

# Корпоративный мессенджер VK Teams

Примеры проблем и их решение

# Оглавление

---

Назначение документа	3
Дополнительная документация	3
Недостаточно места на диске	4
Заканчивается память	6
Проблема с авторизацией	7
Несоответствие логина пользователя и адреса сервера (API endpoints)	9

# Назначение документа

---

В документе рассмотрены потенциальные проблемы, которые не являются специфичными для конкретного сервиса, но могут возникнуть в процессе эксплуатации VK Teams.

Проблемы, специфичные для сервисов (синхронизация пользователей, авторизация, доставка push-сообщений), рассмотрены в [документации по администрированию](#).

Все описанные ниже проблемы можно определить и устранить заранее, пока они не стали мешать функционированию VK Teams. Для этого достаточно ввести [мониторинг](#) этих параметров и устранять проблему при возникновении статуса Warning (то есть не доводить до статуса Critical).

Документ предназначен для использования администраторами организации.

## Дополнительная документация

---

[Руководство по администрированию VK Teams](#) — в документе рассмотрены проблемы, специфичные для сервисов (синхронизация пользователей, авторизация, доставка push-сообщений).

[Мониторинг VK Teams](#)— в документе приведен перечень параметров инсталляции, которые необходимо контролировать.

# Недостаточно места на диске

Частота ротации лог-файлов и время хранения подобраны так, чтобы места на диске всегда хватало. Тем не менее возможны ситуации, при которых место на диске может заканчиваться.

Примеры:

- Инсталляция используется для большего числа пользователей, чем предполагалось.
- Один из сервисов слишком активно создает сообщения об ошибках. Например, Keycloak создает большие лог-файлы в случае дубликатов пользователей.

## Как решить проблему

Найдите источник проблемы, освободите место и сообщите о проблеме разработчику:

**Шаг 1.** Проверьте место на диске, выполнив команду `df -h`.

**Шаг 2.** Выясните, чем занято место:

```
du -smx /* 2>/dev/null | sort -rn | head
```

Ключ `-x` обязателен.

Если обнаружен каталог, который сильно превышает допустимые размеры, то выполните команду `du` в этом каталоге и найдите проблемное место. В дистрибутив включена утилита `ncdu`, которой удобно осуществлять поиск занятого места:

```
>ncdu / // искать по всем fs
>ncdu -x / // искать только по корневой fs и не тратить время на расчет занятого места на data-дисках
```

**Шаг 3.** Соберите информацию о проблеме и передайте ее разработчикам:

```
ls -alh /<путь к каталогу с большим лог-файлом>/
head -n 1000 <путь к большому лог-файлу>
tail -n 1000 <путь к большому лог-файлу>
```

**Шаг 4.** Удалите старые лог-файлы и выполните команду `truncate` по текущему, если он большого размера.

Возможна ситуация, когда команды `df` и `du` выдают разные результаты. Например, команда `df` показывает, что занято 50 Гб, а команда `du` показывает только 10 Гб. Это значит, что в файловой системе есть удаленные и незакрытые файлы. Найти такие файлы можно, выполнив:

```
ls -l +L1 | sort -rn -k 7 | head
```

## Особенности удаленных файлов

В активной системе такие файлы есть практически всегда, и нужно различать, когда это является проблемой, а когда нет. В большинстве случаев проблему с нехваткой места создают файлы журналов, которые не были переоткрыты сервисом. При этом важно понимать, насколько старый лог остался незакрытым.

### Пример

Логи не были переоткрыты сервисом Nginx-im:

```
nginx 729949 quantum 115w REG 252,1 17601 608228
/mnt/log/oap/icq/domains/local_proxy.icq.com/logs/old_logs/u-error.log-20200410-1800.rot
(deleted)

nginx 729949 quantum 150w REG 252,1 398647142 608229
/mnt/log/oap/icq/domains/local_proxy.icq.com/logs/old_logs/u-access.log-20200410-1800.rot
(deleted)
```

Если с 18:00 (время ротации исходя из имени файла) прошло менее двух часов, то никаких действия не требуется. Nginx обрабатывает длинные запросы (long polling), поэтому после отправки ему команды `reopen` еще долгое время остаются старые дочерние процессы, которые продолжают держать этот файл. Если же с 18:00 прошло много времени, нужно отправить команду `reopen`:

```
/usr/local/nginx-im/sbin/nginx -c /usr/local/nginx-im/conf/nginx.conf -s reopen
```

Если лог-файлы остались в статусе `deleted`, то необходимо проверить правильность конфигурационных файлов Nginx. Вероятно, в них есть синтаксическая ошибка:

```
/usr/local/nginx-im/sbin/nginx -c /usr/local/nginx-im/conf/nginx.conf -t
```

# Заканчивается память

---

Излишнее потребление памяти может происходить по разным причинам.

Примеры:

- Утечка в ПО.
- Некорректные пропорции выделенного RAM и выставленных лимитов в приложениях (наиболее вероятный вариант). Разные клиенты используют разное количество аккаунтов, и профиль нагрузки заранее неизвестен, поэтому невозможно предугадать, насколько корректны выставленные настройки и лимиты.
- Непрогнозируемое повышение нагрузки. Обычно повышение нагрузки связано с потреблением CPU, но расход памяти в этом случае может тоже увеличиваться. Также может не хватать ресурсов CPU для работы сборщиков мусора.

## Как решить проблему

**Шаг 1.** Выполните `free -m`.

**Шаг 2.** Изучите параметры `free`, `available`, `buff`, `cache`.

`Free` — это неиспользуемая память.

`Available` — это память, которую система может освободить при необходимости, в том числе туда входят кэш и буфер. Если же память `available` составляет менее 20-30% от общей, то это может быть проблемой, так как системе для быстрой работы необходимы буфер и кэш.

**Шаг 3.** Изучите список процессов, которые потребляют память больше всего. Можно использовать любой из способов:

- `top -o RES`
- `smem -s rss -p`
- `ps -ax -o pid,rss,command --sort rss`

**Шаг 4.** Для временного устранения проблемы перезапустите процессы, которые занимают наибольшее количество памяти. Однако нельзя гарантировать, что проблема не повторится, поэтому обязательно пришлите разработчику следующую информацию:

- вывод `smem -s rss -p`
- вывод `top -o RES -n 1`
- вывод `free -m`

После изучения этих данных мы предложим варианты для предотвращения подобной ситуации в дальнейшем.

# Проблема с авторизацией

**Пример:** поступило обращение со стороны клиента, что сотрудник с логином `user@vkteams.example.com` не может зайти в систему.

## Как решить проблему

Проверьте, что пользователь `user@example.com` есть в системе — через веб-интерфейс сервиса Keycloak (см. раздел [Авторизация в системе](#) документации по администрированию) или базу данных:

```
mysql -S keycloak-mysql-mysql-cluster-im-db-mysql-master.keycloak.svc.cluster.local -e "SELECT * FROM USER_ENTITY WHERE EMAIL = 'example@example.com'\G" keycloak
```

## Пользователя в системе нет

Это означает, что есть проблемы с синхронизацией пользователей. Дальнейшие действия:

**Шаг 1.** Проверьте с помощью `ldapsearch`, что пользователь действительно существует в корпоративном LDAP клиента.

**Шаг 2.** Если пользователь найден, выполните полную синхронизацию, чтобы убедиться в корректности синхронизации. Учитывайте, что полная синхронизация может занять несколько минут.

Запуск синхронизации:

```
kccli ldap sync --name <ИМЯ LDAP-ПОДКЛЮЧЕНИЯ>
```

В случае если вы хотите запустить принудительную синхронизацию всех LDAP-серверов, выполните:

```
kccli ldap sync
```

Если пользователь появился и был добавлен недавно, то дальнейших действий не требуется. Однако нужно проверить, что у пользователя заработала авторизация. Если пользователь не появился или он заведен давно, то выполните действия далее.

**Шаг 3.** Проверьте логи сервиса Keycloak — скорее всего, обнаружится ошибка (например, дубликаты записей пользователя). Исправьте ошибку и перезапустите сервис, чтобы закрыть все существующие соединения с LDAP-сервером клиента (так как все существующие соединения продолжают работать со старыми настройками).

## Пример использования `ldapsearch`

```
LDAPTLS_REQCERT=never ldapsearch -H 'CONNECTION_URI' -W -D 'BIND_DN' -b 'BASE_DN' '(&(ORIGINAL_FILTER)(mail=example@example.com))'
```

- Флаг `-W` — пароль нужно вводить при выполнении запроса.
- `LDAPTLS_REQCERT=never` — позволяет не регистрировать сертификат LDAP-сервера в ОС при использовании `ldapsearch`.

- `-H (CONNECTION_URI)` — указание полной строки подключения к LDAP согласно данным клиента (из файла конфигурации `defaults.yaml` или Keycloak).
- `-D (BIND_DN)` — логин для авторизации в LDAP.
- `-b (BASE_DN)` — базовый путь поиска.
- `ORIGINAL_FILTER` — фильтр, который используется в Keycloak (предоставляется клиентом, может быть найден в `/usr/local/etc/premsetup/ldap.yaml`). В данном примере к оригинальному фильтру добавлено требование найти объект с почтой `user@example.com`.

 **Внимание**

Скобки обязательны.

### Пользователь в системе есть

1. Проверьте, что запрос на авторизацию со стороны пользователя был выполнен. Подробности см. в разделе [Пример работы с журналами](#) документации по администрированию.
2. Проверьте отправку OTP-сообщения. Подробности см. в разделе [Пример работы с журналами](#) документации по администрированию.

# Несоответствие логина пользователя и адреса сервера (API endpoints)

Когда пользователь вводит логин вида `username@vkteams.EXAMPLE.com`, приложение обращается по следующим адресам для получения конечных точек (эндпоинтов) API:

- `https://u.vkteams.EXAMPLE.com/myteam-config.json`
- `https://vkteams.EXAMPLE.com/myteam-config.json`

Файл **myteam-config.json** генерируется автоматически скриптом конфигурации сервера VK Teams и не требует ручного редактирования.

Если сервер VK Teams установлен, например, по адресу `vkteams.EXAMPLE.com`, а адрес пользователя — `username@EXAMPLE.com`, приложение не сможет найти конфигурационный файл по адресам:

- `https://u.EXAMPLE.com/myteam-config.json`
- `https://EXAMPLE.com/myteam-config.json`

В этом случае приложение отобразит пользователю диалоговое окно с предложением ввести адрес сервера, на котором установлен VK Teams. Чтобы пользователям не пришлось выполнять дополнительные действия, настройте редирект:

```
https://EXAMPLE.com/myteam-config.json -> https://u.vkteams.EXAMPLE.com/myteam-config.json
```

Для корректной работы браузерной версии (WebIM) необходимо к редиректу добавить CORS:

```
access-control-allow-credentials: true  
access-control-allow-origin: https://webim.vkteams.EXAMPLE.com
```

Если настройка редиректа невозможна (например, для гостевых учетных записей с внешним доменом), пользователь может:

- указать в диалоговом окне адрес сервера (`vkteams.EXAMPLE.com` для примера выше);
- сразу ввести логин с адресом сервера через знак `#`:

```
username@example.com#vkteams.EXAMPLE.com
```

Тогда приложение будет сразу обращаться по адресам:

- `https://u.vkteams.EXAMPLE.com/myteam-config.json`
- `https://vkteams.EXAMPLE.com/myteam-config.json`