МойОфис Профессиональный 3

Руководство по администрированию

ПОЧТОВАЯ СИСТЕМА

© ООО «НОВЫЕ ОБЛАЧНЫЕ ТЕХНОЛОГИИ», 2013–2024

ООО «НОВЫЕ ОБЛАЧНЫЕ ТЕХНОЛОГИИ»

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ «МОЙОФИС ПРОФЕССИОНАЛЬНЫЙ 3» ПОЧТОВАЯ СИСТЕМА

3.1

РУКОВОДСТВО ПО АДМИНИСТРИРОВАНИЮ

Версия 1

На 115 листах

Дата публикации: 27.08.2024

Москва
2024

Все упомянутые в этом документе названия продуктов, логотипы, торговые марки и товарные знаки принадлежат их владельцам.

Товарные знаки «МойОфис» и «MyOffice» принадлежат ООО «НОВЫЕ ОБЛАЧНЫЕ ТЕХНОЛОГИИ».

Ни при каких обстоятельствах нельзя истолковывать любое содержимое настоящего документа как прямое или косвенное предоставление лицензии или права на использование товарных знаков, логотипов или знаков обслуживания, приведенных в нем. Любое несанкционированное использование этих товарных знаков, логотипов или знаков обслуживания без письменного разрешения их правообладателя строго запрещено.

© ООО «НОВЫЕ ОБЛАЧНЫЕ ТЕХНОЛОГИИ», 2013–2024

СОДЕРЖАНИЕ

© ООО «НОВЫЕ ОБЛАЧНЫЕ ТЕХНОЛОГИИ», 2013–2024

© ООО «НОВЫЕ ОБЛАЧНЫЕ ТЕХНОЛОГИИ», 2013–2024

© ООО «НОВЫЕ ОБЛАЧНЫЕ ТЕХНОЛОГИИ», 2013–2024

© ООО «НОВЫЕ ОБЛАЧНЫЕ ТЕХНОЛОГИИ», 2013–2024

© ООО «НОВЫЕ ОБЛАЧНЫЕ ТЕХНОЛОГИИ», 2013–2024

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

В настоящем документе используются следующие сокращения (см. таблицу 1).

Таблица 1 – Сокращения и расшифровки

Сокращение	Расшифровка и определение
389-ds	389 Directory Server, служба каталогов
API	Application Programming Interface, интерфейс программирования приложений
AD	Active Directory
CO	CloudOffice, Облачный Офис, общее название продукта (группы редакторов)
Docker	Программное обеспечение для автоматизации развертывания и управления приложениями в средах с поддержкой контейнеризации
Doveadm	Инструмент администрирования сервиса Dovecot
DN	Distinguished Name - уникальное имя объекта в нотации LDAP
IMAP	Internet Messagess Access Protocol, протокол доступа к ящику электронной почты
LDAP	Lightweight Directory Access Protocol, облегченный протокол доступа к каталогам
Node (нода)	Сервер одной из ролей
PBM	Poseidon Backend Manager, внутренний сервис конфигурирования
PGS	File Storage, Pythagoras, программный продукт «МойОфис Хранилище»
PPS	Postfix Policy Server, сервис политик для Postfix

© ООО «НОВЫЕ ОБЛАЧНЫЕ ТЕХНОЛОГИИ», 2013–2024

1 ОБЩИЕ СВЕДЕНИЯ

1.1 Назначение

«МойОфис Профессиональный 3» – продукт для организации безопасного хранения файлов, совместной работы с документами, ведения переписки по электронной почте и планирования рабочего времени в государственных организациях и крупных коммерческих предприятиях. В состав продукта входят:

- Система хранения данных для безопасного хранения корпоративных файлов и обеспечения возможностей авторизации, аутентификации и разграничения прав доступа пользователей;
- Система редактирования и совместной работы для индивидуального и совместного редактирования текстовых документов, электронных таблиц и презентаций;
- Почтовая система для обеспечения работы с почтовыми сервисами, календарями, личной и глобальной адресными книгами, а также инструментами управления задачами;
- Административная панель системы хранения для управления пользователями, группами, общими папками, доменами и тенантами.

Подробное описание возможностей продукта приведено в документе «МойОфис Профессиональный 3. Функциональные возможности».

В данном руководстве описано администрирование серверного программного обеспечения.

1.2 Системные требования

Перечень требований к программному и аппаратному обеспечению приведен в документе «МойОфис Почта 3. Системные требования».

1.3 Требования к квалификации

Администратор «МойОфис Почта» должен соответствовать следующим требованиям:

- администрирование информационных систем;
- техническое обслуживание средств вычислительной техники, на которых устанавливается ПО «МойОфис»;

© ООО «НОВЫЕ ОБЛАЧНЫЕ ТЕХНОЛОГИИ», 2013–2024

– опыт работы с операционными системами Linux, Windows, macOS.

Для работы с ПО «МойОфис» администратору необходимо ознакомиться со следующими документами:

– «МойОфис Почта. Руководство по администрированию»;
– RFC3501 (IMAP);
– RFC5321 (SMTP);
– RFC5322 (IMF).

© ООО «НОВЫЕ ОБЛАЧНЫЕ ТЕХНОЛОГИИ», 2013–2024

2 ОПИСАНИЕ ОПЕРАЦИЙ

Пользователи получают доступ к функциям административной панели через веб-браузер. Дополнительные возможности администрирования (более тонкая настройка) осуществляются через запросы к API, которые выполняются из любого места, откуда обеспечен доступ по сети. Посредством API поддерживается работа с такими сущностями, как пользователи, группы рассылок, ресурсы, тенанты и т.д. В таком случае авторизация администратора с настроенными правами доступа происходит при помощи получения токена авторизации (см. раздел Авторизация через PBM API).

В случае установки «МойОфис Почта» в качестве отдельного приложения, пользователи также получают доступ к функциям административной панели, в том числе через веб-браузер.

2.1 Запуск, остановка и перезагрузка системы

Запуск подсистемы осуществляется при инициализации и запуске аппаратной части программно-технического комплекса. Для выполнения команд остановки и перезагрузки системы администратору необходимо обеспечить ssh-доступ к серверам подсистем в контуре установки.

Остановка «МойОфис Почта» выполняется с любой ноды с помощью следующих консольных команд:

```
docker stack rm psn-backend psn-nginx-proxy psn-mail psn-frontend
psn-etcd psn-ldap psn-postgres psn-redis psn-syslog_ng <psn-monitoring>
```

Данная команда останавливает работу сервисов, относящихся к МойОфис Почта.

Параметр `<psn-monitoring>` используется в случае указания группы хостов monitoring инвентарного файла установки.

Для запуска остановленных компоненов необходимо с первой ноды роли proxy выполнить следующие команды

```
docker stack deploy -c /opt/poseidon/psn-postgres-stack.yml \
--with-registry-auth psn-postgres
docker stack deploy -c /opt/poseidon/psn-ldap-stack.yml \
--with-registry-auth psn-ldap
docker stack deploy -c /opt/poseidon/psn-back-stack.yml \
--with-registry-auth psn-backend
docker stack deploy -c /opt/poseidon/psn-front-stack.yml \
--with-registry-auth psn-frontend
```

© ООО «НОВЫЕ ОБЛАЧНЫЕ ТЕХНОЛОГИИ», 2013–2024

```
docker stack deploy -c /opt/poseidon/psn-mail-stack.yml \
--with-registry-auth psn-mail
docker stack deploy -c /opt/poseidon/psn-redis-stack.yml \
--with-registry-auth psn-redis
docker stack deploy -c /opt/poseidon/psn-proxy-stack.yml \
--with-registry-auth psn-nginx-proxy
docker stack deploy -c /opt/poseidon/psn-etcd.yml \
--with-registry-auth psn-etcd
docker stack deploy -c /opt/poseidon/ psn-syslog_ng-stack.yml \
--with-registry-auth psn-syslog_ng
<docker stack deploy -c /opt/poseidon/psn-monitoring.yml
--with-registry-auth psn-monitoring>
```

Команда `<docker stack deploy -c /opt/poseidon/psn-monitoring.yml --with-registry-auth psn-monitoring>` используется только в случае указания группы хостов monitoring инвентарного файла установки.

Перезапуск компонентов системы осуществляется командой следующего вида:

```
docker service update --force --with-registry-auth <service>
```

Где `<service>` – перезапускаемый сервис. Для получения списка запущенных сервисов необходимо выполнить следующую команду:

```
docker service ls --format {{.Name}}
```

2.2 Авторизация

2.2.1 Авторизация в административной панели

Для запуска административной панели «МойОфис» необходимо:

1. Открыть веб-браузер при активном сетевом подключении.
2. Ввести адрес административной панели «МойОфис» в адресную строку веб-браузера и осуществить переход по ссылке.

Административная панель «МойОфис» считается работоспособной, если в результате данных действий пользователя на экране отобразилась стартовая страница входа без выдачи сообщений о сбое в работе.

В случае, если административная панель открывается в составе МойОфис Профессиональный, на экране возникает панель логина (см. Рисунок 1).

© ООО «НОВЫЕ ОБЛАЧНЫЕ ТЕХНОЛОГИИ», 2013–2024

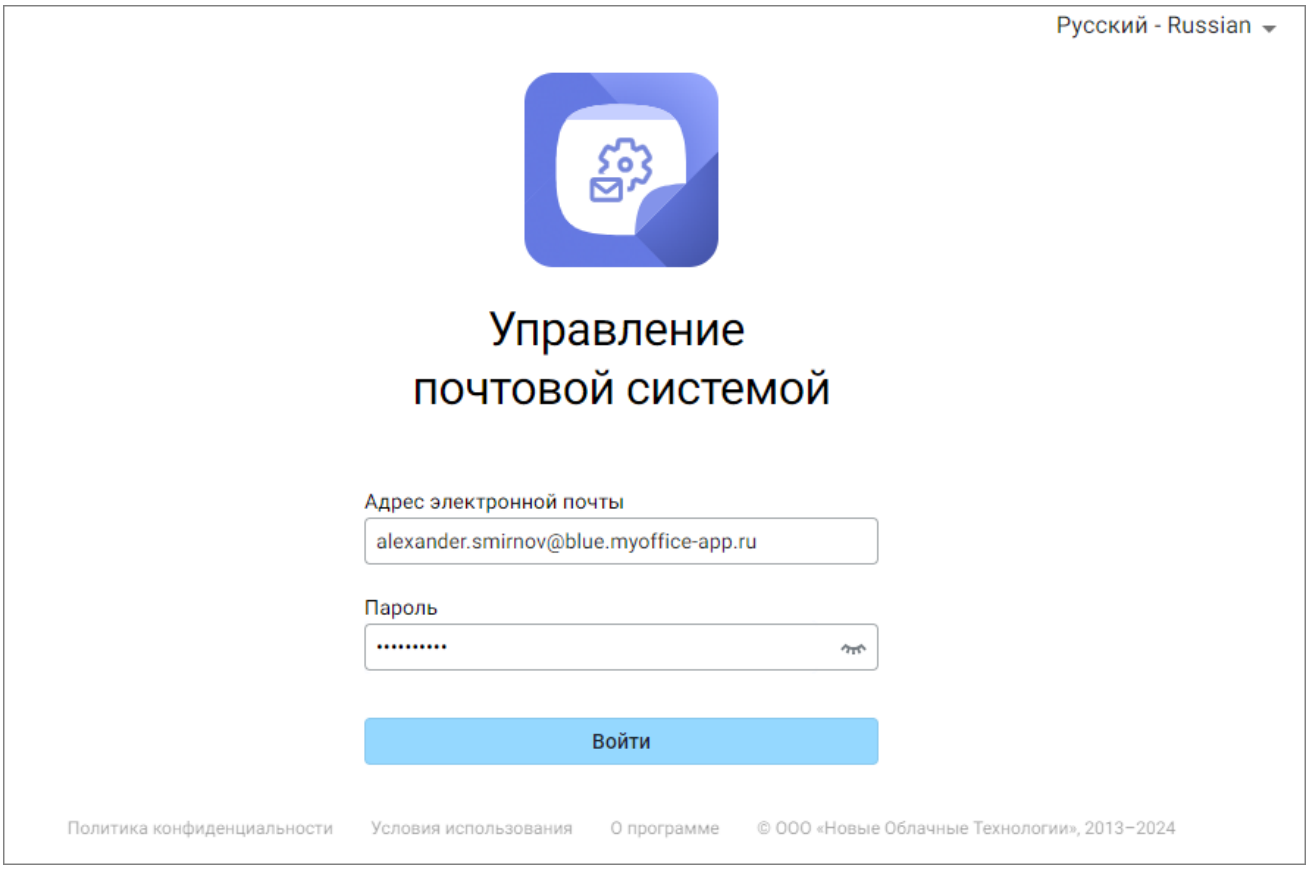


Рисунок 1 – Стартовая страница приложения в составе МойОфис

На стартовой странице представлены:

- управляющий элемент для смены языка с возможностью выбора из выпадающего списка;
- поля для ввода логина (адрес электронной почты) и пароля (для зарегистрированных пользователей с ролью «Администратор»);
- кнопка **Войти**.

В случае, если количество ошибочных входов превысит допустимое количество, на экране возникнет диалог защиты от робота, в котором необходимо ввести код с картинки (см. Рисунок 2).

© ООО «НОВЫЕ ОБЛАЧНЫЕ ТЕХНОЛОГИИ», 2013–2024

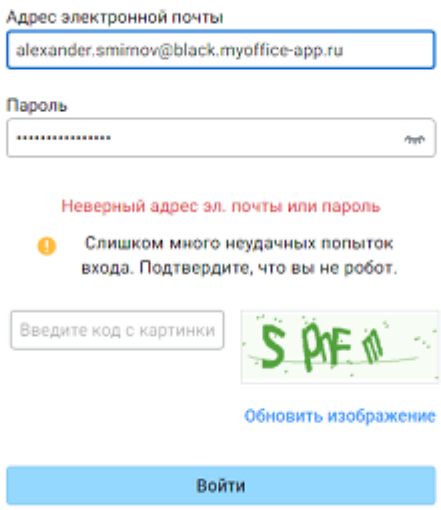


Рисунок 2 – Защита от повторного ввода

В случае, если авторизацию прошел пользователь, который является администратором тенанта, на экране откроется меню только для текущего тенанта (см. Рисунок 3).

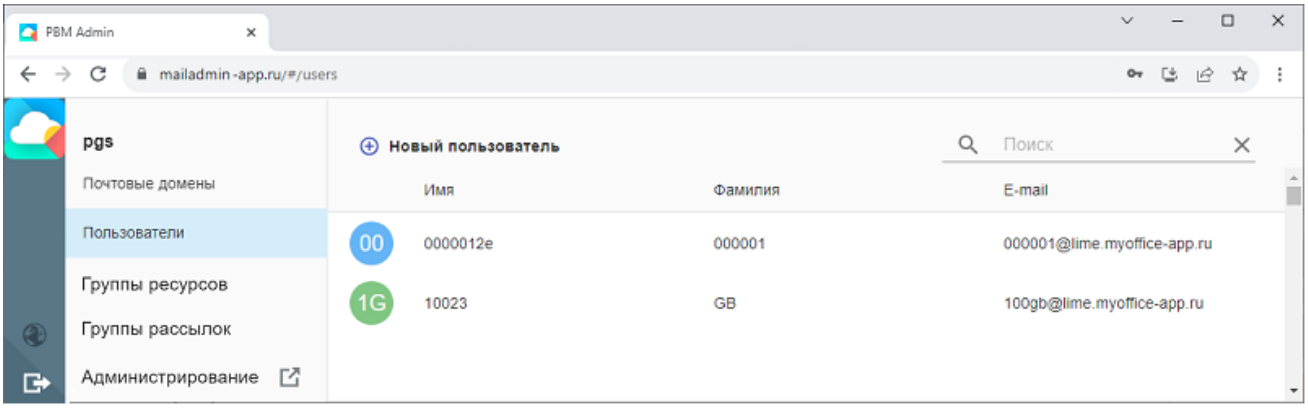


Рисунок 3 – Основной экран административной панели

Для администратора тенанта доступна кнопка **Администрирование**, которая переводит на экран логина панели администрирования PGS.

В случае, если авторизацию прошел пользователь, который является суперадминистратором почтовой системы, на экране откроется список всех доступных тенантов.(см. Рисунок 4).

© ООО «НОВЫЕ ОБЛАЧНЫЕ ТЕХНОЛОГИИ», 2013–2024

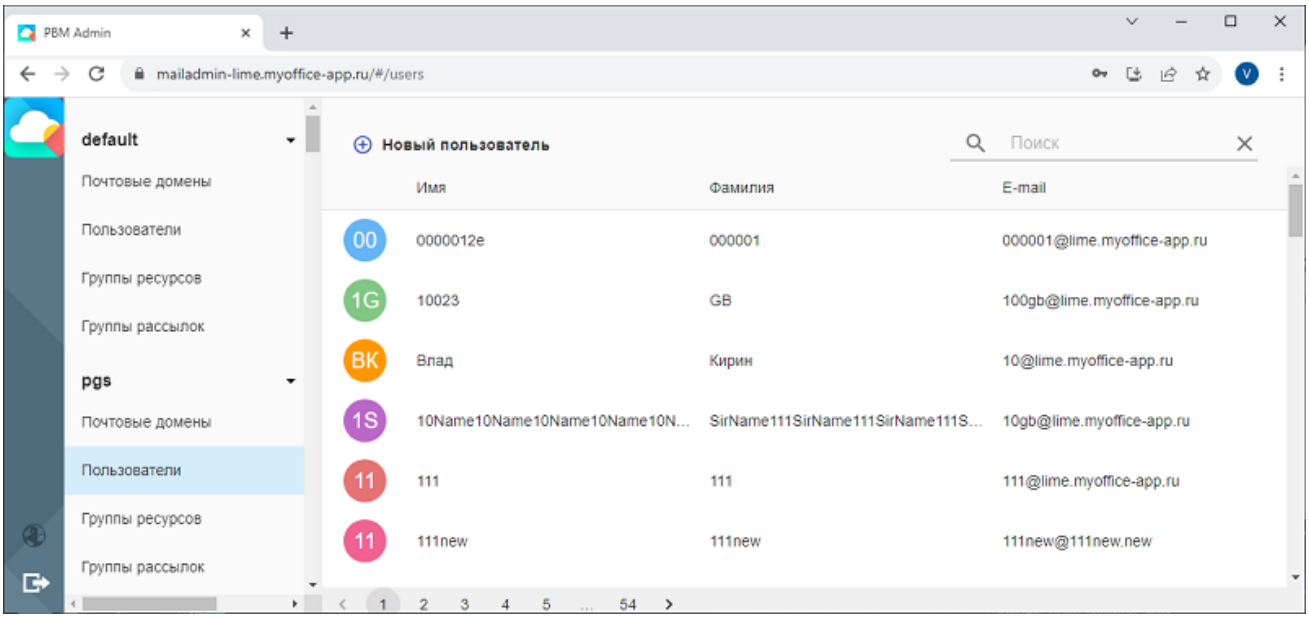


Рисунок 4 – Основной экран административной панели

На основном экране представлены:

- панель управления, содержащая кнопки (**Поменять язык**) и (Выход);
- в каждом из тенантов меню для перехода по разделам (**Почтовые домены**, **Пользователи**, **Группы ресурсов**, **Группы рассылок**);
- рабочая панель, отображающая текущий раздел;

При запуске приложения по умолчанию открывается панель **Пользователи**.

2.2.2 Авторизация через PBM API

Для того, чтобы начать работу через PBM API, необходимо осуществить авторизацию в Poseidon Backend Manager (PBM, внутренний сервис конфигурирования).

Для суперпользователя (creator) авторизация осуществляется со следующими параметрами:
Логин: creator@<domain>
Пароль: находится в переменной `ds389_manager_user` инвентарного файла (см. документ «МойОфис Почта 3. Руководство по установке почтового сервера 3.1», раздел «Конфигурирование инвентарного файла: переменные»).

© ООО «НОВЫЕ ОБЛАЧНЫЕ ТЕХНОЛОГИИ», 2013–2024

Для авторизации следует выполнить следующие действия:

1. Запустить консоль из любого места, где реализован доступ к «МойОфис Почта» по сети.
2. Получить токен авторизации, выполнив следующую команду для PBM API:

```
curl -X POST "https://<pbm_url>/v2/auth" \
-d "login=<login>" \
-d "password=<password>"
```

Где:

`<pbm_url>` – доменное имя сервера PBM (префикс будет иметь вид `pbm`, например `pbm.domain.com`);

`<login>` – логин пользователя (администратора), для которого выполняется авторизация;

`<password>` – пароль пользователя (администратора), для которого выполняется авторизация.

3. В случае успешного выполнения команды появится сообщение следующего вида (для PBM API):

```
{
 "access_token": "<access_token>",
 "refresh_token": "<refresh_token>",
 "expire": <expire_time>,
 "tenant-id": "<tenant-id>",
 "role": <role>
}
```

Где:

`<access_token>` – значение токена авторизации.

`<refresh_token>` – значение refresh-токена, необходимого для обновления токена авторизации.

`<expire_time>` – время жизни токена.

`<tenant-id>` – id тенанта, для которого создается токен авторизации.

`<role>` – роль авторизованного пользователя, для которого создается токен: **1** – администратор, **2** – пользователь, **3** – супер администратор.

© ООО «НОВЫЕ ОБЛАЧНЫЕ ТЕХНОЛОГИИ», 2013–2024

4. Полученный токен авторизации используется при работе с консолью следующим образом (для PBM API):

```
<request> -H "Authorization: Bearer <access token>"
```

Где `<request>` – сформированный запрос.

5. Полученный refresh-токен возможно использовать следующим образом:

```
curl -X POST "https://<pbm_url>/v2/auth" \
-d "refresh_token=<refresh_token>"
-H "Authorization: Bearer <access_token>"
```

Такая команда позволяет обновить токен авторизации, не создавая новый. Результат операции будет аналогичен указанному выше.

2.3 Работа с тенантами

Тенант в «МойОфис Почта» – это логическая сущность, имеющая возможность использовать ресурсы и сервисы программного комплекса. По умолчанию, пользователи и ресурсы создаются в тенанте default. Работа с тенантами возможна только через PBM API пользователем роли супер администратор (см. раздел Авторизация).

2.3.1 Получение массива тенантов

Команда позволяет получить массив существующих в системе тенантов. Пример:

```
curl -X GET "https://<pbm_url>/v2/tenants" \
-H "Authorization: Bearer <access_token>"
```

2.3.2 Добавление тенанта

Для добавления тенанта в систему необходимо выполнить следующий запрос:

```
curl -X POST "https://<pbm_url>/v2/tenants" -d domain=<domain> \
-H "Authorization: Bearer <access_token>"
```

Где `<domain>` – обслуживаемый домен тенанта.

В указанном выше примере имя тенанта будет присвоено автоматически. Если необходимо создать тенант с указанным именем, следует применить следующий метод:

© ООО «НОВЫЕ ОБЛАЧНЫЕ ТЕХНОЛОГИИ», 2013–2024

```
curl -X PUT "https://<pbm_url>/v2/tenants/<tenant-id>" \
-d domain=<domain>
-H "Authorization: Bearer <access_token>"
```

Где `<tenant-id>` – имя (id) создаваемого тенанта.

2.3.3 Удаление тенанта

Тенант из системы удаляется следующей командой:

```
curl -X DELETE "https://<pbm_url>/v2/tenants/<tenant-id>" \
-H "Authorization: Bearer <access_token>"
```

Параметр `<tenant-id>` – обязателен.

2.3.4 Список тенантов в административной панели

Работа с тенантами (организациями) в административной панели реализована только для пользователя, являющегося суперадминистратором.

В случае, если пользователь авторизован от имени суперадминистратора:

1. Пользователю доступен раздел **Настройки** / **Список организаций** (см. Рисунок 5). При выборе данного раздела на экране появляется список тенантов (организаций).

© ООО «НОВЫЕ ОБЛАЧНЫЕ ТЕХНОЛОГИИ», 2013–2024

2. В левой панели отображается список тенантов, каждый из них имеет структуру:
   - Почтовые домены;
   - Пользователи;
   - Группы ресурсов;
   - Группы рассылки.

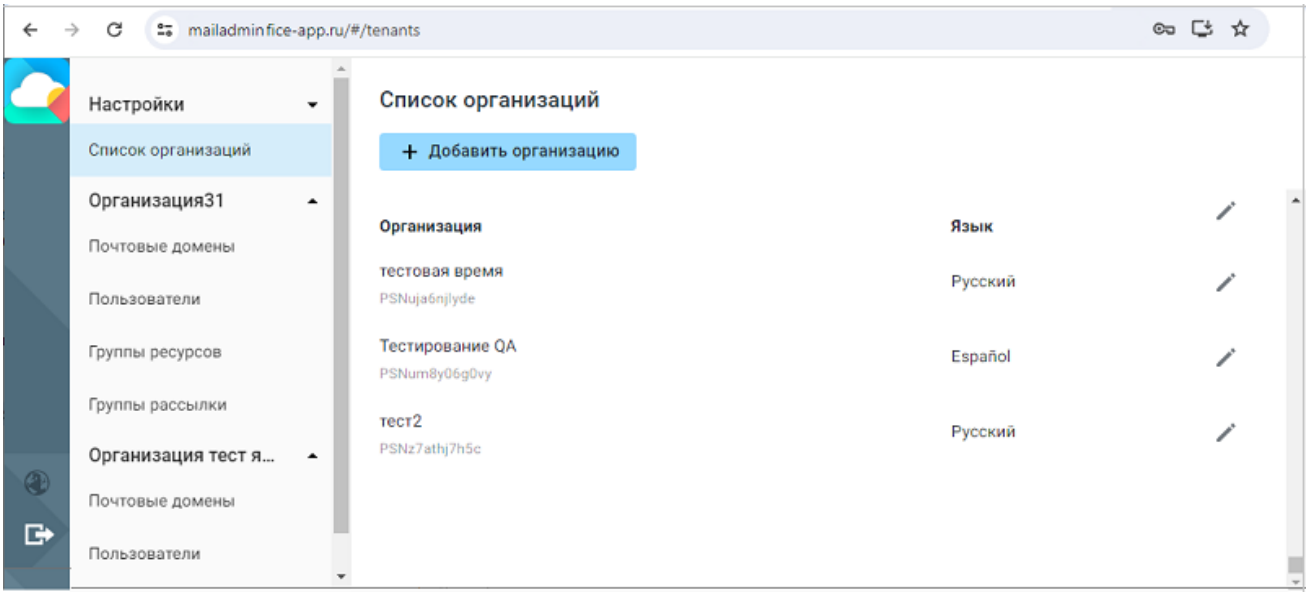


Рисунок 5 – Список тенантов (организаций)

2.3.5 Добавление тенанта в административной панели

Для добавления нового тенанта (организации) необходимо нажать **Добавить организацию**. На экране возникнет панель ввода (см. Рисунок 6).

© ООО «НОВЫЕ ОБЛАЧНЫЕ ТЕХНОЛОГИИ», 2013–2024

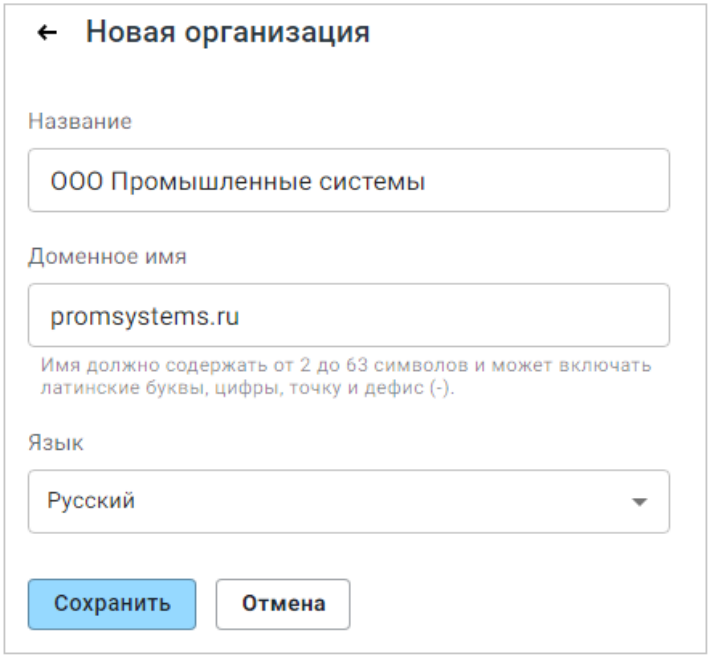


Рисунок 6 – Создание организации

После ввода названия и доменного имени следует нажать **Сохранить**.

1. На экране появится сообщение «Организация добавлена».
2. Новый тенант (организация) появится в списке организаций.
3. Структура новой организации появится в дереве организаций в составе следующих элементов:
   - Почтовые домены;
   - Пользователи;
   - Группы ресурсов;
   - Группы рассылки.

2.3.6 Изменение тенанта в административной панели

Для редактирования записи тенанта (организации) необходимо нажать нажать на строку в списке тенантов, либо кнопку . На экране откроется диалоговая панель редактирования записи тенанта (см. Рисунок 7).

© ООО «НОВЫЕ ОБЛАЧНЫЕ ТЕХНОЛОГИИ», 2013–2024

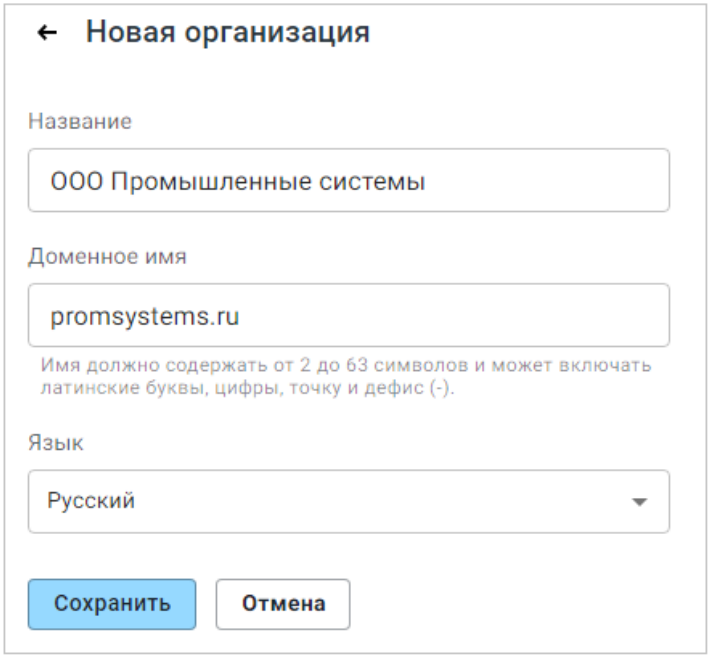


Рисунок 7 – Редактирование тенанта

После ввода названия и доменного имени нажать **Сохранить**, параметры тенанта (организации) будут обновлены в списке.

2.4 Работа с пользователями

Для работы с пользователями тенанта (организации) необходимо перейти в раздел **Пользователи**, на экране отобразится панель со списком пользователей (см. Рисунок 8):

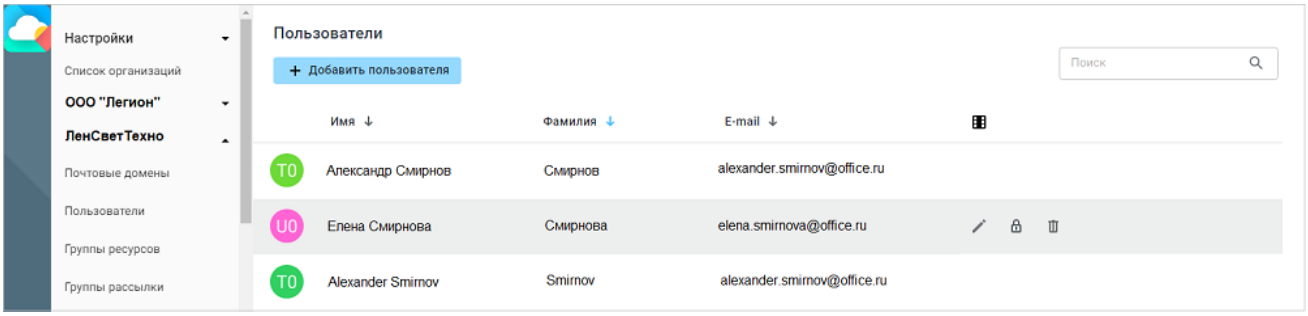


Рисунок 8 – Список пользователей

По умолчанию список пользователей включает столбцы: **Имя**, **Фамилия**, **E-Mail**. Заголовки столбцов содержат символы стрелок для указания направления сортировки. Стрелка, отображающая текущую сортировку, подсвечена синим цветом. При нажатии на заголовок производится сортировка по выбранному столбцу. Направление сортировки изменяется при каждом нажатии на заголовок.

© ООО «НОВЫЕ ОБЛАЧНЫЕ ТЕХНОЛОГИИ», 2013–2024

Существует возможность включения дополнительных отображаемых столбцов. При нажатии на кнопку на экране возникает панель включения / выключения дополнительных столбцов (см. Рисунок 9):

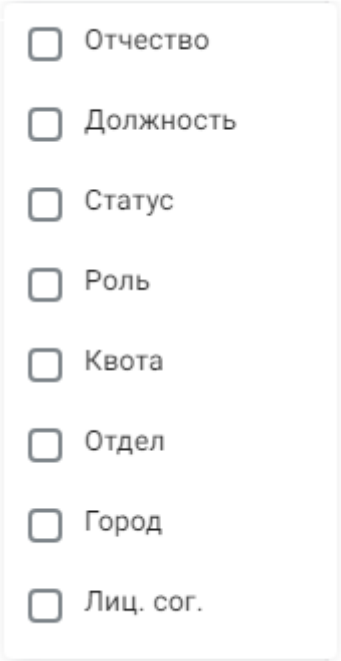


Рисунок 9 – Выбор отображаемых столбцов

При включении или выключении столбцов в данной панели настройки в списке пользователей будут добавляться или скрываться дополнительные столбцы.

2.4.1 Добавление пользователя

2.4.1.1 Добавление пользователя в административной панели

Для создания нового пользователя необходимо перейти в раздел **Пользователи** и нажать кнопку **Новый пользователь**. На экране откроется панель ввода данных нового пользователя (см. Рисунок 10):

© ООО «НОВЫЕ ОБЛАЧНЫЕ ТЕХНОЛОГИИ», 2013–2024

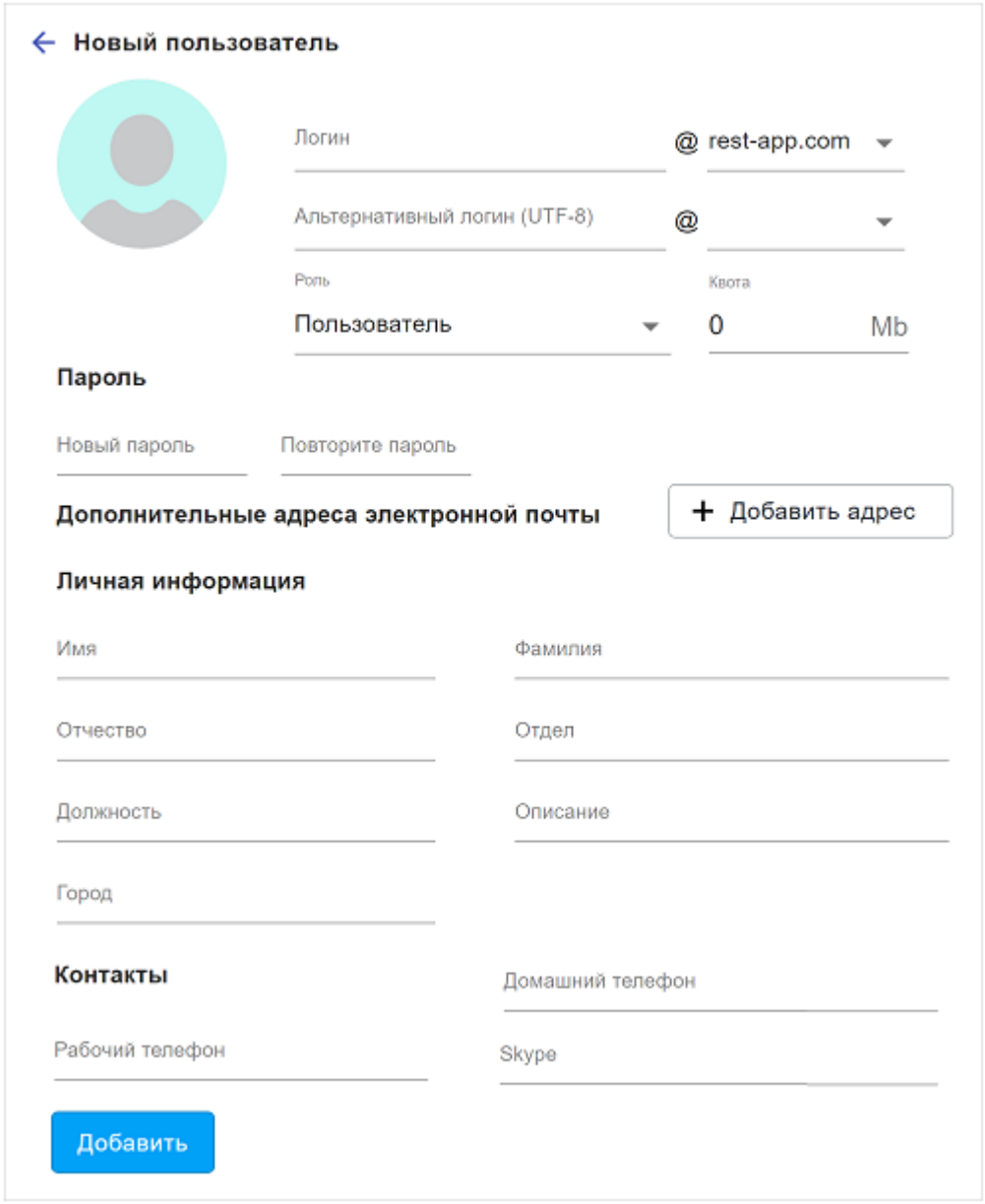


Рисунок 10 – Панель ввода данных нового пользователя

Для заполнения профиля пользователя доступны следующие поля:

1. Изображение («аватар») пользователя. Для выбора изображения необходимо кликнуть в область аватара.
2. Поле **Логин** для ввода логина пользователя с использованием латиницы.
3. Выпадающий список для выбора домена логина.
4. Поле **Альтернативный логин (UTF-8)** для ввода логина с использованием кириллицы.
5. Выпадающий список для выбора домена альтернативного логина.

© ООО «НОВЫЕ ОБЛАЧНЫЕ ТЕХНОЛОГИИ», 2013–2024

6. Выпадающий список для выбора роли, доступны варианты **Пользователь** или **Администратор**.
7. Поле **Квота**, содержащее размер (в Мбайт), ограничивающий размер хранилища писем.
8. Поля для ввода и проверки пароля пользователя: **Новый пароль**, **Повторите пароль**.

Требования к паролю (можно изменить, см. главу Настройка ETCD):

- минимальная длина: 6 символов;
- максимальная длина: 128 символов;
- минимальное количество цифр: 1 цифра;
- допустимые символы: латинские буквы, цифры, спецсимволы (их наличие в пароле необязательно): -_!@#$%^&*();
- пароль не должен содержать кириллицу.

9. Раздел **Дополнительные адреса электронной почты** для добавления дополнительных почтовых адресов (алиасов).
10. Поля для заполнения личных данных пользователя **Личная информация**
11. Поля для заполнения контактной информации в разделе **Контакты**.
12. Для завершения создания профиля пользователя необходимо нажать кнопку **Добавить** или кнопку , расположенную в левом верхнем углу формы ввода для отмены создания пользователя.

Администратору доступны все действия, рассматриваемые в настоящем руководстве, ограничений на количество администраторов «МойОфис» нет.

В результате операции новый пользователь будет отображен в списке пользователей.

2.4.1.2 Добавление пользователя через PBM API

Добавление пользователей в БД также может быть произведено при помощи PBM API. Обязательная информация, указываемая при создании нового пользователя, приведена в таблице 2.

© ООО «НОВЫЕ ОБЛАЧНЫЕ ТЕХНОЛОГИИ», 2013–2024

Таблица 2 – Обязательная информация при создании пользователя

Параметр	Расшифровка
`mail`	Почтовый ящик
`mailAlternateAddress`	Альтернативный логин (UTF-8)
`userPassword`	Пароль (требования к паролю можно изменить, см. главу Настройка ETCD)
`employeeNumber`	Роль создаваемого пользователя. Можно указать следующие значения: **1** - администратор, **2** - обычный пользователь, **3** - супер администратор
`tenant-id`	Тенант пользователя
`cn`	Имя
`sn`	Фамилия

Пример заполнения дополнительной информации о пользователе приведен в таблице 3.

Таблица 3 – Дополнительная информация при создании пользователя

Параметр	Расшифровка
`employeeType`	Видимость пользователя в адресной книге. Возможные значения: **0** - не виден в разделе «Коллеги», но виден в списке автозаполнения, **1** - виден в адресной книге и в списке автозаполнения, **2** - не виден, **3** - виден в разделе «Коллеги», но не виден в списке автозаполнения.
`initials`	Отчество
`ou`	Отдел
`title`	Должность
`alias`	Дополнительные адреса электронной почты (почтовые алиасы). Указываются через запятую без пробела
`description`	Описание
`homePhone`	Домашний номер телефона. Используются только цифры и специальные символы

© ООО «НОВЫЕ ОБЛАЧНЫЕ ТЕХНОЛОГИИ», 2013–2024

Параметр	Расшифровка
`telephoneNumber`	Рабочий номер телефона. Используются только цифры и специальные символы
`l`	Город
`telegram`	Telegram
`skype`	Skype
`quota`	Квота занимаемого почтовым ящиком пространства, отличная от квоты по умолчанию. Используются только цифры, размер задается в байтах
`displayName`	Отображаемое в адресной книге имя
`inetUserStatus`	Статус блокировки пользователя. Доступные значения: **0** - заблокирован; **1** - разблокирован, **2** - пользователь заблокирован и не принял пользовательское соглашение. Пользователь со статусом **2** не может отправлять и просматривать почту, только принимать. Значение по умолчанию - **2**
`lang`	Язык пользователя, доступные значения: **en-US** (значение по умолчанию), **ru-RU**, **es-PA**, **fr-FR**, **it-IT**, **pt-BR**, **ba-RU**, **tt-RU**

Пример создания пользователя с ролью администратор (**1**) в тенанте по умолчанию `<tenant-id>`, почтовым ящиком `<mail>`, паролем `<password>`, именем и фамилией `<name>` и `<surname>` соответственно:

```
curl -X PUT "https://<pbm_url>/v2/users/<tenant-id>/<mail>" \
-d "userPassword=<password>" -d "employeeNumber=1" \
-d "cn=<name>" -d "sn=<surname>"\
-H "accept: application/json" \
-H "Authorization: Bearer <access_token>"
```

При успешном выполнении запрос вернет следующий ответ:

```
{
  "success": true
}
```

© ООО «НОВЫЕ ОБЛАЧНЫЕ ТЕХНОЛОГИИ», 2013–2024

2.4.2 Поиск пользователя

2.4.2.1 Поиск пользователей в административной панели

Для поиска пользователей используется поисковая строка, расположенная в верхней части панели раздела **Пользователи**.

Чтобы осуществить поиск, необходимо перейти в раздел **Пользователи**, ввести запрос в поисковую строку **Поиск** и нажать **ENTER**.

Результат, соответствующий введенному запросу, будет отображен в списке пользователей.

Для выхода из режима поиска и возврата к исходному списку пользователей следует нажать кнопку ✕.

2.4.2.2 Поиск пользователей через PBM API

Для получения списка пользователей необходимо выполнить cURL-запрос **GET** со следующими параметрами (см. таблицу 4):

Таблица 4 – Параметры запроса получения списка пользователей

Параметр	Расшифровка
`tenant-id`	Тенант пользователя (обязательный параметр)
`search`	Строка для поиска, работающая по значениям полей `mail`, `cn` и `sn`. Возвращает первую страницу с результатами и общее количество совпадений
`page`	Выбор страницы результата, не вместившегося на один экран
`sort`	Тип сортировки. **0** - по возрастанию (в алфавитном порядке), **1** - по убыванию (в обратном порядке)
`orderby`	Сортировка по значению указанного поля. Может принимать значения `mail`, `cn` и `sn`

При вызове команды без параметров будет возвращена первая страница списка пользователей, отсортированная по полю `mail`, а также их общее количество.

Пример команды, возвращающей первую страницу списка пользователей тенанта `tenant-id`, отсортированную по почтовому адресу:

© ООО «НОВЫЕ ОБЛАЧНЫЕ ТЕХНОЛОГИИ», 2013–2024

```
curl -X GET "https://<pbm_url>/v2/users/<tenant-id>?page=1&orderby=mail" \
-H "Authorization: Bearer <access_token>"
```

Для получения подробной информации о конкретном пользователе системы необходимо выполнить запрос с указанием почтового ящика этого пользователя. Обязательные к указанию параметры – `<mail>` и `<tenant-id>`. Пример:

```
curl -X GET "https://<pbm_url>/v2/users/<tenant-id>/<mail>" \
-H "Authorization: Bearer <access_token>"
```

В текущем релизе запрос всех пользователей может завершиться ошибкой `Internal server error`. Для исправления необходимо на всех нодах ldap выполнить следующие команды:

```
docker exec $(docker ps -qf name=ldap) dsconf localhost backend index \
add --index-type eq --attr tenant-id --reindex userRoot
docker exec $(docker ps -qf name=ldap) dsconf localhost backend index \
add --index-type eq --attr employeeNumber --reindex userRoot
docker exec $(docker ps -qf name=ldap) dsconf localhost backend index \
add --index-type eq --attr employeeType --reindex userRoot
```

2.4.3 Редактирование профиля пользователя

2.4.3.1 Редактирование профиля пользователя в административной панели

Для редактирования профиля пользователя необходимо перейти в раздел **Пользователи** нужного тенанта, далее воспользоваться одним из следующих способов:

- в списке пользователей навести курсор мыши на необходимую строку, далее нажать на кнопку ;
- левой клавишей мыши выбрать нужную запись в списке.

В открывшемся окне доступны поля профиля пользователя для внесения изменений (см. Рисунок 11).

© ООО «НОВЫЕ ОБЛАЧНЫЕ ТЕХНОЛОГИИ», 2013–2024

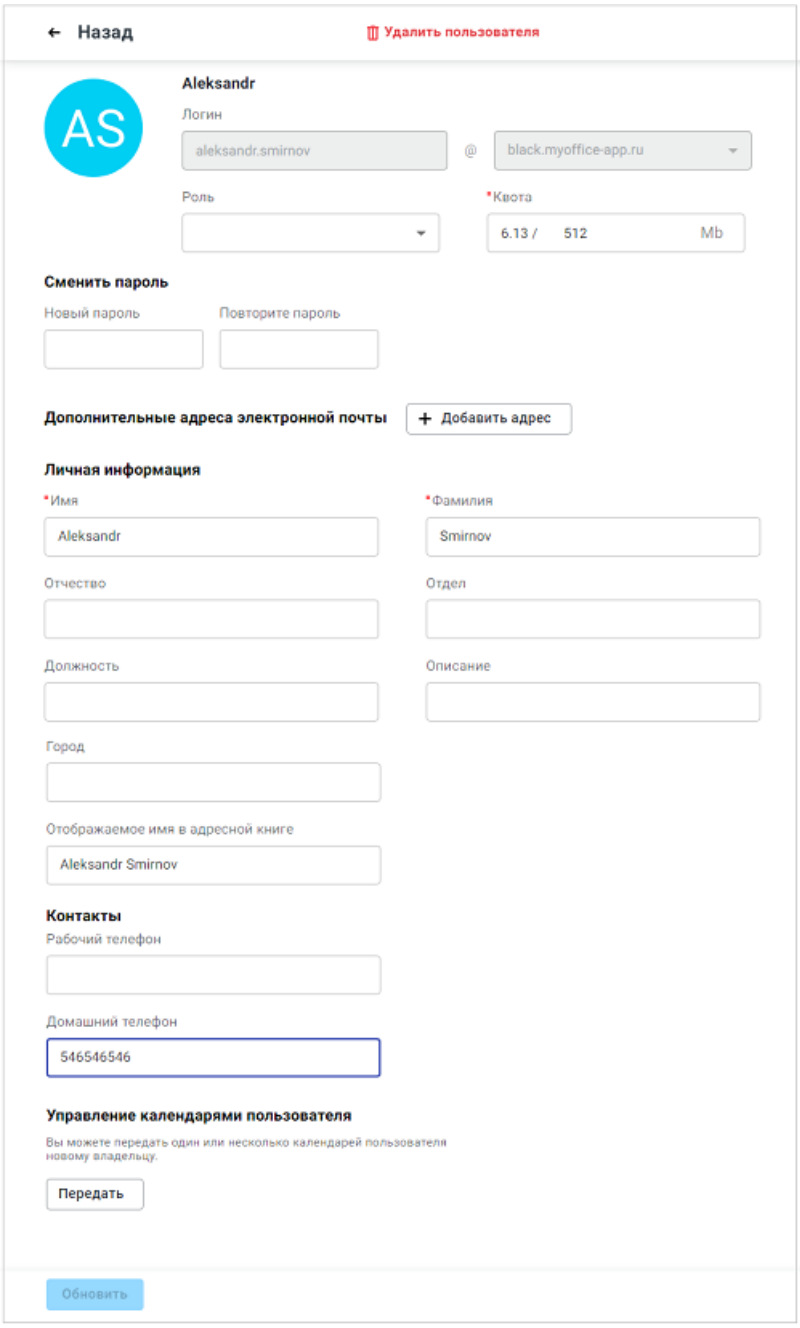


Рисунок 11 – Редактирование профиля пользователя

В панели редактирования пользователя присутствует раздел **Управление календарями пользователя**. Он дает возможность настраивать передачу календарей пользователя новому владельцу. При нажатии на кнопку **Передать** на экране появляется панель **Управление календарями пользователя** (см. Рисунок 12).

© ООО «НОВЫЕ ОБЛАЧНЫЕ ТЕХНОЛОГИИ», 2013–2024

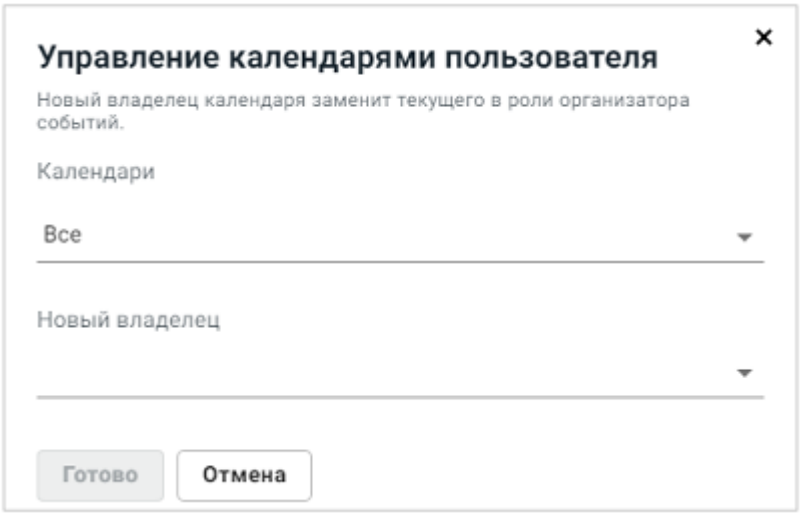


Рисунок 12 – Редактирование профиля пользователя

Для передачи календарей другому пользователю следует выбрать необходимые календари, а также нового владельца. После нажатия на кнопку **Готово** на экране появится сообщение «Календари пользователя переданы новому владельцу».

Для сохранения изменений в панели редактирования пользователя необходимо нажать кнопку **Обновить**, для выхода без изменений нажать кнопку ← **Назад**, расположенную в левом верхнем углу панели профиля.

2.4.3.2 Редактирование профиля пользователя через PBM API

Для обновления и корректировки полей уже созданных пользователей используется команда **PATCH**.

Обязательными параметрами, используемыми в запросе, являются `tenant-id` и `mail`, наименования остальных полей указаны в разделе Добавление пользователя через PBM API.

Пример команды, добавляющей поле `ou` со значением «Development» и обновляющей язык web-интерфейса `lang` на английский для пользователя <mail>:

```
curl -X PATCH "https://<pbm_url>/v2/users/<tenant-id>/<mail>" \
--data-raw '\
[{ "op": "add", "path": "/ou", "value": "Development" }, \
 { "op": "replace", "path": "/sn", "value": "MailTest" }]' \
-H 'Content-Type: application/json-patch+json' \
-H "Authorization: Bearer <access_token>"
```

При успешном выполнении запрос вернет следующий ответ:

© ООО «НОВЫЕ ОБЛАЧНЫЕ ТЕХНОЛОГИИ», 2013–2024

```
{
  "success": true
}
```

2.4.4 Блокировка пользователя

2.4.4.1 Блокировка пользователя в административной панели

В Административной Панели имеется возможность блокировки пользователей. Администратор при необходимости может заблокировать пользователя, после чего:

- пользователь не сможет войти в свою учетную запись;
- пользователь не будет получать новые письма;
- пересылка писем для данного пользователя станет недоступна (в случае, если была ранее настроена);
- пользователь не будет отображаться в списке контактов, подсказках в Почте, Календаре и т.д.;
- у пользователей, для которых заблокированный пользователь предоставил доступ к своим почтовым папкам, пропадет доступ к этим папкам;
- отправка писем от имени заблокированного пользователя станет недоступна (в случае, если была ранее настроена).

Для блокировки пользователя следует перейти в раздел **Пользователи** выбранного тенанта, далее воспользоваться одним из следующих способов:

- в списке пользователей навести курсор мыши на необходимую строку, далее нажать на кнопку 🔒;
- левой клавишей мыши выбрать нужную запись в списке, далее в открывшейся панели редактирования профиля нажать кнопку **Заблокировать** в верхней части окна.

На экране появится диалоговая панель, приведенная на рисунке 13.

© ООО «НОВЫЕ ОБЛАЧНЫЕ ТЕХНОЛОГИИ», 2013–2024

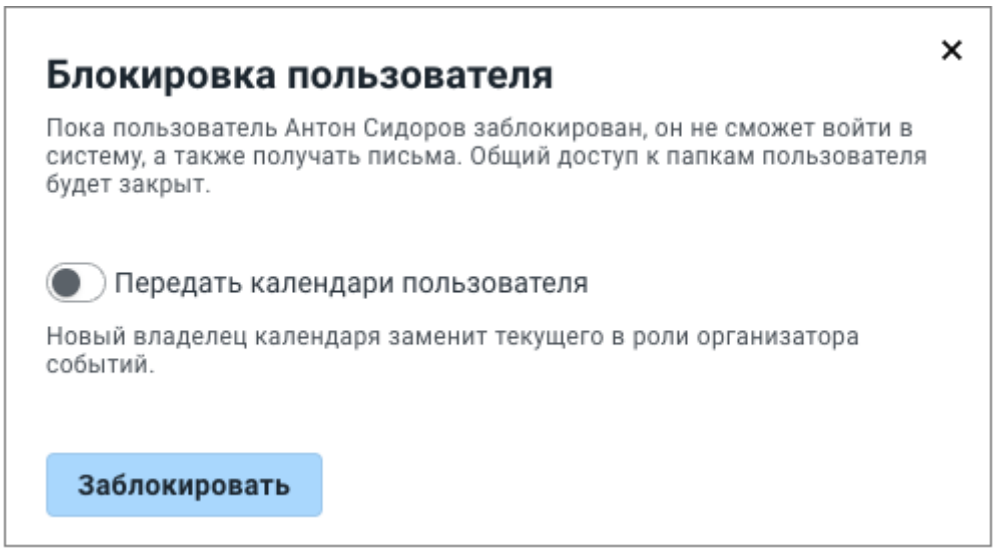


Рисунок 13 – Диалог блокировки пользователя

При блокировке пользователя предоставляется возможность передачи его календарей другому владельцу. Это связано с тем, что после удаления пользователя могут оставаться события, организатором которых он является. Смена владельца календаря подразумевает под собой смену организатора у подобных событий. При включении переключателя **Передать календари пользователя** на панели появляются поля для выбора календарей и их нового владельца (см. рисунок 14). После передачи календаря у другого владельца появляется возможность отменить / изменить встречи.

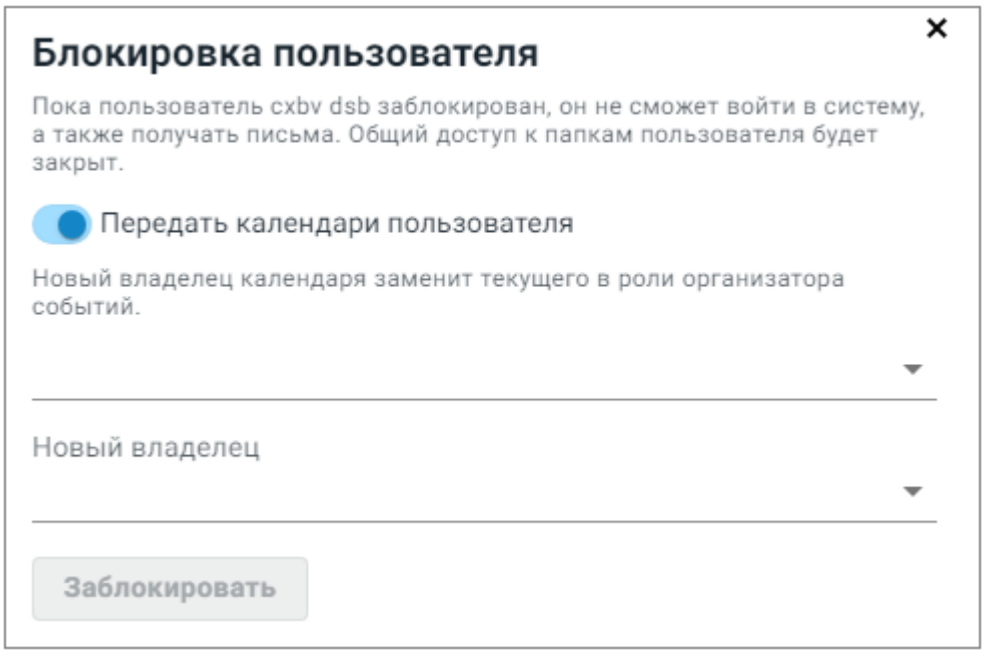


Рисунок 14 – Передача календарей при блокировке пользователя

© ООО «НОВЫЕ ОБЛАЧНЫЕ ТЕХНОЛОГИИ», 2013–2024

Администратор при необходимости также может снять блокировку пользователя. Для разблокировки пользователя в разделе **Пользователи** следует воспользоваться одним из следующих способов:

- в списке пользователей навести курсор мыши на необходимую строку, далее нажать на кнопку ;
- левой клавишей мыши выбрать нужную запись в списке, далее в открывшейся панели редактирования профиля нажать кнопку **Параметры блокировки** в верхней части окна.

На экране откроется диалоговая панель разблокировки пользователя, которая также дает возможность передачи календарей пользователю (см. рисунок 15). После нажатия на **Разблокировать** ограничения на пользователя снимутся.

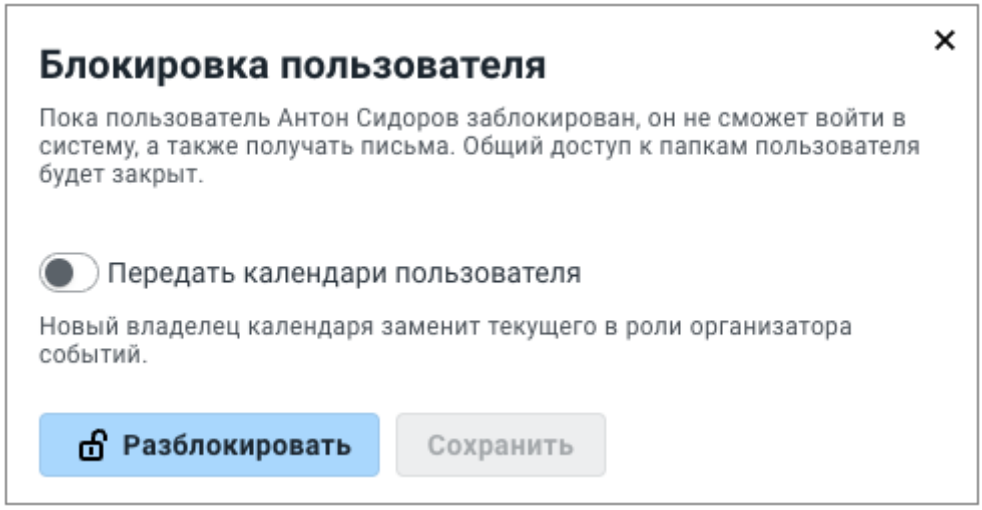


Рисунок 15 – Диалог разблокировки пользователя

Особенности блокировки пользователя

– администратор не может заблокировать сам себя;

Ограничения текущей версии (3.1):

– на данный момент доступна только полная блокировка;
– недоступна возможность настройки автоматической пересылки писем заблокированного пользователя другому пользователю.

Функция блокировки доступна в случае установки Почты без интеграции с «МойОфис. Частное облако». При интеграции с «МойОфис. Частное облако» происходит полная блокировка пользователя без возможности передачи календарей пользователя.

© ООО «НОВЫЕ ОБЛАЧНЫЕ ТЕХНОЛОГИИ», 2013–2024

2.4.4.2 Блокировка пользователя через PBM API

Для блокировки пользователя выполняются действия из раздела Добавление пользователя через PBM API с указанием значения параметра `inetUserStatus`. Доступные значения: **0** – заблокирован; **1** – разблокирован, **2** - пользователь заблокирован и не принял пользовательское соглашение. Пользователь со статусом **2** не может отправлять и просматривать почту, но письма, отправленные этому пользователю будут доставляться в его почтовый ящик.

Пример блокировки пользователя `<mail>` тенанта `<tenant-id>`:

```
curl -X PATCH "https://<pbm_url>/v2/users/<tenant-id>/<mail>" \
--data-raw '[{ "op": "replace", "path": "/inetUserStatus", "value": "0" }]' \
-H 'Content-Type: application/json-patch+json' \
-H "Authorization: Bearer <access_token>"
```

При успешном выполнении запрос вернет следующий ответ:

```
{
  "success": true
}
```

2.4.5 Удаление пользователя

2.4.5.1 Удаление пользователя в административной панели

Для удаления профиля пользователя следует перейти в раздел **Пользователи** выбранного тенанта, затем левой клавишей мыши выбрать нужную запись в списке.

Далее в открывшемся панели редактирования профиля необходимо:

- нажать кнопку **Удалить** в верхней части окна;
- на экране появится диалоговая панель, приведенная на рисунке 16.

При удалении пользователя предоставляется возможность передачи его календарей другому владельцу. Это связано с тем, что после удаления пользователя остаются события, организатором которых он является. После удаления организатора его события никто не может отменить или изменить. Смена владельца календаря подразумевает под собой смену организатора у подобных событий. После передачи календаря другому владельцу появляется возможность отменить / изменить встречи.

© ООО «НОВЫЕ ОБЛАЧНЫЕ ТЕХНОЛОГИИ», 2013–2024

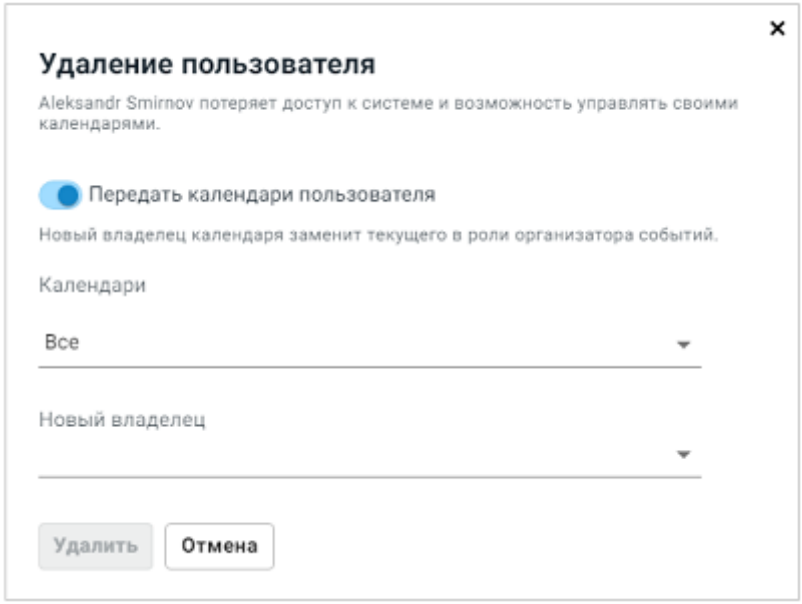


Рисунок 16 – Диалог удаления пользователя

При включении переключателя **Передать календари** пользователя на панели появляются поля для выбора календарей и их нового владельца.

По нажатии на **Удалить** отображение удаленного пользователя в списке будет отключено, но окончательное удаление из базы данных произойдет только через 30 суток. На протяжении этого времени создание пользователя с аналогичным логином невозможно.

2.4.5.2 Удаление пользователя через PBM API

При удалении пользователей через PBM API используются обязательные параметры: `tenant-id`, `mail`.

Таким образом, удаление пользователя тенанта `<tenant-id>` с ящиком `<mail>` осуществляется следующим запросом:

```
curl -X DELETE "https://<pbm_url>/v2/users/<tenant-id>/<mail>" \
-H "Authorization: Bearer <access_token>"
```

При успешном выполнении запрос вернет следующий ответ:

```
{
  "success": true
}
```

© ООО «НОВЫЕ ОБЛАЧНЫЕ ТЕХНОЛОГИИ», 2013–2024

2.4.6 Изменение квоты пользователя

2.4.6.1 Изменение квоты пользователя в административной панели

Для управления размером хранилища для писем пользователя «МойОфис» в разделе **Пользователи** необходимо:

1. Выбрать левой клавишей мыши нужного пользователя в списке пользователей выбранного тенанта.
2. В открывшемся окне профиля ввести новое значение размера хранилища в поле **Квота** (см. Рисунок 15).
3. Нажать кнопку **Обновить** для сохранения изменений или кнопку ← **Назад**, расположенную в левом верхнем углу окна профиля для выхода без изменений.

2.4.6.2 Изменение квоты пользователя через PBM API

Для изменения квоты пользователя выполняются действия из раздела Редактирование профиля пользователя через PBM API с указанием значения параметра `quota` (в байтах).

Пример команды, задающей квоту в 1Гб пользователя `<mail>` тенанта `<tenant-id>`:

```
curl -X PATCH "https://<pbm_url/v2/users/<tenant-id>/<mail>" \
--data-raw '[{ "op": "replace", "path": "/quota", "value": "1073741824" }]' \
-H 'Content-Type: application/json-patch+json' \
-H "Authorization: Bearer <access_token>"
```

При успешном выполнении запрос вернет следующий ответ:

```
{
  "success": true
}
```

При запросе информации о пользователе квота отображается в килобайтах.

2.4.7 Дополнительные адреса электронной почты

Дополнительные адреса электронной почты используются для пересылки писем.

© ООО «НОВЫЕ ОБЛАЧНЫЕ ТЕХНОЛОГИИ», 2013–2024

2.4.7.1 Добавление дополнительного адреса в административной панели

Для добавления дополнительного почтового адреса пользователя в разделе **Пользователи** необходимо выполнить следующие действия:

1. Выбрать левой клавишей мыши нужного пользователя в списке пользователей выбранного тенанта.
2. В открывшемся окне профиля пользователя в разделе **Дополнительные адреса электронной почты** нажать кнопку **Добавить адрес** (см. Рисунок 15).
3. В появившемся поле **Адрес электронной почты** ввести почтовый адрес пользователя, затем выбрать домен из выпадающего списка.
4. Нажать кнопку **Обновить** для сохранения изменений или кнопку ← **Назад**, расположенную в левом верхнем углу окна профиля для выхода без изменений.

2.4.7.2 Добавление дополнительного адреса через PBM API

Для добавления почтового алиаса выполняются действия из раздела Добавление пользователя через PBM API с указанием значения параметра `alias`. Если алиасов несколько, они указываются через запятую без пробела.

Пример команды, задающей алиас пользователя `<mail>` тенанта `<tenant-id>`:

```
curl -X PATCH "https://<pbm_url>/v2/users/<tenant-id>/<mail> \
--data-raw '\
[{ "op": "add", "path": "/alias", "value": <alias1>}, \
 { "op": "add", "path": "/alias", "value": <alias2>}]' \
-H 'Content-Type: application/json-patch+json' \
-H "Authorization: Bearer <access_token>"
```

2.4.7.3 Удаление дополнительного адреса

Для удаления дополнительного адреса электронной почты в панели профиля пользователя необходимо:

1. Нажать кнопку 🗑 справа от строки дополнительного адреса.
2. Нажать кнопку **Обновить** для сохранения изменений или кнопку ← **Назад**, расположенную в левом верхнем углу окна профиля для выхода без изменений.

© ООО «НОВЫЕ ОБЛАЧНЫЕ ТЕХНОЛОГИИ», 2013–2024

2.4.7.4 Удаление дополнительного адреса через PBM API

Пример команды, удаляющей все алиасы пользователя `<mail>` тенанта `<tenant-id>`:

```
curl -X PATCH "https://<pbm_url>/v2/users/<tenant-id>/<mail>" \
--data-raw '[{ "op": "remove", "path": <path1> },
             { "op": "remove", "path": <path2> }]' \
-H 'Content-Type: application/json-patch+json' \
-H "Authorization: Bearer <access_token>"
```

При успешном выполнении запрос вернет следующий ответ:

```
{
  "success": true
}
```

2.4.8 Изменение пароля пользователя

2.4.8.1 Изменение пароля пользователя в административной панели

Для изменения пароля пользователя «МойОфис» в разделе **Пользователи** необходимо:

1. Выбрать в общем списке пользователя, пароль которого необходимо изменить, затем двойным кликом мыши открыть панель редактирования.
2. В открывшемся окне профиля пользователя в разделе **Сменить пароль** ввести новый пароль пользователя в полях **Новый пароль** и **Повторите пароль**.
3. Нажать кнопку **Обновить** для сохранения изменений или кнопку ← **Назад**, расположенную в левом верхнем углу окна профиля для выхода без изменений.

Требования к паролю приведены в главе Добавление пользователя.

2.4.8.2 Изменение пароля пользователя через PBM API

Для изменения пароля пользователя выполняются действия из раздела Редактирование профиля пользователя данного руководства с указанием значения параметра `userPassword`.

Пример команды, задающей пароль `<password>` пользователя `<mail>` тенанта `<tenant-id>`:

© ООО «НОВЫЕ ОБЛАЧНЫЕ ТЕХНОЛОГИИ», 2013–2024

```
curl -X PATCH "https://<pbm_url>/v2/users/<tenant-id>/<mail>" \
--data-raw '[{ "op": "replace", "path": "/userPassword", "value": "Reader02" }]'
\
-H 'Content-Type: application/json-patch+json' \
-H "Authorization: Bearer <access_token>"
```

При успешном выполнении запрос вернет следующий ответ:

```
{
   "success": true
}
```

2.5 Работа с группами ресурсов

Ресурс в «МойОфис Почта» представляет собой инструмент для работы с занимаемыми на заданный промежуток времени объектами. В виде таких объектов могут выступать, например, виртуальные или физические переговорные комнаты. Таким образом, пользователи почтового клиента имеют возможность бронировать эти объекты (т.е. непосредственно ресурсы), а информация о них будет видна всем пользователям тенанта при создании события в клиенте.

Для начала работы с инструментом необходимо создать в тенанте специальные группы и добавить в них планируемые к использованию ресурсы.

2.5.1 Создание группы ресурсов в административной панели

Чтобы создать новую группу ресурсов, в административной панели необходимо перейти в раздел **Группы ресурсов** и нажать кнопку **Новая группа ресурсов**. В правой части рабочей области откроется панель ввода имени новой группы (см. Рисунок 17).

Для добавления новой группы ресурсов следует:

1. В поле **Название группы ресурсов** ввести имя создаваемой группы.
2. Нажать кнопку **Сохранить** для создания группы с указанным именем или кнопку **Отмена** для отмены создания группы и выхода без сохранения.

© ООО «НОВЫЕ ОБЛАЧНЫЕ ТЕХНОЛОГИИ», 2013–2024

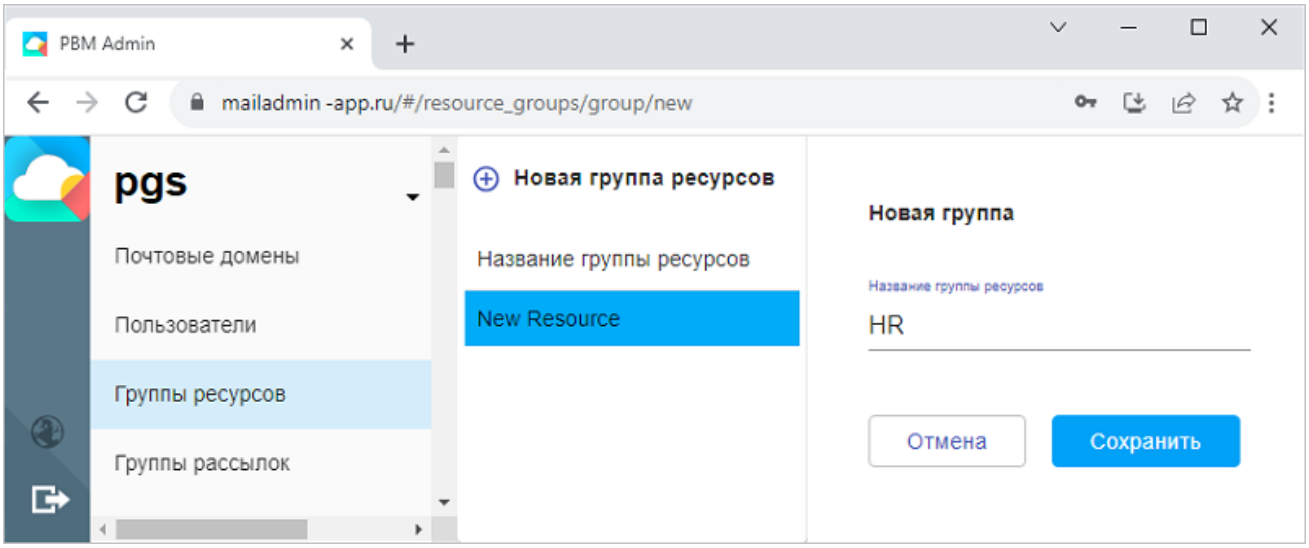


Рисунок 17 – Создание группы ресурсов

В результате операции в списке будет отображена новая группа.

2.5.2 Создание группы ресурсов через PBM API

Для получения списка уже имеющихся групп ресурсов тенанта `<tenant-id>` (обязательный параметр `tenant-id`) необходимо воспользоваться командой вида:

```
curl -X GET "https://<pbm_url>/v2/resourcegroups/<tenant-id>" \
-H "Authorization: Bearer <access_token>"
```

Создание группы ресурсов выполняется командой следующего вида:

```
curl -X PUT "https://<pbm_url>/v2/resourcegroups/<tenant-id>/<name>" \
-H "Authorization: Bearer <access_token>"
```

Где `<name>` – имя создаваемой группы, обязательный параметр.

2.5.3 Удаление группы ресурсов в административной панели

Для удаления группы ресурсов необходимо перейти в раздел **Группы ресурсов**, затем выбрать левой клавишей мыши нужную группу в списке.

Далее в открывшемся панели со списком группы ресурсов необходимо:

- нажать кнопку 🗑 в верхней правой части окна;
- подтвердить необходимость удаления в открывшемся диалоговом окне (см. Рисунок 18):

© ООО «НОВЫЕ ОБЛАЧНЫЕ ТЕХНОЛОГИИ», 2013–2024

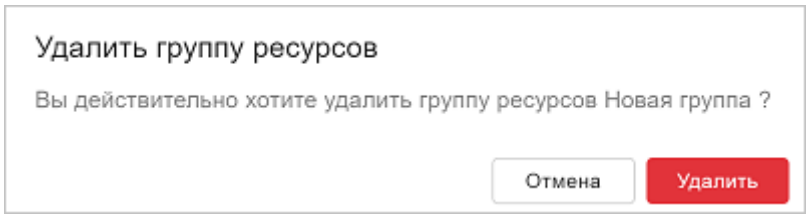


Рисунок 18 – Подтверждение удаления группы ресурсов

Группа ресурсов будет удалена из списка.

2.5.4 Переименование группы ресурсов в административной панели

Для переименования группы ресурсов необходимо перейти в раздел **Группы ресурсов**, затем выбрать левой клавишей мыши нужную группу в списке.

Далее в открывшемся панели со списком ресурсов необходимо отредактировать имя группы в поле с именем и нажать кнопку **Переименовать**.

Имя группы будет обновлено.

2.5.5 Переименование группы ресурсов через PBM API

Для получения списка уже имеющихся групп ресурсов тенанта `<tenant-id>` (обязательный параметр `tenant-id`) необходимо воспользоваться командой вида:

```
curl -X GET "https://<pbm_url>/v2/resourcegroups/<tenant-id>" \
-H "Authorization: Bearer <access_token>"
```

Переименование группы ресурсов выполняется командой следующего вида:

```
curl -X PATCH "https://<pbm_url>/v2/resourcegroups/<tenant-id>/<name>" \
--data-raw '[{ "op": "replace", "path": "/name", "value": "newName" }]' \
-H 'Content-Type: application/json-patch+json' \
-H "Authorization: Bearer <access_token>"
```

Где `<name>` – имя группы, `<newName>` – новое имя группы.

2.5.6 Удаление группы ресурсов через PBM API

При удалении группы ресурсов вместе с ней удаляются все вложенные в нее ресурсы. Для выполнения действия необходимо воспользоваться командой следующего вида:

© ООО «НОВЫЕ ОБЛАЧНЫЕ ТЕХНОЛОГИИ», 2013–2024

```
curl -X DELETE "https://<pbm_url>/v2/resourcegroups/<tenant-id>/<name>" \
-H "Authorization: Bearer <access_token>"
```

Где `<name>` – имя удаляемой группы.

2.6 Работа с ресурсами

2.6.1 Добавление ресурса в административной панели

Чтобы добавить новый ресурс в группу ресурсов, необходимо перейти в раздел **Группы ресурсов** в административной панели и выбрать группу, в которую необходимо добавить ресурс. В правой части рабочей области откроется перечень ресурсов, входящих в группу.

Далее следует:

1. Нажать кнопку **Новый ресурс**, чтобы заполнить поля вновь создаваемого ресурса.
2. В открывшемся окне ввести **Имя**, **Адрес**, **Город**, **Описание** (см. Рисунок 19).
3. Нажать кнопку **Сохранить** для создания ресурса или кнопку **Отмена** для отмены создания ресурса и выхода без сохранения.

© ООО «НОВЫЕ ОБЛАЧНЫЕ ТЕХНОЛОГИИ», 2013–2024

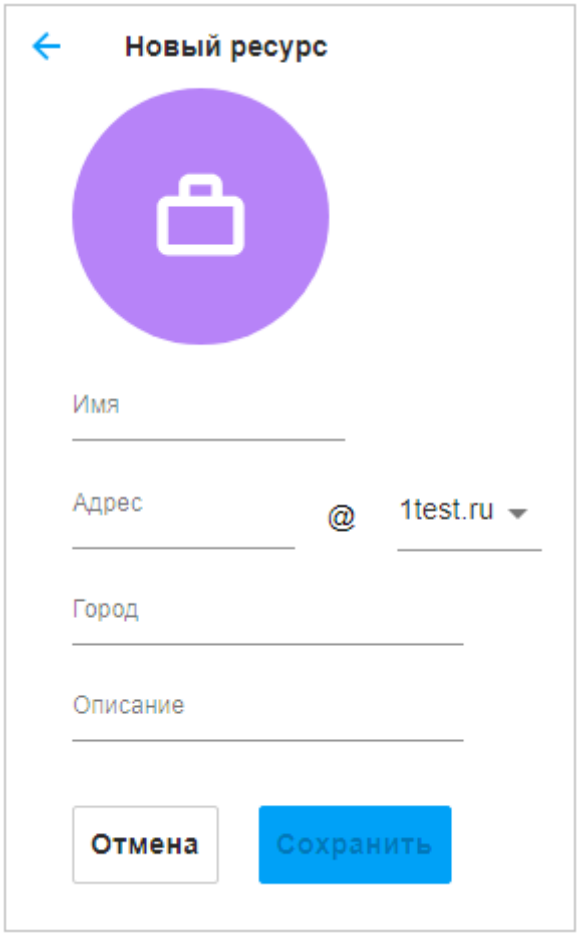


Рисунок 19 – Создание нового ресурса

В результате операции новый ресурс будет отображен в списке ресурсов, входящих в текущую группу.

2.6.2 Добавление ресурса через PBM API

Для получения списка уже имеющихся ресурсов в тенанте `<tenant-id>` группы `<gname>` необходимо воспользоваться командой вида:

```
curl -X GET "https://<pbm_url>/v2/resources/<tenant-id>/<group>" \
-H "Authorization: Bearer <access_token>"
```

Где `group` – имя создаваемой группы.

Параметры `tenant-id` и `group` обязательны к указанию.

Создание ресурса в тенанте `tenant-id` выполняется командой следующего вида:

© ООО «НОВЫЕ ОБЛАЧНЫЕ ТЕХНОЛОГИИ», 2013–2024

```
curl -X PUT "https://<pbm_url>/v2/resources/<tenant-id>/<group>/<mail>" \
-d "displayName=<displayName>" \
-d "description=<description>" \
-d "l=<l>" \
-d "employeeType=<employeeType>" \
-H "Authorization: Bearer <access_token>"
```

Где обязательные параметры:

- `displayName` – имя создаваемого ресурса;
- `group` – имя создаваемой группы;
- `mail` – создаваемый для ресурса почтовый ящик. По идентификатору данного ящика ресурс добавляется в событие.

Необязательные параметры:

- `description` – описание ресурса;
- `l` – город, указываемый для ресурса.
- `employeeType` – параметр отображения пользователя в адресной книге. **0** – отображается только в предлагаемых контактах, **1** – отображается в списке предлагаемых контактов и коллег, **2** – не отображается.

Ресурс может быть создан только в **Группе ресурсов**.

2.6.3 Обновление ресурса в административной панели

Для обновления ресурса необходимо перейти в раздел **Группы ресурсов**, затем выбрать левой клавишей мыши нужную группу в списке.

Далее в открывшемся панели со списком ресурсов нажать кнопку на выбранном ресурсе.

В открывшейся панели отредактировать необходимые поля ресурса, затем нажать кнопку **Сохранить** (см. Рисунок 20).

© ООО «НОВЫЕ ОБЛАЧНЫЕ ТЕХНОЛОГИИ», 2013–2024

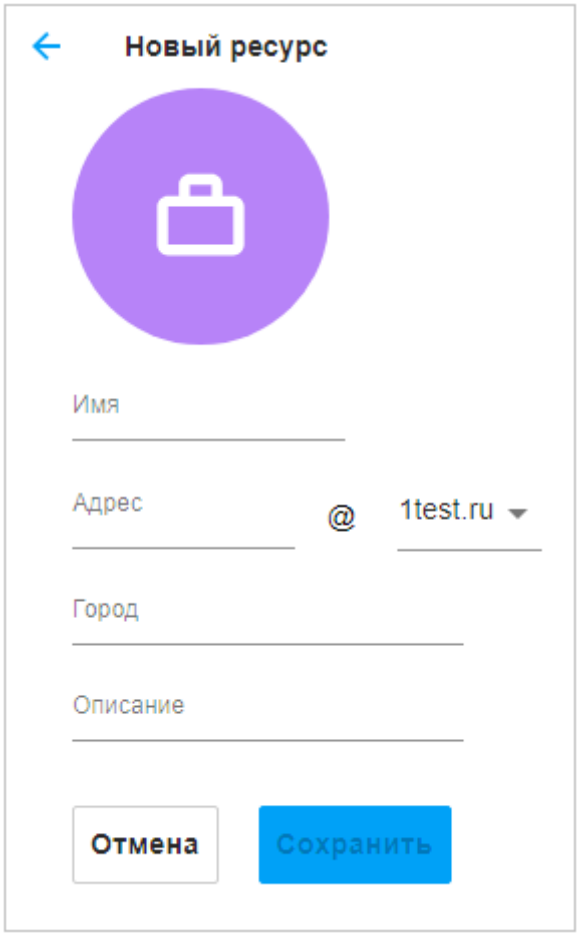


Рисунок 20 – Панель редактирования ресурса

2.6.4 Обновление информации о ресурсе через PBM API

Система позволяет дополнять и обновлять информацию об уже созданных ресурсах. Для подобных операций следует выполнить команду следующего вида:

```
curl -X PATCH "https://<pbm_url>/v2/resources/<tenant-id>/<group>/<mail> \
--data-raw '[{ "op": "replace", "path": "/displayName", "value": "test2res" }]' \
-H 'Content-Type: application/json-patch+json' \
-H "Authorization: Bearer <access_token>"
```

Описание параметров аналогично приведенному в разделе Добавление ресурса через PBM API. Почтовый ящик ресурса и группу, в которой он состоит, изменить данным методом нельзя.

Для превращения ресурса в Zoom-комнату после создания ресурса необходимо отредактировать ключ `psn/zoom` в ETCD Browser (см. раздел Настройка ETCD).

© ООО «НОВЫЕ ОБЛАЧНЫЕ ТЕХНОЛОГИИ», 2013–2024

2.6.5 Удаление ресурса в административной панели

Для удаления ресурса необходимо перейти в раздел **Группы ресурсов** выбранного тенанта, затем выбрать левой клавишей мыши нужную группу в списке.

Далее в открывшемся панели со списком ресурсов нажать кнопку на выбранном ресурсе и подтвердить необходимость удаления в открывшемся диалоговом окне (см. Рисунок 21).

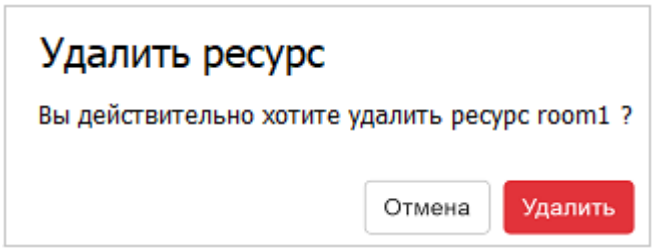


Рисунок 21 – Подтверждение удаления ресурса

Ресурс будет удален из списка.

2.6.6 Удаление ресурса через PBM API

Для удаления ресурса необходимо воспользоваться командой следующего вида (приведена для тенанта `<tenant-id>` ресурса `<mail>`):

```
curl -X DELETE "https://<pbm_url>/v2/resources/<tenant-id>/<group>/ \
<mail>" -H "Authorization: Bearer <access_token>"
```

2.7 Работа с рассылками

2.7.1 Создание группы рассылок в административной панели

Существует возможность создания групп рассылок следующих типов:

- **Статическая** – имеет заданный, постоянный список участников;
- **Динамическая** – список участников группы формируется динамически, на основе каталога внутренних пользователей и соответствия их заданным условиям включения в группу (подразделение, город, должность и др).

Чтобы создать новую группу рассылок, следует в административной панели перейти в раздел **Группы рассылки** и нажать кнопку **Новая группа рассылок**. В правой части рабочей области откроется панель ввода данных группы.

© ООО «НОВЫЕ ОБЛАЧНЫЕ ТЕХНОЛОГИИ», 2013–2024

2.7.1.1 Создание статической группы рассылок

Чтобы создать статическую группу рассылок, на панели **Новая группа** (см. Рисунок 22) следует :

1. Указать Имя группы.
2. В поле **Тип** указать значение **Статическая**.
3. Ввести адрес почтового ящика группы и выбрать домен из выпадающего списка, содержащего доступные варианты.
4. Указать участников группы в поле **Участники**.
5. Для сохранения данных новой группы нажать кнопку **Сохранить**. Будет создана новая статическая группа.

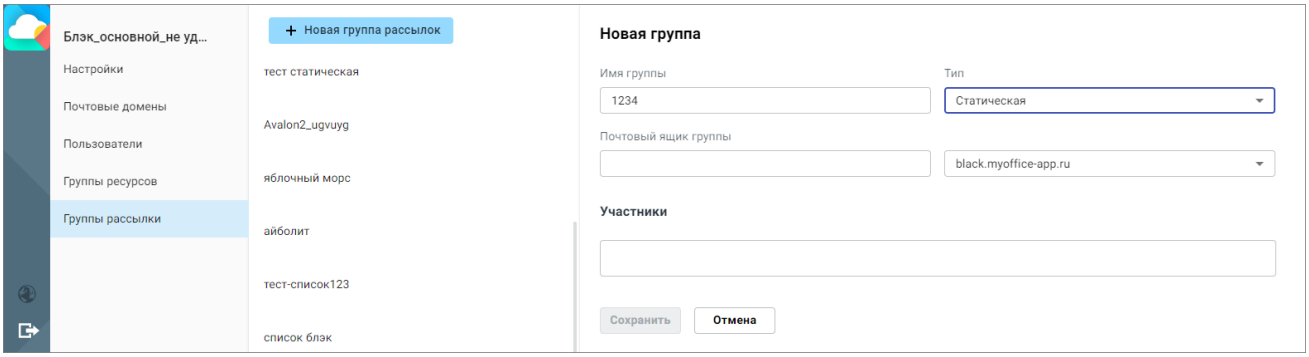


Рисунок 22 – Создание статической группы рассылок

2.7.1.2 Создание динамической группы рассылок

Чтобы создать динамическую группу рассылок, на панели **Новая группа** (см. Рисунок 23) следует :

1. Указать имя группы.
2. В поле **Тип** указать значение **Динамическая**.
3. Ввести адрес почтового ящика группы и выбрать домен из выпадающего списка, содержащего доступные варианты.
4. В группе полей **Добавлять в группу если** задать условие включения участников в группу.
5. Для добавления дополнительных условий (не более 10):
   - нажать кнопку **Добавить условие**;
   - в появившихся полях задать еще одно условие включения участников в группу;

© ООО «НОВЫЕ ОБЛАЧНЫЕ ТЕХНОЛОГИИ», 2013–2024

– указать способ применения условий – **выполнено хотя бы одно условие** либо **выполнены все условия**.

6. Для сохранения данных новой группы нажать кнопку **Сохранить**. Будет создана новая статическая группа.

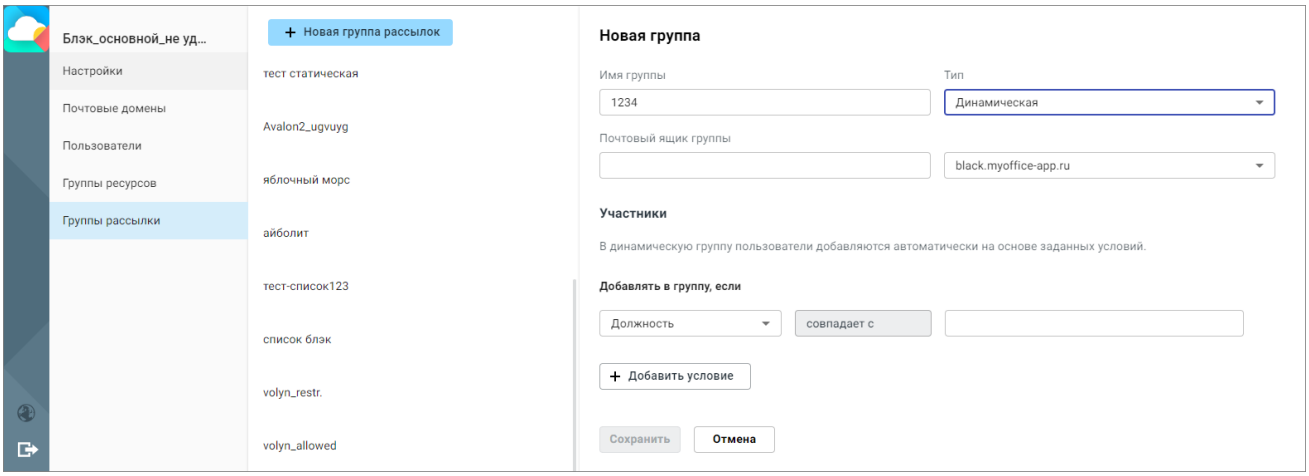


Рисунок 23 – Создание динамической группы рассылок

2.7.2 Создание группы рассылок через PBM API

1. Для получения списка уже имеющихся групп рассылок тенанта `<tenant-id>` необходимо воспользоваться командой вида:

```
curl -X GET "https://<pbm_url>/v2/maillists/<tenant-id>" \
-H "Authorization: Bearer <access_token>"
```

Где:

– `tenant-id` – тенант выполняемой операции, обязательный параметр.

2. Создание статической группы рассылок выполняется командой следующего вида:

```
curl -X PUT "https://<pbm_url>/v2/maillists/<tenant-id>/<mail>" \
-d "alias=<alias>" \
-d "displayName=<displayName>" \
-d "employeeType=<employeeType>" \
-H "Authorization: Bearer <access_token>"
```

Где обязательными параметрами являются:

– `tenant-id` – тенант выполняемой операции;

– `mail` – почтовый ящик группы рассылок;

© ООО «НОВЫЕ ОБЛАЧНЫЕ ТЕХНОЛОГИИ», 2013–2024

– `alias` – участники группы рассылок. Синтаксис указания почтовых ящиков и алиасов для команды следующий:

```
-d "alias=[<alias1>,<alias2>]"
```

– `displayName` – отображаемое имя создаваемой группы рассылки;

Необязательные параметры:

– `employeeType` – вариант отображения пользователя в адресной книге: **0** – отображается только в предлагаемых контактах, **1** – отображается в списке предлагаемых контактов и коллег, **2** – не отображается. Значение по умолчанию **1**.

3. Создание динамической группы рассылок выполняется аналогично предыдущей команде, с указанием параметра вместо `alias` параметра `filterInfo` :

```
-d "filterInfo=[{"type":<filter>,"value":<value>}]"
```

Где:

- `filterInfo` – строка фильтров для поиска участников динамической группы рассылки. Возможные фильтры:

`title` – должность,

`ou` – отдел,

`l` – город,

`domain` – домен,

`custom` – кастомный.

Указывается только для динамических групп рассылок.

4. Для получения информации о конкретной группе используется команда следующего вида:

```
curl -X GET "https://<pbm_url>/v2/maillists/<tenant-id>/<mail>" \
-H "Authorization: Bearer <access_token>"
```

Где обязательными параметрами являются:

– `tenant-id` – тенант выполняемой операции;

– `mail` – почтовый ящик группы рассылок.

© ООО «НОВЫЕ ОБЛАЧНЫЕ ТЕХНОЛОГИИ», 2013–2024

2.7.3 Редактирование группы рассылок в административной панели

Чтобы отредактировать группу рассылок, в административной панели необходимо перейти в раздел **Группы рассылки** и выбрать в списке необходимую группу. В правой части рабочей области откроется панель **Редактирование группы**, набор полей которой зависит от типа (статическая или динамическая) выбранной группы.

После внесения изменений и нажатия кнопки **Сохранить** группа рассылок будет обновлена.

2.7.4 Обновление группы рассылок через PBM API

Система позволяет дополнять и обновлять информацию об имеющихся на сервере группах рассылки. Для обновления группы рассылок следует выполнить команду следующего вида:

```
curl -X PATCH "https://pbm-gost.myoffice-app.ru/v2/maillists/<tenant-id>/<mail>"
\
-H 'Content-Type: application/json-patch+json' -H "Authorization: Bearer $token"
\
--data-raw \
'[{ "op": "replace", "path": "/displayName", "value": "testgroup" }, \
  { "op": "add", "path": "/alias", "value": <alias1> }, \
  { "op": "add", "path": "/alias", "value": <alias2> }]'
```

Где:

- `tenant-id` – обязательный параметр, тенант выполняемой операции;
- `mail` – обязательный параметр, почтовый ящик группы рассылок.

Параметры для изменения:

- `displayName` – необязательный параметр, отображаемое имя группы рассылок;
- `alias` – необязательный параметр, при помощи данного параметра возможно добавить участников в статическую группу рассылки;
- `filterInfo` – необязательный параметр, при помощи данного параметра возможно добавить участников в динамическую группы рассылки.

© ООО «НОВЫЕ ОБЛАЧНЫЕ ТЕХНОЛОГИИ», 2013–2024

2.7.5 Удаление группы рассылок в административной панели

Для удаления ресурса необходимо перейти в раздел **Группы рассылок** необходимого тенанта, затем рядом с необходимой группой нажать кнопку **Удалить**, далее подтвердить необходимость удаления в открывшемся диалоговом окне (см. Рисунок 24):

Рисунок 24 – Подтверждение удаления группы рассылки

Выбранная группа будет удалена из списка.

2.7.6 Удаление группы рассылок через PBM API

Для удаления группы рассылок необходимо воспользоваться командой следующего вида:

```
curl -X DELETE "https://<pbm_url>/v2/maillists/<tenant-id>/<mail>" \
-H "Authorization: Bearer <token>"
```

Где:

- `tenant-id` – обязательный параметр, тенант выполняемой операции;
- `mail` – обязательный параметр, почтовый ящик группы рассылок.

2.8 Синхронизация адресной книги с внешними источниками данных

На данный момент поддерживается синхронизация с Битрикс 24 и службой каталогов. Перед использованием методов необходимо заполнить значения в ETCD Browser (`services/ad` и/или `services/bitrix24`, см. раздел Настройка ETCD данного руководства).

© ООО «НОВЫЕ ОБЛАЧНЫЕ ТЕХНОЛОГИИ», 2013–2024

Для Битрикс 24 используется метод POST с обязательным параметром `tenant-id`, пример:

```
curl -X POST https://<pbm_url>/v2/actions/cabsync/ \
<tenant-id>/bitrix24 -H "Authorization: Bearer <access_token>"
```

Для служб каталогов возможна синхронизация групп:

```
curl -X POST https://<pbm_url>/v2/actions/groupsync/ \
<tenant-id>/ad -H "Authorization: Bearer <access_token>"
```

И пользователей:

```
curl -X POST https://<pbm_url>/v2/actions/cabsync/ \
<tenant-id>/ad -H "Authorization: Bearer <access_token>"
```

2.9 Работа с письмами

2.9.1 Поиск и удаление писем

Операции поиска и удаления писем реализуются при помощи консольных команд ПО `dovecot`, выполняющихся на сервере почтовой службы службы с ролью `mail` из-под аккаунта администратора. Перед исполнением команд необходимо зайти в контейнер почты на сервере:

```
docker exec -it $(docker ps -qf name=dovecot) bash
```

2.9.2 Поиск по содержимому писем

Для выполнения поиска по содержимому необходимо выполнить команду doveadm search с одним из следующих ключей:

- -u – поиск по конкретному почтовому ящику. Допускается использование маски (* и ?);
- -A – поиск по всем пользователям;
- для поиска по конкретному каталогу в профиле пользователя необходимо указать его название после параметра `mailbox`;
- ключевая фраза поиска указывается после параметра `subject`.

Пример команды, которая выполняет поиск поиск ключевого слова «`example`» в каталоге `INBOX` почтового ящика `user@example.com`:

© ООО «НОВЫЕ ОБЛАЧНЫЕ ТЕХНОЛОГИИ», 2013–2024

```
doveadm search -u user@example.com mailbox INBOX subject example
```

Если необходимо выполнить более точный поиск по теме, необходимо использовать параметр `HEADER` для поиска по заголовку письма, `FROM` или `TO` – для поиска по полям отправитель и получатель. Пример поиска по всем ящикам заголовка письма «`example`»:

```
doveadm search -A HEADER example
```

2.9.3 Просмотр содержимого найденных писем

Найденные письма отображаются в виде списка с указанием идентификатора почтового ящика `mailbox-guid` и идентификатора письма `uid`. Для просмотра содержимого найденных писем в `dovecot` используется команда `fetch` с одним из следующих ключей:

- -u – выполнение команды для указанных ящиков;
- -A – выполнение команды для всех ящиков сервера;
- после ключа в команде указываются желаемые для отображения элементы письма (в кавычках через пробел): `body` – тело письма, `hdr` – заголовок письма, `text` – заголовок и тело письма вместе и т.д.;
- далее в команде указывается `mailbox-guid` и `uid`.

Пример команды для отображения содержимого и заголовка писем из почтового ящика пользователя user@example.com с идентификатором 403dcf30048f9e601b100000654d370e и идентификаторами письма 2 и 3:

```
doveadm fetch -u user@example.com "text" mailbox-guid \
403dcf30048f9e601b100000654d370e uid 2,3
```

2.9.4 Удаление писем

Удаление писем из почтовых ящиков осуществляется при помощи команды expunge со следующими ключами и параметрами:

- -u – поиск и удаление писем в конкретном почтовом ящике, допускается использование маски (* и ?);
- -A – поиск и удаление писем всех пользователей;
- для удаления писем из конкретного каталога в профиле пользователя, необходимо указать его название после параметра mailbox;

© ООО «НОВЫЕ ОБЛАЧНЫЕ ТЕХНОЛОГИИ», 2013–2024

Удаление писем по ключевым фразам производится при помощи параметров:

- BODY – поиск ключевых фраз по содержимому письма;
- FROM – поиск ключевых фраз по отправителю письма;
- HEADER – поиск ключевых фраз по заголовку письма.

Пример команды удаления всех писем от автора spam@example.com в каталоге spam пользователя user@example.com:

```
doveadm expunge -u user@example.com mailbox spam FROM spam@example.com
```

Более подробно о параметрах команд в руководстве по dovecot:

- search и searchquery
- fetch
- expunge

2.9.4.1 Удаление писем с использованием PBM API

Отзыв (удаление) письма также возможно реализовать через PBM API. Для этого используется метод **POST** со следующими обязательными параметрами:

- `cmd` – параметр, определяющий операцию. Значение по умолчанию expunge;
- `messageid` – идентификатор письма из заголовка (см. раздел Просмотр содержимого писем);
- `emails` – почтовые ящики, у которых необходимо удалить письмо;
- `force` – параметры удаления. Возможные значения: **1** – удалить письмо, даже если пользователь его прочитал, **0** – не удалять письмо, если получатель его прочитал (значение по умолчанию);
- `notify` – оповещение пользователя о результатах отзыва. Возможные значения: **1** – оповестить пользователя (значение по умолчанию), **0** – не оповещать пользователя.

Пример отзыва письма с идентификатором `<id>` почтового ящика `<mail>`:

```
curl -X POST "https://<pbm_url>/v2/actions/expunge \
-d "messageid=<messageId>" \
-d "emails=<emails>" \
-d "force=0" \
-d "notify=1" \
-H "Authorization: Bearer <access_token>"
```

© ООО «НОВЫЕ ОБЛАЧНЫЕ ТЕХНОЛОГИИ», 2013–2024

Пример параметра `<emails>`:

```
-d "emails=[<amail>]"
```

2.9.5 Настройка общего доступа к почтовому ящику

Настройка общего доступа к почтовому ящику в «МойОфис Почта» реализуется при помощи консольных команд ПО `dovecot`, выполняющихся на сервере почтовой службы с ролью `mail` из-под аккаунта администратора. Например, предоставление доступа к каталогу INBOX почтового ящика `<user1>` для пользователя `<user2>` с помощью утилиты `doveadm` осуществляется следующим образом:

```
doveadm acl set -u <user1> INBOX user=<user2>
<RIGHTS>
```

```
doveadm mailbox subscribe -u <user2> shared/
testuser1@myoffice.ru/INBOX
```

Где RIGHTS – ACL (Access Control List) для каталога INBOX

Список поддерживаемых прав ACL:

- lookup;
- read;
- write;
- write-seen;
- write-deleted;
- insert;
- post;
- expunge;
- create;
- delete;
- admin.

Более подробно параметры команды описаны в документации по dovecot и стандарте RFC 4314.

Просмотр списка пользователей, которым предоставлен доступ к каталогу почтового ящика осуществляется при помощи следующей команды:

```
doveadm acl get -u <user> <mailbox>
```

© ООО «НОВЫЕ ОБЛАЧНЫЕ ТЕХНОЛОГИИ», 2013–2024

Где `<user>` – пользователь, для которого запрашиваются права, `<mailbox>` – ящик, для которого запрашиваются права. Общий пример исполнения команды выглядит следующим образом:

```
ID Global Rights
user=<user> <rights>
```

Где `<rights>` – действующие права доступа для пользователя `<user>`.

2.9.6 Настройка максимального размера сообщений и вложений

Максимальный размер вложений можно задать на этапе деплоя (см. раздел **Настройка дополнительных параметров установки** в документе «МойОфис Почта 3. Руководство по установке почтового сервера 3.1»).

Если значения необходимо изменить на работающей системе необходимо на всех нодах группы `frontend`

– В `/opt/poseidon/web_mail/config.json`
и `/opt/poseidon/web_calendar/config.json` изменить значение `maxUploadSizeInMb`;

– В `/opt/poseidon/nginx/nginx.conf` изменить `SIZE` в `smtp_capabilities` на всех нодах группы `mail`;

– В `/opt/poseidon/postfix/main.cf` изменить `message_size_limit`.

После чего выполнить следующую команду:

```
docker service update --force psn-frontend_web_calendar && \
docker service update --force psn-frontend_web_mail && \
docker service update --force psn-mail_postfix && \
docker service update --force psn-nginx-proxy_nginx
```

Существует дополнительный вариант: изменить значения в инвентарном файле и выполнить установку с параметрами `-t frontend,mail` (см. раздел **Настройка дополнительных параметров установки** документа «МойОфис Почта 3. Руководство по установке почтового сервера 3.1»).

© ООО «НОВЫЕ ОБЛАЧНЫЕ ТЕХНОЛОГИИ», 2013–2024

2.10 Работа с почтовыми доменами

2.10.1 Добавление почтового домена в административной панели

Чтобы создать новый домен в административной панели, необходимо перейти в раздел **Почтовые домены** выбранного тенанта и нажать кнопку **Добавить домен**. В правой части рабочей области откроется окно ввода данных (см. Рисунок 25). В нем следует заполнить поля: **ID организации**, **Доменное имя**, **Описание**, после чего нажать кнопку **Сохранить**.

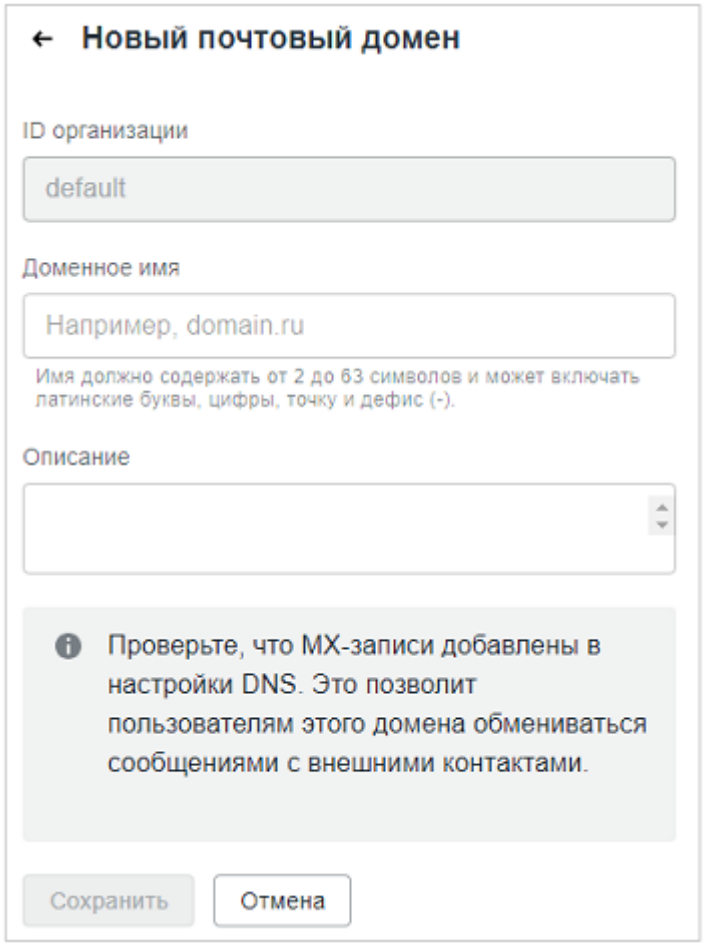


Рисунок 25 – Панель создания домена

В результате операции новый домен будет отображен в списке.

2.10.2 Добавление почтового домена через PBM API

Процедура добавления почтового домена выполняется следующим образом:

```
curl -X PUT "https://<pbm_url>/v2/maildomains/<tenant-id>/<domain>" \
-H "Authorization: Bearer <access_token>"
```

© ООО «НОВЫЕ ОБЛАЧНЫЕ ТЕХНОЛОГИИ», 2013–2024

После создания домена и пользователей в нем PSN будет готов принимать почту на новом домене (внутри стенда). Для получения корреспонденции с внешних адресов требуется внести соответствующие MX-записи в DNS.

2.10.3 Редактирование домена в административной панели

Для обновления домена необходимо перейти в раздел **Почтовые домены** выбранного тенанта, затем нажать кнопку на выбранном домене.

В открывшейся панели отредактировать необходимые поля домена, затем нажать кнопку **Сохранить** (см. Рисунок 26).

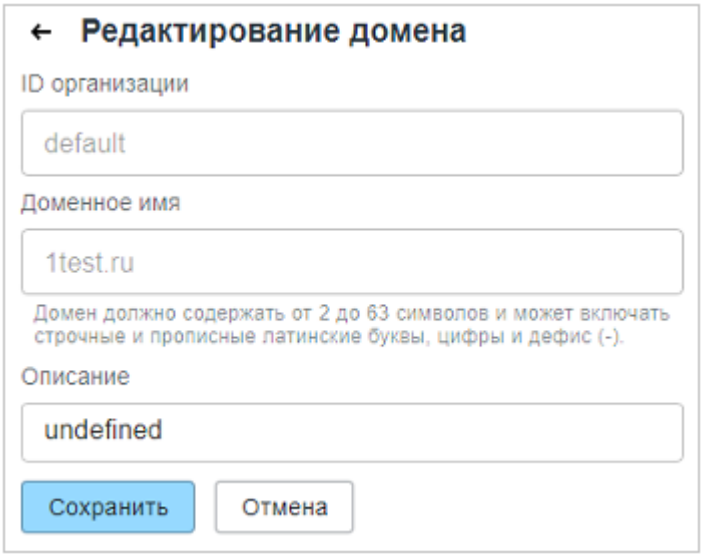


Рисунок 26 – Панель редактирования домена

2.10.4 Редактирование домена через PBM API

Процедура редактирования почтового домена выполняется следующим образом:

```
curl -X PATCH "https://<pbm_url>/v2/maildomains/<tenant-id>/<domain>" \
--data-raw \
'[{ "op": "add", "path": "/displayName", "value": "test2domain" }, \
  { "op": "add", "path": "/description", "value": "test2domain_desk" }, \
  { "op": "add", "path": "/associatedDomain", "value": "false" }]' \
-H 'Content-Type: application/json-patch+json' \
-H "Authorization: Bearer <access_token>"
```

© ООО «НОВЫЕ ОБЛАЧНЫЕ ТЕХНОЛОГИИ», 2013–2024

2.10.5 Установка домена по умолчанию в административной панели

Для обновления домена необходимо перейти в раздел **Почтовые домены** выбранного тенанта, затем нажать кнопку на выбранном домене.

В открывшейся панели отредактировать необходимые поля домена, затем нажать кнопку **Сохранить** (см. Рисунок 27).

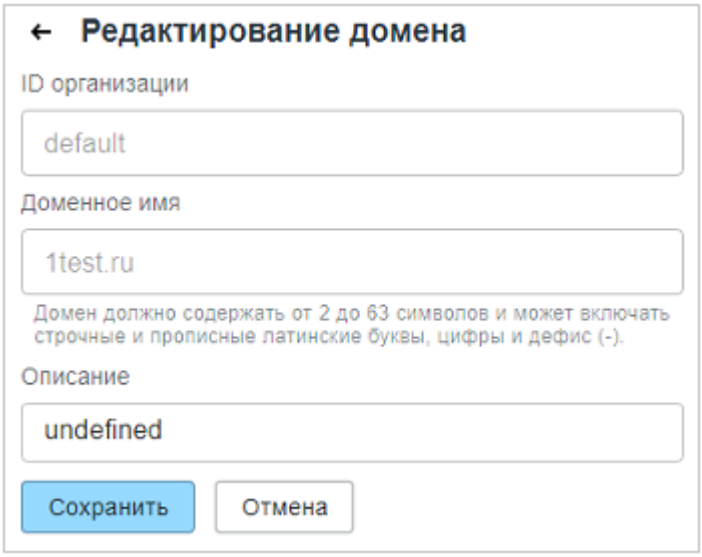


Рисунок 27 – Панель редактирования домена

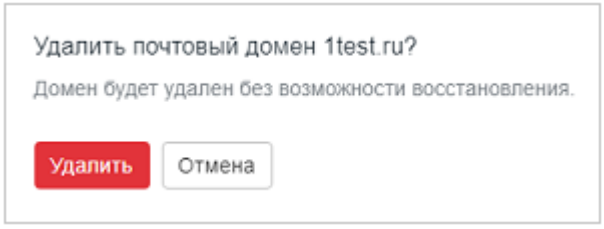
2.10.6 Получение списка почтовых доменов через PBM API

Для получения списка почтовых доменов выполните следующий запрос:

```
curl -X GET "https://<pbm_url>/v2/maildomains/<tenant-id>" \
-H "Authorization: Bearer <access_token>"
```

2.10.7 Удаление почтового домена в административной панели

Для удаления почтового домена необходимо перейти в раздел **Почтовые домены** выбранного тенанта, затем рядом с необходимой строкой нажать кнопку , далее подтвердить необходимость удаления в открывшемся диалоговом окне (см. Рисунок 28):



© ООО «НОВЫЕ ОБЛАЧНЫЕ ТЕХНОЛОГИИ», 2013–2024

Рисунок 28 – Подтверждение удаления домена

Выбранный домен будет удален из списка.

2.10.8 Установка почтового домена по умолчанию

На экране со списком почтовых доменов присутствует столбец с флагами, позволяющими управлять доменом по умолчанию. Для смены почтового домена по умолчанию необходимо снять или выбрать флаг на соответствующей строке (см. Рисунок 29):

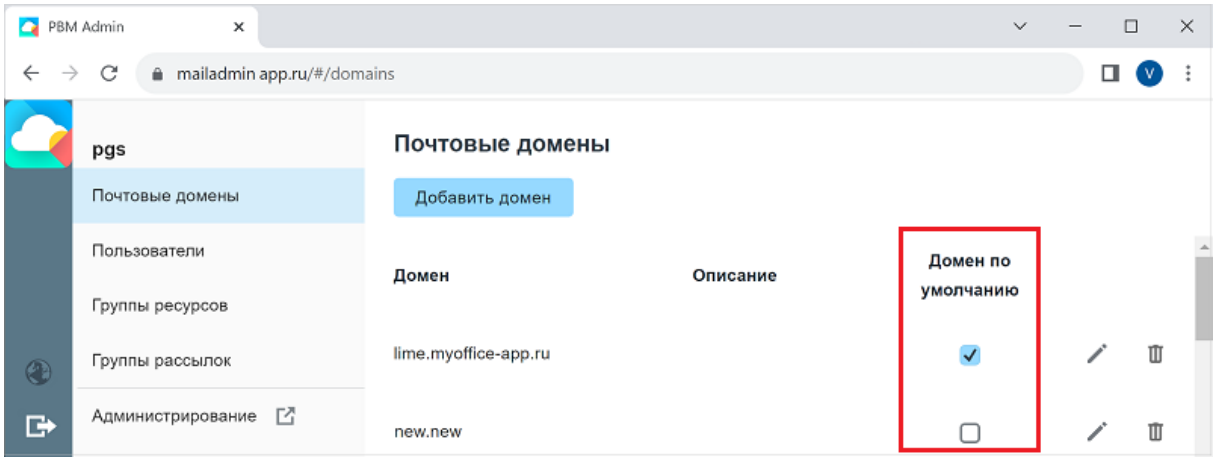


Рисунок 29 – Подтверждение удаления домена

2.10.9 Удаление почтового домена через PBM API

Для удаления почтового домена выполните следующий запрос:

```
curl -X DELETE "https://<pbm_url>/v2/maildomains/<tenant-id>/<domain>" \
-H "Authorization: <access_token>"
```

2.11 Работа с веб доменами

Работа с веб доменами доступна только через PBM API для пользователя с ролью суперадминистратора почтовой системы (см. раздел Авторизация).

Возможность работы с веб доменами настраивается посредством переменной `dynamic_webdomains` (см. «Руководство по установке почтового сервера», раздел «Конфигурирование инвентарного файла: переменные»).

© ООО «НОВЫЕ ОБЛАЧНЫЕ ТЕХНОЛОГИИ», 2013–2024

2.11.1 Добавление веб домена через PBM API

Для добавления веб домена выполните следующий запрос:

```
curl -X PUT "https://<pbm_url>/v2/webdomains/<domain>" \
-d "key=<key>" -d "crt=<crt>" \
-H "Authorization: Bearer <access_token>"
```

Где:

`<domain>` – домен тенанта для веб интерфейса почты;

`<key>` – ключ сертификата почтового веб-домена, можно отправить через форму вместо параметра;

`<crt>` – сертификат почтового веб домена, можно отправить через форму вместо параметра.

При успешном выполнении запрос вернет следующий ответ:

```
{
  "success": true
}
```

2.11.2 Обновление веб домена через PBM API

Для обновления веб домена выполните следующий запрос:

```
curl -X PATCH "https://<pbm_url>/v2/webdomains/<domain>" \
-d "key=<key>" -d "crt=<crt>" \
-H "Authorization: Bearer <access_token>"
```

Где:

`<domain>` – домен тенанта для веб интерфейса почты;

`<key>` – ключ сертификата почтового веб-домена, можно отправить через форму вместо параметра;

`<crt>` – сертификат веб домена, можно отправить через форму вместо параметра.

При успешном выполнении запрос вернет следующий ответ:

```
{
  "success": true
}
```

© ООО «НОВЫЕ ОБЛАЧНЫЕ ТЕХНОЛОГИИ», 2013–2024

2.11.3 Удаление веб домена через PBM API

Для удаления веб домена выполните следующий запрос:

```
curl -X DELETE "https://<pbm_url>/v2/webdomains/<domain>" \
-H "Authorization: Bearer <access_token>"
```

Где:

`<domain>` – домен тенанта для веб интерфейса почты.

При успешном выполнении запрос вернет следующий ответ:

```
{
  "success": true
}
```

© ООО «НОВЫЕ ОБЛАЧНЫЕ ТЕХНОЛОГИИ», 2013–2024

3 РАБОТА С СЕРВИСОМ ПОЛИТИК

Чтобы начать работу с сервисом политик через PPS API, необходимо осуществить авторизацию в Postfix Policy Server. Для этого потребуется использовать токен авторизации, находящийся в сервисе ETCD (см. раздел Настройка ETCD) по ключу:

```
services/policy_api/token
```

Выполнение команд через PPS API осуществляется непосредственно на одной из backend-нод в docker-контейнере сервиса Postfix Policy Server. Для перехода в контейнер сервиса необходимо выполнить команду:

```
docker exec $(docker ps -qf name=pps) ash
```

3.1 Получение списка политик через PPS API

Для получения списка политик необходимо выполнить команду без токена авторизации:

```
curl -s https://pps:8080/api/rules | jq
```

Если список политик пуст, при успешном выполнении запроса будет возвращен следующий ответ:

```
{
 "items": null,
 "page": {
   "next": 0,
   "previous": 0,
   "limit": 10,
   "current": 1,
   "total_items": 0
 }
}
```

В случае, если политики были добавлены, ответ может выглядеть, например, так:

```
{
 "items": [
   {
     "rule_name": "rule_name_1",
     "description": "string",
```

© ООО «НОВЫЕ ОБЛАЧНЫЕ ТЕХНОЛОГИИ», 2013–2024

```
      "policy_item": "string",
      "policy_item_value": "string",
      "cmp_policy_item": "string",
      "cmp_operator": "string",
      "cmp_value": "string",
      "rule_action": int,
      "text_msg": "string"
    },
    {
      "rule_name": "rule_name_2",
      "description": "string",
      "policy_item": "string",
      "policy_item_value": "string",
      "cmp_policy_item": "string",
      "cmp_operator": "string",
      "cmp_value": "string",
      "rule_action": int,
      "text_msg": "string"
    }
  ],
  "page": {
    "next": 0,
    "previous": 0,
    "limit": 10,
    "current": 1,
    "total_items": 0
  }
}
```


3.2 Добавление политики через PPS API

Для добавления политики необходимо выполнить команду вида:

```
curl -X POST http://pps:8080/api/rules -H "Authorization: <token>" \
-H "Content-Type: application/json" -d '<item_json>'
```

где:

`<token>` – токен авторизации сервиса Postfix Policy Server,

`<item_json>` – JSON-запись добавляемой политики вида:

© ООО «НОВЫЕ ОБЛАЧНЫЕ ТЕХНОЛОГИИ», 2013–2024

```
{
  "rule_name": "string",
  "description": "string",
  "policy_item": "string",
  "policy_item_value": "string",
  "cmp_policy_item": "string",
  "cmp_operator": "string",
  "cmp_value": "string",
  "rule_action": int,
  "text_msg": "string"
}
```

Все приведенные выше поля являются обязательными. В таблице 5 представлены описание полей и их возможные значения.

Таблица 5 – Описание полей политики

Поле	Описание	Значения
`rule_name`	Название политики	Строка, до 120 символов
`description`	Описание политики	Строка, до 50 символов
`policy_item`	–	recipient
`policy_item_value`	Адрес получателя, для которого устанавливается политика	Строка, до 50 символов
`cmp_policy_item`	–	sender
`cmp_operator`	Оператор политики	eq, ne, contains, notcontains
`cmp_value`	Адрес отправителя или его подстрока	Строка, до 50 символов
`rule_action`	–	5
`text_msg`	Текст сообщения для логов сервиса	Строка, до 50 символов

Пример добавления политики, которая для адреса `target_user@domain` разрешает прием писем только от адреса `allowed_user@domain`:

```
curl -X POST http://pps:8080/api/rules -H "Authorization:token" \
-H "Content-Type: application/json" \
-d '{
```

© ООО «НОВЫЕ ОБЛАЧНЫЕ ТЕХНОЛОГИИ», 2013–2024

```
     "rule_name": "deny_all_but_one",
     "description": "deny all but one",
     "policy_item": "recipient",
     "policy_item_value": "target_user@domain",
     "cmp_policy_item": "sender",
     "cmp_operator": "ne",
     "cmp_value": "allowed_user@domain",
     "rule_action": 5,
     "text_msg": "deny all but one"
}'
```

Пример добавления политики, которая для адреса `target_user@domain` запрещает прием писем от адресов, доменное имя которых содержит `denied_domain`:

```
curl -X POST http://pps:8080/api/rules -H "Authorization:token" \
-H "Content-Type: application/json" \
-d '{
     "rule_name": "deny_domains",
     "description": "deny domains",
     "policy_item": "recipient",
     "policy_item_value": "target_user@domain",
     "cmp_policy_item": "sender",
     "cmp_operator": "contains",
     "cmp_value": "denied_domain",
     "rule_action": 5,
     "text_msg": "deny domains"
}'
```

В случае успеха политика будет добавлена в список политик. Для контроля можно воспользоваться запросом получения политики из раздела Получение конкретной политики через PPS API. Запрос должен вернуть добавленную политику.

3.3 Получение конкретной политики через PPS API

Для получения конкретной политики необходимо выполнить команду без токена авторизации:

```
curl -s https://pps:8080/api/rules/<rule_name> | jq
```

где `<rule_name>` – имя политики, которую необходимо запросить (см. таблицу 5).

© ООО «НОВЫЕ ОБЛАЧНЫЕ ТЕХНОЛОГИИ», 2013–2024

Пример ответа на запрос:

```
{
  "rule_name": "rule_name",
  "description": "string",
  "policy_item": "string",
  "policy_item_value": "string",
  "cmp_policy_item": "string",
  "cmp_operator": "string",
  "cmp_value": "string",
  "rule_action": int,
  "text_msg": "string"
}
```

3.4 Удаление политики через PPS API

Для удаления добавленной ранее политики необходимо выполнить команду:

```
curl -X DELETE http://pps:8080/api/rules/<rule_name> \
-H "Authorization: <token>"
```

где:

`<rule_name>` – имя политики, которую необходимо удалить, соответствует полю rule_name (см. таблицу 5),

`<token>` – токен авторизации сервиса Postfix Policy Server.

В случае успеха политика будет удалена из списка политик. Для контроля можно воспользоваться запросом получения политики из раздела Получение конкретной политики через PPS API. Запрос получения удаленной политики должен вернуть:

```
{
 "error": "no rows in result set"
}
```

3.5 Редактирование политик через PPS API

Для обновления политики необходимо воспользоваться методом PATCH, выполнив команду вида:

© ООО «НОВЫЕ ОБЛАЧНЫЕ ТЕХНОЛОГИИ», 2013–2024

```
curl -X PATCH http://pps:8080/api/rules/<rule_name> \
-H "Authorization: <token>" -H "Content-Type: application/json" \
-d '{
     "rule_name": "<rule_name>",
     "description": "string",
     "policy_item": "string",
     "policy_item_value": "string",
     "cmp_policy_item": "string",
     "cmp_operator": "string",
     "cmp_value": "string",
     "rule_action": int,
     "text_msg": "string"
}'
```

где:

`<rule_name>` – имя политики, которую необходимо обновить,

`<token>` – токен авторизации сервиса Postfix Policy Server.

При редактировании политики необходимо указывать все поля.

В случае успеха политика будет обновлена. Для контроля обновления можно воспользоваться запросом получения политики из раздела Получение конкретной политики через PPS API. Запрос должен вернуть политику с обновленными значениями полей.

© ООО «НОВЫЕ ОБЛАЧНЫЕ ТЕХНОЛОГИИ», 2013–2024

4 РЕЗЕРВНОЕ КОПИРОВАНИЕ

Созданные резервные копии следует регулярно сохранять на другой дисковый/сетевой ресурс для возможности восстановления данных в случае необходимости или аварийной ситуации.

4.1 Резервное копирование etcd

В `etcd` хранятся настройки компонентов стенда. Ценность представляют некоторые настройки компонентов, отличающиеся от стандартных, а также состояние кластера `postgresql` (в случае кластерной инсталляции). Для сохранения значений всех настроек `etcd` в текстовый файл необходимо на любой ноде группы `etcd` выполнить команду

```
docker exec $(docker ps -qf name=etcd_etcd[0-9]) etcdctl get --prefix '' \
> <path_to_backup>/etcd_keys.txt
```

Все стандартные настройки могут быть восстановлены в случае утери данных `etcd` путем запуска деплоя с параметром `-t etcd`, а остальные через etcd browser.

Дополнительно рекомендуется делать снимок данных etcd

```
docker exec $(docker ps -qf name=etcd_etcd[0-9]) etcdctl snapshot
save /etcd-data/snapshot.db
```

После выполнения команды он будет доступен по следующему пути:

```
/var/lib/docker/volumes/psn_etcd_data/_data/snapshot.db
```

4.2 Экспорт и импорт каталогов LDAP

Процедура **резервирования** службы каталогов выполняется следующей командой:

```
docker exec $(docker ps -qf 'name=ldap') ldapsearch -xD dn=Manager, \
dc=<external_domain> -w <ds389_manager_user> '*' > <path_to_backup> \
/ldap.ldif
```

Где:

- `<external_domain>` – зарегистрированный домен инсталляции; запись домена второго уровня в нотации LDAP выглядит следующим образом для example.com: `dc=example,dc=com`

© ООО «НОВЫЕ ОБЛАЧНЫЕ ТЕХНОЛОГИИ», 2013–2024

- `<ds389_manager_user>` – значение переменной `ds389_manager_user` из инвентарного файла инсталляции.
- `<path_to_backup>` – путь к создаваемой резервной копии.

Процедура **восстановления** данных LDAP из резервной копии выполняется следующим образом:

```
cp <path_to_backup>/ldap.ldif /var/lib/docker/volumes/psn-ldap_ldap_data \
/_data/ldap.ldif
```

```
docker exec $(docker ps -qf 'name=ldap') ldapadd -xD cn=Manager, \
dc=<external_domain> -w <ds389_manager_user> -f /data/ldap.ldif -c
```

Первая команда скопирует файл резервной копии в примонтированную к Docker-контейнеру директорию, вторая – произведет восстановление данных.

Вышеупомянутые способы не позволяют изменить уже существующие записи LDAP. В случае, если это требуется, возможно полностью **очистить** данные в LDAP перед восстановлением следующей командой:

```
docker exec $(docker ps -qf 'name=ldap') ldapdelete -xD cn=Manager, \
dc=<external_domain> -w <ds389_manager_user> -r <external_domain>
```

Если данные перед восстановлением не будут зачищены, то при восстановлении добавятся только отсутствующие записи. Существующие записи не будут изменены, даже если данные различаются.

Для кластерной инсталляции процедура резервирования и восстановления выполняется **единожды** на любом из хостов группы ldap (см. инвентарный файл установки).

4.3 Процедура резервирования БД Postgres

Процедура **резервирования** базы данных Postgres выполняется следующей командой:

```
docker exec $(docker ps -qf name=postgres_postgres) pg_dump \
-Fc --clean --create psn -U psn > <path_to_backup>
```

Где `<path_to_backup>` – путь до файла резервной копии с указанием его имени (рекомендуемое расширение `.dump`).

© ООО «НОВЫЕ ОБЛАЧНЫЕ ТЕХНОЛОГИИ», 2013–2024

Процедура **восстановления** базы данных Postgres выполняется следующей командой:

```
docker exec -i $(docker ps -qf name=postgres_postgres) pg_restore -d psn \
-c -U psn < <path_to_restore>
```

Где `<path_to_restore>` – путь до файла резервной копии, из которого выполняется восстановление.

4.4 Резервное копирование писем

Резервное копирование писем в текущем релизе рекомендуется выполнять утилитой `rsync`. Для этого необходимо создать резервную копию данных из `/var/dovecot/` командой

```
rsync -a /var/dovecot <path_to_backup>
```

4.5 Резервное копирование вложений к событиям в календаре

Резервное копирование вложений к календарным событиям в текущем релизе рекомендуется выполнять утилитой `rsync`. Для этого необходимо создать резервную копию данных из `/opt/poseidon/triton/eattach/` командой:

```
rsync -a /opt/poseidon/triton/eattach <path_to_backup>
```

4.6 Резервное копирование аватаров

Резервное копирование аватаров пользователей в текущем релизе рекомендуется выполнять утилитой `rsync`. Для этого необходимо создать резервную копию данных из `/opt/poseidon/triton/photos/` командой:

```
rsync -a /opt/poseidon/triton/photos <path_to_backup>
```

© ООО «НОВЫЕ ОБЛАЧНЫЕ ТЕХНОЛОГИИ», 2013–2024

5 РАБОТА С СЕРТИФИКАТАМИ

5.1 Генерация dkim ключей

Процесс создания DKIM ключей описан в главе «Генерация DKIM ключей» Руководства по установке сервера.

5.2 Замена сертификатов

Если возникает необходимость заменить сертификат в уже установленной системе, для «МойОфис Почта» существует два алгоритма действий: через запуск установщика с параметром и вручную.

В первом случае необходимо разместить новые сертификаты и ключи в каталоге с дистрибутивом (см. раздел «Настройка сертификатов» Руководства по установке почтового сервера). Способ подходит как для конфигурации с отказоустойчивостью, так и без. После выполнения подготовительных действий следует запустить установку командой следующего вида:

```
./deploy_psn.sh <inventory> -t proxy
```

Где `<inventory>` - инвентарный файл установки (заполненный в соответствии с разделом «Настройка основных параметров установки» Руководства по установке PSN).

Для ручной замены всех сертификатов необходимо на каждой из нод proxy найти каталог:

```
/opt/poseidon/certificates/
```

В ней находятся требующие замены сертификаты. После выполнения операций над файлами будет необходимо перезапустить сервис proxy с любого целевого сервера:

```
docker service update --force --with-registry-auth psn-nginx-proxy_nginx
```

В файле сертифката `server.crt` должны быть указаны все промежуточные сертификаты, кроме корневого доверенного. Расположение промежуточных сертификатов соответствует описанию в документации nginx.)

Если был заменен сертификат `dkim`, то следует выполнить следующую команду для перезапуска службы `rspamd`:

© ООО «НОВЫЕ ОБЛАЧНЫЕ ТЕХНОЛОГИИ», 2013–2024

```
docker service update --force --with-registry-auth psn-mail_rspamd
```

© ООО «НОВЫЕ ОБЛАЧНЫЕ ТЕХНОЛОГИИ», 2013–2024

6 ИНТЕГРАЦИИ

6.1 Настройка интеграции с Kaspersky Security for Linux Mail Server

Данный раздел описывает процедуру интеграции решения **Kaspersky Security for Linux Mail Server** (в дальнейшем - KLMS) в почтовую систему «МойОфис Почта».

Для выполнения интеграции KLMS должен быть установлен до внесения изменений в конфигурационные файлы «МойОфис Почта». Общая процедура инсталляции антивирусного решения описана в документации по следующей ссылке. KLMS возможно устанавливать как на одну машину с MTA (Mail Transfer Agent, почтовый сервер), так и на отдельную; в «МойОфис Почта» роль MTA исполняет сервис Postfix.

Информация, предоставленная ниже, описывает подготовительные действия, которые администратор системы должен выполнить в ходе установки KLMS.

В диалоговом окне Setting up integration with MTA:

- Выбрать тип MTA: `Postfix`;
- Выбрать метод интеграции: `milter`;
- В методе коммуникации по протоколу `milter` необходимо указать TCP-сокет, свободный TCP-порт и IP-адрес для взаимодействия KLMS и «МойОфис Почта» по сети.

Пример записи:

```
inet:10025@10.10.22.22
```

В режиме с отказоустойчивостью АО «Лаборатория Касперского» рекомендует иметь количество установок KLMS равное количеству MTA. Инсталлятор для текущего релиза PSN при установке позволяет указать только один хост. Для выполнения рекомендаций вендора антивирусного решения после установки «МойОфис Почта» администратору системы необходимо сконфигурировать `Postfix` на каждой ноде так, чтобы пересылка писем с нее осуществлялась на отдельный выделенный для нее KLMS.

Интеграция в кластерном режиме требует обеспечивать синхронность настроек на разных экземплярах KLMS. Для выполнения подобных операций в антивирусном решении существует функция импорта и экспорта настроек через файл в XML-формате. Работа с импортом и экспортом настроек выполняется как через командную строку, так и через веб-интерфейс KLMS. Более подробная информация предоставлена в онлайн-справке KLMS:

© ООО «НОВЫЕ ОБЛАЧНЫЕ ТЕХНОЛОГИИ», 2013–2024

- Экспорт параметров программы;
- Импорт параметров программы;
- Экспорт и импорт параметров через командную строку.

После установки KLMS на сервере с антивирусным решением следует:

1. Установить исправление для протокола `milter`, заменив исполняемый файл по пути `/opt/kaspersky/klms/libexec/klms-milter`. Исправление запрашивается заказчиком (администратором) самостоятельно в кабинете технической поддержки АО «Лаборатория Касперского».
2. Установить пакет msmtp из стандартных репозиториев системы. Данный шаг необходим для настройки отправки почтовых уведомлений непосредственно от KLMS и возможности отправки из административной панели KLMS писем, попавших в карантин. После установки пакета в директории установки необходимо создать конфигурационный файл `/etc/msmtprc` и заполнить его следующим образом:

```
defaults
auth plain
tls on
tls_starttls off
logfile # путь до логов утилиты вида path/to/log.log
host # адрес сервера «МойОфис Почта»
account system
from # учетная запись, от имени которой будут отправляться уведомления адрес вида system@domain
port 3525
user # логин в системную учетную запись из инвентарного файла «МойОфис Почта» адрес вида system@domain
password # пароль от системной учетной записи из инвентарного файла «МойОфис Почта»
account default : system
```

Выполнив все вышеперечисленные действия, администратор системы может перейти непосредственно к включению интеграции на стороне сервера «МойОфис Почта». Для этого необходимо:

1. В инвентарном файле установки в секции переменных `integrations: klms:`
   - Указать значение параметра `enabled: true`.

© ООО «НОВЫЕ ОБЛАЧНЫЕ ТЕХНОЛОГИИ», 2013–2024

– Вписать в значении параметра `host` данные, соответствующие указанным при настройке `milter` (адрес, порт, TCP-сокет). Следует отметить, что синтаксис записи в `Postfix` отличается от синтакиса `milter` (вместо знака @ используется двоеточие, порт указывается после хоста). Пример записи:

```
inet:10.10.22.22:10025
```

2. Запустить специальный плейбук для интеграции следующей командой:

```
./deploy_psn.sh <inventory> -t nginx, mail
```

6.2 Настройка интеграции с Infowatch Traffic Monitor

`InfoWatch Traffic Monitor` – DLP-система, которая предотвращает утечки конфиденциальной информации на основе полноценного контентного анализа информационных потоков.

Раздел описывает порядок и особенности настройки «МойОфис Почта» и `InfoWatch Traffic Monitor` для совместной работы. Методы развертывания DLP-системы различаются в зависимости от рабочей среды (веб-браузер, настольный и мобильный клиент).

6.2.1 Установка InfoWatch Traffic Monitor в разрыв трафика

Метод установки InfoWatch Traffic Monitor в разрыв трафика работает при использовании «МойОфис Почта» в веб-браузере, настольном или мобильном клиентах. Существует два способа перехвата информационных потоков:

– по протоколу SMTP;
– по протоколу HTTP/S.

6.2.2 Перехват SMTP-трафика методом отправки скрытой копии

В результате работы данного метода сервис Postfix, встроенный в систему InfoWatch Traffic Monitor, получает копии писем, отправленных по SMTP-протоколу. Предполагается, что письма, содержащие конфиденциальную информацию (в т.ч. файлы вложений), созданы в клиенте «МойОфис Почта». В DLP-системе создается событие для каждого из писем, информация о которых затем помещается в базу данных.

Схема работы приведена на рисунке 30:

© ООО «НОВЫЕ ОБЛАЧНЫЕ ТЕХНОЛОГИИ», 2013–2024

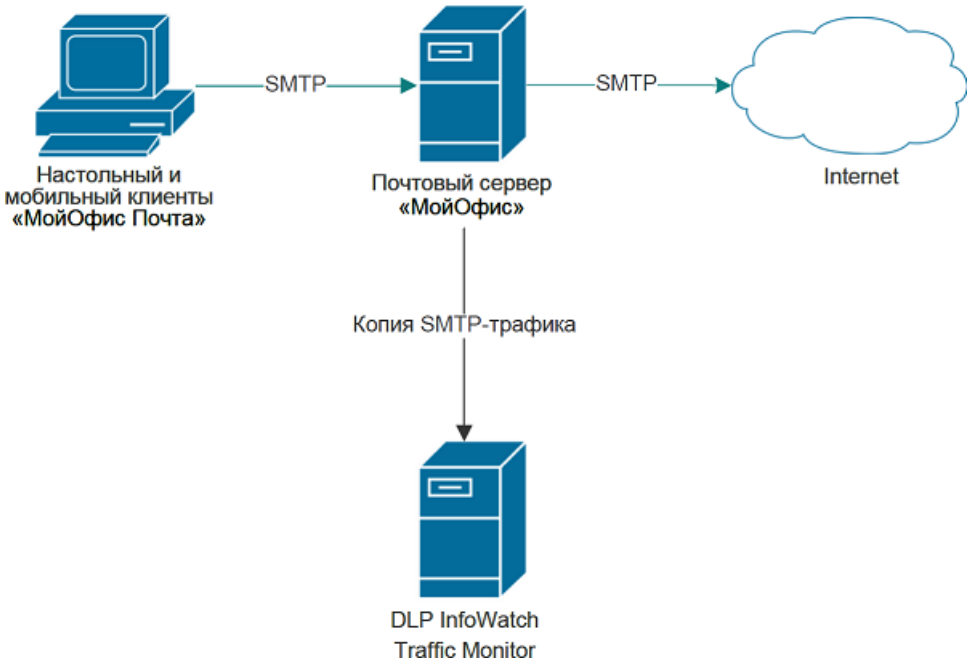


Рисунок 30 - Установка DLP Infowatch Traffic Monitor в разрыв (режим “скрытая копия”)

Для настройки перехвата трафика по SMTP-протоколу необходимо настроить правило, позволяющее отправлять скрытую копию (BCC) для каждого отправленного письма. Правило настраивается в сервисе Postfix на стороне почтовой системы (сервер «МойОфис Почта» с ролью `mail`). На вышеупомянутом сервере следует найти конфигурационный файл по следующему адресу:

```
/opt/poseidon/postfix/main.cf
```

И прописать в нем следующий параметр:

```
always_bcc = <dlp_mail_address>
```

Где `<dlp_mail_address>` – почтовый адрес домена, MX-запись которого указывает на сервер InfoWatch Traffic Monitor.

После выполнения настройки следует перезапустить контейнеризатор следующей командой:

```
docker service update psn-mail_postfix --force --with-registry-auth
```

Более подробно ознакомиться с совместимыми системами и настройкой прокси-сервера возможно в документе «Руководство администратора InfoWatch Traffic Monitor 7.1» (раздел 4.5.1 Прием копии с почтового сервера).

© ООО «НОВЫЕ ОБЛАЧНЫЕ ТЕХНОЛОГИИ», 2013–2024

6.2.3 Перехват HTTP/S-трафика методом отправки почты на корпоративный прокси-сервер

Данный метод актуален только при работе в почтовой системе «МойОфис Почта» через веб-браузер. Подмену сертификата и разбор HTTPS-трафика осуществляет корпоративный прокси-сервер.

После разбора HTTPS-трафика, прокси-сервер отправляет разобранный трафик в виде HTTP по ICAP-протоколу на сервер InfoWatch Traffic Monitor (см. Рисунок 31).

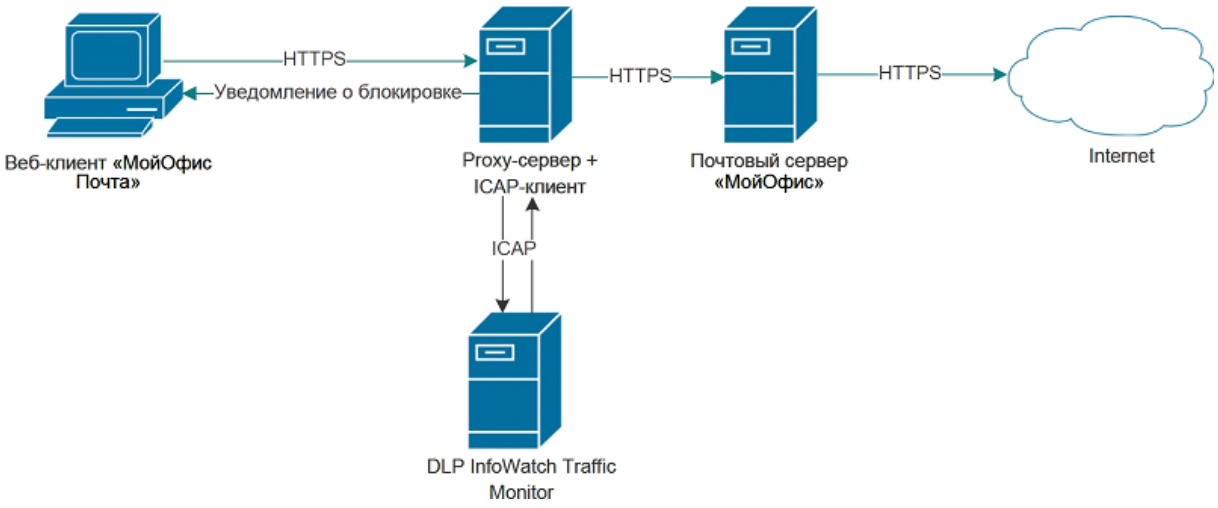


Рисунок 31 - Установка DLP Infowatch traffic monitor “в разрыв” (режим блокировки)

Существует два способа работы метода:

– **Копия** – письма, содержащие конфиденциальную информацию (в т.ч. вложения и изображения) не фильтруются, и их копии отправляются на сервер InfoWatch Traffic Monitor.
– **Блокировка** – обнаружение конфиденциальной информации происходит на уровне DLP-сервера InfoWatch Traffic Monitor. Далее производится разрешение или запрет на передачу HTTPS-трафика. При блокировке трафика конфиденциальная информация не доходит до сервера «МойОфис Почта».

Более подробно ознакомиться с совместимыми системами и настройкой прокси-сервера возможно в документе «Руководство администратора InfoWatch Traffic Monitor 7.1» (раздел «Перехват трафика, передаваемого по протоколу ICAP»).

При использовании данного метода настройки со стороны сервера «МойОфис Почта» не требуется.

Для браузера каждой клиентской рабочей станции в настройках необходимо:

© ООО «НОВЫЕ ОБЛАЧНЫЕ ТЕХНОЛОГИИ», 2013–2024

– добавить сертификат прокси-сервера в список доверенных корневых сертификатов;

– указать IP-адрес используемого прокси-сервера.

6.2.4 Установка агента InfoWatch Device Monitor

Агент InfoWatch Device Monitor работает при использовании с системой «МойОфис Почта» в веб-браузере и настольном клиенте. Весь перехваченный по протоколам HTTPS и SMTPS трафик будет отправлен для анализа на сервер Traffic Monitor.

Одним из преимуществ метода установки агента на устройства пользователей является возможность постепенного внедрения анализа трафика в организации. Недостатком данного метода является повышенное внимание к потребностям каждого пользователя. Схема взаимодействия данного метода приведена на рисунке 32:

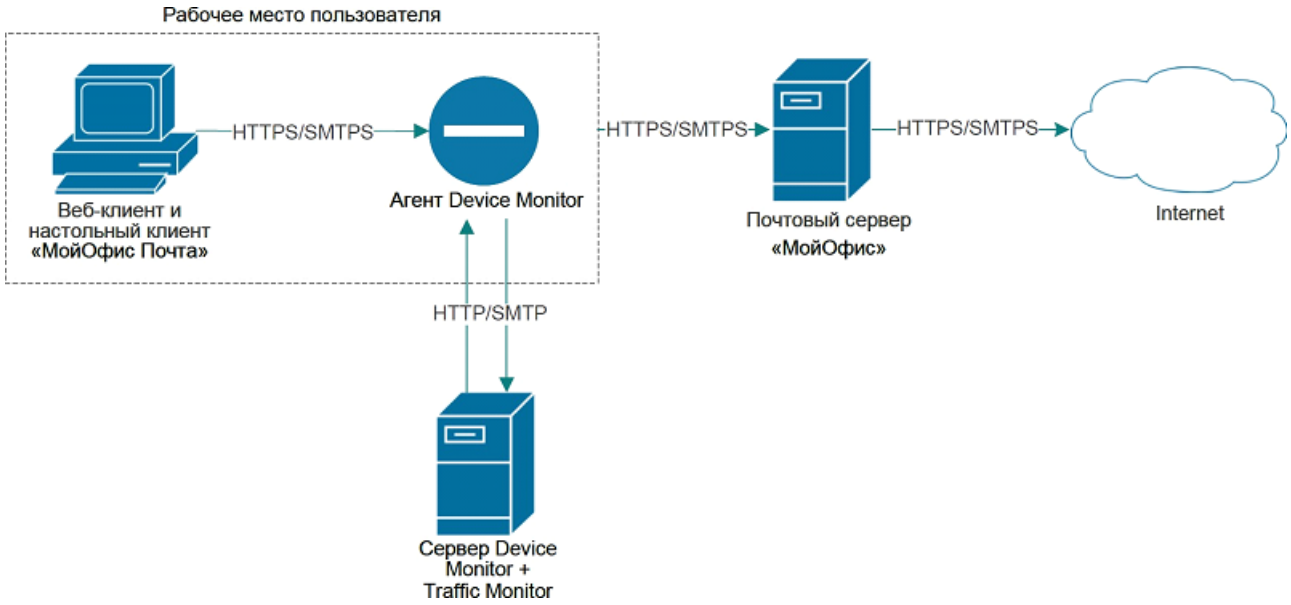


Рисунок 32 - Установка агента Infowatch Device Monitor

Обнаружение конфиденциальной информации происходит на уровне агента InfoWatch Device Monitor.

При блокировке трафика конфиденциальная информация не доходит до сервера «МойОфис Почта».

Установка агента осуществляется соответственно документу «InfoWatch Traffic Monitor. Руководство пользователя».

После установки агента InfoWatch Device Monitor для почтового клиента «МойОфис Почта», установленного в ОС Windows необходимо произвести следующие действия:

© ООО «НОВЫЕ ОБЛАЧНЫЕ ТЕХНОЛОГИИ», 2013–2024

- На машине пользователя необходимо зайти в оснастку `certlm.msc` (из меню **Пуск**).
- В дереве сертификатов найти `InfoWatch Transparency Proxy Root`:

```
Сертификаты - локальный компьютер\Доверенные корневые центры
сертификации\Сертификаты\InfoWatch Transparency Proxy Root
```

- В контекстном меню выбранного сертификата выбрать **Все задачи - Экспорт…** и экспортировать выбранный сертификат (в формате `.CER`, кодировка `DER`) на доступный локальный или сетевой ресурс.
- В почтовом клиенте «МойОфис Почта» зайти в настройки сертификатов (кнопка  - пункт меню **Настройки - Приватность и защита** - кнопка **Управление сертификатами**) и нажать кнопку **Импортировать…**
- Выбрать экспортированный ранее сертификат `InfoWatch Transparency Proxy Root`, в появившемся диалоговом окне проставить галки напротив опций:
  - Доверять при идентификации веб-сайтов;
  - Доверять при идентификации пользователей электронной почты.
- Нажать кнопку **ОК** два раза для сохранения настроек.

6.3 Интеграция со сторонней службой каталогов

Стороннюю службу каталогов возможно использовать как базу данных пользователей «МойОфис Почта». Для этого следует заполнить блок интеграции (`integrations: catalog:`) в инвентарном файле PSN (подробнее в разделе «Конфигурирование инвентарного файла: переменные» Руководства по установке почтового сервера).

Интеграция тестировалась с AD, Samba DC, FreeIPA, ALDPro, OpenLDAP и 389ds.

6.3.1 Установка квоты из сторонней службы каталогов

В AD необходимо выбрать атрибут, в котором будет храниться квота. Значение задается в байтах целым числом. Например, квота в 1Гб это 1073741824.

© ООО «НОВЫЕ ОБЛАЧНЫЕ ТЕХНОЛОГИИ», 2013–2024

На ВСЕХ нодах группы `mail` в конфигурационном файле `/opt/poseidon/dovecot/conf/dovecot-ad-pass.conf.ext` необходимо изменить секции `pass_attrs` и `user_attrs` следующим образом:

```
pass_attrs = \
  ...
  =userdb_gid=vmail, \
  атрибутad=userdb_quota_rule=*:bytes=%{ldap:атрибутad}

user_attrs = \
  ...
  =gid=vmail, \
  атрибутad=quota_rule=*:bytes=%{ldap:атрибутad}
```

(пример можно посмотреть в файле `/opt/poseidon/dovecot/conf/dovecot-ldap-pass.conf.ext`, для квот используется атрибут `quota`).

Если в атрибуте не будет задана квота или она будет равна 0, то квота считается бесконечной. Можно задать квоту по умолчанию. Если в атрибуте не задана квота, то будет использоваться она. Для этого На ВСЕХ нодах группы `mail` в конфигурационном файле `/opt/poseidon/dovecot/dovecot.conf` необходимо изменить параметр следующим образом:

```
quota_rule = *:bytes=ЗначениеКвотыПоУмолчанию
```

Далее после редактирования конфигурационных файлов перезапустить `dovecot`:

```
docker service update --force psn-mail_dovecot
```

Значение квоты по пользователям можно посмотреть через `doveadm` на любой из нод группы `mail` командой:

```
docker exec $(docker ps -qf name=dovecot) doveadm quota get -u email
```

либо через консоль администрирования PSN.

6.4 Интеграция с ВКС системами

Для интеграции с ВКС сервер должен быть продеплоен с параметрами:

- `conference.enabled=True`
- `conference.<ВКС система>.enabled=True`

© ООО «НОВЫЕ ОБЛАЧНЫЕ ТЕХНОЛОГИИ», 2013–2024

где `<ВКС система>` - требуемая ВКС система (см. «МойОфис Почта 3. Руководство по установке почтового сервера 3.1», раздел «Конфигурирование инвентарного файла: переменные»).

Если на этапе деплоя включение интеграции не было задано, можно изменить значение соответствующих переменных и перезапустить деплой командой `./deploy.sh <hosts> -t frontend` (см. «МойОфис Почта 3. Руководство по установке почтового сервера 3.1», раздел «Запуск установки»).

Либо сделать это вручную, для чего на серверах роли `frontend` необходимо выполнить следующие действия:

Изменить следующие значения в переменных конфигурационного файла `/opt/poseidon/web_calendar/config.json`:

```
"useConference": true,
"use<ВКС система>Conference": true,
```

где `<ВКС система>` - требуемая ВКС система,

и перезапустить сервис календарей командой

```
docker service update psn-frontend_web_calendar --force
```

Вышеупомянутые действия выполнять не требуется, если настройка уже была произведена в инвентарном файле до инсталляции.

6.4.1 Интеграция с сервисом TrueConf

Предварительно следует выполнить общие рекомендации, описанные в главе Интеграция с ВКС системами.

Варианты синхронизации пользователей:

- привязать `trueconf` и «МойОфис Почта» к одной службе каталогов;
- создавать соответствующих пользователей через `admin interface` в `trueconf` (см. раздел Настройки административной панели TrueConf);
- привязать `trueconf` к `ldap psn` (см. раздел Настройки административной панели TrueConf).

© ООО «НОВЫЕ ОБЛАЧНЫЕ ТЕХНОЛОГИИ», 2013–2024

6.4.1.1 Настройки административной панели TrueConf

– В административной панели TrueConf на вкладке **Веб / Настройки** в разделе **Внешний адрес веб страницы TrueConf Server** необходимо указать адрес, соответствующий значению поля `services/trueconf/url` из раздела «Конфигурирование инвентарного файла: переменные». Руководства по установке почтового сервера.
– Следующим шагом будет заполнение настроек LDAP на вкладке **LDAP / Active Directory**, раздел **LDAP**, кнопка **Настройки LDAP** в административной панели TrueConf. Пример заполнения указан в таблице 6.

Таблица 6 - Настройки LDAP административной панели TrueConf

Параметр	Значение
Тип сервера	389 Directory Server
Безопасное соединение	Да
Ручная настройка	Да
Сервер	Сервер инсталляции LDAP-сервиса «МойОфис Почта» (адрес хоста с установленным сервисом 389 Directory Server)
Порт	636
Базовый DN	`ou=People,dc=<domain>,dc=ru`, где `<domain>` – основной домен установки «МойОфис Почта».
Аутентификация	Простая
Имя	`cn=Manager,dc=<domain>,dc=ru`, где `<domain>` – основной домен установки
Пароль	Значение переменной `ds389_manage_user` из инвертарного файла установки (см. раздел «Конфигурирование инвентарного файла: переменные» Руководства по установке почтового сервера)
Включить NTLM-аутентификацию для автоматического входа пользователей домена	Да

© ООО «НОВЫЕ ОБЛАЧНЫЕ ТЕХНОЛОГИИ», 2013–2024

Параметр	Значение
Active Directory	

Заполнение настроек также необходимо и в разделе Дополнительно (см. таблицу 7):

Таблица 7 - Дополнительные настройки в административной панели TrueConf

Параметр	Значение
Login	trueconflogin
Display Name	cn
First Name	givenName
Last Name	sn
Email	mail
Max Results	50000
Filter Disabled	(!(nsrole=cn=nsdisablerole.*))
Group Member	uniqueMember
Filter Login	(trueconflogin=%s)
Filter CallID	(trueconflogin=%S)
Filter Group	(objectClass=GroupOfUniqueNames)
Work Phone	telephoneNumber
Home Phone	homePhone
TrustPartner Attr	trustPartner
FlatName Attr	flatName
TrustedDomain Filter	(objectClass=trustedDomain)
ForeignSecurityPrincipal Filter	(objectClass=foreignSecurityPrincipal)
Trust Enabled	1
Use Avatars	1
Allow Avatar Propagating	1
AddressBook Refresh	900
TimeOut	30
thumbnailPhoto Attr	thumbnailPhoto

© ООО «НОВЫЕ ОБЛАЧНЫЕ ТЕХНОЛОГИИ», 2013–2024

Параметр	Значение
jpegPhoto Attr	jpegPhoto

Остальные значение следует оставить пустыми. После заполнения всех настроек необходимо нажать кнопку Применить. При корректном заполнении всех параметров в разделе **Пользователи / Учетные записи пользователей** загрузится список учетных записей следующего вида (см. Рисунок 33):

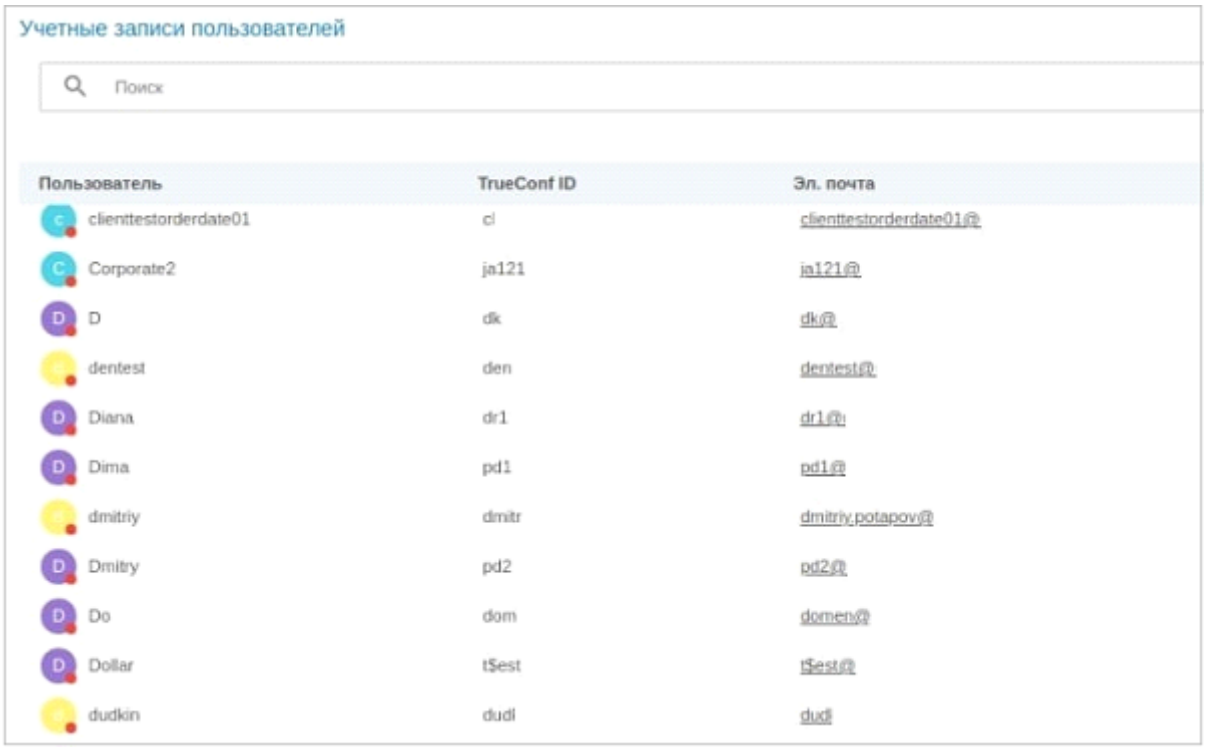


Рисунок 33 - Учетные записи «МойОфис Почта» в административной панели TrueConf

6.4.2 Настройка интеграции со Squadus

В данном разделе приведены настройки для «МойОфис Почта», остальная информация доступна в документации Squadus.

Предварительно следует выполнить общие рекомендации, описанные в главе Интеграция с ВКС системами.

Далее следует заполнить параметры ETCD в секции `services/squadus` (см. раздел Настройка ETCD). При копировании корневого сертификата из административной панели Squadus в поле ETCD `services/squadus/ca_cert` следует привести его к виду с переносом строк (Base64):

© ООО «НОВЫЕ ОБЛАЧНЫЕ ТЕХНОЛОГИИ», 2013–2024

```
-----BEGIN CERTIFICATE-----
MIID9jCCAt6gAwIBAgIUOq+mT23yNOfL68m4nddEjJjGJh4wDQYJKoZIhvcNAQEL
BQAwgZIxCzAJBgNVBAYTAlJVMQ8wDQYDVQQIEwZNb3Njb3cxDzANBgNVBAcTBk1v
c2NvdzEfMB0GA1UEChMWTmV3IENsb3VkIFRlY2hub2xvZ2llczEQMA4GA1UECxMH
.....................................................................
CXKCiw6pavWk8c3LkQaIOCTwPJOkD5hl7UyOtA7KWJd7ESmDDjtmW7iEc59GsASM
x6New1KYghE/nn7Rp8WolrO1UIkbpglHMfHHMsJEhfEE0WlZ+YV6a9RIpoxtNBdO
AvxgHMKCtDIenPor6Z2/Sjd4LxGmjoJNSNL+ild7Q65sI3pgw53NQHQfY7pVRNcf
7tAJBPPcen/ykDcTco6M5H22ENGbhkqnHyCKFdhQy7hssHzqUUzcjxPG3JToAMJf
WbFKGp1cvt3nKA==
-----END CERTIFICATE-----
```

Варианты синхронизации пользователей:

- привязать `squadus` и `psn` к одной службе каталогов или «МойОфис Частное Облако»;
- создать соответствующих пользователей через административную панель Squadus.

Для создания пользователем событий с ссылкой на конференцию сквадус пользователю необходимо хотя бы один раз удачно залогиниться в `squadus`.

6.4.3 Интеграция с сервисом Webinar

Предварительно следует выполнить общие рекомендации, описанные в главе Интеграция с ВКС системами.

Далее следует заполнить параметры ETCD в секции `services/webinar` (см. раздел Настройка ETCD).

Варианты синхронизации пользователей:

- привязать `webinar` и «МойОфис Почта» к одной службе каталогов или «МойОфис Частное Облако»;
- создать соответствующих пользователей через административную панель в `webinar`.

© ООО «НОВЫЕ ОБЛАЧНЫЕ ТЕХНОЛОГИИ», 2013–2024

6.4.4 Интеграция с сервисом VideoMost

Предварительно следует выполнить общие рекомендации, описанные в главе Интеграция с ВКС системами.

Далее следует заполнить параметры ETCD в секции `services/videomost` (см. раздел Настройка ETCD).

Варианты синхронизации пользователей:

– привязать `videomost` и «МойОфис Почта» к одной службе каталогов;
– создать соответствующих пользователей через административную панель в `videomost`.

© ООО «НОВЫЕ ОБЛАЧНЫЕ ТЕХНОЛОГИИ», 2013–2024

7 НАСТРОЙКА ETCD

ETCD – это распределенная система хранения ключей и конфигураций для сервисов. Внесение изменений в параметры ETCD предоставляет расширенные возможности для настройки системы под конкретные нужды пользователя и администратора. Для доступа к редактированию параметров в ETCD, следует выполнить следующие действия на стороне сервера инсталляции:

1. Авторизоваться в сервисе ETCD через браузер, используя адрес вида:

```
http://domain:8081
```

где `<domain>` – основной домен установки «МойОфис Почта», 8081 – порт.

2. Данные для авторизации:
   - логин `psnuser`;
   - пароль: значение переменной `etcd_browser_user` из инвентарного файла установки (см. документ «МойОфис Почта. Руководство по установке»).

После изменения настроек для их применения необходимо перезапустить backend сервисы **triton** и/или **pbm**, чтобы настройки перечитались:

```
docker service update --force psn-backend_triton
docker service update --force psn-backend_pbm
```

Параметры, доступные для изменения, приведены в таблице 8:

Таблица 8 – Параметры ETCD

Ключ	Описание	Доступные значения
`autoconfig/`	Секция настроек сервиса автоконфигурации	
`autoconfig/common/`	Секция общих настроек сервиса автоконфигурации	
`autoconfig/common/auth_salt`	Соль для подключения к глобальной адресной книге. Используется при интеграции со сторонней службой каталогов.	
`autoconfig/common/generate_ldap_account`	Генерировать запись в локальной службе каталогов для возможности подключения к глобальной адресной книге. Используется при интеграции со сторонней службой каталогов.	true или false

© ООО «НОВЫЕ ОБЛАЧНЫЕ ТЕХНОЛОГИИ», 2013–2024

Ключ	Описание	Доступные значения
autoconfig/common/log_path	Путь до лог-файла приложения	Относительный или абсолютный путь
autoconfig/common/recovery_url	Ссылка для восстановления пароля (используется в настольном клиенте)	url
autoconfig/fcm/	Секция клиентских настроек для работы с мобильными уведомлениями (Firebase Cloud Messaging и Huawei)	Информацию о настройках и их возможных значениях см. в документе «МойОфис Почта 3. Руководство по установке почтового сервера», раздел «Конфигурирование инвентарного файла: переменные»
autoconfig/fcm/exists	Включение push-уведомлений	true (строго в нижнем регистре)
autoconfig/services	Настройка внешнего доступа к сервисам для клиентов	
autoconfig/services/external_imap_host	Внешний адрес для подключения IMAP	Домен или IP-адрес
autoconfig/services/external_imap_port	Внешний порт для подключения IMAP	Цифры (целое число)
autoconfig/services/external_imap_ssl	Протокол безопасного подключения IMAP	NO/SSL/STARTTLS
autoconfig/services/external_ldap_host	Внешний адрес для подключения LDAP	Домен или IP-адрес
autoconfig/services/external_ldap_port	Внешний порт для подключения LDAP	Цифры (целое число)
autoconfig/services/external_smtp_host	Внешний адрес для подключения SMTP	Домен или IP-адрес
autoconfig/services/external_smtp_ssl	Протокол безопасного подключения SMTP	NO/SSL/STARTTLS
autoconfig/services/external_smtp_port	Внешний порт для подключения SMTP	Цифры (целое число)
autoconfig/services/external_tritonapi_url	Внешний адрес для подключения к psnapi	Строка, URL
pbm/	Секция настроек PSN Backend Manager	

© ООО «НОВЫЕ ОБЛАЧНЫЕ ТЕХНОЛОГИИ», 2013–2024

Ключ	Описание	Доступные значения
pbm/auth/	Секция настроек аутентификации в PSN Backend Manager (настройка сервиса описана в данном документе)	
pbm/auth/access_token_exp_time	время жизни access-токена в секундах	
pbm/auth/refresh_token_exp_time	Время жизни refresh-токена в секундах (для v2)	Цифры (целое число). 360000
pbm/auth/enc_salt	Соль для хэширования аутентификационных данных	Строка
pbm/common/	Общие настройки для PSN Backend Manager	
pbm/common/b24_attr_to_surname	Параметр для интеграции с Bitrix24, добавляет значение атрибута в карточке пользователя. Позволяет дифференцировать пользователей с одинаковыми ФИО	Атрибут в карточке пользователя Bitrix24. Пример: PERSONAL_ICQ
pbm/common/haar_cascade_tmpl	Используемый шаблон алгоритма распознавания лиц на фотографии. Используется в различных целях, например для обрезки фотографии для аватара.	Абсолютный путь до файла.
pbm/common/log_path	Путь до лог-файла PSN Backend Manager	Относительный или абсолютный путь
pbm/common/log_lvl	Уровень логирования	info / debug
pbm/firebase	Секция настроек подключения к Firebase Cloud Messaging и Huawei, а также параметры PBM для работы с мобильными уведомлениями	
pbm/firebase/android_bundle	Идентификатор приложения на Android, используется для составления шаблона пуша	Строка, пример: amail
pbm/firebase/aquarius_bundle	Идентификатор приложения Aquarius, используется для составления шаблона пуша	aquarius
pbm/firebase/huawei_bundle	Идентификатор приложения в консоли Huawei	Строка, пример: huawei

© ООО «НОВЫЕ ОБЛАЧНЫЕ ТЕХНОЛОГИИ», 2013–2024

Ключ	Описание	Доступные значения
pbm/firebase/ios_bundle	Идентификатор приложения в консоли iOS	Строка, пример: iosmailemb
pbm/firebase/webpush_bundle	Идентификатор web-приложения	Строка, пример: webpush
pbm/firebase/google_keyfile	Конфигурационный шаблон в формате JSON для аутентификации в Firebase Cloud Messaging	JSON, пример содержимого см. в документе «МойОфис Почта 3. Руководство по установке почтового сервера», раздел «Конфигурирование инвентарного файла: переменные».
psn/	Секция настроек серверной и web части PSN	
psn/bruteforce	Секция настроек сервиса защиты от перебора паролей	
psn/bruteforce/enabled	Включить защиту от перебора паролей	true или false
psn/bruteforce/max_attempts	Количество попыток входа, после которого IP-адрес источника блокируется. Не учитываются попытки с одной и той же неверной комбинацией логина и пароля	Целое число больше нуля
psn/bruteforce/penalty	Время в секундах, на которое блокируется IP-адрес	Целое число больше нуля
psn/cab/	Секция настроек корпоративной адресной книги	
psn/cab/bind_dn	Атрибуты bind dn административного аккаунта	Полный DN (distinguished name).
psn/cab/cab_ou	OU (organisational unit) корпоративной адресной книги	Название OU с наименованием атрибута ou=NAME. Пример: ou=CAB
psn/cab/enabled	Включает показ корпоративной книги в web-интерфейсе (false, ограничивает создание там новых пользователей)	true или false
psn/cab/host	Внутренний адрес подключения к LDAP-серверу	Домен или IP-адрес

© ООО «НОВЫЕ ОБЛАЧНЫЕ ТЕХНОЛОГИИ», 2013–2024

Ключ	Описание	Доступные значения
psn/cab/ldapusers_ou	OU (organisational unit) для привязки внешних пользователей к LDAP (в настольном клиенте)	Название OU с наименованием атрибута ou=NAME. Пример: ou=ldapusers
psn/cab/maillist_ou	OU (organisational unit) групп рассылки	Название OU с наименованием атрибута ou=NAME. Пример: ou=Groups
psn/cab/password	Пароль от административного аккаунта	Буквы, цифры или специальные символы
psn/cab/port	Внутренний порт подключения к LDAP-серверу	Цифры
psn/cab/resources_ou	OU (organisational unit) ресурсов	Название ou с наименованием атрибута ou=NAME. Пример: ou=resources
psn/cab/root_dn	Корневой DN (distinguished name) LDAP-сервера	Последние два уровня в DIT (Directory Information Tree). Пример: dc=example.myoffice-app,dc=ru
psn/cab/web_cache/enabled	Включение или отключение LDAP-кэша для web-клиента	true или false
psn/cab/web_cache/lifetime	Время жизни кэша в секундах	Цифры, пример: 3600
psn/common/	Секция общих настроек PSN	
psn/common/allow_upload_photo	Разрешение изменения аватара пользователем в web-интерфейсе	true или false
psn/common/cookie_domain	Домен PSN для хранения cookies	Строка
psn/common/event_attach_size_limit	Лимит размера вложений в события (в мегабайт)	Цифры, пример: 5
psn/common/revoke_email	Разрешить отзыв отправленных писем.	True / False.
psn/common/force_revoke	Разрешение отзыва письма пользователем, даже если оно прочитано	true или false
psn/common/gost	Подтверждение установки PSN с настройками для ГОСТ-шифрования	true или false

© ООО «НОВЫЕ ОБЛАЧНЫЕ ТЕХНОЛОГИИ», 2013–2024

Ключ	Описание	Доступные значения
psn/common/photo_path	Путь для хранения аватаров	Относительный или абсолютный путь
psn/common/password_requirements	Требования к сложности пароля. Данная политика игнорируется при интеграции с МойОфис Хранилище PGS и для учетных записей из сторонней службы каталогов.	
psn/common/password_requirements/min_length	Требования к сложности пароля: минимальное число символов.	
psn/common/password_requirements/max_length	Требования к сложности пароля: максимальное число символов.	
psn/common/password_requirements/min_digits_count	Требования к сложности пароля: минимальное число цифр.	
psn/common/password_requirements/min_uppercase_letter_count	Требования к сложности пароля: минимальное число букв в верхнем регистре.	
psn/common/password_requirements/min_lowercase_letter_count	Требования к сложности пароля: минимальное число букв в нижнем регистре.	
psn/common/password_requirements/min_spec_symbols_count	Требования к сложности пароля: минимальное число спецсимволов.	
psn/common/pgs_integration	Включение интеграции с PGS	true или false
psn/common/photo_size_limit	Лимит размера загружаемого пользователем аватара	Цифра с обозначением единицы измерения, пример: 10M
psn/common/use_friendlyname	Управление отображением имени отправителя для писем, отправленных из внешних систем	true - отображать имя отправителя письма, так как оно было передано, false - отображать дополнительно email
psn/db	Секция настроек подключения к базе данных Postgres	

© ООО «НОВЫЕ ОБЛАЧНЫЕ ТЕХНОЛОГИИ», 2013–2024

Ключ	Описание	Доступные значения
psn/db/dbname	Имя основной базы данных для web-приложения	Имя БД, пример: psn
psn/db/host	Внутренний адрес подключения к БД	Домен или IP-адрес
psn/db/login	Логин для подключения к БД	Строка
psn/db/password	Пароль для подключения к БД	Буквы, цифры или специальные символы
psn/db/port	Внутренний порт подключения к БД	Цифры
psn/db/schema	Схема (пространство имен) для БД web-приложения	Строка, пример: psn
psn/file_manager	Настройки работы менеджера файловой системы	
psn/file_manager/file_dir	Место хранения вложений в события на диске	Относительный или абсолютный путь
psn/ldap	Секция настроек подключения к LDAP userdb	
psn/ldap/bind_dn	Атрибуты bind dn административного аккаунта	Полный DN (distinguished name), пример: ou=Blocked,dc=example,dc=ru
psn/ldap/password	Пароль от административного аккаунта	Буквы, цифры и специальные символы
psn/ldap/blocked_ou	OU (organisational unit) заблокированных пользователей	Полный DN (distinguished name)
psn/ldap/domains_ou	OU (organisational unit) для хранения информации по почтовым доменам	Полный DN (distinguished name)
psn/ldap/groups_ou	OU (organisational unit) групп рассылки	Полный DN (distinguished name)
psn/ldap/people_ou	OU (organisational unit) пользователей	Полный DN (distinguished name)
psn/ldap/port	Внутренний порт подключения к LDAP-серверу	Цифры
psn/ldap/host	Внутренний адрес подключения к LDAP-серверу	Домен или IP-адрес

© ООО «НОВЫЕ ОБЛАЧНЫЕ ТЕХНОЛОГИИ», 2013–2024

Ключ	Описание	Доступные значения
psn/ldap/web_cache/enabled	Включение LDAP-кэша для web-клиента	true или false
psn/ldap/web_cache/time	Время хранения кэша	Цифры и лексическое обозначение временных единиц (на английском, через пробел). Пример: 15 minutes
psn/mail	Секция настроек внутреннего подключения к почтовым протоколам	
psn/mail/imap_host	Внутренний адрес для IMAP-подключения	Домен или IP-адрес
psn/mail/imap_port	Внутренний порт для IMAP-подключения	Цифры
psn/mail/imap_protocol	Внутренний протокол безопасного IMAP-подключения	NO/SSL/STARTTLS
psn/mail/smtp_host	Внутренний адрес для SMTP-подключения	Домен или IP-адрес
psn/mail/smtp_port	Внутренний протокол безопасного SMTP-подключения	NO/SSL/STARTTLS
psn/mail/smtp_protocol	Внутренний порт для SMTP-подключения	Цифры (целое число)
psn/mail/sieve_host	Внутренний адрес для подключения SIEVE	Домен или IP-адрес
psn/mail/sieve_port	Внутренний порт для подключения SIEVE	Цифры
psn/mail/xmailer	Уникальный для установки заголовок XMAILER в письмах	Строка, пример: example.ru poseidon webmail client
psn/mail/ios	Секция настроек профилей (конфигурационных файлов автонастройки) для устройств Apple	
psn/mail/ios/cert_path	Путь до сертификата Apple, которым подписывается профиль конфигурации	false или относительный/абсолютный путь
psn/mail/ios/key_path	Путь до ключа сертификата Apple	false или относительный/абсолютный путь

© ООО «НОВЫЕ ОБЛАЧНЫЕ ТЕХНОЛОГИИ», 2013–2024

Ключ	Описание	Доступные значения
psn/mail/service_emails	Секция настроек и информации о системных почтовых ящиках	
psn/mail/service_emails/system	Почтовый ящик системных уведомлений	email
psn/mail/service_emails/system_pass	Пароль от системного почтового ящика	Строка
psn/mail/service_emails/reminders_name	Отображаемое имя для служебных писем от подсистемы напоминаний	MyOffice Reminders
psn/mail/service_emails/system_name	Отображаемое имя для служебных писем	MyOffice System Notifications
psn/mail/service_emails/resourse_name	Отображаемое имя для служебных писем от подсистемы ресурсов	MyOffice Resources
psn/mail/signatures	Секция настроек сервиса автогенерации подписей	
psn/mail/signatures/exclusions	Исключения, для которых подпись не создается, возможно исключать домены или конкретных пользователей	JSON-массив. Пример: {"domain": ["example.com"],"users": ["user@example.ru"]}
psn/mail/signatures/ldap_mapping	Расположение полей LDAP и переменных в шаблоне подписи	JSON-массив.

psn/mail/signatures/template_path	Путь до файла с шаблоном для формирования подписей относительно /opt/triton/ в контейнере triton. В текущем релизе для изменения шаблона необходимо создать свой шаблон и указать путь до него. Рекомендуется использовать уже проброшенный в контейнер каталог /opt/poseidon/triton/eattach/, содержимое которого реплицируется в случае кластерной установки. В таком случае пример путь до нового шаблона примет вид, например, eattach/mytemplate.template.	Пример содержимого файла:
		`<div style="font-family: XO Tahion, Tahoma, sans-serif; font-size: 16px; direction: ltr">`
		`<div style=" margin-top: 2px">--</div>`
		`<div style="font-family: XO Tahion, Tahoma, sans-serif; font-size: 16px; direction: ltr; margin-top: 5px">С уважением,`
		`</div>`
		`<div style="font-family:`

© ООО «НОВЫЕ ОБЛАЧНЫЕ ТЕХНОЛОГИИ», 2013–2024

Ключ	Описание	Доступные значения
		XO Tahion, Tahoma, sans-serif; font-size: 16px; direction: ltr; margin-top: 1px "> {{FULLNAME}} {% if TITLE is defined and TITLE != "" %} {{TITLE}} {% endif %} {% if DEPARTMENT is defined and DEPARTMENT != "" %} {{DEPARTMENT}} {% endif %} {% if PHONE is defined and PHONE != "" %} {{PHONE}} {% endif %} {% if WORKPHONE is defined and WORKPHONE != PHONE and WORKPHONE != "" %} {{WORKPHONE}} {% endif %} <div style="font-family: XO Tahion, Tahoma, sans-serif; font-size: 16px;

© ООО «НОВЫЕ ОБЛАЧНЫЕ ТЕХНОЛОГИИ», 2013–2024

МойОфис

Ключ	Описание	Доступные значения
		direction: ltr;">{{MAIL}} www.myoffice.ru
psn/mail/signatures/tenant_id_list	Список тенантов, у которых включено создание подписи	JSON-массив
psn/tokens_manager	Настройки менеджера работы с аутентификационными и авторизационными токенами	
psn/tokens_manager/storage	Место хранения refresh-токенов	Значение по умолчанию, изменять не следует: db
psn/web/defaults	Секция настроек пользователя по умолчанию в веб-приложении	
psn/web/defaults/lang	Язык пользователей по умолчанию	Строка (наименование языка на английском). Пример: Russian
psn/web/defaults/tz	Часовой пояс пользователей по умолчанию	Часовой пояс в формате tz database. Пример:Europe/Moscow
psn/web/logger	Секция настроек логирования веб-приложения	
psn/web/logger/cef_enabled	Включение логирования событий	true/false
psn/web/logger/cef_filename	Имя файла журнала для сохранения информации о собитиях	cef, изменять не следует
psn/web/logger/cef_prefix	Префикс для SIEM подсистемы. Генерируется автоматически на этапе деплоя	CEF:23|MyOffice|MyOffice Mail|
psn/web/logger/date	Формат даты в лог-файлах web-приложения	Срока, стандарт datetime. Пример:D, Y-m-d H:i:s O

© ООО «НОВЫЕ ОБЛАЧНЫЕ ТЕХНОЛОГИИ», 2013–2024
99

Ключ	Описание	Доступные значения
psn/web/logger/default	Название лог-файла по умолчанию	Строка
psn/web/logger/dir	Путь хранения логов	Относительный или абсолютный путь
psn/web/logger/format	Формат строки в лог-файле	Строка с переменными лог-файлов. Пример:%date% [%type %] %message%
psn/web/logger/loglevel	Уровень логирования syslog	Число от 0 до 8: EMERGENCY 0, CRITICAL 1, ALERT 2, ERROR 3, WARNING 4, NOTICE 5, INFO 6, DEBUG 7, CUSTOM 8
psn/web/secure	Секция настроек безопасности и шифрования	
psn/web/secure/cipher	Алгоритм шифрования	Строка (наименование алгоритма), пример: aes-128-cbc
psn/web/secure/jwt_key	Ключ JSON Web Token (JWT)	Строка
psn/web/secure/key	Открытый ключ Encryption/Decryption	Строка
psn/web/secure/secret_key	Закрытый ключ Encryption/Decryption	Строка
psn/web/websocket	Секция настроек работы с протоколом WebSocket	
psn/websocket/calendar_sync	Синхронизация событий при помощи WebSocket	true или false
psn/zoom_info	Параметры Zoom для ресурса	Пример как сделать zoomdemo@url.domain Zoom-комнатой: {"zoomdemo@url.domain" :"link":"https:\/ \/us02web.zoom.us\/j\/123? pwd=123" ,"login" :"zoom@url.domain" ,"password":"1234"}}

© ООО «НОВЫЕ ОБЛАЧНЫЕ ТЕХНОЛОГИИ», 2013–2024

Ключ	Описание	Доступные значения
push/aquarius/server_api_key	API-ключ для включения веб-пушей Aquarius	API-ключ из настроек Aquarius
push/firebase/	Секция клиентских настроек для работы с мобильными уведомлениями (Firebase Cloud Messaging и Huawei)	Информацию о настройках и их возможных значениях см. в документе «МойОфис Почта 3. Руководство по установке почтового сервера», раздел «Конфигурирование инвентарного файла: переменные».
services	Секция внешних настроек подключения к сервисам	
services/ad	Секция настроек параметров импорта адресной книги из сторонней службы каталогов	
services/ad/groups	Секция настроек параметров импорта групп рассылок в адресную книгу	
services/ad/groups/aliases	Алиасы (псведонимы) для групп, импортированных из сторонней службы каталогов	Пары "ключ":"значение", заключенные в фигурные скобки { }, пример {"test@example.com": "test@domain.ru"}
services/ad/groups/cab_exclusions	Массив групп рассылок, которые не будут добавлены в адресную книгу	Набор значений, разделенных запятыми. Находится внутри квадратных скобок []. Пример: ["test1@test.ru", "test2.test.ru"]
services/ad/groups/base_dn	Полный DN (distinguished name)	Строка
services/ad/groups/filter	Фильтр групп рассылок	Рекомендованное значение для AD: (&(objectClass=group)(mail=*)). Рекомендованное

© ООО «НОВЫЕ ОБЛАЧНЫЕ ТЕХНОЛОГИИ», 2013–2024

Ключ	Описание	Доступные значения
		значение для FreeIPA/ALDPro/OpenLDAP/389 ds: (&(objectClass=groupOfNames)(mail=*))
services/ad/groups/mapping	Задает соответствие атрибутов групп рассылок между сторонней и локальной службой каталогов	Пары "ключ":"значение", заключенное в фигурные скобки «{ }. Где ключ - атрибут в AD, а значение - ключ в LDAP. Значение по умолчанию: {"mail":"mail","cn":"cn","displayname":"displayname"}
services/ad/groups/rename_domains	Задает возможность изменять домен всех групп рассылок при импорте	Пары "ключ":"значение", заключенные в фигурные скобки { }. Пример: {"test.com": "test.ru"}.
services/ad/groups/rename_emails	Задает возможность изменять почтовые адреса	Пары "ключ":"значение", заключенные в фигурные скобки { }. Пример: {"test@domain.ru": "alias@domain.ru"}
services/ad/enabled	Включение синхронизации адресной книги с Active Directory	true или false
services/ad/host	Адрес контроллера домена	Строка
services/ad/password	Пароль учетной записи, от имени которой будет осуществляться вход и поиск по БД службы каталогов	
services/ad/port	Порт для подключения к службе каталогов по протоколу LDAP	Цифры. Обычно принимает значения 389 (для подключения без шифрования) или 636 (с шифрованием)

© ООО «НОВЫЕ ОБЛАЧНЫЕ ТЕХНОЛОГИИ», 2013–2024

Ключ	Описание	Доступные значения
services/ad/ssl	Использование протокола с шифрованием	true или false
services/ad/users	Секция настроек параметров импорта пользователей в адресную книгу	
services/ad/users/base_dn	Полный DN (distinguished name)	Строка
services/ad/users/filter	Фильтр пользователей	Значение по умолчанию (&(objectClass=person)(mail=*))
services/ad/users/mapping	Соответствие атрибутов пользователей между сторонней и локальной службой каталогов	Пары "ключ":"значение", заключенные в фигурные скобки { }. Где ключ - атрибут в AD, а значение - ключ в LDAP. Значение по умолчанию: {"mail":"mail","cn":"cn","displayname":"displayname","title":"title","physicaldeliveryofficename":"physicaldeliveryofficename","telephonenumber":"telephonenumber","mobile":"mobile","streetaddress":"streetaddress","l":"l","sn":"sn"}
services/bitrix24	Секция настроек подключения к API Bitrix24	
services/bitrix24/admin_userid	ID административного аккаунта	Строка
services/bitrix24/enabled	Включение синхронизации адресной книги с Bitrix24	true или false
services/bitrix24/url	URI системы Bitrix24	uri, пример: https://example.b24.ru
services/bitrix24/webhook	Аутентификационный токен для получения данных пользователей	Строка

© ООО «НОВЫЕ ОБЛАЧНЫЕ ТЕХНОЛОГИИ», 2013–2024

Ключ	Описание	Доступные значения
services/co	Секция настроек интеграции к CO	
services/co/landing_url	URL-адрес для лендинга CO	Строка
services/co/public_link_url	Публичная ссылка для файлов PGS	Строка
services/co/psn_mail{{external_domain}}	Настройка PSN как клиента Single Sign-On для CO.	Пример: {"client_secret":"MAIL_OAUTH2_CLIENT_SECRET","redirect_uri":"https://mail{{external_domain}}/sso","client_id":"psn","sso_url":"https://auth{{external_domain}}"}
services/doveadm	Секция настроек подключения к HTTP API Doveadm	
services/doveadm/login	Логин административного аккаунта в Doveadm	Значение из конфигурационного файла PSN
services/doveadm/url	URI для HTTP-доступа к Doveadm	uri, пример: http://dovecot:2222/doveadm/v1
services/pbm	Секция настроек подключения к API Poseidon Backend Manager	
services/pbm/pbm_url	Внутренний URL PBM API	url
services/policy_api	Секция настроек Postfix Policy Server	
services/policy_api/token	Токен авторизации Postfix Policy Server	
services/pps/db	Секция настроек Postfix Policy Server для подключения к БД Postgres	
services/pps/dbname	Имя основной базы данных приложения	Имя БД, пример: psn

© ООО «НОВЫЕ ОБЛАЧНЫЕ ТЕХНОЛОГИИ», 2013–2024

Ключ	Описание	Доступные значения
services/pps/host	Внутренний адрес подключения к БД	Домен или адрес
services/pps/login	Логин для подключения к БД	Строка
services/pps/password	Пароль для подключения к БД	Буквы, цифры или специальные символы
services/pps/port	Внутренний порт подключения к БД	Цифры
services/pgs	Секция настроек подключения к сервисам PGS	
services/pgs/adminapi_login	Логин в Adminapi PGS	Значение из конфигурационного файла PGS
services/pgs/adminapi_password	Пароль от Adminapi PGS	Значение из конфигурационного файла PGS
services/pgs/adminapi_url	Внешний URL Adminapi PGS	url
services/pgs/api_url	Внешний URL PGSAPI	url
services/psnapi	Секция настроек подключения к PSN RESTAPI	
services/psnapi/admin_login	Логин административного аккаунта в PSN RESTAPI	Значение из конфигурационного файла PSN
services/psnapi/url	Внешний URL PSN RESTAPI	url
services/redis	Секция настроек подключения к БД Redis	
services/redis/host	Хост для БД Redis	Строка (адрес домена)
services/redis/password	Пароль от БД Redis	Значение из конфигурационного файла PSN
services/redis/port	Порт для БД Redis	Цифры

© ООО «НОВЫЕ ОБЛАЧНЫЕ ТЕХНОЛОГИИ», 2013–2024

Ключ	Описание	Доступные значения
services/redis/sentinel_enabled	Используется ли система сборки кластера Redis Sentinel	true или false
services/squadus/	Секция настроек интеграции со Squadus	
services/squadus/ca_cert	Корневой сертификат из настроек Jitsi мессенджера Squadus	Строка
services/squadus/conference_url	URL конференции	Строка вида https://im-<squadus_domain>/call
services/squadus/delete_after	Устанавливаемый таймаут для интеграции	Значение в секундах, по умолчанию 120
services/squadus/enabled	Включение интеграции со Squadus	true или false
services/squadus/host	Хост сервиса без порта из настроек Jitsi мессенджера Squadus	Строка
services/squadus/port	Порт сервиса из настроек мессенджера Squadus	Число
services/squadus/squadus_client	Цепочка сертификатов в формате PEM	Строка
services/squadus/squadus_key	Приватный ключ в формате PEM	Строка
services/squadus/service_url	URL доступа к Squadus	Строка вида https://im-<squadus_domain>
services/trueconf	Секция настроек подключения к сервису видеоконференций Trueconf	
services/trueconf/delete_after	Время в секундах, по прошествии которого с конца	Цифры (целое число), пример: 1234000

© ООО «НОВЫЕ ОБЛАЧНЫЕ ТЕХНОЛОГИИ», 2013–2024

Ключ	Описание	Доступные значения
	события конференция будет удалена	
services/trueconf/enabled	Включение интеграции с Trueconf	true или false
services/trueconf/url	URL для API Trueconf	url
services/trueconf/client_secret	Секретный ключ, получаемый при создании приложения OAuth для Trueconf	Более подробно о значении возможно узнать по ссылке
services/trueconf/client_id	Идентификатор, получаемый при создании приложения OAuth для Trueconf	Более подробно о значении возможно узнать по ссылке
services/videomost/enabled	Включение интеграции с videomost	true или false
services/videomost/url	Videomost API URL	Строка (https://im2.videomost.com)
services/videomost/auth_url	URL для аутентификации Videomost	Строка (http://im2.videomost.com:8443)
services/videomost/secretword	Параметр авторизации в Videomost	Строка
services/webinar/enabled	Включение интеграции с webinar	true или false
services/webinar/api_url	Webinar API URL	Строка (https://userapi.webinar.ru/v3)
services/webinar/auth_token	Токен для Webinar API	Строка

© ООО «НОВЫЕ ОБЛАЧНЫЕ ТЕХНОЛОГИИ», 2013–2024

8 МОНИТОРИНГ

«МойОфис Почта» предоставляет возможность использования встроенной системы мониторинга, которая становится доступна в случае указания группы хостов monitoring инвентарного файла установки.

Встроенная система мониторинга состоит из трех основных компонент:

- **Prometheus** – производит сбор и хранение метрик;
- **Loki** – производит сбор и хранение логов;
- **Grafana** – обеспечивает визуализацию метрик и логов.

Данные компоненты работают совместно для обеспечения достаточного уровня мониторинга и анализа работы системы. Визуализация данных производится в дашбордах Grafana (наборах предустановленных графических панелей).

Для входа в систему мониторинга необходимо:

1. В браузере перейти на URL: https://grafana-<domain>, где <domain> – основной домен установки «МойОфис Почта».
2. На странице авторизации:
   - В поля **Email or username** и **Password** ввести корректные логин и пароль пользователя, соответствующие инвентарному файлу установки;
   - Нажать кнопку **Log In**.

После успешной авторизации будет произведен переход на страницу со списком дашбордов **Dashboards** (см. Рисунок 34).

© ООО «НОВЫЕ ОБЛАЧНЫЕ ТЕХНОЛОГИИ», 2013–2024

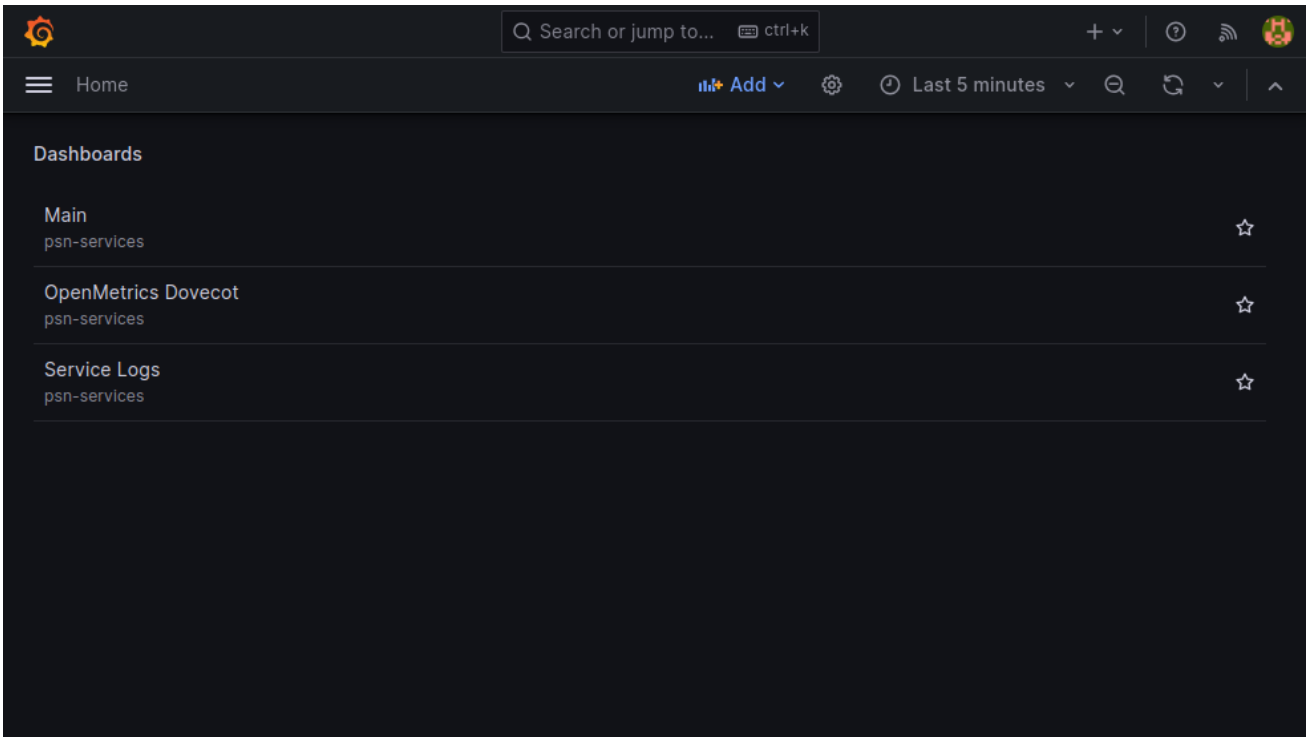


Рисунок 34 – Страница со списком дашбордов

8.1 Описание дашборда OpenMetrics Dovecot

Дашборд **OpenMetric Dovecot** предназначен для оценки работы почтового сервера в справочных целях. Он имеет следующие панели:

- **Throughput** – служит для оценки количества запросов почтового сервера в секунду (RPS, англ. Requests Per Second) в разрезе нескольких нод (см. Рисунок 35);
- **Latency, 95%** – служит для оценки длительности выполнения IMAP команд (см. Рисунок 36);
- **SUCCESS и BAD** – служат для отображения количества удачных и неудачных IMAP запросов (см. Рисунок 37).

© ООО «НОВЫЕ ОБЛАЧНЫЕ ТЕХНОЛОГИИ», 2013–2024

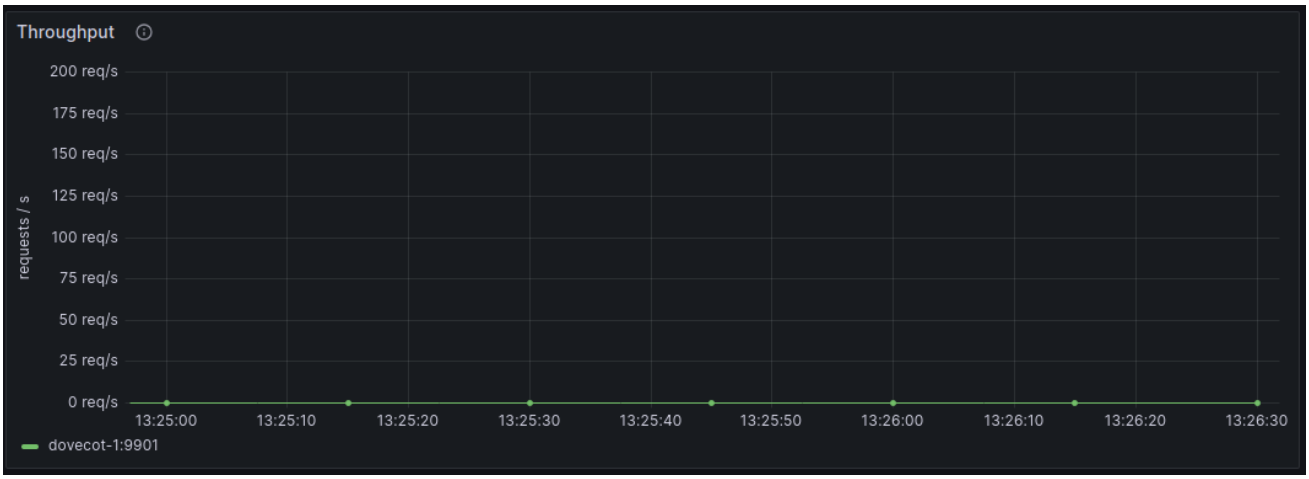


Рисунок 35 – Панель Throughput

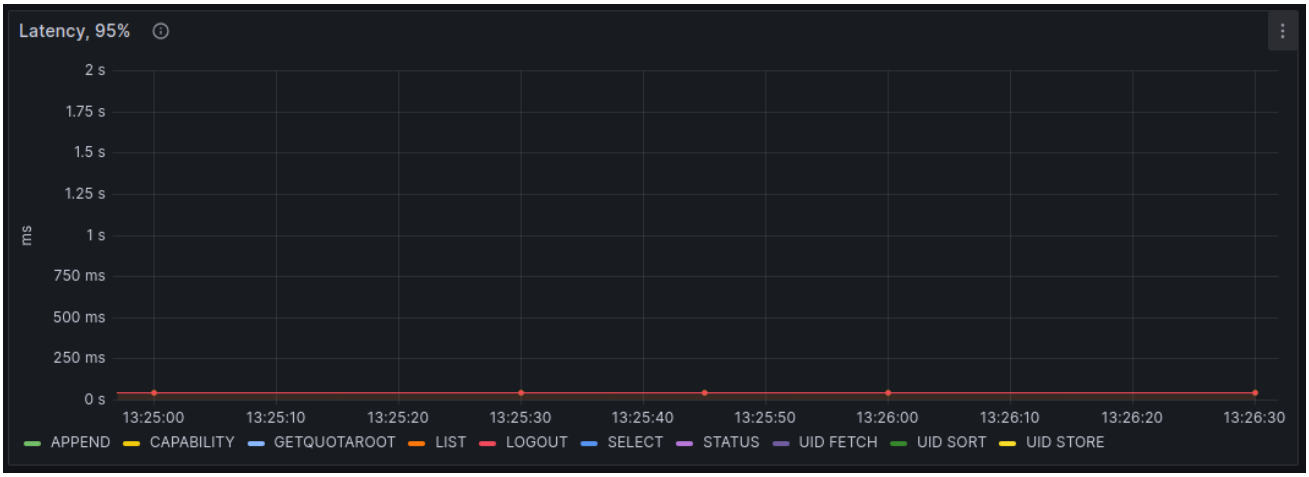


Рисунок 36 – Панель Latency, 95%

Рисунок 37 – Панели SUCCESS и BAD

Для построения графиков используются данные, поступившие от компонента **Prometheus**. Собранные компонентом **Prometheus** данные хранятся 24 часа.

8.2 Описание дашборда Service Logs

Дашборд **Service Logs** предназначен для визуализации логов приложений. Он имеет панель **Logs**, где отображаются логи всех сервисов в виде журнала (см. Рисунок 38).

© ООО «НОВЫЕ ОБЛАЧНЫЕ ТЕХНОЛОГИИ», 2013–2024

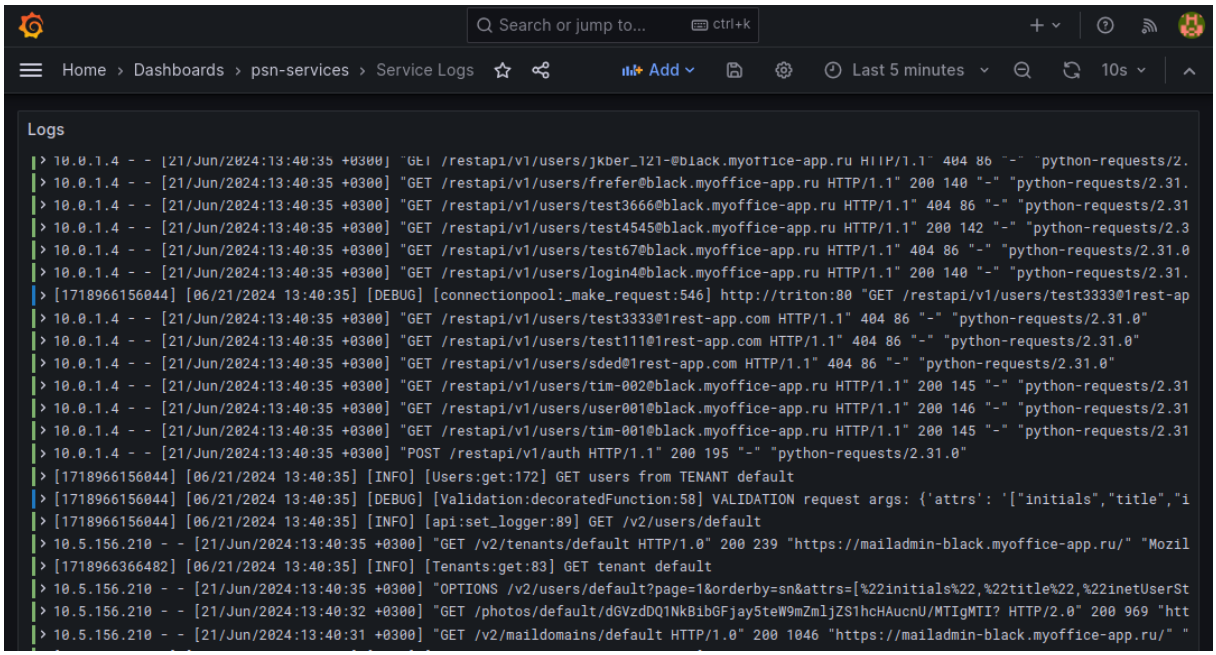


Рисунок 38 – Панель Logs

Для отображения логов используются данные, поступившие от компонента **Loki**. Собранные компонентом **Loki** данные хранятся 72 часа.

© ООО «НОВЫЕ ОБЛАЧНЫЕ ТЕХНОЛОГИИ», 2013–2024

9 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

«МойОфис Почта» позволяет использовать стороннее программное обеспечение с целью повышения информационной безопасности.

9.1 Антиспам

Для фильтрации спама «МойОфис Почта» использует программное обеспечение Rspamd.

Программное обеспечение Rspamd – это современная система фильтрации спама, которая позволяет оценивать письма по ряду правил, включая регулярные выражения, статистический анализ и пользовательские сервисы.

Более подробно о настройке данного программного обеспечения рассказано в документации Rspamd.

9.2 Сбор и анализ логов

Логирование на сервере «МойОфис Почта» производится в журнальные файлы соответствующего сервиса. К данным сервисам относятся элементы почтового ядра:

- postfix (пересылка почты, статистика по письмам);
- dovecot (получение почты, подключения к imap-серверу);
- rspamd (антиспам-фильтр).

Также логи в почтовой системе «МойОфис Почта» собирают следующие сервисы:

- triton (backend веб-интерфейса);
- pbm (Poseidon Backend Manager);
- nginx (прокси-сервер);
- autoconfig (сервис распространения автоконфигурации для клиентов).

Для доступа к директории логов необходимо войти на сервер установленной системы под аккаунтом администратора или супер администратора. По умолчанию путь к директории логов выглядит следующим образом:

```
cd /opt/poseidon/logs/syslog-collector/<service>-all.log
```

Где `<service>` – один из вышеуказанных сервисов. Пример для postfix:

© ООО «НОВЫЕ ОБЛАЧНЫЕ ТЕХНОЛОГИИ», 2013–2024

```
cd /opt/poseidon/logs/syslog-collector/postfix-all.log
```

Просмотр журнальных файлов сервисов осуществляется штатными средствами системы, например редактором Vim:

```
vim /opt/poseidon/logs/syslog-collector/<log>.log
```

© ООО «НОВЫЕ ОБЛАЧНЫЕ ТЕХНОЛОГИИ», 2013–2024

10 КОДЫ И РАСШИФРОВКА ОШИБОК В КОНСОЛИ

При возникновении ошибки в API-запросе, консоль может выдать следующие сообщения:

1. **Ошибка 400**: Не переданы обязательные параметры команды (указаны в данном руководстве, как обязательные, или выделены полужирным шрифтом).

```
{
     "message":
     {
         "{REQUIRED_PARAM_NAME}": "{REQUIRED_PARAM_NAME} is a required value"
     }
}
```

2. **Ошибка 401**: Истек срок действия токена. Необходимо пересоздать токен авторизации (раздел 2.4.1 данного руководства).

```
{
    "message": "TOKEN EXPIRED"
}
```

3. **Ошибка 403**: Доступ запрещен. Необходимо проверить права доступа к ресурсу.

```
{
     "message": "You don't have the permission to access the requested resource.
It is either read-protected or not readable by the server."
}
```

© ООО «НОВЫЕ ОБЛАЧНЫЕ ТЕХНОЛОГИИ», 2013–2024

11 ТЕХНИЧЕСКАЯ ПОДДЕРЖКА

Контактная информация службы технической поддержки ООО ««Новые облачные технологии» в случае возникновения вопросов, не описанных в данном руководстве:

Адрес электронной почты: support@service.myoffice.ru

Телефон: 8-800-222-1-888.

© ООО «НОВЫЕ ОБЛАЧНЫЕ ТЕХНОЛОГИИ», 2013–2024