Почтовая система RuPost

Что нового в версии

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: https://www.rupost.ru/

Оглавление

Версия 4.3.4 5
Обзор релиза 5
Нововведения 5
Автоматическое добавление администраторов по фильтрам LDAP 5
Автоматическое назначение ролей администраторов по фильтрам LDAP 6
Оптимизация репликации данных для нескольких “горячих” реплик 6
Геокластер - резервный сайт 6
Адресная книга – поддержка поддоменов LDAP (Microsoft AD) 7
Мониторинг – количество писем за период 8
Расширение возможностей транспортных правил 9
Расширение механизма назначения прав на общие ящики 9
Политики очистки почтовых ящиков 10
Управление периодом синхронизации с LDAP 11
Поле “Комментарий” для доверенного источника 11
Настройка “Возможность предоставлять совместный доступ” 11
Изменение логики работы индикатора проверки записей DNS 12
Настройка размера памяти для Rupost-cs (Memcached) 12
Настройки для сервиса рассылок 13
CLI - настройка периодичности и времени запуска ребалансировки пользователей 13
Автодобавление событий в календарь для псевдонимов 14
Пулер для подключений к СУБД 14
Обновление страницы “Экземпляры” 14
Создание ключа для интеграции с WorksPad сервером 15
Расширение функциональности веб-клиента 15
Поддержка Yandex браузера 16
Аутентификация пользователей веб-клиента по протоколу Kerberos 16
Изменение расположения почтовых компонентов 19
Обновление версий почтовых компонентов 19
Улучшения и исправления 19
Приложение. Настройка инфраструктуры Kerberos 21

© 2021-2026 РуПост

Внимание!

Перед обновлением версии RuPost выполните **резервное копирование** узлов кластера и баз данных.

Внимание!

В связи с тем, что в версии 4.3.4 внесены существенные изменения в настройки почтовых компонентов - если у вас применен пользовательский шаблон, то перед обновлением основного кластера, нужно обязательно провести проверку обновления на стейдж среде. Если ошибок нет, то можно проводить обновление основного кластера.
Если при обновлении стейдж среды появились ошибки в работе, то:

1. Разверните на стейдж среде встроенный шаблон, на основе которого был разработан пользовательский.
2. Внесите необходимые изменения в пользовательский шаблон и проверьте его в работе.
3. Перед обновлением основного кластера, разверните на нем встроенный шаблон.
4. Обновите версию.
5. Разверните шаблон, разработанный на шаге 2.

Внимание!

Если у вас в организации используются почтовые клиенты Desktop X и Workspad X рекомендуем, после завершения обновления RuPost, обновить сервер Workspad на актуальную версию.

Внимание!

Перед обновлением версии RuPost обратите внимание на выбор варианта обновления:

- **обычное** – все узлы кластера обновляются одновременно, но требуется предварительный вывод из эксплуатации всех экземпляров RuPost;

- **непрерывное** – обновление без прерывания обслуживания пользователей с последовательным обновлением узлов кластера.

Внимание!

После завершения **непрерывного** обновления возможно неравномерное распределение пользователей по узлам кластера.

При необходимости, для перераспределения пользователей на менее загруженные узлы, на всех узлах с большим количеством пользователей выполните команду:

```
rupost kick-local-users
```

© 2021-2026 РуПост

Версия 4.3.4

Дата релиза 10.11.2026

Обзор релиза

В этой версии основное внимание было уделено совершенствованию внутренних механизмов, направленное, в первую очередь, на повышение быстродействия, снижение потребления ресурсов и повышение надежности Геокластера и кластера RuPost.

Кроме того, добавлена новая функциональность в следующих областях:

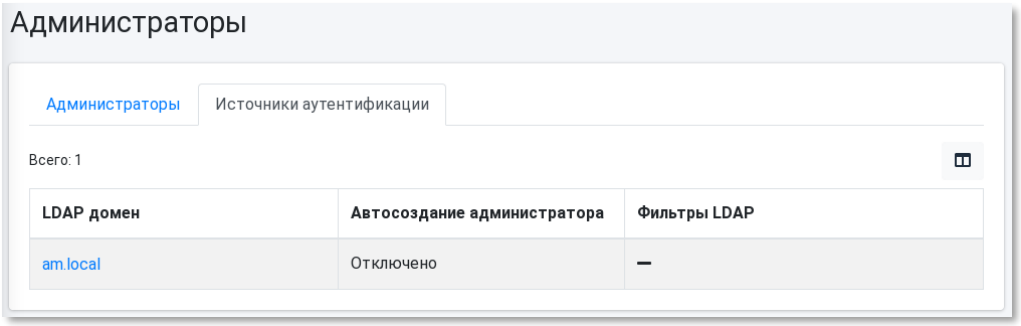
- **Почтовые правила** – расширен набор обрабатываемых условий.
- **Сервис рассылок** – повышение скорости доставки сообщений и поддержка дедупликации.
- **Аутентификация пользователей** – в части поддержки единого входа (SSO / Kerberos) для веб-клиента.
- **Управление администраторами** – автоматизация создания учетных записей и назначение ролей.
- **Геокластер** – усовершенствована работа резервного сайта.
- **Мониторинг** – в частности, статистика по количеству обрабатываемых сообщений за период.
- **Веб-клиент** – расширен набор операций, которые пользователь может совершать над списком писем и календарными событиями.

Нововведения

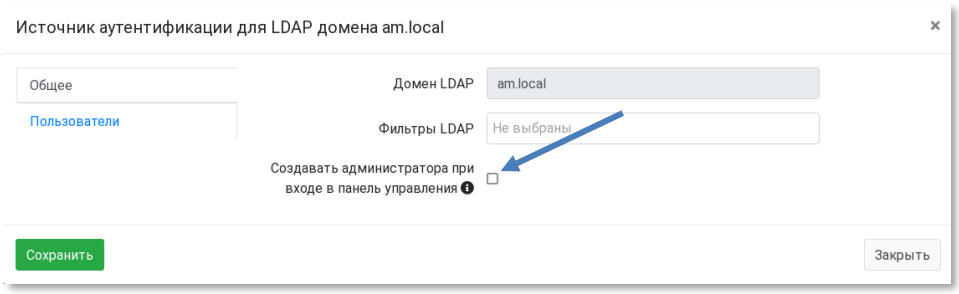
Автоматическое добавление администраторов по фильтрам LDAP

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.

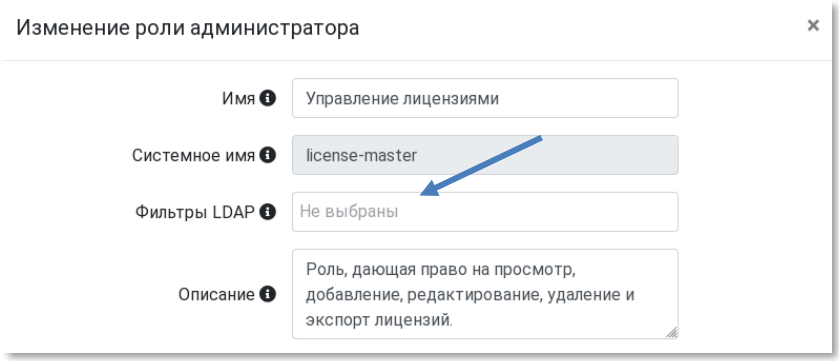


На вкладке “Пользователи” можно просмотреть список пользователей, из выбранных фильтров LDAP.

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.



Оптимизация репликации данных для нескольких “горячих” реплик

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.

Геокластер - резервный сайт

Оптимизация передачи данных

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).

Оптимизация механизма переключения на 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.

Внимание!

Для обеспечения доставки почты на резервный сайт от внешних адресатов, обновите данные в DNS – укажите адрес резервного сайта вместо адреса основного.

Встречное переключение – основной/ резервный

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.

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.

Адресная книга – поддержка поддоменов LDAP (Microsoft AD)

В версии 4.3.4 добавлена возможность сбора данных для формирования корпоративной адресной книги с использованием Глобального каталога (Microsoft Active Directory Global Catalog).

© 2021-2026 РуПост

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:

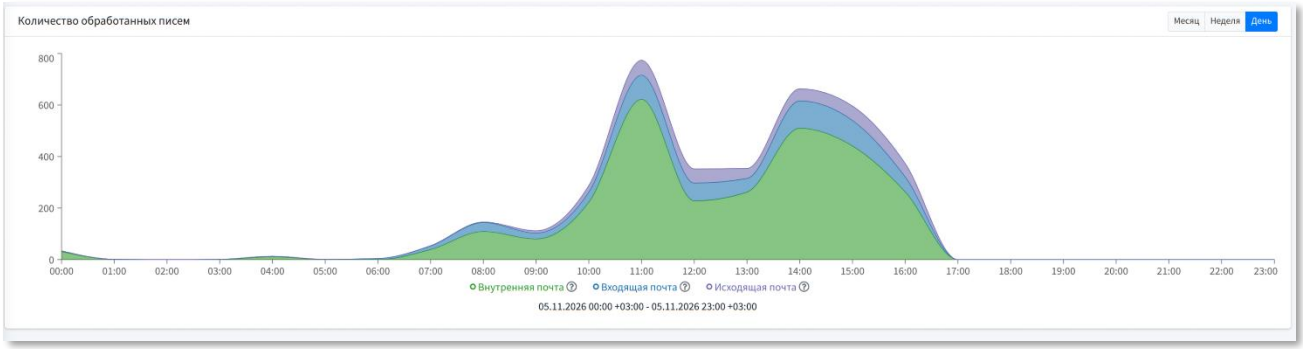
- **3268** – обычное подключение.
- **3269** – SSL/TLS.

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.

Мониторинг – количество писем за период

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.

© 2021-2026 РуПост

Расширение возможностей транспортных правил

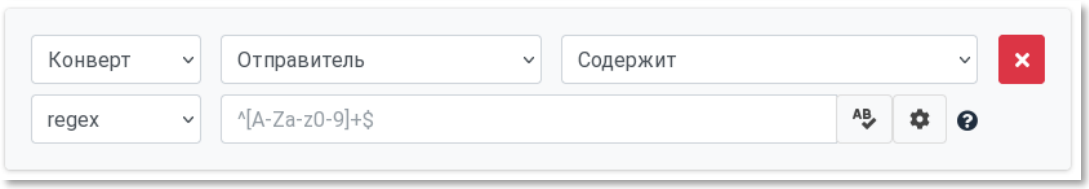
В версии 4.3.4 расширены возможности транспортных правил – добавлен ряд новых условий.

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.

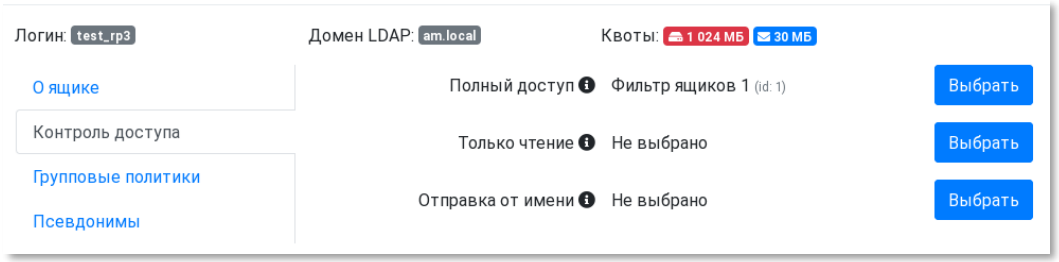


Расширение механизма назначения прав на общие ящики

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

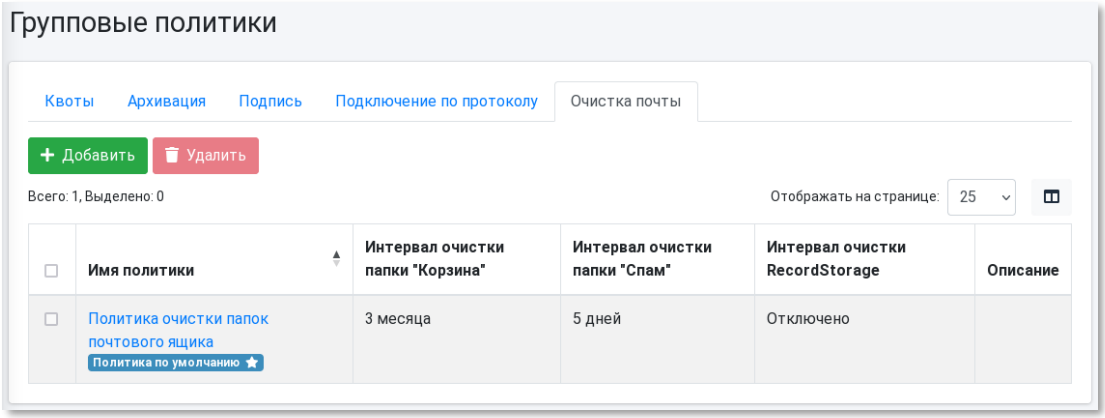
Доступ управляется при помощи фильтров ящиков в трех категориях:

- **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.



Политики очистки почтовых ящиков

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

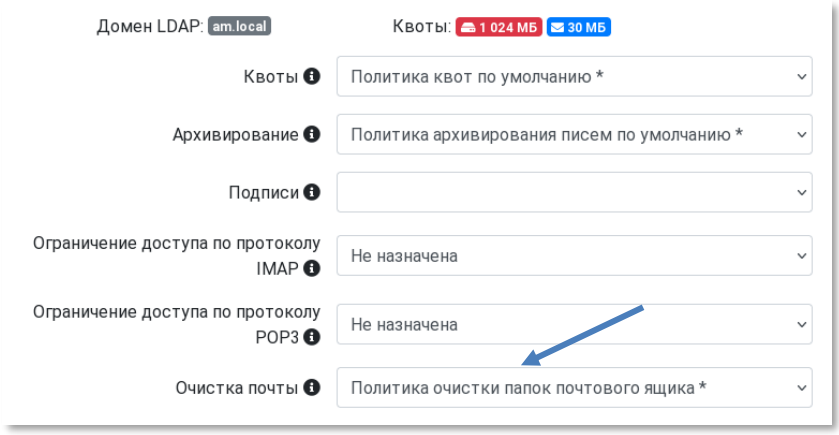


В политике можно указать интервала очистки следующих папок:

- 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.

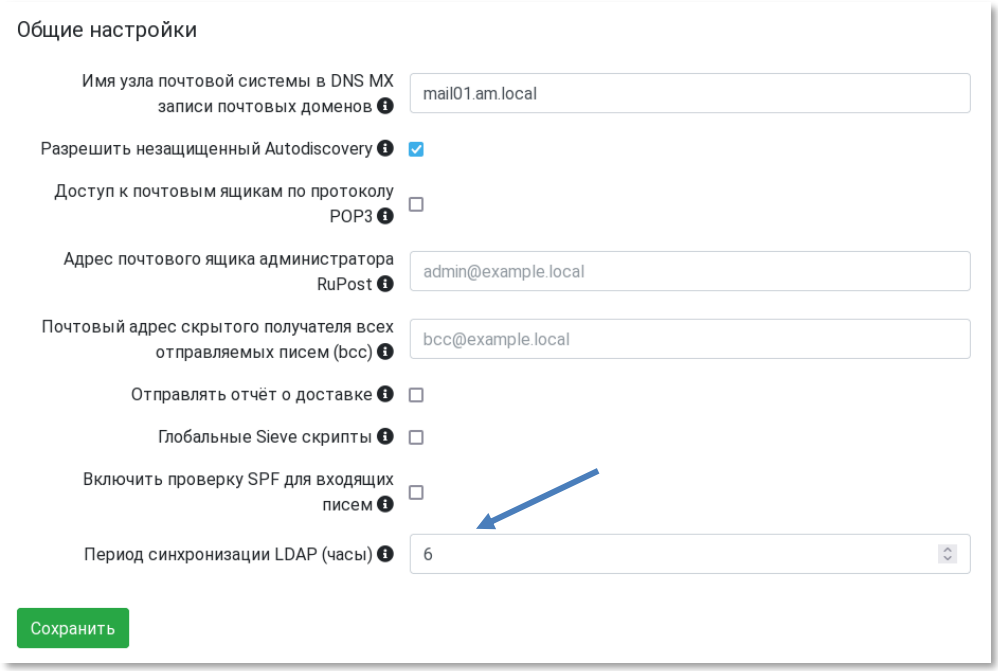
Процедура очистки работает один раз в сутки (в 02:15) - сначала произойдет архивирование и, после его окончания, произойдет очистка.

© 2021-2026 РуПост

Управление периодом синхронизации с LDAP

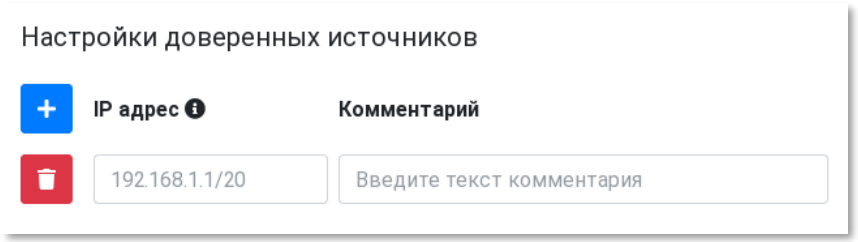
В версии 4.3.4 добавлена возможность управлять периодом синхронизации данных с LDAP в Панели управления.

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



Поле “Комментарий” для доверенного источника

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.

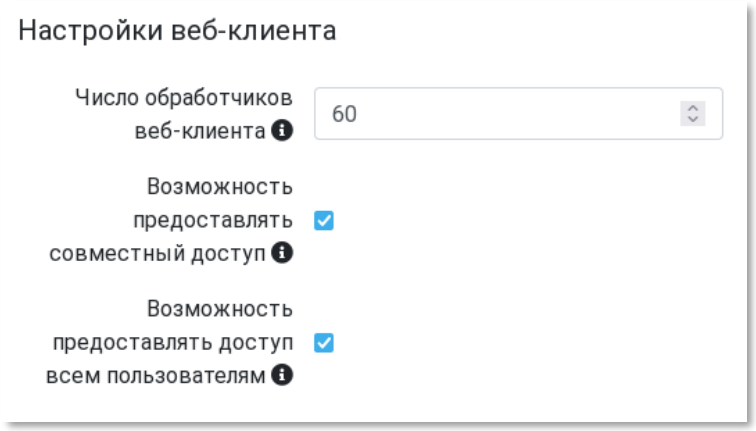


Настройка “Возможность предоставлять совместный доступ”

В версии 4.3.4 добавлена возможность полного запрета пользователям предоставлять доступ к своим данным (почте, календарям и адресным книгам) другим пользователям.

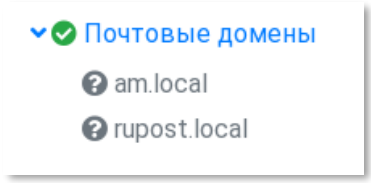
Для того, чтобы отключить возможность предоставления доступа другим пользователям, снимите переключатель “Возможность предоставлять совместный доступ” (вкладка “Почта” на странице “Общие настройки”).

Параметр “Возможность предоставлять доступ всем пользователям”, в отличие от “Возможность предоставлять совместный доступ”, управляет только возможностью пользователя предоставить доступ к своим данным **всем** пользователям.



Изменение логики работы индикатора проверки записей DNS

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.

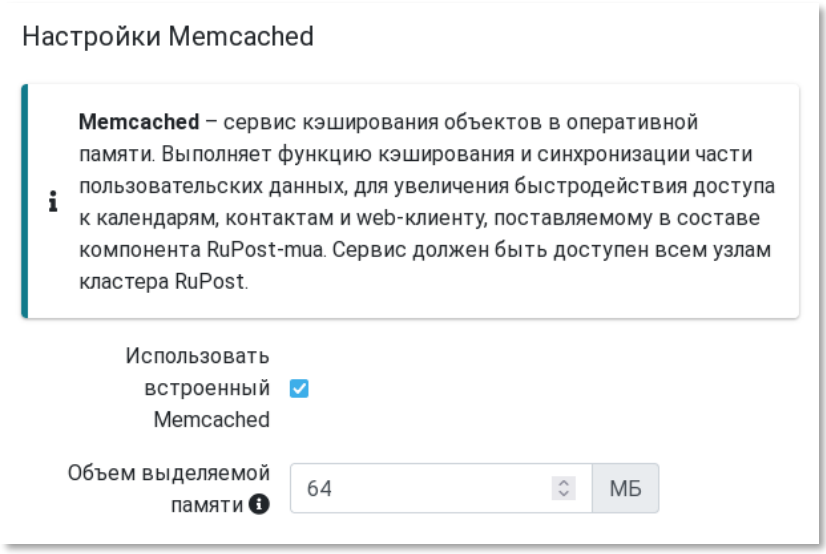


Настройка размера памяти для Rupost-cs (Memcached)

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

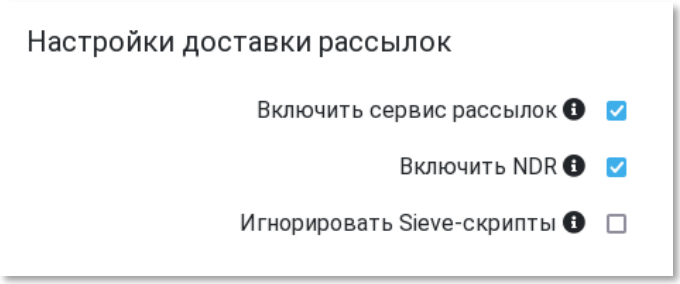
Размер памяти, используемый компонентом Memcached для кеширования данных, определяется параметром “Объем выделяемой памяти” (вкладка “Memcached” на странице “Общие настройки”). Минимально необходимый размер памяти – 64 МБ.

© 2021-2026 РуПост



Настройки для сервиса рассылок

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.

CLI - настройка периодичности и времени запуска ребалансировки пользователей

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

© 2021-2026 РуПост

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”.

Автодобавление событий в календарь для псевдонимов

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

Пулер для подключений к СУБД

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.

Обновление страницы “Экземпляры”

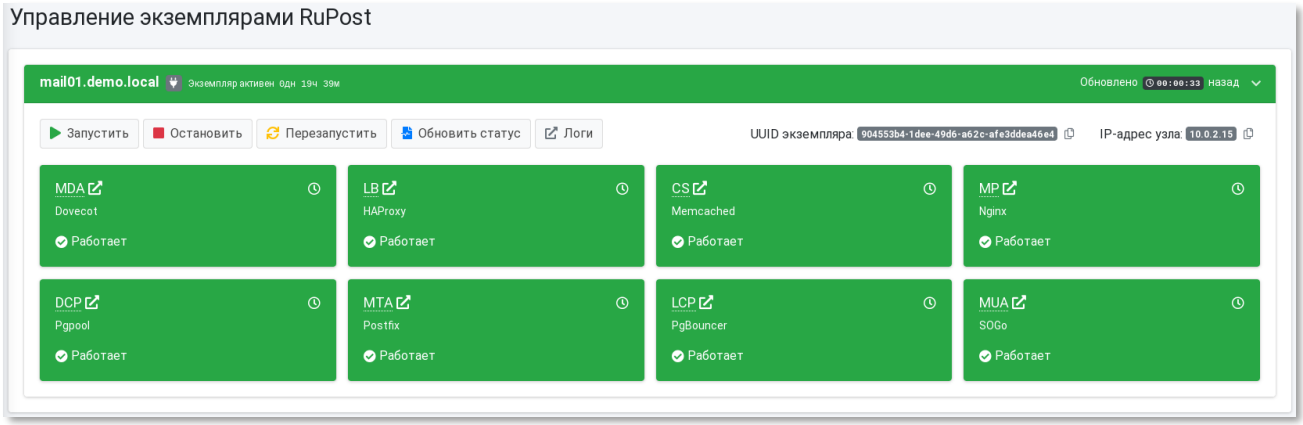
В версии 4.3.4 обновлен внешний вид страницы “Экземпляры”.

Расширен набор отображаемых компонентов – добавлены:

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

А также изменено расположение индикаторов статусов компонентов.

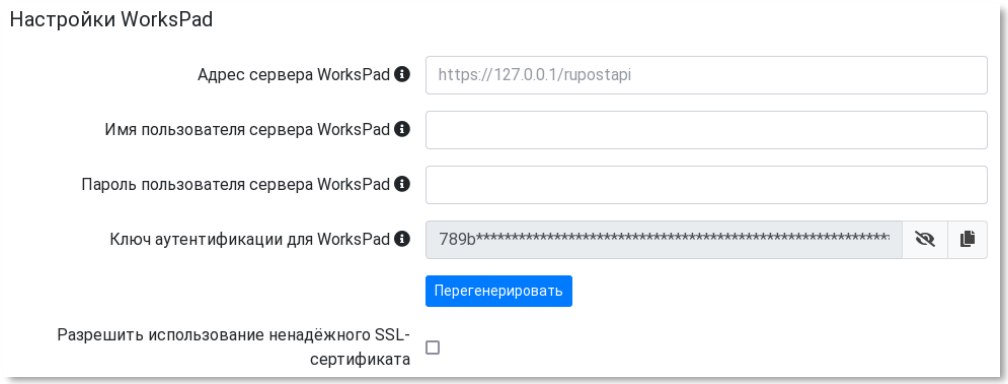
© 2021-2026 РуПост



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.

Расширение функциональности веб-клиента

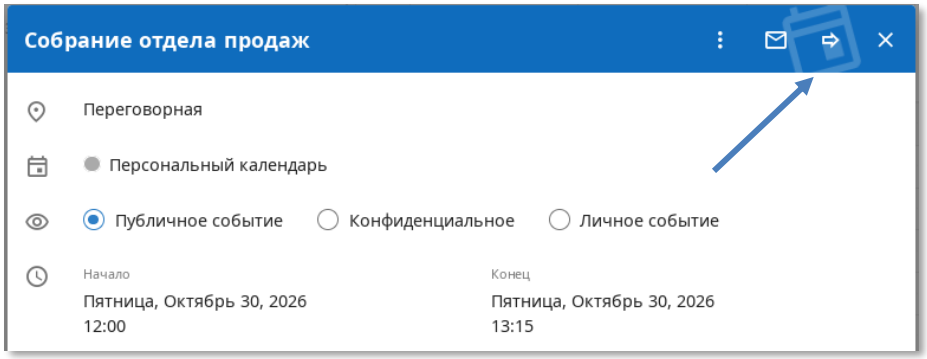
В версии 4.3.4 расширены функциональные возможности веб-клиента rupost-mua – добавлено:

- 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.

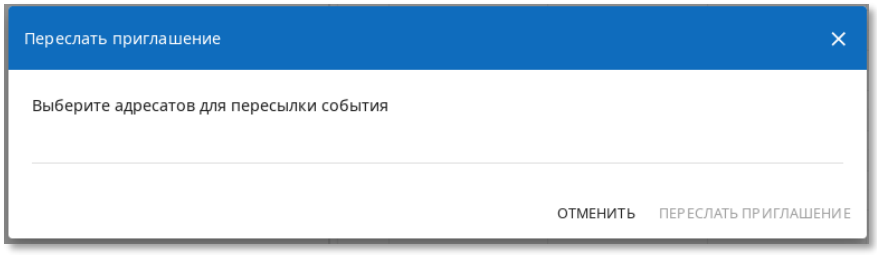
© 2021-2026 РуПост

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.

Поддержка Yandex браузера

В версии 4.3.4 было проведено дополнительное тестирование на совместимость – подтверждаем, что RuPost полноценно работает в браузере Yandex.

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.

Для того, чтобы работала Kerberos-аутентификация пользователей при использовании веб-клиента, необходимо настроить соответствующие параметры в браузерах пользователей. Для всех компьютеров пользователей, добавленных в домен, это можно сделать с помощью применения Групповых политик (GPO). Если же компьютер пользователя не добавлен в домен, то для операционной системы пользователя необходимо добавить поддержку Kerberos и настроить параметры браузера вручную. Настройки для различных типов браузеров описаны в Приложении – “Настройка инфраструктуры Kerberos”.

© 2021-2026 РуПост

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”.

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.

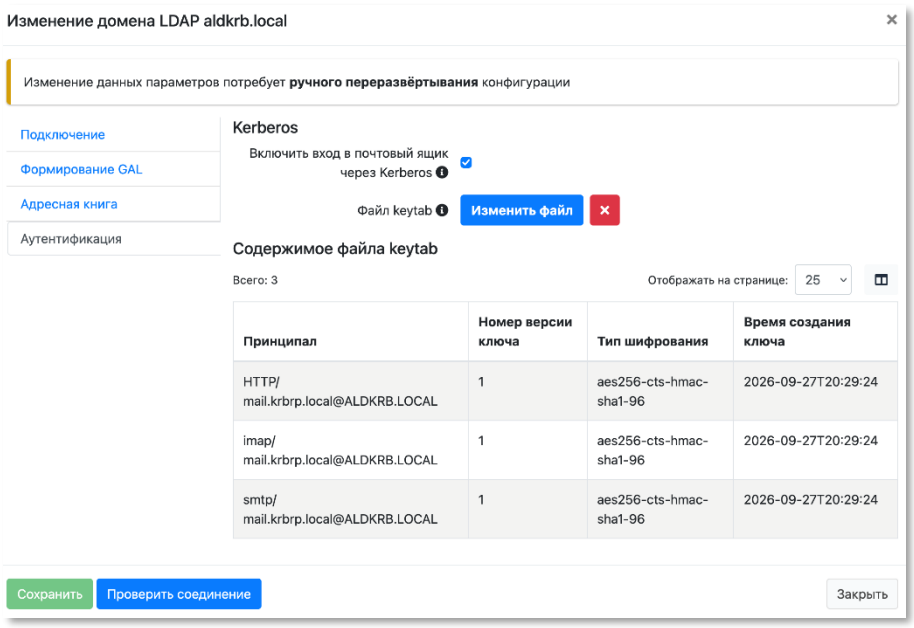
© 2021-2026 РуПост

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.

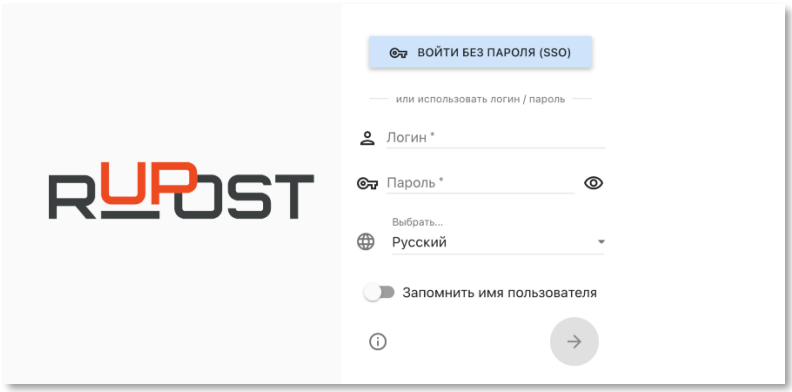
Настройки Kerberos в Панели управления

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.

Изменение расположения почтовых компонентов

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`.

Логи этих компонентов находятся в соответствующих подпапках папки `/var/log/rupost`.

Обновление версий почтовых компонентов

В версии 4.3.4 были обновлены следующие компоненты:

- **rupost-mda** (Dovecot) до версии 2.4.5
- **rupost-mua** (SOGo) до версии 5.12.12
- **rupost-mp** (NGinx) до версии 1.31.6

Улучшения и исправления

#47854 Защита от уязвимости сертификатов eMudhra.
#47207 Генерация имени конфигурации на сервере.
#47205 Откорректирован текст ошибки при обновлении почтового ящика.
#47128 Экземпляры: если время обновления статуса узла превышает 5 минут, то устанавливаем желтый цвет фона.
#46967 Обновление механизма управления правами доступа к почтовомцу ящику.
#46924 Изменены параметры кеширования для NFS.
#46788 Расширена обработка ошибок в установщике.
#46719 Оптимизирована обработка списка ящиков для данной политики архивирования.
#46534 Расширена обработка ошибок при создании подписи.
#46478 Оптимизировано кеширование записей для динамических списков рассылки.
#46421 Логи: Установлен период по умолчанию 60 секунд.
#46398 Общие почтовые ящики: Настройки доступа вынесены в отдельную вкладку.
#46396 Групповые политики: Расширена обработка ошибок при сохранении.
#46357 Оптимизировано выполнение фоновых задач холодной репликации.
#46316 Rupost-mua: удалены дополнительные HTML теги в подписи.
#46297 Rupost-mua: добавлено отображение полного имени пользователя при автоответе.
#46255 PGPool: запрет установки значения num_init_children через CLI команду.
#46175 Rupost-mua: добавлена локализация полей CC и BCC.
#46165 Общие настройки / Аутентификация: замаскирован ввод в поле "Секретный ключ".
#46104 Расширена обработка ошибок при выполнении фоновых задач.
#45948 Rupost-mua: сохранение состояния подпапок при создании новой папки
#45915 Оптимизировано отображение адресатов динамического списка рассылки.
#45841 Секрвис рассылок: оптимизирована доставка сообщений по LMTP.
#45730 Транспортные правила: расширены возможности по указанию расширений файлов.
#45640 Расширена проверка прав на корневые каталоги почтовых ящиков при горячей репликации.
#45509 Rupost-mua: исправлена переименование почтовых папок.
#45508 Rupost-mua: исправлено удаление одного события из ряда (внешний организатор).

© 2021-2026 РуПост

#45506 Экземпляры: кнопка "Действия над всеми экземплярами" скрыта при наличии только одного узла.
#45505 Rupost-mda: при превышении частной квоты на размер письма возвращаем постоянный ответ.
#45492 CalDAV: устранен сбой синхронизации, когда UID события содержит символ "_".
#45351 Геокластер: исправлено распространение настроек типа "глобальные, переопределяемые" на ведомые сайты.
#45311 Rupost-mua: исправлена ошибка загрузки вложения при создании календарного события.
#45297 Rupost-mua: добавлена локализация настройки "Показывать вложения над письмом".
#45170 Списки рассылки: Добавлена пагинация в предпросмотр получателей/отправителей в динамическом списке рассылки.
#45062 Трассировка: расширена обработка ошибок.
#44982 Изменен формат вывода информации команды CLI "rupost admins list".
#44981 Расширение набора параметров лога аудита.
#44853 Транспортные правила: Добавлена возможность ввода дробных чисел для размера вложения.
#44781 Расширена обработка выхода из строя горячей реплики.
#44780 Добавлена поддержка сертификатов, содержащих пробел в имени файла.
#44540 Транспортные правила: Увеличен лимит по количеству символов для поля расширений файлов.
#44536 Оптимизирован механизм эвакуации почтовых очередей.
#44451 Отзыв писем: добавлена возможность отозвать письмо, отправленное на псевдоним.
#44441 Геокластер: оптимизирован механизм синхронизация сайтов.
#44293 Адресная книга: исключены записи с некорректным первичным адресом.
#44285 Rupost-mua: добавлена возможность сохранить подпись в режиме отображения HTML кода.
#44174 Почтовые домены: откорректирована проверка наличия домена при повторном создании.
#44173 Мониторинг: исправлено отображение статуса почтовых доменов, когда есть удаленные.
#44108 Экземпляры: Добавлена возможность скопировать UUID или IP-адрес экземпляра.
#44022 Общие почтовые ящики: настройки групповых политик вынесены на отдельную вкладку “Групповые политики”.
#44008 Отзыв писем: разрешен отзыв писем, отправленных от имени общего почтового ящика.
#43789 Трассировка: отображение событий трассировки письма при не заполненном поле "Отправитель".
#43757 Общие настройки / Аутентификация: добавлена кнопка "Проверить соединение".
#43726 Memcached: добавлена защита встроенного Memcached от доступа извне (не с узлов кластера).
#43400 Оптимизировано архивирование почтовых ящиков.
#43337 Расширена обработка точек монтирования NFS при остановке сервиса rupost.
#43248 Фильтры LDAP: откорректирован подсчет количества почтовых ящиков при проверке фильтра LDAP во время его добавления.
#43231 Добавлена команда CLI "local-restore" для локального восстановление очереди.
#42874 Rupost-mua: Запрет на изменение календаря при изменении одного вложения серии событий.
#42541 Мониторинг: Добавление информации о расположении хранилища.
#42500 Добавлен параметр csv в команду CLI "rupost mailbox list --search".
#42480 LDAP домен: добавлен поиск в адресной книге для предпросмотра карточки контакта.
#42473 LDAP домены: расширена проверка условий успешности подключения.
#42454 Общие настройки: добавлена проверка на корректность введенного адреса инструмента миграции.
#42453 Rupost-mua: добавлено маскирование реквизитов подключения к базе данных в логах.
#42364 Расширена обработка ошибок при переименовании ящика, когда к нему предоставлен доступ другим пользователям.
#42213 Перенесены команды CLI из группы "mailboxes" в группу "mailbox".

© 2021-2026 РуПост

#42058 Удалена устаревшая группа команд CLI "restrictions".
#41915 Rupost-mua: добавлена обработка ошибок при выходе пользователя из системы, когда используется OpenID.
#41331 Оптимизировано разворачивание конфигурации почтовых компонентов.
#41294 Устранена возможность входа в почтовый ящик после удаления.
#41060 Геокластер: расширена обработка ошибок при перемещении почтового ящика между сайтами.
#40839 Устранена возможность развертывания кластера при использовании локального хранилища.
#40834 Добавлена дополнительная проверка условий автостарта узла.
#40760 Геокластер: оптимизирована работа динамических списков рассылки.
#40325 Транспортные правила: добавлена возможность выбора нескольких фильтров LDAP.
#40297 Групповые политики: добавлена проверка на уникальность назначения политики каждого типа для почтового ящика.
#39861 Исправлен вывод команды CLI "rupost admins permissions list mailadmin --csv" для суперадминистратора.
#39556 Исправлена ошибка импорта почтовых ящиков из csv при наличии данных в LDAP в разных регистрах.
#38988 Расширена проверка доступности LDAP домена при добавлении через CLI.
#38759 Исправлено разворачивание конфигурации через CLI при наличии локального хранилища.
#37127 Откорректирован шаблон письма-оповещения о превышении квоты.
#34452 Логи: Добавлена возможность указать диапазон времени для получения логов.
#33326 Расширена обработка ограничений для писем, отправленных на псевдоним.
#29567 Фильтры ящиков: расширен поиск пользователей и фильтров LDAP
#14980 Расширена обработка ошибок при повторной попытке создания почтового ящика из LDAP.
#9703 Добавлено сообщение об успешной эвакуации очереди выведенного из эксплуатации узла.

Приложение. Настройка инфраструктуры Kerberos

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.

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`

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)
```

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)
```

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
```

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

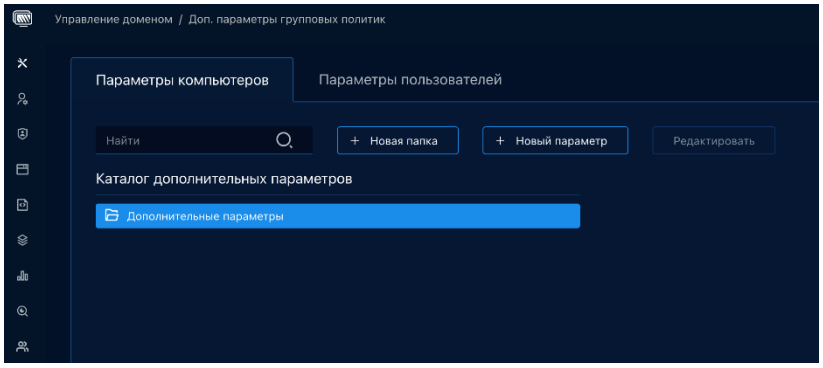
Или на английском:

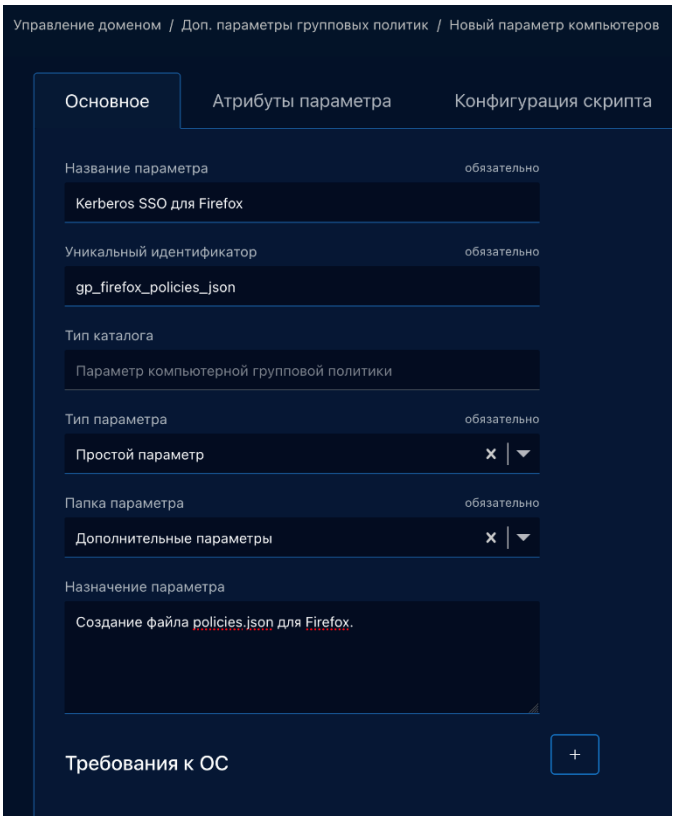
Computer Configuration →
Policies →
Administrative Templates →
FireFox →
Authentication

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'
```

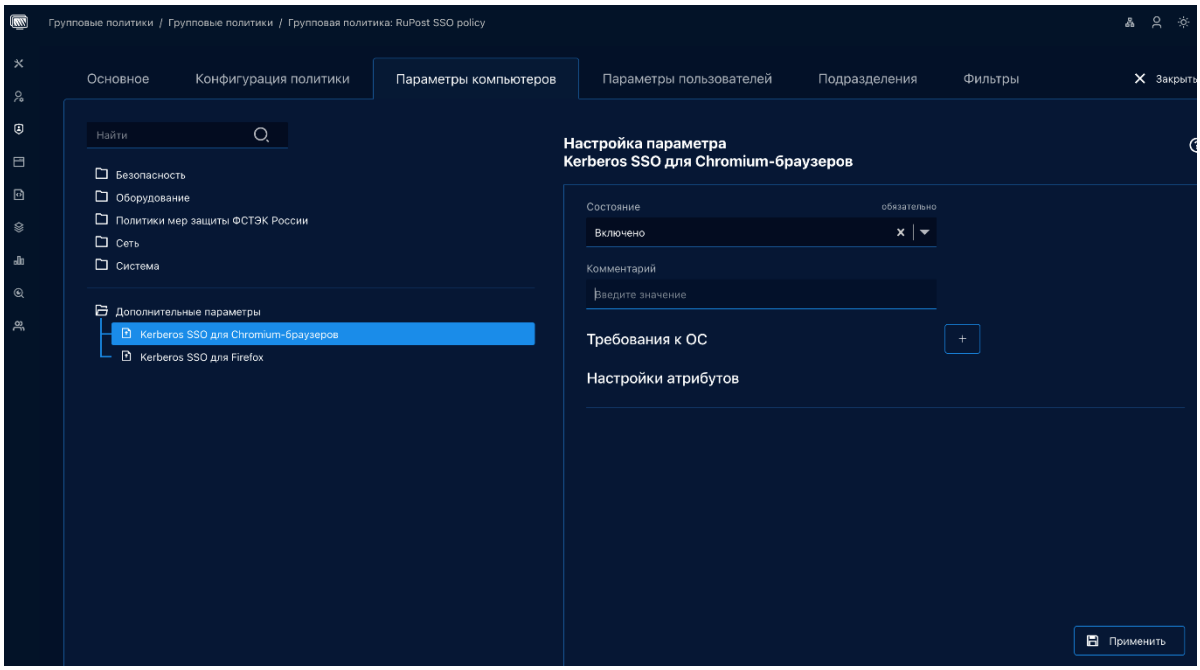
```
    - backup: minion
    - contents: |
        {
          "policies": {
            "Certificates": {
              "ImportEnterpriseRoots": true,
              "Install": [
                "/etc/ipa/ca.crt"
              ]
            },
            "Authentication": {
              "SPNEGO": [
                "mail.krbrp.local"
              ]
            }
          }
        }
    - require:
      - file: aldpro_firefox_distribution_directory
```

Для браузеров на основе Chrome создать отдельный параметр и в конфигурация скрипта указать:

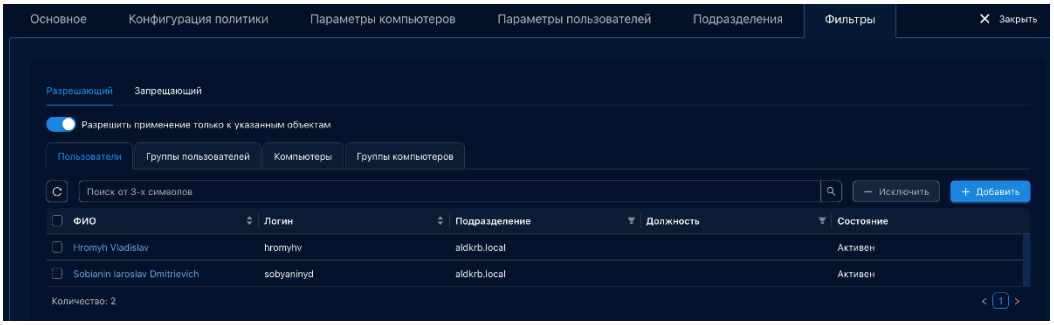
```
aldpro_yandex_policy_directory:
  file.directory:
    - name: /etc/opt/yandex/browser/policies/managed
    - user: root
    - group: root
    - mode: '0755'
    - makedirs: true
    - onlyif:
      - /usr/bin/test -x /usr/bin/yandex-browser

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'
```

Настройка браузеров для компьютеров вне домена

Настройка Safari (macOS)

После настройки Kerberos на уровне операционной системы, браузер Safari дополнительных настроек не требует.

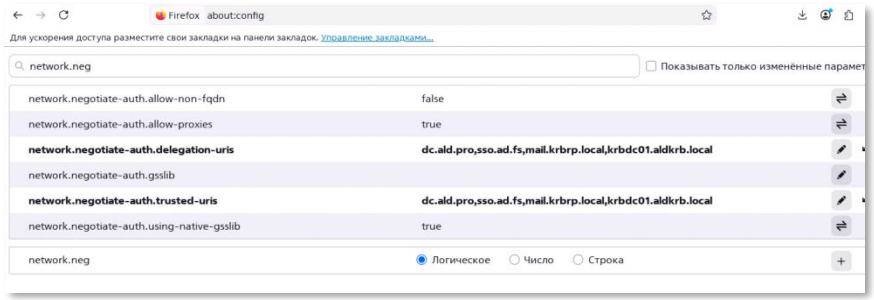
Настройка Firefox

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
```

