Мессенджер и ВКС

Инструкция по установке кластера. Версия 26.1

Портал с документацией: https://biz.mail.ru/docs/on-premises/

Оглавление

Назначение документа 4

Дополнительная документация 4

Архитектура кластера 5

- Обязательные компоненты 5
- Опциональные компоненты 6

Технические требования 7

Совместимость 8

Предварительные условия для установки 9

- Роутинг исходящих соединений 9
- SMTP-сервер 9
- NTP-серверы 9
- Исходящие соединения на стороне клиента 9
- LDAP 9
- Требования к L7-балансировщику 10

Установка кластера без DMZ 12

- Шаг 1. Предварительные условия для установки 12
- Шаг 2. Проверка целостности полученных образов виртуальных машин 12
- Шаг 3. Создание виртуальной машины 13
- Шаг 4. Запуск образа виртуальной машины 13
- Шаг 5. Подключение к виртуальной машине 13
- Шаг 6. Генерация SSH-ключа для установщика 13
- Шаг 7. IP-адрес 14
- Шаг 8. Настройки DNS-зоны 14
- Шаг 9. Выпуск SSL-сертификата 0
- Шаг 10. Открыть доступы до внутренних ресурсов 0
- Шаг 11. Запуск установщика 0
- Шаг 12. Добавление сервера в установщик 0
- Шаг 13. Настройки Мессенджер и ВКС 0
  - Домен пользователя 0

Внутренний домен 0
Список DNS-серверов 0
Список серверов точного времени (NTP) 0
Настройка SMTP-сервера 0
Настройка сервиса записи звонков 0
Настройка SSO-аутентификации 0
Установка разрешений для пользователей 0
Кластерные настройки 0
Настройки DMZ 0
Настройки SSL-сертификата 0
Настройка окружения администратора 0
Настройка обратной связи 0
Настройка LDAP 0
Шаг 14. Проверка конфигурации 0
Шаг 15. Запуск установки 0
Установка кластера с DMZ 0
Проверки после инсталляции 0

Назначение документа

В инструкции описана кластерная установка Мессенджер и ВКС:

- 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 описано управление параметрами синхронизации LDAP.

Управление пользователями без контроллера домена — в документе описано управление пользователями без контроллера домена.

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

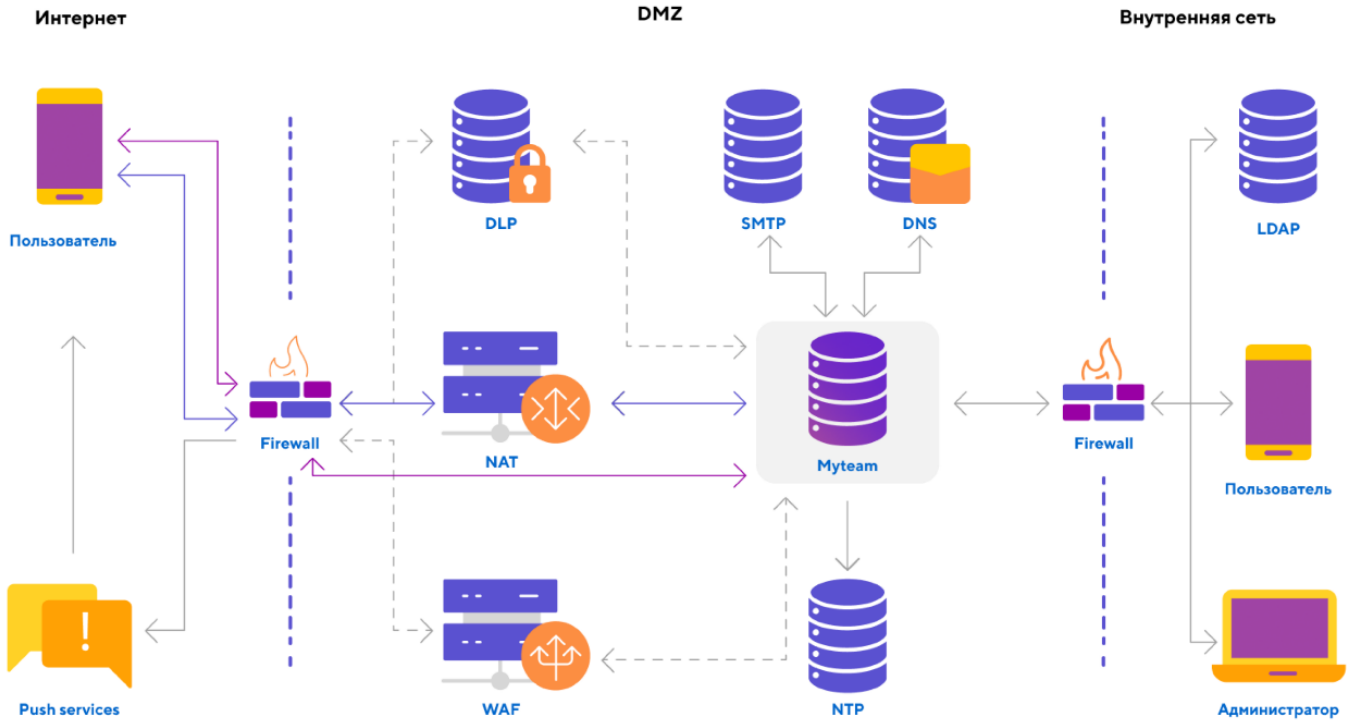
> **Примечание**
>
> Ранее Мессенджер и ВКС назывался Myteam, что находит отражение в технических моментах (например, команды в консоли).

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 Мессенджер и ВКС не требует отдельных компонентов вне сегмента сети DMZ. Однако Мессенджер и ВКС активно взаимодействует с внешними и внутренними компонентами сети.

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



Обязательные компоненты

Сервер Мессенджер и ВКС

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 Мессенджер и ВКС требуются исходящие соединения к этим сервисам и не требуются входящие соединения.

Суперапп VK WorkSpace

Пользовательское приложение, установленное на одной из допустимых платформ. Сервер Мессенджер и ВКС 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. Мессенджер и ВКС 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.

Технические требования

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

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

Если планируется настройка Федерации, на серверы каждой инсталляции необходимо добавить дополнительные вычислительные ресурсы:

- 10% от имеющихся мощностей vCPU
- 1 ГБ SSD
- 2 ГБ RAM на каждую тысячу федеративных пользователей. Ожидаемый прирост RAM — около 1 ГБ в год в зависимости от количества сообщений федерации

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.

Не допускайте переподписку. Суммарные vCPU на хосте не должны превышать количество физических ядер, выделенных всем виртуальным машинам. При этом не рекомендуется считать Hyper-Threading полноценными ядрами.

Не выделяйте одной виртуальной машине количество ядер больше, чем количество ядер на физическом сокете.

RAM

Не назначайте суммарную vRAM выше физической RAM хоста.

Механизмы экономии памяти

Не включайте механизмы ballooning и сжатия памяти.

swap

Не используйте swap — как на гипервизоре, так и внутри виртуальных машин.

Резервирования ресурсов виртуальных машин

Устанавливайте всю выделенную память и процессоры в резерв для виртуальных машин системы.

Хранилище

Не используйте тонкие диски (диски типа Thin) — диски с отложенным выделением пространства на СХД.

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 Мессенджер и ВКС 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 Мессенджер и ВКС 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 Мессенджер и ВКС 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. Управление пользователями без контроллера домена).

Требования к L7-балансировщику

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

Для публикации Мессенджер и ВКС во внешней сети вы можете настроить промежуточный балансировщик нагрузки.

При использовании L7-балансировки необходимо ограничивать на уровне сети доступ к виртуальным машинам Мессенджер и ВКС напрямую.

Входящий трафик в Мессенджер и ВКС обеспечивается при помощи Istio Ingress, который доступен на портах 80 и 443 на нодах Kubernetes-кластера с метками im/ingress: "true" (далее ingress-ноды).

В случае кластера все ingress-ноды равноправны — каждая нода может обработать любой запрос, и трафик необходимо равномерно респределить по нодам.

Балансировщик должен проставлять следующие заголовки при проксировании запросов в Мессенджер и ВКС:

- Host
- X-Real-IP — в этот заголовок должен записываться IP-адрес, откуда пришел запрос. Заголовок можно изменить — см. раздел Кластерные настройки.
- X-CUSTOM-SSL-OFFLOAD и X-SSL-OFFLOAD — в эти заголовки должно записываться значение «1». Эти заголовки сигнализируют о том, что балансировщик терминирует SSL.

Также балансировщик должен обеспечивать таймауты на чтение с сервера не менее 60 секунд.

В случае терминации SSL-трафика на балансировщике сгенерируйте и настройте сертификаты на балансировщике.

Пример конфигурации Nginx:

```
# Адреса ingress-нод Мессенджер и ВКС
upstream im-cluster {
    server 192.168.0.1:80;
    server 192.168.0.2:80;
    server 192.168.0.3:80;
    server 192.168.0.4:80;
```

```
}

# Конфигурация защищенного протокола работы
server {
    # Домен, на котором вы публикуете Мессенджер и ВКС
    server_name domain.company.ru *.domain.company.ru;

    listen 443 http2 ssl;

    access_log /var/log/nginx/domain.company.ru-access.log;
    error_log /var/log/nginx/domain.company.ru-error.log;
    # Путь до сертификатов SSL/TLS в формате x509, соответствующих указанным доменным именам
    ssl_certificate /etc/nginx/ssl/domain.company.ru.crt;
    ssl_certificate_key /etc/nginx/ssl/domain.company.ru.key;
    # Настройка проксирования трафика
    location / {
        # Адреса нод VKTeams
        proxy_pass http://im-cluster;
        # Проброс заголовков
        proxy_set_header    Host                $host;
        proxy_set_header    X-Real-IP           $remote_addr;
        proxy_set_header    X-CUSTOM-SSL-OFFLOAD 1;
        proxy_set_header    X-SSL-OFFLOAD       1;
        proxy_http_version 1.1;
        proxy_set_header Connection "";
        # Увеличение таймаутов на чтение
        proxy_read_timeout 120s;
    }
}
# Конфигурация редиректа на защищенный протокол
server {
    server_name domain.company.ru *.domain.company.ru;

    listen 80;

    access_log /var/log/nginx/domain.company.ru-access.log;
    error_log /var/log/nginx/domain.company.ru-error.log;
    location / {
        return 301 https://domain.company.ru$request_uri;
    }
}
```

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 Мессенджер и ВКС необходимо сгенерировать ключ на сервере Мессенджер и ВКС:

```
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):

- admin — адрес API управления Мессенджер и ВКС (административного веб интерфейса).
- akesadmin
- api — API бота.
- biz — адрес сервера Мессенджер и ВКС, где находится сервис Grafana.
- calendar — API календаря. Работает только в интеграции с Почтой VK WorkSpace.
- calendar-mobile — API мобильного календаря. Работает только в интеграции с Почтой VK WorkSpace.
- call — URL для формирования ссылок на звонки.
- di — поддомен сервиса Keycloak для версий до 25.2.
- dl — портал загрузки дистрибутивов (система автоматического обновления клиентских приложений).
- files-n — оргструктура организаций.
- kc — поддомен сервиса Keycloak для версии 25.2 и выше.
- notp
- outlook-plugin — плагин MS Outlook для создания конференций.
- rapi

- s — обмен стикерпаками.
- stentor — адрес API Мессенджер и ВКС для добавления/удаления пользователей.
- u — адрес клиентского API Мессенджер и ВКС.
- ub — файловое API.
- webim — веб-версия Мессенджер и ВКС.

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 Мессенджер и ВКС и запись Wildcard CNAME, указывающую на A-запись сервера Мессенджер и ВКС.

```
$ 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 Мессенджер и ВКС, 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
admin.vkteams.example.com.            3600  IN     CNAME   vkteams.example.com.
akesadmin.vkteams.example.com.        3600  IN     CNAME   vkteams.example.com.
api.vkteams.example.com.              3600  IN     CNAME   vkteams.example.com.
biz.vkteams.example.com.              3600  IN     CNAME   vkteams.example.com.
calendar.vkteams.example.com.         3600  IN     CNAME   vkteams.example.com.
calendar-mobile.vkteams.example.com.  3600  IN     CNAME   vkteams.example.com.
call.vkteams.example.com.             3600  IN     CNAME   vkteams.example.com.
di.vkteams.example.com.               3600  IN     CNAME   vkteams.example.com. # только для
версий до 25.2
dl.vkteams.example.com.               3600  IN     CNAME   vkteams.example.com.
files-n.vkteams.example.com.          3600  IN     CNAME   vkteams.example.com.
kc.vkteams.example.com.               3600  IN     CNAME   vkteams.example.com. # только для
версии 25.2 и выше
notp.vkteams.example.com.             3600  IN     CNAME   vkteams.example.com.
outlook-plugin.vkteams.example.com.   3600  IN     CNAME   vkteams.example.com.
rapi.vkteams.example.com.   3600  IN     CNAME   vkteams.example.com.
s.vkteams.example.com.                3600  IN     CNAME   vkteams.example.com.
stentor.vkteams.example.com.          3600  IN     CNAME   vkteams.example.com.
u.vkteams.example.com.                3600  IN     CNAME   vkteams.example.com.
ub.vkteams.example.com.               3600  IN     CNAME   vkteams.example.com.
webim.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.