VK WorkSpace

Корпоративный мессенджер VK Teams

Инструкция по установке на одну виртуальную машину (версия 24.3)

Оглавление

Назначение документа

В данной инструкции представлено описание процесса установки корпоративного мессенджера VK Teams на одну виртуальную машину.

В документе рассматриваются два способа установки системы:

1. Установка из графического интерфейса
2. Установка из консоли

Документ предназначен для использования администраторами организации.

Дополнительная документация

Инструкция по интеграции с контроллером домена по протоколу LDAP — в документе представлена информация по управлению параметрами синхронизации LDAP.

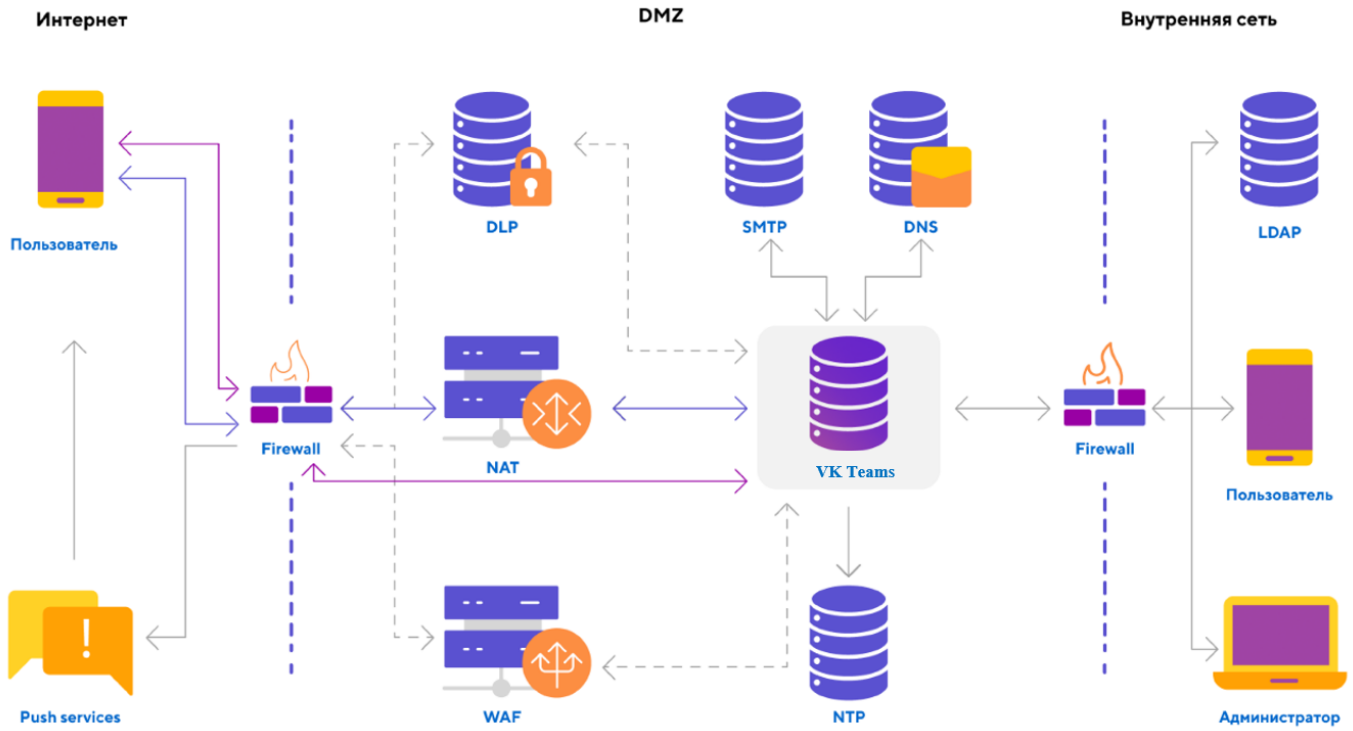
Инструкция по установке обновлений на одну виртуальную машину — в документе прописан процесс обновления системы, установленной на 1 виртуальную машину.

Архитектура и описание системы — в документе представлено описание архитектуры инсталляции на одну виртуальную машину, кластерной инсталляции, возможные интеграции с VK Teams, а также технические данные и требования. Не является частью публичной документации, обратитесь к представителю VK Tech, чтобы ознакомиться с документом.

> **Внимание**
>
> Ранее мессенджер VK Teams назывался Myteam, что находит отражение некоторых в технических моментах (например, команды в консоли).

Архитектура проекта

В данном разделе представлено краткое описание архитектуры проекта. Подробное описание архитектуры представлено в документе «Архитектура и описание системы» (не является частью публичной документации, обратитесь к представителю VK Tech, чтобы ознакомиться с документом).



VK Teams представляет собой одну виртуальную машину и может рассматриваться как один компонент сети.

Инсталляция VK Teams не требует отдельных компонентов вне сегмента сети DMZ. Однако VK Teams активно взаимодействует с внешними и внутренними компонентами сети.

Как правило, сервер VK Teams устанавливается внутри DMZ и не имеет внешнего IP-адреса. Вместо этого весь необходимый трафик идет через NAT или WAF.

Обязательные компоненты

Сервер VK Teams

В сегменте сети DMZ.

Сервер NTP

Используется для синхронизации времени, предоставляется заказчиком. Может быть использован как публичный, так и ваш собственный сервер. На схеме предполагается, что сервер находится в вашем сегменте DMZ.

Сервер SMTP

Используется для отправки OTP-сообщений, предоставляется заказчиком. Может быть использован как публичный, так и ваш собственный сервер. На схеме предполагается, что сервер находится в вашем сегменте DMZ.

Сервер DNS

Используется для преобразования имен в IP-адреса и обратно, предоставляется заказчиком. Может быть использован как публичный, так и ваш собственный сервер. На схеме предполагается, что сервер находится в вашем сегменте DMZ.

Push-сервисы

Внешние сервисы Apple и Google для отправки push-сообщений на мобильные платформы. Расположены во внешнем периметре. Серверу VK Teams требуются исходящие соединения к этим сервисам и не требуются входящие соединения.

Приложение VK Teams

Пользовательское приложение, установленное на одной из допустимых платформ. Сервер VK Teams должен иметь возможность принимать входящие сообщения от этого приложения, а также отправлять ответы. Основное взаимодействие осуществляется через протокол HTTPS (443/TCP). Для работы видео- и аудиозвонков необходимы протоколы STUN и TURN: входящие соединения на порты 3478/TCP и 3478/UDP, а также входящий и исходящий трафик UDP по портам 1024+ (RTP-трафик).

Опциональные компоненты

WAF (Web application firewall)

Осуществляет фильтрацию входящего HTTP-трафика, а также акселерацию SSL-трафика. Предоставляется заказчиком.

DLP (Data Leak Prevention)

Система для предотвращения утечки данных. Предоставляется заказчиком.

LDAP

Используется для получения списка пользователей в системе. VK Teams может обслуживать как пользователей, заведенных в LDAP заказчика, так и внутренних пользователей. Интеграция с LDAP не является обязательным условием, но очень удобна для тех, кто имеет внутренний LDAP, например MS Active Directory.

Антивирус

Используется для проверки файлов на вирусы. Не является обязательным компонентом. Предоставляется заказчиком.

Описание дистрибутива и технические требования

Дистрибутив мессенджера VK Teams поставляется в виде образа виртуальной машины сервера, а также набора приложений для мобильных устройств или компьютера.

Минимальные требования к серверу в зависимости от количества пользователей:

Количество пользователей	vCPU	RAM, GB	SSD, GB	S3, GB / год
Тестовая установка				
1 000	22	56	350: root 100 GB data 250 GB	-
Продуктивная установка				
От 1 до 2 000	22	56	350: root 100 GB data 250 GB	500
От 2 001 до 5 000	30	72	350: root 100 GB data 250 GB	1 000
От 5 001 до 10 000	40	112	650: root 100 GB data 550 GB	3 500

- vCPU: Обязательная поддержка Time Stamp Counter (TSC). Проверить наличие можно поиском флага **constant_tsc в /proc/cpuinfo**. Любой современный процессор поддерживает эту технологию, однако иногда этого регистра нет внутри виртуальной машины. В этом случае необходимо правильно настроить систему виртуализации.
- Входящий трафик: TCP — 25 Мбит/с; UDP — 25 Мбит/с.

Совместимость:

- ПО VMware версий 6.x — 7.x.
- Любые системы виртуализации, основанные на KVM, например OpenStack.
- VK Cloud Solutions.

Более подробно технические данные и требования представлены в документе «Архитектура и описание системы» (не является частью публичной документации, обратитесь к представителю VK Tech, чтобы ознакомиться с документом).

Предварительные условия для установки

Перед установкой необходимо обеспечить:

Роутинг исходящих соединений

Необходим для отправки push-сообщений (через сервисы Apple, Google) и для работы голосовых и видео-звонков.

SMTP-сервер

Авторизация пользователей в мессенджере выполняется с помощью одноразовых кодов (OTP via email). Для доставки писем с одноразовыми кодами необходим SMTP-сервер, на котором разрешена отправка почтовых сообщений для данной виртуальной машины — без авторизации и блокировки антиспам-системой.

NTP-серверы

Нужны для синхронизации времени. Возможно указание внешних серверов, если нет сложностей с прохождением сетевых фильтров.

Исходящие соединения на стороне клиента

Разрешить подключение: 80/TCP, 443/TCP, 3478/TCP + UDP, UDP-порты выше 1024.

LDAP

Сервис VK Teams может работать как обособленно, так и в связке с корпоративным LDAP-сервером.

Система предоставляет возможность указать настройки для соединения с LDAP-сервером (при его наличии) во время инсталляции или после ее завершения.

Информация по управлению параметрами синхронизации LDAP **после** инсталляции мессенджера представлена в документе «Инструкция по интеграции с контроллером домена по протоколу LDAP».

Если настройки для соединения с LDAP-сервером производятся **в момент** инсталляции, Вам необходимы:

- Доступ к LDAP-серверу;
- Настройки для соединения с LDAP-сервером: bind_dn, user_dn, url, password, CA-сертификат;
- Название группы пользователей, которым будет доступно окружение администратора, например, **myteam-admin**. Название группы будет использовано при настройке доступа к окружению администратора.

Возможна работа без LDAP, с добавлением пользователей вручную (подробнее см. «Руководство по администрированию»).

Установка VK Teams из графического интерфейса

Процесс установки мессенджера условно делится на:

1. Действия в консоли — шаги 1-9;
2. Действия в графическом интерфейсе установщика — шаги 10-14;
3. Рестарт виртуальной машины в консоли — шаг 15.

Для установки VK Teams из графического интерфейса необходимо выполнить шаги, представленные ниже.

> **Внимание**
>
> Все команды в консоли выполняются под пользователем root.

Шаг 1. Предварительные условия для установки

Перед началом инсталляции убедитесь, что выполнены все предварительные условия (см. раздел Предварительные условия для установки).

Шаг 2. Проверка целостности полученных образов виртуальных машин

Чтобы проверить целостность образов виртуальных машин, в директории со скачанными файлами выполните в командной строке:

Linux

```
md5sum *
```

Windows

```
CertUtil -hashfile myteam.ova MD5
CertUtil -hashfile myteam.qcow2 MD5
CertUtil -hashfile myteam-data.qcow2 MD5
```

Mac

```
md5 *
```

Далее сравните полученное значение с хеш-суммой, указанной в текстовом файле **md5.txt**, распространяемом с дистрибутивом.

Шаг 3. Запуск образа виртуальной машины

Запустите образ виртуальной машины.

Шаг 4. Подключение к виртуальной машине

Подключитесь к виртуальной машине по SSH.

Пользователь: **centos**

Пароль: **djhMRG1vO**

> **Внимание**
>
> Чтобы получить пароль для пользователя root, обратитесь в службу технической поддержки.
> После подключения к виртуальной машине пароли для пользователей root и centos необходимо сменить.

macOS или Linux:

```
ssh centos@<VM IP address>
```

Windows: зависит от используемого SSH-клиента.

Шаг 5. Генерация SSH ключа для установщика

Для доступа установщика к серверу VK Teams необходимо сгенерировать ключ на сервере VK Teams:

```
ssh-keygen -f vkt_key
```

После этого публичную часть ключа необходимо добавить пользователю **centos** в список авторизованных ключей:

```
cat vkt_key.pub >> /home/centos/.ssh/authorized_keys
```

Приватная часть ключа (vkt_key) будет использоваться при запуске установщика.

Шаг 6. IP-адрес

Перед началом инсталляции необходимо определить, будет ли доступен сервис в интернете.

Если сервис не будет доступен в интернете, то необходимо использовать внутренний IP-адрес разворачиваемой виртуальной машины.

Если сервис будет доступен в интернете, необходимо использовать внешний IPv4 адрес виртуальной машины. Адрес может быть поднят как внутри виртуальной машины, так и проброшен через NAT. Преобразование сетевых адресов (NAT) должно быть вида 1-в-1 (сеть в сеть), то есть с сохранением номера порта. Иначе видео и голосовые звонки могут не работать.

IP-адрес в дальнейшем будет использоваться при запуске установщика.

При использовании внешнего IP-адреса необходимо произвести настройки DNS-зоны (см. Шаг 7. Настройки DNS-зоны).

Шаг 7. Настройки DNS-зоны

Заведите в DNS-зоне имена хостов, которые будут смотреть на внешний IPv4 адрес.

Список имен (CNAME либо A-записи на ваше усмотрение):

- u
- ub
- s
- webim
- api
- admin
- dl
- di
- di-dark
- biz
- call
- calendar
- mobile-calendar
- stentor

Например, для домена vkteams.example.com имя хоста будет выглядеть как u.vkteams.example.com.

Вариант 1.

Если есть возможность создания записи Wildcard CNAME в DNS, то можно создать A-запись, указывающую на адрес сервера VK Teams, и запись Wildcard CNAME, указывающую на A-запись сервера VK Teams.

```
$ host -t axfr example.com | grep vkteams
vkteams.example.com.           3600    IN      A       172.27.59.10
*.vkteams.example.com.         3600    IN      CNAME   vkteams.example.com.
```

Вариант 2.

Если нет возможности создания записи Wildcard CNAME в DNS, то можно создать A-запись, указывающую на адрес сервера VK Teams, и отдельные записи CNAME, которые будут разрешаться на созданную A-запись. Записи CNAME должны соответствовать перечню имен, представленному выше.

```
$ host -t axfr example.com | grep vkteams
vkteams.example.com.                  3600  IN     A       172.27.59.10
u.vkteams.example.com.                3600  IN     CNAME   vkteams.example.com.
ub.vkteams.example.com.               3600  IN     CNAME   vkteams.example.com.
s.vkteams.example.com.                3600  IN     CNAME   vkteams.example.com.
di.vkteams.example.com.               3600  IN     CNAME   vkteams.example.com.
webim.vkteams.example.com.            3600  IN     CNAME   vkteams.example.com.
api.vkteams.example.com.              3600  IN     CNAME   vkteams.example.com.
admin.vkteams.example.com.            3600  IN     CNAME   vkteams.example.com.
dl.vkteams.example.com.               3600  IN     CNAME   vkteams.example.com.
di.vkteams.example.com.               3600  IN     CNAME   vkteams.example.com.
di-dark.vkteams.example.com.          3600  IN     CNAME   vkteams.example.com.
call.vkteams.example.com.             3600  IN     CNAME   vkteams.example.com.
calendar.vkteams.example.com.         3600  IN     CNAME   vkteams.example.com.
mobile-calendar.vkteams.example.com.  3600  IN     CNAME   vkteams.example.com.
biz.vkteams.example.com.              3600  IN     CNAME   vkteams.example.com.
stentor.vkteams.example.com.          3600  IN     CNAME   vkteams.example.com.
```

> **Внимание**
>
> Не вносите изменения в **etc/resolv.conf**. Если изменения всё же необходимо внести, то первым должен быть указан хост 127.0.0.1.

Шаг 8. Выпуск SSL-сертификата

В целях безопасности используется SSL-шифрование, для работы сервера необходимо выпустить SSL-сертификат.

Если вы используете сертификаты собственного центра сертификации, выпустите сертификат, который далее понадобится при настройке VK Teams (см. Настройки SSL-сертификата). Используйте Wildcard-сертификат, например *.vkteams.EXAMPLE.com, или сертификат с указанием всех необходимых имен (см. раздел Шаг 7. Настройки DNS-зоны).

Для SSL-сертификатов также можно использовать протокол ACME (поддерживается только провайдер Let`s Encrypt). В этом случае получение и продление сертификатов — автоматическое.

Шаг 9. Открыть доступы до внутренних ресурсов

Входящие соединения на стороне сервера VK Teams:

Открыть порты: 80/TCP, 443/TCP, 3478/TCP + UDP, UDP-порты выше 1024.

Исходящие соединения на стороне сервера VK Teams:

- **Открыть доступ для серверов отправки уведомлений**:

  необходимо обеспечить доступ к серверам Google и Apple для отправки и корректной работы push-уведомлений на мобильных платформах Android и iOS.

  Сервер Apple
  TCP 5223;443;2197
  IP 17.0.0.0/8
  Статья на сайте apple.com

  Сервер Google
  TCP 5228;5229;5230;443
  Информация на ipinfo.io
  Статья на сайте google.com

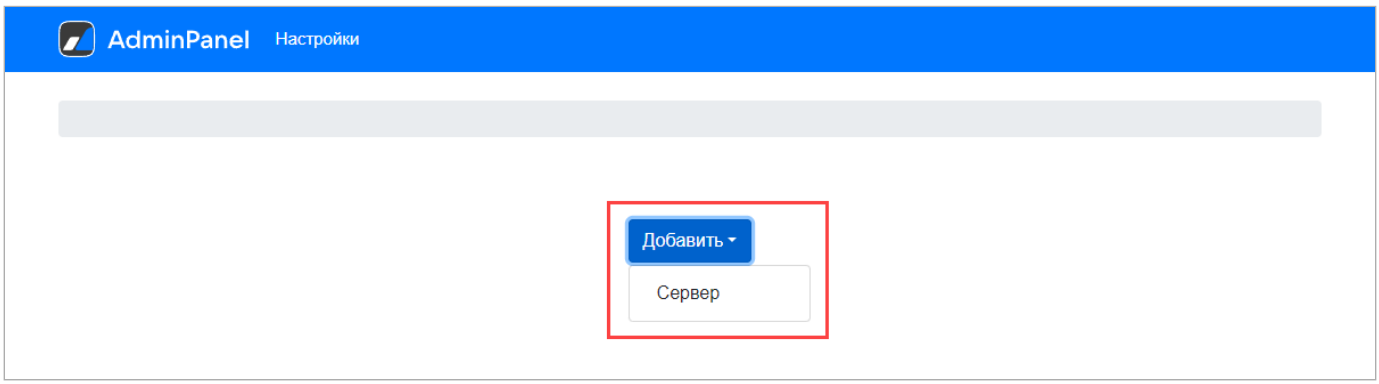
- **Открыть доступ до всех внутренних ресурсов**: LDAP, NTP, SMTP, DNS.

Шаг 10. Запуск установщика

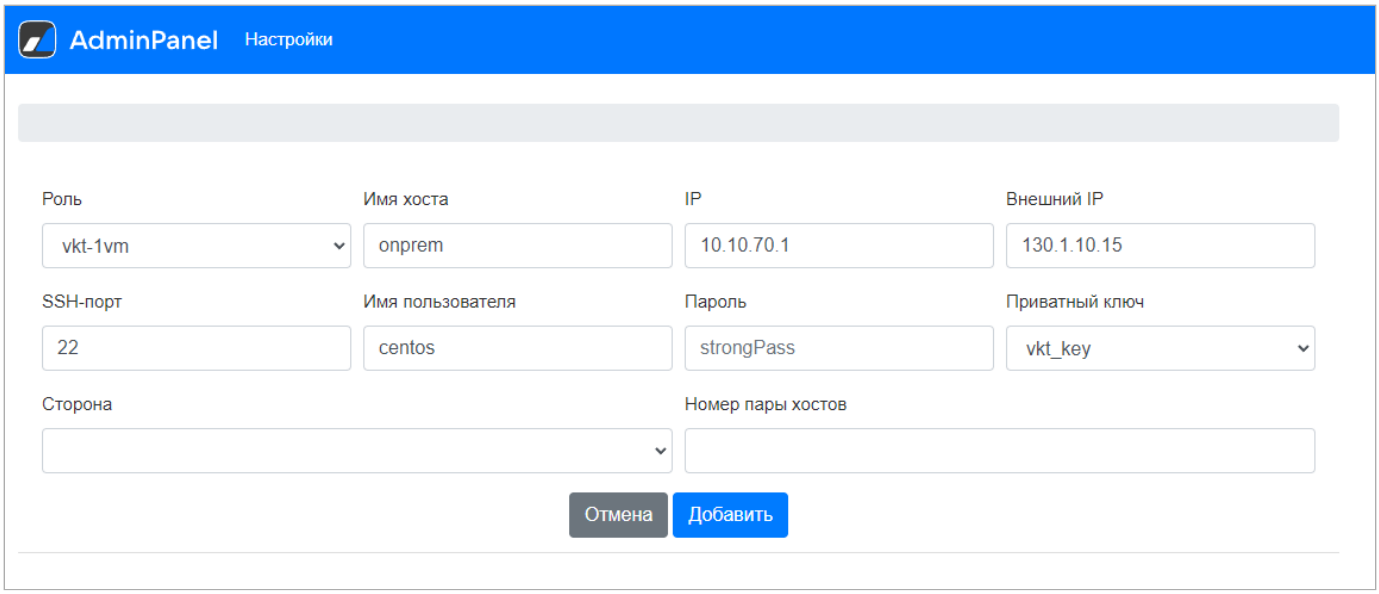
Распакуйте архив **vkt-web-deployer.tar.gz.zip** в отдельную директорию и запустите исполняемый файл. Далее перейдите по адресу http://127.0.0.1:8888.

Шаг 11. Добавление сервера в установщик

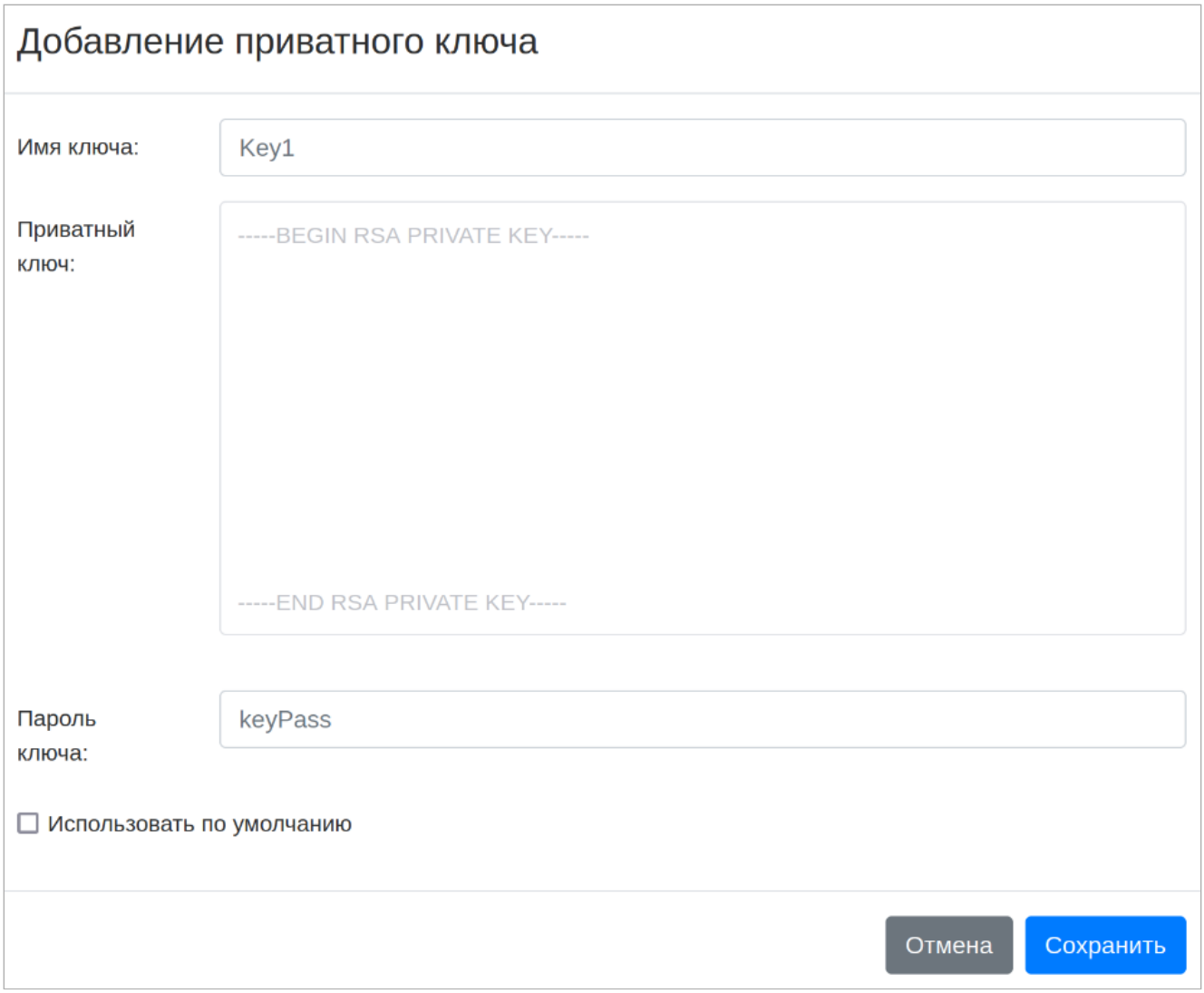
На главной странице установщика нажмите кнопку **Добавить → Сервер:**



На отобразившейся форме добавления сервера заполните поля:



- **Роль** — для установки standalone VK Teams нужно выбрать **vkt-1vm**;
- **Имя хоста** — короткое имя сервера (без домена);
- **IP** — IP-адрес, по которому будет осуществляться доступ установщика к серверу VK Teams;
- **Внешний IP** — внешний или внутренний IP-адрес, присвоенный на шаге Шаг 6. IP-адрес. Может совпадать со значением в поле **IP**;
- **SSH-порт** — порт SSH сервера (по умолчанию — 22);
- **Имя пользователя** — имя пользователя для соединения установщика по SSH (по умолчанию **centos**);
- **Пароль** — при использовании авторизации по паролю — **djhMRG1vO**. Поле не заполняется при использовании приватного ключа;
- **Сторона** — поле не используется при установке standalone;
- **Номер пары хостов** — поле не используется при установке standalone;
- **Приватный ключ** — ключ для доступа установщика к серверу VK Teams. Выберите в выпадающем списке поля **+ Добавить новый ключ**. В отобразившейся форме заполните поля:



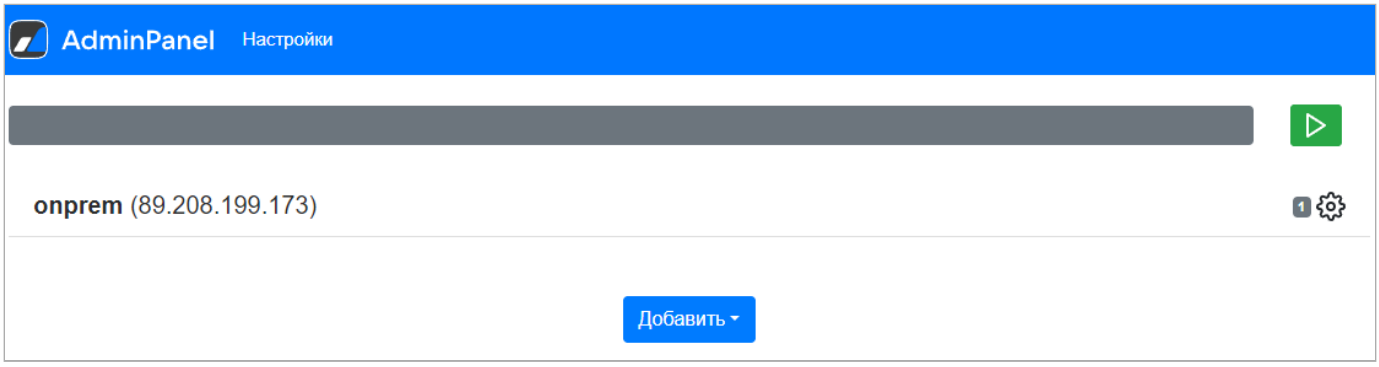
В поле **Приватный ключ** необходимо скопировать содержимое приватной части SSH ключа, созданного на шаге 5 (см. раздел Шаг 5. Генерация SSH ключа для установщика). Приватный ключ необходимо указать полностью, включая `-----BEGIN RSA PRIVATE KEY-----` и `-----END RSA PRIVATE KEY-----`.

В поле **Пароль ключа** указать пароль, созданный при генерации SSH ключа (если пароль не был создать — поле не заполнять).

Нажмите на кнопку **Сохранить**.

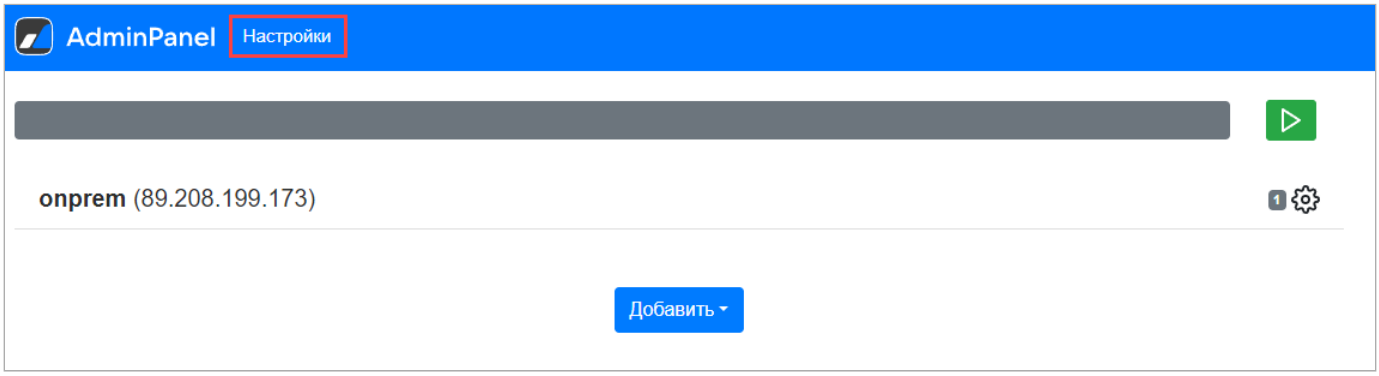
После заполнения полей на форме добавления сервера нажмите на кнопку **Добавить**.

Добавленный сервер отобразится в панели установщика:

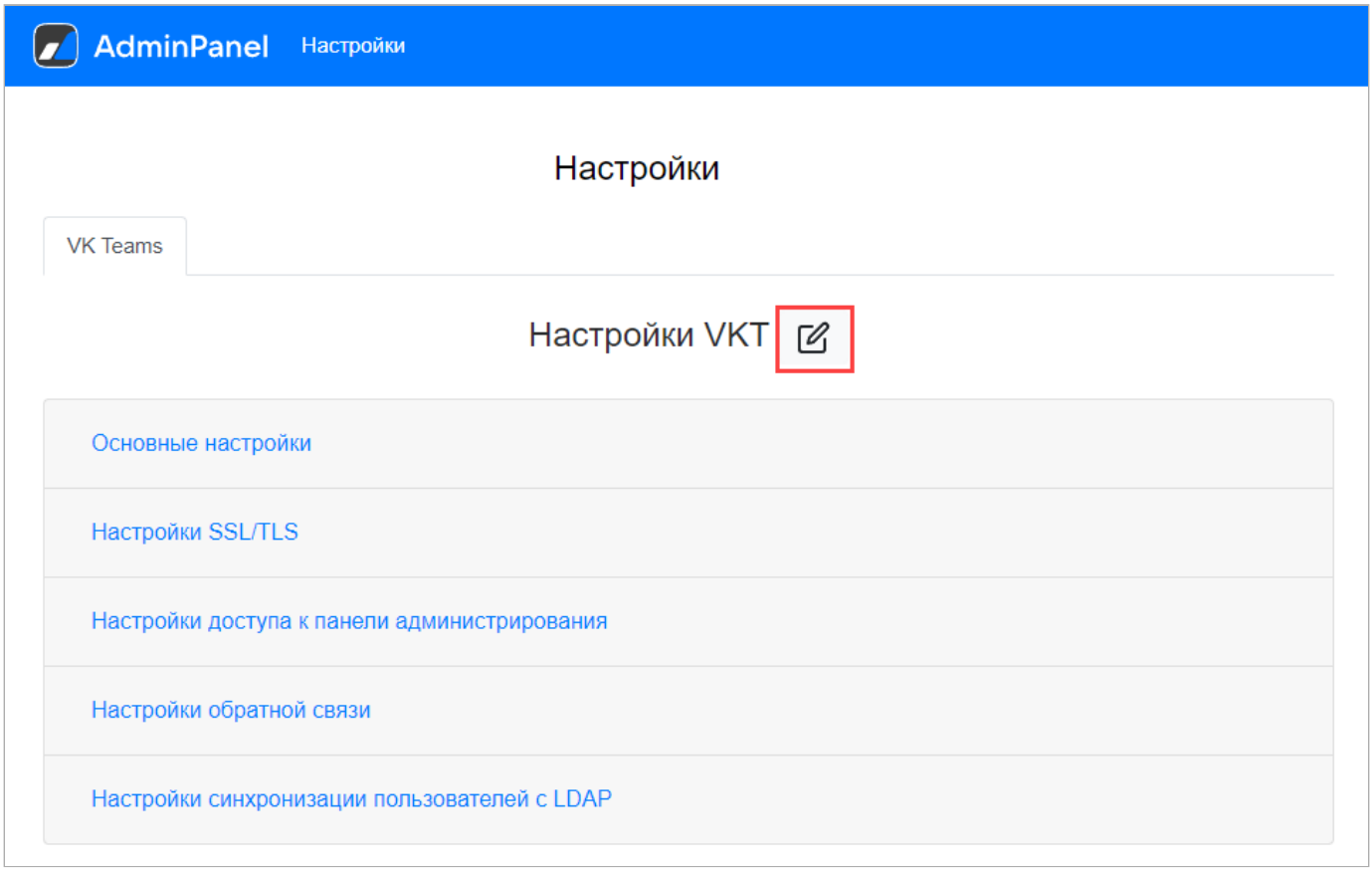


Шаг 12. Настройки VK Teams

После добавления сервера перейдите в раздел **Настройки**:



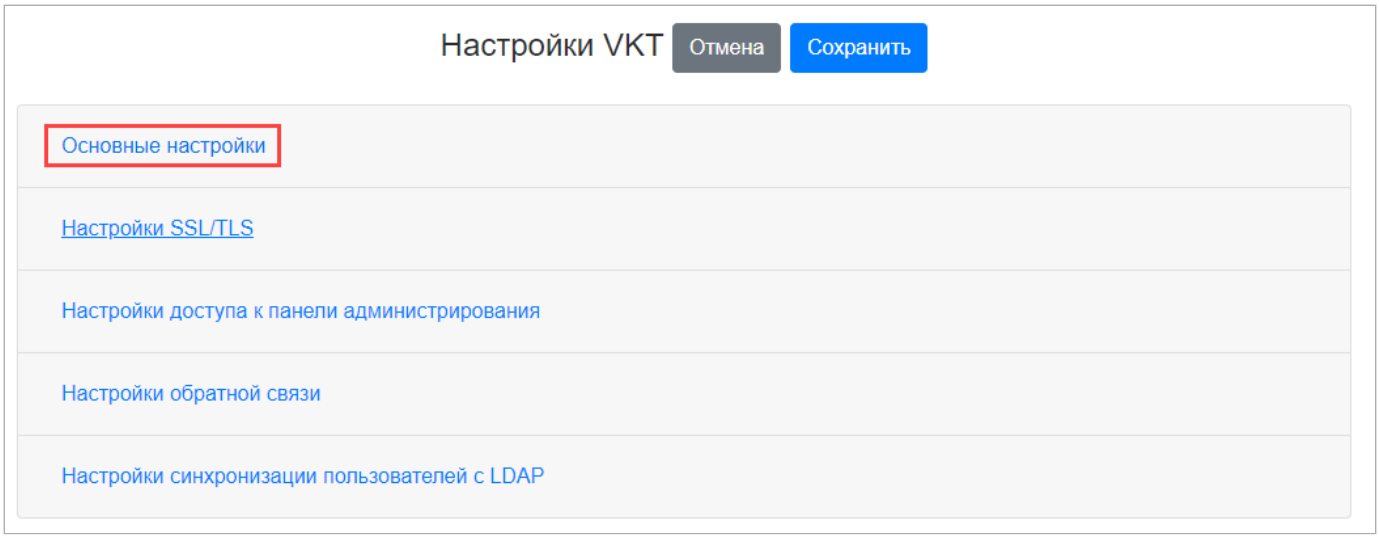
На отобразившейся странице нажмите на пиктограмму  , чтобы перейти в режим редактирования:



Ниже приведено подробное описание каждого пункта конфигурации.

Домен пользователя

Выберите раздел **Основные настройки**:



Для настройки сервера VK Teams укажите базовый домен. Например, vkteams.example.com означает, что клиентские приложения будут пытаться получить доступ к сайтам u.vkteams.example.com, ub.vkteams.example.com и т. д.

Список DNS-серверов

Укажите список DNS-серверов (IP-адреса серверов, которые будут использованы для разрешения имен).

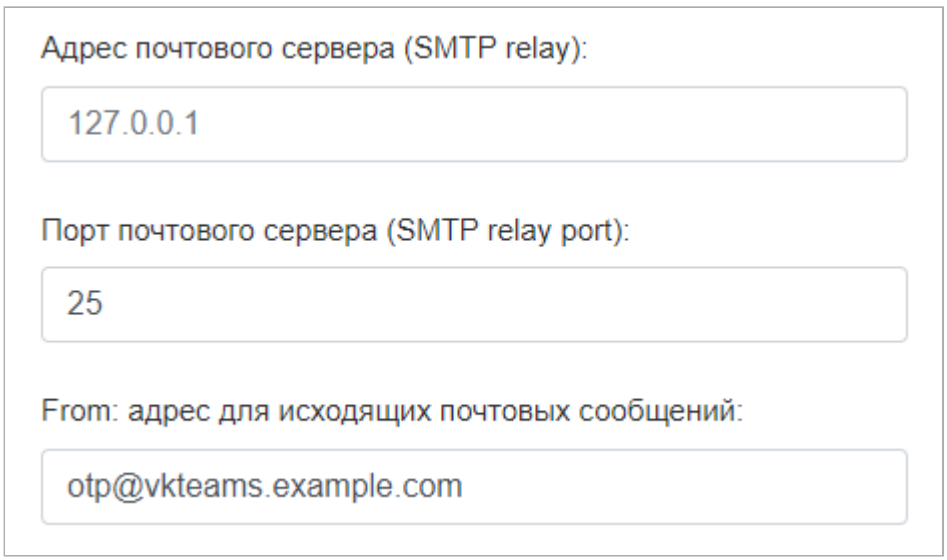
Список серверов точного времени (NTP)

Укажите список NTP-серверов (IP-адреса или имена хостов):

Настройка SMTP-сервера

Чтобы настроить OTP via email, укажите:

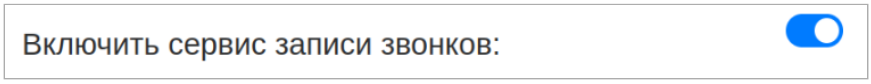
- Имя или IP-адрес SMTP-сервера.
- Порт SMTP-сервера (как правило, не требует редактирования).
- Обратный адрес для сообщений с OTP-кодами (поле **From:** в письме). Рекомендуется использовать реально существующий адрес.



Настройка сервиса записи звонков

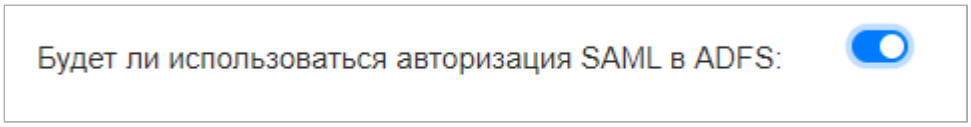
Данный параметр контролирует сервис записи звонков. При его включении звонки будут записываться, готовая запись будет отправлена пользователю в личные сообщения с помощью бота (Recorderbot).

На данный момент, запись доступна только в Desktop приложениях. По умолчанию запись включена.



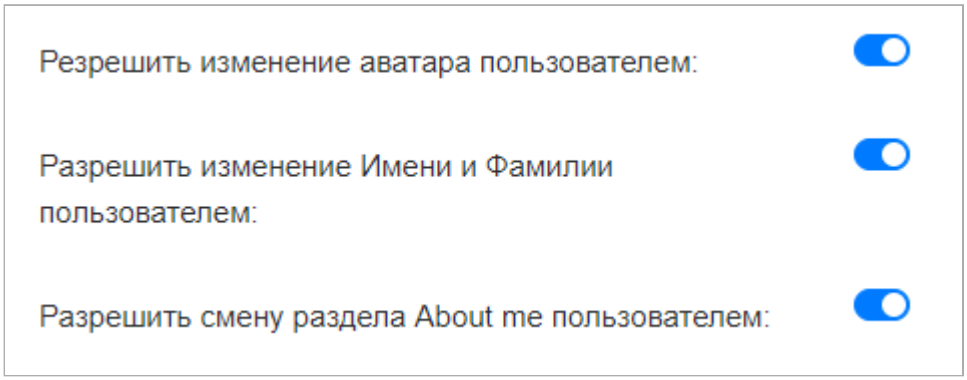
Настройка SSO-аутентификации

Если в дальнейшем планируется настройка SSO-аутентификации по протоколу SAML, установите переключатель в активное положение:

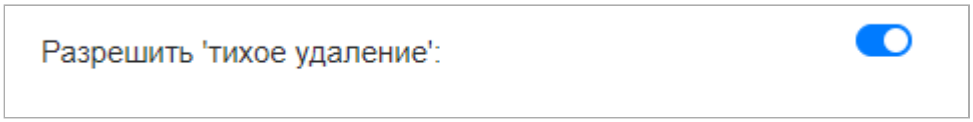


Установка разрешений для пользователей

Чтобы разрешить пользователям изменять информацию о себе в профиле мессенджера, установите переключатели:

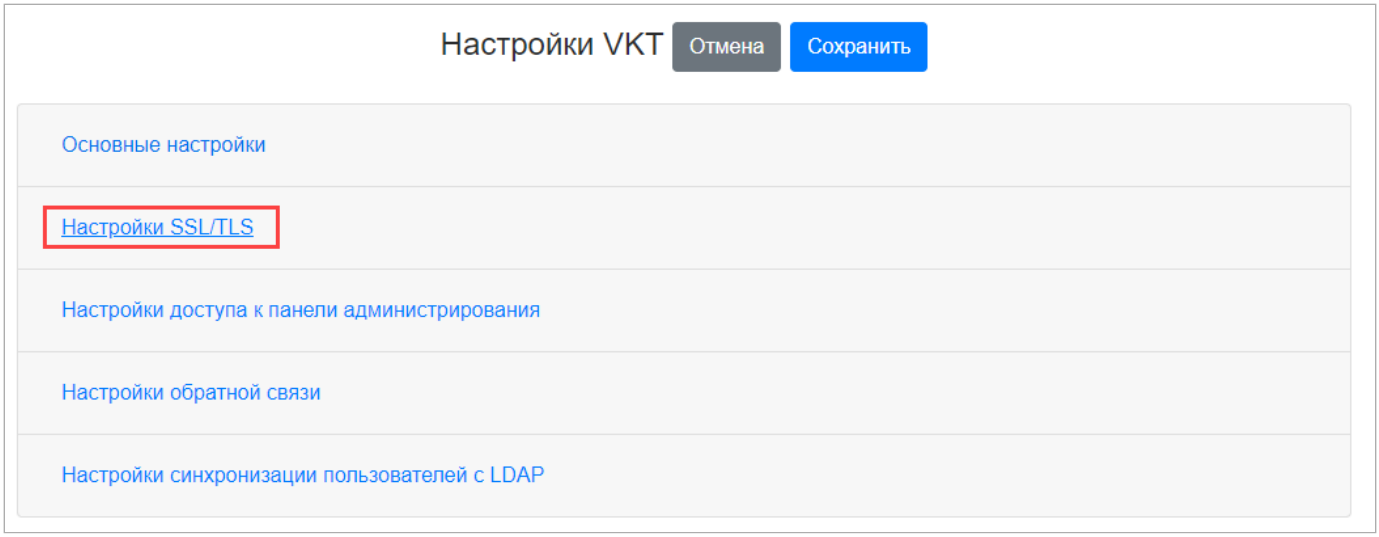


Чтобы разрешить удаление отправленного сообщения в личных чатах/группах без уведомления участников, установите переключатель:



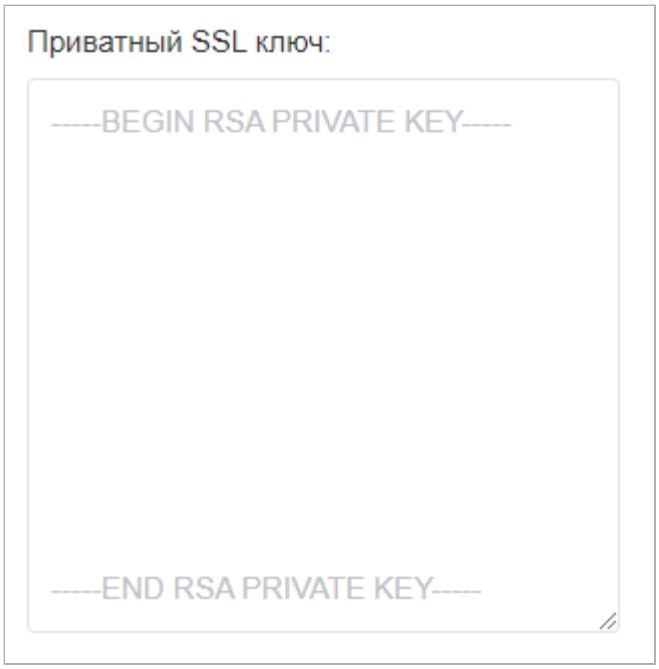
Настройки SSL-сертификата

Чтобы указать сертификаты, перейдите в раздел **Настройки SSL/TLS**:



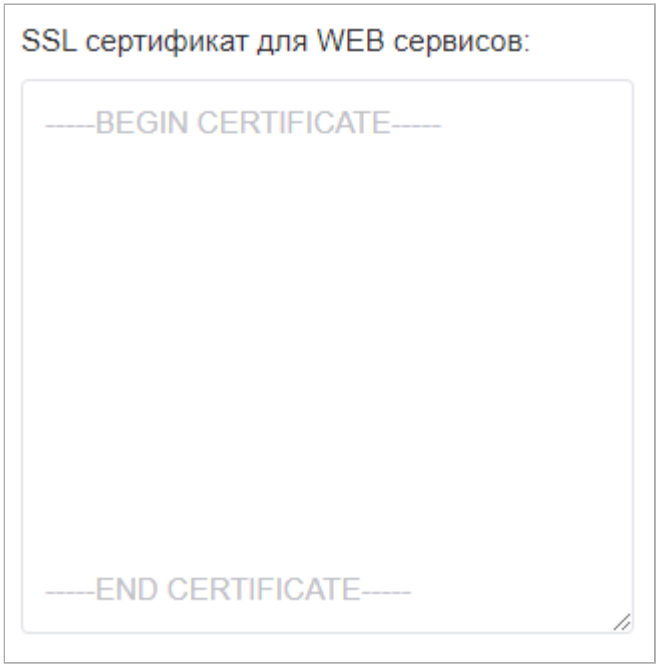
Укажите SSL-сертификат, выпущенный на шаге 8 (см. Шаг 8. Выпуск SSL-сертификата).

1. Приватный ключ для SSL-сертификата указывается в формате PEM и не должен быть защищен паролем:



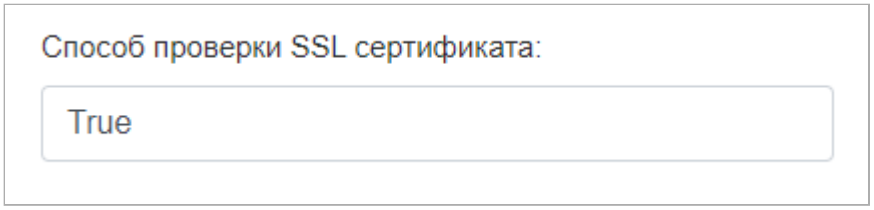
Приватный ключ необходимо указать полностью, включая `-----BEGIN RSA PRIVATE KEY-----` и `-----END RSA PRIVATE KEY-----`.

2. SSL-сертификат сервера в формате PEM. Для корректной работы укажите всю цепочку сертификатов (full chain):



SSL сертификаты необходимо указать полностью, включая `-----BEGIN RSA PRIVATE KEY-----` и `-----END RSA PRIVATE KEY-----`.

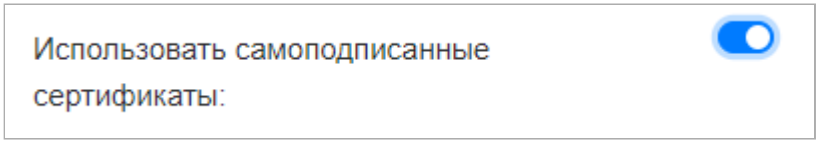
3. Укажите способ проверки SSL-сертификата:



Способ проверки SSL сертификата, может принимать 3 вида значений: True, False, путь до файла **.ca_bundle**:

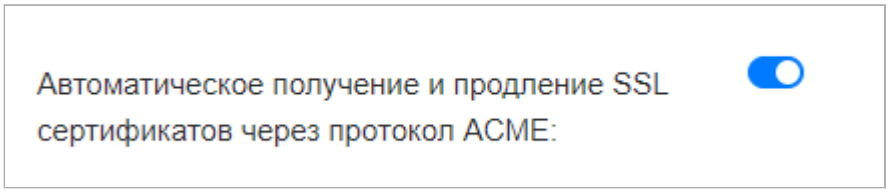
- True — проверять сертификат с центрами сертификации (CA) встроенными в ОС (по умолчанию);
- False — не проверять SSL сертификат, например, в случае использования самоподписанного сертификата;
- Путь до файла **.ca_bundle** — использовать свой центр сертификации (CA) для проверки сертификата.

4. Если планируется добавлять самоподписанные сертификаты, установите соответствующий переключатель:



Протокол ACME (Let`s Encrypt) для SSL-сертификатов

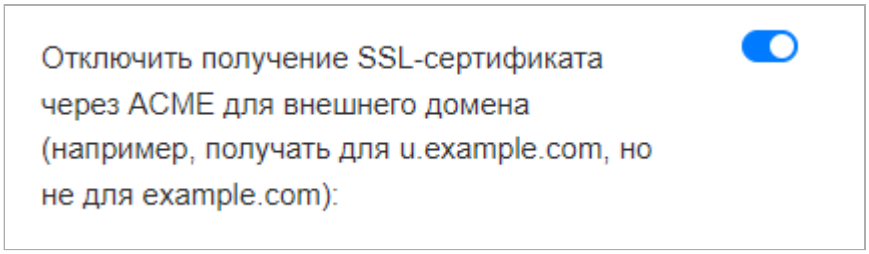
1. Чтобы использовать протокол ACME, установите переключатель Автоматическое получение и продление SSL сертификатов через протокол ACME:



> **Внимание**
>
> Включение этой опции и использование этого функционала означает согласие с условиями использования сервиса Let's Encrypt, с которыми можно ознакомиться по адресу https://letsencrypt.org/repository/.

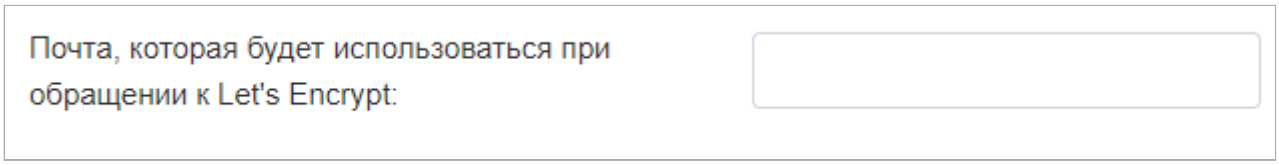
Поля **SSL сертификат для WEB сервисов** и **Приватный SSL ключ** можно не заполнять, при включении сертификатов через ACME они игнорируются.

2. Чтобы отключить получение SSL-сертификата через ACME для внешнего домена VK Teams, установите переключатель в соответствующее поле:



Данный переключатель необходимо установить, если в DNS нет записи, которая позволяет разрешить имя домена на внешний IP-адрес. Если переключатель неактивен, сертификат будет выпускаться.

3. Укажите почту, которая будет использоваться при обращении к Let's Encrypt (обязательный параметр, без корректной почты сертификаты выданы не будут). На эту почту будут поступать уведомления от сервиса Let's Encrypt:

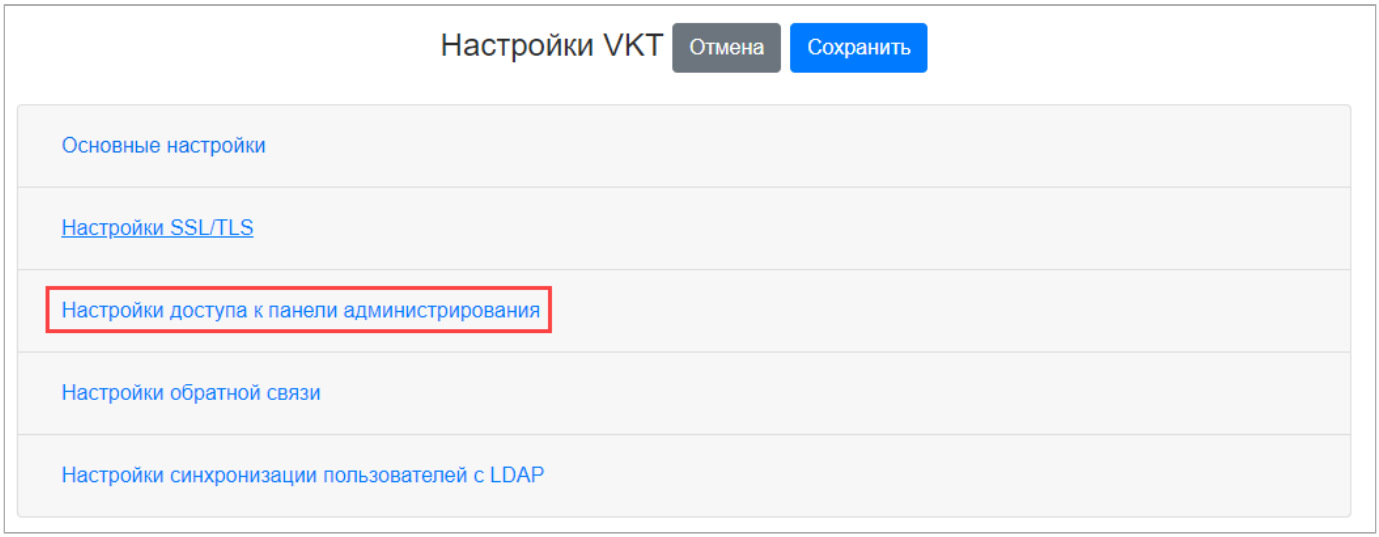


Примечание

Сертификат продлевается автоматически каждые 3 месяца, поэтому 80й порт должен быть открыт — иначе сертификат не обновится.

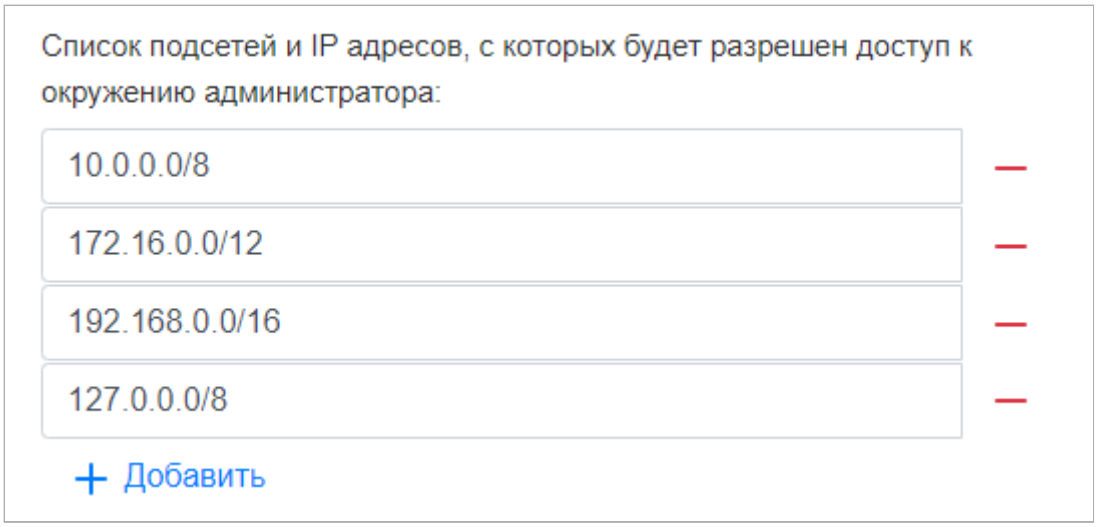
Настройка окружения администратора

Перейдите в раздел **Настройки доступа к панели администрирования**:



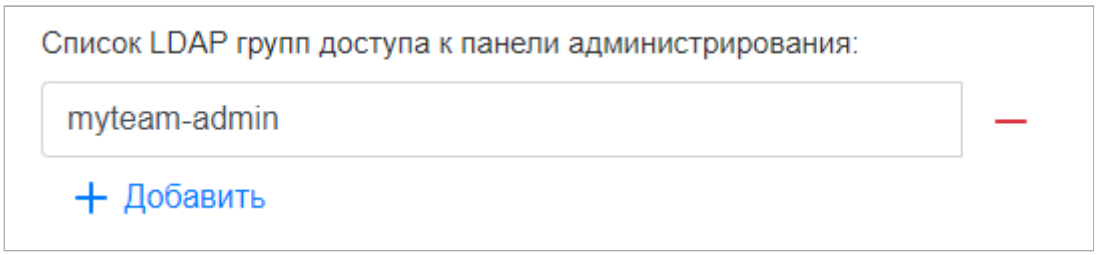
Интерфейс администратора доступен только с выбранных IP-адресов и только выбранным пользователям. Также предусмотрена настройка ограничения доступа к выбранным разделам окружения администратора (например, к выгрузке чатов).

По умолчанию окружение администратора доступно с IP-адресов приватных сетей (10.0.0.0/8, 172.16.0.0/12 и 192.168.0.0/16):



Доступ в окружение администратора настраивается через группы. Изначально перечень групп с доступом в окружение администратора пуст, потому окружение недоступно никому.

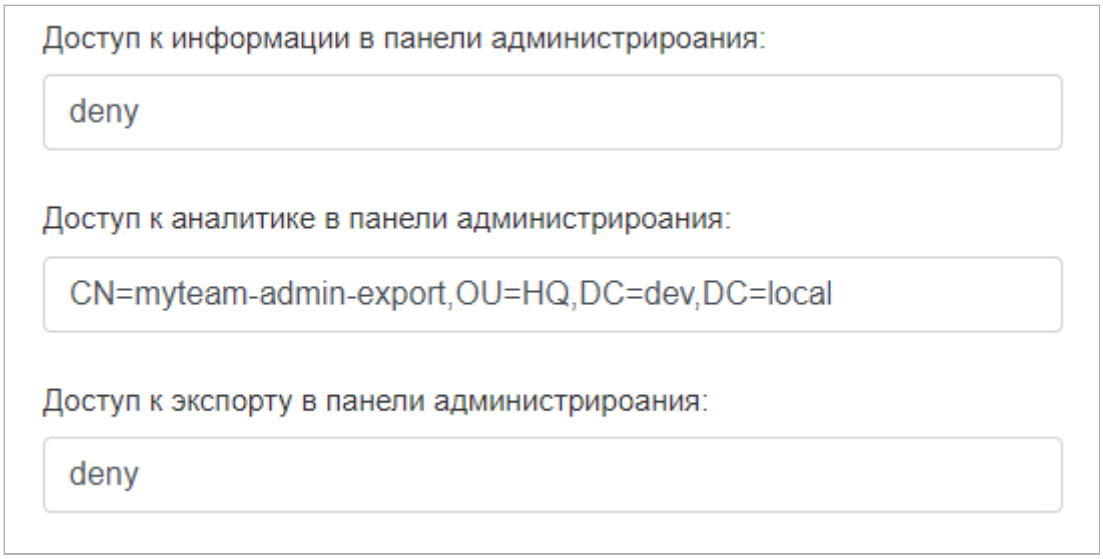
Если настройки для соединения с LDAP-сервером производятся **во время инсталляции**, укажите в поле **Список LDAP групп доступа к панели администрирования** заранее подготовленное наименование группы из LDAP, в которую будут входить пользователи с доступом в окружение администратора (см. раздел LDAP в предусловиях):



Если инсталляция производится без связи с корпоративным LDAP-сервером укажите в поле **Список LDAP групп доступа к панели администрирования** наименование группы из LDAP, в которую будут входить пользователи с доступом в окружение администратора (см. раздел LDAP в предусловиях). Информация по управлению параметрами синхронизации LDAP после инсталляции мессенджера представлена в документе «Инструкция по интеграции с контроллером домена по протоколу LDAP».

При отсутствии LDAP — укажите в поле **Список LDAP групп доступа к панели администрирования** наименование группы, которое будете использовать при создании пользователей в системе ручную после окончания процесса инсталляции (описание процесса представлено в документе «Руководство по администрированию»).

Управление доступом по группам к компонентам панели администрирования осуществляется через следующие параметры:

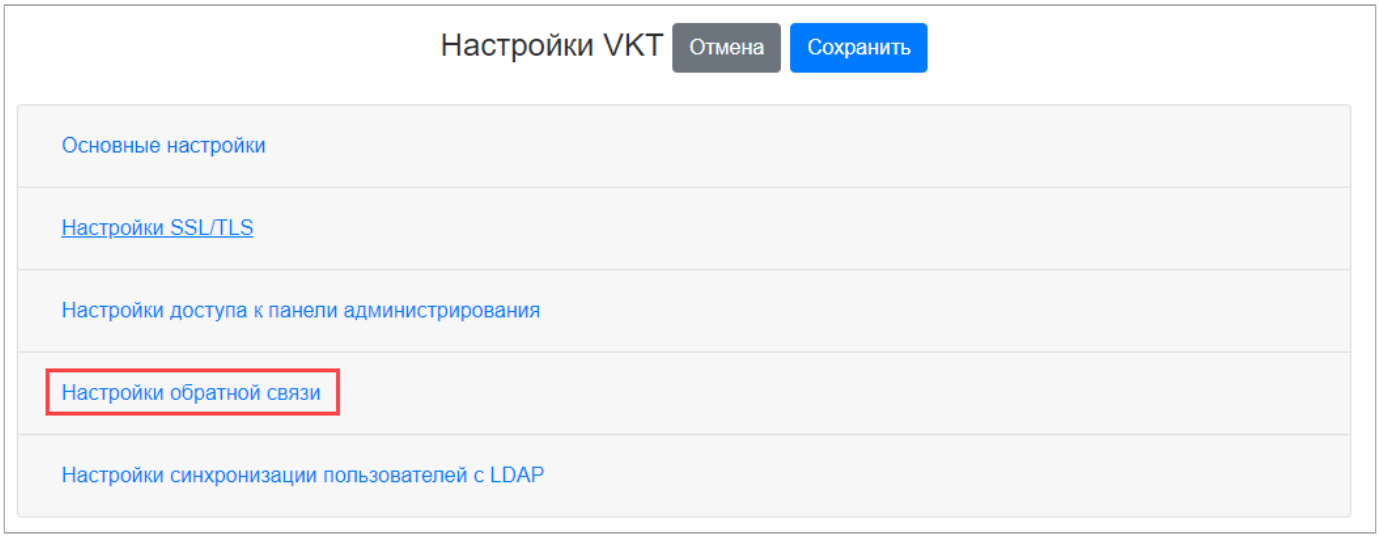


Каждое поле может принимать следующие значения:

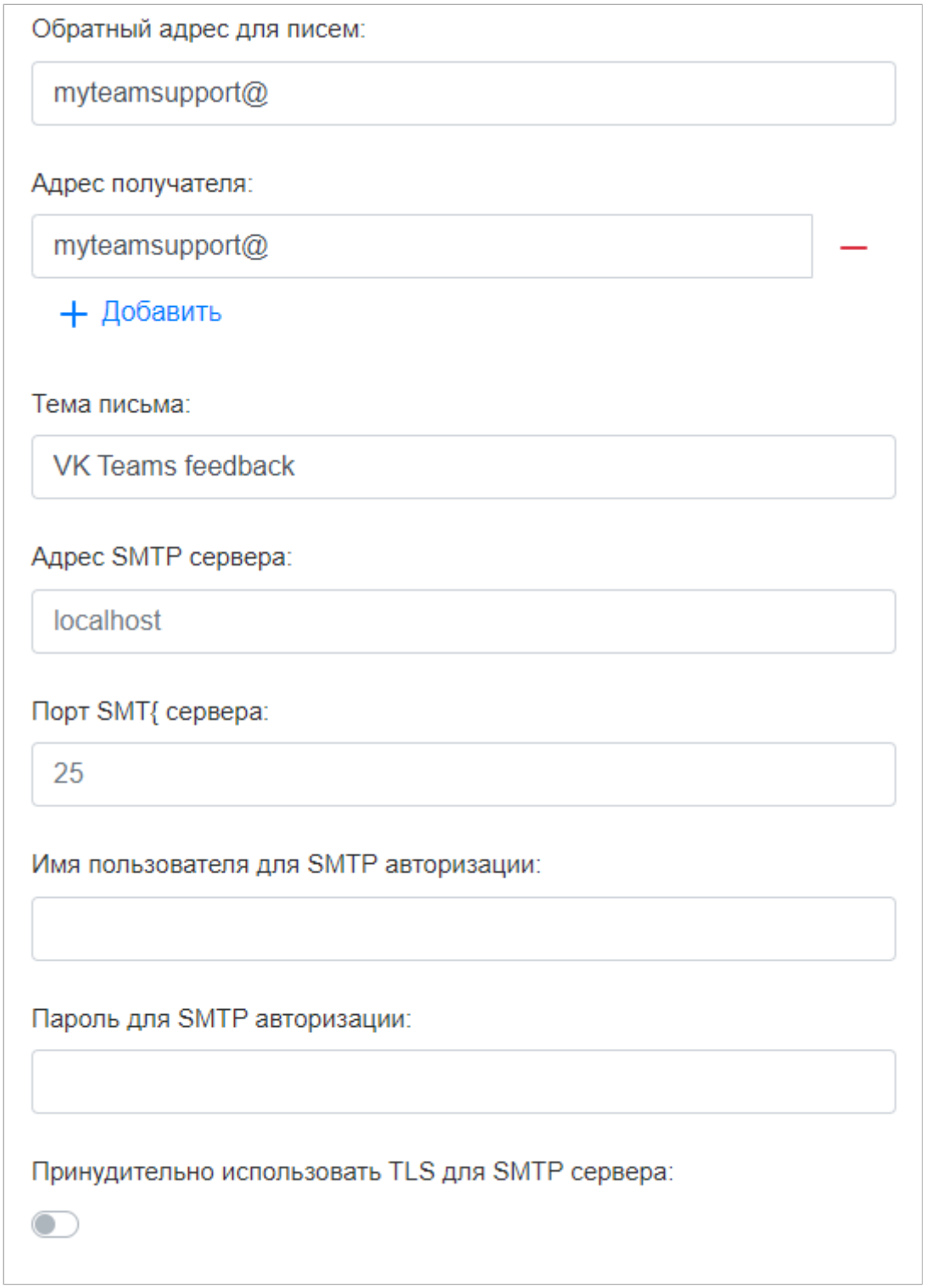
- deny — доступ запрещен для всех пользователей;
- allow — доступ разрешен для всех пользователей;
- любое другое значение — наименование группы, которой будет разрешен доступ к данному компоненту. Можно перечислить несколько групп через пробел.

Настройка обратной связи

Перейдите в раздел **Настройка обратной связи**:



По умолчанию все обращения пользователей поступают на адрес myteamsupport@USER-DOMAIN, через локальный SMTP-релей. Например, в случае домена **example.com** обращение поступит на адрес **myteamsupport@example.com**.



В полях **Обратный адрес для писем** и **Адрес получателя** в адреса, оканчивающиеся символом @, автоматически подставляется домен пользователя.

Параметр	Описание	Примеры
Обратный адрес для писем	Обратный адрес для письма, формируемого системой в адрес технической поддержки	• test@ — обратный адрес будет test@user-domain • test@example.com — обратный адрес будет test@example.com, независимо от домена пользователя

Параметр	Описание	Примеры
Адрес получателя	Адрес получателей. Получателей может быть несколько	• ['test@'] — получателем письма будет test@user-domain • ['test@', 'example@example.com'] — получателями письма будут test@user-domain и example@example.com
Тема письма	Тема отправляемого письма	

Расширенные настройки сервиса:

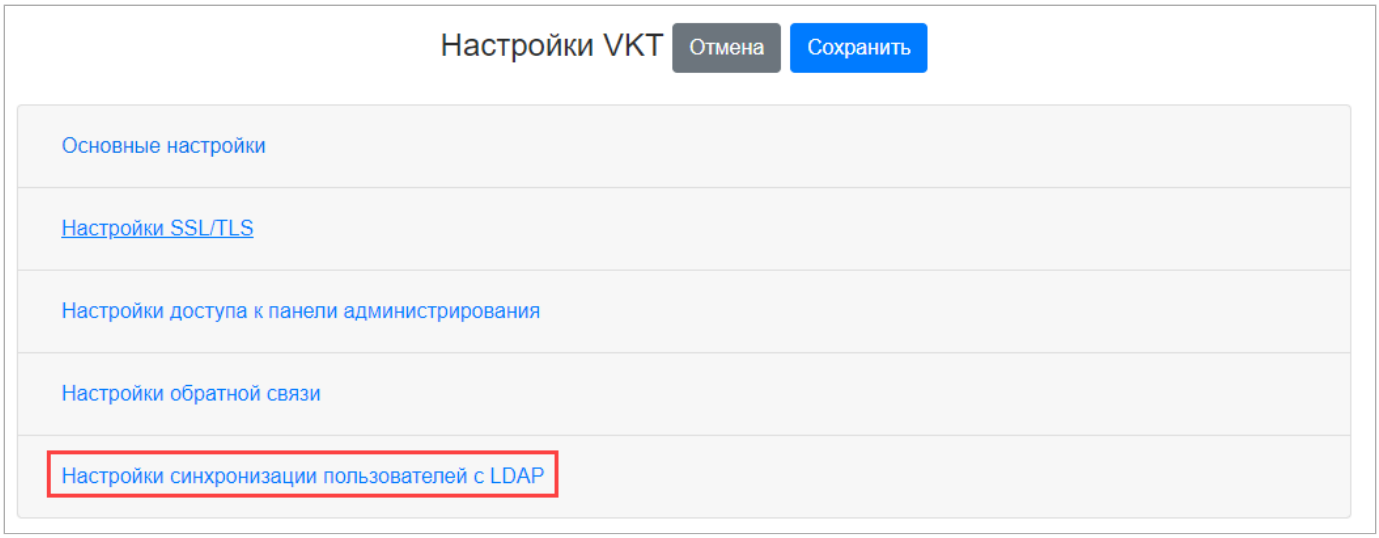
Используйте расширенные настройки, если хотите отправлять обращения пользователей через отдельный SMTP-сервер с использованием авторизации.

Настройка LDAP

Система предоставляет возможность указать настройки для соединения с LDAP-сервером во время инсталляции или после ее завершения.

Если инсталляция производится без связи с корпоративным LDAP-сервером или LDAP-сервер отсутствует, пропустите данный шаг и перейдите к Шаг 13. Проверка конфигурации. Описание процесса настройки интеграции с LDAP после инсталляции представлено в документе «Инструкция по интеграции с контроллером домена по протоколу LDAP».

Если настройки для соединения с LDAP-сервером производятся во время инсталляции, в установщике перейдите в раздел **Настройка синхронизации пользователей с LDAP**:

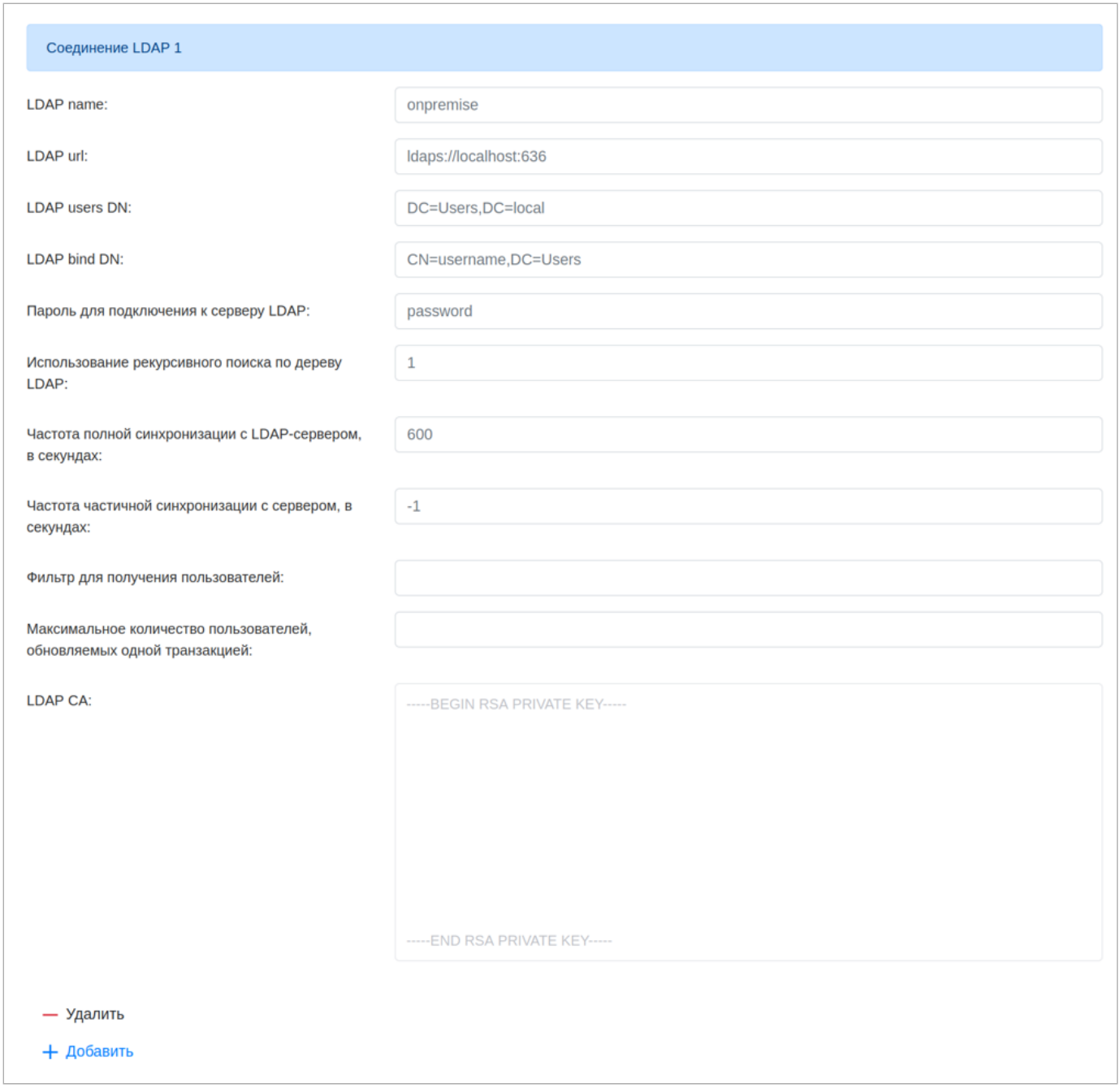


Рекомендуется предварительно проверить корректность заданных конфигурационных параметров LDAP с помощью утилиты **ldapsearch**:

```
//установка клиента для подключения к AD
yum install openldap-clients -y
```

```
// проверка, что параметры подключения к AD валидны
ldapsearch -H <ldap_url> -w <ldap_password> -x -D
<ldap_bind_dn> -b <ldap_users_dn> mail=ldap-user-email@EXAMPLE.com
```

, где **mail=ldap-user-email@EXAMPLE.com** — почтовый ящик пользователя



Если одно из полей не заполнено, устанавливается значение по умолчанию для сервиса Keycloak.

Основные доступные поля:

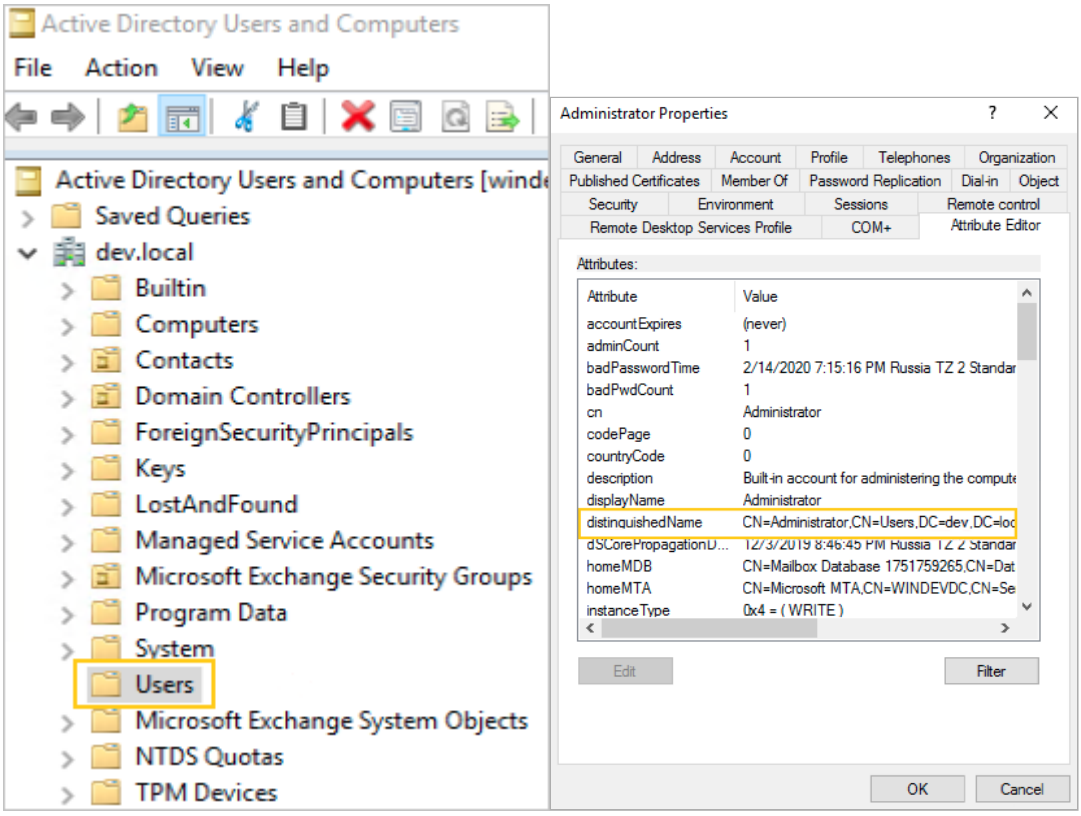
- **LDAP name** — имя LDAP-сервера. Данное имя уникально, может быть заведен только один сервер с определенным именем;
- **LDAP url** — адрес подключения к LDAP-серверу;
- **LDAP users DN** — указание на точку входа для поиска в LDAP;
- **LDAP bind DN** — пользователь под которым осуществляется подключение к LDAP-серверу;
- **Пароль для подключения к серверу LDAP** — пароль для подключения к LDAP-серверу;

- **Использование рекурсивного поиска по дереву LDAP** — использовать ли рекурсивный поиск по дереву LDAP:
  - 1 - искать в одном уровне (по умолчанию);
  - 2 - искать по всем уровням.
- **Частота полной синхронизации с LDAP-сервером, в секундах** — как часто осуществлять полную синхронизацию с LDAP-сервером, в секундах;
- **Частота частичной синхронизации с сервером, в секундах** — как часто осуществлять частичную синхронизацию с LDAP-сервером, в секундах (значение **-1** — отключить);
- **Максимальное количество пользователей, обновляемых одной транзакцией** — изменяйте в случае, если ваш LDAP-сервер отказывается отдавать пользователей с ошибкой о превышении размера транзакции;
- **Фильтр для получения пользователей** — позволяет получать не всех пользователей из указанного дерева. По умолчанию выборка пользователей не ограничена.

Как получить Distinguished Name для bindDN и usersDN в Active Directory

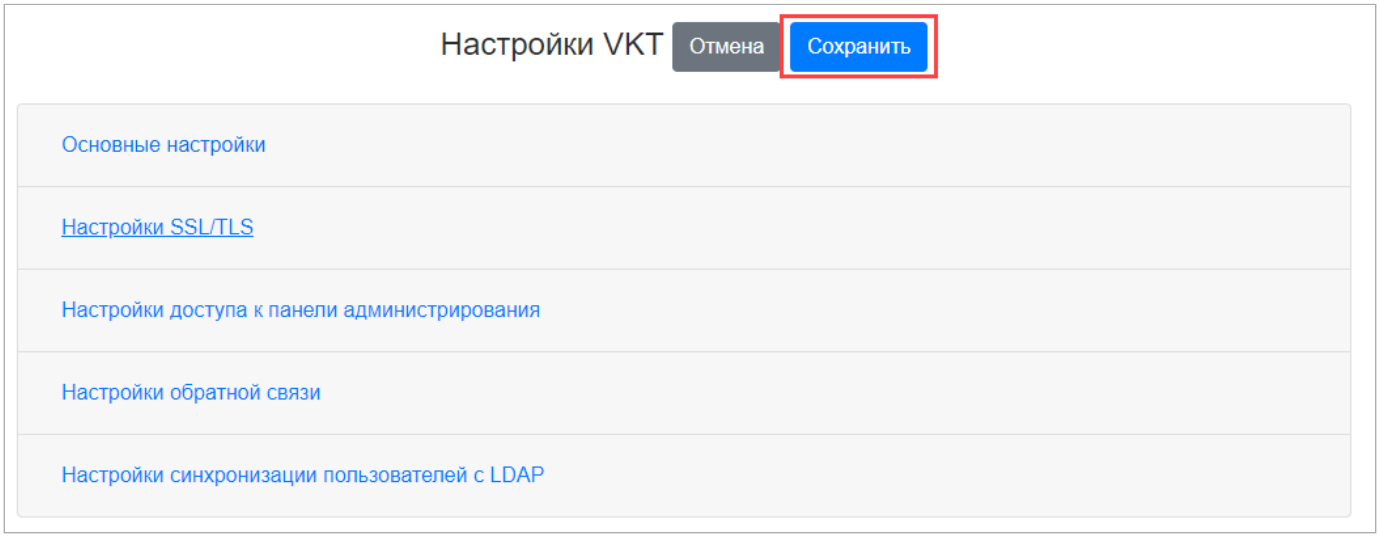
1. В оснастке **Active Directory Users and Computers** выберите пользователя, под которым будет происходить подключение и поиск пользователей;
2. Выберите свойства и перейдите на вкладку **Attribute Editor** (если вкладки нет, выберите в меню **View**, затем **Advanced Features**).

   На вкладке будет отображено значение **distinguishedName**. Повторите операцию, чтобы получить **distinguishedName** для каталога, в котором будет выполняться поиск пользователей.

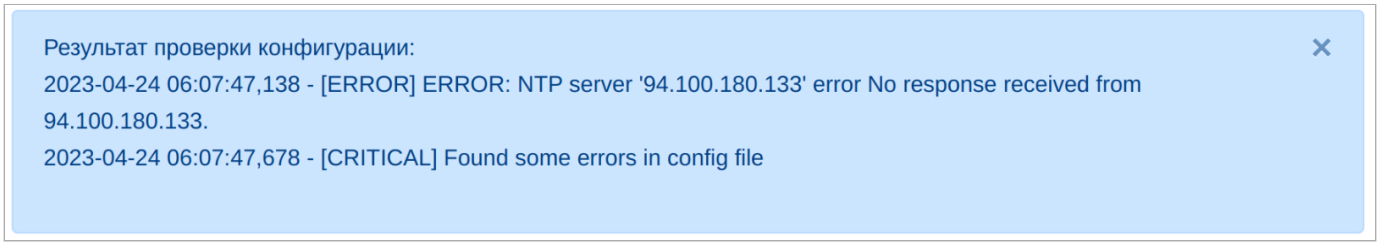


Шаг 13. Проверка конфигурации

Чтобы сохранить указанные настройки, нажмите на кнопку Сохранить:



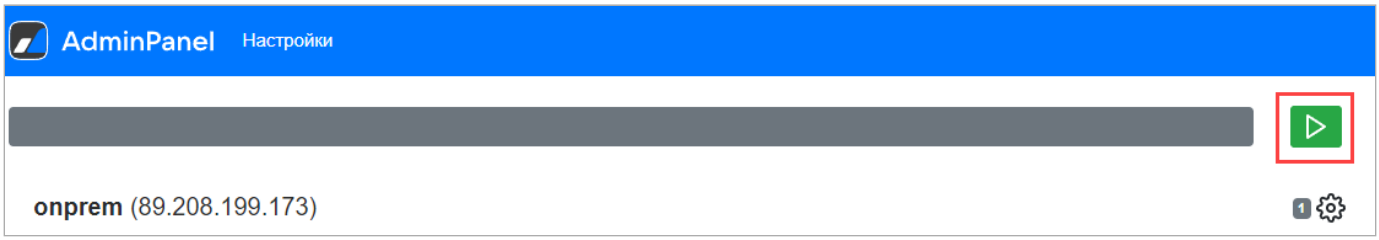
После сохранения настроек будет произведена их проверка. Если открыты не все нужные порты, либо нет интеграции с базовым набором сервисов (DNS, SMTP, NTP), отобразится уведомление о необходимости правок:



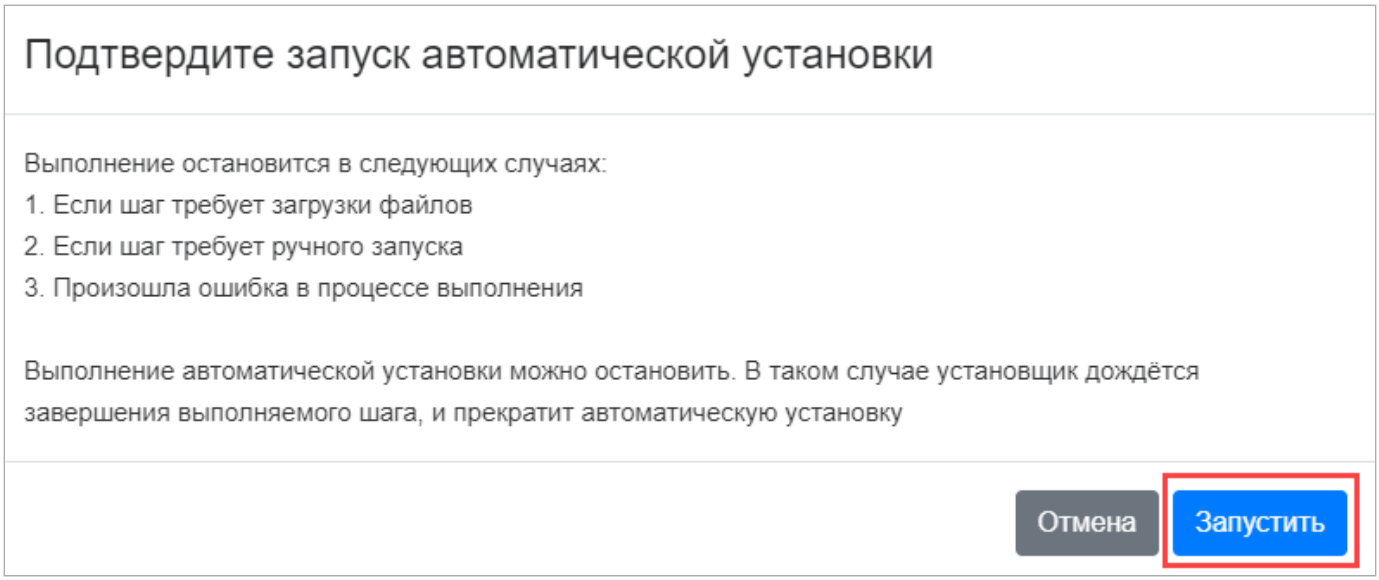
В случае обнаружения ошибок, их необходимо исправить.

Шаг 14. Запуск установки

После завершения настройки и проверки ошибок необходимо перейти на главную страницу и запустить установку нажатием на кнопку  :

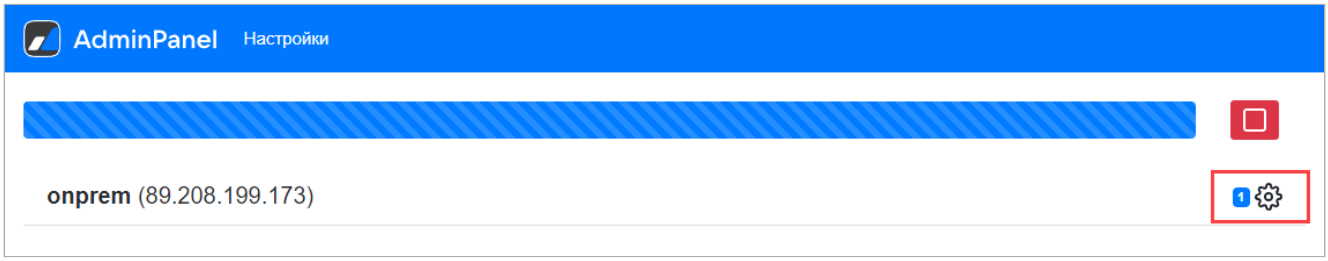


Подтвердите запуск автоматической установки, нажав на кнопку **Запустить**:

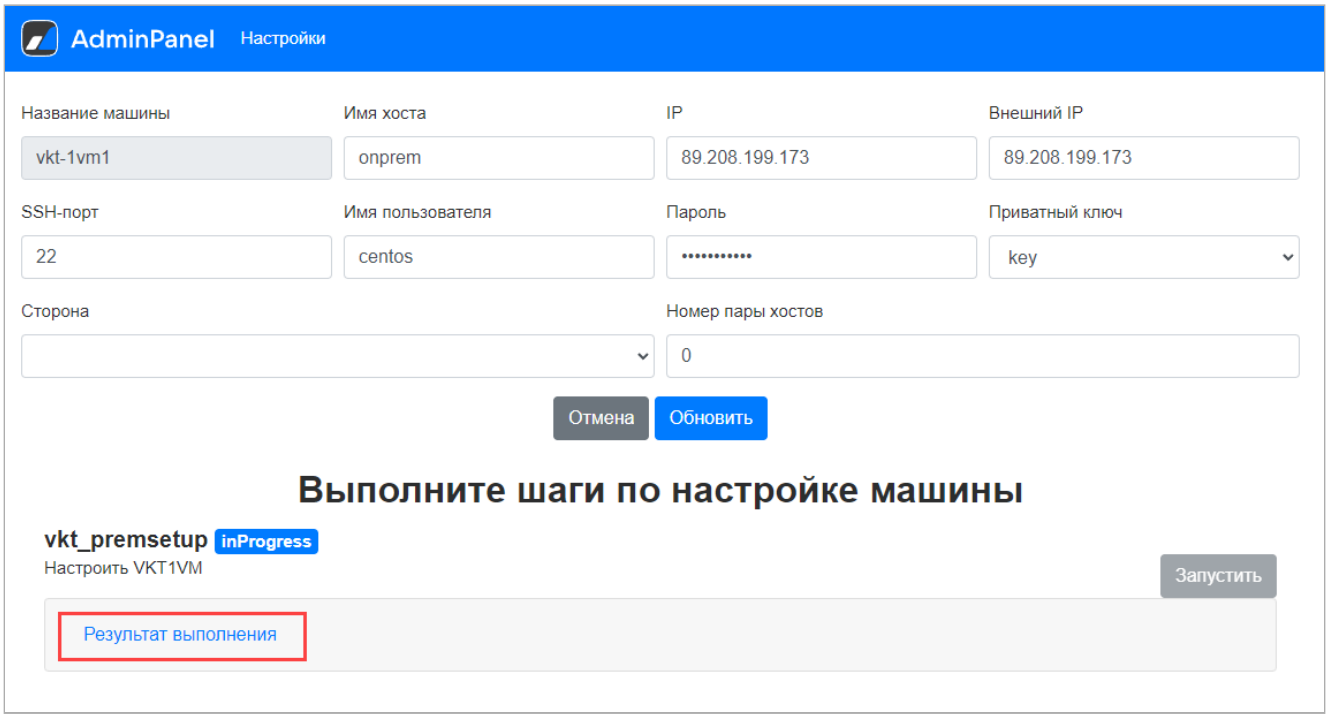


Для просмотра результата выполнения установки:

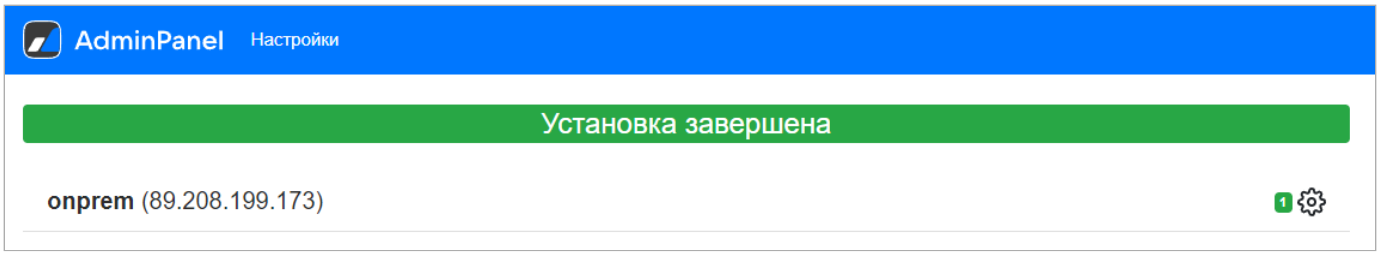
1. Нажмите на пиктограмму  :



2. Нажмите на ссылку **Результат выполнения**:



По окончании процесса инсталляции в строке состояния отображается сообщение **Установка завершена**:



Шаг 15. Рестарт машины

По окончании процесса установки выполните в консоли рестарт машины:

```
reboot
```

На этом установка мессенджера считается завершенной.

По прошествии 30 минут после рестарта машины проверьте результаты выполнения скриптов внутреннего мониторинга системы. Для этого подключитесь к машине по ssh и выполните команды:

```
mon.sh clean
mon.sh
```

После этого проанализируйте вывод команды в соответствии руководством по администрированию, см. раздел Мониторинг параметров сервиса.

Примечание

Отличие скрипта `mon.sh` от приведенного в руководстве по администрированию `/usr/share/check-mk-agent/local/local_check_exec.py` в том, что скрипт `mon.sh` отображает только ошибки, игнорируя успешно выполненные проверки.

Установка VK Teams из консоли

Для установки VK Teams из консоли необходимо выполнить шаги, представленные ниже.

> **Внимание**
>
> Все команды в консоли выполняются под пользователем root.

Шаг 1. Предварительные условия для установки

Перед началом инсталляции убедитесь, что выполнены все предварительные условия (см. раздел Предварительные условия для установки).

Шаг 2. Проверка целостности полученных образов виртуальных машин

Чтобы проверить целостность образов виртуальных машин, в директории со скачанными файлами выполните в командной строке:

Linux

```
md5sum *
```

Windows

```
CertUtil -hashfile myteam.ova MD5
CertUtil -hashfile myteam.qcow2 MD5
CertUtil -hashfile myteam-data.qcow2 MD5
```

macOS

```
md5 *
```

Далее сравните полученное значение с хеш-суммой, указанной в текстовом файле **md5.txt**, распространяемом с дистрибутивом.

Шаг 3. Запуск образа виртуальной машины

Запустите образ виртуальной машины.

Шаг 4. Подключение к виртуальной машине

Подключитесь к виртуальной машине по SSH.

Пользователь: **centos**

Пароль: **djhMRG1vO**

> ⚠ **Внимание**
>
> Чтобы получить пароль для пользователя root, обратитесь в службу технической поддержки.
> После подключения к виртуальной машине пароли для пользователей root и centos необходимо сменить.

macOS или Linux:

```
ssh centos@<VM IP address>
```

Windows: зависит от используемого SSH-клиента.

Шаг 5. Настройка сети

По умолчанию сеть настроена под использование DHCP.

Сконфигурировать сетевой интерфейс **eth0** или **ens160:**

1. В файле **/etc/sysconfig/network-scripts/ifcfg-ens160** указать необходимые параметры (адреса, маску и mac-адрес от конкретной инсталляции):

```
BOOTPROTO=none
DEFROUTE=yes
DEVICE=eth0
GATEWAY=85.192.35.254
HWADDR=fa:16:3e:a4:72:39
IPADDR=85.192.33.158 MTU=1500 NETMASK=255.255.252.0
ONBOOT=yes
STARTMODE=auto
TYPE=Ethernet
USERCTL=no
```

> **Важно**
>
> HWADDR должен совпадать с тем, что отображается у виртуальной машины в веб-интерфейсе виртуализации.

2. Активировать сетевой интерфейс командой:

```
ifup ens160
```

Шаг 6. IP-адрес

Перед началом инсталляции необходимо определить, будет ли доступен сервис в интернете.

Если сервис не будет доступен в интернете, то необходимо использовать внутренний IP-адрес разворачиваемой виртуальной машины.

Если сервис будет доступен в интернете, необходимо использовать внешний IPv4 адрес виртуальной машины. Адрес может быть поднят как внутри виртуальной машины, так и проброшен через NAT. Преобразование сетевых адресов (NAT) должно быть вида 1-в-1 (сеть в сеть), то есть с сохранением номера порта. Иначе видео и голосовые звонки могут не работать.

IP-адрес в дальнейшем будет использоваться для заполнения конфигурационного файла инсталляции.

При использовании внешнего IP-адреса необходимо произвести настройки DNS-зоны (см. Шаг 7. Настройки DNS-зоны).

Шаг 7. Настройки DNS-зоны

Заведите в DNS-зоне имена хостов, которые будут смотреть на внешний IPv4 адрес.

Список имен (CNAME либо A-записи на ваше усмотрение):

- u
- ub
- s
- webim
- api
- admin
- dl
- di
- di-dark
- biz
- call
- calendar
- mobile-calendar
- stentor

Например, для домена vkteams.example.com имя хоста будет выглядеть как u.vkteams.example.com.

Вариант 1.

Если есть возможность создания записи Wildcard CNAME в DNS, то можно создать A-запись, указывающую на адрес сервера VK Teams, и запись Wildcard CNAME, указывающую на A-запись сервера VK Teams.

```
$ host -t axfr example.com | grep vkteams
vkteams.example.com.           3600    IN      A       172.27.59.10
*.vkteams.example.com.         3600    IN      CNAME   vkteams.example.com.
```

Вариант 2.

Если нет возможности создания записи Wildcard CNAME в DNS, то можно создать A-запись, указывающую на адрес сервера VK Teams, и отдельные записи CNAME, которые будут разрешаться на созданную A-запись. Записи CNAME должны соответствовать перечню имен, представленному выше.

```
$ host -t axfr example.com | grep vkteams
vkteams.example.com.                3600  IN     A       172.27.59.10
u.vkteams.example.com.              3600  IN     CNAME   vkteams.example.com.
ub.vkteams.example.com.             3600  IN     CNAME   vkteams.example.com.
s.vkteams.example.com.              3600  IN     CNAME   vkteams.example.com.
di.vkteams.example.com.             3600  IN     CNAME   vkteams.example.com.
webim.vkteams.example.com.          3600  IN     CNAME   vkteams.example.com.
api.vkteams.example.com.            3600  IN     CNAME   vkteams.example.com.
admin.vkteams.example.com.          3600  IN     CNAME   vkteams.example.com.
dl.vkteams.example.com.             3600  IN     CNAME   vkteams.example.com.
di.vkteams.example.com.             3600  IN     CNAME   vkteams.example.com.
di-dark.vkteams.example.com.        3600  IN     CNAME   vkteams.example.com.
call.vkteams.example.com.           3600  IN     CNAME   vkteams.example.com.
calendar.vkteams.example.com.       3600  IN     CNAME   vkteams.example.com.
```

```
mobile-calendar.vkteams.example.com. 3600  IN     CNAME   vkteams.example.com.
biz.vkteams.example.com.             3600  IN     CNAME   vkteams.example.com.
stentor.vkteams.example.com.         3600  IN     CNAME   vkteams.example.com.
```

> **Внимание**
>
> Не вносите изменения в **etc/resolv.conf**. Если изменения всё же необходимо внести, то первым должен быть указан хост 127.0.0.1.

Шаг 8. Выпуск SSL-сертификата

В целях безопасности используется SSL-шифрование, для работы сервера необходимо выпустить SSL-сертификат.

Если Вы используете сертификаты собственного центра сертификации, выпустите сертификат, который далее понадобится при настройке VK Teams (см. Настройки SSL-сертификата). Используйте Wildcard-сертификат, например *.vkteams.EXAMPLE.com, или сертификат с указанием всех необходимых имен (см. раздел Шаг 7. Настройки DNS-зоны).

Для SSL-сертификатов также можно использовать протокол ACME (поддерживается только провайдер Let`s Encrypt). В этом случае получение и продление сертификатов — автоматическое.

Шаг 9. Открыть доступы до внутренних ресурсов

Входящие соединения на стороне сервера VK Teams:

Открыть порты: 80/TCP, 443/TCP, 3478/TCP + UDP, UDP-порты выше 1024.

Исходящие соединения на стороне сервера VK Teams:

- **Открыть доступ для серверов отправки уведомлений**:

  необходимо обеспечить доступ к серверам Google и Apple для отправки и корректной работы push-уведомлений на мобильных платформах Android и iOS.

  Сервер Apple TCP 5223;443;2197.
  IP 17.0.0.0/8
  Статья на сайте apple.com

  Сервер Google TCP 5228;5229;5230;443
  Информация на ipinfo.io
  Статья на сайте google.com

- **Открыть доступ до всех внутренних ресурсов**: LDAP, NTP, SMTP, DNS.

Шаг 10. Настройка LDAP

Система предоставляет возможность указать настройки для соединения с LDAP-сервером во время инсталляции или после ее завершения.

Если инсталляция производится без связи с корпоративным LDAP-сервером или LDAP-сервер отсутствует, пропустите данный шаг и перейдите к Шаг 11. Подготовка конфигурационного файла инсталляции. Описание процесса настройки интеграции с LDAP после инсталляции представлено в документе «Инструкция по интеграции с контроллером домена по протоколу LDAP».

Ниже представлено описание процесса настройки интеграции с LDAP во время инсталляции мессенджера.

Для включения интеграции с LDAP необходимо скопировать в каталог **/usr/local/etc/premsetup/ldap**:

- настройки ваших LDAP-серверов — файлы с расширением ***.yaml**. Название файла может быть произвольным.
- root CA сертификаты ваших LDAP серверов в формате PEM — файлы с расширением ***.pem**. Требуются только для подключения с использованием SSL (протокол ldaps://) и не требуются для подключения без SSL (протокол ldap://).

Далее выполните команды:

```
//установка клиента для подключения к AD
yum install openldap-clients -y

// проверка, что параметры подключения к AD валидны
ldapsearch -H <ldap_url> -w <ldap_password> -x -D
<ldap_bind_dn> -b <ldap_users_dn> mail=ldap-user-email@EXAMPLE.com
```

, где **mail=ldap-user-email@EXAMPLE.com** — почтовый ящик пользователя

Пример настройки LDAP-сервера в ***.yaml**:

```
name: onpremise
config:
  connectionUrl: "ldaps://ad.ad.on-premise.ru:636"
  usersDn: "OU=ad,DC=ad,DC=onpremise,DC=ru"
  bindDn: "CN=VKTeams Syncer,CN=Users,DC=ad,DC=onpremise,DC=ru"
  bindCredential: "PASSWORD"
  searchScope: 1
  fullSyncPeriod: 600
  changedSyncPeriod: -1
```

В случае если одно из полей не заполнено, то устанавливается значение по умолчанию для сервиса Keycloak. Основные доступные поля:

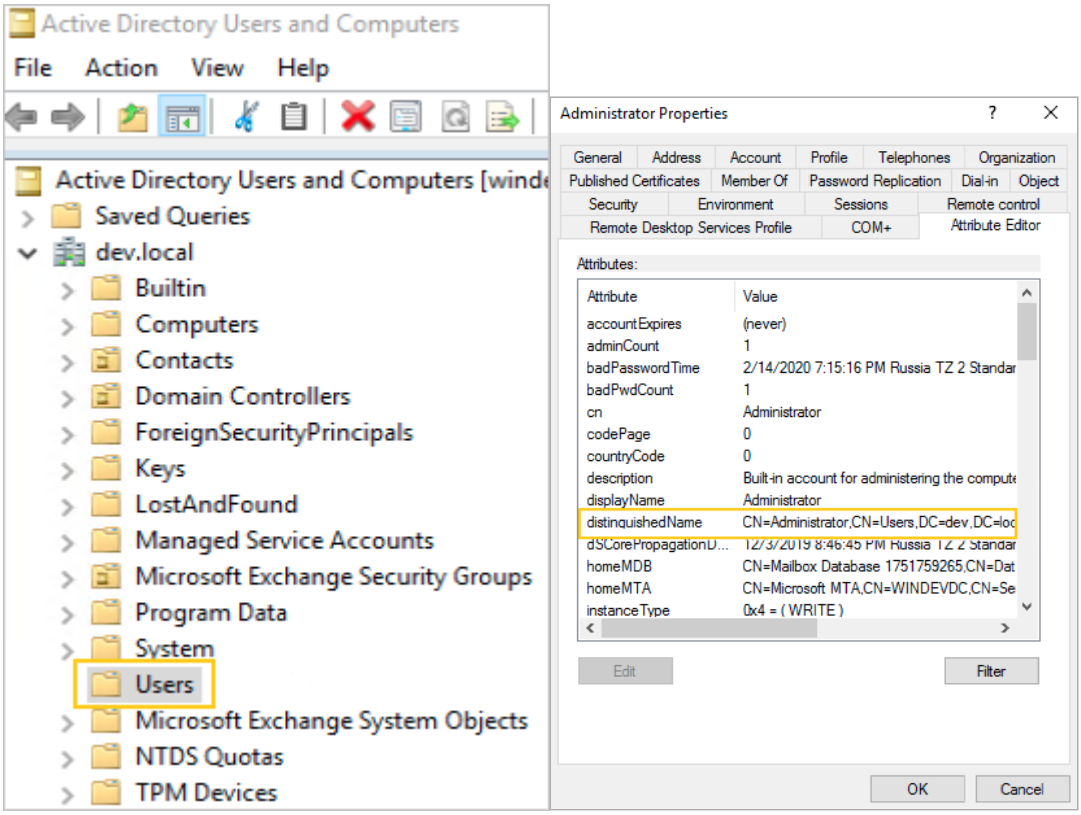
- **name** — имя LDAP-сервера. Данное имя уникально, может быть заведен только один сервер с определенным именем.
- **connectionUrl** — адрес подключения к LDAP-серверу.
- **usersDn** — указание на точку входа для поиска в LDAP.

- **bindDn** — пользователь, под которым осуществляется подключение к LDAP-серверу.
- **bindCredential** — пароль для подключения к LDAP-серверу.
- **searchScope** — использование рекурсивного поиска по дереву LDAP:
  - 1 — искать в одном уровне (по умолчанию).
  - 2 — искать по всем уровням.
- **fullSyncPeriod** — частота полной синхронизации с LDAP-сервером, в секундах.
- **changedSyncPeriod** — частота частичной синхронизации с LDAP-сервером, в секундах (значение **-1** — отключить).
- **batchSizeForSync** — максимальное количество пользователей, обновляемых одной транзакцией. Изменяйте в случае, если ваш LDAP-сервер отказывается отдавать пользователей с ошибкой о превышении размера транзакции.
- **customUserSearchFilter** — фильтр для получения пользователей. Позволяет получать не всех пользователей из указанного дерева. По умолчанию выборка пользователей не ограничена.

Как получить Distinguished Name для bindDN и usersDN в Active Directory

1. В оснастке **Active Directory Users and Computers** выберите пользователя, под которым будет происходить подключение и поиск пользователей;
2. Выберите свойства и перейдите на вкладку **Attribute Editor** (если вкладки нет, выберите в меню **View**, затем **Advanced Features**).

   На вкладке будет отображено значение **distinguishedName**. Повторите операцию, чтобы получить **distinguishedName** для каталога, в котором будет выполняться поиск пользователей.



Шаг 11. Подготовка конфигурационного файла инсталляции

Настройки сервера VK Teams расположены в файле **/usr/local/etc/premsetup/defaults.yaml**.

Все настройки задокументированы внутри файла. Необходимо удалить дефолтные значения и указать параметры Вашей инсталляции.

> **Примечание**
>
> Изменения необходимо вносить под учетной записью root.

```
sudo su
vi /usr/local/etc/premsetup/defaults.yaml
```

Нажать клавишу клавиатуры **I** для перехода в режим вставки и указать параметры инсталляции. Ниже приведено более подробное описание каждого пункта конфигурации.

Список серверов точного времени (NTP)

Укажите список NTP-серверов (IP-адреса или имена хостов) в виде массива имен или IP-адресов серверов точного времени.

Тип — Массив строк

Пример:

```
ntp: [ '0.pool.ntp.org', '1.pool.ntp.org' ]
```

или

```
ntp:
  - 0.pool.ntp.org
  - 1.pool.ntp.org
```

Список DNS-серверов

Укажите список DNS-серверов (IP-адреса серверов, которые будут использованы для разрешения имен).

Тип — Массив строк

Пример:

```
dns: [ '8.8.8.8', '1.1.1.1']
```

или

```
dns:
  -'1.1.1.1'
  -'8.8.8.8'
```

Настройка SMTP-сервера

Чтобы настроить OTP via email, укажите:

- Имя или IP-адрес SMTP-сервера:

  Тип — Строка

  Пример:

  ```
  smtp_server: '127.0.0.1'
  ```

- Порт SMTP-сервера. Как правило, не требует редактирования:

  Тип — Строка

  Пример:

  ```
  smtp_port: '25'
  ```

- Обратный адрес для сообщений с OTP-кодами (поле **«From:»** в письме). Рекомендуется использовать реально существующий адрес:

  Тип — Строка

  Пример:

  ```
  smtp_from:  'otp@vkteams.EXAMPLE.com'
  ```

Настройка SSO-аутентификации

Если в дальнейшем планируется настройка SSO-аутентификации по протоколу SAML, установите в секции **saml_enabled:** значение **True**.

Тип — Булевый

Пример:

```
saml_enabled: True
```

Доменное имя сервера VK Teams

Для настройки сервера VK Teams укажите базовый домен. Например, vkteams.example.com означает, что клиентские приложения будут пытаться получить доступ к сайтам u.vkteams.example.com, ub.vkteams.example.com и т. д.

Тип — Строка

Пример:

```
domain: 'vkteams.EXAMPLE.com'
```

IP-адрес

Укажите внешний или внутренний IP-адрес, присвоенный на шаге Шаг 6. IP-адрес.

Внешний IP-адрес должен быть проброшен внутрь виртуальной машины. Без его указания будут некорректно работать голосовые и видео-шлюзы.

Тип — Строка

Пример:

```
ext_ip: '172.27.59.10'
```

Настройка сервиса записи звонков

Данный параметр контролирует сервис записи звонков. При его включении звонки будут записываться, готовая запись будет отправлена пользователю в личные сообщения с помощью бота (Recorderbot). На данный момент, запись доступна только в Desktop приложениях. По умолчанию запись включена.

Тип — Булевый

Пример:

```
call-recording-enabled: True
```

, где:

- флаг **True** — включает запись звонка;
- флаг **False** — выключает запись.

Настройки SSL-сертификата

Укажите SSL-сертификат, выпущенный на шаге 8 (см. Шаг 8. Выпуск SSL-сертификата).

- **ssl_key:''** — приватный ключ для SSL-сертификата. Указывается в формате PEM и не должен быть защищен паролем. Приватный ключ необходимо указать полностью, включая `-----BEGIN RSA PRIVATE KEY-----` и `-----END RSA PRIVATE KEY-----`;
- **ssl_cert:''** — SSL-сертификат сервера в формате PEM. Для корректной работы укажите всю цепочку сертификатов (full chain). SSL-сертификаты необходимо указать полностью, включая `-----BEGIN RSA PRIVATE KEY-----` и `-----END RSA PRIVATE KEY-----`;
- **verify_ssl** — способ проверки SSL-сертификата. Возможные значения: True, False, путь до файла .ca_bundle:
  - True — проверять сертификат с центрами сертификации (CA), встроенными в ОС (по умолчанию).
  - False — не проверять SSL-сертификат, например в случае использования самоподписанного сертификата.
  - Путь до **.ca_bundle** — использовать свой центр сертификации для проверки сертификата.
- **self_signed_cert** — если планируется добавлять самоподписанные сертификаты, то необходимо добавить этот флаг со значением True. По умолчанию значение False, а флага нет в файле **defaults.yaml**. Флаг нужно добавить самостоятельно и только в случае использования самоподписанных сертификатов.

> **Внимание**
>
> Обязательно указание вертикальной черты **|** после переменной и четырех пробелов в начале строк (см. пример ниже).

Тип — Многострочные переменные

Пример:

```
ssl_key: |
    -----BEGIN PRIVATE KEY-----
    your private key could be here
    -----END PRIVATE KEY-----
ssl_cert: |
    -----BEGIN CERTIFICATE-----
    First certificate in chain
    -----END CERTIFICATE-----
    -----BEGIN CERTIFICATE-----
    Second certificate in chain
    -----END CERTIFICATE-----
```

Протокол ACME (Let`s Encrypt) для SSL-сертификатов

Переменные **ssl_key** и **ssl_cert** можно не заполнять, при включении сертификатов через ACME они игнорируются.

Настройки для управления ACME:

- **ssl_acme_enabled** — установите True, чтобы использовать протокол ACME (**ssl_key** и **ssl_cert** игнорируются). По умолчанию установлено False (ACME не используется).
- **ssl_acme_email** (строка) — почта, используемая при обращении к Let's Encrypt. На эту почту будут поступать уведомления от сервиса Let's Encrypt. Обязательный параметр, без корректной почты сертификаты выданы не будут.
- **use_default_domain** — включает получение SSL-сертификата через ACME для домена, указанного в переменной **domain** файла **defaults.yaml**. Если в DNS нет записи, которая позволяет разрешить имя домена на внешний IP-адрес, этот параметр нужно выключить (False). По умолчанию сертификат будет выпускаться (True).

Внимание

Включение этой опции и использование указанной функциональности означает согласие с условиями использования, с которыми можно ознакомиться по адресу https://letsencrypt.org/repository/

Тип — Булевый/строка

Пример:

```
// использовать сертификаты от Let's Encrypt:
ssl_key: ''
ssl_cert: ''
ssl_acme_enabled: true
ssl_acme_email: ssl@vkteams.EXAMPLE.com

// использовать ssl_key / ssl_cert (вариант по умолчанию):
ssl_acme_enabled: false
ssl_key: |
    -----BEGIN PRIVATE KEY-----
    your private key could be here
    -----END PRIVATE KEY-----
ssl_cert: |
    -----BEGIN CERTIFICATE-----
    First certificate in chain
    -----END CERTIFICATE-----
    -----BEGIN CERTIFICATE-----
    Second certificate in chain
    -----END CERTIFICATE-----
```

Примечание

Сертификат продлевается автоматически каждые 3 месяца, поэтому 80-й порт должен быть открыт — иначе сертификат не обновится.

Установка разрешений для пользователей

Чтобы разрешить пользователям изменять информацию о себе в профиле мессенджера, установите значение **True** в следующих секциях:

- Разрешить изменение аватара:

  Тип — Булевый

  Пример:

  ```
  allow_self_avatar_change:  True
  ```

- Разрешить изменение имени и фамилии:

  Тип — Булевый

  Пример:

  ```
  allow_self_name_change: True
  ```

- Разрешить внесение изменений в раздел «О себе»:

  Тип — Булевый

  Пример:

  ```
  allow_self_info_change: True
  ```

Чтобы разрешить удаление отправленного сообщения в личных чатах/группах без уведомления участников, установите значение **True** в секции **silent_message_delete**.

Тип — Булевый

Пример:

```
silent_message_delete: True
```

Настройка окружения администратора

Интерфейс администратора доступен только с выбранных IP-адресов и только выбранным пользователям. Также предусмотрена настройка ограничения доступа к выбранным разделам окружения администратора (например, к выгрузке чатов).

По умолчанию окружение администратора доступно с IP-адресов приватных сетей (10.0.0.0/8, 172.16.0.0/12 и 192.168.0.0/16).

Доступ в окружение администратора настраивается через группы.

Изначально перечень групп с доступом в окружение администратора пуст, потому окружение недоступно никому. Управление доступом по группам осуществляется через параметр **otp_permission**, который управляет настройками OTP-авторизации для разных сценариев.

Если настройки для соединения с LDAP-сервером производятся **во время инсталляции** — для параметра **otp_permission** необходимо указать заранее подготовленное наименование группы из LDAP, в которую будут входить пользователи с доступом в окружение администратора (см. раздел LDAP в предусловиях).

Если инсталляция производится без связи с корпоративным LDAP-сервером — укажите для параметра **otp_permission** наименование группы из LDAP, в которую будут входить пользователи с доступом в окружение администратора (см. раздел LDAP в предусловиях). Информация по управлению параметрами синхронизации LDAP после инсталляции мессенджера представлена в документе «Инструкция по интеграции с контроллером домена по протоколу LDAP».

При отсутствии LDAP — укажите для параметра **otp_permission** наименование группы, которое будете использовать при создании пользователей в системе вручную после окончания процесса инсталляции (описание процесса представлено в документе «Руководство по администрированию»).

Тип — Словарь строка → Массив строк

Пример:

```
// окружение администратора  доступно всем пользователям:
otp_permission: {}

// окружение администратора  недоступно никому (значение по умолчанию):
otp_permission:
  myteam-admin: []

// окружение администратора доступно группе myteam-admin в LDAP  (через distinguished name,
подробнее про получение distinguished name из AD см. в разделе "Как получить Distinguished
Name для bindDN и usersDN в Active Directory" выше):
otp_permission:
  myteam-admin:
    - 'CN=myteam-admin,OU=HQ,DC=dev,DC=local'

// окружение администратора  доступно группе myteam-admin без LDAP:
otp_permission:
  myteam-admin:
    - 'myteam-admin'
```

Управление доступом по группам к выбранным компонентам осуществляется через параметры **myteam_admin_permissions** и **myteam_admin_default_permissions**.

Перечень доступных компонентов:

- **Information** — информация о системе, документация.
- **Analytics** — информация о состоянии системы, графики и аналитика.
- **Export** — выгрузка участников групп.

Параметр **myteam_admin_default_permissions** определяет правило доступа к компоненту по умолчанию, а параметр **myteam_admin_permissions** позволяет разграничить доступ на уровне групп в LDAP.

По умолчанию доступ к компонентам **Information** (раздел «Информация») и **Analytics** (раздел «Аналитика») имеют все пользователи с доступом к окружению администратора. К компоненту **Export** (раздел «Выгрузка») доступа нет ни у кого.

Тип — Массив строк

Пример:

```
// компоненты Information и Analytics доступны всем, Export — никому (значение по умолчанию):
myteam_admin_default_permissions:
myteam_admin_permissions:

// компоненты Information и  Analytics доступны всем, а Export — группе myteam-admin-export в
LDAP (через distinguished name, подробнее см. в разделе "Как получить Distinguished Name для
bindDN и usersDN в Active Directory" выше):
myteam_admin_default_permissions:
myteam_admin_permissions:
  Export:
    - 'CN=myteam-admin-export,OU=HQ,DC=dev,DC=local'

// компоненты Information и  Export доступны всем, а Analytics — группе myteam-admin-analytics
без LDAP:
myteam_admin_default_permissions:
  Export: allow
  Analytics: deny
myteam_admin_permissions:
  Analytics:
    - 'myteam-admin-analytics'
```

Управление доступом на уровне IP осуществляется через параметр **myteam_admin_acl**. По умолчанию доступ предоставляется из подсетей rfc1918 (10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16) и 127.0.0.0/8.

Тип — Массив строк

Пример:

```
// окружение администратора недоступно ни с одного IP-адреса:
myteam_admin_acl: []

// окружение администратора доступно для подсетей rfc1918 и 127.0.0.0/8 (значение по
умолчанию):
myteam_admin_acl:

// окружение администратора доступно с адреса 1.1.1.1 и 10.11.12.0/24:
myteam_admin_acl:
  - '1.1.1.1'
  - '10.11.12.0/24'
```

Настройка обратной связи

По умолчанию все обращения пользователей поступают на адрес myteamsupport@USER-DOMAIN, через локальный SMTP-релей. Например, в случае домена **example.com** обращение поступит на адрес **myteamsupport@example.com**.

Базовые настройки сервиса:

В полях **from** и **rcpt_to** в адреса, оканчивающиеся символом @, автоматически подставляется домен пользователя.

```
feedback_config:
  from: "myteamsupport@"
  rcpt_to: ["myteamsupport@"]
  subject: "VK Teams Feedback"
```

Параметр	Тип	Описание	Примеры
from	Строка	Обратный адрес для письма, формируемого системой в адрес технической поддержки	• test@ — обратный адрес будет test@USER-DOMAIN • test@example.com — обратный адрес будет test@example.com, независимо от домена пользователя
rcpt_to	Массив	Адрес получателей. Получателей может быть несколько	• ['test@'] — получателем письма будет test@USER-DOMAIN • ['test@', 'example@example.com'] — получателями письма будут test@USER-DOMAIN и example@example.com
subject	Строка	Тема отправляемого письма	

Расширенные настройки сервиса:

Используйте расширенные настройки, если хотите отправлять обращения пользователей через отдельный SMTP-сервер с использованием авторизации.

```
feedback_config:
  host: "localhost"
  port: 25
  username: ""
  password: ""
  use_tls: false
  from: "myteamsupport@"   # myteamsupport@external_domain
  rcpt_to: ["myteamsupport@"]   # myteamsupport@external_domain
  subject: "Myteam Feedback"
```

Параметр	Тип	Описание	Значение / настройка по умолчанию
host	Строка	Адрес SMTP-сервера	localhost
port	Int	Порт SMTP-сервера	25

Параметр	Тип	Описание	Значение / настройка по умолчанию
username	Строка	Имя пользователя для авторизации на SMTP-сервере	без авторизации
password	Строка	Пароль для авторизации на SMTP-сервере	без авторизации
use_tls	Boolean	Форсировать использование TLS для SMTP-сервера	выключено

Примечание

По окончании заполнения конфигурационного файла инсталляции необходимо последовательно нажать **Esc :wq Enter** для сохранения внесенных изменений.

Шаг 12. Инициализация сервисов

После заполнения конфигурационного файла инсталляции необходимо произвести инициализацию сервисов VK Teams.

Для инициализации всех сервисов выполните команду:

```
premsetup.py --init
```

Шаг 13. Проверка конфигурационного файла на ошибки

Чтобы проверить конфигурационный файл инсталляции **/usr/local/etc/premsetup/defaults.yaml** на ошибки, выполните команду:

```
premsetup.py -t
```

Данная команда позволяет проверить, верно ли указаны настройки системы. Если открыты не все нужные порты, либо нет интеграции с базовым набором сервисов (DNS, SMTP, NTP), в консоли отобразится уведомление о необходимости правок.

Шаг 14. Запуск скрипта конфигурации

Чтобы запустить скрипт конфигурации сервера VK Teams, выполните команду:

```
premsetup.py
```

Если скрипт отработал без ошибок, в результатах выполнения отобразится список установленных модулей и сообщение в консоли `all is fine`.

Шаг 15. Рестарт машины

Далее выполните рестарт виртуальной машины командой:

```
reboot
```

На этом установка мессенджера считается завершенной.

По прошествии 30 минут после рестарта машины проверьте результаты выполнения скриптов внутреннего мониторинга системы. Для этого подключитесь к машине по ssh и выполните команды:

```
mon.sh clean
mon.sh
```

После этого проанализируйте вывод команды в соответствии руководством по администрированию, см. раздел Мониторинг параметров сервиса.

> **Примечание**
>
> Отличие скрипта `mon.sh` от приведенного в руководстве по администрированию `/usr/share/check-mk-agent/local/local_check_exec.py` в том, что скрипт `mon.sh` отображает только ошибки, игнорируя успешно выполненные проверки.

Шаг 16. Проверка готовности сервисов

После перезагрузки виртуальной машины необходимо проверить готовность сервисов командой:

```
ic srvs
```

Если все сервисы находятся в статусе alive, можно переходить в веб-интерфейс мессенджера. Установка мессенджера считается завершенной.

Когда все сервисы находятся в статусе alive, можно дополнительно вывести в консоль список подов командой:

```
kubectl get pods -A
```

Повторный запуск конфигуратора

Конфигуратор возможно запускать повторно в случае возникновения ошибок во время инсталляции или при обновлении дистрибутива.

Однако при повторном запуске нужно учитывать некоторые особенности — они определяются флагами, создаваемыми командой `premsetup.py --install` при первом запуске:

- **/var/tmp/premsetup.run** — удалите этот флаг, после чего команду `premsetup.py --install` можно запустить снова.
- **/mnt/data/premsetup/flags/premsetup.run** — при наличии этого флага команда `premsetup.py --install` не будет изменять настройки LDAP, однако будет изменять остальные настройки. Это предотвращает поломку системы синхронизации пользователей, в случае если изменения вносились через веб-интерфейс.

Внесение изменений в настройки инсталляции

Если необходимо внести изменения в конфигурацию:

1. Подключитесь к виртуальной машине (шаг 4).
2. Внесите необходимые изменения в настройки сети, LDAP, DNS, открытые доступы и/или конфигурационный файл инсталляции (шаги 5-11).
3. Выполните проверку конфигурации на ошибки и запустите скрипт конфигурации (шаги 13-14).

> **Примечание**
>
> Инициализацию сервисов VK Teams (шаг 12) производить не надо.

4. Перезагрузить виртуальную машину и проверьте готовность сервисов VK Teams (шаги 15-16).

Дата обновления документа: 18.04.2024 г.