возникало дополнительной нагрузки на компоненты RuPost, предусмотрен специальный тип Хранилища – Backup (“холодная реплика”), которое используется как источник данных для системы резервного копирования (СРК). Периодичность синхронизации Backup-хранилища, в общем случае, имеет гораздо больший интервал (т.е. больше "отстает" от мастер-хранилища) чем у slave-хранилищ ("горячих" реплик). Backup-хранилище не может быть назначено мастером, т.е. на него нельзя переключить обслуживание почты. В каждое Пространство хранения может быть добавлено только одно Backup-хранилище.

Схема взаимодействия RuPost и СРК:



Для обеспечения двустороннего обмена между RuPost и СРК корневая структура папок Backup-хранилища состоит из двух папок - Backup и Restore. Папку Backup создает RuPost после завершения формирования «холодной» реплики. Папку Restore создает СРК после завершения восстановления из РК. Соответственно, RuPost периодически (в соответствии со свойством Пространства хранения "Период обновления "Backup" хранилища") копирует контент хранилища-источника (одной из "горячих" реплик) в папку Backup. При запуске администратором RuPost утилиты командной строки

`rupost backup cold-restore` с заданными параметрами происходит обработка данных, лежащих в папке Restore. В разделе 3.2.2. Восстановление из «холодной реплики» данного документа приведены различные примеры восстановления.

Для того, чтобы разгрузить мастер-хранилище, в качестве источника данных для Backup-хранилища выбирается slave-хранилище с минимальным весом из имеющих статус Active.

Для обеспечения возможности использования Backup-хранилища как единой точки взаимодействия с СРК для нескольких Пространств хранения, проверка на уникальность отключена для точек монтирования Backup-хранилища в рамках Пространств хранения. Это означает, что одни и те же точки монтирования могут быть заданы для Backup-хранилища в нескольких Пространствах хранения - таким образом, резервное копирование всех почтовых ящиков RuPost может осуществляться через единую точку взаимодействия с СРК.

Так как никакие механизмы блокировки / разделения доступа между RuPost и СРК не используются, то совместная работа этих двух систем с Backup-хранилищем обеспечивается за счет разделения времени (time-sharing). В настройках Пространства хранения задается интервал, когда RuPost не производит никаких операций с Backup-хранилищем (свойство "Интервал для СРК") - в это время СРК может производить любые операции с файлами Backup-хранилища.

При копировании данных на Backup-хранилище, для возможности определения соответствия основного почтового адреса пользователя почтового ящика и папки MailDir, в каждой папке почтового ящика MailDir создается дополнительный файл, содержащий адрес электронной почты пользователя (Primary e-mail), идентификатор группы ящиков и название группы ящиков.

Файл-идентификатор расположен в корневом каталоге папки Maildir:

<путь до хранилища>/<mailbox_id>/srk_index.

Пример содержания файла-идентификатора:

test_email@am.local,89d5f93a-3aa9-454d-80bc-f51596856822,test group name

3.1. Основные сценарии работы с СРК

Резервное копирование Пространства хранения в СРК
RuPost периодически (в соответствии со свойством Пространства хранения "Период обновления "backup" реплики") копирует контент хранилища-источника ("горячей" реплики) в папку Backup. Для ускорения операций с Backup-хранилищем, RuPost не очищает папку Backup перед началом копирования, а, при наличии контента в папке Backup, обновляет его. Операция копирования из "горячей" реплики в Backup-хранилище завершается до начала интервала для СРК. СРК осуществляет дальнейшее резервное копирование в рамках интервала для СРК.
Восстановление существующего почтового ящика из СРК
При необходимости восстановления почтового ящика из СРК, СРК (в рамках своего временного "окна") копирует папки восстанавливаемых ящиков из СРК в папку Restore Backup-хранилища. Если в папке Restore есть Maildir папка, то RuPost будет ее использовать для восстановления содержимого почтового ящика. Порядок восстановления ящика следующий:

- Поиск почтового ящика по его ID или Primary-email (если поиск по ID не дал результатов).
- Восстановление ящика. Восстановление ящика выполняется переносом информации с Backup-хранилища на мастер-хранилище.

Восстановление ранее удаленного почтового ящика из СРК

Если почтовый ящик уже был ранее удален, то перед восстановлением нужно создать ящик для этого пользователя (через импорт или Панель управления RuPost). Затем, порядок действий такой же, как описано в "Восстановление существующего почтового ящика из СРК".

Восстановление Пространства хранения из СРК

Для восстановления Пространства хранения из СРК, все почтовые ящики этого Пространства хранения должны быть восстановлены из СРК в папку Restore Backup-хранилища. В ходе восстановления, почтовый ящик автоматически не создается и не перепривязывается к другой Группе ящиков - т.е. восстановление будет произведено только существующих ящиков в соответствии с порядком, описанным в "Восстановление существующего почтового ящика из СРК".

3.2. Восстановление данных пользователей на сервере RuPost

Одной из важных возможностей системы RuPost является **восстановление данных пользователей из резервной копии.**

Внимание!

Для обеспечения сохранности пользовательских данных необходимо использовать возможности системы RuPost по созданию резервных почтовых очередей, «горячей» и «холодной» реплик каталога сообщений, а также регулярно выполнять резервное копирование «холодной реплики» с использованием СРК или другим способом.

Выполнение резервная копии службы каталогов сохранит логин/пароль и основной почтовый адрес пользователей.

Периодическое создание резервной копии на сервере СУБД PostgreSQL баз данных RuPost (rupost, rupost_gamma, rupost_data, rupost_shared) обеспечит сохранность данных о конфигурации системы RuPost.

При наличии резервной копии «холодной реплики» почтовая система RuPost предоставляет администратору широкие возможности восстановления как данных всех пользователей системы, так и отдельного почтового ящика, сообщений электронной почты или календаря пользователя. Начиная с **версии 3.2** восстановление выполняется с использованием группы команд утилиты командной строки **rupost backup**.



Синтаксис команд для работы с резервными копиями приведены в разделе **«rupost backup группа команд для работы с резервными копиями»** Справочного руководство по командной строке.

3.2.1. Создание «холодной реплики»

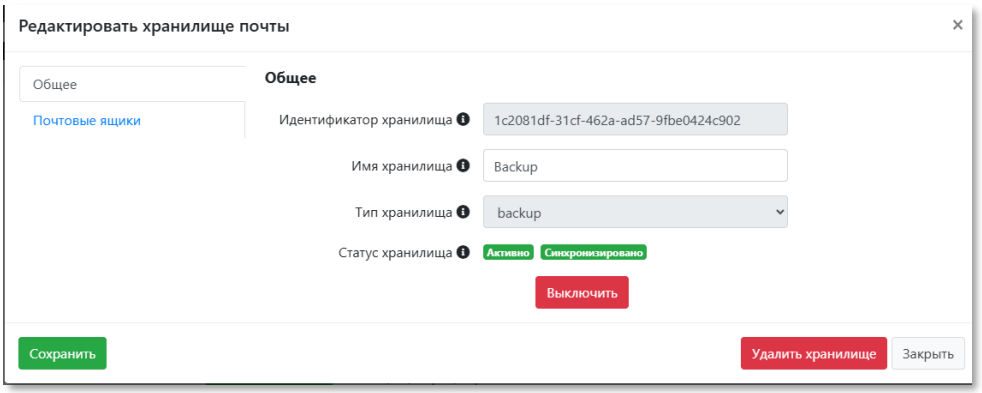
Пример просмотра структуры каталога «холодной реплики системы RuPost.

```
tree -a -L 3 /home/rupost/1c2081df-31cf-462a-ad57-9fbe0424c902

/home/rupost/1c2081df-31cf-462a-ad57-9fbe0424c902 <- ID «холодной реплики»*
└── mailboxes
    ├── Backup                                    <- каталог для СРК (создание РК, RuPost)
    │   ├── 178c5b8c-c94f-42e0-ae87-237bd8bdca24  <- каталог сообщений пользователя
                        ...
    │   ├── d6b193d4-799b-43f1-a6b8-e2be04430718  <- каталог сообщений пользователя
    │   ├── rupost_version                        <- файл с версией RuPost
    │   └── sogo-backup                           <- каталог календарей пользователей
    └── Restore                                   <- каталог для СРК (восстановление РК, СРК)
        ├── 178c5b8c-c94f-42e0-ae87-237bd8bdca24  <- каталог сообщений пользователя
                        ...
        ├── d6b193d4-799b-43f1-a6b8-e2be04430718  <- каталог сообщений пользователя
        ├── rupost_version                        <- файл с версией RuPost
        └── sogo-backup                           <- каталог календарей пользователей
```

*** получить ID «холодной реплики» можно:**

- В графическом интерфейсе администратора RuPost

Настройки -> Пространства хранения -> Backup -> Редактировать хранилище почты -> Идентификатор хранилища



- Командой `rupost mailstore list`

```
│  ID пространства хранения:        87d6d7f8-27ea-45b0-9ac6-ea41c2c29a4f  │
│  Название пространства хранения:  Пространство хранения по умолчанию   │
│  ID:                              1c2081df-31cf-462a-ad57-9fbe0424c902  │<--
-
│  Название:                        Backup                                │
│  Тип:                             backup                                │
│  Дата проверки:                   2024-12-16 13:18:10.663260+03:00      │
│  Статус:                          active                                │
│  Синхронизировано:                Да                                    │
│  Почтовые ящики:                  nfs://192.168.186.41/tst/msp01/bkp    │
```

```
|   Пользовательские архивы:          nfs://                                  |
|   RecordStorage:                    nfs://                                  |
```

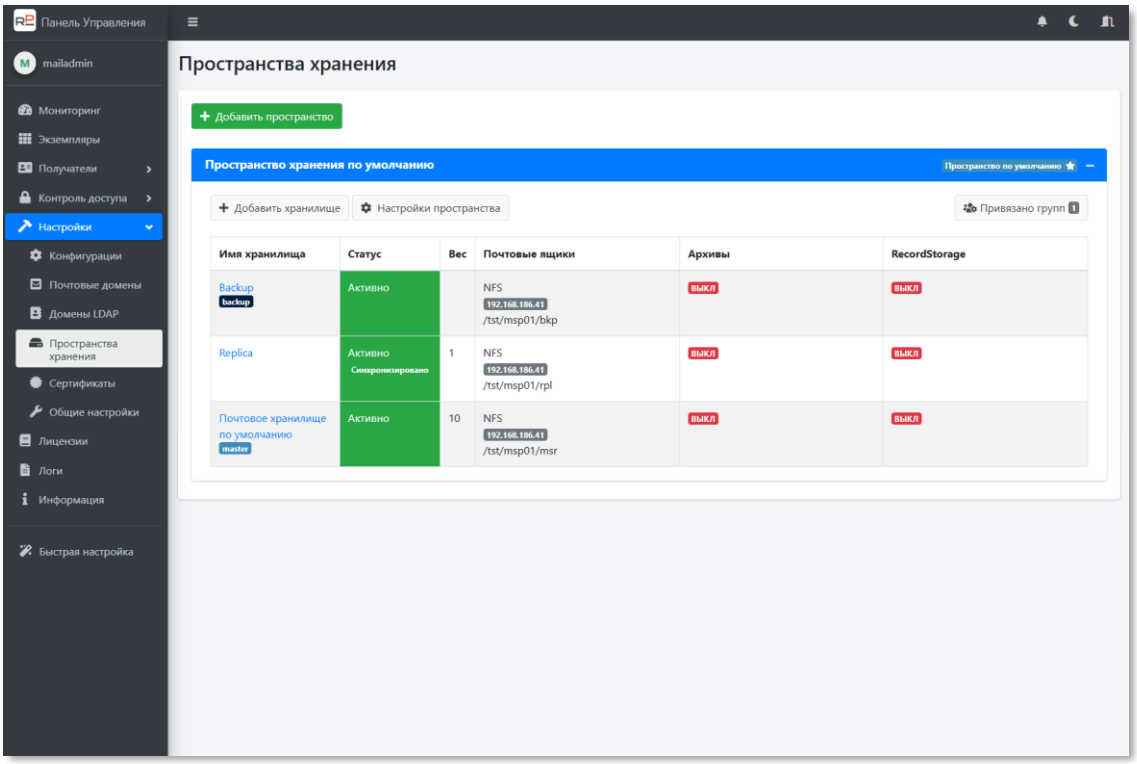
Система RuPost предоставляет два варианта создания «холодной реплики»:

1. Согласно правилам, заданным в графическом интерфейсе администратора RuPost.
2. По требованию, в любое время.

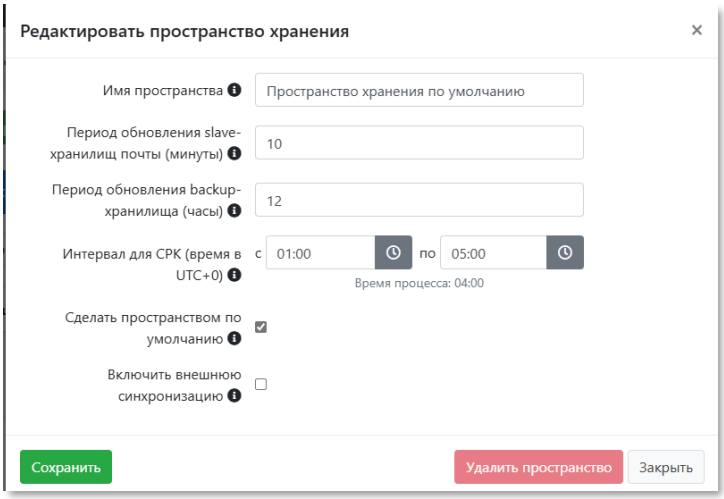
Процесс создания «холодной реплики» по расписанию в начале создает каталог `.ReadyBackup`, в который производит копирование данных из «горячей реплики», после завершения копирования каталог переименовывается в `Backup`. С этого момента каталог может быть использован для создания РК.

Правила создания «холодной реплики» определяются в графическом интерфейсе администратора RuPost.

Настройки -> Пространства хранения -> Настройки пространства



… -> Настройки пространства -> Редактировать пространство хранения



Используемые параметры:

«Период обновления backup-хранилища (часы)» задает период времени в часах между выполнением копирования данных из «горячей реплики» в «холодную реплику» (каталог **Backup)**.

«Интервал для СРК (время в UTC +0)» определяет временной интервал в часах для создания СРК копии «холодной реплики», по истечении которого система RuPost выполняет копирование данных из «горячей реплики» в «холодную реплику» (каталог **Backup)**.

Внимание!

Выполнение восстановления СРК данных из РК в «холодную реплику» системы RuPost возможно в любое время, поскольку данные из СРК помещаются в отдельный каталог **Restore** (создается СРК).

Администратор системы RuPost может выполнить создание «холодной реплики» в любое время используя команду:

`rupost backup cold-backup –id` <Идентификатор почтового хранилища типа backup>

В данном случае будет создана копия данных почтовых ящиков и календарей всех пользователей.

Выше рассмотрено как получить «Идентификатор почтового хранилища типа backup», который является ID «холодной реплики».

Пример:

```
root@al181uu1lvm0g31:~# rupost backup cold-backup --id 1c2081df-31cf-462a-ad57-9fbe0424c902
```

Внимание!

При выполнении создания «холодной реплики» по требованию происходит проверка на наличие работающего процесса автоматизированного создания «холодной реплики по расписанию». В случае наличия автоматизированного процесса приоритет остается за ним и выдается сообщение об ошибке:

[56632] «Холодная репликация уже выполняется. Хранилище: Backup.»

Выполнить ручное создание «холодной реплики» возможно после завершения процесса создания этой реплики по расписанию.

В случае необходимости присутствует возможность создания копии в «холодной реплике» для группы пользователей (ключ --mailbox-group) или отдельного почтового ящика (ключ --mailbox-address).

3.2.2. Восстановление из «холодной реплики»

Обязательным условием корректной работы функциональности восстановления системы RuPost является наличие каталога Restore с необходимыми данными (РК каталога Backup). Система RuPost обеспечивает широкий набор возможностей восстановления данных пользователя и гибкие варианты настройки, начиная от восстановления всех данных почтовых ящиков до восстановления отдельного почтового ящика, сообщений или календаря.

Внимание!

В случае восстановления данных **удаленного пользователя** во **вновь созданный ящик** или при **полном отсутствии во всех папках существующего ящика каких-либо сообщений,** сообщения из РК помещаются **в те же папки и с тем же статусом** (просмотрено/не просмотрено) в каких они были **на момент создания РК**.

Если восстановление происходит **в существующий почтовый ящик** и в почтовом ящике **присутствуют сообщения**, то для исключения ситуации с дублированием или замещением, восстановление сообщений производится **в отдельно созданную** папку **Restore**, с сохранением той же структуры размещения по папкам и статуса (просмотрено/не просмотрено), в котором они были на момент создания РК.

Пользователю предоставляется возможность самостоятельно переместить необходимые сообщения из папки Restore в нужную папку, а затем удалить папку Restore.

Внимание!

После завершения работы утилиты восстановления `rupost backup cold-restore` данные в каталоге Restore удаляются.

Восстановленную в каталог Restore РК можно проверить на наличие в ней данных выбранного пользователя. В примере рассмотрены варианты проверки наличия данных пользователей, в основном почтовом адресе которых есть «user». Для проверки используется информация из файла `srk_index`, рассмотренного выше, в разделе 3.

```
grep --include=\srk_index \
-rT '/home/rupost/1c2081df-31cf-462a-ad57-9fbe0424c902/mailboxes/Restore/' \
-e 'user' | sort -k2,2
```

```
root@al18luu1lvm0g31:~# grep --include=\srk_index \
> -rT '/home/rupost/1c2081df-31cf-462a-ad57-9fbe0424c902/mailboxes/Restore/' \
> -e 'user' | sort -k2,2
/home/rupost/1c2081df-31cf-462a-ad57-9fbe0424c902/mailboxes/Restore/7023e47d-627a-4bd0-93bf-c8b7fd38f470/srk_index:     user10@example.internal
/home/rupost/1c2081df-31cf-462a-ad57-9fbe0424c902/mailboxes/Restore/b2bd0739-5e5a-4057-9dcd-47f81c13f0f3/srk_index:     user11@example.internal
/home/rupost/1c2081df-31cf-462a-ad57-9fbe0424c902/mailboxes/Restore/3c55a03e-89d7-4cd5-855c-ea7a9ec8aaed/srk_index:     user12@example.internal
/home/rupost/1c2081df-31cf-462a-ad57-9fbe0424c902/mailboxes/Restore/66f13249-9200-4103-8196-60743c58d7fa/srk_index:     user13@example.internal
/home/rupost/1c2081df-31cf-462a-ad57-9fbe0424c902/mailboxes/Restore/178c5b8c-c94f-42e0-ae87-237bd8bdca24/srk_index:     user14@example.internal
/home/rupost/1c2081df-31cf-462a-ad57-9fbe0424c902/mailboxes/Restore/7d1bc28e-0ff6-4675-bf83-4ce096c1fde1/srk_index:     user15@example.internal
/home/rupost/1c2081df-31cf-462a-ad57-9fbe0424c902/mailboxes/Restore/5f83e61a-0945-448f-b890-4e200daf7dcb/srk_index:     user16@example.internal
/home/rupost/1c2081df-31cf-462a-ad57-9fbe0424c902/mailboxes/Restore/d6b193d4-799b-43f1-a6b8-e2be04430718/srk_index:     user17@example.internal
/home/rupost/1c2081df-31cf-462a-ad57-9fbe0424c902/mailboxes/Restore/24449735-5bae-45bc-a628-d435c6c0d205/srk_index:     user18@example.internal
/home/rupost/1c2081df-31cf-462a-ad57-9fbe0424c902/mailboxes/Restore/5928bebd-4361-4390-b34c-b673ed6888e1/srk_index:     user19@example.internal
```

Рассмотрим несколько примеров восстановления.

Примеры

- **Полное восстановление данных пользователей**

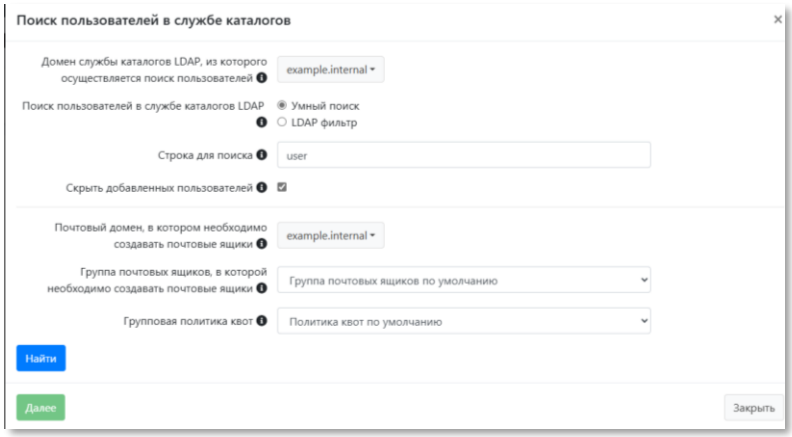
Используется для восстановления всей информации пользователей (сообщения, календари), при потере всех данных и каталога MailDir. В этом случае почтовые ящики пользователей создаются заново.

Предварительные действия

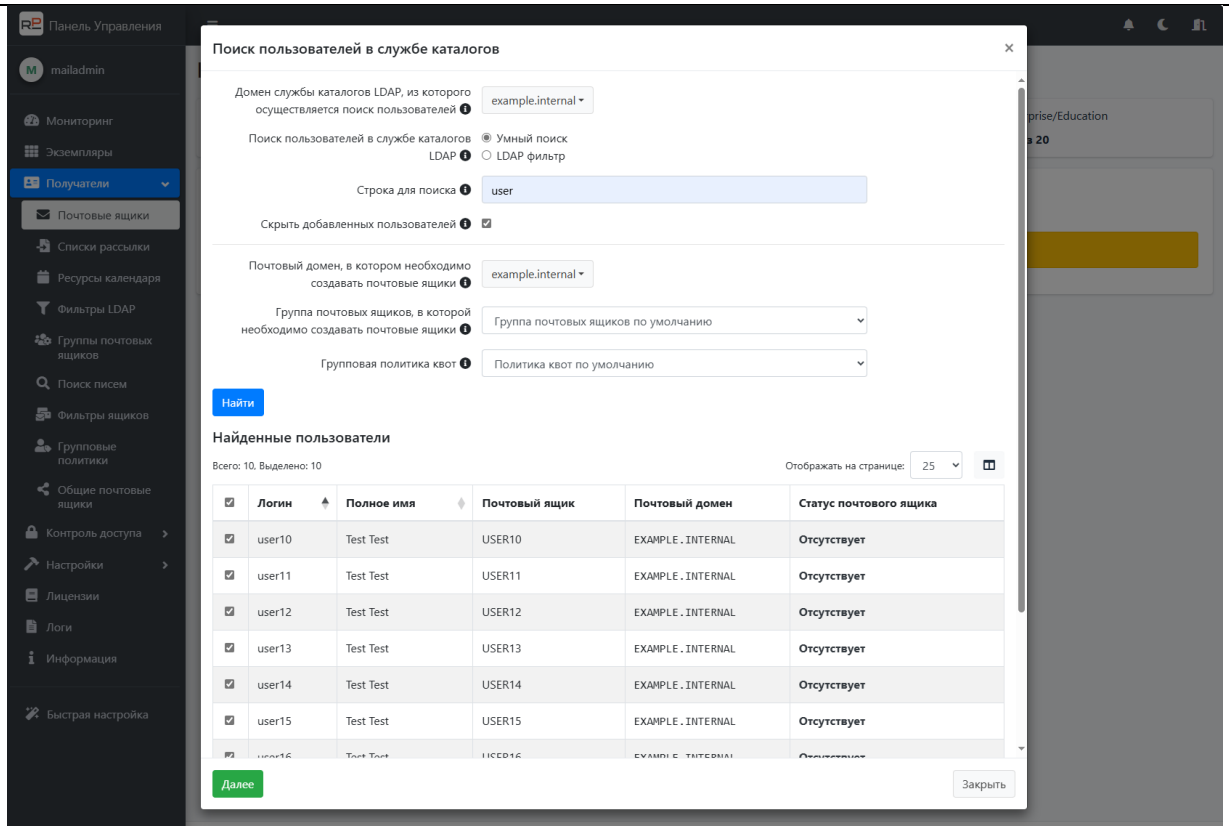
Восстановить в каталог Restore «холодной реплики» необходимую РК.

В графическом интерфейсе администратора RuPost загрузим данные пользователей из каталога LDAP создадим новые почтовые ящики.

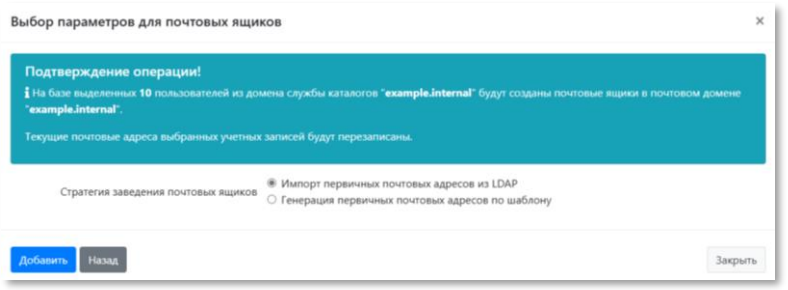
Получатели -> Почтовые ящики -> Добавить из LDAP -> Поиск пользователей в службе каталогов



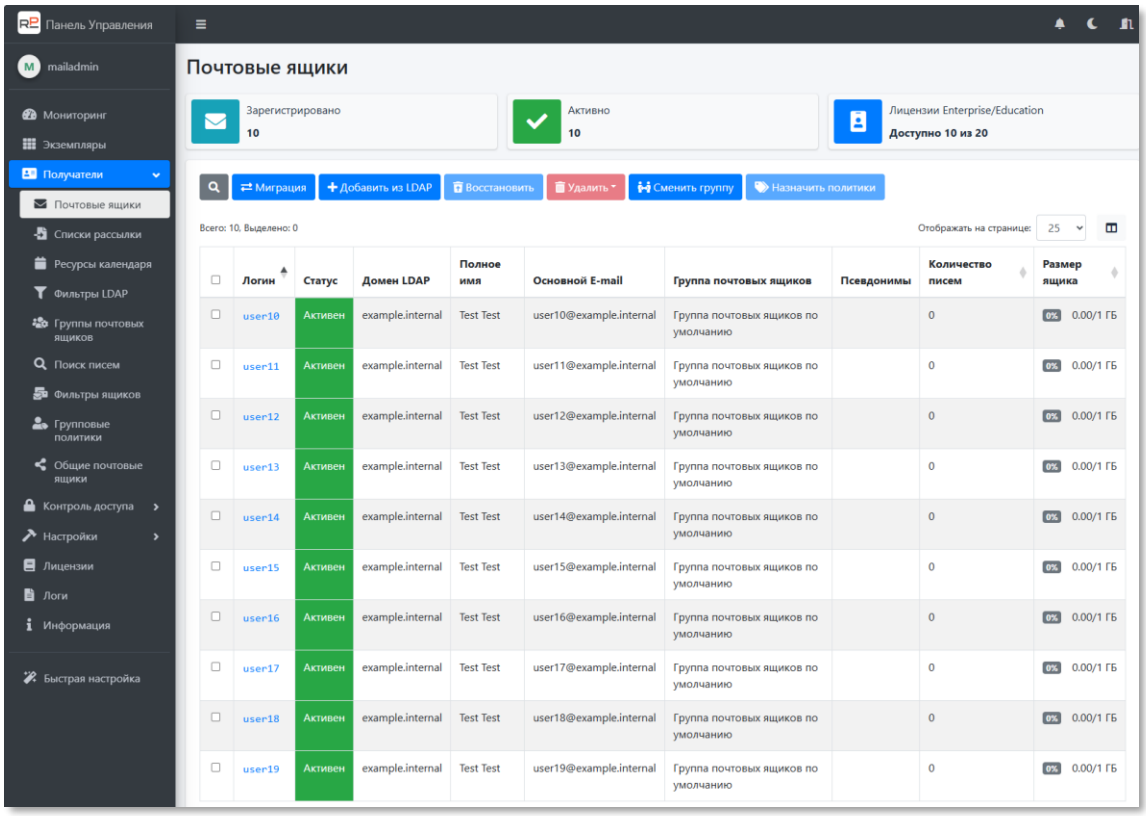
В поле «Строка для поиска» вводим шаблон для поиска «user» и нажимаем «Найти»



Выбираем пользователей и нажимаем «Далее»



Почтовые ящики пользователей созданы



В командной строке администратора системы RuPost выполняем следующую команду

Внимание!

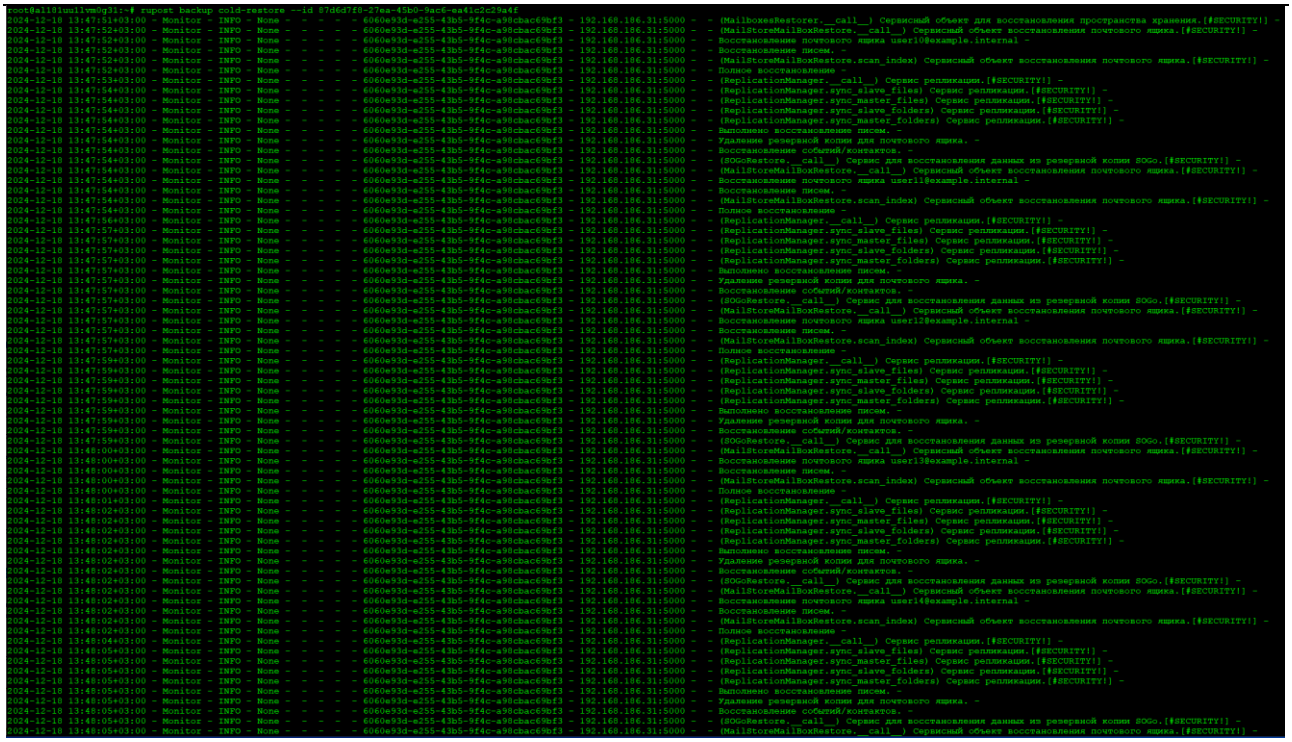
В случае полного восстановления используется ID Пространства хранения по умолчанию

Получение ID Пространства хранения по умолчанию

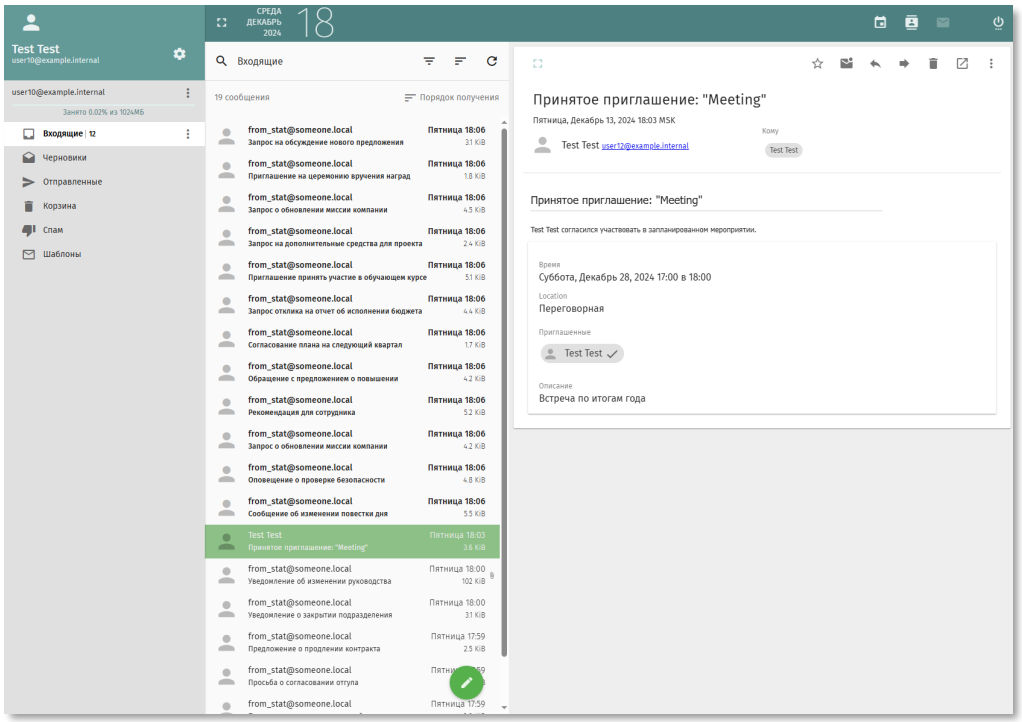
```
rupost mailspace list
```

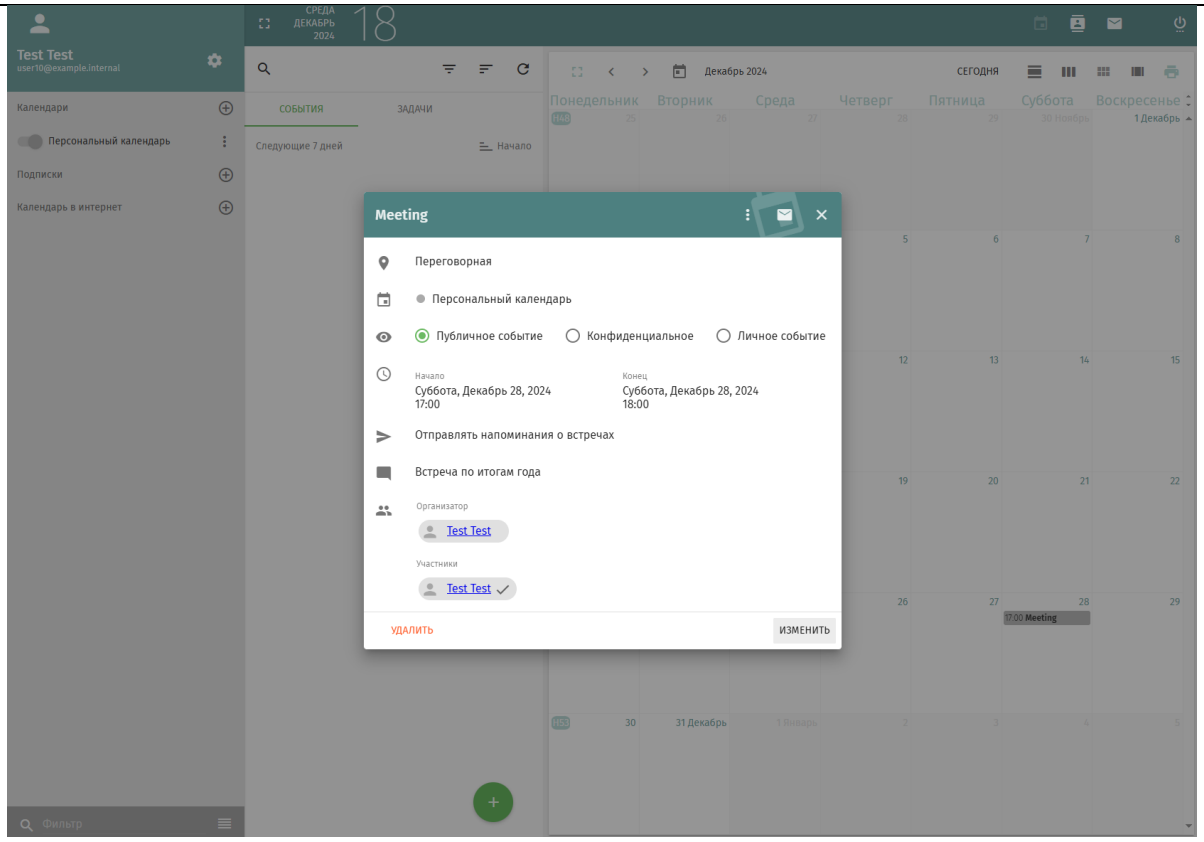
```
root@a1181uu1lvm0g31:~# rupost mailspace list
  ID:                                  87d6d7f8-27ea-45b0-9ac6-ea41c2c29a4f
  Название:                            Пространство хранения по умолчанию
  По умолчанию:                        Да
  Количество групп почтовых ящиков:    1 шт
  Количество почтовых хранилищ:        3 шт
  Период обновления реплики:           10 мин
  Период обновления backup:            12 ч
  Начало работы СРК:                   01:00
  Конец работы СРК:                    05:00
  Автопереключение на реплику:         Нет
  Внешняя синхронизация:               Нет
```

```
rupost backup cold-restore --id 87d6d7f8-27ea-45b0-9ac6-ea41c2c29a4f
```



В WEB интерфейсе клиента и подключаемся к почтовым ящикам





- **Восстановление почтового ящика пользователя после удаления**

Используется для восстановления всей информации выбранного пользователя (сообщения, календари). В этом случае почтовый ящик пользователя создается заново.

Исходные данные

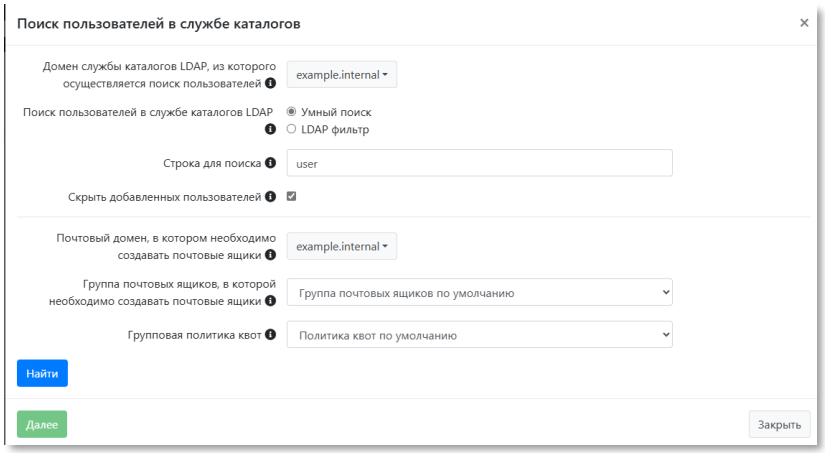
Почтовый ящик пользователя user10@example.internal был удален, но в восстановленной РК этот ящик есть. Необходимо создать почтовый ящик заново и восстановить в него данные из РК.

Предварительные действия

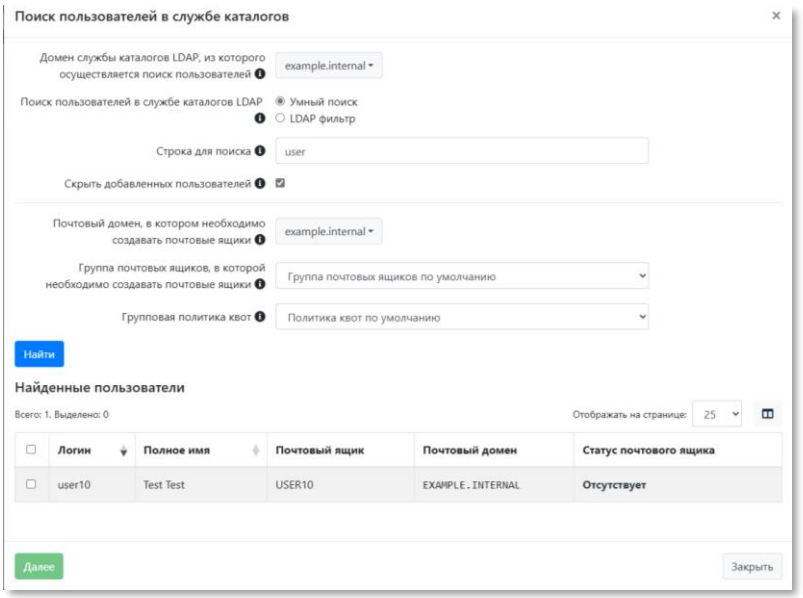
Восстановить в каталог Restore «холодной реплики» необходимую РК.

В графическом интерфейсе администратора RuPost загрузим данные пользователя user10@example.internal из каталога LDAP создадим новый почтовый ящик.

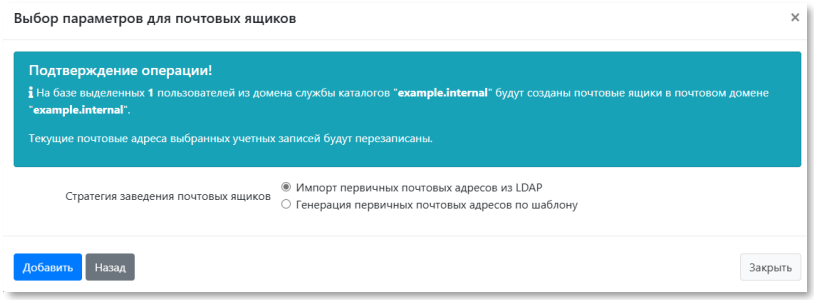
Получатели -> Почтовые ящики -> Добавить из LDAP -> Поиск пользователей в службе каталогов



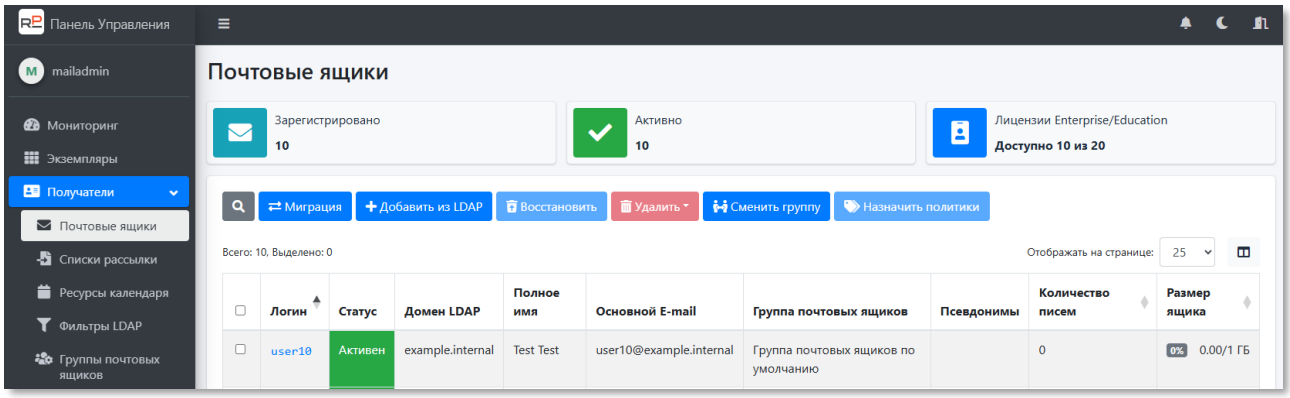
В поле «Строка для поиска» вводим шаблон для поиска «user» и нажимаем «Найти»



Ставим галочку рядом с искомым пользователем и нажимаем «Далее»

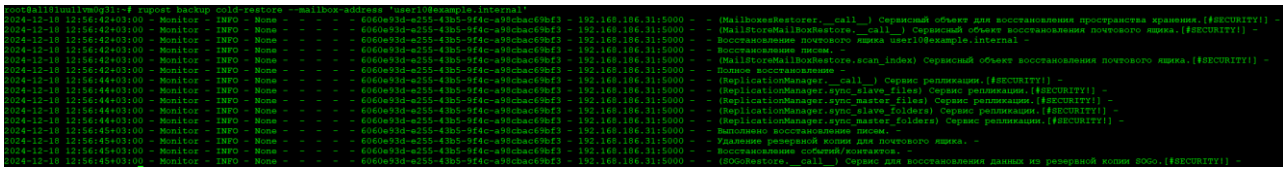


Выбираем «Добавить» и создаем почтовый ящик пользователя user10@example.internal

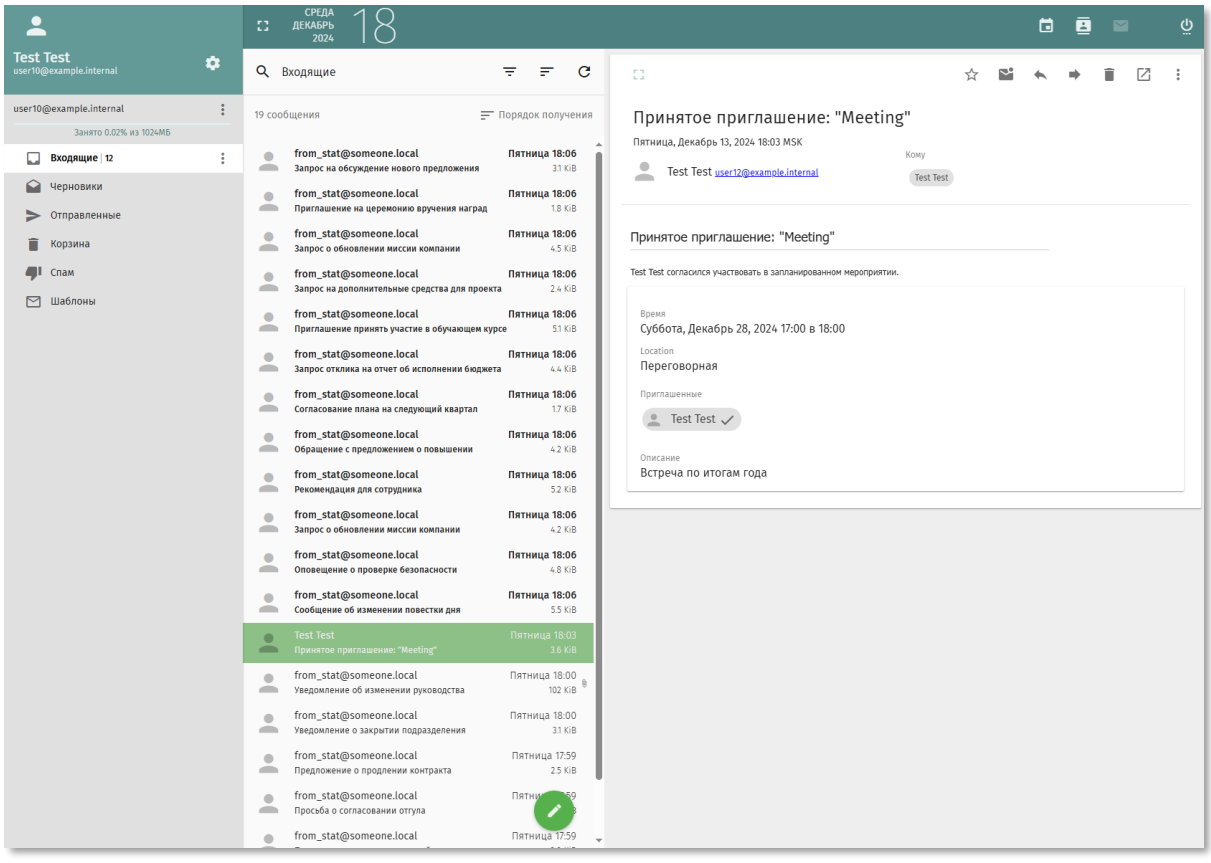


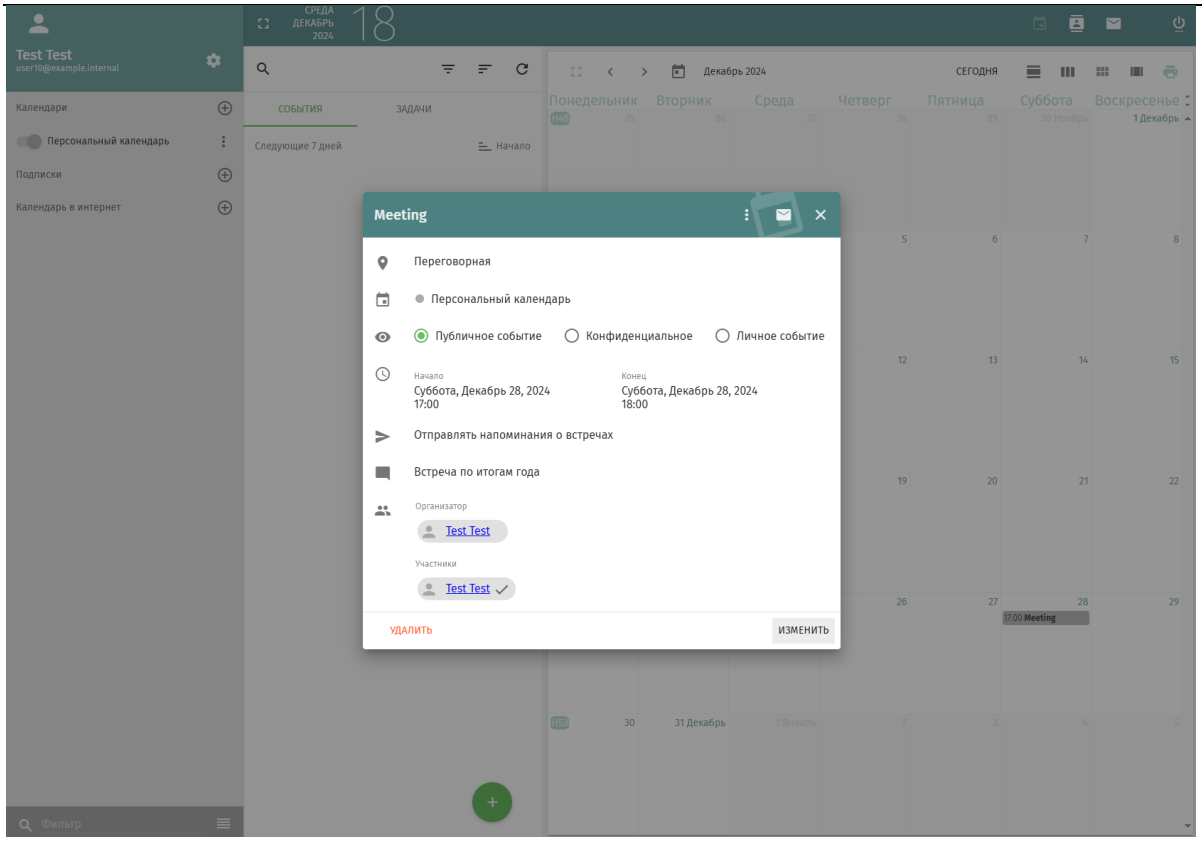
В командной строке администратора системы RuPost выполняем следующую команду

```
rupost backup cold-restore --mailbox-address 'user10@example.internal'
```



В WEB интерфейсе клиента и подключаемся к почтовому ящику `user10@example.internal`





Сообщения пользователя и события календаря восстановлены.

- **Восстановление в существующий почтовый ящик пользователя**

Используется для восстановления запрошенной пользователем информации (сообщения, календари). В этом случае восстановление происходит в отдельный каталог Restore почтового ящика пользователя. Пользователь самостоятельно находит в каталоге Restore искомое сообщение и перемещает его в нужный каталог (на пример «входящие»). После завершения поиска пользователь может самостоятельно удалить каталог Restore.

Исходные данные

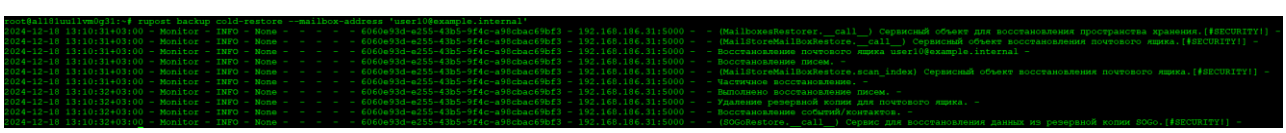
Пользователь `user10@example.internal` удалил одно или несколько важных сообщений и просит восстановить полную копию его почтового ящика.

Предварительные действия

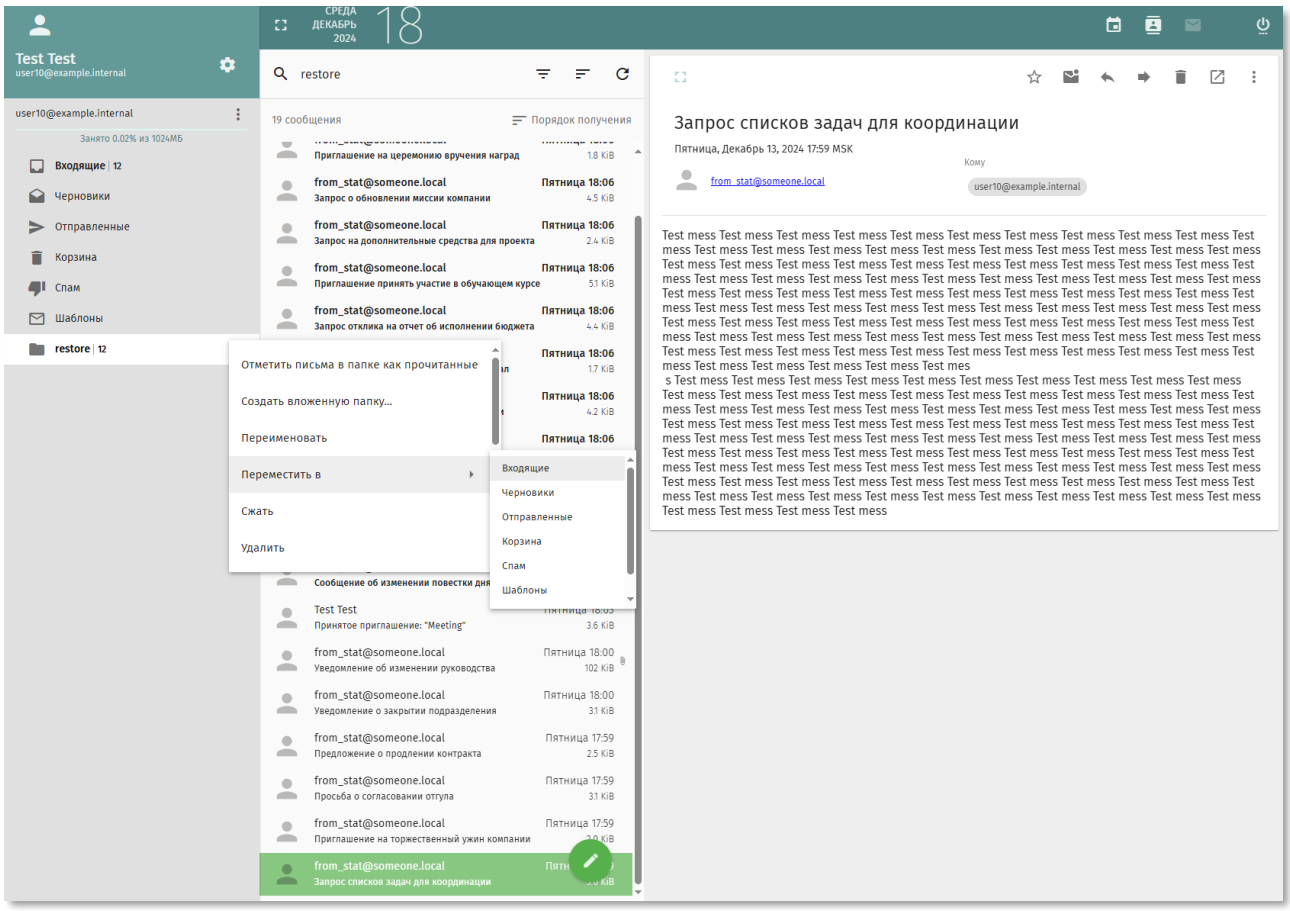
Восстановить в каталог Restore «холодной реплики» необходимую РК.

В командной строке администратора системы RuPost выполняем следующую команду

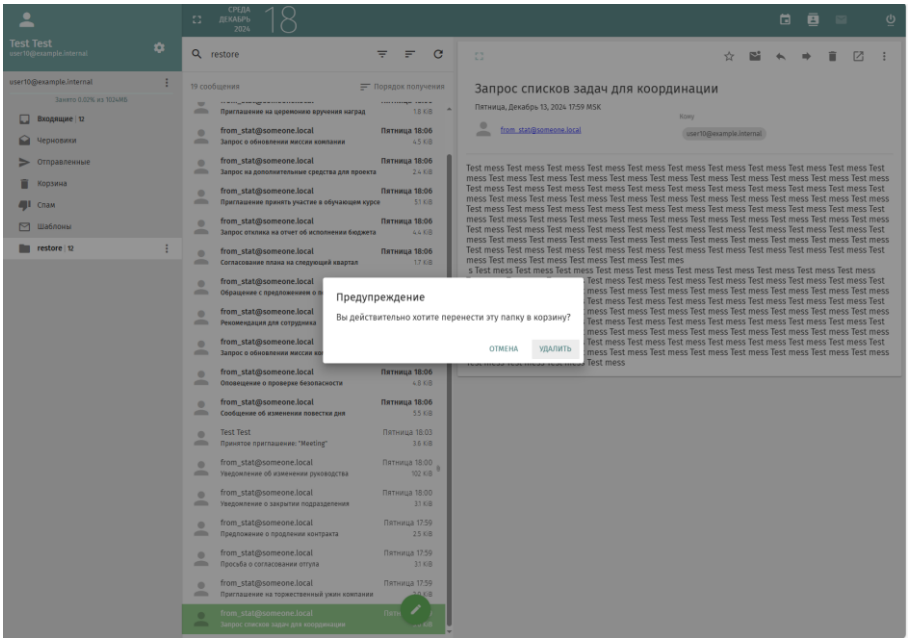
```
rupost backup cold-restore --mailbox-address 'user10@example.internal'
```



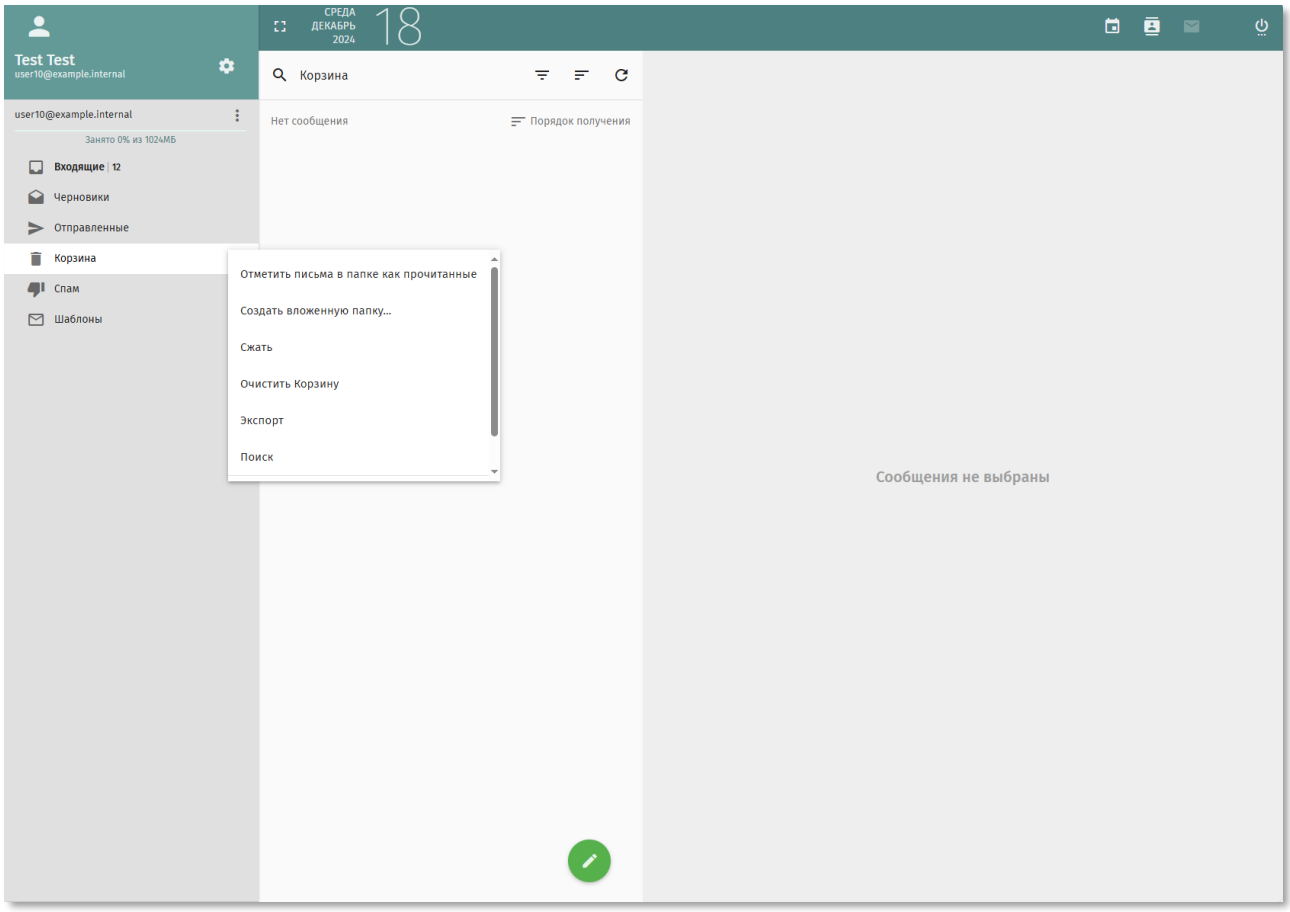
В WEB интерфейсе клиента и подключаемся к почтовому ящику `user10@example.internal`



Сообщения были восстановлены в каталог Restore, далее пользователь может самостоятельно найти нужные сообщения и переместить их. Каталог Restore пользователь должен удалить после завершения работы по поиску и перемещению сообщений.



После удаления папки restore необходимо очистить корзину



- **Восстановление удаленного календаря пользователя**

Используется для восстановления только событий календаря пользователя.

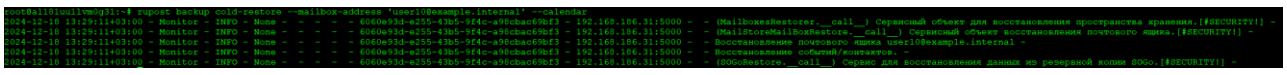
Исходные данные

Пользователь user10@example.internal удалил календарь и просит восстановить его.

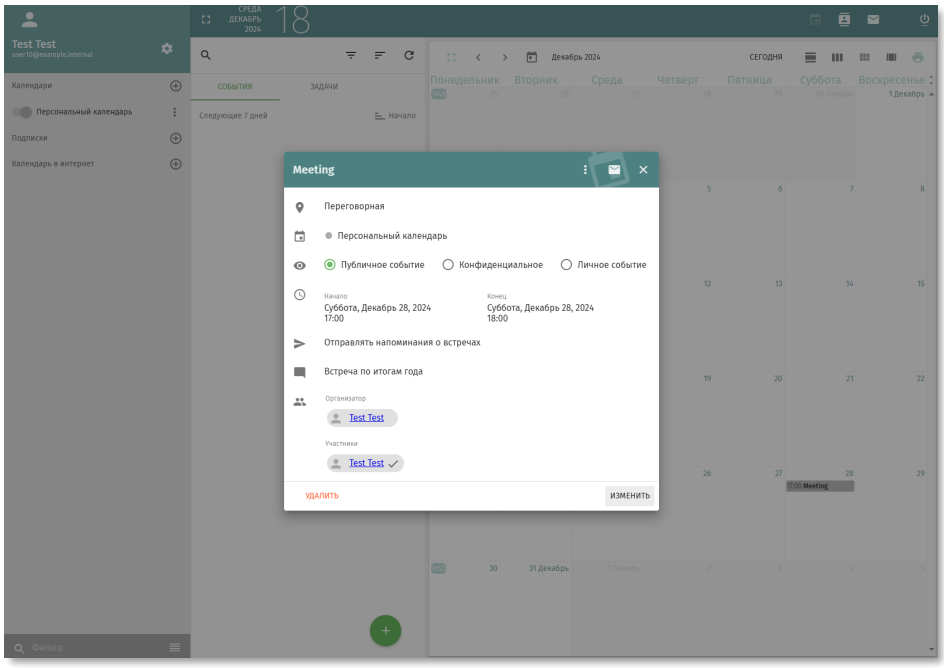
Предварительные действия

Восстановить в каталог Restore «холодной реплики» необходимую РК.

В командной строке администратора системы RuPost выполняем следующую командуrupost backup cold-restore --mailbox-address 'user10@example.internal' --calendar



В WEB интерфейсе клиента и подключаемся к почтовому ящику user10@example.internal



Календарь пользователя `user10@example.internal` восстановлен.

4. Структуры хранения данных

4.1. Почтовые ящики

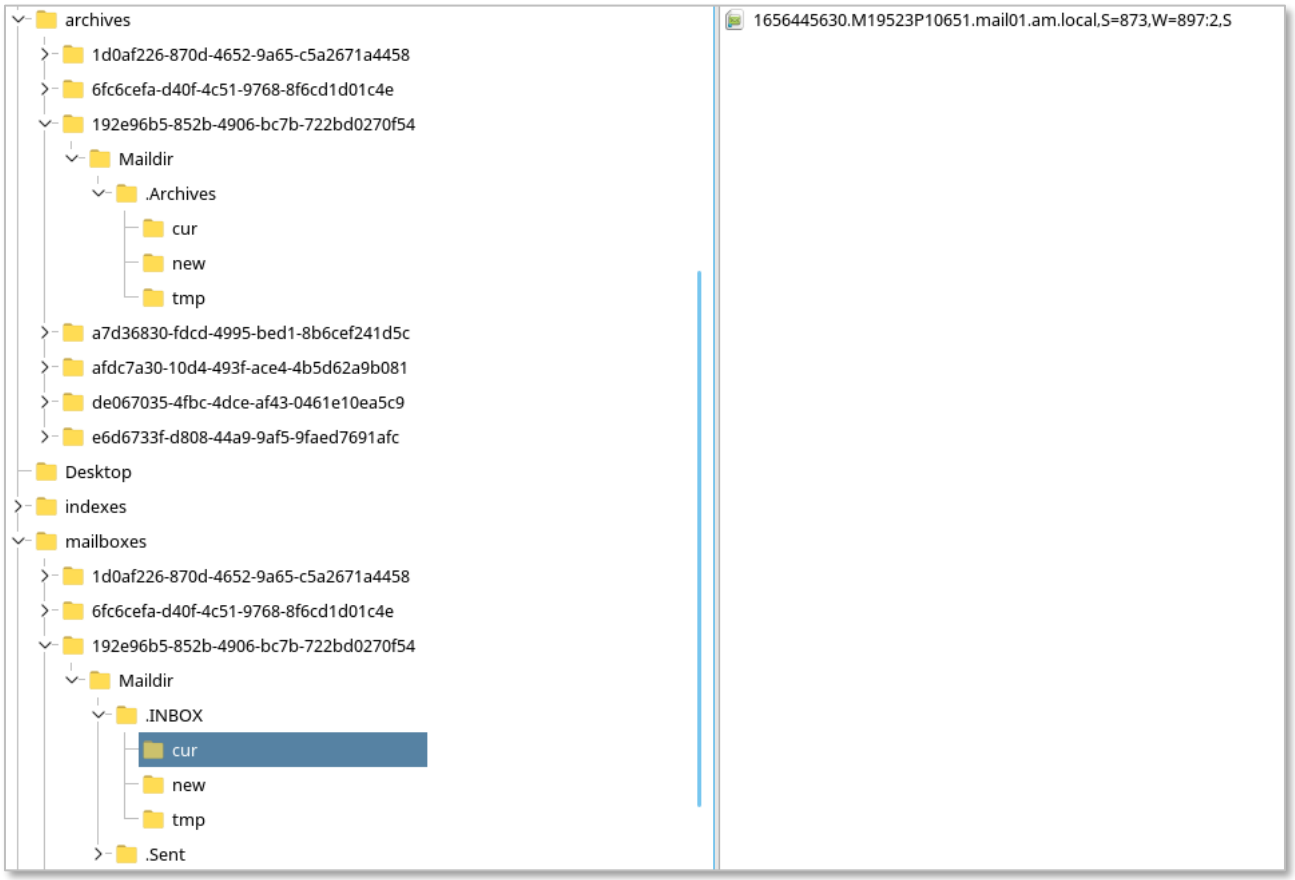
Почтовые ящики – сообщения и файловые вложения - хранятся в заданной файловой системе (см. Общие настройки системы) в формате MailDir.

Папки верхнего уровня:

- `archives` – почтовые архивы, доступные пользователям в клиентских приложениях
- `mailboxes` – почтовые ящики
- `records` – хранилище записей, т.е. копии удаленных писем, недоступные пользователям

В случае локального размещения почты на том же узле, где развернут RuPost, все почтовые папки находятся в папке `/home/rupost` пользователя `root`.

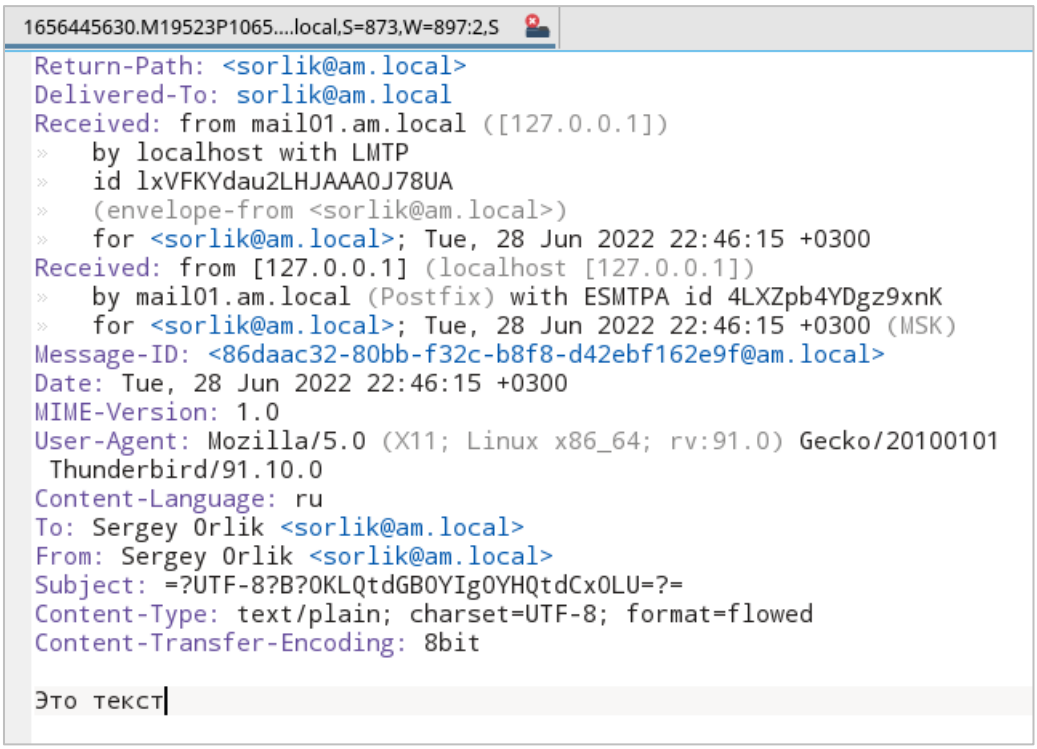
Примечание: archives и records по умолчанию выключены и требуют явного включения в соответствующих параметрах общих настроек.



Внутри папок верхнего уровня находятся вложенные папки, чьи имена соответствуют идентификаторам почтовых ящиков пользователя - UUID ящика (отображаются в информации о почтовом ящике; не путайте с LDAP UUID, которые являются идентификаторами пользователей в службе каталогов). Каждая из папок почтового ящика содержит подпапку MailDir, которая в свою

очередь уже содержит как таковые почтовые папки (с атрибутом hidden) – INBOX, Sent и др, представленные в расширенном формате хранения MailDir (см. https://ru.wikipedia.org/wiki/Maildir и https://doc.dovecot.org/admin_manual/mailbox_formats/maildir/) .

Сами сообщения представлены в виде отдельных текстовых файлов (см. RFC 822 (https://datatracker.ietf.org/doc/html/rfc822).

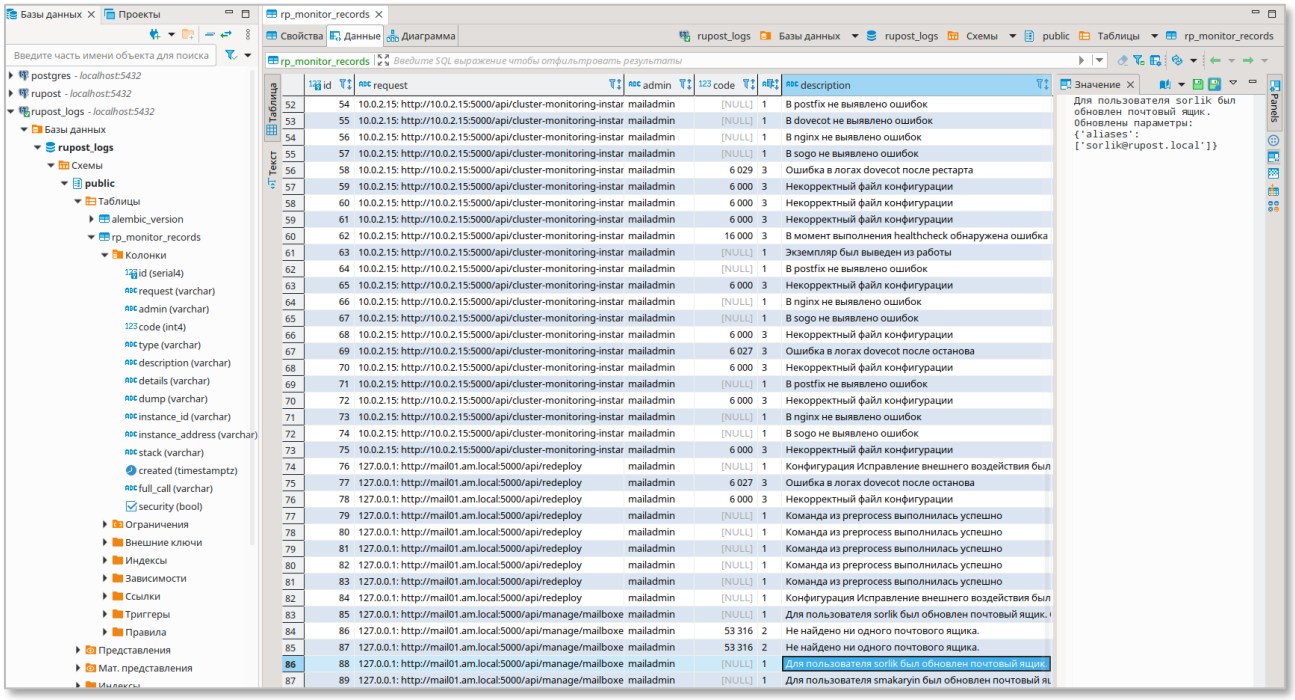


4.2. Базы данных RuPost

Программа установки RuPost автоматически создает базы данных PostgreSQL, общие для всех узлов RuPost:

- `rupost` – конфигурационные данные системы и корпоративная адресная книга
- `rupost_data` – пользовательские данные (календари, контакты, параметры общего доступа, настройки web-клиента и т.п.)
- `rupost_shared` – информация о квотах

Системный журнал RuPost записывается в файл `/var/log/rupost/monitor.log` на каждом из узлов системы.



4.2.1. Смена пароля доступа к базе данных

СУБД является инфраструктурным ресурсом для системы RuPost. В процессе обслуживания СУБД может понадобиться сменить пароль служебной (сервисной) учетной записи (полномочия) для доступа системы RuPost к СУБД, например, на основании политики контролируемого доступа, принятой в организации. Для функционирования системы RuPost необходимо указать новый служебный пароль доступа к базе данных. Информация о подключении к базе данных хранится в локальном файле с настройками на каждом из узлов системы.

Внимание!

Для корректного функционирования системы необходимо соблюдать правильный порядок выполнения соответствующих операций для смены параметров базы данных следующий:

1. Останавливаем почтовые компоненты на всех узлах (через консоль администратора или команду CLI: `rupost componenets stop --all`);
2. Меняем параметры на базе данных на новые;
3. На каждом узле:
   3.1 Останавливаем службу RuPost (выполняем из консоли команду `systemctl stop rupost`);
   3.2 Меняем параметры подключения к базе данных с помощью команды CLI `rupost db`;
   3.3 Запускаем службу RuPost (выполняем из консоли команду `systemctl start rupost`);
4. Переразворачиваем почтовую конфигурацию через консоль администратора.

Для смены пароля доступа к базе данных необходимо на каждом экземпляре RuPost (на всех узлах кластера) выполнить соответствующую команду RuPost CLI.



Синтаксис команды и примеры управления базой данных из командной строки приведены в разделе **«rupost db группа команд для управления базой данных»** Справочного руководство по командной строке.

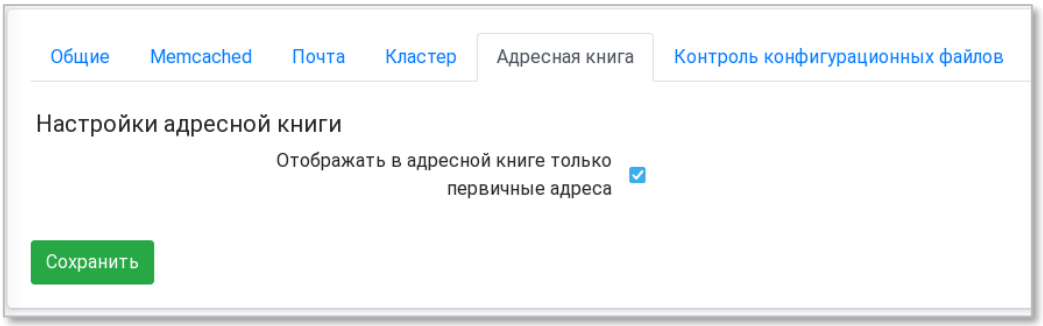
5. Глобальная адресная книга (GAL)

Глобальная адресная книга RuPost GAL (Global Address List) автоматически формируется на основе значимой информации о пользователях, собираемой из подключенных служб каталогов.
Обновление адресной книги происходит:

- Периодически – раз в 6 часов;
- При разворачивании почтовой конфигурации;
- Вручную, с помощью команды CLI.

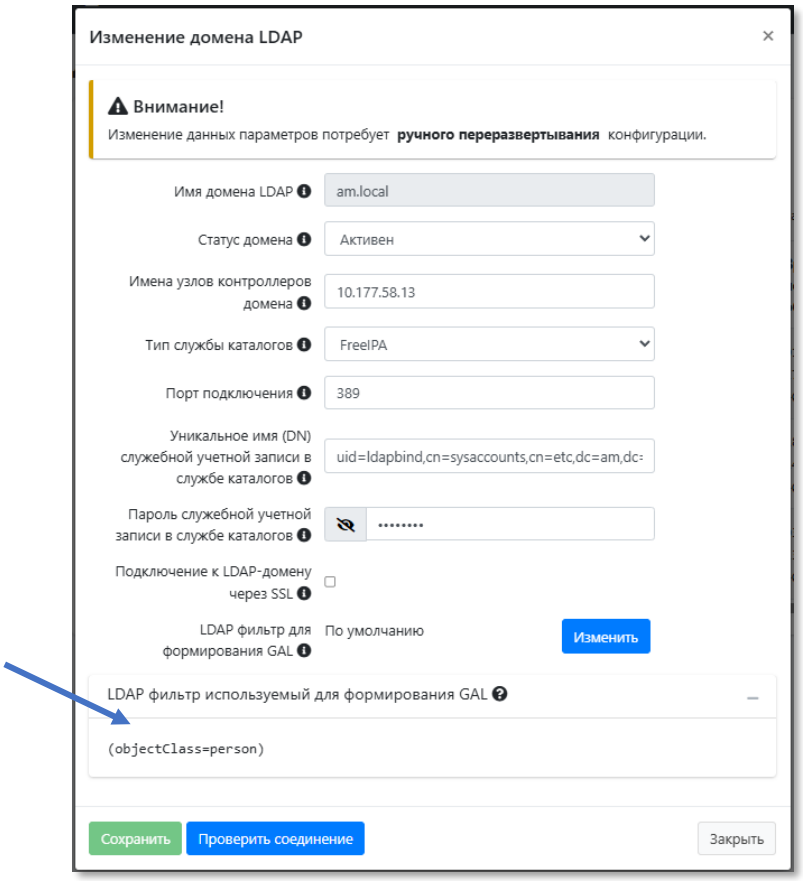
Синтаксис команды и примеры обновление корпоративной адресной книги из командной строки приведены в разделе **«rupost make-gal выполнить обновление корпоративной адресной книги»** Справочного руководство по командной строке.

Для того, чтобы в корпоративную адресную книгу попадали только первичные (основные - primary) адреса электронной почты пользователей в разделе (вкладке) “Адресная книга” страницы “Общие настройки” Панели управления системы необходимо включить настройку “ Отображать в адресной книге только первичные адреса”. При этом псевдонимы (алиасы) почтовых ящиков пользователей собираться в адресную книгу не будут.

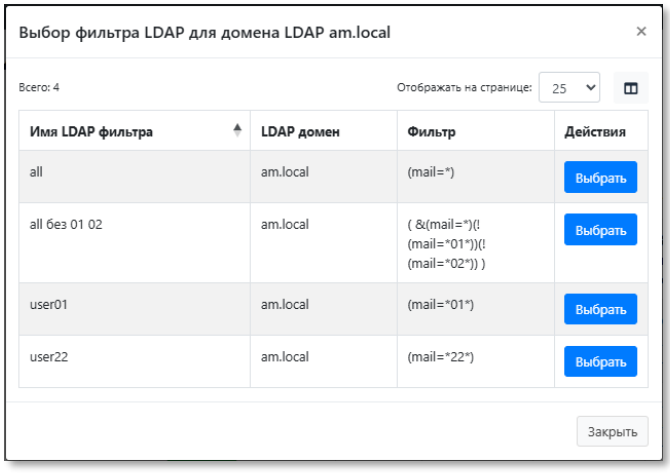


В версии 3.3.0 добавлена возможность для каждого LDAP домена указать LDAP фильтр, который будет использован при формировании адресной книги (GAL).

Если LDAP фильтр не выбран, то отображается текст запроса в LDAP, который используется при формировании адресной книги по умолчанию.



Изменить условие отбора записей LDAP, которые будут добавлены в адресную книгу, можно нажав на кнопку “Изменить”.



В версии 4.3.4 добавлена возможность сбора данных для формирования корпоративной адресной книги с использованием Глобального каталога (Microsoft Active Directory Global Catalog).

При использовании Глобального каталога, данные для корпоративной адресной книги собираются со всех доменов, входящих в “лес” (forest).

Для того, чтобы обрабатывался не одиночный LDAP домен, а Глобальный каталог, необходимо в настройках LDAP подключения указать порт Глобального каталога:

- **3268** – обычное подключение.
- **3269** – SSL/TLS.

При использовании Глобального каталога, не рекомендуется создавать подключения к отдельным доменам, входящим в Глобальный каталог.

Если сконфигурированы одновременно и подключение к отдельному LDAP домену и подключение к Глобальному каталогу, в который входит этот домен, то, при создании корпоративной адресной книги, будут использованы только настройки подключения к Глобальному каталогу – настройки по адресной книге для отдельного домена будут проигнорированы.

5.1. Атрибуты, используемые для формирования глобальной адресной книги (GAL)

В версии 2.5.0 в глобальную адресную книгу добавлена следующая информация:

- Адреса списков рассылки;
- Контакты сервера Microsoft Exchange – при сосуществовании RuPost и Microsoft Exchange;
- Обработка атрибута LDAP DisplayName для получения данных – Фамилия, Имя и Отчество контакта;

5.1.1. FreeIPA

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`	Тип пользователя
`facsimileTelephoneNumber`	Факс
`ou`	Департамент
`pager`	Пейджер
`proxyAddresses`	Электронная почта

5.1.2. 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

5.1.3. Active Directory

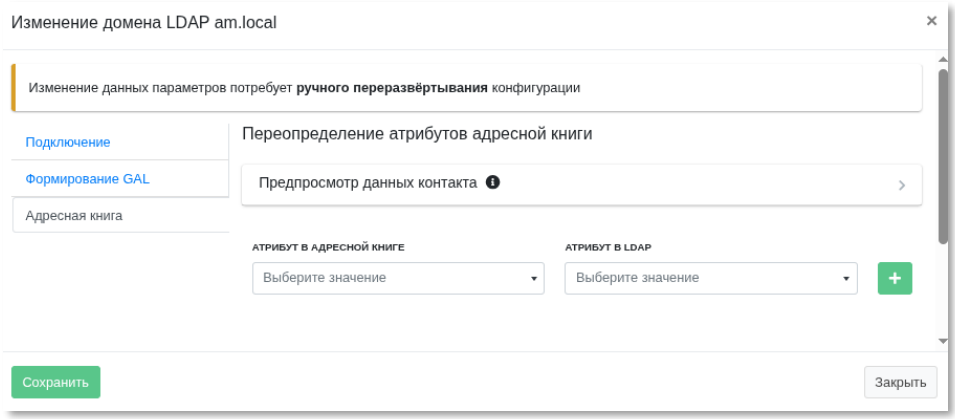
Имя attributeTypes	Функциональное назначение
cn	Полное имя
givenName	Имя
l	Город
mail	Первичный адрес электронной почты
mobile	Мобильный телефон
sn	Фамилия
st	Регион
street	Улица
title	Должность
company	Компания
department	Департамент
facsimileTelephoneNumber	Факс
homePhone	Домашний телефон
pager	Пейджер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

`telephoneNumber`	Рабочий телефон

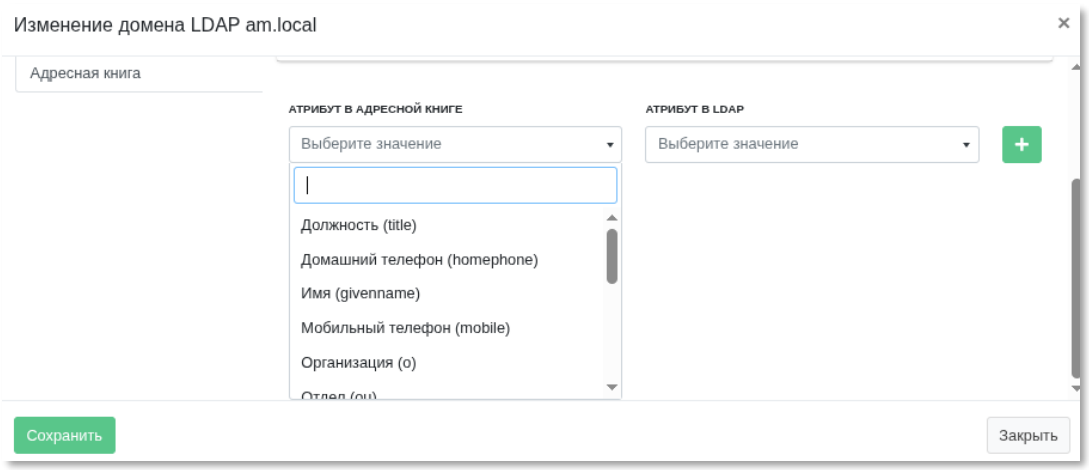
5.1.4. Редактор атрибутов адресной книги

В версии 4.0 добавлена возможность управлять набором атрибутов LDAP, которые будут использованы для формирования адресной книги.

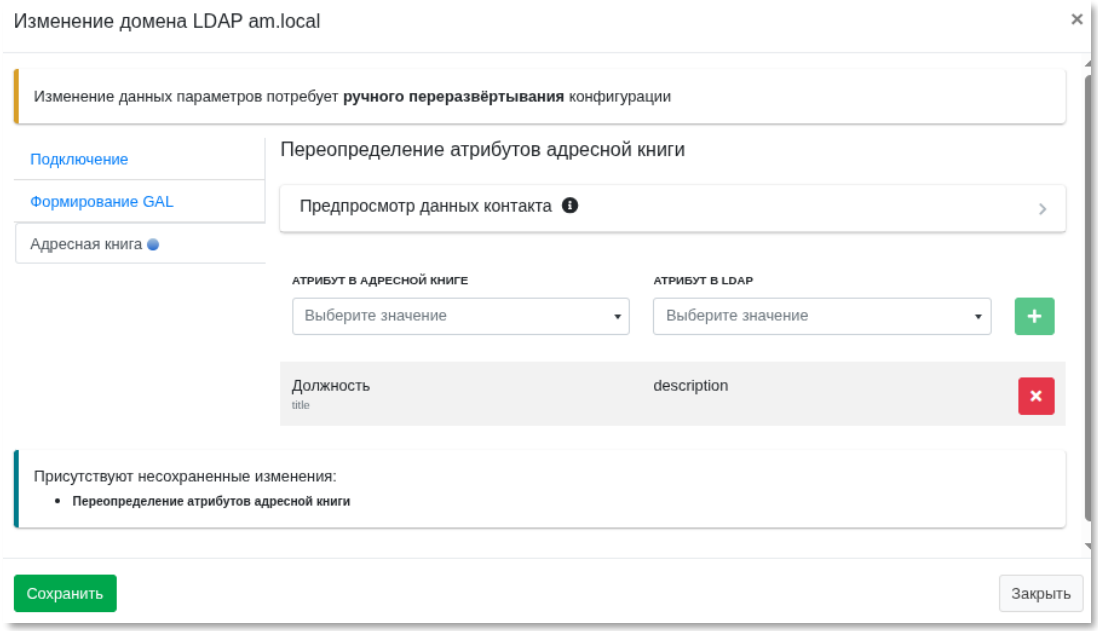
Для того, чтобы для изменить источник данных для отдельного поля адресной книги необходимо из окна свойств LDAP домена открыть редактор атрибутов адресной книги.



В окне редактирования, для каждого поля адресной книги, можно выбрать соответствующий атрибут LDAP из выпадающего списка.



После завершения редактирования атрибутов можно увидеть, какими атрибутами LDAP будут заполнены выбранные поля карточки контакта в адресной книге.



При формировании адресной книги, те поля карточки контакта, которые не переопределены, будут заполнены алгоритмом по умолчанию.

6. Геокластер

Рекомендуется

Перед планированием развертывания Геокластера **необходимо ознакомиться** с документом “RuPost – Предпочтительная архитектура развертывания”.

6.1. Введение

Геокластер RuPost - совокупность территориально разнесенных кластеров RuPost (сайтов), объединенных единой системой управления и взаимодействующих друг с другом без ограничений возможности автономной работы отдельных кластеров.

Геокластер является эволюцией кластера RuPost, сохраняя те же подходы и принципы:

- **Простота** – как в установке, так и в эксплуатации.
- **Масштабируемость** – добавляйте новые сайты по мере необходимости.
- **Управляемость** – все параметры функционирования Геокластера настраиваются централизованно с помощью Панели управления.
- **Надежность** – функционирование системы продолжается даже при выходе из строя части сайтов.
- **Безопасность** – все соединения между сайтами осуществляются по протоколам SSL / TLS.

Сайты Геокластера (кластеры RuPost), размещенные в различных ЦОД, объединены в единую систему четырьмя “слоями” взаимодействия:

- **Единая Панель управления** (см. “Создание Геокластера”).
- **Единые настройки** (см. “Глобальные настройки Геокластера”).
- **Единая маршрутизация почты** (см. “Маршрутизация почты между сайтами”).
- **Единая система мониторинга** (см. “Средства обеспечения надежности Геокластера”).

Система управления Геокластером имеет иерархическую структуру – один сайт является **ведущим.**

Ведущий сайт управляет составом Геокластера, а также задает глобальные параметры функционирования Геокластера.

Права управления Геокластером имеют только суперадминистраторы ведущего сайта Геокластера.

Каждый сайт обслуживает свою группу пользователей / почтовых ящиков – таким образом, у каждого пользователя есть только один “домашний” сайт.

Внимание!

Для корректного функционирования Геокластера, необходимо **средствами инфраструктуры** обеспечить синхронизацию записей о пользователях на серверах LDAP всех сайтов.

6.2. Создание Геокластера

Создание Геокластера заключается в объединении уже развернутых кластеров RuPost в единый Геокластер.

Администратор Геокластера

Администратором Геокластера является администратор ведущего сайта, имеющий права доступа к Панели управления Геокластером.

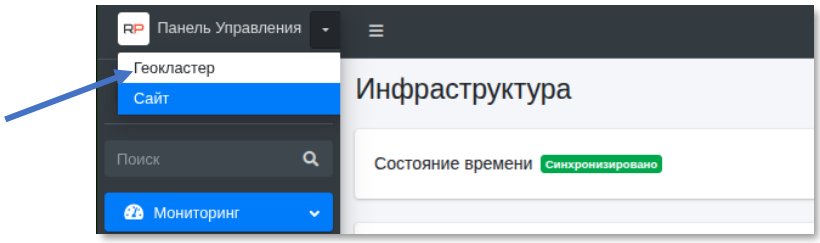
Соответственно, права на создание Геокластера имеет администратор любого кластера RuPost (будущего сайта), имеющий права доступа к Панели управления Геокластером.

Создание Геокластера

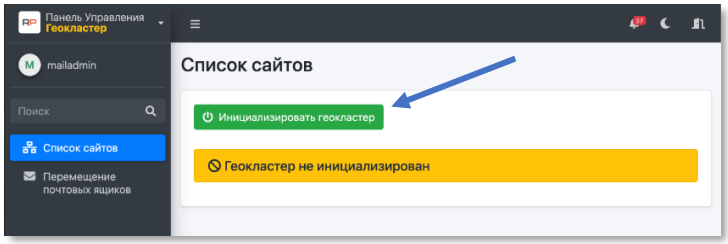
Геокластер создается в момент добавления первого сайта. Сайт, на котором создается Геокластер, будет первым сайтом Геокластера и, соответственно, объявляется ведущим сайтом Геокластера. В дальнейшем, при наличии нескольких сайтов в составе Геокластера, роль ведущего сайта может быть назначена любому сайту.

Каждый сайт в составе Геокластера должен иметь лицензию Enterprise.

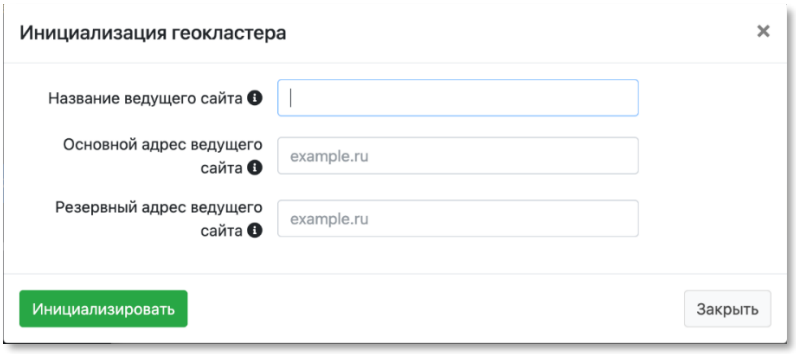
Для создания Геокластера, перейдите в Панель управления Геокластером - для этого необходимо выбрать пункт меню “Геокластер”на верхней панели.



Нажмите кнопку “Инициализировать Геокластер”.



Откроется окно свойств ведущего сайта Геокластера.



Введите следующие параметры будущего сайта:

- **Название ведущего сайта** – обязательный параметр - рекомендуется использовать географическую привязку, например, “Сайт (Москва)”.
- **Основной адрес ведущего сайта** – обязательный параметр – IP адрес (FQDN), который будет использоваться для доступа к Панели управления, SMTP, IMAP подключений и вызовов API Геокластера.
- **Резервный адрес ведущего сайта** – необязательный параметр – IP адрес (FQDN), который будет использоваться для SMTP подключений при отказе в работе основного канала доставки.

Нажмите кнопку “Инициализировать” - после этого в списке сайтов Геокластера появится одна запись.

Создание Геокластера завершено.

Добавление сайтов

Для того, чтобы существующий кластер RuPost был добавлен в Геокластер, должны быть выполнены следующие условия – на удаленном сайте:

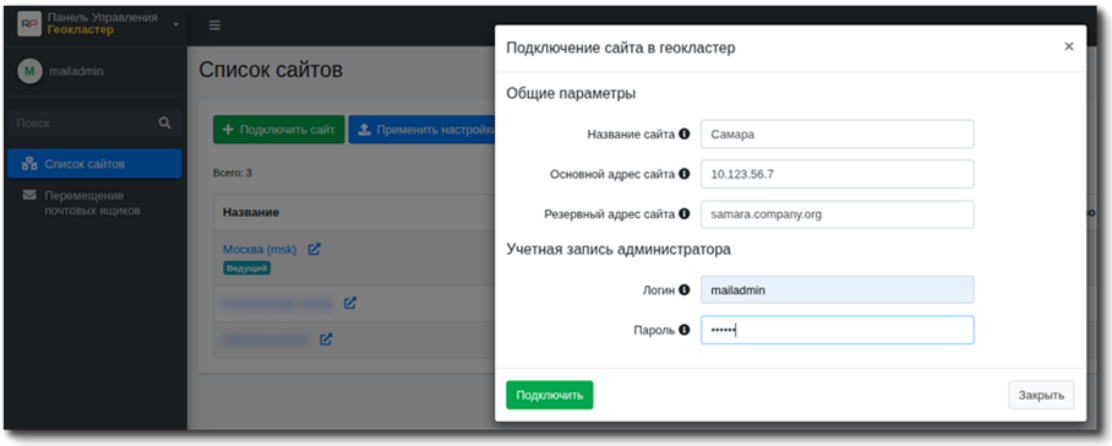
- Активные LDAP домены (FQDN) те же, что и на ведущем сайте.
- Переданные пользователем логин и пароль являются реквизитами суперадминистратора на удаленном сайте (при этом логин и uuid (из LDAP) пользователя должны совпадать с таковыми на ведущем сайте).
- Панель управления доступна по переданному адресу.
- SMTP порт доступен по переданному адресу.
- Сайт не является членом федерации.
- Лицензия – Enterprise.

Для добавления сайта в Геокластер:

1. Войдите в Панель управления ведущего сайта (с правами управления Геокластером).
2. Перейдите в Панель управления Геокластером.
3. Нажмите кнопку “Подключить сайт” – откроется окно свойств сайта.
4. Заполните необходимую информацию о добавляемом сайте:

a. **Название сайта** – обязательный параметр - рекомендуется использовать географическую привязку, например, “Сайт (Казань)”.
b. **Основной адрес сайта** – обязательный параметр – IP адрес (FQDN), который будет использоваться для доступа к Панели управления, SMTP, IMAP подключений и вызовов API Геокластера.
c. **Резервный адрес сайта** – необязательный параметр – IP адрес (FQDN), который будет использоваться для SMTP подключений при отказе в работе основного канала доставки.

5. Введите логин / пароль текущего администратора (ведущего сайта).
6. Нажмите кнопку “Сохранить”.



После этого будут проведены проверки сетевой доступности добавляемого сайта, а также проверки на совместимость параметров добавляемого сайта с Геокластером. Если сайт успешно добавлен в Геокластер, то он появится в списке сайтов Геокластера.

Внимание!

Так как к каждому сайту Геокластера применяются глобальные настройки (см. “Глобальные настройки Геокластера”), то, для начала функционирования сайта в составе Геокластера, необходимо на добавленном сайте переразвернуть существующую конфигурацию.

6.3. Средства обеспечения надежности Геокластера

Система электронной почты является классическим примером системы высокой сложности с соответствующими требованиями обеспечения отказоустойчивости. В силу этого, корпоративная версия RuPost разработана в кластерной архитектуре и все три уровня кластеризации – системы управления, хранения почты и СУБД строятся в кластерном варианте.

Механизмы кластеризации системы хранения и СУБД основываются на многолетней практике обеспечения отказоустойчивости этих инфраструктурных систем.

Инновационная система управления кластером, являющаяся ядром и уникальным преимуществом RuPost, разработана и развивается с применением специальных механизмов мониторинга состояния и защиты от сбоев, которые упрощенно можно назвать средствами самодиагностики (или

healthcheck, как это принято в индустрии). При этом система самодиагностики не только проверяет узлы и компоненты как системы управления кластера RuPost, но в определенном объеме и инфраструктурные системы хранения почты и базы данных.

При решении задачи обеспечения надежности для подобных систем, обязательным является наличие встроенной подсистемы мониторинга, которая является источником информации для:

- обеспечения автоматической реакции на обнаруженный сбой;
- оперативного принятия решения оператором;
- регистрации событий для последующего анализа и оптимизации работы системы.

Геокластер RuPost имеет четыре “контура” мониторинга, покрывающих все аспекты его работы. В соответствии со структурой Геокластера, обеспечивается мониторинг следующих уровней:

- Геокластер;
- Кластер;
- Инфраструктура кластера;
- Экземпляр RuPost / узел кластера.

Мониторинг Геокластера

Геокластер состоит из нескольких сайтов (кластеров RuPost), расположенных в территориально удаленных друг от друга ЦОД. На этом уровне критичным для функционирования системы являются следующие факторы:

- **Сетевая доступность** сайтов (в соответствии с сетевой архитектурой Геокластера) – проверяется периодическими запросами API с ведущего сайта на все сайты Геокластера.

- **Консолидация информации** о состоянии Геокластера на ведущем сайте – в Панели управления Геокластером по каждому сайту отображается как информация о его сетевой доступности, так и информация о работоспособности экземпляров данного кластера.

Мониторинг кластера

На уровне отдельного сайта (кластера RuPost) критичными являются все параметры, влияющие на доставку и обработку электронной почты. Мониторинг на этом уровне осуществляется периодической проверкой доступности следующих портов почтовых компонентов для всех экземпляров кластера:

- **LMTP / SMTP**
- **IMAP / IMAPS**
- **POP3 / POP3S**
- **HTTP / HTTPS**

Автоматически – при обнаружении сбоя, доступ к сбойному экземпляру полностью блокируется на уровне балансировщика и все сетевые запросы перенаправляются на работающие экземпляры. Информация о наличии сбоя, также, передается системе управления подключениями IMAP клиентов

и клиенты IMAP, подключенные в данный момент к сбойному экземпляру, перераспределяются на другие экземпляры обратно пропорционально количеству уже обрабатываемых ими IMAP подключений.

Мониторинг инфраструктуры

Корректность работы системы электронной почты в большой степени зависит от качества настройки и работы инфраструктуры.

Критичными параметрами на данном уровне являются:

- **DNS** – наличие и корректность записей;
- **LDAP** – сетевая доступность серверов LDAP и необходимые права доступа для сервисной учетной записи;
- **СУБД** – сетевая доступность, возможность выполнения запросов от системного пользователя и, в случае использования кластера Patroni, статус узлов и состояние синхронизации кластера баз данных;
- **NFS** – сетевая доступность и наличие прав доступа на сервере NFS;
- **Memcached** – сетевая доступность.

Все вышеперечисленные параметры периодически контролируются, информация о результатах проверок отображается в Панели управления кластером RuPost.

Мониторинг экземпляра

Работа отдельного экземпляра (сервера) RuPost в составе кластера зависит от работы всех почтовых компонентов:

- **Балансировщик** (HAProxy)
- **Web** (Nginx)
- **MTA** (Postfix)
- **MDA** (Dovecot)
- **MUA** (SOGo)
- **Кеш запросов** к базам данных (PGPool)

Периодически проверяется статус каждого компонента и наличие критических ошибок в логах.

Автоматически - при обнаружении сбоя, делаются 3 попытки перезапуска сбойного компонента и, в случае неудачи, экземпляр выводится из эксплуатации и запускается процедура эвакуации почтовых очередей данного экземпляра на корректно работающий экземпляр. Таким образом, минимизируются ошибки обработки почты, вызванные сбоем на конкретном экземпляре RuPost в составе кластера.

Так же, периодически проверяется статус точки монтирования NFS почтовых очередей MTA.

Автоматически – при обнаружении сбоя, происходит переключение на резервную точку монтирования почтовых очередей.

6.4. Глобальные настройки Геокластера

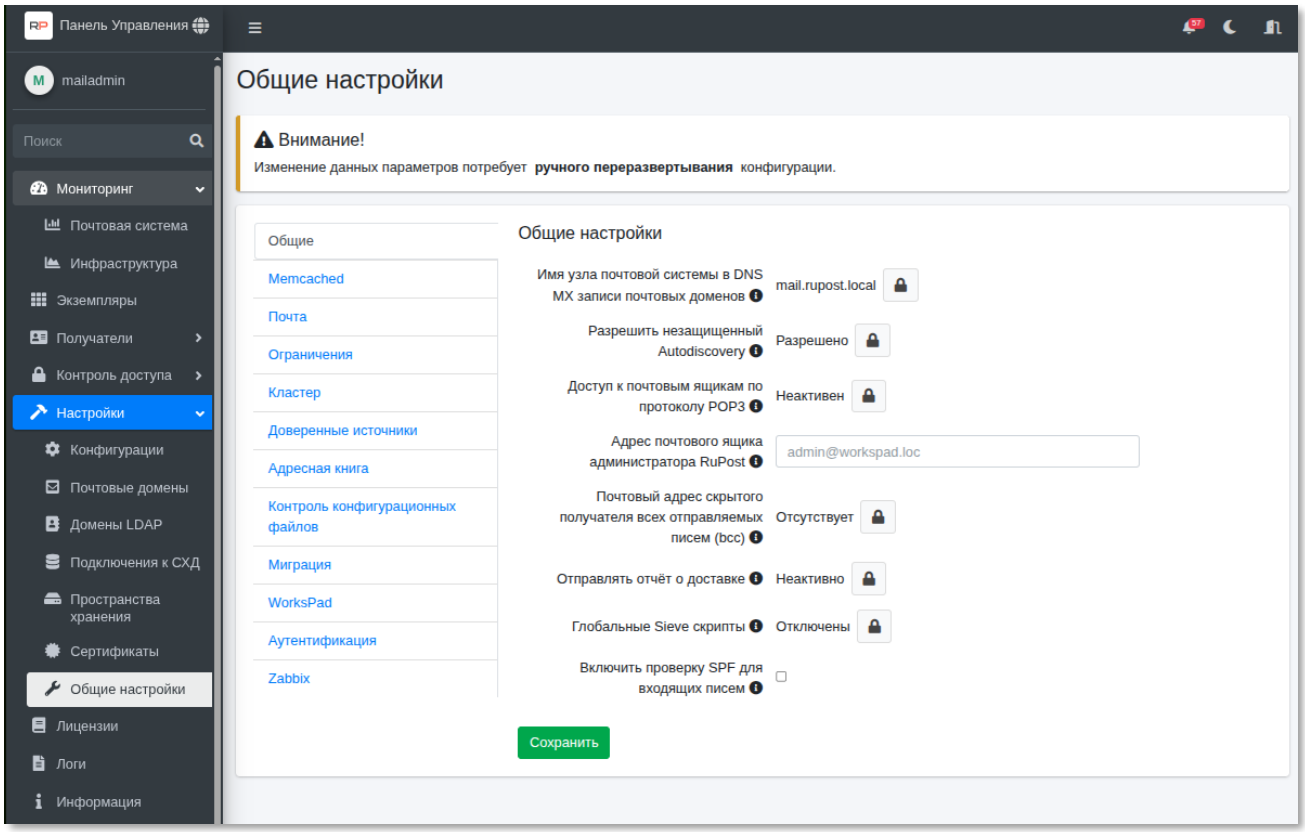
Ряд основных параметров, определяющих функционирование системы электронной почты, являются **глобальными**.

Глобальные параметры являются одинаковыми для всех сайтов Геокластера - конфигурируются на ведущем сайте и, затем, распространяются по всем сайтам.

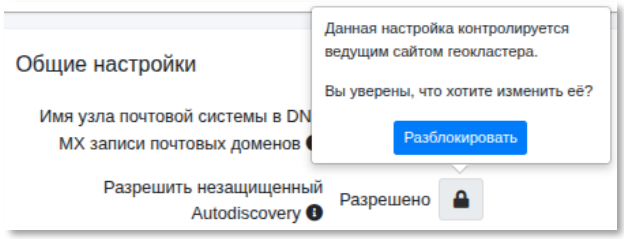
Перечень глобальных настроек в версии 4.0:

- Имя узла почтовой системы в DNS MX записи почтовых доменов
- Разрешить незащищенный Autodiscovery
- Доступ к почтовым ящикам по протоколу POP3
- Адрес почтового ящика администратора RuPost
- Почтовый адрес скрытого получателя всех отправляемых писем (bcc)
- Отправлять отчёт о доставке
- Глобальные Sieve скрипты
- Ограничения (все настройки)
- Настройки адресной книги
- Имя домена LDAP
- Почтовые домены

Если настройка является глобальной, то на сайте она будет помечена значком “замок”:

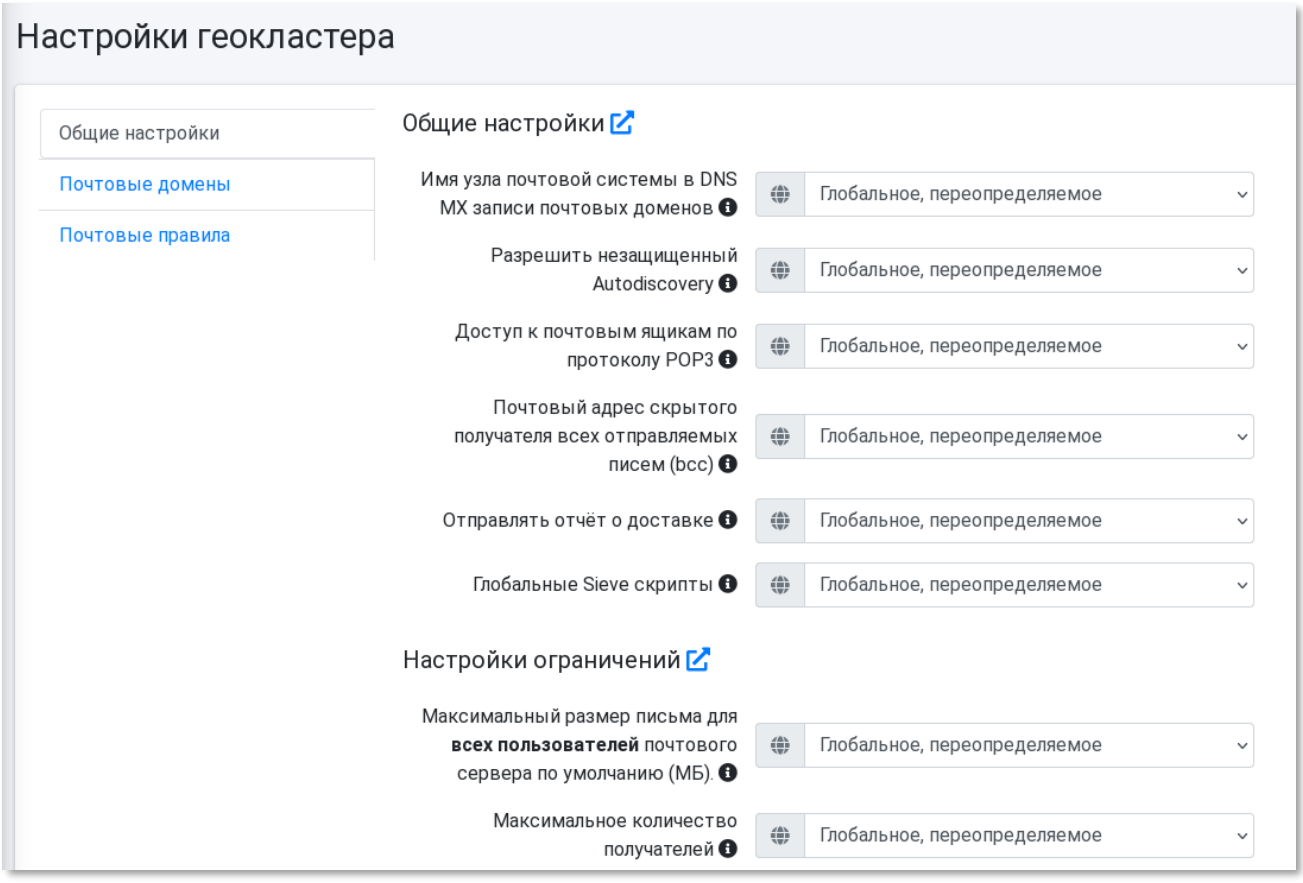


Для обеспечения надежности функционирования системы электронной почты при временном отсутствии доступности ведущего сайта, локальный администратор имеет возможность изменить значение глобальной настройки. При этом, локальному администратору будет показано предупреждение:



6.4.1. Геокластер - редактор глобальных настроек

В версии 4.1.0 добавлено назначение настройки глобальной с выбором политики применения этой настройки на ведомых сайтах.



Все параметры можно разделить на две группы – однозначные (строка / число / переключатель) и многозначные (список значений). Для каждой группы доступны различные политики назначения:

Для однозначных (например, “Отправлять отчет о доставке”) значений параметров возможны следующие варианты:

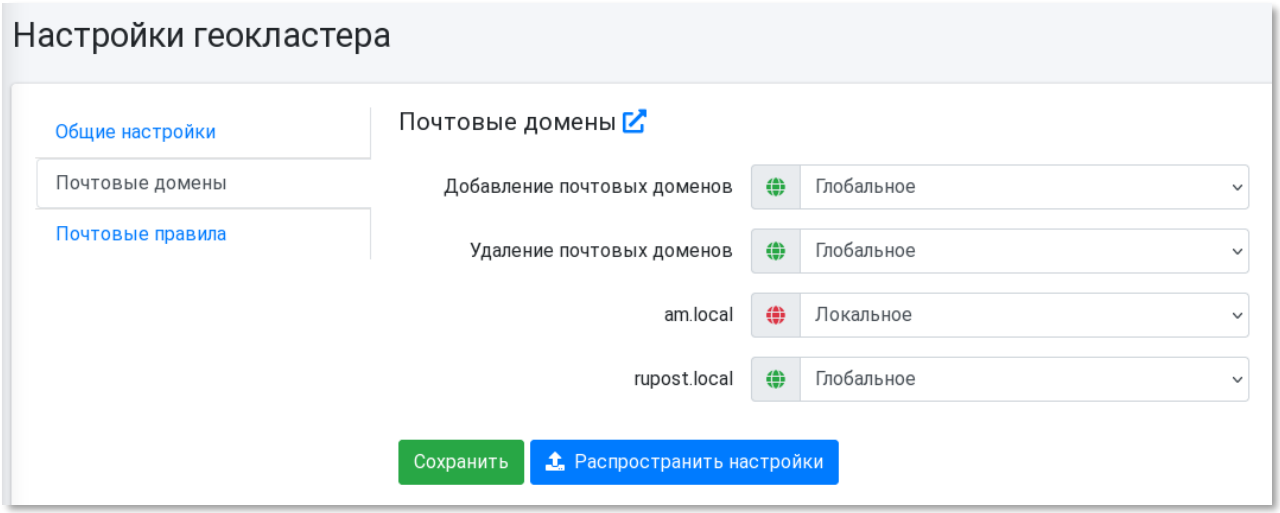
- **Глобальное** – значение параметра, заданное на ведущем сайте, переписывает значение на ведомом сайте. Администратор сайта не может изменить значение параметра.
- **Глобальное переопределяемое** - значение параметра, заданное на ведущем сайте, переписывает значение на ведомом сайте. Администратор сайта имеет возможность изменить значение параметра.
- **Локальное** – значение параметра является локальной настройкой ведущего сайта и не распространяется на другие сайты.

Для значений многозначных параметров (например, “Почтовые домены”), возможны следующие варианты для каждого элемента списка:

- **Глобальное** – элемент списка будет добавлен на всех сайтах Геокластера.
- **Локальное** – элемент списка является локальной настройкой ведущего сайта и не распространяется на другие сайты.

Для многозначных параметров есть дополнительные политики, задающие правила управления списком для добавления и удаления элементов:

- **Глобальное** – элементы списка могут быть добавлены только на ведущем сайте.
- **Локальное** – действие над списком не контролируется со стороны Геокластера.

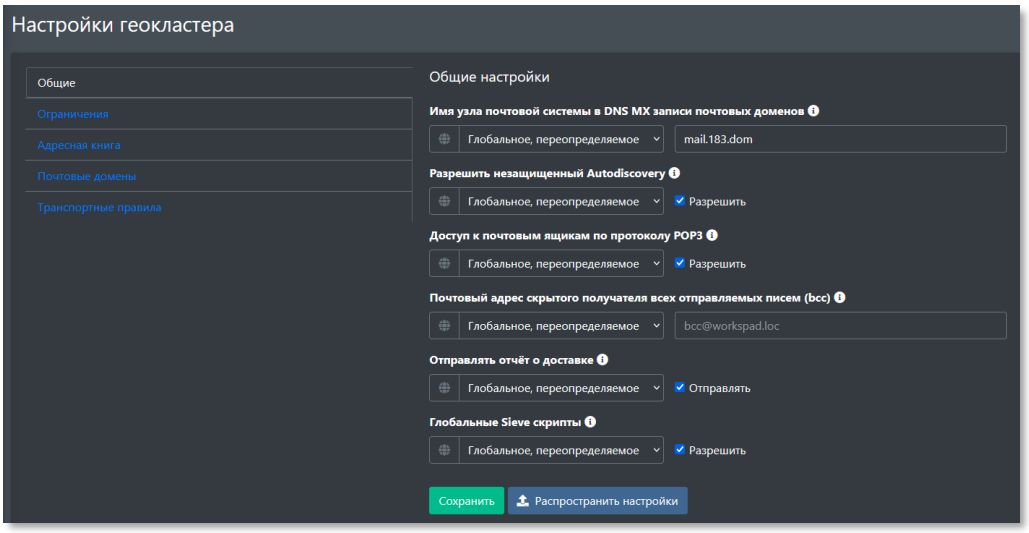


По нажатию на кнопку “Распространить настройки” произойдет оперативная рассылка внесенных изменений с ведущего на все ведомые сайты.

В версии 4.2.0 добавлена возможность редактирования настроек Геокластера непосредственно а Панели управления Геокластером.

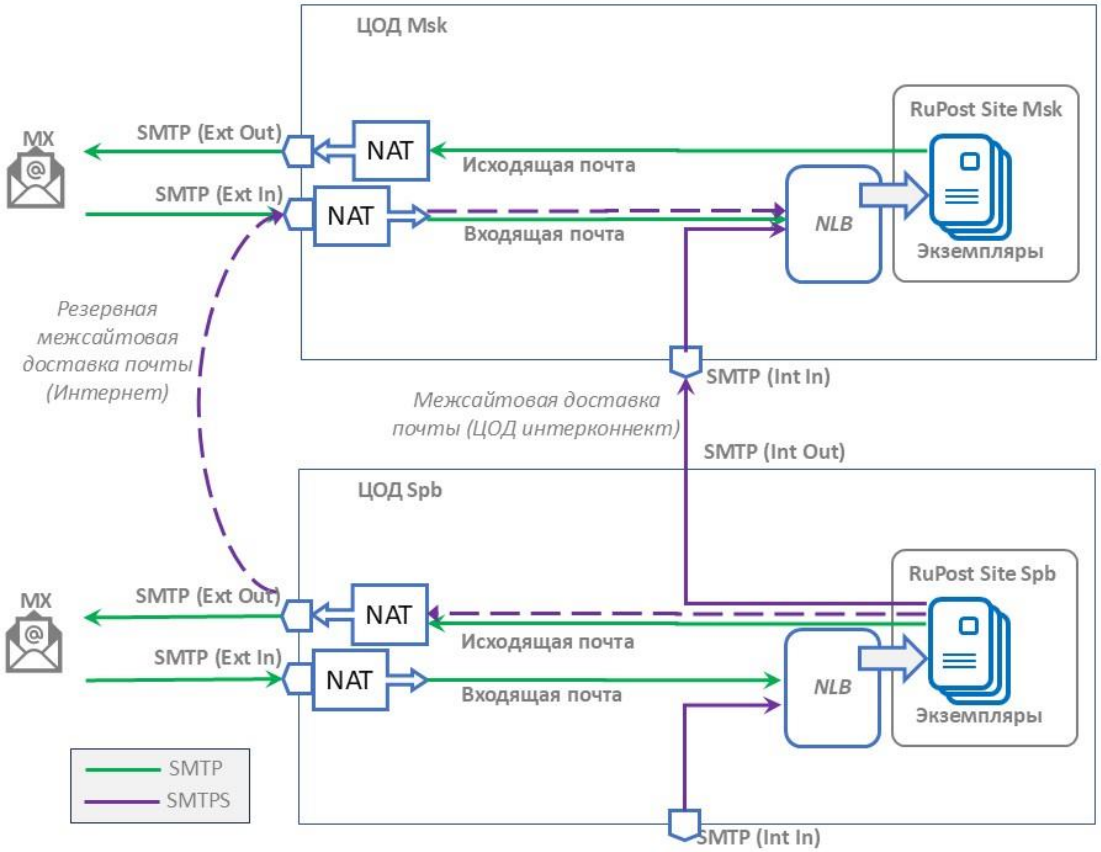
Ранее, настройки Геокластера являлись частью настроек ведущего сайта, т.е. при изменении настроек ведущего сайта вносились изменения в настройки Геокластера, теперь настройки Геокластера независимы от настроек ведущего сайта.

© 2021-2026 РуПост



6.5. Маршрутизация почты между сайтами

Схема маршрутизации почты в Геокластере приведена на диаграмме:



По сравнению с кластером RuPost, доставка почты в Геокластере имеет следующие особенности:

- **Автоматическая маршрутизация** почты – любой сайт может принимать всю почту, независимо от того, находится ли почтовый ящик адресата на этом сайте. Если почтовый

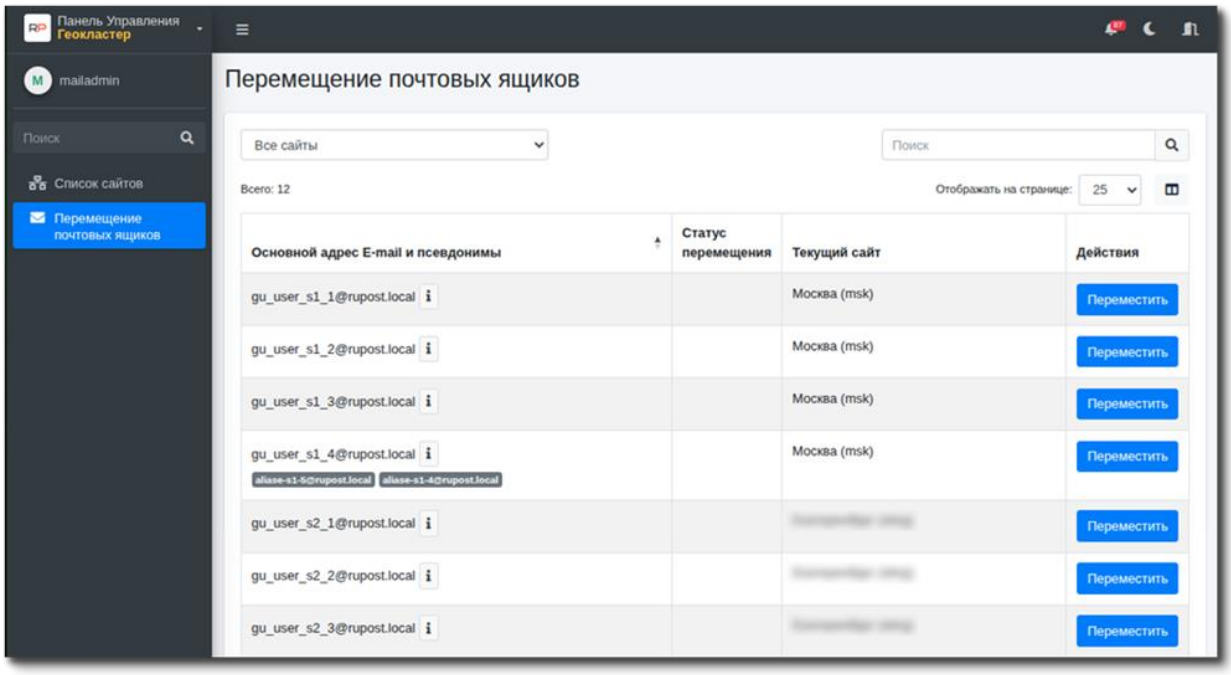
ящик адресата находится на другом сайте, то письмо будет передано на нужный сайт автоматически.

- **Два канала доставки** почты (основной и резервный) – доставка почты между сайтами осуществляется по основному каналу доставки - по внутренним адресам SMTP сайтов (SMTP Int In). Если основной канал не доступен, то почта будет доставлена по резервному каналу (на адрес SMTP Ext In).

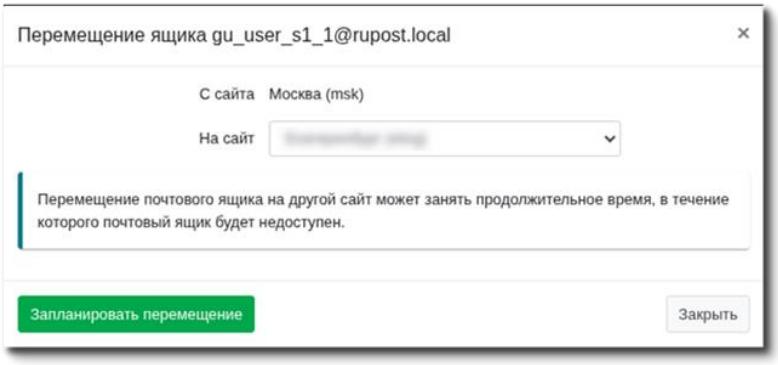
6.6. Перенос почтового ящика между сайтами

При необходимости (например, при переезде пользователя в другой город, либо оптимизации структуры системы электронной почты) почтовые ящики пользователей могут быть перемещены с “домашнего” сайта на другой сайт.

Для перемещения почтового ящика пользователя на другой сайт, в Панели управления Геокластером откройте окно “Перемещение почтовых ящиков” – будет показан список всех почтовых ящиков с указанием их “домашних” сайтов.



Для перемещения почтового ящика, нажмите кнопку “Переместить” на соответствующей строке – откроется окно, в котором можно выбрать сайт-приёмник.



После нажатия на кнопку “Запланировать перемещнение”, начнется процесс переноса ящика на сайт-приёмник, состоящий из двух этапов:

Этап 1:

1. Проверка возможности сайта-приёмника разместить копию переносимого ящика.
2. Создание почтового ящика на сайте-приёмнике (в статусе “Удален”).
3. Архивирование почтового ящика, создание основного архива.
4. Передача основного архива на сайт-приёмник.
5. Разархивирование основного архива на сайте-приёмнике в созданный ранее ящик.

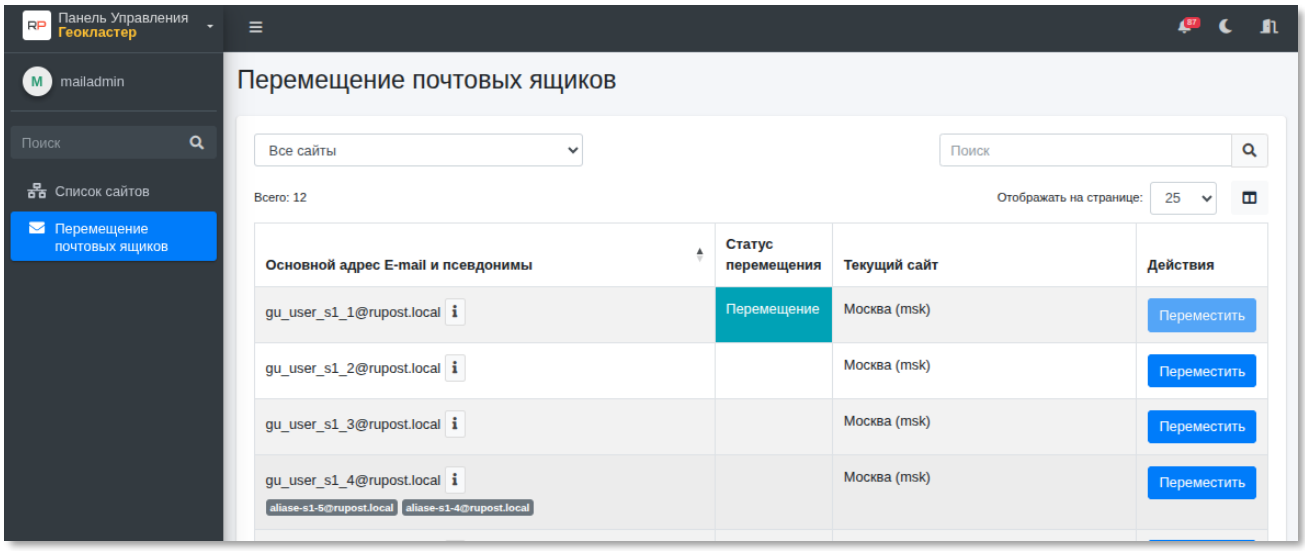
Этап 2:

6. Отключение почтового ящика на “домашнем” сайте (устанавливается статус “Выключен”).
7. На “домашнем” сайте формируется дельта-архив, содержащий изменения, произошедшие в почтовом ящике во время переноса основного архива, а также календари и адресные книги пользователя.
8. Передача дельта-архива на сайт-приёмник.
9. Разархивирование дельта-архива на сайте-приёмнике в созданный ранее ящик.
10. Включение ящика на сайте-приёмнике (перевод в статус “Активный”) – смена “домашнего” сайта.
11. Удаление ящика на бывшем “домашнем” сайте.

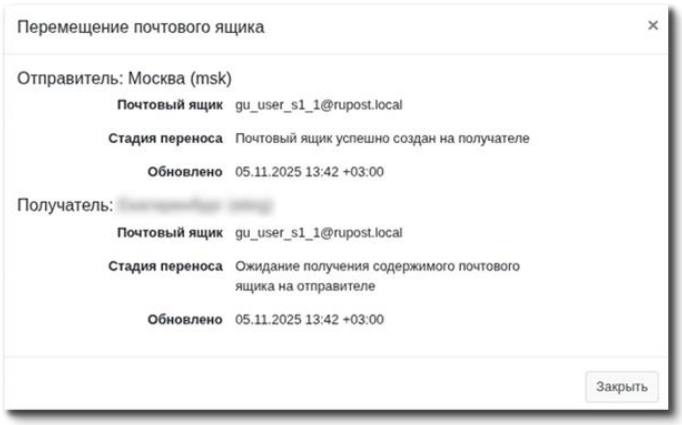
За счет организации переноса почтового ящика в два этапа, время отсутствия доступа пользователя к своему почтовому ящику минимизировано и равно времени обработки дельта-архива (шаги с 6-го по 10-й).

В окне “Перемещение почтовых ящиков” те почтовые ящики, которые в данный момент перемещаются, имеют статус “Перемещение”.

© 2021-2026 РуПост



В ходе переноса ящика, администратор имеет возможность отслеживать текущий статус процесса в окне статуса переноса:



Отображаемый статус соответствует шагам процесса переноса, описанным выше.

6.7. Списки рассылок и общие ящики

В Геокластере пользователи имеют те же возможности, что и в кластере RuPost, включая использование списков рассылки и общих ящиков.

В Геокластере у каждого списка рассылки и общего ящика есть свой “домашний” сайт – тот, на котором список рассылки или общий ящик был создан. При этом, список пользователей, как для списка рассылки, так и для общего ящика, не ограничен списком пользователей “домашнего” сайта, а может включать всех пользователей Геокластера независимо от расположения их почтовых ящиков.

Соответственно, если пользователь подключен к своему “домашнему” сайту с использованием веб-клиента либо через IMAP и имеет права доступа к общему ящику, находящемуся на другом сайте, то он может работать с этим общим ящиком также, как в кластере RuPost (см. “Ограничения в работе Геокластера”).

Рассмотрим, как происходит распределенная обработка почты на примере списка рассылки. При отправке письма пользователем сайта 1 на список рассылки, находящийся на сайте 2, письмо будет сначала доставлено на сайт 2, обработано на сайте 2 и затем отправлено всем адресатам списка рассылки с сайта 2.

При отправке письма пользователем от имени общего ящика, находящегося на другом сайте, схема обработки почты аналогична вышеописанной.

Обновление прав доступа пользователей динамических списков рассылки и общих ящиков происходит раз в 6 часов.

При необходимости, обновление динамического списка рассылки можно выполнить командой CLI:

```
rupost distribution-lists sync-geocluster-dynamic-users
```

Для запуска синхронизации прав доступа пользователей на общий почтовый ящик можно использовать команду CLI:

```
rupost shared-mailbox sync-master
```

6.8. Ограничения в работе Геокластера

В версии 4.0 Геокластер имеет следующие ограничение:

Работа с календарями, находящимися на других сайтах – расширенные функции работы с календарями, находящимися на разных сайтах и других почтовых серверах (например, в режиме сосуществования RuPost с Exchange) доступны при использовании клиентов WorksPad X и Desktop X и соответствующей регистрации сайтов и сторонних почтовых серверов на соответствующих серверах WorksPad.

6.9. Геокластер – резервный сайт

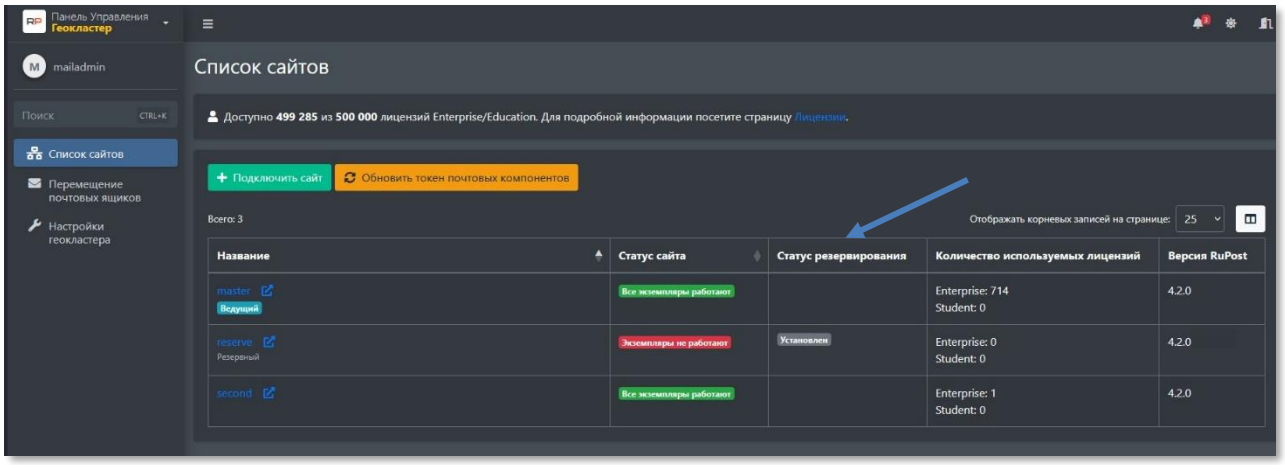
В версии 4.2.0 добавлена возможность создания в Геокластере сайтов специального типа – “Резервный”.

Резервный сайт является “зеркалом” одного из сайтов Геокластера (назовем его - Основной). Соответственно, данные пользовательских почтовых ящиков, а также локальные настройки (такие как списки рассылки, ресурсы и т.д.) постоянно реплицируются с Основного сайта на Резервный с тем, чтобы, при необходимости, можно было максимально быстро и с минимально возможными потерями переключить обслуживание пользователей с Основного на Резервный сайт.

Для обеспечения корректной репликации данных, Резервный сайт должен иметь такую же структуру Хранилищ, что и Основной сайт. Соответственно, Резервный сайт может использоваться для резервирования только одного сайта Геокластера.

Для снижения нагрузки на канал связи между ЦОДами Основного и Резервного сайтов, производится только репликация мастер-хранилищ почты и баз данных, а архивы и записи (records) – не реплицируются.

Управление Резервными сайтами осуществляется с помощью Панели управления Геокластером. Для мониторинга состояния Резервного и Основного сайтов в таблицу Список сайтов добавлен столбец “Статус резервирования”.



В этом столбце отображаются три статуса:

- **Общий статус (ОС)** сайта с точки зрения процесса управления Резервным сайтом. Возможные значения – *Установлен, Подключен, Готов к репликации, Первичная репликация, Репликация, Активен.*
- **Статус репликации баз данных (СБД)**. Возможные значения – *Не реплицировано, Реплицируется, Реплицировано, Не реплицировалось.*
- **Статус репликации хранилища почтовых данных (СХП)**. Возможные значения - *Не реплицировано, Реплицируется, Реплицировано, Не реплицировалось.*

Для лучшего понимания процесса работы с Резервным сайтом в целом, приведем его краткое пошаговое описание:

1. Установка кластера RuPost в резервном ЦОД (при установке подтверждаем, что устанавливаем Резервный сайт).
2. В Панели управления Геокластером:
    a. Добавление нового сайта в Геокластер (Общий статус для Резервного сайта, ОС = “Установлен”).
    b. Связывание основного и резервного сайтов (ОС = “Подключен”, СБД = “Не реплицировалось”, СХП = “Не реплицировалось”).
    c. Начинается однократная репликация баз данных и создание структур хранения данных на Резервном сайте (СБД = “Реплицируется”).
    d. По завершению первой репликации баз данных (СБД = “Реплицировано”) все Пространства хранения и Хранилища почты созданы на Резервном сайте автоматически.
3. В Панели управления Резервным сайтом - администратор Резервного сайта:
    a. Настраивает все Хранилища (с помощью команд CLI указывает точки монтирования NFS)

   b. При необходимости, восстанавливает из резервной копии Хранилищ Основного сайта содержимое соответствующих Хранилищ Резервного сайта.
   c. Переводит все Хранилища в статус “Активно”, начинается репликация почтовых данных с Основного на Резервный сайт (СХП = “Реплицируется”).
4. По завершении первой репликации почтовых данных (СХП = “Реплицировано”), Резервный сайт полностью готов (ОС = “Репликация”). С этого момента, при необходимости, обслуживание пользователей Основного сайта может быть переведено на Резервный сайт. Начинается периодическая синхронизация содержимого баз данных и почтовых данных с соответствующими изменениями статусов СБД и СХП.

Рассмотрим каждый шаг приведенного выше процесса подробнее.

6.9.1. Создание резервного сайта

Для создания Резервного сайта, необходимо установить кластер RuPost в резервном ЦОД. При установке, необходимо указать, что происходит установка Резервного сайта:

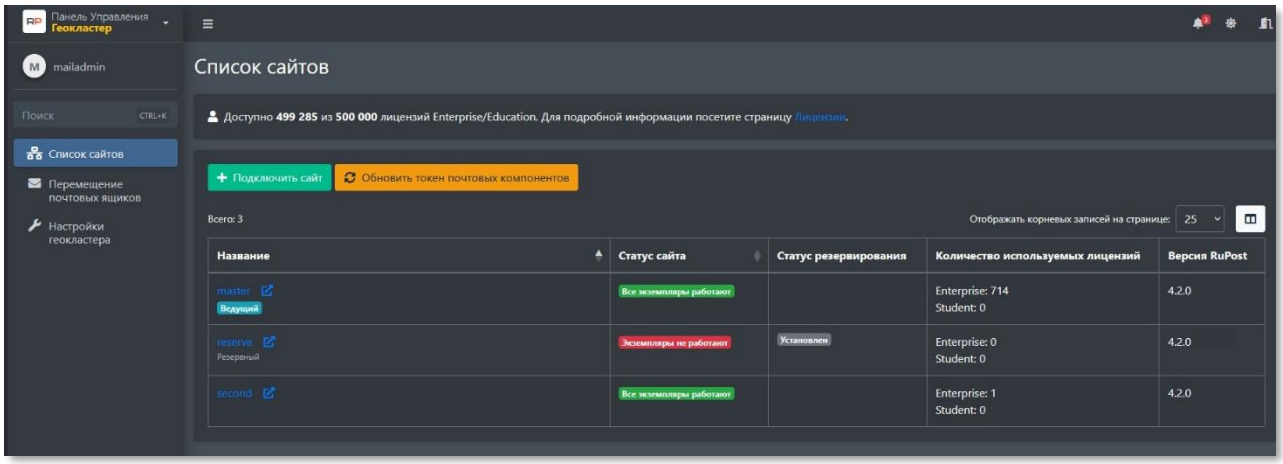


При установке Резервного сайта не будут созданы структуры хранения данных и, соответственно, не будут запущены почтовые компоненты. В дальнейшем, информация о структурах данных (Пространства хранения и Хранилища) будет получена Резервным сайтом с Основного сайта.

При выборе инфраструктуры для Резервного сайта, нужно исходить из того, что Резервный сайт должен иметь возможность обслуживать такое же количество пользователей, что и Основной сайт, поэтому должен иметь схожие характеристики как по количеству и мощности узлов кластера, так и по объему выделяемых хранилищ NFS.

После завершения установки, необходимо добавить Резервный сайт в Геокластер, в котором находится основной сайт.

После успешного добавления Резервного сайта в Геокластер, он будет иметь статус ОС = “Установлен”.



6.9.2. Назначение резервного сайта

Внимание!

Перед назначением резервного сайта необходимо остановить работу экземпляра RuPost на резервном сайте в панели управления резервного сайта.

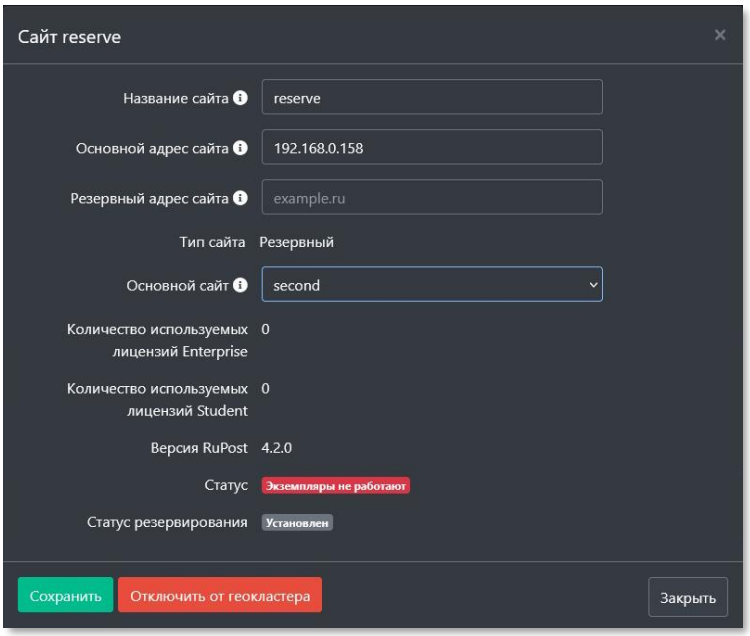
Назначение резервного сайта происходит в панели управления геокластера на ведущем сайте.

После назначения резервного сайта необходимо запустить экземпляр RuPost на резервном сайте в панели управления резервного сайта.

Убедиться в работе резервного сайта и подключении можно в панели управления геокластера на ведущем сайте.

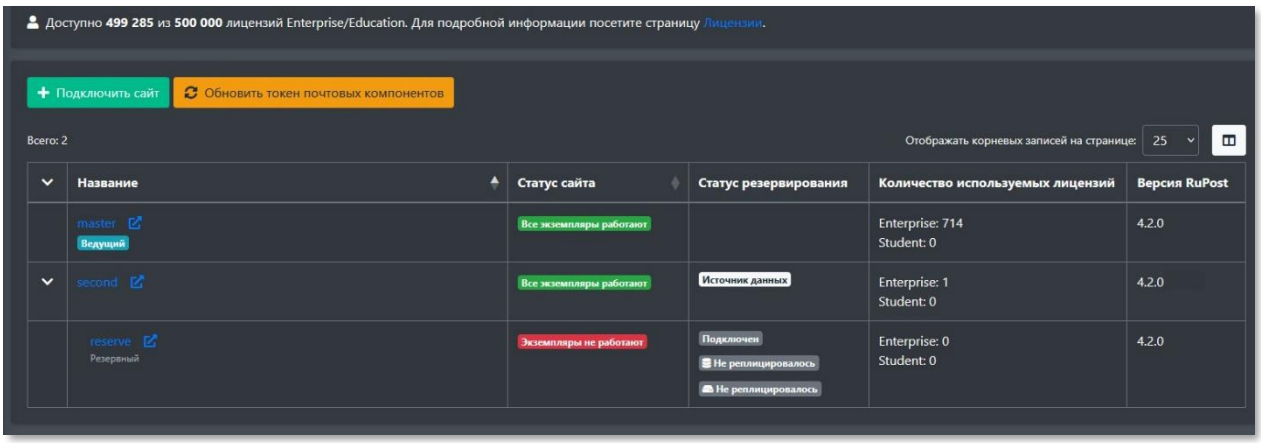
После добавления Резервного сайта в Геокластер, появится возможность выбора Основного сайта, т.е. сайта, который будет “резервироваться” этим Резервным сайтом и, соответственно, с которого будет проводится постоянная репликация почтовых данных.

Выбор Резервного сайта осуществляется в выпадающем списке в строке основного сайта:



После “связывания” Основного и Резервного сайта назначение уже нельзя изменить, так как, сразу же после назначения, начинается синхронизация структур данных.

После назначения Резервного сайта, он станет отображаться в списке сайтов непосредственно под основным и его статус ОС станет “Подключен”.



После подключения к Основному сайту, начнется первая репликация баз данных (СБД = “Реплицируется”).

6.9.3. Репликация баз данных на резервный сайт

В рамках репликации баз данных с Основного на Резервный сайт пересылается следующая информация:

- Структура Пространств хранения и мастер-хранилищ почты.

- Настройки почтовых сервисов – все настройки Основного сайта, не имеющие привязки к локальной инфраструктуре (почтовые и LDAP домены, почтовые ящики, списки рассылки, LDAP-фильтры и пр.).
- Пользовательские Календари, Контакты и адресные книги.

Текущий статус репликации баз данных (СБД) отображается на Панели управления Геокластером в Списке сайтов в столбце “Статус резервирования” – помечен иконкой “База данных”.

Репликация баз данных с Основного на Резервный сайт происходит в два этапа:

- Первоначальная репликация.
- Постоянная репликация.

Первоначальная репликация баз данных начинается в момент подключения Резервного сайта к Основному (СБД = “Реплицируется”). В этот момент, на Основном сайте формируется архив баз данных, который пересылается на Резервный сайт. После получения и распаковки архива на Резервном сайте, информация из баз данных Основного сайта переносится в соответствующие базы данных Резервного сайта (СБД = “Реплицировано”). В результате на Резервный сайт будут автоматически перенесены все настройки Основного сайта и внесены изменения в структуры хранения почтовых данных - будут созданы Пространства хранения и мастер-Хранилища, аналогичные соответствующим структурам Основного сайта.

Будут созданы копии не всех Хранилищ Основного сайта, а только те Хранилища, которые будут, в дальнейшем, использоваться для репликации данных, а именно – почтовые мастер-хранилища. Почтовые реплики созданы не будут, а мастер-хранилища для Архивов и Записей (Records) будут созданы, но не будут реплицироваться с Основного на Резервный сайт.

Внимание!

Рекомендуем регулярно выполнять резервное копирование данных Основного сайта, в том числе, архивов и записей (records).

После успешного завершения первоначальной репликации начинается постоянная репликация. Постоянная репликация баз данных функционально не отличается от первоначальной, но выполняется периодически - раз в 60 минут. Таким образом, при переключении обслуживания пользователей с Основного на Резервный сайт возможна потеря информации за последние 60 минут.

6.9.4. Конфигурирование резервного сайта

После завершения первичной репликации баз данных, для того чтобы Резервный сайт мог принимать данные с Основного сайта, на нем должны быть полностью сконфигурированы все автоматически созданные почтовые Хранилища - для каждого Хранилища, администратор Резервного сайта должен указать точки монтирования NFS. Это можно сделать с помощью команды CLI:

```
rupost mailstore update --id {UUID хранилища} --storage-type "nfs" --
  host {адрес nfs сервера} --path {путь до папки хранилища}
```

Когда конфигурирование Хранилищ завершено, для уменьшения объема данных при первоначальной репликации, администратор Резервного сайта может восстановить почтовые данные из резервной копии мастер-Хранилищ основного сайта – напрямую в Хранилища Резервного сайта с помощью средств резервного копирования. Так как Резервный сайт, в данный момент, не обслуживает пользователей и его почтовые компоненты отключены на всех узлах кластера, то прямое копирование данных из резервной копии напрямую в файловую структуру Хранилищ безопасно (не приведет к нарушению структур данных Maildir).

После того, как сделаны все необходимые настройки и восстановление данных из резервной копии завершено, администратор должен включить все Хранилища Резервного сайта (перевести их в статус “Активно”) – после этого начнется первоначальная репликация почтовых данных с основного сайта (СХП = “Реплицируется”).

6.9.5. Репликация почтовых данных на резервный сайт

Репликация почтовых данных с Основного на Резервный сайт происходит в два этапа:

- Первоначальная репликация.
- Постоянная репликация.

Текущий статус репликации почтовых данных (СХП) отображается на Панели управления Геокластером в Списке сайтов в столбце “Статус резервирования” – помечен иконкой “Хранилище”.

Первоначальная репликация почтовых данных начинается после включения администратором Резервного сайта всех Хранилищ (СХП = “Реплицируется”). В этот момент, на основном сайте для каждого мастер-хранилища формируется архив почтовых данных, который пересылается на Резервный сайт.

Если администратор Резервного сайта перед включением Хранилищ восстанавливал данные из резервной копии, то, соответственно, эти данные не нужно повторно копировать с Основного на Резервный сайт и первоначальная репликация будет включать данные только с указанного администратором момента времени.

Для того, чтобы указать время, с которого нужно начинать копирование, нужно для каждого Хранилища, выполнить следующую команду CLI:

```
rupost mailstore set-reserve-sync-timestamp –timestamp {дата и время}
  –id {идентификатор хранилища}
```

После получения и распаковки архива на Резервном сайте, почтовые данные из мастер-хранилищ Основного сайта попадают в соответствующие мастер-хранилища Резервного сайта (СХП = “Реплицировано”). После успешного завершения первоначальной репликации начинается постоянная репликация.

Постоянная репликация функционально не отличается от первоначальной, но выполняется периодически - раз в 60 минут. Таким образом, при переключении обслуживания пользователей с основного на Резервный сайт возможна потеря почты, полученной за последние 60 минут.

В версии 4.3.4 усовершенствована репликация данных с основного на резервный сайт.

Отказоустойчивость сайта Геокластера, обеспечиваемая резервным сайтом, существенно зависит от времени репликации данных с основного на резервный сайт. Для повышения скорости передачи данных на резервный сайт был полностью переработан механизм репликации. Передача данных осуществляется с использованием прямого (socket) сетевого подключения с основного на резервный сайт по порту **5010** (SSL).

6.9.6. Переключение на резервный сайт

Внимание!

Для того, чтобы пользователи подключались к Резервному, а не к основному сайту Геокластера, необходимо внести соответствующие правки в записи DNS.

После того, как успешно завершилась первая репликация почтовых данных (ОС = “Реплицировано”), администратор Резервного сайта имеет возможность переключить обслуживание пользователей на Резервный сайт. Переключение производится только вручную, разворачиванием конфигурации и последующим вводом в эксплуатацию экземпляров RuPost на Резервном сайте.

Основной и резервный сайт не должны одновременно обслуживать пользователей.

Рассмотрим два сценария переключения обслуживания пользователей с Основного на Резервный сайт, отличающиеся наличием связи между Основным и Резервным сайтами в момент переключения:

- **Связь есть** – штатное переключение (например, при смене ЦОД для кластера RuPost).
- **Связи нет** – аварийное переключение (ЦОД Основного сайта вышел из строя).

При наличии связи между Основным и Резервным сайтами, для исключения возможности одновременной работы Основного и Резервного сайтов, при попытке ввести Резервный сайт в эксплуатацию проводится проверка – включен ли Основной сайт. Если Основной сайт работает, то Резервный не может быть введен в эксплуатацию. Соответственно, перед включением Резервного сайта, администратор Основного сайта должен отключить все узлы кластера RuPost на Основном сайте. В данном случае, **вывода из эксплуатации недостаточно**, нужно, чтобы все компоненты были отключены, включая *rupost* и *HAProxy*. После того, как основной сайт полностью выключен, Резервный может быть включен разворачиванием конфигурации почтовых компонентов и вводом в эксплуатацию экземпляров RuPost.

Рекомендуемая последовательность действий при штатном переключении на Резервный сайт:

1. **Вывести из эксплуатации** все экземпляры Основного сайта (при этом новые данные перестанут поступать, но сервис *rupost* продолжит работу).

2. **Обновить записи в DNS** – переключить обслуживание пользователей с Основного на Резервный сайт.
3. **Обновить настройки LDAP** – нужно указать адреса локальных серверов LDAP и, если используется выделенный сервер Memcached, его адрес.
4. Чтобы дать возможность провести завершающую репликацию почтовых данных, необходимо, перед следующим шагом, **подождать** не менее 2-х часов (интервал синхронизации + время на передачу архива на Резервный сайт).
5. Если Основной сайт не является мастер-сайтом Геокластера, то его нужно удалить из Геокластера.
6. **Отключить** узлы кластера RuPost (остановить сервис RuPost, либо отключить полностью) на Основном сайте.
7. **Включить** Резервный сайт - развернуть конфигурацию и ввести в эксплуатацию экземпляры RuPost.

При отсутствии связи с Основным сайтом, RuPost считает, что Основной сайт уже отключен, поэтому администратор Резервного сайта имеет возможность сразу же включить Резервный сайт.

В версии 4.3.4 оптимизирован механизм переключения с основного на резервный сайт в части получения последней порции данных (дельта) перед переключением.

Для того, чтобы полностью исключить потерю данных при переключении с основного на резервный сайт, при штатном переключении (когда основной сайт в момент переключения имеет связь с резервным) выполняется следующая последовательность действий:

1. **Отключение основного сайта** (остановка всех почтовых компонентов) – сайт не принимает и не отправляет почту.
2. **Репликация баз данных**.
3. **Репликация данных хранилищ** – данные, которые появились на основном сайте с момента последней репликации.
4. При успешном завершении п. 2 и 3 происходит разворачивание конфигурации на резервном сайте и запуск почтовых компонентов – переключение завершено, сайт полностью готов обслуживать пользователей основного сайта.

В версии 4.3.4 происходит автоматическое назначение основного сайта резервным при переключении.

При штатном переключении обслуживания пользователей с основного на резервный сайт, в момент переключения данные пользователей на обеих сайтах полностью идентичны, и конфигурация основного сайта является достаточной для обслуживаемого числа пользователей. Таким образом, основной сайт является наилучшим “кандидатом” на выполнение роли резервного сайта после переключения. Соответственно, при переключении происходит не только назначение резервного сайта основным, но и назначение основного резервным – т.е. роли сайтов меняются местами, но сайты остаются связанными друг с другом.

© 2021-2026 РуПост

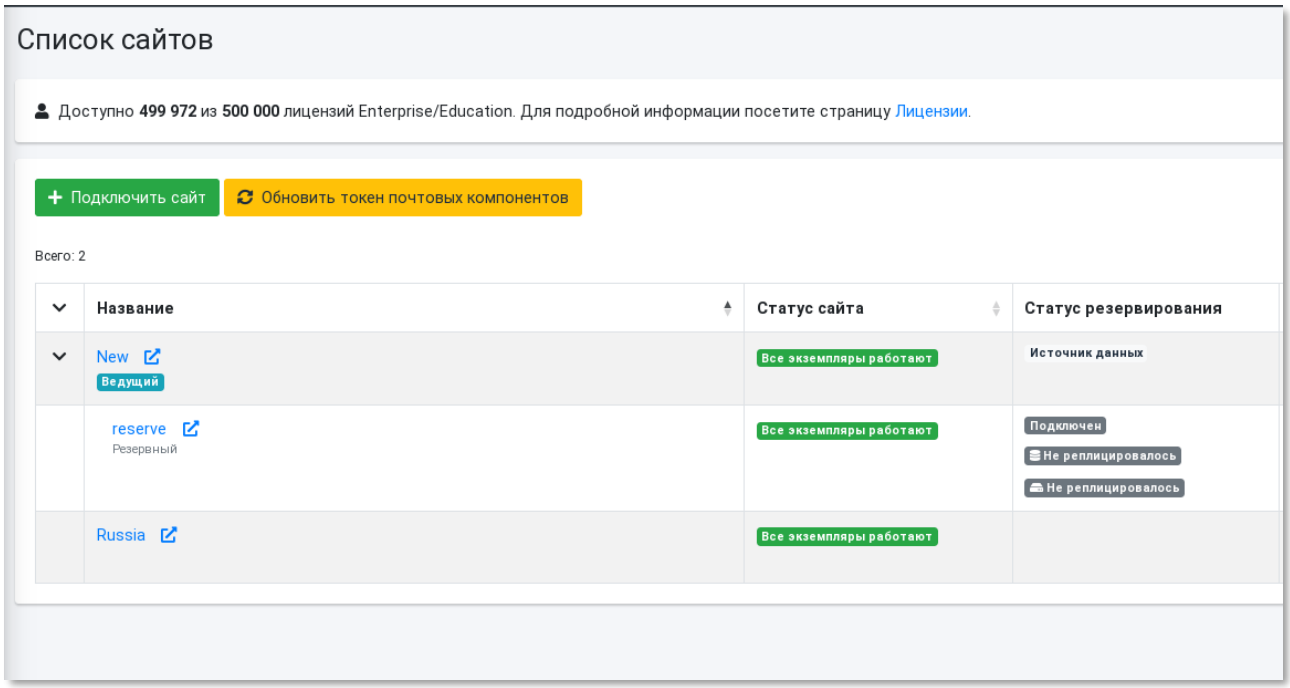
Назначение бывшего основного сайта резервным не означает, что репликация начнет автоматически работать в обратную сторону. Для того, чтобы репликация заработала, необходимо пройти на сайте все процедуры, предшествующие включению резервного сайта.

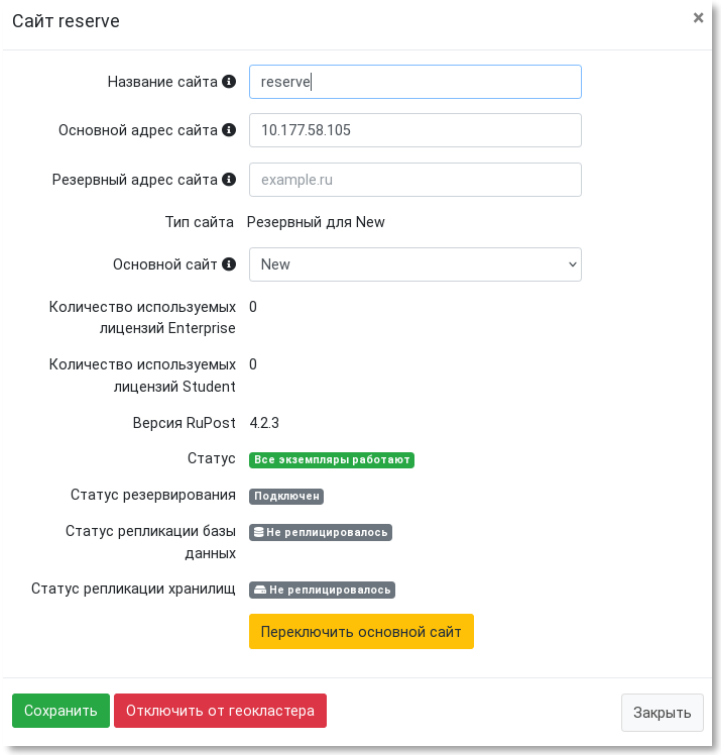
6.9.7. Отключение резервного сайта

При необходимости, для отключения Резервного сайта, его следует удалить из Геокластера. В этот момент будет остановлена репликация как баз данных, так и почтовых данных с Основного сайта.

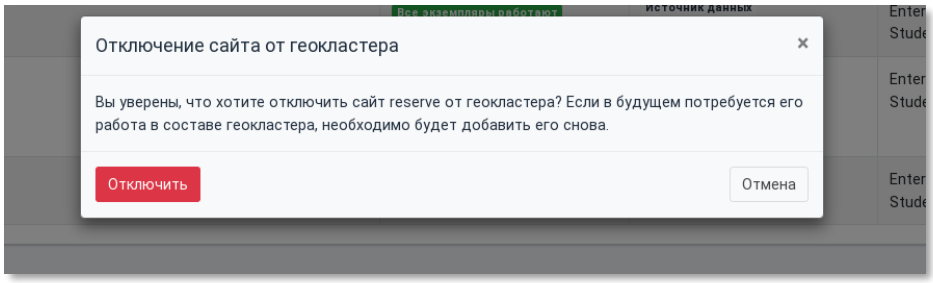
Последовательности действий по удалению резервного сайта из геокластера.

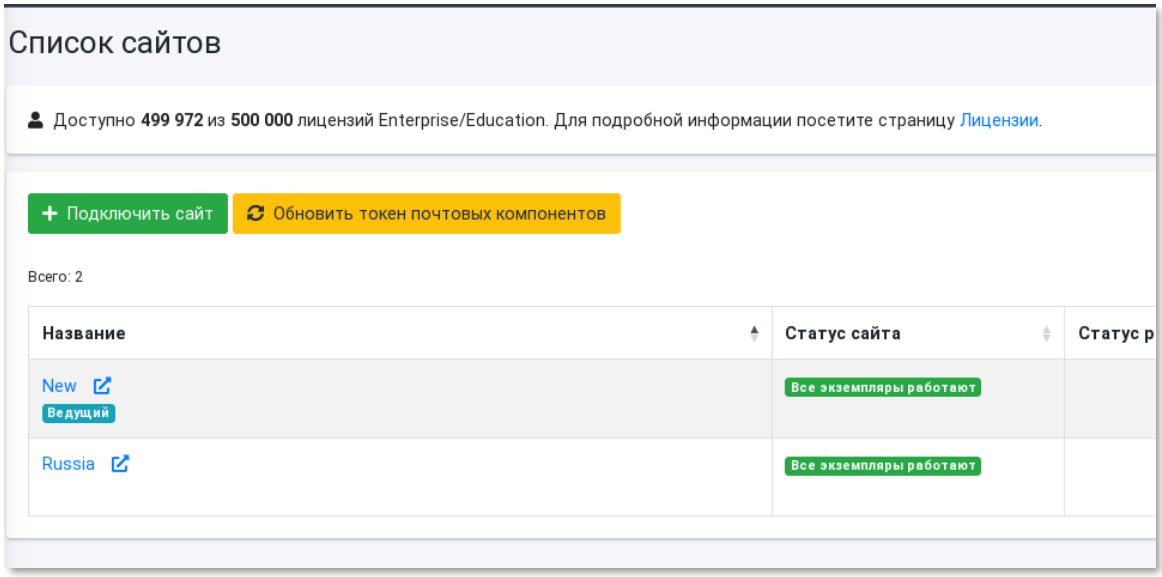
Необходимо кликнуть на имя сайта в панели управления геокластером и выбрать кнопку удаления. Переходим в панель управление геокластера на ведущем сайте. Открываем опции резервного сайта





Затем отключаем от геокластера с помощью соответствующей кнопки





Далее необходимо переразвернуть конфигурацию на серверах отключенного резервного сайта.

6.10. Геокластер – трассировка писем

В версии 4.2.0 расширена функциональность трассировки писем – находясь на одном из сайтов Геокластера можно отследить путь доставки письма даже в том случае, когда оно пересылалось между несколькими сайтами Геокластера.

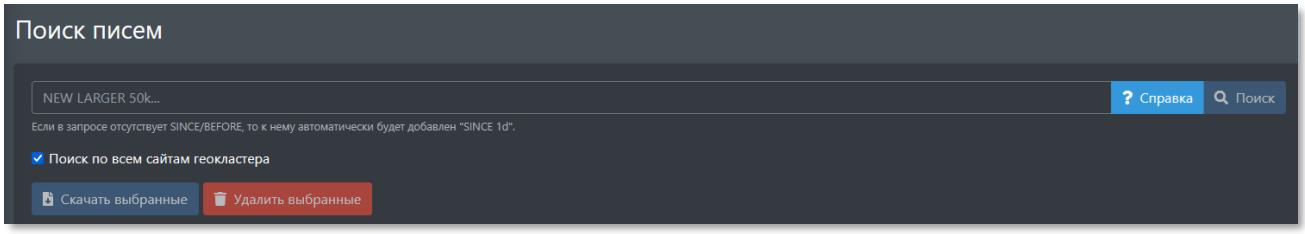
6.11. Геокластер – отзыв писем

В версии 4.2.0 расширена функциональность отзыва писем – когда пользователь запросит отзыв письма, эта операция будет выполнена на всех сайтах Геокластера.

6.12. Геокластер – поиск и выгрузка найденных писем

В версии 4.2.0 добавлена возможность поиска писем на всех сайтах Геокластера.

Для того, чтобы поиск письма осуществлялся на всех сайтах Геокластера, необходимо на странице ”Поиск писем” отметить переключатель “Поиск по всем сайтам Геокластера”.



Также расширена функциональность сохранения найденного письма – появилась возможность сохранить найденное письмо, даже если почтовый ящик, где оно находится, расположен на другом сайте Геокластера.

6.13. Геокластер – лицензирование

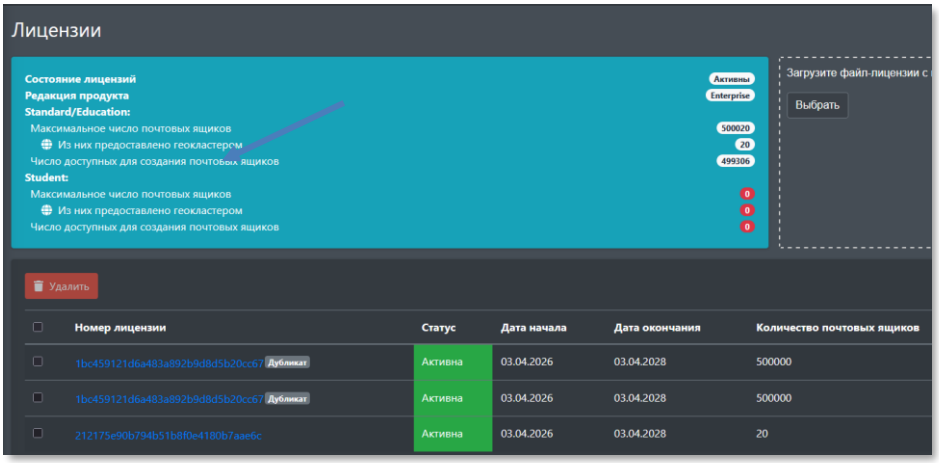
В версии 4.2.0 расширен механизм лицензирования – все сайты, входящие в Геокластер, используют единый пул лицензий.

При добавлении сайта в Геокластер, его лицензии добавляются в общий пул лицензий Геокластера. Соответственно, при удалении сайта из Геокластера, его лицензии удалятся из общего пула лицензий Геокластера и, как и ранее, они продолжают использоваться в рамках отдельного кластера RuPost.

Например, предположим, что до создания Геокластера кластер RuPost1 имел *100* Enterprise лицензий, из которых было использовано *80* (т.е. на RuPost1 было *80* почтовых ящиков), кластер RuPost2 имел *200* Enterprise лицензий, из которых было использовано *50*. При создании Геокластера, объединяющего эти два кластера, общее количество лицензий будет *100 + 200 = 300* Enterprise лицензий, из которых будет использовано *80 + 50 = 130* лицензий. Таким образом, количество доступных лицензий *300 – 130 = 170* может быть использовано на любом сайте Геокластера. Если до

добавления в Геокластер на RuPost1 можно было добавить только *20* почтовых ящиков, то в рамках Геокластера можно добавить все *170*.

Статистика по лицензиям в Геокластере отображается на странице “Лицензии”.



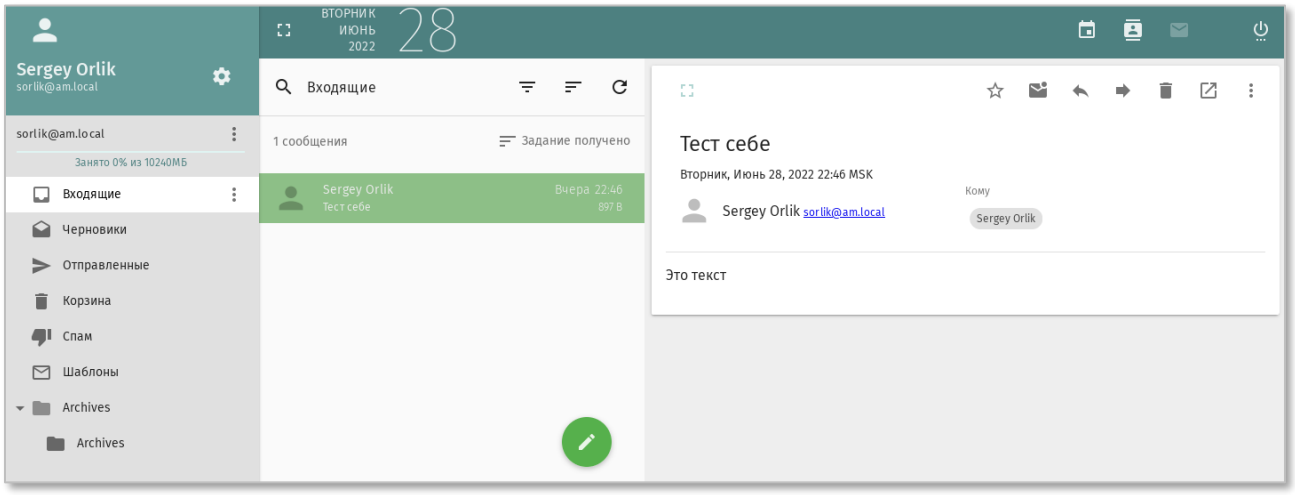
Как и раньше, в списке лицензий отображаются только лицензии, загруженные на конкретном кластере / сайте Геокластера. Однако, если данная лицензия уже была использована на другом сайте, то у нее добавляется пометка “Дубликат”.

Каждая лицензия учитывается в пуле лицензий только один раз. Если на различных кластерах была использована одна и та же лицензия (например, для установки с последующим добавлением в Геокластер), то, при добавлении сайта в Геокластер, количество доступных лицензий не увеличится.

7. Клиентские приложения

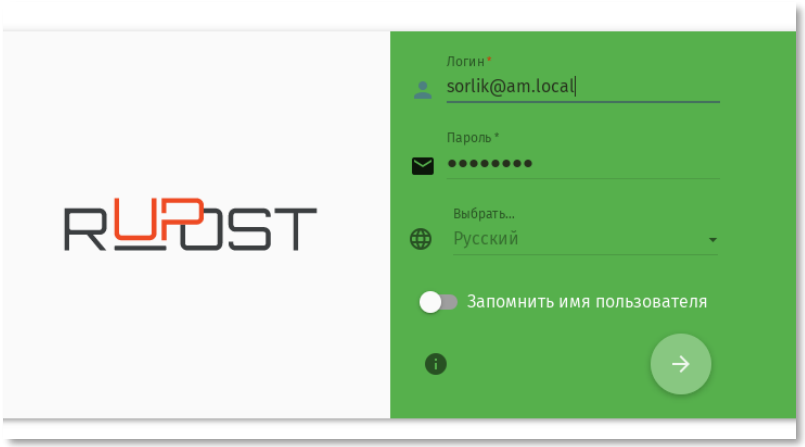
7.1. Встроенный web-клиент

Все редакции RuPost включают в себя встроенный web-клиент (интегрированный почтовый компонент SOGo). Web-клиент предоставляет средства работы с письмами, календарями, контактами, корпоративной адресной книгой (GAL) и специальными настройками почтового ящика, как например, использование псевдонимов не только для получения, но и для отправки почты.

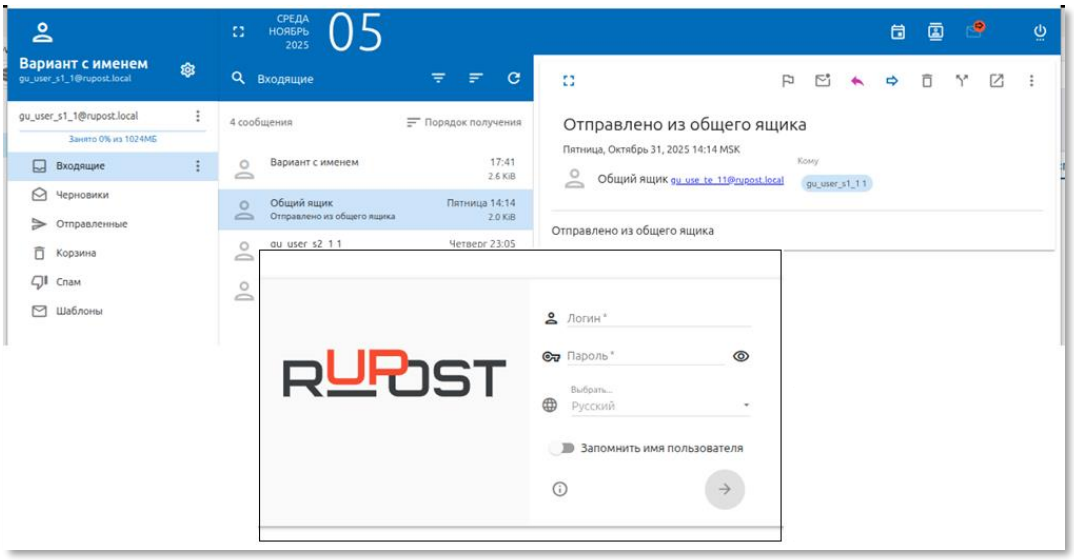


Для доступа в web-клиент RuPost необходимо в браузере ввести адрес узла почтового сервера. Для входа в web-клиент указывается:

- Логин: основной адрес электронной почты пользователя (myname@mydomain.ru)
- Пароль: пароль пользователя в службе каталогов



В версии 4.0 обновлен пользовательский интерфейс при сохранении принципов навигации по функциям. Пометка требующих внимания сообщений приведена к общепринятому "флаг", вместо "звездочка".



В версии 4.3.4 расширены функциональные возможности веб-клиента rupost-mua – добавлено:

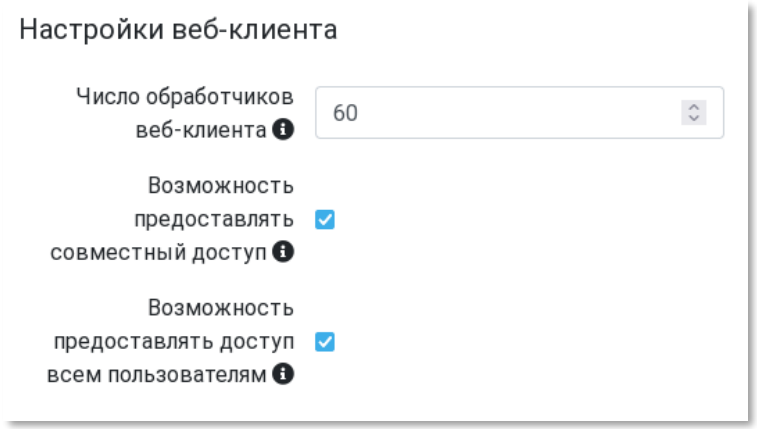
- На папке “Черновики” - меню “Очистить папку Черновики”.
- Возможность фиксировать размеры ячеек таблицы в письме.
- Сохранение позиции в списке сообщений при смене папок.
- Раскрытие списков рассылки в адресной строке письма.
- Снятие выделения в списке сообщений через Shift.
- Пользовательская сортировка папок – через меню папки.
- Удаление выбранных сообщений без помещения в корзину.

7.1.1. Настройка “Возможность предоставлять совместный доступ”

В версии 4.3.4 добавлена возможность полного запрета пользователям предоставлять доступ к своим данным (почте, календарям и адресным книгам) другим пользователям.

Для того, чтобы отключить возможность предоставления доступа другим пользователям, снимите переключатель “Возможность предоставлять совместный доступ” (вкладка “Почта” на странице “Общие настройки”).

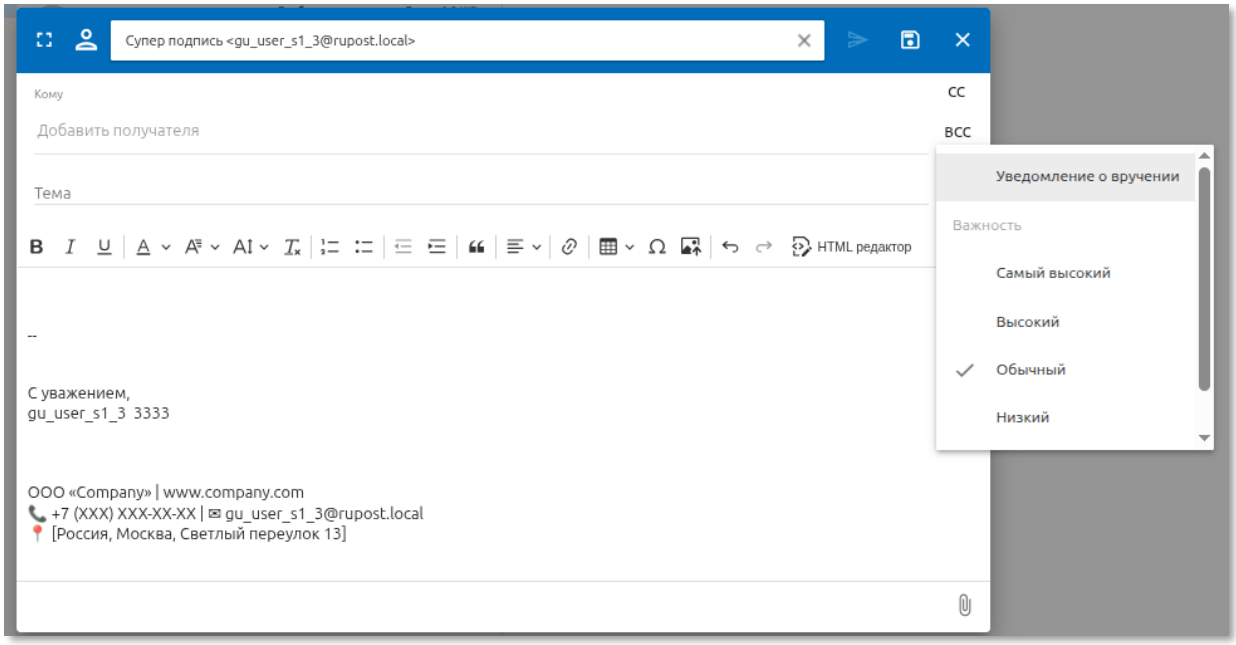
Параметр “Возможность предоставлять доступ всем пользователям”, в отличие от “Возможность предоставлять совместный доступ”, управляет только возможностью пользователя предоставить доступ к своим данным **всем** пользователям.



7.1.2. Уведомление о прочтении

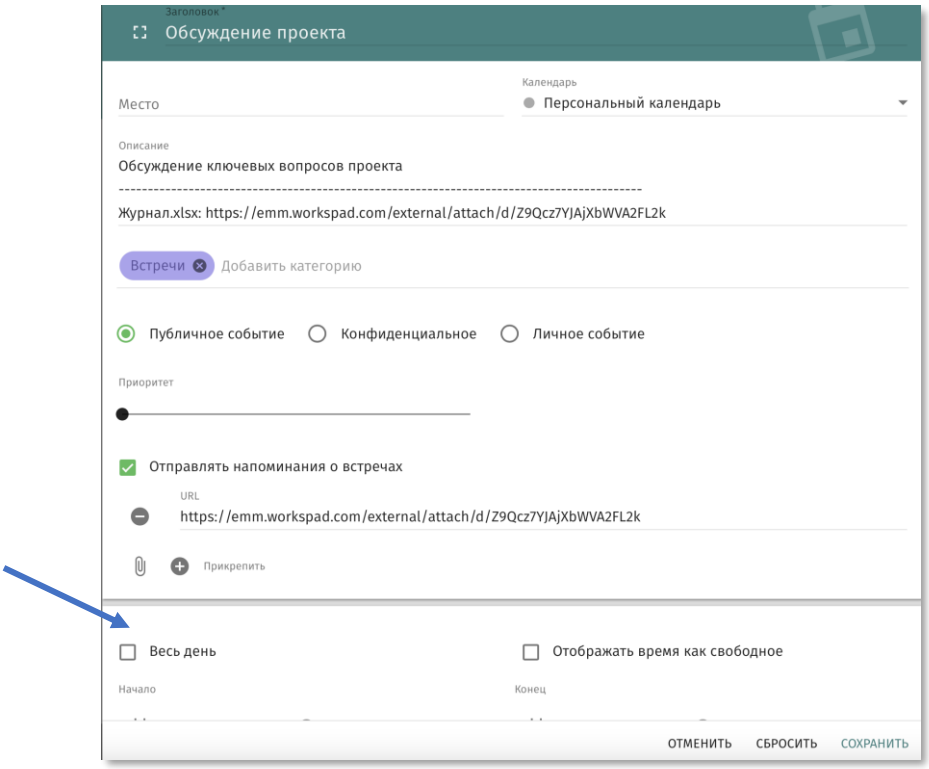
В версии 4.0 добавлена возможность запроса получения уведомления о прочтении письма.

Для этого, при отправке письма в веб-клиенте, выберите выпадающее меню настроек и установите переключатель “Уведомление о вручении”.



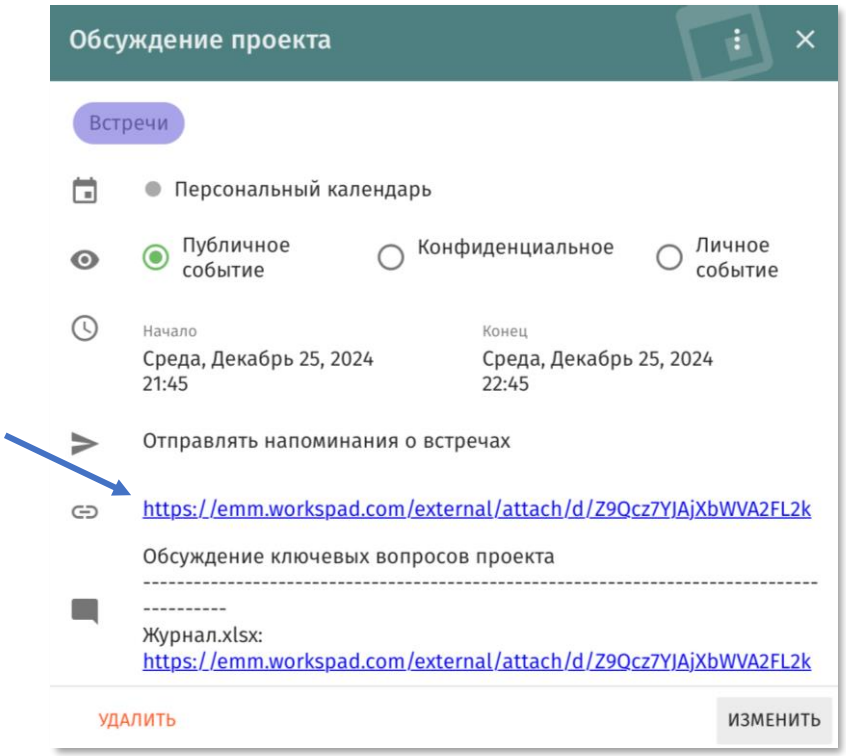
7.1.3. Вложения в календарные события

В версии 3.2.0 добавлена возможность добавлять вложения к календарным событиям в веб-клиенте.

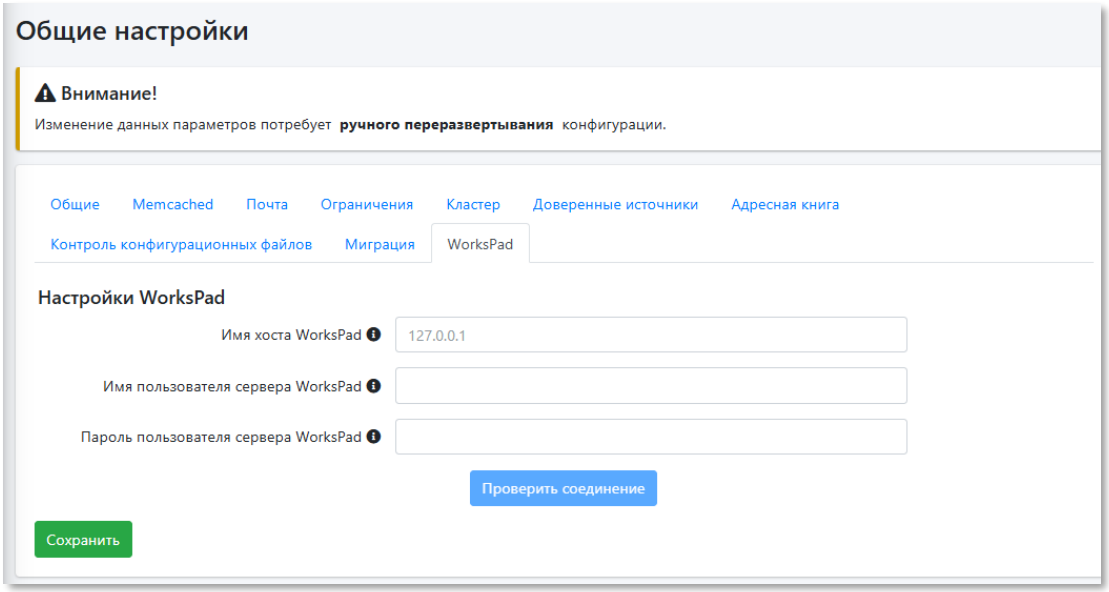


Для добавления вложения к календарному событию в веб-клиенте можно воспользоваться пунктом меню “Прикрепить”.

В свойствах события прикрепленный документ будет выглядеть как веб-ссылка на сервер WorksPad, содержащая идентификатор документа.



Так как файлы вложений сохраняются на сервере WorksPad, то данная функциональность доступна только при наличии установленного **WorksPad** сервера версии **6.3.20 и выше**. Настройка интеграции с WorksPad сервером находится на закладке “WorksPad” страницы “Общие настройки”



В версии 3.3.0 добавлена обработка входящих писем-приглашений, содержащих вложения.

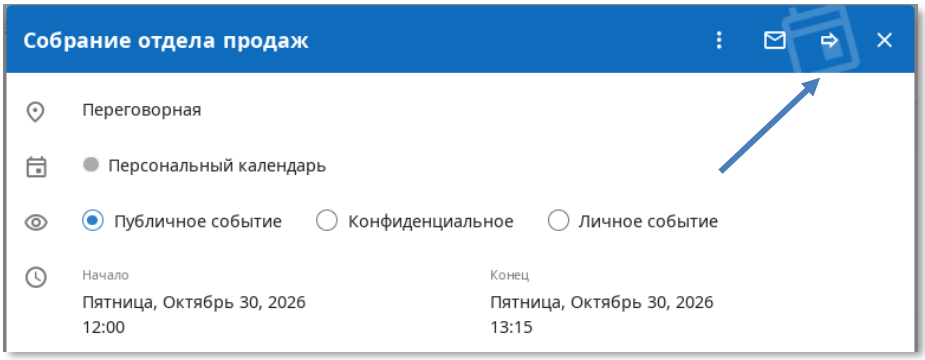
В процессе обработки такого письма-приглашения вложения сохраняются на сервере WorksPad с подготовкой ссылок для каждого вложения, затем ссылки добавляются в событие и, таким образом, вложения становятся доступны для просмотра из календарного события.

Если используется WorksPad сервер версии 7.0 и выше, то меняется формат указания его адреса – новый формат:

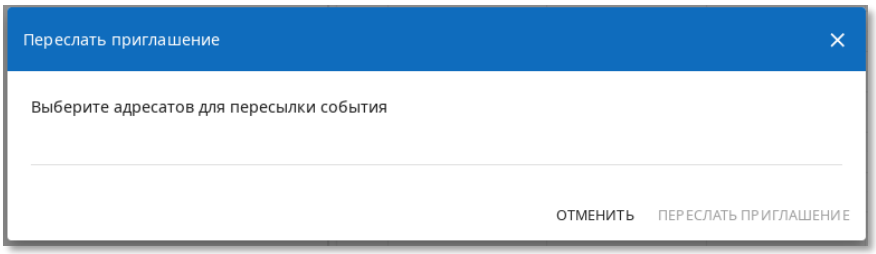
```
https://<WorksPadGateway>/rupostapi
```

7.1.4. Пересылка приглашения на событие

В версии 4.3.4 добавлена возможность пересылки приглашения на событие из карточки события.



При нажатии на кнопку “Переслать” появится окно выбора адресатов.



После добавления адресатов, нажмите кнопку “Отправить приглашение”. Приглашение будет отправлено, но изменения в календаре организатора и приглашенного адресата отобразятся только после того, как приглашение будет принято адресатом.

7.1.5. Поддержка аутентификации Kerberos и OpenID Connect для веб-клиента

Внимание!

В версии 4.3.4 добавлена прямая (без дополнительного Identity Provider) поддержка протокола Kerberos для веб-клиента – см. ниже раздел “Аутентификация пользователей веб-клиента по протоколу Kerberos”.

В версии 4.0 добавлена поддержка аутентификации OpenID Connect для работы со встроенным web-клиентом, что позволяет организовать для пользователей единый вход (SSO). В этом случае, проверка прав пользователей производится без дополнительного ввода данных для аутентификации (логин, пароль). Наличие поддержки OpenID Connect позволяет, также, поддержать аутентификацию по протоколу Kerberos (с установкой дополнительного Identity Provider).

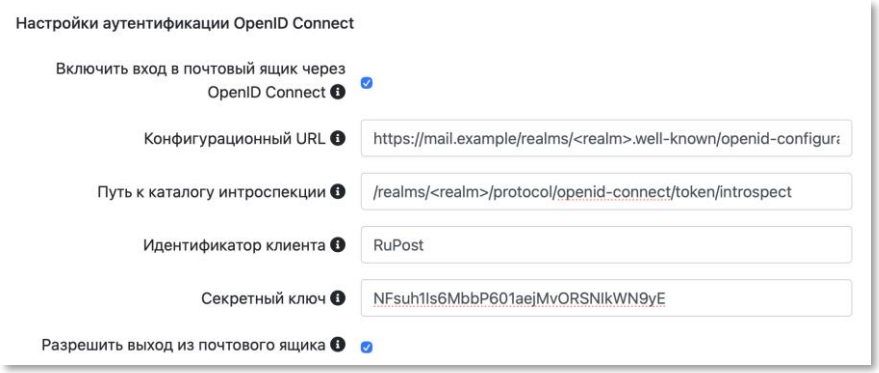
Требования для работы OpenID-аутентификации

- Синхронизация времени (NTP) между всеми узлами и OpenID-провайдером — расхождение более 30 секунд приведёт к отказу в аутентификации.
- Корректное DNS разрешение всех FQDN OpenID-провайдера и сервисов, участвующих в аутентификации (например, через правильно настроенный DNS или /etc/resolv.conf).
- Наличие действительных SSL-сертификатов.

Включение OpenID Connect

Перед включением OpenID Connect необходимо зарегистрировать почтовую систему как клиента в IdP (OpenID-провайдере), чтобы получить client ID, secret и задать корректный redirect URI.

1. В панели управления откройте раздел «Общие настройки» → вкладку «Аутентификация».
2. Установите флажок «Включить вход в почтовый ящик через OpenID Connect».
3. Укажите URL автоконфигурации, содержащий сведения о провайдере OpenID.
4. Укажите путь к endpoint’у интроспекции токенов (token/introspect).
5. Задайте идентификатор клиента и секретный ключ, полученные при регистрации клиента у провайдера OpenID Connect.



Далее необходимо настроить браузеры пользователей для использования OpenID Connect. Это можно сделать при помощи соответствующих доменных групповых политик, либо вручную.

Для Microsoft Edge и браузеров на базе Chromium

1. Добавьте адрес IdP в список сайтов. Для этого, откройте Панель управления → Свойства браузера → Безопасность → Местная интрасеть → Сайты → Дополнительно.
   Добавьте адрес IdP (например, https://auth.example.com) в список.
2. Перейдите в раздел «Свойства браузера» → «Дополнительно» → «Безопасность» и установите флажок «Разрешить встроенную проверку подлинности Windows».

Для Mozilla Firefox

1. В адресной строке введите: about:config.
2. Найдите и задайте параметры:
   - network.negotiate-auth.trusted-uris
   - network.negotiate-auth.delegation-uris
   - network.automatic-ntlm-auth.trusted-uris

   Добавьте в значения адрес IdP (например, auth.example.com).

7.1.5.1. *Настройка Kerberos-провайдера в Keycloak*

Встроенный веб-клиент поддерживает только OpenID Connect аутентификацию, поэтому, для поддержки протокола Kerberos необходимо осуществить “стыковку” протокола Kerberos и OpenID Connect. Для этой цели необходимо установить дополнительный Identity Provider, например, Keycloak.

1. В панели управления Keycloak откройте раздел User Federation.
2. Добавьте новый источник типа Kerberos.
3. Укажите параметры подключения к вашему домену и путь к keytab-файлу, содержащему необходимые SPN-записи (регистр важен), например:
   `HTTP/mail.rupost.ru@RUPOST.LOCAL`
4. Убедитесь, что указанный keytab-файл доступен пользователю Keycloak и имеет корректные права доступа.

Keytab-файл — это файл, содержащий долгосрочные ключи для одного или нескольких субъектов (principal) системы Kerberos. Он создаётся администратором LDAP/AD-сервера и содержит SPN-записи, используемые для проверки подлинности сервисов.

Требования к регистрации пользователей

Пользователь, проходящий Kerberos-аутентификацию, должен быть зарегистрирован в системе Keycloak. Его адрес электронной почты (email) должен соответствовать основному адресу пользователя в RuPost и иметь статус Verified.

Настройка потока аутентификации (Flows)

1. Перейдите в раздел Authentication → Flows.
2. Создайте дубликат стандартного потока browser с именем, например, RuPost.
3. В новом потоке переместите Kerberos на первое место.
4. Установите для него параметр Requirement в значение Alternative. Это позволит использовать Kerberos при наличии билета, а при его отсутствии — переходить к стандартной OpenID-аутентификации.

Создание клиента в Keycloak

1. В разделе Clients создайте новый клиент (или используйте существующий).
2. В поле Client ID укажите идентификатор, который будет использоваться в настройках панели управления RuPost.
3. В поле Valid redirect URIs добавьте адрес web-клиента, например: `https://mail.rupost.ru/SOGo/*`
4. На вкладке Settings (Capability config) включите:
   - Client authentication — On
   - Authorization — On
5. В блоке Authentication flow отметьте:
   - Standard flow
   - Direct access grants
   - OAuth 2.0 Device Authorization Grant
   - OIDC CIBA Grant
   - Standard Token Exchange
6. После сохранения клиента перейдите на вкладку Credentials и скопируйте значение Client Secret. Этот секрет указывается в панели управления RuPost при включении аутентификации через OpenID Connect.

Настройка аутентификации встроенного почтового веб-клиента по протоколу Kerberos завершена.

7.1.6. Аутентификация пользователей веб-клиента по протоколу Kerberos

В версии 4.3.4 добавлена возможность аутентификации пользователей веб-клиента RuPost по протоколу Kerberos. Применение Kerberos позволяет реализовать единый вход (SSO) для пользователей веб-клиента, не требующий ввода пароля при доступе к электронной почте, календарям и адресным книгам.

При реализации аутентификации Kerberos было уделено внимание поддержке смешанных схем аутентификации – когда часть пользователей входят с использованием Kerberos (обычно, с устройств, находящихся в домене), а часть, по-прежнему, имеют возможность входить по логину / паролю.

Если в организации используется несколько LDAP доменов, Kerberos аутентификация может быть включена только для части доменов LDAP. Пользователи, с учетными записями, находящимися в тех доменах LDAP, где Kerberos не включен, смогут получать доступ к сервисам RuPost как и ранее – по логину / паролю.

Протокол Kerberos основан на обмене криптографическими ключами (билетами) между клиентским приложением (браузером), контроллером домена LDAP (KDC) и сервером, предоставляющим сервис. Для проверки корректности билета Kerberos, сервер должен иметь возможность декодировать информацию, содержащуюся в билете. Для этого, сервер должен получить от контроллера домена LDAP настройки своего сервиса, а также ключи для декодирования и верификации данных билета. Такая информация передается администратором вручную в виде файла специального формата – так называемого keytab-файла.

Формирование keytab-файла для различных типов контроллеров LDAP подробно описано в Приложении – “Настройка инфраструктуры Kerberos”.

7.1.6.1. *Требования для работы аутентификации Kerberos*

Аутентификация Kerberos выполняется при помощи программного интерфейса безопасности GSSAPI и протокола SPNEGO, что требует взаимодействия клиента, сервера и центра распределения ключей (KDC, эту роль может выполнять контроллера домена).

Соответственно, требования для работы Kerberos протокола следующие:

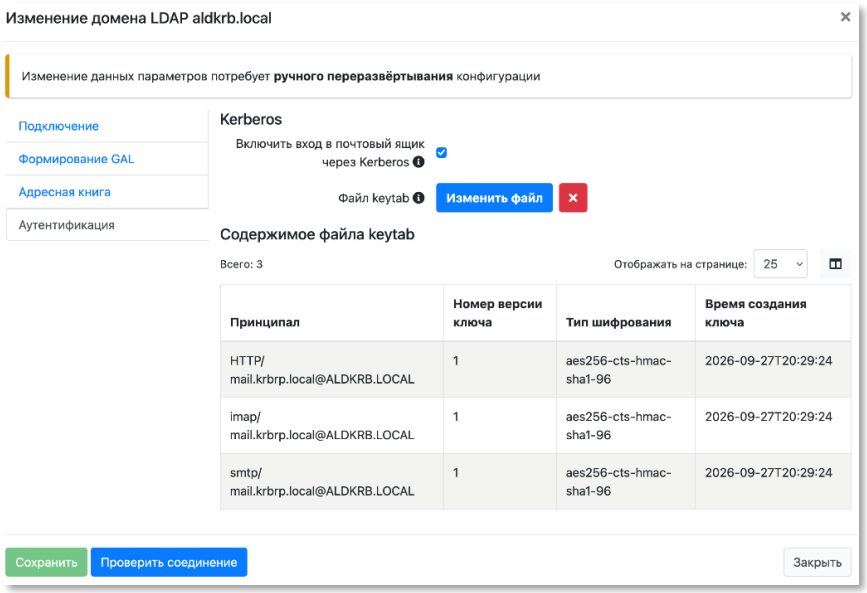
1. Между клиентскими устройствами, узлами RuPost и KDC должна быть обеспечена сетевая связность. Для взаимодействия с KDC должен быть разрешён сетевой трафик по TCP/UDP на порт 88.
2. На стороне клиентов и узлов RuPost должно обеспечиваться разрешение доменных имён, включая обнаружение KDC и узлов RuPost. При использовании автоматического обнаружения KDC должны быть настроены соответствующие DNS SRV-записи.
3. Время на клиентских устройствах, узлах RuPost и контроллерах домена должно быть синхронизировано. Допустимое расхождение времени определяется настройками Kerberos и действующими политиками безопасности домена. По умолчанию в распространённых реализациях Kerberos допустимое расхождение составляет 5 минут, однако данное значение может быть изменено администратором.
4. Клиентские устройства должны иметь корректную конфигурацию Kerberos, обеспечивающую определение используемых Realm и соответствующих KDC.
5. Пользователи должны иметь действующие учётные записи в Kerberos Realm.
6. Для сервиса HTTP в инфраструктуре Kerberos должны быть зарегистрированы необходимые сервисные принципалы (SPN).
7. На узлах RuPost должны быть размещены keytab-файлы, содержащие ключи соответствующих сервисных принципалов.

При использовании нескольких Kerberos Realm должны быть обеспечены необходимые доверительные отношения и маршрутизация аутентификации между ними - в случае, если пользователи одного Realm обращаются к сервисам другого Realm.

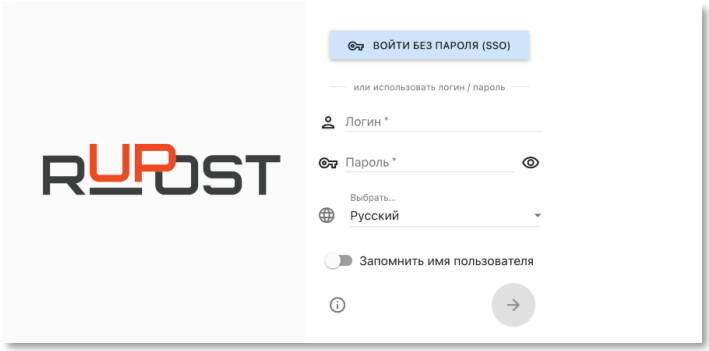
7.1.6.2. *Настройки Kerberos в Панели управления*

Использование Kerberos включается в настройках LDAP домена:

1. На странице “Домены LDAP” нажать имя нужного домена LDAP, чтобы открыть его настройки.
2. В окне “Изменение домена LDAP” открыть вкладку “Аутентификация”.
3. В блоке “Kerberos” установите переключатель “Включить вход в почтовый ящик через Kerberos“.
4. В поле “Файл keytab” выбрать подготовленный файл .keytab.
5. Нажать «Сохранить».
6. Затем применить изменения, развернув конфигурацию.



После включения Kerberos, окно входа в веб-клиент позволит пользователю выбрать метод входа:



При нажатии на кнопку “Войти без пароля” будет осуществлен вход с использованием билета Kerberos.

7.2. Совместимые настольные почтовые клиенты

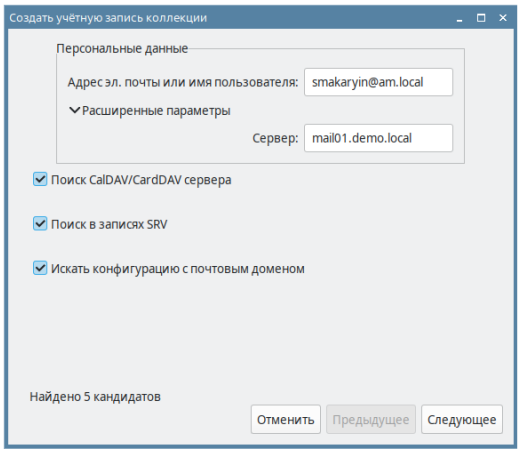
7.2.1. Клиенты на базе Thunderbird

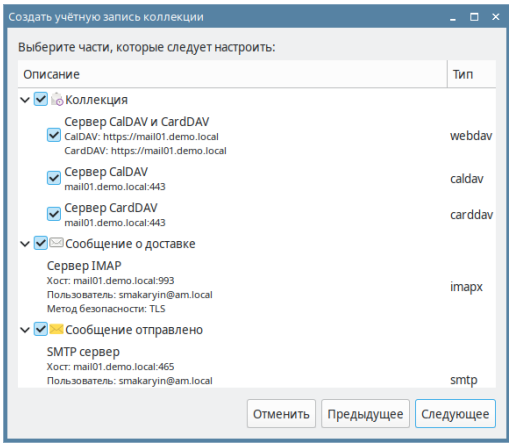
Автоконфигурация клиентского подключения почты, календарей, контактов и корпоративной адресной книги доступна для клиентов на базе Thunderbird (например, RuPost Desktop Personal) начиная с версии 91. Для корректной работы автоконфигурации необходимо указание соответствующих значений CNAME и SRV в записи DNS (см. “*Руководство по установке и конфигурированию*”, раздел 2.8).

7.2.2. Evolution

Автоконфигурация клиентского подключения почты, календарей, контактов и корпоративной адресной книги доступна для Evolution начиная с версии 44. Для корректной работы автоконфигурации необходимо указание соответствующих значений CNAME и SRV в записи DNS (см. “*Руководство по установке и конфигурированию*”, раздел 2.8).

При настройке клиентских приложений необходимо кроме подключения почтовой учетной записи также **создать учетную запись коллекции**, отвечающую за подключение календарей, задач, контактов и корпоративных адресных книг.





7.2.3. Microsoft Outlook

Автоконфигурация Outlook (2013 и выше) в настоящее время доступна только для клиентского подключения почты на базе штатных механизмов autodiscovery для протокола IMAP. Подключение календарей, контактов и корпоративной адресной книги в Outlook возможны при установке специального дополнения (плагина) RuPost, обеспечивающего поддержку необходимых для этого версий протоколов CalDAV и CardDAV почтовой системы RuPost с учетом ее особенностей и расширений.

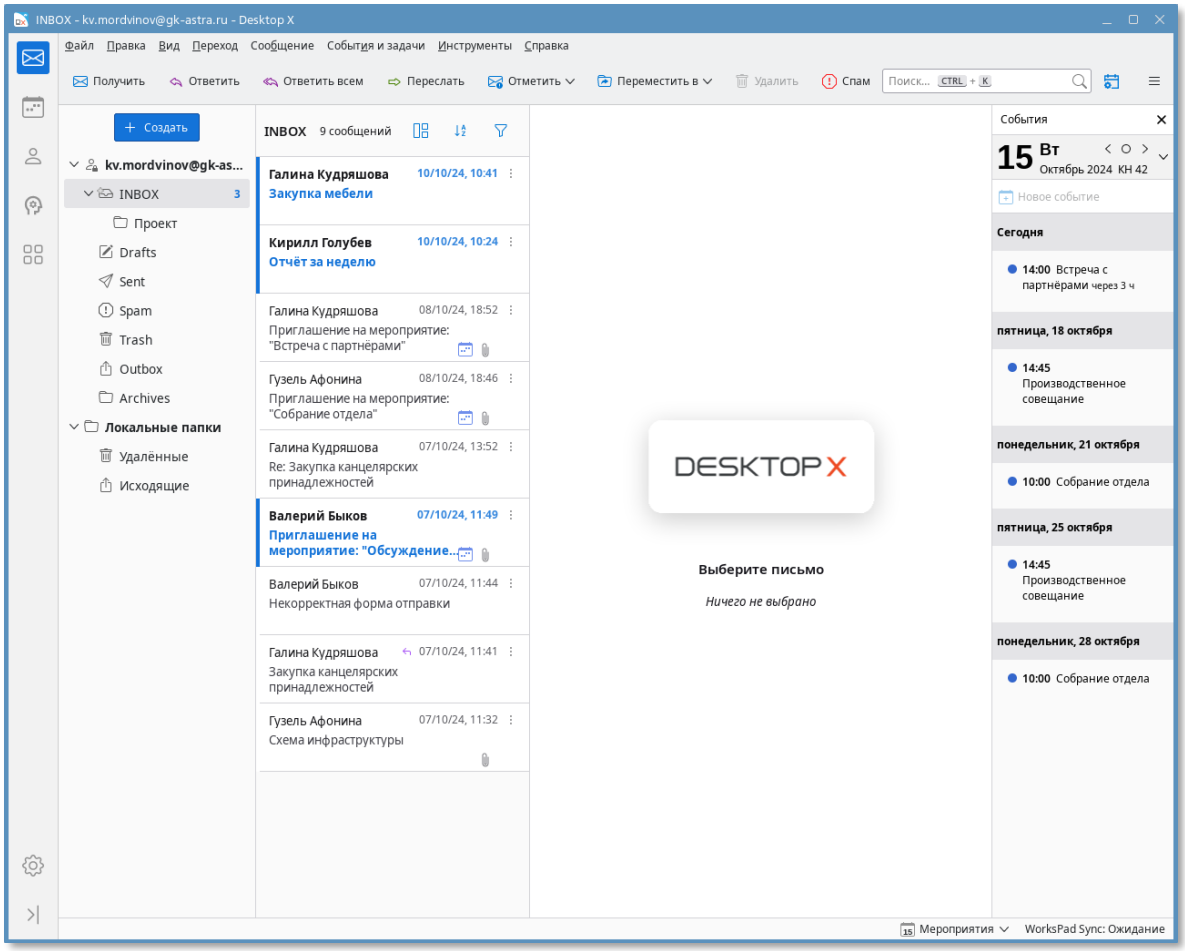
Плагин RuPost для Outlook автоматически подключает календари, контакты и т.п. для заведенных и подключенных к серверу RuPost учетных записей IMAP. Плагин поддерживает календари пользователя и календари других пользователей, подключенные с соответствующими правами в web-клиенте RuPost.

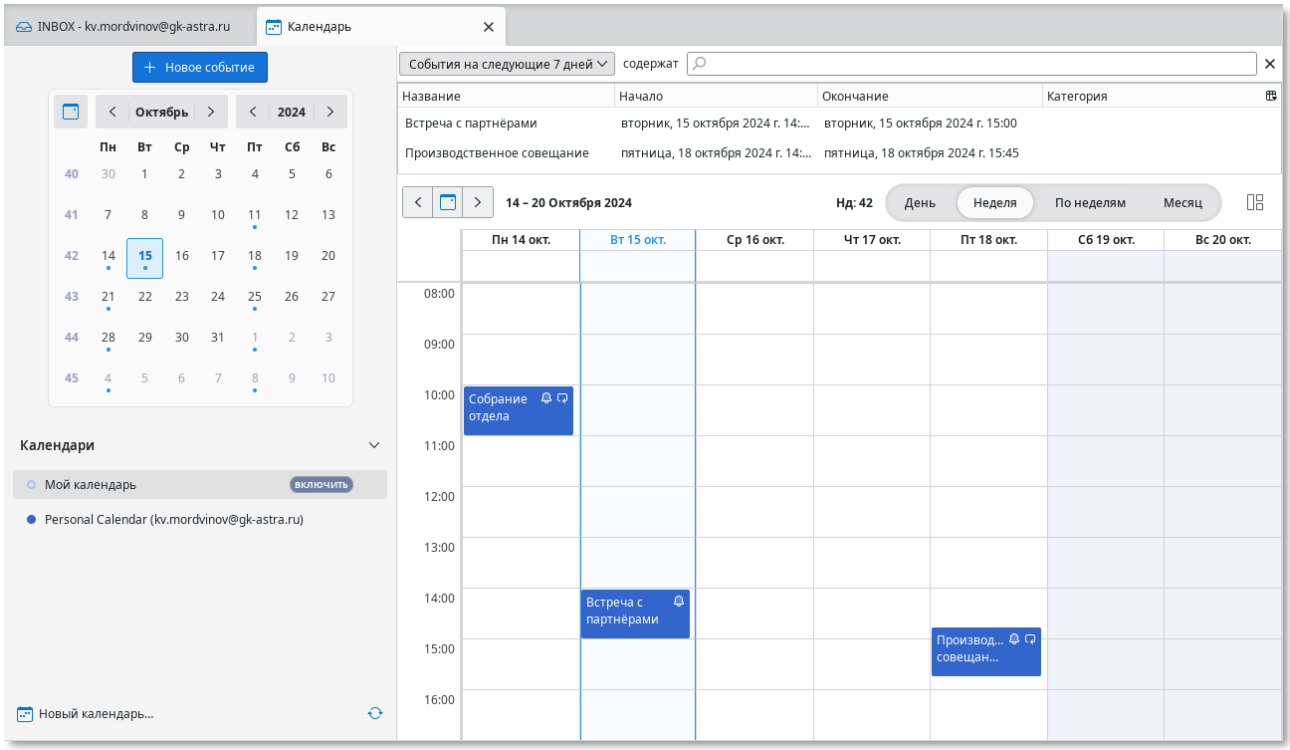
Для корректной работы автоконфигурации необходимо указание соответствующих значений CNAME и SRV в записи DNS (см. “*Руководство по установке и конфигурированию*”, раздел 2.8).

7.3. Настольный клиент Desktop X

Desktop X это кроссплатформенный почтовый клиент (Windows, ALSE 1.7.x, 1.8.x) в знакомом UX/UI стиле “Outlook New”, который обеспечивает работу с электронной почтой, календарями, адресными книгами и сервисами организации. Для работы Desktop X необходимо наличие сервера управления с которым он взаимодействует с помощью собственного протокола.

Desktop X позволяет интегрироваться с рабочими мессенджерами, ВКС, CRM, микро приложениями WorksPad Assistant и другими информационными системами предприятия. Благодаря работе с сервером управления с использованием собственного протокола, обеспечивается высокий уровень корпоративного контроля и возможность гибкой настройки доступа к ресурсам организации, а также ограничение добавления в Desktop X публичных почтовых ящиков, работающих по открытым протоколам.





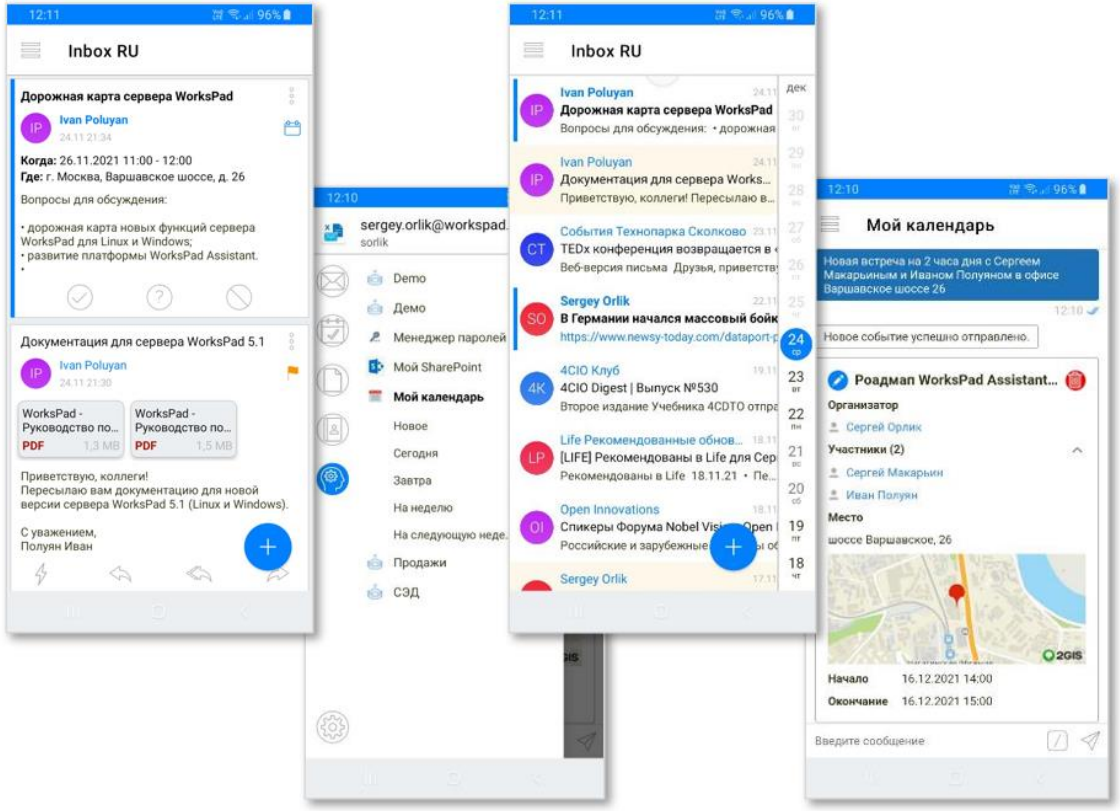
- Работа с почтой, календарями, большими адресными книгами через сервер управления по собственному протоколу
- Гибкая возможность интеграции корп. сервисов (CRM, ВКС, Мессенджеры и т.д.)
- Отсутствие необходимости использования VPN для доступа к корпоративным сервисам
- Контроль доступа и применение серверных политик к клиенту
- Удобный интерфейс в стиле Microsoft Outlook
- Позволяет работать со всеми популярными корпоративными почтовыми системами через сервер управления
- Работает на Astra Linux и Windows и т.д.

Решение Desktop X приобретается и поставляется отдельно.

Автоконфигурирование Desktop X происходит в момент подключения к серверу управления.

7.4. Мобильный клиент WorksPad

Для обеспечения контролируемой работы с системой электронной почты с личных и корпоративных мобильных устройств Android и iOS необходимо использовать другое решение компании “РуПост” – мобильное рабочее место WorksPad с клиентскими приложениями нового поколения WorksPad X. Решение WorksPad приобретается и поставляется отдельно.

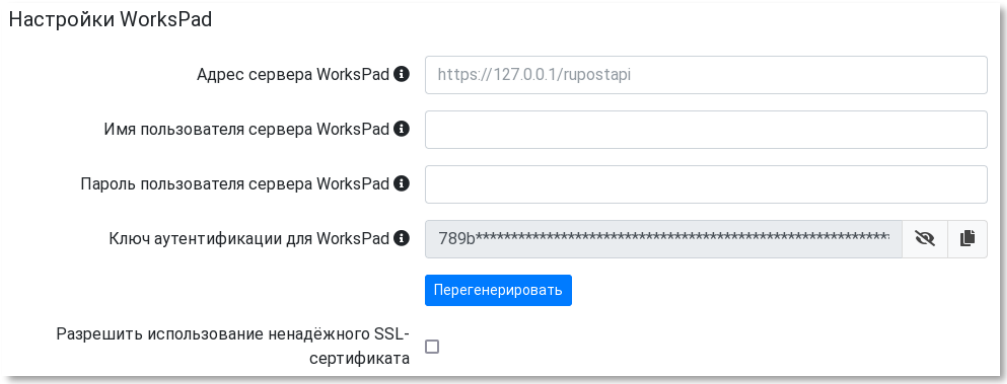


Настройка сервера WorksPad для работы с RuPost описана в соответствующих руководствах WorksPad.

7.4.1. Создание ключа для интеграции с WorksPad сервером

В версии 4.3.4 добавлена возможность изменения аутентификационного ключа, который позволяет WorksPad серверу вызывать API RuPost.

Для изменения значения ключа, перейдите на вкладку “WorksPad” на странице “Общие настройки” и нажмите кнопку “Перегенерировать” – значение ключа изменится и отобразится в поле “Ключ аутентификации для WorksPad”.



Для корректной работы, ключи на сервере RuPost и сервере WorksPad должны быть идентичны, поэтому, после изменения значения ключа, новый ключ необходимо скопировать и добавить в настройки сервера WorksPad.

8. Дополнительные комментарии

Почтовая система RuPost активно развивается и функционально расширяется. Руководства по продукту отражают ключевые аспекты применения конкретной версии продукта, но может не освещать те или иные нюансы использования системы – всегда используйте актуальную версию документации, соответствующую применяемой версии RuPost. В случае возникновения вопросов – обращайтесь в службу технической поддержки.

Внимание!

При написании пользовательских шаблонов, например, для собственных транспортных правил postfix, файлы с этими правилами (согласно общедоступных инструкций) размещаются в /etc/postfix, однако при проведении обновления Rupost данный каталог перезаписывается и сторонние файлы становятся недоступны.

Во избежание потерь при обновлении данные файлы должны либо генерироваться в рамках пользовательского шаблона, либо быть скопированы, либо храниться вне системных каталогов компонентов.

© 2021-2026 РуПост

9. Приложение 1 – Шаблон “Интеграция RuPost с внешним релей сервером”

Сервер RuPost может маршрутизировать исходящую почту через внешний Релей-сервер (SMTP-relay) для пересылки почтовых сообщений внешним адресатам, либо внутренним, которые обслуживаются другой системой электронной почты организации.

9.1. Сценарии использования

Эта функция может быть полезна:

- для отправки корреспонденции другому почтовому серверу, который обслуживает почтовые ящики доменов, отсутствующих на данном узле RuPost;
- при запуске разделенного почтового домена во время миграции, когда нужно направить всю исходящую почту через почтовый узел вашего поставщика услуг связи;
- по какой-либо причине требуется отправить всю почту через другой почтовый сервер, который используется в качестве ретранслятора электронной почты.



9.2. Требования к инфраструктуре

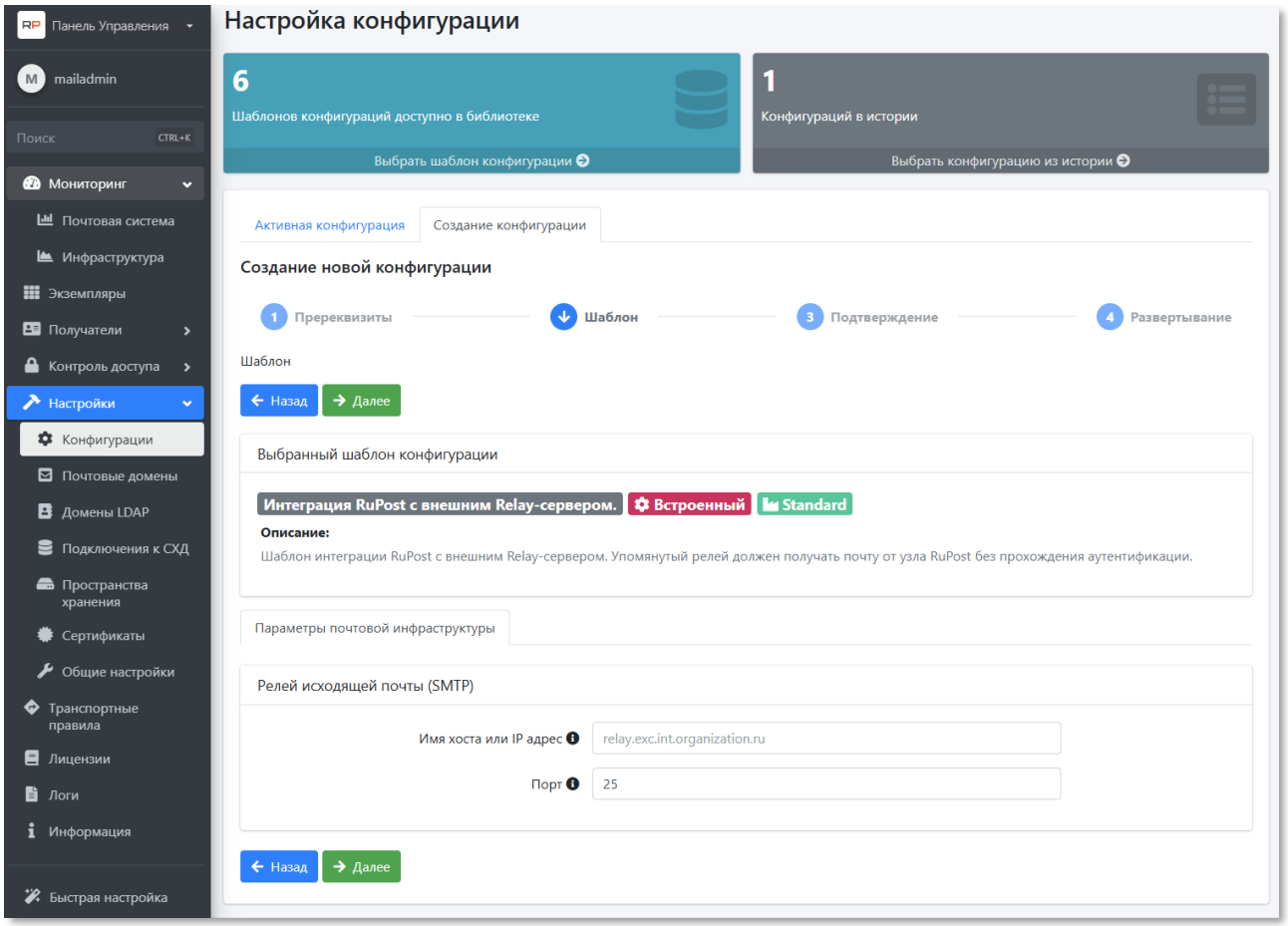
Для применения шаблона интеграции RuPost с Релей-сервером необходимо настроить следующие элементы инфраструктуры:

- сервер RuPost;
- используется база данных RuPost, созданная в СУБД PostgreSQL;
- применяется локально установленное программное обеспечение HAProxy;
- релей-сервер должен получать почту от узла RuPost без прохождения проверки.

9.3. Подключение шаблона

- В веб-интерфейсе панели управления RuPost перейти в пункт меню “Конфигурация”.
- Выбрать шаблон конфигурации “Интеграция RuPost с внешним Relay-сервером”.

© 2021-2026 РуПост



- Во вкладке “**Параметры хостов почтовой инфраструктуры**” заполнить следующие поля:

Релей исходящей почты (SMTP):

- - “Имя хоста или IP адрес” - имя хоста или IP адрес relay сервера исходящей почты. Указанный relay должен быть настроен на получение входящей корреспонденции от анонимных пользователей из подсети, в которой расположен узел (кластер) RuPost.
- - “Порт” - Порт relay сервера исходящей почты.

  После заполнения всех полей шаблона, в веб интерфейсе Панели Управления развернуть эту почтовую конфигурацию.

10. Приложение 2 – Шаблон “Интеграция RuPost с Microsoft Exchange”

Почтовая система RuPost позволяет сосуществование с Microsoft Exchange Server, использующих один и тот же почтовый домен, посредствам применения специального шаблона конфигурации. Транспортировка внешней почтовой корреспонденции осуществляется через Релей-сервер.

Внимание!

Шаблон доступен для развертывания только при наличии лицензии редакции Enterprise.

Внимание!

На время сосуществования двух почтовых систем, при необходимости создания новых почтовых ящиков в RuPost рекомендуется следующий порядок действий:

1. Создаем новый почтовый ящик в Microsoft Exchange;

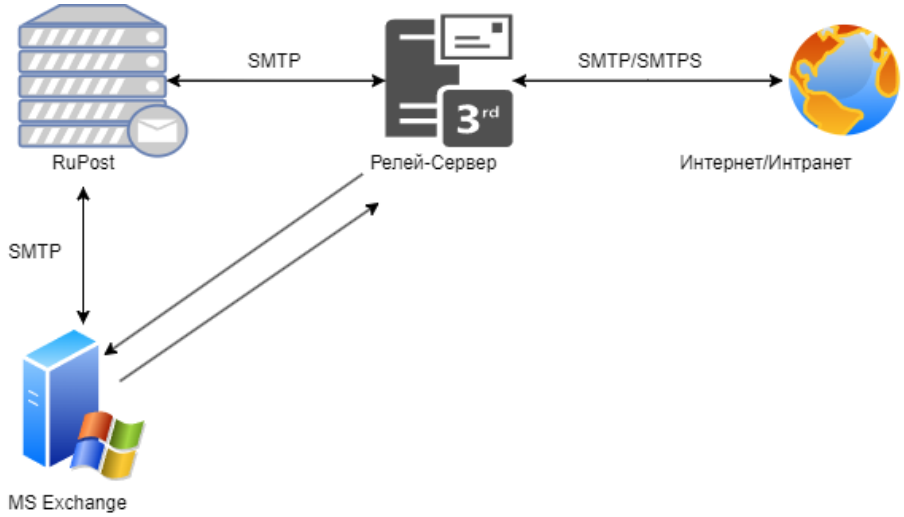
2. Мигрируем только что созданный ящик в RuPost используя **RuPost Migration Tool.**

Такая последовательность действий гарантирует создание правильных записей о созданном ящике на сервере Microsoft Exchange (даже если ящик планируется расположить на сервере RuPost).

10.1. Сценарии использования

Этот шаблон может быть полезен:

- для отправки корреспонденции почтовому серверу Microsoft Exchange, который обслуживает почтовые ящики доменов, отсутствующих на данном узле RuPost;
- при запуске разделенного почтового домена во время миграции, когда нужно направить всю исходящую почту через почтовый узел вашего поставщика услуг связи(релей-сервер);



10.2. Требования к инфраструктуре

Для применения шаблона интеграции RuPost с Microsoft Exchange Server необходимо наличие следующих элементов инфраструктуры:

- RuPost с лицензией редакции продукта Enterprise;
- используется база данных RuPost, созданная в СУБД PostgreSQL;
- применяется локально установленное программное обеспечение HAProxy;
- в Microsoft Exchange необходимо настроить Receive Connector с разрешением на получение входящих писем от анонимных пользователей от узла RuPost. В свою очередь, RuPost регистрируется в Exchange как Send Connector типа Smart Host.
- Топология предполагает наличие релей-сервиса, через который RuPost будет отправлять корреспонденцию пользователям внешних почтовых доменов. Упомянутый релей должен получать почту от узла RuPost без прохождения проверки. Если в организации отсутствует внешний релей-сервер, в этом случае нужно настроить Microsoft Exchange в виде релей-сервиса для сервера RuPost.

10.3. Подключение шаблона

1. Выбор шаблона конфигурации:

   - В веб-интерфейсе панели управления RuPost перейти в пункт меню “Конфигурация”.

     Пример: *https://localhost:5000/admin/redeploy*

   - Выбрать шаблон конфигурации “Интеграция RuPost с Microsoft Exchange”.

2. Настройка конфигурации шаблона:

   Во вкладке “**Параметры хостов почтовой инфраструктуры**” заполнить следующие поля:

   Сервер Exchange (receive connector):

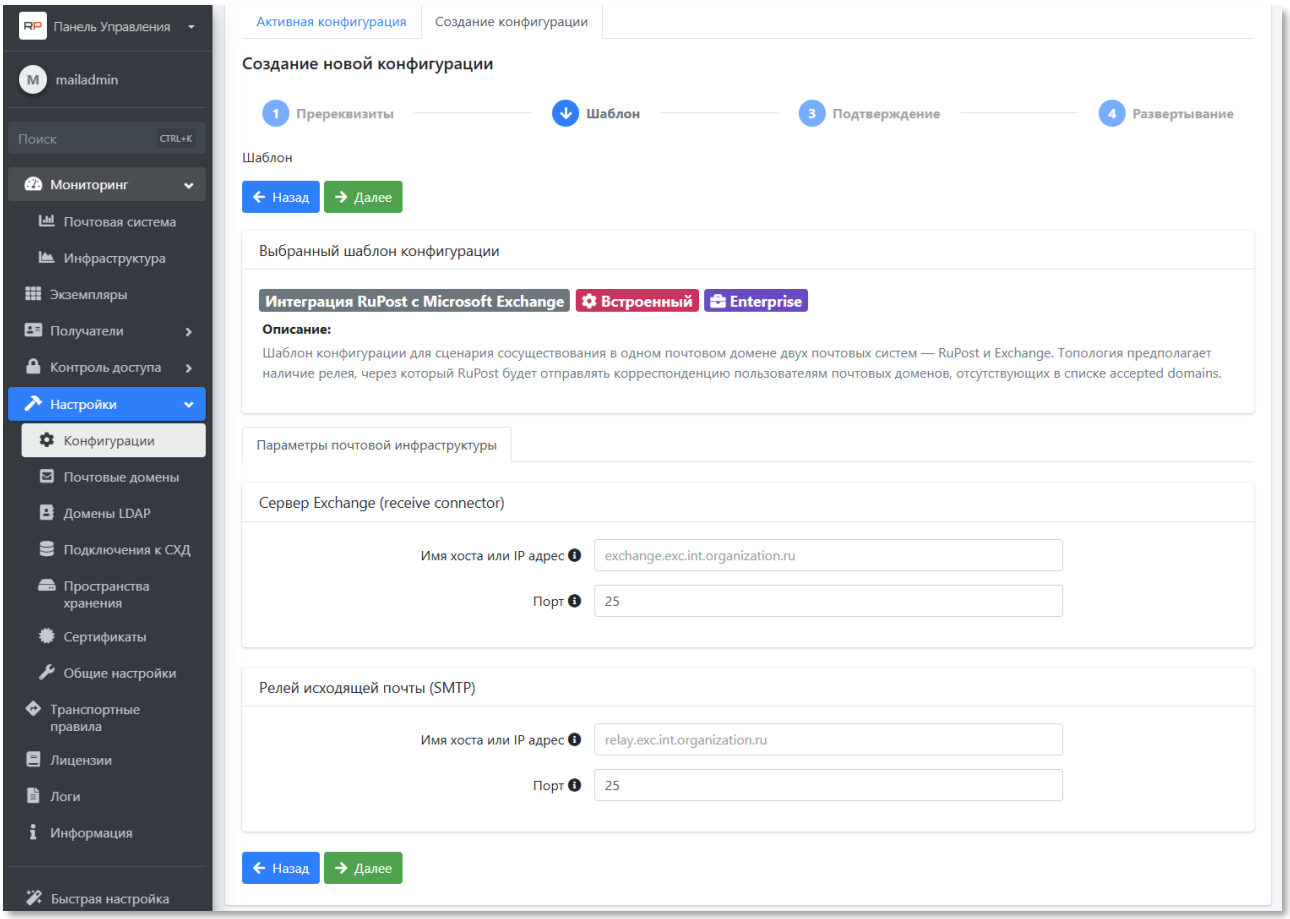
   - “Имя хоста или IP адрес” - имя хоста или IP сервера Exchange, на котором настроен receive connector с разрешением на получение входящей корреспонденции от анонимных пользователей.

   - “Порт” - Порт сервера Exchange, на котором настроен receive connector.

   Релей исходящей почты (SMTP):

   - “Имя хоста или IP адрес” - имя хоста или IP адрес relay сервера исходящей почты. Указанный relay должен быть настроен на получение входящей корреспонденции от анонимных пользователей из подсети, в которой расположен узел (кластер) RuPost.

   - “Порт” - Порт relay сервера исходящей почты.



3. После заполнения всех полей шаблона, в веб интерфейсе Панели Управления развернуть эту почтовую конфигурацию.

11. Приложение 3 – Шаблоны интеграции с Kaspersky и Dr. Web

Почтовая система RuPost позволяет использовать продукты “Kaspersky Security для Linux Mail Server” и “Anti-virus Dr.Web for UNIX mail servers”, обеспечивающие защиту от вредоносного ПО и спама, а также фильтрацию контента.

Интеграция RuPost с данным ПО происходит путем взаимодействия систем по протоколу Milter.

Milter - это краткое название Content Management API. Оно также относится к программному обеспечению, написанному с использованием этого API. Milter предоставляет подключаемый интерфейс для стороннего программного обеспечения для проверки, изменения или блокирования сообщений по мере их прохождения через MTA. Milters могут обрабатывать информацию о соединении (IP) сообщения, элементы протокола конверта, заголовки сообщения и / или содержимое тела сообщения, а также изменять получателей, заголовки и тело сообщения.

Дополнительную информацию об используемых продуктах можно получить по ссылкам:

https://support.kaspersky.com/KLMS/8.2/ru-RU/43931.htm

https://download.geo.drweb.com/pub/drweb/unix/doc/HTML/MailD/ru/integration_mail_postfix_setup_milter.html

11.1. Сценарии использования

Возможные варианты использования фильтров ПО “Kaspersky Security для Linux Mail Server” и “Anti-virus Dr.Web for UNIX mail servers”, включают в себя отклонение нежелательной почты, фильтрацию вирусов и контроль содержимого почтовой корреспонденции.

11.2. Требования к инфраструктуре

Для применения шаблонов интеграции RuPost с “Kaspersky Security для Linux Mail Server” и “Anti-virus Dr.Web for UNIX mail servers” необходимо выполнить следующие требования для элементов инфраструктуры:

- Сервер RuPost;
- используется база данных RuPost, созданная в СУБД PostgreSQL;
- Доступность по сети для узлов RuPost установленного ПО “Kaspersky Security для Linux Mail Server” или “Anti-virus Dr.Web for UNIX mail servers” (возможно их вариаций, работающих по протоколу Milter).

11.3. Подключение шаблона

1. Выбор шаблона конфигурации

   - В веб-интерфейсе панели управления RuPost перейти в пункт меню “Конфигурация”.

     Пример: *https://localhost:5000/admin/redeploy*

- Выбрать стандартный шаблон конфигурации “Базовый шаблон конфигурации + Kaspersky” или “Базовый шаблон конфигурации + Dr.Web” (в зависимости от используемого продукта).

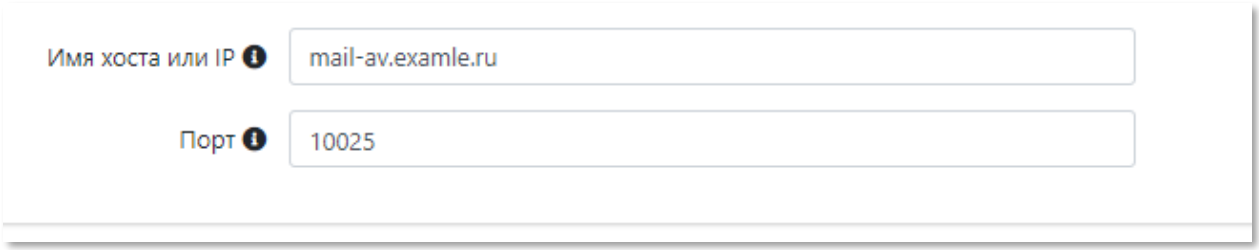
2. Настройка конфигурации шаблона

   Во вкладке “**Параметры хостов почтовой инфраструктуры**” заполнить следующие поля:

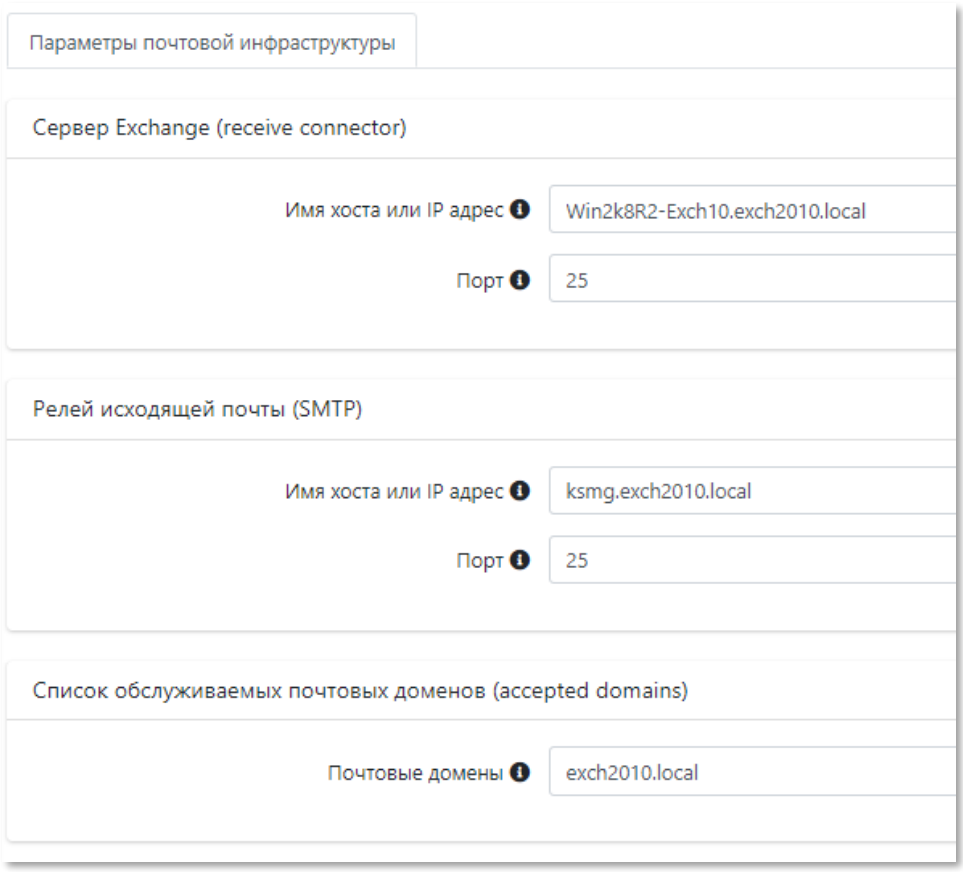
   - “Имя хоста или IP адрес” - имя хоста или IP сервера фильтрации почтовых объектов по протоколу Milter

   - “Порт” - Порт сервера фильтрации почтовой корреспонденции по протоколу Milter

   Пример:



3. После заполнения всех полей шаблона, в веб интерфейсе Панели Управления развернуть эту почтовую конфигурацию



12. Приложение 4 – Пример скриптов интеграции с СХД для работы с SDS Linstor

Программно-определяемое хранилище системы хранения данных (СХД) развернуто на двух группах узлов. Первая группа состоит из 4 узлов, вторая группа состоит из 3 узлов. Каждая группа и представляет собой отдельное хранилище. Сетевая инфраструктура представляет собой два независимых сегмента (сети). Первый сегмент предназначен для управления (1 Гбит/с), второй сегмент (10 Гбит/с) используется для передачи данных. Наименования узлов и их ресурсы представлены в таблице.

СХД 1				
Наименование узла		Сеть управления IP адрес	Сеть передачи данных IP адрес	Шлюз NFS ресурса IP адрес
1	astra-1	10.177.161.51	10.177.60.1	10.177.60.227
2	astra-2	10.177.161.52	10.177.60.2	
3	astra-3	10.177.161.53	10.177.60.3	
4	astra-4	10.177.161.54	10.177.60.4	
СХД 2				
Наименование узла		Сеть управления IP адрес	Сеть передачи данных IP адрес	Шлюз NFS ресурса IP адрес
1	linstor-1	10.177.161.190	10.177.60.220	10.177.60.230
2	linstor-2	10.177.161.191	10.177.60.221	
3	linstor-3	10.177.161.192	10.177.60.222	

Представленные примеры скриптов выполняют:

- создание снимка и копии почтового хранилища на СХД 1 (скрип 1),
- передачу его на СХД 2 (скрипт 2),
- развертывание на СХД 2 и выдачу через NFS шлюз (скрипт 3).

Скрипт 1 выполняет следующие шаги:

- блокировка на запись файловой системы на СХД 1 для обеспечения создания консистентного снимка;
- выполнение снимка файловой системы;
- снятие блокировки на запись файловой системы;
- создание копии файловой системы.

© 2021-2026 РуПост

Пример скрипта 1

```
#!/bin/sh
#
echo ""
echo "Step 1 Create Snapshot and Compressed Copy of MailDir "
echo ""
#
snapshotsds1="/dev/astra-4-vg/mysnap"
mdcopysds1="/mnt/vdd/syncer/backups/full_astra-4-vg-
share4_00001_1741874774.zst"
#
echo "Connect to NFS gateway And Freeze file system"
echo ""
ssh -t locadmin@10.177.60.227 sudo -- "sh -c 'fsfreeze --freeze /srv/gateway-
exports/share4'"
echo ""
#
if [ -e $snapshotsds1 ]; then
    echo "Remove old snapshot"
    sudo -i lvremove -f /dev/astra-4-vg/mysnap
    echo ""
fi
echo "Create snapshot of file system"
sudo -i lvcreate -ay -Ky --snapshot -n mysnap astra-4-vg/share4_00001
echo ""
#
echo "Connect to NFS gateway And Unfreeze file system"
echo ""
ssh -t locadmin@10.177.60.227 sudo -- "sh -c 'fsfreeze --unfreeze /srv/gateway-
exports/share4'"
echo ""
#
echo "Create Compressed Copy of file system on SDS 1"
echo ""
if [ -e $mdcopysds1 ]; then
    echo "Remove Old copy "
    sudo -i rm /root/syncer/backups/full_astra-4-vg-share4_00001_1741874774.zst
    echo ""
fi
echo "Create compressed copy "
sudo bash -c 'dd if=/dev/mapper/astra--4--vg-mysnap bs=1G status=progress |
zstd -o /root/syncer/backups/full_astra-4-vg-share4_00001_1741874774.zst'
echo ""
echo ""
#
```

Скрипт 2 выполняет копирование сжатой копии на СХД 2

Пример скрипта 2

```
#!/bin/bash
#
#
#
echo ""
echo "Step 2 Transferring Copy of MailDir To SDS 2"
```

```
echo ""
usrhstsds2="locadmin@10.177.60.222"
mdcopysds2="/mnt/vdd/syncer/backups/full_astra-4-vg-
share4_00001_1741874774.zst"

if ssh $usrhstsds2 stat $mdcopysds2 \> /dev/null 2\>\&1
   then
     echo "Old copy exists on sds2, deleted"
     echo ""
       ssh -t locadmin@10.177.60.222 sudo -- "sh -c 'rm /mnt/vdd/syncer/back-
ups/full_astra-4-vg-share4_00001_1741874774.zst'"
     echo ""
fi
      echo "Transfer copy to sds2"
      echo ""
        sudo bash -c 'rsync -av --progress --stats /root/syncer/back-
ups/full_astra-4-vg-share4_00001_1741874774.zst locad-
min@10.177.60.222:/mnt/vdd/syncer/backups'
echo ""
```

Третий скрипт выполняет следующие шаги:

- распаковывает копию на СХД 2 в реплику;
- удаляет имеющиеся на узлах СХД резервные копии реплики;
- создает новые резервные копии реплики на узлах СХД 2;
- выдает доступ к реплике через NFS шлюз

Пример скрипта 3

```
#!/bin/sh
#
#
#
echo ""
echo "Step 3 Create Replica from Copy of MailDir "
echo ""
echo "     Write Copy To Replica on SDS 2"
echo ""
#
ssh -t locadmin@10.177.161.192 sudo -- "sh -c 'sudo -i zstd -d -c
/mnt/vdd/syncer/backups/full_astra-4-vg-share4_00001_1741874774.zst | dd
of=/dev/mapper/astra--4--vg-share4_00001 bs=1G status=progress'"
#
#
echo "     Remove old Replica's Copies"
echo ""
ssh -t locadmin@10.177.161.190 sudo -- "sh -c 'sudo -i linstor r d linstor-
1.sds.test share4'"
ssh -t locadmin@10.177.161.190 sudo -- "sh -c 'sudo -i linstor r d linstor-
2.sds.test share4'"
echo ""
echo "     Create New Replica's Copies "
echo ""
ssh -t locadmin@10.177.161.190 sudo -- "sh -c 'sudo -i linstor r c linstor-
2.sds.test share4'"
```

```
ssh -t locadmin@10.177.161.190 sudo -- "sh -c 'sudo -i linstor r c linstor-
1.sds.test share4'"
echo ""
#
#
#
echo "     Connect to NFS gateway And Share MailDir"
echo ""
ssh -t locadmin@10.177.161.192 sudo -- "sh -c 'sudo -i mv /etc/drbd-reac-
tor.d/share4.toml /home/locadmin'"
sleep 5
echo ""
ssh -t locadmin@10.177.161.192 sudo -- "sh -c 'sudo -i drbdsetup secondary
share4'"
echo ""
ssh -t locadmin@10.177.161.192 sudo -- "sh -c 'sudo -i cp -av
/root/syncer/share4.toml /etc/drbd-reactor.d/'"
echo ""
sleep 10
ssh -t locadmin@10.177.161.192 sudo -- "sh -c 'sudo -i showmount -e'"
#
#
#
```

13. Приложение 5 – Настройка инфраструктуры Kerberos

13.1. Регистрация сервисов (SPN)

SPN (Service Principal Name) — это уникальное имя экземпляра сетевого сервиса, зарегистрированного в Kerberos. SPN связывает тип сервиса, имя узла и учётную запись сервисного принципала, например:

```
HTTP/mail.krbrp.local
```

При подключении, клиент формирует SPN целевого сервиса и запрашивает для него сервисный билет у KDC. Сервер принимает этот билет и проверяет его с помощью соответствующего ключа из keytab-файла.

Для RuPost регистрируются отдельные SPN для сервисов HTTP, IMAP и SMTP. Каждый SPN должен быть уникальным в пределах домена Kerberos (Kerberos Realm) и точно соответствовать имени узла, которое используют клиенты.

13.2. Настройка для Microsoft Active Directory

Пользователь владелец сервисов: `authservice`.

1. Регистрация необходимых принципалов (SPN):
```
setspn -U -S HTTP/ mail.krbrp.local EXCH2013\authservice
setspn -U -S imap/ mail.krbrp.local EXCH2013\authservice
setspn -U -S smtp/ mail.krbrp.local EXCH2013\authservice
```

2. Формирование keytab-файла:

Перед формированием keytab-файла необходимо определить текущую версию Kerberos-ключа (KVNO) сервисной учётной записи.

```
$kvno = (Get-ADUser -Identity authservice -Properties 'msDS-
KeyVersionNumber').'msDS-KeyVersionNumber'
```

Для формирования keytab-файла используется штатная утилита Microsoft ktpass.
Формирование файла выполняется последовательно: сначала создаётся запись для HTTP, затем добавляются записи для IMAP и SMTP.

```
ktpass /princ HTTP/mail.krbrp.local@EXCH2013.LOCAL /mapuser
EXCH2013\authservice /pass * /crypto AES256-SHA1 /ptype KRB5_NT_PRINCIPAL
/kvno $kvno /mapop add -setpass -setupn /rawsalt
EXCH2013.LOCALauthservice +dumpsalt /out C:\keytab\http.keytab

ktpass /princ imap/mail.krbrp.local@EXCH2013.LOCAL/mapuser
EXCH2013\authservice /pass * /crypto AES256-SHA1 /ptype KRB5_NT_PRINCIPAL
/kvno $kvno /mapop add -setpass -setupn /rawsalt
EXCH2013.LOCALauthservice +dumpsalt /in C:\keytab\http.keytab /out
C:\keytab\http-imap.keytab
```

```
ktpass /princ smtp/mail.krbrp.local@EXCH2013.LOCAL/mapuser
EXCH2013\authservice /pass * /crypto AES256-SHA1 /ptype KRB5_NT_PRINCIPAL
/kvno $kvno /mapop add -setpass -setupn /rawsalt
EXCH2013.LOCALauthservice +dumpsalt /in C:\keytab\http-imap.keytab /out
C:\keytab\authservice.keytab
```

Итоговый keytab-файл: `C:\keytab\authservice.keytab`

13.3. Настройка для Samba DC

Пользователь владелец сервисов: `authservice`

1. Регистрация необходимых принципалов (SPN):

```
samba-tool spn add HTTP/mail.krbrp.local authservice
samba-tool spn add imap/mail.krbrp.local authservice
samba-tool spn add smtp/mail.krbrp.local authservice
```

Проверка:

```
samba-tool user show authservice | sed -n 's/^servicePrincipalName: //p'
http/mail.krbrp.local
imap/mail.krbrp.local
smtp/mail.krbrp.local
```

2. Формирование keytab:

```
root@dc1:~# sudo samba-tool domain exportkeytab /root/smb-http.keytab -
principal=HTTP/mail.krbrp.local

root@dc1:~# sudo samba-tool domain exportkeytab /root/smb-imap.keytab -
principal=imap/mail.krbrp.local

root@dc1:~# sudo samba-tool domain exportkeytab /root/smb-smtp.keytab --
principal=smtp/mail.krbrp.local
```

Объединение нескольких keytab-файлов в один:

```
ktutil
ktutil: rkt /tmp/http.keytab
ktutil: rkt /tmp/imap.keytab
ktutil: rkt /tmp/smtp.keytab
ktutil: wkt /etc/smballspn.keytab
ktutil: quit
klist -kte /Kerberos/keytab/smb.local/smballspn.keytab
Keytab name: FILE:/Kerberos/keytab/smb.local/smballspn.keytab
```

Результат:

```
KVNO Timestamp           Principal
---- ------------------- ------------------------------------------------------
   2 29.10.2026 13:25:14 HTTP/mail.krbrp.local@SMB.LOCAL (aes256-cts-hmac-sha1-96)
   2 29.10.2026 13:25:14 HTTP/mail.krbrp.local@SMB.LOCAL (aes128-cts-hmac-sha1-96)
   2 29.10.2026 13:25:14 imap/mail.krbrp.local@SMB.LOCAL (aes256-cts-hmac-sha1-96)
   2 29.10.2026 13:25:14 imap/mail.krbrp.local@SMB.LOCAL (aes128-cts-hmac-sha1-96)
```

```
   2 29.10.2026 13:25:14 smtp/mail.krbrp.local@SMB.LOCAL (aes256-cts-hmac-sha1-96)
   2 29.10.2026 13:25:14 smtp/mail.krbrp.local@SMB.LOCAL (aes128-cts-hmac-sha1-96)
```

13.4. Настройка для ALD.PRO и FreeIPA

1. Создание хоста:
   `ipa host-add mail.krbrp.local`

где `mail.krbrp.local` – “Имя узла почтовой системы” в DNS MX записи почтовых доменов.

2. Регистрация необходимых принципалов (SPN):
   ```
   ipa service-add HTTP/ mail.krbrp.local
   ipa service-add imap/mail.krbrp.local
   ipa service-add smtp/mail.krbrp.local
   ```

Principal	**Назначение**
HTTP/mail.krbrp.local@ALDKRB.LOCAL	Аутентификация в web клиенте RuPost (rupost-mua)
imap/mail.krbrp.local@ALDKRB.LOCAL	Аутентификация IMAP-клиентов
smtp/mail.krbrp.local@ALDKRB.LOCAL	Аутентификация SMTP-клиентов

3. Формирование keytab-файла:

Создание отдельных keytab-файлов:

```
ipa-getkeytab -s krbdc01.aldkrb.local -p
HTTP/mail.krbrp.local@ALDKRB.LOCAL -k ./HTTP.keytab
ipa-getkeytab -s krbdc01.aldkrb.local -p imap/mail.krbrp.local@
ALDKRB.LOCAL -k ./imap.keytab
ipa-getkeytab -s krbdc01.aldkrb.local -p smtp/mail.krbrp.local@
ALDKRB.LOCAL -k ./smtp.keytab
```

Объединение в один keytab-файл:

```
ktutil
rkt HTTP.keytab
rkt imap.keytab
rkt smtp.keytab
wkt aldkrb.keytab
```

Результат:

```
KVNO Timestamp           Principal
---- ------------------- ------------------------------------------------------
   1 27.09.2026 22:29:24 HTTP/mail.krbrp.local@ALDKRB.LOCAL (aes256-cts-hmac-sha1-96)
   1 27.09.2026 22:29:24 imap/mail.krbrp.local@ALDKRB.LOCAL (aes256-cts-hmac-sha1-96)
   1 27.09.2026 22:29:24 smtp/mail.krbrp.local@ALDKRB.LOCAL (aes256-cts-hmac-sha1-96)
```

© 2021-2026 РуПост

13.5. Проверка созданного keytab-файла

Для проверки пригодности полученного keytab-файла к расшифровке сервисного билета Kerberos можно использовать команду:

```
kvno -k test.keytab HTTP/mail.krbrp.local@EXCH2013.LOCAL
```

Команда получает сервисный билет для указанного сервисного принципала (либо использует ранее полученный билет из кэша) и проверяет возможность его расшифровки с использованием ключа из указанного keytab-файла.

Успешное выполнение команды с сообщением:

```
keytab entry valid
```

подтверждает, что keytab-файл содержит действительный ключ для расшифровки сервисного билета указанного сервисного принципала.

Пример:

```
kvno -k ~/Kerberos/keytab
/dc01.exch2013.local/fullkrbexch2013local.keytab
HTTP/mail.krbrp.local@EXCH2013.LOCAL
HTTP/mail.krbrp.local@EXCH2013.LOCAL: kvno = 3, keytab entry valid
```

13.6. Настройка браузеров через Групповые политики домена

Подготовка браузеров на основе Chrome через групповые политики (GPO) Microsoft AD

Групповые политики:

Конфигурация компьютера →
Политики →
Административные шаблоны →
Система →
Передача учетных данных

Или на английском:

Computer Configuration →
Policies →
Administrative Templates →
System →
Credentials Delegation

Включить:

- Разрешить передачу учетных данных, установленных по умолчанию (Allow delegating default credentials)

- Разрешить передачу учетных данных, установленных по умолчанию, с проверкой подлинности сервера «только NTLM» (Allow delegating default credentials with NTLM-only server authentication)

Задать для них значения:

```
HTTP/ mail.krbrp.local
```

Далее в

Конфигурация компьютера →
Политики →
Административные шаблоны →
Компоненты Windows →
Internet Explorer →
Панель управления браузером →
Вкладка "Безопасность"

Или на английском:
Computer Configuration →
Policies →
Administrative Templates →
Windows Components →
Internet Explorer →
Internet Control Panel →
Security Page

Включить:

- Список назначений зоны для веб-сайтов (Site to Zone Assignment List)

Value name	**Value**
mail.krbrp.local	1

После применения групповой политики все браузеры на основе Chrome смогут аутентифицироваться по Kerberos при наличии tgt билета в системе пользователя.

Подготовка Firefox через групповые политики (GPO) Microsoft AD

Необходимо загрузить шаблон политик:
https://github.com/mozilla/policy-templates/releases

Шаблоны политики скопировать в каталог:
В `C:\Windows\PolicyDefinitions\` - файл .admx
В `C:\Windows\PolicyDefinitions\ru-RU` – файл .adml

Структура размещения административных шаблонов Mozilla Firefox:

C:\Windows\PolicyDefinitions
firefox.admx
mozilla.admx
en-US
firefox.adml
mozilla.adml
ru-RU
firefox.adml
mozilla.adml

Конфигурация компьютера →
Политики →
Административные шаблоны →
FireFox →
Аутентификация

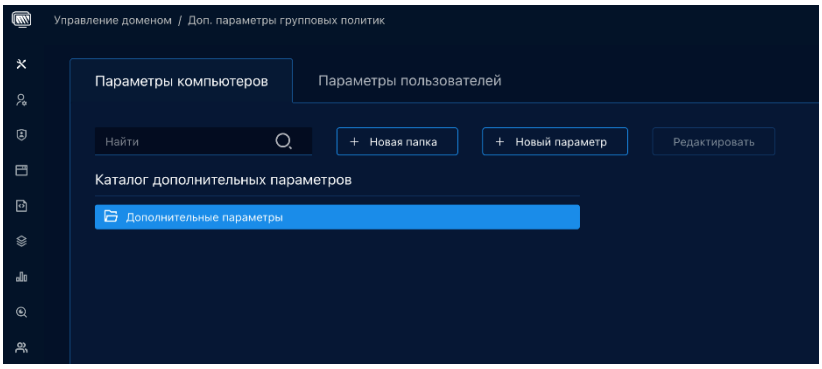
Или на английском:

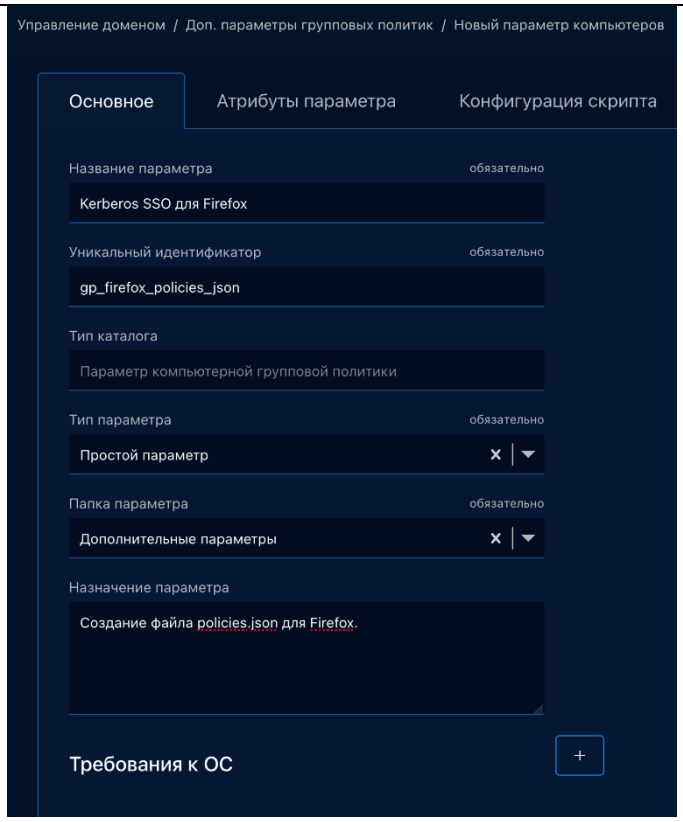
Computer Configuration →
Policies →
Administrative Templates →
FireFox →
Authentication

Задать политики:

`SPNEGO` - значение `mail.krbrp.local`

Настройка браузеров через групповые политики ALD.PRO





На вкладке “Конфигурация скрипта” добавить:

```
aldpro_firefox_distribution_directory:
  file.directory:
    - name: /usr/lib/firefox/distribution
    - user: root
    - group: root
    - mode: '0755'
    - makedirs: true

aldpro_firefox_policies_json:
  file.managed:
    - name: /usr/lib/firefox/distribution/policies.json
    - user: root
    - group: root
    - mode: '0644'
    - backup: minion
    - contents: |
        {
          "policies": {
            "Certificates": {
              "ImportEnterpriseRoots": true,
              "Install": [
                "/etc/ipa/ca.crt"
              ]
            },
            "Authentication": {
```

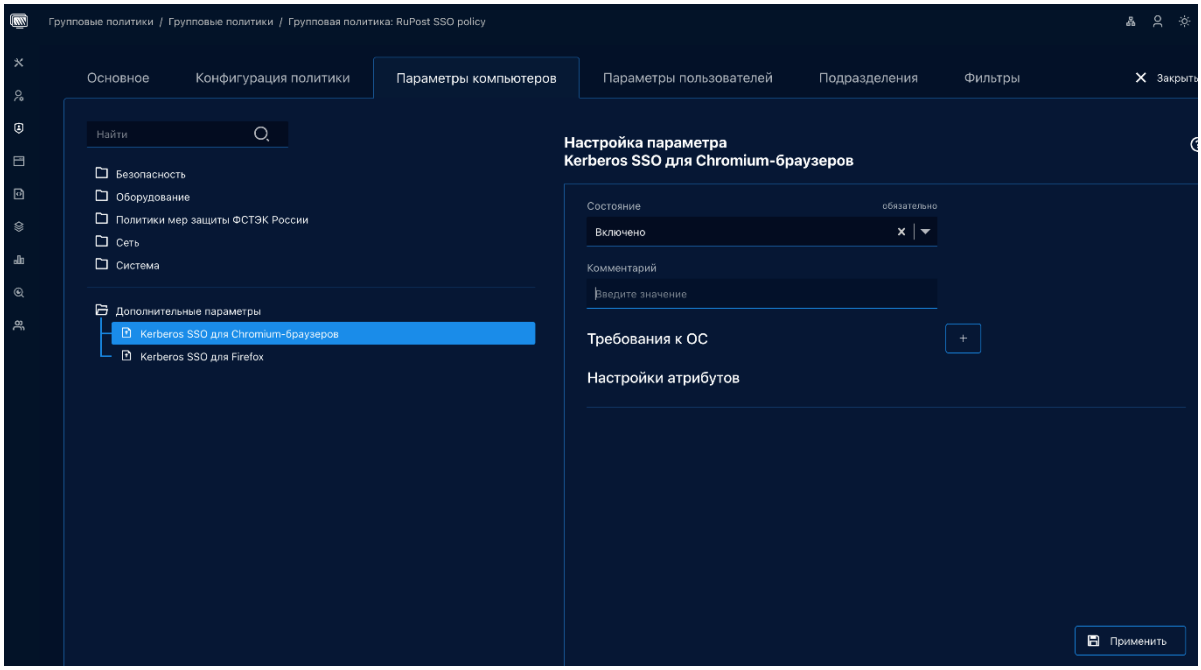
```
                "SPNEGO": [
                  "mail.krbrp.local"
                ]
              }
            }
          }
      - require:
        - file: aldpro_firefox_distribution_directory
```

Для браузеров на основе Chrome создать отдельный параметр и в конфигурация скрипта указать:

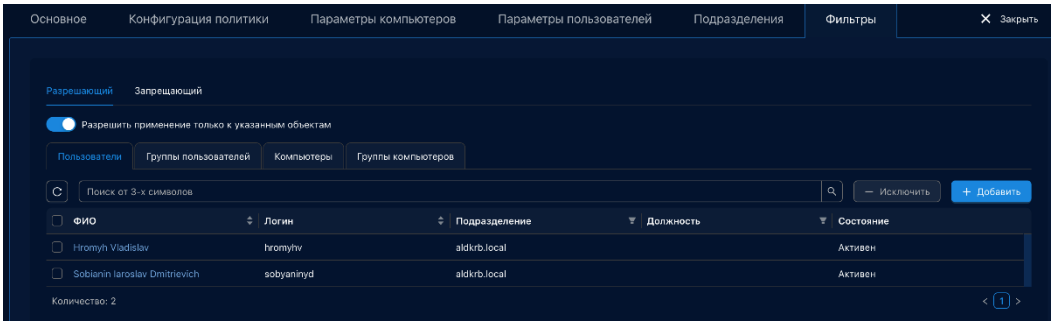
```
aldpro_yandex_policy_directory:
  file.directory:
    - name: /etc/opt/yandex/browser/policies/managed
    - user: root
    - group: root
    - mode: '0755'
    - makedirs: true
    - onlyif:
      - /usr/bin/test -x /usr/bin/yandex-browser

aldpro_yandex_kerberos_sso:
  file.managed:
    - name:
/etc/opt/yandex/browser/policies/managed/aldpro_kerberos_sso.json
    - user: root
    - group: root
    - mode: '0644'
    - backup: minion
    - contents: |
        {
          "AuthServerAllowlist": "mail.krbrp.local"
        }
    - require:
      - file: aldpro_yandex_policy_directory
    - onlyif:
      - /usr/bin/test -x /usr/bin/yandex-browser

aldpro_edge_policy_directory:
  file.directory:
    - name: /etc/opt/edge/policies/managed
    - user: root
    - group: root
    - mode: '0755'
    - makedirs: true
    - onlyif:
      - /usr/bin/test -x /usr/bin/microsoft-edge

aldpro_edge_kerberos_sso:
  file.managed:
    - name: /etc/opt/edge/policies/managed/aldpro_kerberos_sso.json
    - user: root
```

```
      - group: root
      - mode: '0644'
      - backup: minion
      - contents: |
          {
            "AuthServerAllowlist": "mail.krbrp.local"
          }
      - require:
        - file: aldpro_edge_policy_directory
      - onlyif:
        - /usr/bin/test -x /usr/bin/microsoft-edge

aldpro_chromium_policy_directory:
  file.directory:
    - name: /etc/chromium/policies/managed
    - user: root
    - group: root
    - mode: '0755'
    - makedirs: true
    - onlyif:
      - /usr/bin/test -x /usr/bin/chromium

aldpro_chromium_kerberos_sso:
  file.managed:
    - name: /etc/chromium/policies/managed/aldpro_kerberos_sso.json
    - user: root
    - group: root
    - mode: '0644'
    - backup: minion
    - contents: |
        {
          "AuthServerAllowlist": "mail.krbrp.local"
        }
    - require:
      - file: aldpro_chromium_policy_directory
    - onlyif:
      - /usr/bin/test -x /usr/bin/chromium

aldpro_google_chrome_policy_directory:
  file.directory:
    - name: /etc/opt/chrome/policies/managed
    - user: root
    - group: root
    - mode: '0755'
    - makedirs: true
    - onlyif:
      - /usr/bin/test -x /usr/bin/google-chrome-stable

aldpro_google_chrome_kerberos_sso:
  file.managed:
    - name: /etc/opt/chrome/policies/managed/aldpro_kerberos_sso.json
    - user: root
```

```
- group: root
- mode: '0644'
- backup: minion
- contents: |
    {
      "AuthServerAllowlist": "mmail.krbrp.local"
    }
- require:
  - file: aldpro_google_chrome_policy_directory
- onlyif:
  - /usr/bin/test -x /usr/bin/google-chrome-stable
```



Далее на вкладке фильтры включить разрешающее применение к объектам и указать объекты к которым должна быть применена политика



Далее необходимо дождаться применения групповой политики на клиентах или выполнить принудительную синхронизацию на клиенте

```
sudo aldpro-gpupdate --gp –verbose
```

Настройка браузеров через групповые политики Samba DC

Необходимо создать групповую политику

```
samba-tool gpo create 'SSO-Browsers-Kerberos' -U 'SMB\Administrator'
```

Будет создана групповая политика и отображен присвоенный GUID политики.

Необходимо подготовить файл конфигураций политики.

Пример файла `/root/browser-sso-gpo.json` :

```
[
  {
    "keyname":
"Software\\Policies\\Mozilla\\Firefox\\Authentication\\SPNEGO",
    "valuename": "1",
    "class": "MACHINE",
    "type": "REG_SZ",
    "data": "mail.krbrp.local"
  },
  {
    "keyname": "Software\\Policies\\Mozilla\\Firefox\\Authentication",
    "valuename": "Locked",
    "class": "MACHINE",
    "type": "REG_DWORD",
    "data": 1
  },
  {
    "keyname": "Software\\Policies\\Google\\Chrome",
    "valuename": "AuthServerAllowlist",
    "class": "MACHINE",
    "type": "REG_SZ",
    "data": "mail.krbrp.local"
  },
  {
    "keyname": "Software\\Policies\\Google\\Chrome",
    "valuename": "DisableAuthNegotiateCnameLookup",
    "class": "MACHINE",
    "type": "REG_DWORD",
    "data": 1
  },
  {
    "keyname": "Software\\Policies\\Chromium",
    "valuename": "AuthServerAllowlist",
    "class": "MACHINE",
    "type": "REG_SZ",
    "data": "mail.krbrp.local"
  },
  {
    "keyname": "Software\\Policies\\Microsoft\\Edge",
    "valuename": "AuthServerAllowlist",
    "class": "MACHINE",
    "type": "REG_SZ",
```

```
        "data": "mail.krbrp.local"
      },
      {
        "keyname": "Software\\Policies\\Microsoft\\Edge",
        "valuename": "DisableAuthNegotiateCnameLookup",
        "class": "MACHINE",
        "type": "REG_DWORD",
        "data": 1
      },
      {
        "keyname": "Software\\Policies\\YandexBrowser",
        "valuename": "AuthServerAllowlist",
        "class": "MACHINE",
        "type": "REG_SZ",
        "data": "mail.krbrp.local"
      },
      {
        "keyname": "Software\\Policies\\YandexBrowser",
        "valuename": "DisableAuthNegotiateCnameLookup",
        "class": "MACHINE",
        "type": "REG_DWORD",
        "data": 1
      }
    ]
```

Далее необходимо загрузить файл конфигурации в групповую политику:

```
samba-tool gpo load '{204666AC-3988-4AC4-9066-532D94575295}' --
content=/root/browser-sso-gpo.json -U 'SMB\Administrator'
```

`204666AC-3988-4AC4-9066-532D94575295` – это GUID созданной ранее групповой политики.

После создания групповой политики необходимо присвоить политику необходимым объектам в LDAP.

Пример присвоения для OU:

```
samba-tool gpo setlink 'OU=Test OU,DC=smb,DC=local' '{204666AC-3988-4AC4-
9066-532D94575295}' -U 'SMB\Administrator'
```

13.7. Настройка браузеров для компьютеров вне домена

Настройка Safari (macOS)

После настройки Kerberos на уровне операционной системы, браузер Safari дополнительных настроек не требует.

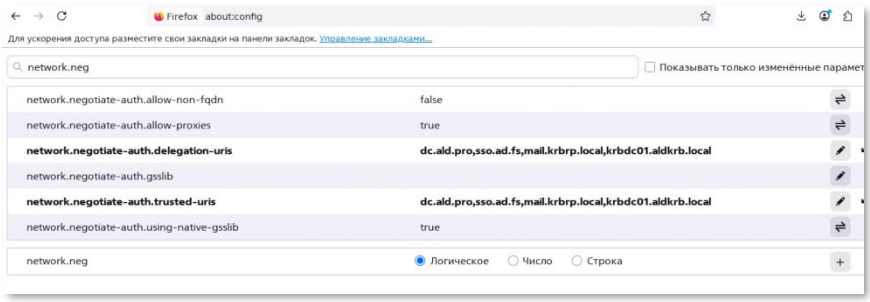
Настройка Firefox

Браузер Firefox можно настроить вручную через `about:config`.

Необходимо задать параметр:

```
network.negotiate-auth.trusted-uris
```

И разрешить SPNEGO/Kerberos для сайта - пример:



Настройка браузеров на основе Chrome

Для поддержки работы с билетами Kerberos, необходимо в настройках браузера указать:

```
AuthServerAllowlist
DisableAuthNegotiateCnameLookup
```

