

Руководство администратора AlterOffice Облако

2023 г.

Содержание

Часть I	Аннотация	3
Часть II	Общее описание	4
Часть III	Настройки системы	6
1	Общие сведения	6
2	Основные параметры	6
	Выполнение фоновых заданий	6
	Настройка почтового сервера в графическом режиме	9
	Настройка почтового сервера через консоль	
3	Общий доступ	
	Общии доступ к фаилам внутри сервера Настройка доступа к федерации облачных хранидиш	
4	Безопасность	
	Шифрование	
	Использование HTTPS	16
	Включение SSL	17
-	Правила задания паролей	
5	модуль календарь	
6	Модуль Разговор	
	Настройка TURN-сервераКоманди и ОСС для настройки разгороров	
7	AlterOffice Облако	
	Обзор использования	32
	Журналирование	
Часть IV	Приложения	35
1	Работа с приложениями в командной строке	35
Часть V	Пользователи	37
1	Создание нового пользователя	37
2	Группы пользователей	38
3	Сброс пароля	39
	Сброс пароля пользователя	39
	Сброс пароля администратора	39
4	Управление пользователями	40
Часть VI	Операции с файлами в хранилище	41
Часть VII	Сообщения администратору	43

3

1 Аннотация

Настоящий документ является руководством администратора сервера AlterOffice Облако.

В документе приведены общие принципы работы и настройки сервера в графическом режиме и через консоль. Предполагается, что администратором сервера является пользователь, имеющий опыт в администрировании.

2 Общее описание

4

AlterOffice Облако – многокомпонентный программный продукт, предоставляющий пользователям широкие возможности облачного офиса и файлового хранилища.

AlterOffice Облако позволяет организовать безопасное хранение, совместное использование и синхронизацию файлов для организации работы любого масштаба.

Пакет офисных онлайн редакторов поддерживает создание и редактирование документов в режиме реального времени, а также поддерживают импорт и экспорт всех популярных форматов файлов.

Функциональные возможности облачного офиса позволяют организовать совместную работу пользователей над документами и хранит версионность файлов.

Полное описание функциональных возможностей сервиса рассмотрено в документе «Руководство пользователя AlterOffice Облако». Далее рассмотрим возможности администратора сервера.

Доступ к модулю администратора в графическом режиме осуществляется через кнопку личного профиля в правом верхнем углу экрана (см. на рисунке ниже).

🦺 號 🖿 🗕 🗛 🖾 Q	4 8	۹ ۴ 🕼
Все файлы Недавать изменёлоние Избранные Спубликованные редурсы	• • • • • • • • • • • • • • • • •	Новая презентация ррт Настройки Надавно изменено Истримозсения Ш Польователи Р Польователи Р Польователи
Merron	D Mass -	Размер 🕑 Винётия
	Тестовый документ.боск	🛫 7 1/3 8 дней назад
	Видео	🖉 Общий д ··· 454 КВ месяц назад
	Документы	🔩 🚥 2,7 МВ месяц назад
Koosana	Изображения	на на 532 № 24 дня назад
 Motionacoeaero 15 MB vis 1 GB 		< 4 КЗ 11 дней назад
О Настройки	Виступление на конференции pptx	 212 K8 10 дней назад

Переход к модулю администрирования сервера

Далее функциональные настройки распределены по разделам:

- Настройки, где выполняются настройки личного профиля и все основные конфигурации сервера;
- Приложения, где можно подключить к системе дополнительные приложения или отключить действующие;
- Пользователи, где выполняется управление пользователями системы;
- Помощь, где находиться вся справочная информация по работе с системой;
- Выйти, для выхода из системы.

5

Далее рассмотрим подробнее возможности администратора сервера по работе с системой и настройке конфигураций сервера.

3 Настройки системы

Основные настройки системы Администратор сервера может выполнить, перейдя в раздел **Настройки** и далее в блок **Администрирование**.

A	Alter Office 4 🖬 Q	4 🗎		* e 🔒
	Личное			
i	Личная информация	Аватар 🚢 -	Полное имя 😃 -	Адрес эл. почты 🕮 -
	Безопасность		Nadezhda	email@email.ru
4	События			Для сброса пароля и уведомлений
<	Общий доступ		Номер телефона 🔒 -	Адрес 🚔 -
O.	Конфиденциальность	•	+ 79998887766	Ваш почтовый адрес
	AlterOfficeOnline	рпд или јрд, макс. 20 МБ		
	Администрирование	Подробные сведения		
E	Общие сведения	Вы являетесь участником следующих	Сайт 🔒 🗸	Twitter 🚔 -
¢	Основные параметры	rpynn: TestGroup, admin	Ссылка https://	Имя в Twitter @
۹	Поддержка	Вы используете 15 MB из 1 GB (1 %)		
<	Общий доступ			
۵	Безопасность			Риссиий (Россия)
n	Темы оформления			Русский (Россия)

Блок Администрирование

3.1 Общие сведения

Во вкладке **Общие сведения** указываются сведения о проверке параметров безопасности текущей конфигурации сервера. Ознакомьтесь с результатами проверки в блоке **Проверка безопасности и параметров**.

В блоке **Версия** указывается информация о текущей версии системы, установленной на вашем сервере. Для выполнения обновлений системы или проверки наличия обновлений нажмите на кнопку **Открыть окно обновления**.

AlterOffice Облако может автоматически направлять информационное письмо о наличии обновлений для сервера. Для этого внесите названия групп пользователей, которым будут направлены уведомления, в соответствующее поле ввода в блоке **Версия**.

3.2 Основные параметры

3.2.1 Выполнение фоновых заданий

Некоторые задачи на сервере AlterOffice Облако могут выполняться автоматически в фоновом режиме и без участия пользователя, после их настройки администратором сервера.

Автоматические задания cron настраиваются администратором с определенной периодичностью запуска или выполняются в фиксированное время и дату и записываются в файл cron.php.

Задачи сгоп могут быть настроены на сервере тремя способами: AJAX, Webcron или сгоп (см. рисунок ниже).

Фоновые задания 🔵 Последнее задание выполнено 1 минута назад. i
For optimal performance it's important to configure background jobs correctly. For bigger instances 'Cron' is the recommended setting. Please see the documentation for more information
Выполнять одно задание с каждой загруженной страницей
O Webcron cron.php зарегистрирован в службе webcron и будет вызываться каждые 5 минут по HTTP.
○ Cron Использовать системный сгоп для вызова файла сгоп.php каждые 5 минут. сгоп.php должен исполняться из под пользователя "apache".

Типы выполнений фоновых заданий в AlterOffice Облако

Далее кратко рассмотрим особенности этих методов.

AJAX

Данный метод выполнения фоновых задач используется на сервере по умолчанию. При использовании AJAX на сервере выполняется одно фоновое задание каждый раз, когда пользователь посещает страницу системы AlterOffice. Данный способ выполнения фоновых заданий не является самым надежным, а также требует регулярных посещений пользователем страницы для выполнения заданий.

Данный механизм не требует авторизаций и доступа к дополнительным серверам и сервисам.

Обратите внимание, что при работе с приложениями, хранилищем или многопользовательской работе на сервере рекомендуется использовать метод cron.

Webcron

Данный способ может быть использован для маленького количества пользователей на сервере (от 1 до 5).

Для использования данного метода необходима регистрация вашего файла cron.php на внешнем сервере Webcron к которому будет осуществляться доступ по сети Интернет, где будет обеспечиваться регулярное исполнение ваших заданий.

Поскольку доступ к стороннему серверу Webcron будет осуществляться через веб-ресурсы по протоколам HTTP, данный тип доступа ограничит количество обращений сервера. Чтобы избежать прерываний заданий за каждый вызов сервера, выполняется только одно задание. При вызове сервера каждые 5 минут, в день будет доступно выполнение только 288 фоновых заданий, что не всегда подходит для Cron

Данный метод является предпочтительным для выполнения обычных фоновых задач и не обладает ограничениями, как решение Webcron.

Для запуска заданий Cron в Unix системах настройте данное cron задание для запуска cron.php от имени вашего установленного Web-cepвepa (обычно www-data или wwwrun):

crontab -u www-data -e

И добавьте в файл строку:

*/5 * * * * php -f /var/www/alteroffice/cron.php

Для проверки добавления и выполнения задания выполните:

crontab -u www-data -l

В ответ вы должны получить следующий ответ:

[snip]

*/5 * * * * php -f /var/www/alteroffice/cron.php

Важно отметить, что если в разделе настроек Администратора не выбран метод выполнения фоновых задач Cron, то после запуска файла **cron.php** в данном разделе этот метод установится автоматически.

Systemd

Если в системе работает Systemd, то встроенный таймер Systemd может заменить отложенные задачи cronjob.

Для реализации данного решения необходимо создать два файла: **alteroffice.service** и **alteroffice.timer** в /etc/system/.

Файл **alteroffice.service** должен иметь следующее содержание:

[Unit] Description=alteroffice cron.php job

[Service] User=www-data ExecStart=/usr/bin/php -f /var/www/alteroffice/cron.php KillMode=process

Где необходимо заменить имя пользователя www-data на имя пользователя вашего http-cepвepa и /var/www/alteroffice/cron.php на местоположение файла cron.php на вашем сервере, если оно отличается.

Файл alteroffice.timer должен иметь следующее содержание:

[Unit]

Description=Run Alteroffice cron.php every 5 minutes

[Timer]

OnBootSec=5min OnUnitActiveSec=5min Unit=alteroffice.service

[Install] WantedBy=timers.target

Где параметр OnBootSec запускает таймер автоматически через 5 минут после загрузки системы. Без данного параметра автоматическая загрузка выполнена не будет. Параметр OnUnitActiveSec устанавливает 5 минутный таймер после последней активации сервисного устройства.

Для включения и запуска таймера выполните команду: systemctl enable --now alteroffice.timer

3.2.2 Настройка почтового сервера в графическом режиме

Настройки почтового сервера осуществляются в блоке **Почтовый сервер**, где задается сервер для приемки и отправки электронной почты. Данный сервер должен обладать возможностью отправлять сообщения для таких системных действий, как сброс паролей и отправка уведомлений от сервера. Настройка уведомлений от сервера происходит в разделе **Настройка** на вкладке **События** и может регулироваться пользователем.

Почтовый сервер і

Способ отправки	SMTP	•	Шифрование	SSL/TLS	•
Адрес отправителя			@ ·		
Метод проверки подлинности	Простой	-	У Требуется	аутентифи	кация
Адрес сервера			:		
Учётные данные					Сохранить

Параметры настройки почтового сервера

С помощью настройки доступа к почтовому серверу через графический интерфейс AlterOffice будут автоматически заполнены все значения команд в файле **config/config.php**, после чего выполнено подключение к почтовому серверу.

В AlterOffice Облако поддерживается два типа подключения к почтовому серверу: SMTP, и Sendmail. Конфигурация SMTP используется для удаленного сервера, конфигурация Sendmail для почтовых серверов, находящихся на том же сервере, что и AlterOffice Облако.

Для настройки вашего SMTP-сервера в AlterOffice Облако необходимо заполнить следующие параметры:

- выбрать тип шифрования: отсутствует, SSL/TLS или STARTTLS;
- внести адрес отправителя, для исходящих писем с сервера AlterOffice Облако;
- выбрать метод проверки подлинности: нет, проверка через логин, простой или через менеджера NT LAN;
- в параметр Адрес сервера внести IP-адрес сервера или полное доменное имя и после знака двоеточия номер порта SMTP;
- учетные данные для входа на ваш почтовый сервер.

Для проверки правильности внесенных данных можно отправить проверочное письмо (которое будет направлено на почтовый ящик, указанный в личном профиле Администратора сервера), нажав на кнопку **Отправить** сообщение.

Настройка Sendmail

Для настройки Sendmail выберите соответствующий параметр в поле Способ отправки и далее введите желаемый обратный адрес электронной почты.

	Способ отправки	Sendmail	• Pe	жим sendmail	smtp (-bs) 🔻
	Адрес отправителя	example	0	name.ru	smtp (-bs)
					pipe (-t)
Проверка настроек эл.почты	Отправить сообще	ение			

Настройка почтового сервера через Sendmail

3.2.3 Настройка почтового сервера через консоль

Настройка SMTP

Для настройки почтового SMTP-сервера через консоль используйте следующую команду, где необходимо задать адрес вашего SMTP-сервера или ввести его имя, (IP-адрес или имя и после знака двоеточия номер порта), для примера рассмотрен адрес smtp.server.dom:425:

"mail_smtpmode" => "smtp", "mail_smtphost" => "smtp.server.dom:425",

или

"mail_smtpmode" => "smtp",
"mail_smtphost" => "smtp.server.dom",
"mail_smtpport" => 425,

Если на SMTP-сервере запущен сканер вредоносного программного обеспечения или спама, может потребоваться увеличить время ожидания от сервера, например, до 30 секунд:

"mail_smtptimeout" => 30,

Если SMTP-сервер принимает небезопасные соединения, можно использовать настройку по умолчанию:

"mail smtpsecure" => ",

Настройка шифрования

Если ваш SMTP-сервер принимает только безопасные соединения выполните настройки следующих параметров:

SSL

Безопасное соединение будет инициировано с использованием протокола SMTPS, использующего порт 465. Выполните следующие команды для установки SSL:

```
"mail_smtphost" => "smtp.server.dom:465",
"mail_smtpsecure" => 'ssl',
```

TLS

Безопасное соединение будет инициировано с использованием протокола

STARTTLS, который использует порт по умолчанию 25/tcp:

```
"mail_smtphost" => "smtp.server.dom",
"mail_smtpsecure" => 'tls',
```

Настройка аутентификации

Если для вашего SMTP-сервера не требуются настройки аутентификации, используйте следующие значения по умолчанию:

```
"mail_smtpauth" => false,
"mail_smtpname" => ""',
"mail_smtppassword" => ""',
```

Если на SMTP-сервере требуется аутентификация, вы должны установить необходимое имя пользователя и пароль и также выбрать тип аутентификации: LOGIN (по умолчанию) или PLAIN:

"mail_smtpauth" => true, "mail_smtpauthtype" => "LOGIN", "mail_smtpname" => "username", "mail_smtppassword" => "password",

Настройка Sendmail

Для настройки собственного почтового сервера Sendmail используется

команда:

/usr/sbin/sendmail

Настройте сервер Sendmail следующими параметрами:

'mail_smtpmode" => "sendmail", 'mail_smtphost" => "127.0.0.1", 'mail_smtpport" => 25, 'mail_smtptimeout" => 10, 'mail_smtpsecure" => "", 'mail_smtpauth' => false, 'mail_smtpauthtype" => 'ILOGIN'', 'mail_smtpname" => "",

После завершения настроек SMTP или Sendmail проверьте правильность настроек путем отправки тестового сообщения (письмо будет направлено на почтовый ящик, указанный в личном профиле Администратора сервера). Для этого в графическом режиме перейдите к разделу Администрирование > Основные параметры > блок Почтовый сервер и нажмите на кнопку Отправить сообщение.

Если не удается отправить письмо, попробуйте включить отладку. Для этого включите параметр mail_smtpdebug файле config/config.php: "mail_smtpdebug" => true;

3.3 Общий доступ

Общий доступ к файлам реализует возможности обмена файлами как между внутренними пользователями хранилища AlterOffice, так и с пользователями других серверов, а также предоставляет доступ к файлам сторонним пользователям по общедоступным ссылкам.

3.3.1 Общий доступ к файлам внутри сервера

Настройки общего доступа к файлам внутри сервера осуществляются Администратором на вкладке **Общий доступ** (см. рисунок ниже).

Общий доступ
Администратор может тонко настроить поведение механизма предоставления общего доступа. Обратитесь к документации для получения дополнительной информации.
🐷 Позволить приложениям использовать API общего доступа
Разрешить пользователям публикации через ссылки
📨 Разрешить открытые/публичные загрузки
🗹 Всегда запрашивать пароль
📨 Защита паролем обязательна
🗹 Установить дату истечения по умолчанию
Истечение через 5 дней 🗌 Срок действия обязателен
🖂 Разрешить повторное открытие общего доступа
Разрешить делиться с группами
🗹 Запретить делиться с пользователями из других групп
Запретить выбранным группам предоставлять общий доступ
💟 Включить автоматическое завершение имен пользователей в диалоге предоставления общего доступа. Если отключено, то необходимо вводить полное имя или адрес эл. почты.
🗌 Показывать текст об отказе от ответственности на странице отправки публичной ссылки (Показывать только когда список файлов скрыт)
Права общего доступа по умолчанию
Создание Изменение Удаление Предоставление доступа

Настройка параметров общего доступа

Включенный параметр **Позволить приложениям использовать API общего доступа** разрешает пользователям сервера создавать общедоступные ресурсы.

После разрешения данного действия настройте все остальные параметры в блоке **Общий доступ** по вашей необходимости.

Работа с общедоступными ссылками

Для корректной работы общедоступных ссылок также необходимо разрешить внешние подключения на вашем web-cepвере Apache. Также проверьте, что в файле web-cepвера **config.php** параметр mod_rewrite включен и значения trusted_domains заполнены правильно.

Также убедитесь, что ваш сервер создает ссылку общего доступа из URLадреса, который вы использовали для входа на сервер, а не с использованием параметров вашей внутренней локальной сети, если вы выполнили вход через IPадрес в локальной сети. Внешний пользователь не сможет выполнить переход по такой ссылке.

Обратите внимание на то, что пользователи также могут самостоятельно назначать срок действия общедоступных ссылок для их файлов, который не может быть дольше, чем заданный администратором параметр по сроку действия ссылок. Также пользователь может продлевать действие ссылки на новое количество разрешенных дней несколько раз.

Чтобы жестко регулировать количество дней и пользователь не мог бесконечно продлевать свои ссылки, можно установить принудительный срок истечения дней действия, для этого используйте следующие команды ОСС: осс config:app:set --value <DAYS> core internal_defaultExpDays occ config:app:set --value <DAYS> core link_defaultExpDays

Для пользователей можно настроить получение уведомлений об истечении срока действия общего ресурса. Для этого необходимо дополнить настройки **cronjob**, которые будут инициировать следующую команду ОСС один раз в день:

occ sharing:expiration-notification

Уведомление будет отправлено всем пользователям, срок действия ссылок которых истекает в течение следующих 24 часов.

Передача файлов другому пользователю

Администратор может выполнить передачу файлов одного пользователя другому. Это может быть полезным, если вы хотите удалить пользователя с сервера безвозвратно, но оставить его файлы в системе. Переносятся все файлы, связанные с пользователем 1 (включая и общие ресурсы за исключением содержимого корзины) к пользователю 2:

occ files:transfer-ownership user1 user2

Где:

user1 – имя пользователя чьи файлы будут переданы;

user2 – имя пользователя кому будут переданы файлы.

Создание постоянных общих файловых ресурсов

Для создания постоянных, доступных для всех общих ресурсов для всех пользователей сервера создайте специального пользователя от лица Администратора системы, выкладывайте файлы в хранилище под его именем и далее поделитесь файлами с остальными пользователями системы (или определенными группами).

Если необходимые для всех постоянные общедоступные файлы будут выкладываться одним из действующих пользователей, а с течением времени он будет удален из системы, это повлечет также и удаление всех связанных с ним файлов с сервера.

Описанная выше процедура позволит всегда иметь доступ к необходимым файлам для всех или определенных групп пользователей, не зависимо от меняющихся пользователей на сервере.

Предоставление файлов по умолчанию

Каждый пользователь может получать определенный набор файлов по умолчанию при входе в систему. Список файлов можно изменить в параметре core/skeleton и затем настроить в файле **config.php** через параметр skeletondirectory.

15

Чтобы не добавлять файлы по умолчанию в систему, оставьте этот параметр пустым.

Файлы, настроенные в каталоге **skeleton**, станут доступны всем новым пользователям сервера после их первого входа в систему. Если пользователи уже работали в системе до настройки каталога **skeleton**, то им этот каталог доступен не будет. Все файлы в каталоге **skeleton** копируются в собственные каталоги пользователей, поэтому они могут изменять и удалять файлы, не затрагивая оригиналы.

3.3.2 Настройка доступа к федерации облачных хранилищ

В блоке **Доверенные серверы** и **Межсерверный обмен** настраиваются серверы для общего доступа через федеративные хранилища. С помощью федеративных серверов возможно подключиться к любым другим удаленным серверам AlterOffice или другим серверам совместимых с Open Cloud Mesh (OCM).

Межсерверный обмен 👔
Настройте общий доступ между серверами.
Разрешить пользователям делиться с пользователями других серверов Разрешить пользователям получать общие ресурсы с других серверов Разрешить предоставлять общий доступ для групп пользователей других серверов
Разрешить принимать общий доступ, предоставляемый с другого сервера группе пользователей
Истать пользователей в глобальной и открытой адресной книге
изрешить пользователям пуоликовать свои данные в глоовльной и оощедоступной адресной книге
Доверенные серверы
Федерация серверов позволит Вам подключиться к другим доверенным серверам для обмена каталогами пользователей. Это будет использоване, например, для автодополнения имён пользователей при открытии федеративного
oбщero goctyna.
Добавить сервер автоматически после успешного создания федеративного ресурса общего доступа
+ Добавить доверенный сервер
Поделиться по почте
Позволяет пользователям делиться персонализированной ссылкой на файл или каталог, указав адрес электронной почты.
Отправлять пароль по электронной почте
Защита паролем обязательна
Настройка межсерверного доступа к каталогам
Создание нового общего ресурса федерации не требует никаких действий со

стороны пользователя на удаленном сервере, для активации данной функции необходимо на вашем сервере выполнить следующие настройки:

- 1. В блоке Межсерверный обмен включите следующие параметры: Разрешить пользователям делиться с пользователями других серверов и Разрешить пользователям этого сервера получать общие ресурсы с других серверов.
- 2. В блоке Доверенные серверы активируйте параметр Добавлять сервер автоматически после успешного создания федеративного общего ресурса.

После активации данных параметров пользователи смогут поделиться файлами с пользователями доверенных серверов в настройках общего доступа файла.

3.4 Безопасность

3.4.1 Шифрование

По умолчанию сервер AlterOffice Облако не использует шифрование данных в своем хранилище. Данные настройки могут быть изменены в разделе **Настройки** > **Администрирование** > **Безопасность**, однако не рекомендуется устанавливать дополнительные параметры шифрования данных.

Загружаемые и выгружаемые данные на web-сервер по умолчанию шифруются протоколами SSL, что обеспечивает достаточные параметры безопасности передачи информации.

Настройки шифрования, доступные в графическом режиме представлены на рисунке ниже.

```
    Шифрование на стороне сервера i
    Шифрование на стороне сервера позволяет шифровать файлы, которые загружаются на этот сервер. Это связано с ограничениями, такими как снижение производительности, поэтому включите его только в случае необходимости.
    Image: Image:
```

3.4.2 Использование HTTPS

Для выполнения требований безопасности необходимо использовать зашифрованного соединения HTTPS для доступа к web-ресурсам с сервера AlterOffice.

Настоятельно рекомендуется всегда использовать HTTPS на рабочих серверах вместо незашифрованного HTTP.

Далее рассмотрим процесс перенаправления трафика с HTTP протоколов на HTTPS для web-cepвepa Apache (для настройки на других дополнительных webcepвepax обратитесь к их справочной документации). Рекомендуется выполнить постоянное перенаправление трафика с использованием кода состояния 301. В webcepвеpe Apache этого можно добиться с помощью следующей настройки в

17

конфигурации Apache VirtualHosts:

<VirtualHost *:80> ServerName cloud.alteroffice.com Redirect permanent / https://cloud.alteroffice.com/

Администратору также рекомендуется установить заголовок HTTP Strict Transport Security, который предписывает веб-браузерам не разрешать любые подключения к AlterOffice с использованием HTTP и будет предотвращать попытки обхода предупреждений о недействительном сертификате посетителями сайта. Для этого установите следующие параметры в файле Apache VirtualHost:

<VirtualHost *:443>

ServerName cloud.alteroffice.com

<IfModule mod_headers.c>

Header always set Strict-Transport-Security "max-age=15552000; includeSubDomains" </IfModule> </VirtualHost>

3.4.3 Включение SSL

Использование SSL/TLS протоколов для шифрования всего трафика вашего сервера настоятельно рекомендуется для обеспечения параметров безопасности передачи данных.

В web-cepвepe Apache обычно используются настроенные самоподписанные сертификаты и по умолчанию уже выполнены все необходимые настройки, дополнительно необходимо включить модуль ssl. Для этого используйте команду:

a2enmod ssl	
a2ensite default-ssl	
service apache2 reload	

Конфигурации SSL по умолчанию для веб-серверов часто не соответствуют всем требованиям и требуют тонкой настройки для обеспечения оптимальной производительности и безопасности.

Точные параметры настроек SSL полностью зависят от вашей пользовательской среды и не могут являться одинаковыми для всех серверов.

Рекомендуется использовать <u>Генератор конфигураций SSL Mozilla</u> для генерации подходящей вам конфигурации. Чтобы проверить свою конфигурацию, вы можете использовать бесплатную службу <u>Web_TLS Profiler</u>, который выдает подробные сообщения об ошибках, если настройки TLS вашего сервера отличаются от конфигурации Mozilla. Еще одним полезным инструментом для проверки конфигурации TLS сервера является бесплатный <u>тест Qualys SSL Labs</u>, который предоставляет общую информацию о настройках TLS.

3.4.4 Правила задания паролей

Администратор сервера также настраивает правила, по которым будут задаваться пользовательские пароли в системе. Настройка происходит в разделе Настройки > Администрирование > Безопасность. Далее в блоке Правила создания паролей настраиваются следующие параметры:

- Запрет простых паролей;
- Наличие в пароле и прописных и строчных букв;
- Наличие в пароле цифр;
- Наличие в пароле спецсимволов;
- Проверка пароля относительно списка слабых паролей из специальной базы данных паролей.

Отметьте необходимые параметры и сохраните внесенные изменения.

3.5 Модуль Календарь

Некоторые настройки приложения Календарь доступны в разделе Настройки Администрирования > ПО совместного использования.

Многие из опций настроек календаря выполняются в ходе преднастроенных фоновых заданий сервера, а также требуют отправки уведомлений о тех или иных событиях через электронную почту, для чего необходимо иметь правильные настройки сервера электронной почты.

В данном разделе доступны настройки следующих параметров:

- Отправка приглашений пользователям для регистрации в системе;
- Создание автоматического календаря дней рождений пользователей;
- Отправлять уведомления об их участии в запланированных событиях;
- Подключение push-уведомления о событиях.

3.6 Модуль Разговор

Параметры по управлению и настройке модуля Разговор осуществляются как в графическом интерфейсе, так и в командной строке. В разделе **Настройки** администрирования > Разговор доступно изменение следующих параметров:

- Настройка доступа к разговорам (все участники или только указанные группы);
- Доступ к разговору по публичным ссылкам;
- Доступ к чату через меню работы с файлом;
- Добавление STUN-сервера;
- Добавление TURN-сервера;
- Добавление внешнего сервера сигнализации для крупных разговоров,

в которых участвуют более 4 человек.

3.6.1 Настройка TURN-сервера

Для использования AlterOffice за пределами одной локальной сети, для организации разговоров потребуется дополнительная настройка и подключение сервера TURN.

При организации разговоров в пределах одной локальной сети достаточно иметь веб-браузеры, поддерживающие базовый протокол WebRTC.

Загрузите и установите coTURN с помощью команды sudo apt install coturn из официальных репозиториев или с сайта<u>https://pkgs.org/download/coturn</u>, далее следуйте инструкции по настройке сервера:

1. Запуск соTURN как демона при запуске

В некоторых версиях ОС (основанных на Debian и Ubuntu) необходимо включить развернутую службу sysvinit, настроив соответствующую переменную среды с помощью команды:

sudo sed -i '/TURNSERVER_ENABLED/c\TURNSERVER_ENABLED=1' /etc/default/ coturn

В более поздних версиях ОС используется модуль systemd, который не использует /etc/default/coturn, но включается автоматически при установке. Чтобы проверить, доступен ли модуль systemd в ОС используйте команду:

ls -1/lib/systemd/system/coturn.service

Если вы установили сервер coTURN вручную, вы можете создать службу sysvinit, или модуль systemd, или использовать следующую команду для запуска сервера во время загрузки системы:

/path/to/turnserver - c /path/to/turnserver.conf - o

Где параметры:

- -о запускает сервер в режиме демона;
- -с определяет путь к файлу конфигурации.

Также можно воспользоваться официальным примером по настройке cepвepa по aдpecy <u>https://github.com/coturn/coturn/blob/master/examples/etc/coturn.service</u>.

Сервер соTURN должен запускаться с привилегированных портов, в более поздних версиях ОС по умолчанию службы соTURN запускаются от имени непривилегированного пользователя turnserver, для того, чтобы разрешить исполняемому файлу /usr/bin/turnserver привязывать сокеты к привилегированным портам используйте команду:

setcap cap_net_bind_service=+ep /usr/bin/turnserver

Если конфигурация системы не позволяет установить эту возможность или

если процессу coturn требуется доступ к файлам, доступным для чтения только пользователю root, вы можете настроить службу coturn для выполнения пользователем root вместо непривилегированного пользователем, выполнив команду:

systemctl edit coturn

и далее установить следующую конфигурацию, которая изменит параметры по умолчанию:

```
[Service]
User=root
Group=root
```

2. Настройте turnserver.conf для использования с AlterOffice Облако

Настройте файл конфигурации turnserver.conf. Выберите порт прослушивания (по умолчанию 3478) и секретный ключ аутентификации, для которого рекомендуется использовать случайный шестнадцатеричный код, сгенерированный командой openssl rand -hex 32. Далее раскомментируйте/ отредактируйте следующие настройки соответственно:

```
listening-port=<yourChosenPortNumber>
fingerprint
It-cred-mech # Only on coTURN below v4.5.0.8!
use-auth-secret
static-auth-secret=<yourChosen/GeneratedSecret>
realm=your.domain.org
total-quota=0
bps-capacity=0
stale-nonce
no-loopback-peers # Only on coTURN below v4.5.1.0!
no-multicast-peers
```

Если ваш сервер TURN работает с прямым www-соединением и статическим общедоступным IP-адресом, вы можете ограничить IP-адреса, которые он прослушивает, установив их как listening-ip и relay-ip. Для более крупных по количеству пользователей система рекомендуется запускать сервер TURN на выделенной машине, к которой есть прямой доступ из Интернета.

Если ваш сервер TURN имеет доступ к внутренней сети, необходимо запретить доступ к локальным/внутренним IP-адресам с сервера TURN, за исключением тех, которые действительно необходимы. Для этого установите соответствующие параметры denied-peer-ip для запрета адреса и allowed-peer-ip для разрешения. Например:

```
allowed-peer-ip={IP_ADDRESS_OF_THE_HIGH_PERFORMANCE_BACKEND}
denied-peer-ip=0.0.0.0-0.255.255.255
denied-peer-ip=100.0.0-10.255.255.255
denied-peer-ip=100.64.0.0-100.127.255.255
denied-peer-ip=127.0.0.0-127.255.255
```

denied-peer-ip=169.254.0.0-169.254.255.255 denied-peer-ip=172.16.0.0-172.31.255.255 denied-peer-ip=192.0.0.0-192.0.0.255

Если не установить такой запрет, злоумышленники могут получить доступ к службам вашей внутренней сети через сервер TURN.

В качестве альтернативы можно запретить доступ к внутренней сети с сервера TURN с помощью брандмауэра.

3. Настройка сервера TURN в AlterOffice

Дальнейшая настройка TURN-сервера осуществляется в графическом интерфейсе в разделе **Настройки администрирования** > **Разговор.** В блоке **TURN-сервер** введите адрес вашего TURN-сервера без префикса http(s):// и протокола turn(s)://, введите только значения domain:port.

4. Открытие/экспедиция портов

Обратите внимание, что включенный TURN-сервер должен быть доступен для всех пользователей AlterOffice сервера, поэтому он должен работать в сети Интеренет и быть перенаправленным на соответствующую машину, если он развернут за NAT механизмами. Также убедитесь, что установлен параметр --external-ip в случае, если ваш TURN-сервер находится в частной сети.

Если в вашей системе используется высокопроизводительный бэкэнд, сервер TURN должен иметь возможность связаться с ним. Если связь установлена, то параметр external-ip определяет IP-адрес сервера TURN, к которому высокопроизводительный бэкэнд будет подключаться. Таким образом если TURNсервер и высокопроизводительный бэкенд находятся в одной и той же сети, они могут связаться друг с другом, используя свои локальные IP-адреса и установка параметра external-ip им не нужна.

Кроме того, когда оба сервера находятся за брандмауэром, в некоторых случаях (в зависимости от конфигурации брандмауэра) установка внешнего IPадреса может привести к тому, что сервер TURN и высокопроизводительный бэкэнд не смогут связаться друг с другом.

5. Тестирование сервера TURN

Для того чтобы проверить правильность настроек TURN-сервера попробуйте подключиться к нему извне. Для этого запустите команду:

turnutils_uclient -p <port> -W <static-auth-secret> -v -y turn.example.com

Где следующие параметры:

- ort> это порт, на котором прослушивается ваш TURN-сервер;
- <static-auth-secret> значение static-auth-secret, настроенное на вашем сервере TURN;

- -v включает подробный режим, чтобы иметь возможность проверить все детали;
- -у включает соединения клиент-клиент.

По умолчанию соединение между клиентом TURN и сервером TURN будет осуществляться с использованием UDP. Чтобы вместо этого тестировать TCP-соединения, необходимо добавить параметр -t.

Независимо от того, используется ли UDP или TCP, вывод команды должен выглядеть схоже с примером:

0: IPv4. Connected from: 192.168.0.2:50988 0: IPv4. Connected to: 1.2.3.4:3478 0: allocate sent 0: allocate response received: 0: allocate sent 0: allocate response received: 0: success 0: IPv4. Received relay addr: 1.2.3.4:56365 4: Total transmit time is 4 4: Total lost packets 0 (0.00000%), total send dropped 0 (0.00000%) 4: Average round trip delay 32.500000 ms; min = 15 ms, max = 56 ms

4: Average jitter 12.600000 ms; min = 0 ms, max = 41 ms

Если вы испытываете проблемы с получением вывода в какой-то момент, например, задержка на какой-то части вывода, это может означать, что TURNсервер недоступен.

Далее вы должны увидеть в логе сервера TURN успешное соединение.

Этот тест только проверяет, доступен ли сервер TURN извне, но не проверяет, может ли ваш сервер TURN действительно использоваться в работе сервера AlterOffice.

Далее необходимо проверить подключение к TURN-серверу из модуля Разговор на сервере AlterOffice. Для проверки можно заставить браузер отправлять медиафайлы вызова только через сервер TURN:

Необходимо присоединиться к любому вызову через сервер AlterOffice;

открыть консоль браузера и ввести следующую команду:

OCA.Talk.SimpleWebRTC.webrtc.config.peerConnectionConfig.iceTransportPolicy = 'relay' затем нажать Enter;

Покинуть вызов и затем присоединиться к нему снова;
 Если после выполнения команды вызов работает, то сервер TURN работает.

3.6.2 Команды ОСС для настройки разговоров

Далее рассмотрим некоторые базовые команды для управления Модулем Разговор через командную строку.

23

talk:command:add <cmd> <name> <script> <response> <enabled>

Данная команда позволяет внести новые команды в Модуль Разговор.

Где следующие параметры:

- cmd команда, используемая в чате "/help" => "help";
- пате имя пользователя, разместившего ответ;
- script сценарий для выполнения (должен использоваться только абсолютный путь);
- response пользователи, которые будут видеть ответ (0 Никто, 1 Пользователь, 2 Все);
- enabled пользователи, которые могут использовать данную команду (0 -Отключено, 1 - Модераторы, 2 - Пользователи, 3 – Гости).

talk:command:add-samples

Данная команда добавляет такие шаблонные команды, как, например, /wiki.

talk:command:delete <command-id>

Данная команда позволяет удалить внесенные команды в Модуль Разговор, где параметр command-id – имя команды.

talk:command:list [--output [OUTPUT]] [--] [<app>]

Команда выводит список всех доступных команд, где в аргументах:

- арр при указании сиstom будут перечислены все пользовательские команды;
- --output указывается значение формата вывода (plain, json или json_pretty,).

talk:command:update <command-id> <cmd> <name> <script> <response> <enabled>

Обновляет информацию о команде или добавляет новую. Где следующие аргументы:

- command-id имя команды;
- cmd команда, используемая в чате "/help" => "help";
- пате имя пользователя, разместившего ответ;
- script сценарий для выполнения (должен использоваться только абсолютный путь);
- response пользователи, которые должны видеть ответ (0 Никто, 1 Пользователь, 2 Все);
- enabled кто может использовать эту команду (0 Отключено, 1 -

Модераторы, 2 - Пользователи, 3 – Гости)

talk:monitor:calls [--output [OUTPUT]]

Выводит список разговоров, в которых есть активный вызов, а также количество их участников, где в аргументе --output указывается значение формата вывода (plain, json или json_pretty,).

talk:active-calls [--output [OUTPUT]]

Команда проверяет, обрабатываются ли звонки в приложении данный момент, где в аргументе --output указывается значение формата вывода (plain, json или json_pretty,).

talk:monitor:room [--output [OUTPUT]] [--separator SEPARATOR] [--] <token>

Команда выводит список разговоров, в которых есть активный вызов, а также количество их участников. Где следующие параметры:

- token токен комнаты для мониторинга;
- --output указывается значение формата вывода (plain, json или json_pretty,);
- --separator разделитель для списка CSV при использовании output=csv.

talk:room:add [--user USER] [--group GROUP] [--] <token>

С помощью данной команды добавляются новые пользователи в комнату для разговора. Где следующие параметры:

- token токен комнаты для добавления пользователей;
- --user указанные пользователи приглашаются в комнату;
- --group пользователи указанных групп приглашаются в комнату.

talk:room:create [--description DESCRIPTION] [--user USER] [--group GROUP] [--public] [--readonly] [--listable LISTABLE] [--password PASSWORD] [--owner OWNER] [-moderator MODERATOR] [--message-expiration MESSAGE-EXPIRATION] [--] <name>

С помощью данной команды создаются новые комнаты для разговора.

Где в аргументе name указывается имя новой комнаты для создания, и следующие параметры:

- --description задается описание новой комнаты для разговора;
- --user указанные пользователи приглашаются в новую комнату;
- --group пользователи указанных групп приглашаются в новую комнату;
- --public если указан данный параметр, комната создается как общедоступная;

- --readonly если указан данный параметр, комната создастся с доступом только для чтения;
- --listable создается комната с заданной перечисляемой областью;
- --password создаются комната, защищенная паролем;
- --оwner задает указанного пользователя как владельца новой комнаты;
- --moderator повышает указанных пользователей до модераторов комнаты;
- --message-expiration указывается время в секундах до истечения срока действия сообщения после отправки. Если указано ноль, то параметр отключит срок действия сообщения.

talk:room:delete <token>

С помощью данной команды удаляется комната, где в аргументе token указывается токен комнаты для удаления.

talk:room:demote <token> <participant>...

Понижает участников выбранной комнаты до обычных пользователей, где в аргументе token указывается токен комнаты, participant - понижает указанных участников комнаты до обычных пользователей.

talk:room:promote <token> <participant>...

Выдвигает участников указанной комнаты в модераторы, где в аргументе token указывается токен комнаты, participant - повышает указанных участников комнаты до модераторов комнаты.

talk:room:remove <token> <participant>...

С помощью данной команды удаляются указанные пользователи из комнаты, где в аргументе token указывается токен комнаты, participant – указанные участники удаляются из комнаты.

talk:room:update [--name NAME] [--description DESCRIPTION] [--public PUBLIC] [-readonly READONLY] [--listable LISTABLE] [--password PASSWORD] [--owner OWNER] [--message-expiration MESSAGE-EXPIRATION] [--] <token>

Данная команда обновляет сведения о комнате, где в аргументе token указывается токен комнаты, а также следующие параметры:

- --пате новое имя для комнаты;
- --description новое описание для комнаты;
- --public изменяет комнату на общедоступную (значение 1) или личную

- --readonly определяет доступность комнаты только для чтения (значение 1) или для чтения и записи (значение 0);
- --listable изменяет доступную для списка область действия комнаты;
- --разsword устанавливает новый пароль для комнаты; если значение будет оставлено пустым, защиту паролем будет снята;
- --оwner задает указанного пользователя как владельца комнаты; если значение будет оставлено пустым, владелец будет удален;
- --message-expiration указывается время в секундах до истечения срока действия сообщения после отправки. Если будет указано значение ноль, то срок действия сообщения будет отключен.

talk:signaling:add [--verify] [--] <server> <secret>

Добавляет внешний сигнальный сервер, где аргументы

- server строка сервера, например, wss://signaling.example.org;
- secret общая секретная строка;

и параметр – verify - проверяет SSL-сертификат, если он установлен.

talk:signaling:delete <server>

Удаляет существующий сигнальный сервер, где аргумент server это строка внешнего сервера сигнализации, например, wss://signaling.example.org.

talk:signaling:list [--output [OUTPUT]]

Данная команда выводит список внешних сигнальных серверов, --output выходной формат (plain, json или json_pretty, по умолчанию стоит plain).

talk:stun:add <server>

С помощью данной команды добавляется новый сервер STUN, где в параметре

server задается имя домена и номер порта, разделенные двоеточием, например, stun.alterofficecloud.com:443

talk:stun:delete <server>

С помощью данной команды удаляется сервер STUN, где в параметре server задается имя домена и номер порта, разделенные двоеточием, например, stun.alterofficecloud.com:443

talk:stun:list [--output [OUTPUT]]

С помощью данной команды выводиться список серверов STUN, где в параметре --output указывается значение формата вывода (plain, json или json_pretty, по умолчанию задан параметр plain);

talk:turn:add [--secret SECRET] [--generate-secret] [--] <schemes> <server> <protocols>

С помощью данной команды добавляется сервер TURN, где аргументы:

- schemes схемы, turn или turns или turn,turns;
- server доменное имя, например, Turn.alteroffice.com;
- protocols Протоколы могут быть udp или tcp или udp,tcp.
- И параметры:
- --secret указывается секретная строка;
- --generate-secret генерирует секретную строку если указан параметр выше.

talk:turn:delete <schemes> <server> <protocols>

Данная команда удаляет подключенный сервер TURN, где аргументы:

- schemes схемы, turn или turns или turn,turns;
- server доменное имя, например, Turn.alteroffice.com;
- protocols Протоколы могут быть udp или tcp или udp,tcp.

talk:turn:list [--output [OUTPUT]]

Данная команда выводит список серверов TURN, где в параметре --output указывается значение формата вывода (plain, json или json_pretty, по умолчанию задан параметр plain);

talk:user:remove [--user USER]

С помощью данной команды указанные пользователи удаляются из всех разговоров, в которых они участвуют. Где в параметре --user указывается имя пользователя.

talk:user:transfer-ownership [--include-non-moderator] [--remove-source-user] [--] <source-user> <destination-user>

С помощью данной команды все разговоры одного пользователя переходят к другому пользователю. Где следующие аргументы:

source-user – пользователь-владелец разговоров, которые будут

перемещены;

- destination-user пользователь, которому будут переданы разговоры.
- А также следующие параметры:
- --include-non-moderator в передачу будут включены разговоры, в которых исходный пользователь является обычным пользователем, не модератором;
- --remove-source-user удаление исходного пользователя из разговоров.

3.7 AlterOffice Облако

В данном разделе проводится настройка онлайн-редакторов **AlterOffice**. Перейдя во вкладку **Настройки администратора** > **AlterOffice Облако**, необходимо добавить информацию о доверенных хостах WOPI: адрес сервера документов AlterOffice Облако.

Обратите внимание, что запросы на подключение к серверу всегда должны отправляться с одного и того же компьютера.

В графическом интерфейсе также можно отключить проверку сертификатов, этот параметр необходим, если ваш сервер документов AlterOffice использует самоподписные сертификаты. В остальных случаях включение данного параметра будет небезопасным.

В AlterOffice Облако можно ограничить использование онлайн редакторов только для членов указанных групп, внесите названия групп пользователей в соответствующее поле ввода. Также можно ограничить права на внесение изменений только для пользователей заданных групп.

В блоке Расширенные настройки регулируются следующие параметры:

- использование формата ООХМL вместо ODF для новых файлов редактора;
- разрешения доступа для внешних приложений;
- использование канонического расположения корневого каталога.

В блоке **Глобальные шаблоны** можно загрузить дополнительные шаблоны редакторов для пользователей сервера AlterOffice с вашего ПК.

В блоке **Настройки безопасного просмотра** можно включить использование водяных знаков на документах.

Языки словарей онлайн редакторов

Когда в системе установлено много словарей и тезаурусов для проверки орфографии, их предварительная загрузка может занять значительное время при запуске. Поэтому по умолчанию включены словари только для следующих языков:

- немецкий (DE);
- английский (GB, US);
- испанский (ES);

29

- французский (FR);
- итальянский (IT);
- португальский (BR, PT);
- русский (RU).

Данный список можно изменить настройкой allowed_languages, где добавляются или удаляются языковые теги по мере необходимости.

Консоль администратора

С помощью консоли администратора возможно в режиме реального времени отслеживать все сеансы пользователей, запущенные в онлайн редакторах. Для доступа к консоли администратора перейдите на URL-адрес, который строится следующим образом:

https://*hostname*:*port*/browser/dist/admin/admin.html

По умолчанию используется порт 9980, который запросит имя пользователя и пароль, которые установлены в блоке admin_console /etc/coolwsd/coolwsd.xml или -- o:admin_console.username=username в --o:admin_console.password=password командной строке coolwsd. Консоль администратора будет отключена, если какой-либо из этих параметров не установлен.

Обратите внимание, если вы используете аутентификацию с помощью PAM, которая также настроена для coolwsd в вашей системе, можно выполнять вход в консоль администратора с обычным паролем от вашей ОС Linux:

1 auth required pam_unix.so

2 account required pam_unix.so

При входе в консоль администратор может отслеживать такие параметры как:

- открытые документы в реальном времени;
- общее количество пользователей, потребление памяти;
- URL-адреса документов с количеством пользователей, просматривающих этот документ.

Администратор также может удалять документы непосредственно с панели. **Мониторинг показателей использования**

Функции мониторинга AlterOffice могут предоставить информацию по разным показателям, связанным с использованием системы, например. использование памяти или ЦП, количество запущенных процессов комплекта или просмотров в сеансах документов и другие. Метрики можно получить в формате, совместимом с Prometheus, по URL-адресу, который строится по следующей схеме: https://*hostname*:*port*/cool/getMetrics URL-адрес использует ту же аутентификацию, что и консоль администратора, которая описана выше.

Блокировка функций

AlterOffice Облако позволяет запретить пользователю использование определенных функций онлайн редакторов или сделать документы для некоторых пользователей доступными только для чтения. Когда пользователь будет пытаться использовать заблокированную функцию, он увидит всплывающее окно с подробностями о разблокировке.

Для того чтобы отключить какую-либо функцию, вы можете указать ее команду UNO в поле locked_commands. Все связанные параметры можно найти в файле coolwsd.xml.

Чтобы пометить пользователя как заблокированного, клиент WOPI должен вернуть ответ на параметр CheckFileInfo с логическим значением IsUserLocked. Чтобы дать заблокированным пользователям доступ к документам с разрешением только для чтения, установите параметр true для значения is_lock_readonly.

Обратите внимание, что для того, чтобы разрешить функции блокировки feature_lock для каждого хоста WOPI, в параметре lock_hosts allow должно быть установлено значение true.

Удаленная/динамическая конфигурация

Настройка удаленных серверов для онлайн редакторов AlterOffice доступна через отправку измененных параметров в JSON-формате. Изменения в ответе JSON можно производить без перезапуска сервера AlterOffice, он запрашивает ответ JSON на удаленный сервер каждые 60 секунд, и, если в JSON появятся новые изменения, он перезапишет настройки coolwsd.xml. Новая конфигурация вступит в силу при следующем открытии документа.

В AlterOffice использует заголовок ETag, чтобы определить, изменился ли JSON по сравнению с последним запросом или нет. Поэтому рекомендуется добавить заголовок ETag в ответ JSON для удаленного сервера.

Включите настройку удаленного сервера, добавив его URL-адрес в следующей команде:

```
<remote_config >
<remote_url desc="remote server to which you will send request to get remote config in
response" type="string" default="">https://server_url_endpoint</remote_url>
</remote_config>
```

Ответ сервера в JSON-формате для изменения настроек конфигурация поступит в следующем формате:

''kind": "configuration",

31

```
"remote_font_config":
 {
  "url": "https://.../fonts.json"
 },
 "storage":
 {
  "wopi":
    "alias_groups":
    ł
     "mode" : "groups",
     "groups":
       { "host": "scheme://hostname:port", "allow": "true", "aliases": ["scheme://aliasname1:port",
"scheme://alias-regex-pattern:port"]},
     1
    }
  }
 },
 "feature_locking":
 ł
  "locked_hosts":
    "allow":"true",
    "hosts":
    ſ
       { "host": "pattern1", "read_only": true, "disabled_commands": true },
       { "host": "pattern2", "read_only": false, "disabled_commands": true },
   ]
  },
  // unlock dialog customization
  "unlock_image": "https://<hostname>/static/<image_endpoint>",
  "translations":
    [
       "language": "de",
       "unlock title": "Gehen Sie zur Detailseite und entdecken Sie alle Funktionen:",
       "writer_unlock_highlights": "Überprüfen und schreiben Sie mit Leichtigkeit",
       "calc unlock highlights": "Machen Sie sich ein besseres Bild von Ihren Daten",
       "impress_unlock_highlights": "Bringen Sie Ihre nächste Präsentation auf den Punkt",
       "draw_unlock_highlights": "Zeichne und organisiere dich",
     },
     // more translations possible
   1
 },
}
```

Каждый из блоков в ответе JSON является необязательным, таким образом можно использовать любой из блоков remote_font_config, storage, feature_lockingJSON по отдельности.

Конфигурация JSON перезапишет значения, указанные в файле coolwsd.xml.

Включите загрузку и доступность дополнительных шрифтов, указав на файл конфигурации шрифта.

<remote_font_config>

<ur>
 <url desc="URL of optional JSON file that lists fonts to be included in Online" type="string" default="">https://someserver/path/file.json</url></remote font config>

Настройка шрифтов в формате JSON

Для настройки шрифтов укажите пути к шрифтовым файлам в JSON-ответе по следующему принципу:

```
"kind": "fontconfiguration",
"server": "имя_cepвepa",
"fonts": [
    {
        "uri": "https://путь_к_шрифту/path/f1.ttf"
    },
    {
        "uri": "https://путь_к_шрифту/path/f2.ttf",
        "stamp": "foo3"
    },
    {
        "uri": "https://путь_к_шрифту/path/x42.ttf"
    }
]
```

Файл JSON будет просканирован в течение 60 секунд на поступившие изменения и изменит соответствующие конфигурации.

Если элемент в массиве шрифтов имеет свойство stamp, то файл данного шрифта будет повторно загружен на сервер, а предыдущая его версия будет забыта. В свойстве stamp может быть записана любая строка, ее содержимое никак не интерпретируется, сервер будет проверять только меняется ли она, для необходимости проведения новой загрузки данного шрифта.

Имя шрифта будет считываться из содержимого загружаемого файла, которые должны являться шрифтами TrueType или OpenType.

Полный список настроек представлен в файле /etc/coolwsd/coolwsd.xml.

3.7.1 Обзор использования

1

Во вкладке **Обзор использования** Настроек администрирования регулируются статистические данные, которые будут отправлены разработчикам ПО в обезличенном виде для улучшения работы AlterOffice.

По умолчанию отправка данных отключена, если вы решите включить ее,

33

Администратором настраиваются следующие данные для отправки:

- Подробности установки сервера (версия, использование memcache, состояние блокировок / пред. просмотра / аватаров);
- Информация о РНР (версия, лимит памяти, макс. выполнения, макс. размер файла);
- Информация о БД (тип, версия, размер);
- Список приложений (для каждого из приложений: его название, версия, включено или нет);
- Статистика (число файлов, пользователей, хранилищ по типам, комментариев и меток);
- Количество общих ресурсов (по типу и настройкам доступа);
- Информация о применяемом шифровании (используется ли, применяемый по умолчанию модуль).

3.7.2 Журналирование

Просмотр журналов событий осуществляется в разделе **Настройки** администратора > Журналирование.

В графическом режиме представлен список, который можно просматривать по фильтрам уровня журналирования и записей журнала.

Если требуется дополнительная информация аудита, возможно дополнительно активировать приложение admin_audit, которое по умолчанию создает отдельный файл audit.log в каталоге данных.

Уровни ведения журнала варьируются от DEBUG, который регистрирует все действия, до FATAL, который регистрирует только фатальные ошибки:

0 – DEBUG – записывается вся активность на сервере, максимально подробный журнал;

1 – INFO – записываются действия, такие как входы пользователей в систему и действия с файлами, а также предупреждения, ошибки и фатальные ошибки;

2 – WARN – ведутся записи действий, при которых операции выполняются успешно, но с предупреждениями о потенциальных проблемах, а также об ошибках и фатальных ошибках;

3 – ERROR – запись операций, которые завершаются с ошибками, но при

которых другие службы и операции продолжаются, а также записываются фатальные ошибки;

4 – FATAL – критические ошибки, сервер останавливается.

По умолчанию уровень журнала установлен на 2 уровень (WARN). Используйте нулевой уровень DEBUG, когда есть проблемы с диагностикой, а затем сбросьте уровень журнала до менее подробного уровня журналирования, поскольку DEBUG выводит много информации и может повлиять на производительность вашего сервера.

Параметры уровня ведения журнала задаются в файле config/config.php. Виды журналов на сервере:

errorlog: вся информация журнала отправляется в error_log()PHP.

"log_type" => "errorlog"

1.

- file: вся информация данного журнала записывается в отдельный файл, по умолчанию файл с именем alteroffice.log будет создан в каталоге, настроенном с помощью параметра datadirectory в config/ config.php.
- 3. **syslog**: вся информация журнала будет отправлена демону системного журнала по умолчанию.

```
"log_type" => "syslog",
"syslog_tag" => "AlterOffice",
"logfile" => '"',
"loglevel" => 3,
```

4. **systemd**: вся информация журнала будет отправлена в журнал Systemd. Требуется расширение php-systemd.

"log_type" => "systemd", "syslog_tag" => "Alteroffice",

4 Приложения

Администратор сервера AlterOffice Облако может управлять набором приложений, которые доступны для пользователей системы. В разделе **Приложения** Администратор может подключать или отключать их. Обратите внимания на то, что по умолчанию в системе будут включены не все доступные приложения.

При переходе во вкладку открывается список всех доступных приложений на сервере (см. рисунок ниже) с указанием их версии и статуса работы на сервере.

При первом входе в систему будет подключен пакет приложений по умолчанию, настройте его в зависимости от ваших потребностей.

Alter 🖿 4 🖾 Q	4 8			٩ ۽	4
Ваши приложения	Е Версии	1.10.0	✔ Официальное		Отключить
 Активные приложения 	🔛 Галерея	18.4.0	 Официальное 		Отключить
Отключённые приложения	🛗 Календарь	1.7.1	✔ Официальное		Отключить
Пакеты приложении	Комментарии	1.7.0	✔ Официальное		Отключить
Документация для разработчиков 🗡	👪 Контакты	3.1.8	🗸 Официальное		Отключить
	О ⁴ Конфиденциальность	1.1.0	🗸 Официальное		Отключить
	👕 Корзина	1.7.0	✓ Официальное		Отключить
	🦠 Метки совместной работы	1.7.0	✔ Официальное		Отключить
	🔒 Модуль шифрования по умолчанию	2.5.0	✔ Официальное		Отключить
	- Mohutopuhr	1.7.0	🗸 Официальное		Отключить
	🚮 Обзор использования	1.5.0	🗸 Официальное		Отключить
	< обмен файлами Раздел Приложения — список всех	1.9.0 прилож	✓ официальное Кений сервера		Отключить

Управление приложениями происходит через кнопку **Включить** и **Отключить** напротив соответствующего приложения.

Для получения описания функциональных характеристик приложения нажмите на него левой кнопкой мыши, на правой боковой панели откроется подробное описание.

Для удобства работы в разделе предусмотрен просмотр приложений по вкладкам на левой боковой панели: **Активные приложения** и **Отключённые приложения**, где отображаются соответствующие списки.

Во вкладке **Пакеты приложений** настраиваются корпоративный пакет приложений и пакеты для групп пользователей.

4.1 Работа с приложениями в командной строке

Рассмотрим базовые параметры управления приложениями через консоль с помощью команд ОСС.

Для управления приложениями используется параметр арр, список команд,

доступный с данным параметром:

- app:install установка выбранного приложения;
- app:disable отключение выбранного приложения;
- app:enable подключение выбранного приложения;
- app:getpath получить путь к выбранному приложению;
- app:list получить список всех доступных приложений;
- app:update обновить приложение;
- app:removedisable отключить и удалить выбранное приложение.

Для получения списка всех установленных приложений с указанием того включены они или нет используйте следующую команду:

sudo -u www-data php occ app:list

Для включения приложения, (для примера: приложение поддержки внешнего хранилища):

sudo -u www-data php occ app:enable files_external files_external enabled

Для отключения приложения: sudo -u www-data php occ app:disable files_external files_external disabled

Для получения полного путь к файлу приложения: sudo -u www-data php occ app:getpath notifications /var/www/alteroffice/apps/notifications

Для обновления приложения (для примера Контакты): sudo -u www-data php occ app:update contacts

Для обновления всех приложений: sudo -u www-data php occ app:update --all

5 Пользователи

Управление пользователями происходит в разделе **Пользователи**. После перехода в раздел открывается список всех пользователей системы и дополнительные вкладки для доступа к разным категориям пользователей.

Alter 🖿 4 🖂	Q	-12	. 🖴						٩	a 🔒
+ Новый пользователь			Имя пользователя	Отображаемое имя	Пароль	Адрес эл. почты	Участник групп	Администратор групп	Квота	
+ Добавить группу		A	admin	admin	Новый пароль		admin	Назначить админі	Неограничено	
₽ Bce	8	C	Andrey C.	Andrey	Новый пароль	example@email	admin	Назначить админі	Неограничено	•••
Ф Администраторы	8	A	Alexey Stepanov	Alexey	Новый пароль	example@email	admin	Назначить админі	Неограничено	•••
Участник групп		D	Danil Abramov	Danil	Новый пароль	example@email	admin	Назначить админі	5 GB	•••
TestGroup	1	A	Anastasia K.	Anastasia	Новый пароль	example@email	admin +0	Назначить админі	5 GB	
TestGroup2	Ŵ	S	Stepan Kulikov	Stepan	Новый пароль	example@email	admin	Назначить админі	Неограничено	•••
		C	Irina C.	Irina	Новый пароль	example@email	admin	Назначить админі	5 GB	•••
		1	Kristina Ivanova	Kristina	Новый пароль	example@email	admin	Назначить админі	1 GB	
Ф Параметры										
			Раздел Пол	1ьзовате л	и – все п	ользовате	ели сервег	oa -		

5.1 Создание нового пользователя

Для того чтобы создать нового пользователя в системе, нажмите на кнопку

+ Новый пользователь, после чего откроются поля для внесения информации о нем (см. рисунок ниже).

```
        Имя пользователя
        Отображаемое имя
        Пароль
        Адрес эл. почты
        Участник групп
        Администратор групп
        Квота

        +
        Имя пользователя
        Отображаемое имя
        Пароль
        Адрес эл. почты
        Добавить в группу
        Назначить админист]
        Квота по умолчанию
```

Добавление нового пользователя

В параметре **Имя пользователя** введите имя, которое будет использоваться при авторизации на сервере. Параметр может содержать буквы (a-z, A-Z), цифры (0-9), дефисы (-), символы подчеркивания (_), точки (.), пробелы () и знаки (@). Это имя пользователя задается один раз и далее его изменение невозможно.

Отображаемое имя – то, под каким именем пользователя будут видеть в системе другие, оно может отличаться от предыдущего параметра. Этот параметр заполняется Администратором по желанию и дальше может быть изменен самим пользователем.

В параметре **Пароль** задайте пароль для нового пользователя в соответствии с установленными правилами создания паролей.

При необходимости добавьте нового пользователя в одну или несколько групп пользователей в поле **Группы.**

В поле **Администратор групп** можно наделить пользователя правами администратора для соответствующей группы пользователей. Администраторы групп имеют право создавать, редактировать и удалять пользователей в назначенных им группах. Администраторы групп при этом не будут иметь доступ к системным настройкам, не могут удалять или добавлять новых участников в их группы.

В поле **Квота** выберите из выпадающего списка лимит на объем памяти для хранилища пользователя.

Для завершения создания пользователя и сохранения всех внесенных

данных воспользуйтесь кнопкой

5.2 Группы пользователей

В Alter Office Облако можно создавать группы пользователей и наделять эти группы разными правами доступа. Каждый пользователь может быть отнесен к нескольким группам одновременно или не отнесен ни к одной.

Для создания новой группы пользователей воспользуйтесь кнопкой

+ Добавить группу на левой боковой панели. Введите название для новой группы и подтвердите свое действие вводом пароля. После создания группы состав ее участников пуст, для добавления новых перейдите к списку всех пользователей в системе и в параметре **Участник групп** у необходимых пользователей выберите название необходимой группы.

Список групп пользователей представлен на левой боковой панели. Перейдите во вкладку группы и откроется список ее участников (см. рисунок ниже).

• Новый пользователь)	Имя пользователя	Отображаемое имя	Пароль	Адрес эл. почты	Участник групп	Администратор групп	Квота		1
Добавить группу		+	Имя пользователя	Отображаемо	Пароль	Адрес эл. почты	TestGroup	Назначить админ	Квота по		
Bce		A	Alexey Stepanov	Alexey	Новый пароль	example@email	admin +0	Назначить админ	5 GB	•••	
Администраторы	1		Kristina Ivanova	Kristina	Новый пароль	example@email	admin +0	Назначить админ	1 GB		
		1									
TestGroup TestGroup2	2 🕯										
TestGroup2	6	J									

Для удаления группы воспользуйтесь кнопкой **н**апротив соответствующей группы и далее подтвердите свое действие. Обратите внимание, что удаление группы не приводит к удалению пользователей, которые в ней состояли.

5.3 Сброс пароля

5.3.1 Сброс пароля пользователя

Восстановить забытый пароль пользователя невозможно, но возможно установить новый. Для этого воспользуйтесь следующей инструкцией:

- перейдите в раздел Пользователи, в списке всех пользователей выберите необходимого пользователя:
- в графе Пароль заполните форму ввода Новый пароль, где задайте новый пароль пользователя;
- передайте новый пароль пользователю.

Также пользователи могут сбросить пароль самостоятельно при входе в систему нажав на ссылку **Забыли пароль** на странице авторизации, после чего сервер автоматически сбросит пароль и направит письмо на электронную почту пользователя с инструкцией по назначению нового пароля. Однако, это правило не сработает, если используются протоколы LDAP или Active Directory. В этом случае вы можете указать собственный URL-адрес в своем файле config.php, чтобы направить пользователя на сервер, который будет обрабатывать автоматический сброс пароля:

'lost_password_link' => 'https://example.org/link/to/password/reset'

5.3.2 Сброс пароля администратора

Существует несколько способов для сброса утерянного пароля Администратора сервера:

- 1. При входе в систему сбросить пароль можно, нажав на ссылку **Не помню пароль**, после чего указать свой адрес электронной почты, на которую будет выслана ссылка для сброса пароля.
- Сбросить пароль одного Администратора также может другой Администратор системы по инструкции сброса паролей для пользователей, которая описана в данном разделе 4.3.1.Сброс пароля пользователя выше. Сброс пароля администратора также возможен через консоль. Для этого

используйте следующую команду (где также необходимо ввести новый пароль и

подтвердить его повторным вводом):

\$ sudo -u www-data php /var/www/alteroffice/occ user:resetpassword admin

Enter a new password:

Confirm the new password:

Successfully reset password for admin

Где параметр admin является именем пользователя, пароль которого будет сброшен, если ваше имя пользователя отличается, измените данный параметр.

5.4 Управление пользователями

Управление пользователями системы осуществляется через контекстное меню каждого пользователя (см. рисунок ниже).



Контекстное меню по управлению пользователями

В контекстном меню доступны следующие параметры:

- Удалить пользователя пользователь и все его данные удаляются из системы. Обратите внимание на то, что все общие файлы, которыми делился пользователь, также будут удалены;
- Удалить данные со всех устройств
- Отключить пользователя удаляет пользователя из системы с возможностью его восстановления и без удаления данных пользователя, таким образом все его файлы и папки останутся доступными для других пользователей. Если необходимо вернуть пользователя в систему, его можно будет восстановить;
- Отправить приглашение еще раз отправляет электронное письмо на почту пользователя с информацией о созданной для него учетной записи в AlterOffice Облако.

6 Операции с файлами в хранилище

Далее рассмотрим некоторые операции с файлами во внутреннем хранилище AlterOffice, которые доступны Администратору с помощью команд ОСС.

Сканирование

С помощью команды files:scan сканируются файлы хранилища и обновляется кэш файлов. Возможно проводить отдельное сканирование всех файлов для каждого пользователя, или списка пользователей, разделенных пробелами, а также ограничить путь поиска.

Перейдите к справке и получению списка всех команд по сканированию файлов через:

sudo -u www-data php occ files:scan -help

Обратите внимание, что уровни детализации -vv или -vvv автоматически сбрасываются на -v.

Сканирование данных приложений

Файлы, совместно используемые пользователями сервера AlterOffice, например, это изображения аватаров, предварительные просмотры файлов и кэшированные файлы CSS, находятся в папке Appdata внутри каталога данных сервера и помещаются туда соответствующими приложениями.

Поскольку обычное сканирование файлов работает только с пользовательскими файлами, следующая команда проводит сканирование каталога appdata и проверяет, что файловый кеш соответствует файлам в реальном хранилище:

files:scan-app-data [options] [--] [<folder>]

Где аргумент folder это подкаталог appdata который должен быть просканирован.

Очистка

Команда files:cleanup очищает файловый кеш сервера, удаляя все записи файлов, для которых нет соответствующих записей в таблице хранилища.

Восстановление файлового дерева

Если по какой-либо причине путь записи в файловом кеше не совпадает с реальным путем к исходному файлу, вы получите запись в файловом кеше, которая существует в разных местах в зависимости от того, как запись сгенерирована.

Команда files:repair-tree пытается восстановить поврежденные пути к исходному файлу и исправить неверные записи в нем.

Передача файлов

Администратор может передать все файлы и ресурсы от одного пользователя к другому. Это может быть необходимо перед проведением процедуры удаления пользователя, что повлечет за собой удаление всех его данных. Передаваемые файлы появятся в новом подкаталоге в целевого пользователя.

Для передачи данных хранилища от одного пользователя к другому используйте следующую команду:

files:transfer-ownership [options] [--] <source-user> <destination-user>

где следующие аргументы должны быть заменены:

- source-user пользователь, исходный владелец файлов;
- destination-user пользователь, которому будут переданы все файлы; Параметры аргумента [options] могут быть следующими:

--path="имя_папки"

Данный параметр используется, если необходима передача только одного каталога вместе с его содержимым. В данном аргументе указывается путь к необходимому каталогу.

--move

Параметр -- move используется для перемещения данных в каталог целевого пользователя, если его хранилище является абсолютно пустым, дополнительный подкаталог создаваться не будет, все переданные файлы будут отображаться в корневой папке пользователя.

--transfer-incoming-shares

Данный параметр будет передавать входящие общие файловые ресурсы исходного пользователя к целевому пользователю.

7 Сообщения администратору

Сервер AlterOffice имеет встроенную программу проверки конфигурации, которая сообщает Администратору о результатах проверки в блоке **Проверка безопасности и параметров** в разделе **Настройки администратора** > **Общие** (см. рисунок ниже).

Проверка безопасности и параметров i
It's important for the security and performance of your instance that everything is configured correctly. To help you with that we are doing some automatic checks. Please see the linked documentation for more information.
О Предупреждения о текущей конфигурации.
• Заголовок HTTP «Strict-Transport-Security» должен быть настроен как минимум на «15552000» секунд. Для улучшения безопасности рекомендиется включить HSTS согласно нашим подсказкам по безопасности 2.
• Веб-сервер не настроен должным образом для разрешения «/well-known/caldav». Дополнительная информация можат быть найдена в нашей <u>доулентации</u>
 Веб-сервер не настроен должным образом для разрешения «/well-known/carddav». Дополнительная информация может быть найдена в нашей <u>допументации.</u>
 Не настроена система кеширования. Для увеличения производительности сервера, по возможности, настройте memcache. Более подробная информация доступна в до<u>ружентации</u>.
• В системе не установлены рекомендуемые модули РНР. Для улучшения производительности и совместимости рекомендуется установить эти модули.
∘ imagick
• Некоторые индексы базы данных не были преобразованы в тип big int. Так как преобразование таких индексов может занять продолжительное время, оно должно быть запущенно вручную. Чтобы выполнить преобразование, необходимо включить режим обслуживания и запустить в терминале команду «srv db:convert-flecache-bigint». Дополнительные сведения приведены <u>на соответствующей странице дорументации</u> .
 mounts.storage.jd
 mountsroot)d
 mountsmount.jd
Ещё раз внимательно прочитайте <u>руководство по установке /</u> и проверьте <u>журнал</u> на наличие ошибок и предупреждений.

Проверить безопасность AlterOffice нашим сканером .

Сообщения в блоке Проверка безопасности

Также в системе присутствует внутренний сканер безопасности, работу которого можно инициировать, перейдя по соответствующей ссылке внизу блока **Проверка безопасности и параметров**. Сканер проведет проверку обновлений и защиты системы.

Сообщения, отображающиеся в данном блоке, описывают неполадки в работе или примененных настройках программного обеспечения на сервере. За полной информацией обращайтесь к документации по ссылкам в сообщениях, а также к подробной справочной документации на сервере AlterOffice, которую можно найти в каталоге /var/www/alteroffice/core/doc.

Рассмотрим некоторые типы сообщений администратору:

- 1. Предупреждения кэша. Чаще всего данная категория сообщений уведомляет о необходимости установки или обновления текущей версии расширений:
- АРСи (минимально необходимая версия расширения PHP 4.0.6);
- Memcached;
- Redis (минимальная требуемая версия расширения PHP: 2.2.6);
- 2. «Вы заходите на этот сайт через НТТР». Данное сообщение администратора увидит, если доступ к web-ресурсам осуществляется через протоколы НТТР, в то время как сервер требует использования НТТРЅ для обеспечения мер безопасности соединений. Для выполнения требований безопасности необходимо включить использование HTTPS на всех используемых webсерверах (Apache и Nginx), а также настроить параметры SSL, об этом

подробнее выше в разделе 2.4.1. Шифрование.

- 3. Сообщение о том, что /dev/urandom не читается PHP относится к важным сообщениям безопасности. Необходимо предоставить PHP доступ для чтения к /dev/urandom, который необходим для генерации криптографически безопасных псевдослучайных чисел. Для этого при настройке open_basedir в файле php.ini обязательно включите /dev/urandom.
- 4. Устаревшая версия NSS/OpenSSL. Данные типы сообщений сигнализирует о необходимости обновления операционной системы или отдельных функций NSS и OpenSSL, в противном случае это приведет к ошибкам в связи с удаленными хостами, использующими SNI. OpenSSL необходимо обновить как минимум до версии 1.0.2b или 1.0.1d. Для NSS версия зависит от вашего дистрибутива OC.
- 5. Ваш веб-сервер не настроен должным образом для разрешения /.well-known/caldav/ или /.well-known/carddav/. Данная проблема возникает если оба URL-адреса неправильно перенаправлены на конечную точку DAV AlterOffice.
- 6. Ваша база данных не работает с уровнем изоляции транзакций «READ COMMITED». Данное сообщение возникает, если некоторые действия в БД выполняются параллельно, необходимо устранить данные неполадки в вашей БД.