

# Корпоративный мессенджер VK Teams

Инструкция по установке кластера VK Teams  
(версия 24.11)

# Оглавление

---

Назначение документа	4
Дополнительная документация	4
Архитектура кластера	5
Обязательные компоненты	5
Опциональные компоненты	6
Описание дистрибутива	7
Предварительные условия для установки	8
Роутинг исходящих соединений	8
SMTP-сервер	8
NTP-серверы	8
Исходящие соединения на стороне клиента	8
LDAP	8
Требования к L7-балансировщику	9
Установка кластера без DMZ	10
Шаг 1. Предварительные условия для установки	10
Шаг 2. Проверка целостности полученных образов виртуальных машин	10
Шаг 3. Создание виртуальной машины	11
Шаг 4. Запуск образа виртуальной машины	11
Шаг 5. Подключение к виртуальной машине	11
Шаг 6. Генерация SSH-ключа для установщика	11
Шаг 7. IP-адрес	12
Шаг 8. Настройки DNS-зоны	12
Шаг 9. Выпуск SSL-сертификата	13
Шаг 10. Открыть доступы до внутренних ресурсов	14
Шаг 11. Запуск установщика	14
Шаг 12. Добавление сервера в установщик	14
Шаг 13. Настройки VK Teams	17
Домен пользователя	18
Внутренний домен	18

Список DNS-серверов	19
Список серверов точного времени (NTP)	19
Настройка SMTP-сервера	19
Настройка сервиса записи звонков	20
Настройка SSO-аутентификации	20
Установка разрешений для пользователей	20
Кластерные настройки	21
Настройки DMZ	21
Настройки SSL-сертификата	22
Настройка окружения администратора	24
Настройка обратной связи	26
Настройка LDAP	27
Шаг 14. Проверка конфигурации	31
Шаг 15. Запуск установки	32
Установка кластера с DMZ	34
Проверки после инсталляции	37

# Назначение документа

---

В данной инструкции представлено описание процессов кластерной установки VK Teams:

- [Установка кластера без DMZ](#)
- [Установка кластера с DMZ](#)

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.

[Руководство по администрированию VK Teams](#) — в документе описано управление пользователями без контроллера домена.

**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**

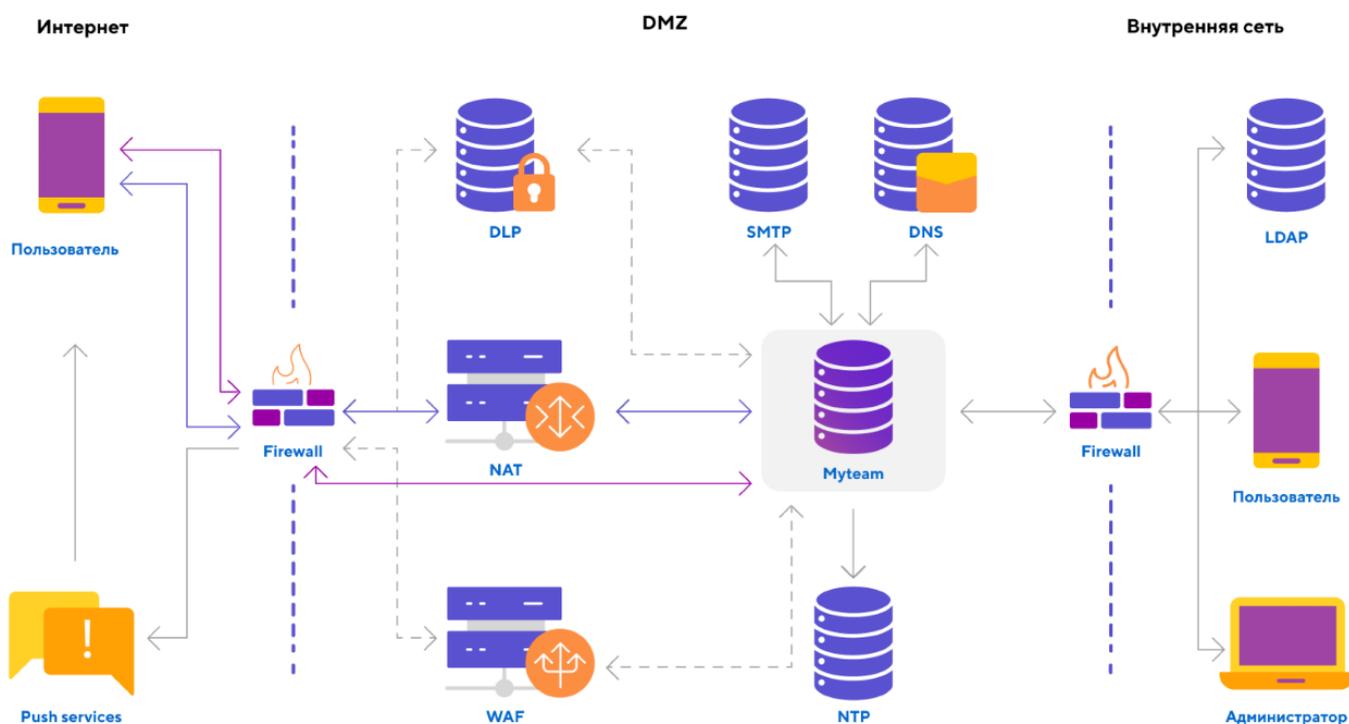
Ранее VK Teams назывался Myteam, что находит отражение в технических моментах (например, команды в консоли).

# Архитектура кластера

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).

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

Как правило, кластер 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 выше 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

---

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

## Системные требования:

В случае кластерной инсталляции требования к предоставляемым вычислительным ресурсам (виртуальным машинам) для продуктивной среды рассчитываются индивидуально для Заказчика. Свяжитесь с представителями VK Teams для помощи с расчетом сайзинга.

- **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 — 10 Мбит/с; UDP — 10 Мбит/с.

## Совместимость:

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

# 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 VK Teams 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 VK Teams 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](#)).

## Требования к L7-балансировщику

Данные требования актуальны как для DMZ, так и для стандартного кластера.

Балансировщик должен проставлять следующие заголовки при проксировании запросов в VK Teams:

- X-Real-IP — в этот заголовок должен записываться IP-адрес, откуда пришел запрос.
- X-CUSTOM-SSL-OFFLOAD и X-SSL-OFFLOAD — в эти заголовки должно записываться значение **1**. Эти заголовки сигнализируют о том, что балансировщик завершает SSL.

При использовании L7-балансировки необходимо ограничивать на уровне сети доступ к виртуальным машинам VK Teams напрямую.

# Установка кластера без DMZ

Процесс установки кластера 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 кластера 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. Создание виртуальной машины

Создайте виртуальную машину на основе предоставленных образов.

При создании виртуальной машины с предоставленного образа (root), необходимо создать и подключить новый пустой раздел data для хранения данных, генерируемых при работе системы. При обновлении версии дистрибутива, раздел root будет пересоздаваться из нового образа, раздел data — переноситься с рабочего экземпляра.

## Шаг 4. Запуск образа виртуальной машины

Запустите образ виртуальной машины.

## Шаг 5. 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 6. 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 7. 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.

## Шаг 8. 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` — адрес клиентского API VK Teams.
- `ub` — файловое API.
- `s` — обмен стикерпаками.
- `webim` — веб-версия VK Teams.
- `api` — API бота.
- `admin` — адрес API управления VK Teams (административного веб интерфейса).
- `dl` — портал загрузки дистрибутивов (система автоматического обновления клиентских приложений).
- `kc` — поддомен сервиса Keycloak.
- `biz` — адрес сервера VK Teams, где находится сервис Grafana.
- `call` — URL для формирования ссылок на звонки.
- `calendar` — API календаря. Работает только в интеграции с Почтой VK WorkSpace.
- `mobile-calendar` — API мобильного календаря. Работает только в интеграции с Почтой VK WorkSpace.
- `stentor` — адрес API VK Teams для добавления/удаления пользователей.
- `files-n` — оргструктура организаций.

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.
kc.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.
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.
files-n.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 9. 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 [Настройки DNS-зоны](#)).

## Шаг 10. 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](#)

Если в вашей организации используются механизмы ограничения доступа сетевого трафика, убедитесь, что открыт доступ к следующим доменам (по HTTPS, порт 443):

fcm.googleapis.com

www.googleapis.com

oauth2.googleapis.com

accounts.google.com

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

## Шаг 11. 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 12. Добавление сервера в установщик

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

Добавить ▾

Сервер

На отобразившейся форме добавления сервера заполните поля:

Роль	Имя хоста	IP	Внешний IP
vkt-cluster (6) ▾	vkt01	10.10.70.37	10.10.70.37
SSH-порт	Имя пользователя	Пароль	Приватный ключ
22	centos	••••••••	vkt_key ▾
Сторона	Номер пары хостов		
a ▾	1		

#### Обязательные к заполнению поля:

- **Роль** — для установки кластера VK Teams нужно выбрать **vkt-cluster**.
- **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 [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.

- **Приватный ключ** — ключ для доступа установщика к серверу VK Teams. Выберите в выпадающем списке поля **+ Добавить новый ключ**. В отобразившейся форме заполните поля:

### Добавление приватного ключа

Имя ключа:

Приватный ключ: 

```
-----BEGIN RSA PRIVATE KEY-----

-----END RSA PRIVATE KEY-----
```

Пароль ключа:

Использовать по умолчанию

Отмена
Сохранить

В поле **Приватный ключ** необходимо скопировать содержимое приватной части SSH-ключа, созданного на шаге выше (см. раздел [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 создан — поле не заполнять). Нажмите на кнопку **Сохранить**.

Топология кластера VK Teams состоит из пар хостов. Внутри каждой пары происходит резервирование сервисов.

- **Сторона** — в каждой паре есть сторона **a** и сторона **b**. Например, для первого хоста в паре сторона будет **a**, а для второго — **b**. И так для каждой пары;
- **Номер пары хостов** — номер пары в топологии. Например, для первых двух хостов это будет 1, для второй пары — 2, и т.д.

Пример топологии кластера из 4 хостов (2 шарда):



Пример топологии кластера из 6 хостов (3 шарда):

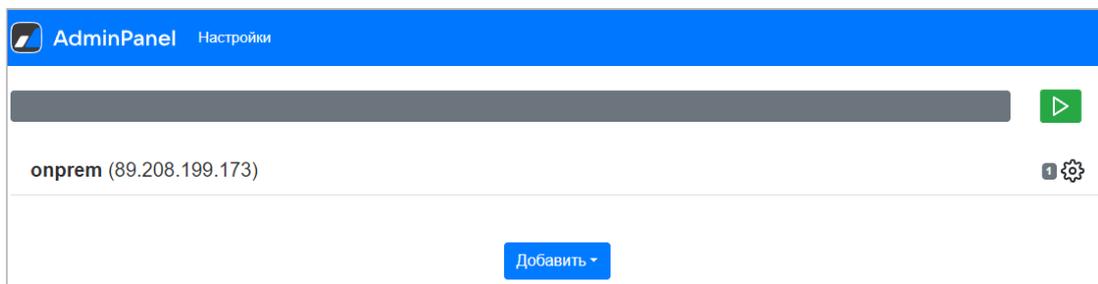


Пример топологии кластера из 10 хостов (5 шардов):



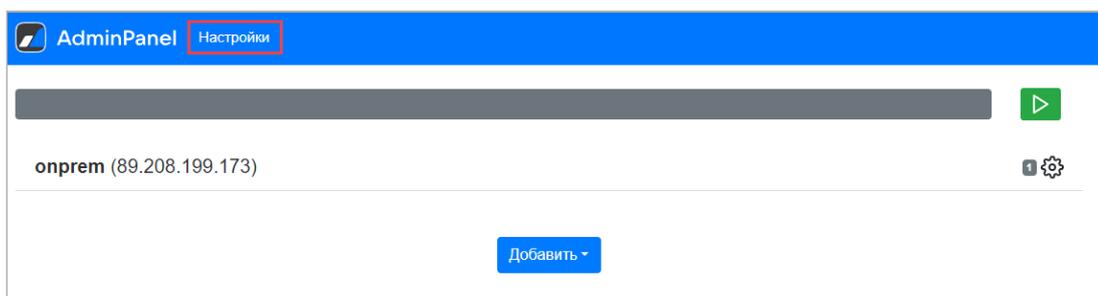
После заполнения полей на форме добавления сервера нажмите на кнопку **Добавить**.

Добавленный сервер отобразится в панели установщика:

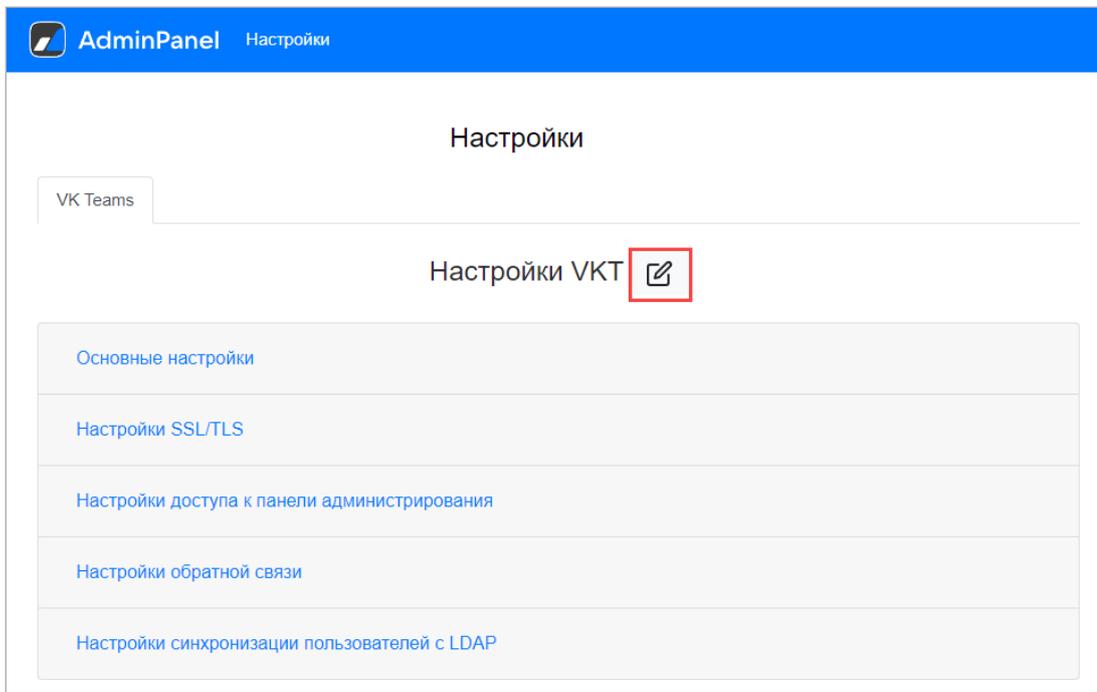


## Шаг 13. Настройки VK Teams

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



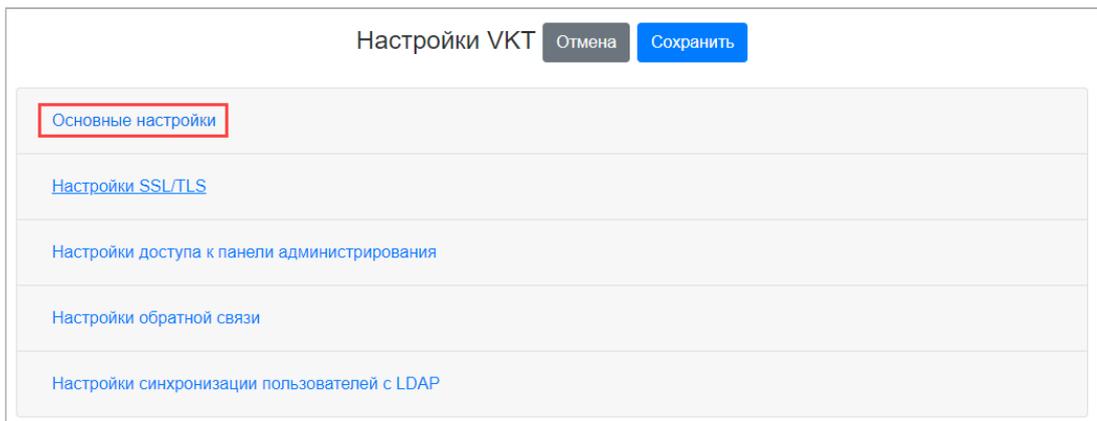
На отобразившейся странице нажмите на пиктограмму , чтобы перейти в режим редактирования:



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.

Внешний домен VK Teams:

## Внутренний домен

Укажите домен, в котором расположены все серверы VK Teams.

Например, для кластера, состоящего из серверов vkt01.novalocal, vkt02.novalocal, vkt03.novalocal, vkt04.novalocal, значение внутреннего домена будет novalocal.

Команда `hostname` на каждом сервере должна выдавать значение <имя хоста>.<внутренний домен>.

Внутренний домен:	novalocal
-------------------	-----------

## Список DNS-серверов

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

Список DNS серверов:	
8.8.8.8	—
8.8.4.4	—
<a href="#">+ Добавить</a>	

## Список серверов точного времени (NTP)

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

Список NTP серверов:	
0.pool.ntp.org	—
1.pool.ntp.org	—
<a href="#">+ Добавить</a>	

## 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.

Адрес почтового сервера (SMTP relay):

Порт почтового сервера (SMTP relay port):

From: адрес для исходящих почтовых сообщений:

## 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.

На данный момент запись доступна только в десктоп-приложениях. По умолчанию запись включена.

Включить сервис записи звонков:

## Настройка SSO-аутентификации

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

Будет ли использоваться авторизация SAML в ADFS:

## Установка разрешений для пользователей

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

Разрешить изменение аватара пользователем:

Разрешить изменение Имени и Фамилии пользователем:

Разрешить смену раздела About me пользователем:

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

Разрешить 'тихое удаление':

# Кластерные настройки

Далее перейдите в раздел **Кластерные настройки**:

Настройки VKT Отмена Сохранить

- Основные настройки
- Кластерные настройки**
- Настройки DMZ
- Настройки SSL/TLS
- Настройки доступа к панели администрирования
- Настройки обратной связи
- Настройки синхронизации пользователей с LDAP

Эти настройки применимы как к схеме с DMZ, так и к стандартному кластеру.

Список IP адресов балансировщика:  —  
 —  
[+ Добавить](#)

Заголовок с клиентским IP адресом:

- **Список IP-адресов балансировщика** — укажите список IP-адресов, с которых приходят запросы от балансировщика на DMZ или стандартный кластер.
- **Заголовок с клиентским IP-адресом** — укажите HTTP-заголовок, куда балансировщик будет записывать оригинальный IP-адрес клиентского запроса.

## Настройки DMZ

Перейдите в раздел **Настройки DMZ**:

Настройки VKT Отмена Сохранить

- Основные настройки
- Кластерные настройки
- Настройки DMZ
- Настройки SSL/TLS
- Настройки доступа к панели администрирования
- Настройки обратной связи
- Настройки синхронизации пользователей с LDAP

Если кластер устанавливается без размещения части серверов в DMZ, укажите для поля **Тип установки** значение **Не использовать DMZ**:

Тип установки:	<input type="text" value="Не использовать DMZ"/>
Порт контроллера IPROS:	<input type="text" value="2410"/>
Список адресов IPROS контроллера:	<a href="#">+ Добавить</a>
Список IP адресов внутренней инсталляции:	<a href="#">+ Добавить</a>
Список IP адресов DMZ:	<a href="#">+ Добавить</a>

#### **Примечание**

Существует возможность терминировать входящие соединения от клиентских приложений в отдельной сети. При такой схеме параллельно работают две независимые инсталляции VK Teams, которые связаны строго определенными сетевыми доступами. Подробнее об установке кластера с DMZ [см. ниже](#).

## Настройки SSL-сертификата

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



Способ проверки SSL сертификата:

True

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.

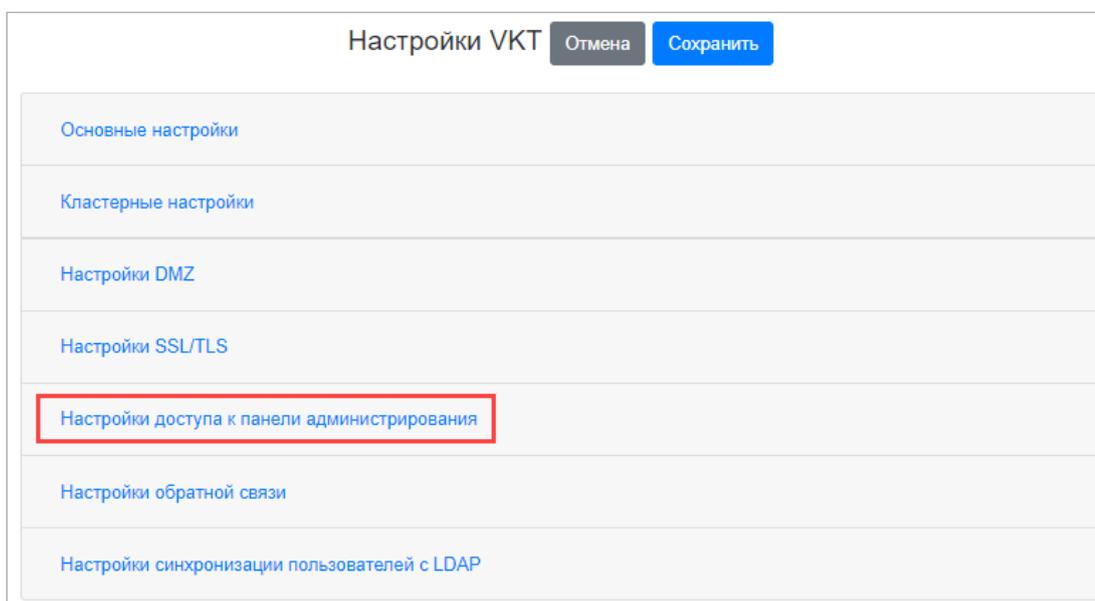
4. Если планируется добавлять самоподписанные сертификаты, установите соответствующий переключатель:

Использовать самоподписанные сертификаты:



## 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 частных сетей (10.0.0.0/8, 172.16.0.0/12 и 192.168.0.0/16).

Список подсетей и IP адресов, с которых будет разрешен доступ к окружению администратора:

10.0.0.0/8	—
172.16.0.0/12	—
192.168.0.0/16	—
127.0.0.0/8	—

[+ Добавить](#)

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):

Список LDAP групп доступа к панели администрирования:

myteam-admin	—
--------------	---

[+ Добавить](#)

Если инсталляция производится без связи с корпоративным LDAP-сервером, укажите в поле поле 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 VK Teams представлена в документе [Инструкция по интеграции с контроллером домена по протоколу LDAP](#).

При отсутствии LDAP — укажите в поле наименование группы, которое будете использовать при создании пользователей в системе вручную после окончания процесса инсталляции (описание процесса представлено в документе [Руководство по администрированию](#)).

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

Доступ к информации в панели администрирования:

deny
------

Доступ к аналитике в панели администрирования:

CN=myteam-admin-export,OU=HQ,DC=dev,DC=local
--

Доступ к экспорту в панели администрирования:

deny
------

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**:

Настройки VKT Отмена Сохранить

- Основные настройки
- Кластерные настройки
- Настройки DMZ
- Настройки SSL/TLS
- Настройки доступа к панели администрирования
- Настройки обратной связи**
- Настройки синхронизации пользователей с LDAP

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**.

Обратный адрес для писем:

Адрес получателя:

 —  
[+ Добавить](#)  

Тема письма:

Адрес SMTP сервера:

Порт SMTP сервера:

Имя пользователя для SMTP авторизации:

Пароль для SMTP авторизации:

Принудительно использовать TLS для SMTP сервера:

**Базовые настройки сервиса:**

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

Параметр	Описание	Примеры
<b>Обратный адрес для писем</b>	Обратный адрес для письма, формируемого системой в адрес технической поддержки	<ul style="list-style-type: none"><li>• test@ — обратный адрес будет test@user-domain</li><li>• test@example.com — обратный адрес будет test@example.com, независимо от домена пользователя</li></ul>
<b>Адрес получателя</b>	Адрес получателей. Получателей может быть несколько	<ul style="list-style-type: none"><li>• [ 'test@' ] — получателем письма будет test@user-domain</li><li>• [ 'test@', 'example@example.com' ] — получателями письма будут test@user-domain и example@example.com</li></ul>
<b>Тема письма</b>	Тема отправляемого письма	

#### Расширенные настройки сервиса:

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

## Настройка LDAP

Пропустите этот шаг, если планируется настройка интеграции VK Teams с панелью администратора VK WorkSpace. Перейдите к шагу проверки конфигурации.

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 проверке 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**:

Настройки VKT Отмена Сохранить

- Основные настройки
- Кластерные настройки
- Настройки DMZ
- Настройки SSL/TLS
- Настройки доступа к панели администрирования
- Настройки обратной связи
- Настройки 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=some-ldap-user-email@example.com](mailto:mail=some-ldap-user-email@example.com)
```

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

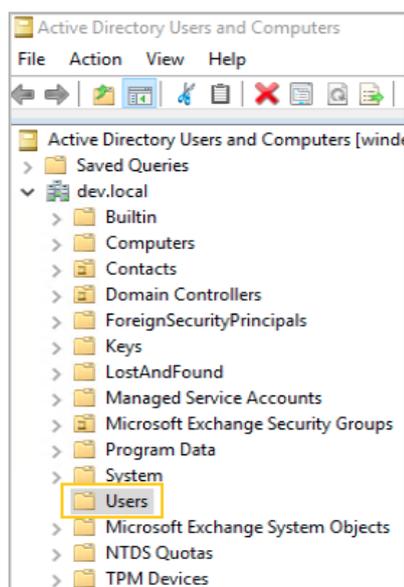


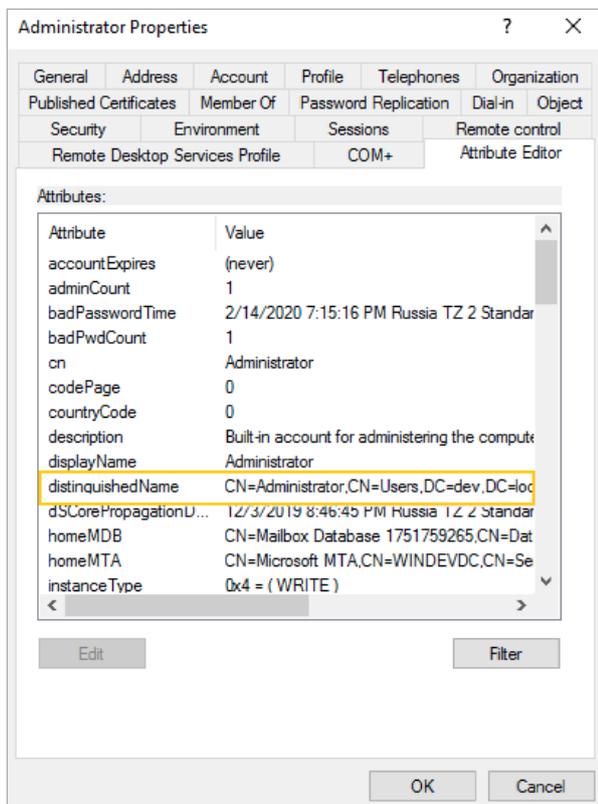
- **Частота полной синхронизации с LDAP-сервером, в секундах** — как часто осуществлять полную синхронизацию с LDAP-сервером, в секундах.
- **Частота частичной синхронизации с сервером, в секундах** — как часто осуществлять частичную синхронизацию с LDAP-сервером, в секундах (значение **-1** — отключить).
- **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).

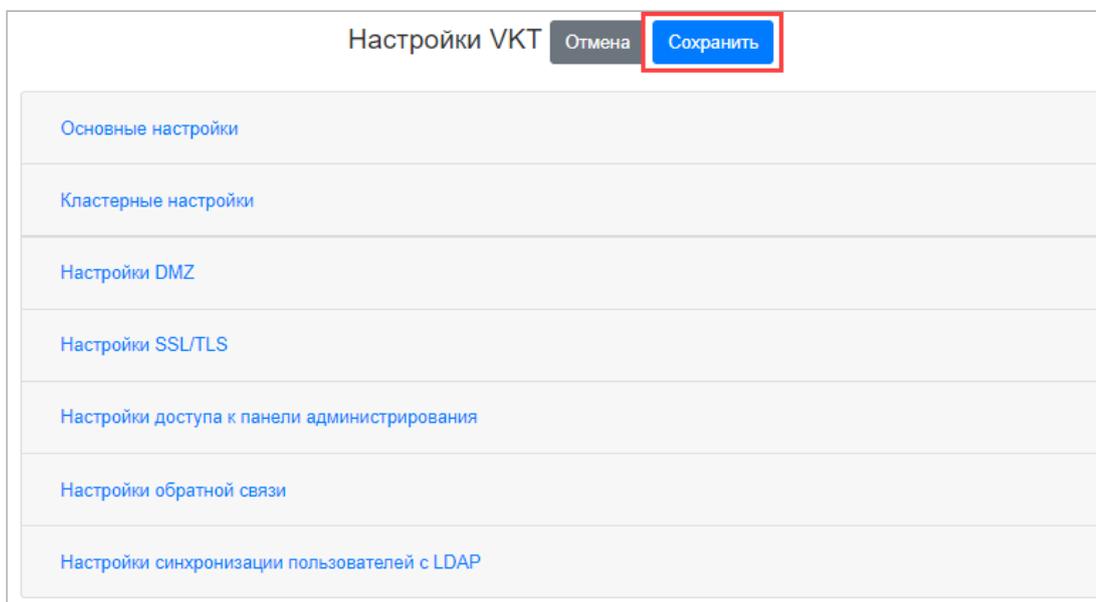
На вкладке будет отображено значение **distinguishedName**. Повторите операцию, чтобы получить **distinguishedName** для каталога, в котором будет выполняться поиск пользователей.





## Шаг 14. Проверка конфигурации

Чтобы сохранить все 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:

Результат проверки конфигурации:

2023-04-24 06:07:47,138 - [ERROR] ERROR: NTP server '94.100.180.133' error No response received from 94.100.180.133.

2023-04-24 06:07:47,678 - [CRITICAL] Found some errors in config file



В случае обнаружения ошибок их необходимо исправить.

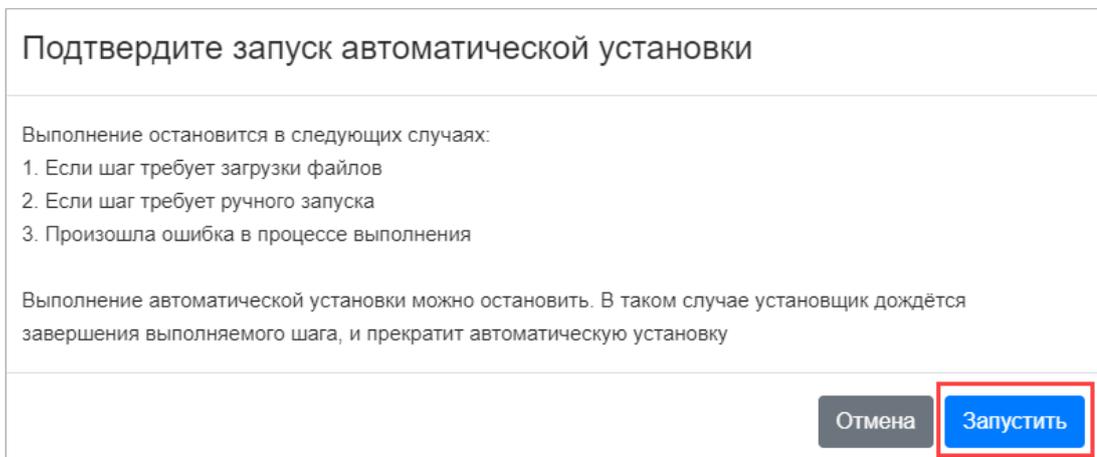
## Шаг 15. Запуск установки

После завершения настройки и проверки ошибок необходимо перейти на главную страницу и запустить

установку нажатием на кнопку  :

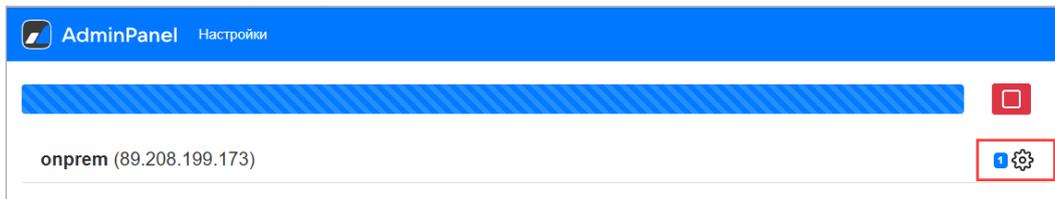


Подтвердите запуск автоматической установки, нажав на кнопку **Запустить**:



Для просмотра результата выполнения установки:

1. Нажмите на пиктограмму  :



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

AdminPanel Настройки

Название машины: vkt-1vm1  
Имя хоста: onprem  
IP: 89.208.199.173  
Внешний IP: 89.208.199.173

SSH-порт: 22  
Имя пользователя: centos  
Пароль: .....  
Приватный ключ: key

Сторона: [dropdown]  
Номер пары хостов: 0

Отмена Обновить

### Выполните шаги по настройке машины

**vkt\_premsetup** inProgress  
Настроить VKT1VM Запустить

[Результат выполнения](#)

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

AdminPanel Настройки

Установка завершена

onprem (89.208.199.173) [gear icon]

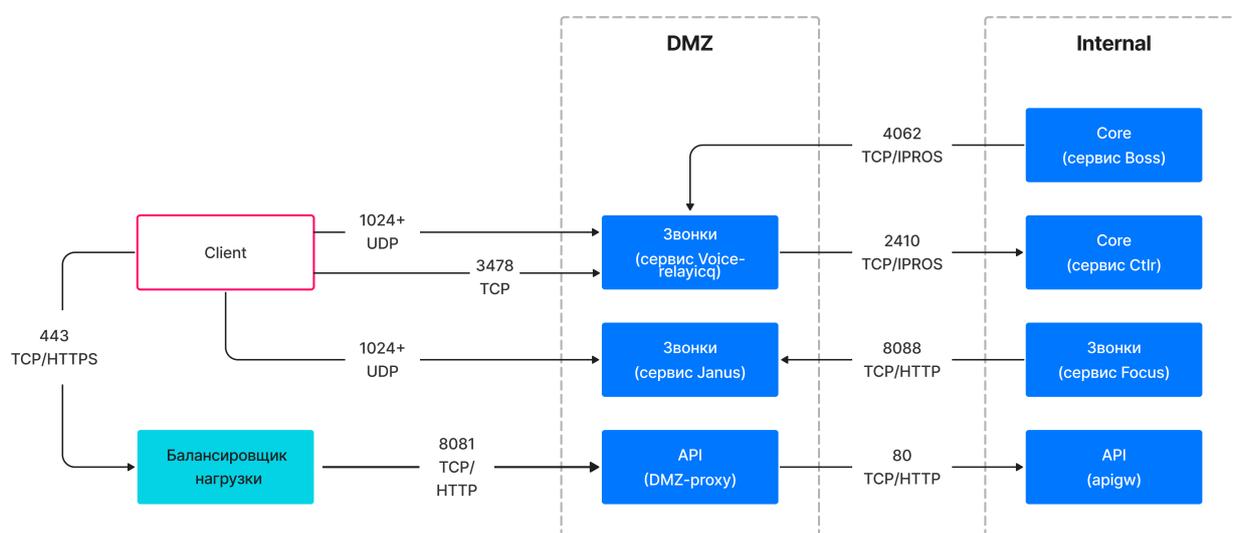
Установка кластера считается завершенной. [Перейдите к проверкам](#) инсталляции и основных функциональностей VK Teams.

# Установка кластера с DMZ

По умолчанию все компоненты VK Teams запускаются в одной сетевой среде.

Начиная с релиза 23.8 вы можете терминировать входящие соединения от клиентских приложений в отдельной сети. Часть компонентов кластера VK Teams выносятся в отдельную сеть для реализации DMZ.

При такой схеме параллельно работают 2 независимые инсталляции VK Teams, которые связаны строго определенными сетевыми доступами. На рисунке ниже часть серверов кластера установлена с типом **DMZ**, другая часть — с типом **Внутренняя инсталляция**.



Чтобы установить кластер с DMZ:

1. Выполните [шаги 1-10](#), описанные выше.

2. Установите кластер с типом **DMZ**:

- Распакуйте архив **vkt\_installer.zip** в отдельную директорию, запустите исполняемый файл и перейдите по адресу <http://127.0.0.1:8888>.
- Добавьте в установщик сервера, которые будут располагаться в DMZ, как описано в [шаге 12](#).
- Произведите настройку компонентов первой инсталляции, как описано в [шаге 13](#).

Дополнительно в блоке **Настройки DMZ** необходимо указать:

**Настройки DMZ**

Тип установки: Не использовать DMZ ▼

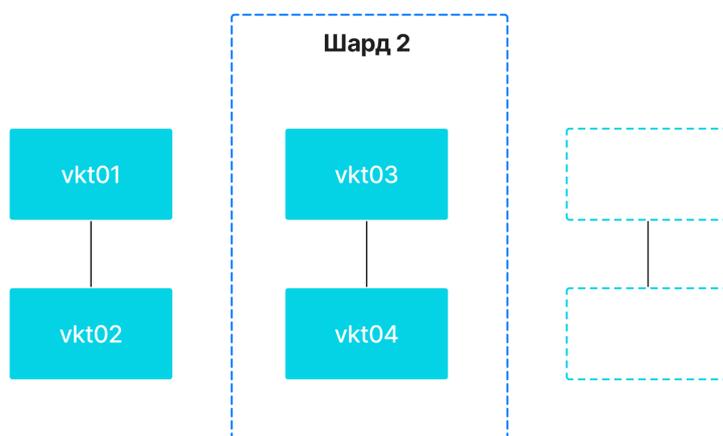
Список адресов IPROS контроллера: + Добавить

Список IP адресов внутренней инсталляции: + Добавить

Список IP адресов DMZ: + Добавить

- **Тип установки — DMZ.**

- **Список адресов IPROS контроллера** — укажите IP-адреса второго шарда внутренней инсталляции.



- **Список IP адресов внутренней инсталляции** — укажите список IP-адресов, по которым DMZ будет проксировать HTTP в кластер внутренней инсталляции.

- **Список IP адресов DMZ** — укажите список IP-адресов хостов в DMZ, которые будут терминировать групповые звонки.

- Выполните [шаги 14-16](#), как описано выше. Установка первой части кластера считается завершенной.

### 3. Установите кластер с типом **Внутренняя инсталляция**:

- Распакуйте архив **vkt\_installer.zip** в **другую** директорию, запустите исполняемый файл и перейдите по адресу <http://127.0.0.1:8888>.

- Добавьте в установщик сервера, которые НЕ будут располагаться в DMZ, как описано в [шаге 12](#).

- Произведите настройку компонентов второй инсталляции, как описано в [шаге 13](#).

В блоке **Настройки DMZ** необходимо указать:

- **Тип установки — Внутренняя инсталляция.**

- **Список адресов IPROS контроллера** — укажите IP-адреса второго шарда внутренней инсталляции.

- **Список IP-адресов внутренней инсталляции** — укажите список IP-адресов, по которым DMZ будет проксировать HTTP в кластер внутренней инсталляции.

- **Список IP-адресов DMZ** — укажите список IP-адресов хостов в DMZ, которые будут терминировать групповые звонки.

- Выполните [шаги 14-15](#), как описано выше. Установка второй части кластера считается завершенной.

4. После установки обеих инсталляций необходимо на одном из серверов внутренней инсталляции выполнить команду:

```
gic utils mapfiller --map-name=voice-relayicq --flush-map
```

5. Установка кластера с DMZ считается завершенной. [Перейдите к проверкам](#) инсталляции и основных функциональностей VK Teams.

# Проверки после инсталляции

По прошествии 15 минут после рестарта машины подключитесь к ней по SSH и выполните следующие проверки инсталляции:

## 1. Правильность версии релиза:

```
cat /etc/myteam-release
```

## 2. Состояние служб:

```
- systemctl status | grep '^ *State:'
```

Если в выводе есть статус «degraded», то список служб, которые завершились с ошибкой, можно посмотреть при помощи команды:

```
- systemctl --all --failed
```

## 3. Результаты выполнения скриптов внутреннего мониторинга системы:

```
mon.sh clean // очищаем логи  
mon.sh
```

Проанализируйте вывод команды в соответствии с [мониторингом параметров сервиса](#).

### Примечание

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

## 4. Готовность сервисов VK Teams:

```
ic srvs
```

Все сервисы должны находиться в состоянии **alive**.

## 5. Состояние подов Kubernetes:

```
kubectl get pods -A
```

Все сервисы должны быть в состоянии Running.

## 6. Понаблюдайте за нагрузкой CPU и памяти при помощи утилиты k9s.

## 7. Работоспособность оркестратора:

```
/usr/local/bin/im_utils --check-orch
```

В выводе команды не должно быть «found orchestrator issues».

#### 8. Релизы Helm:

```
helm list -A --failed --pending
```

В выводе команды не должно быть «pending, failed, unknown».

Также выполните проверки функциональностей VK Teams. Рекомендуется проводить тест при помощи разных типов клиентов, например веб и десктоп.

#### 1. Базовые функциональности:

- Возможность залогиниться в учетной записи.
- Отправить/получить текстовое сообщение с одного клиента на другой и обратно. Убедиться, что сообщения пришли.
- Удалить отправленные сообщения у себя и у всех. Убедиться, что сообщения успешно удаляются.
- Отправить/получить фото/видео/gif с одного клиента на другой и обратно. Проверить, что есть превью.
- Отправить/получить голосовое сообщение с одного клиента на другой и обратно. Убедиться, что запись полноценная и хорошего качества.
- Открыть витрину стикеров, открыть стикерпак. Убедиться, что все отображается корректно.
- Отправить/получить стикер с одного клиента на другой и обратно. Убедиться, что у стикера есть превью.
- Открыть собственный профиль и профиль другого пользователя.

#### 2. Группы:

- Создать группу/канал.
- Добавить пользователя в канал
- Отправить/получить несколько сообщений, которые содержат стикеры и файлы. Убедиться, что сообщения доходят до всех участников.
- Заблокировать/разблокировать участника.
- Закрепить сообщение.
- Удалить пользователя.
- Удалить группу/канал.

#### 3. Звонки:

- Позвонить пользователю. Добавить еще одного пользователя в звонок.
- Создать ссылку на звонок, перейти в звонок по ссылке.
- Проверить работу длительных звонков (около 5 минут).

#### 4. Статусы:

- Поставить/удалить статусы.

 Автор: Белова Ирина

 28 марта 2025 г.