Мессенджер и ВКС

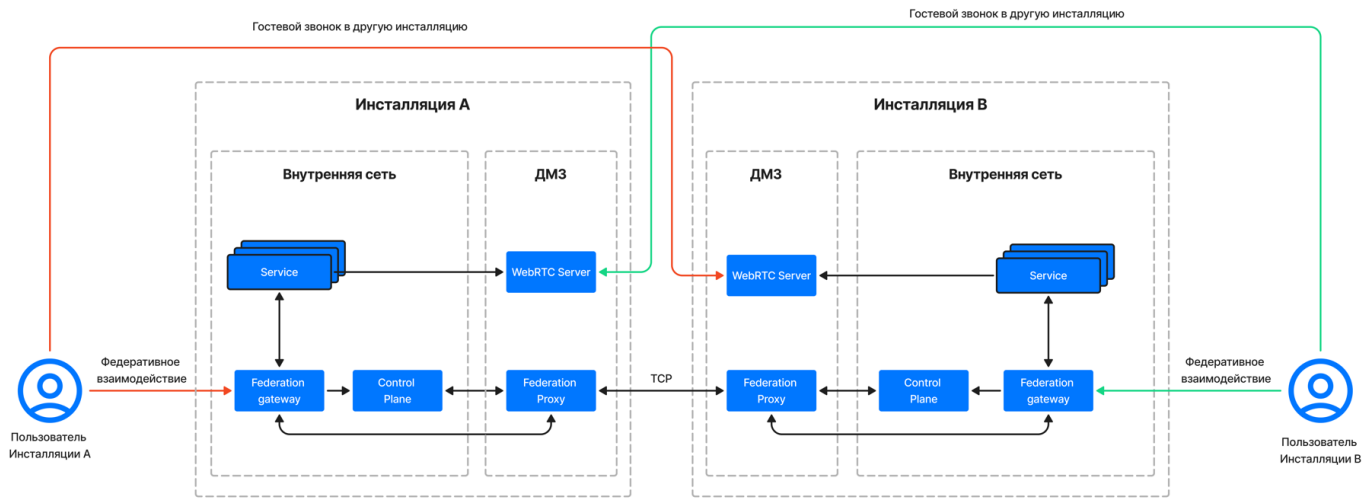
Настройка Федерации

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

Оглавление

Общая информация

На схеме ниже представлено федеративное взаимодействие пользователей из разных тенантов Федерации:



Федерация — протокол взаимодействия тенантов. Является транспортом по доставке данных между тенантами. Отвечает за проверку:

- Соответствия требованиям доверия (Трастов).
- Прав пользователей на внешнюю коммуникацию.
- Готовность сервисов к взаимодействию.
- Обеспечивает надежность и безопасность передачи данных.

Тенант — независимые части организации: отдельные инсталляции, набор доменов или пользователей. Могут находиться в одной или разных инсталляциях. Пользователи не могут взаимодействовать и коммуницировать до формирования траста между тенантами.

Инсталляция — независимые развернутые стенды разных организаций. Могут включать в себя несколько тенантов.

Траст — доверительное отношение между двумя и более тенантами. Могут быть сформированы:

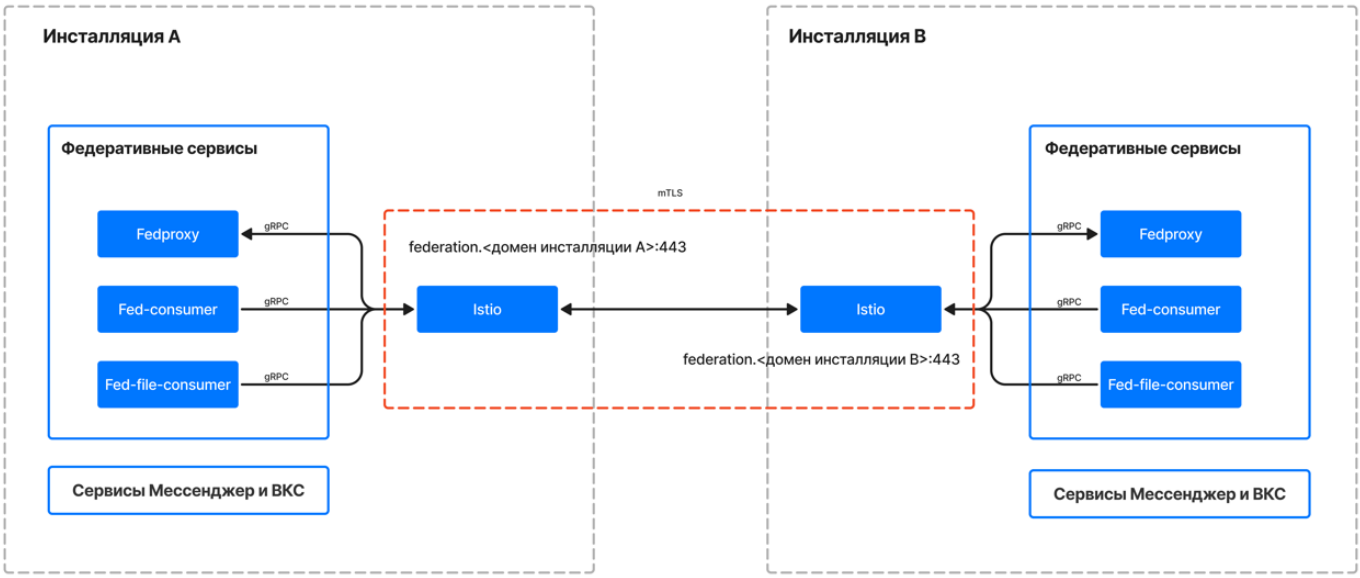
- Между тенантами в разных инсталляциях On-premises.
- Между тенантами внутри одной инсталляции.
- Тенант из On-premise инсталляции с тенантом в SaaS-версии продукта.

Особенности работы Федерации:

- Звонки между федерациями могут быть только гостевые.
- Общение между двумя инсталляциями осуществляется по протоколу gRPC + TLS. Эндпоинт для взаимодействия в общем виде выглядит так:

```
federation.<домен удаленной инсталляции>:443
```

Схема взаимодействия между инсталляциями A и B по протоколу mTLS:



Предварительные условия

1. Для настройки Федерации вам понадобится доступ к серверу Мессенджер и ВКС и доступ к Панели администратора VK WorkSpace по адресу https://biz.<ваш домен>.
2. Для корректной работы сервиса Федерация добавьте на серверы каждой инсталляции 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.
3. Проверьте, что у всех инсталляций Федерации есть доступ друг к другу. Например, проверьте, что запрос из Инсталляции A доходит до Инсталляции B:

   ```
   curl -I federation.<домен Инсталляции B>
   ```

   Если доступов нет, администраторам инсталляций необходимо запросить друг у друга адреса Federation Proxy и разрешить обращаться только по адресам `federation.<домен инсталляции>:443`.
4. Для включения mTLS на каждой инсталляции необходимо сформировать следующий набор артефактов:
   - публичный сертификат CA — cacert.pem
   - публичный сертификат сервера — server.cert.pem
   - приватный (секретный) ключ сервера — server.key.pem

- публичный сертификат клиента — client.cert.pem
- приватный (секретный) ключ клиента — client.key.pem

Как создать сертификаты — см. в разделе ниже.

Для осуществления взаимодействия Инсталляция А должна передать публичный сертификат клиента и приватный ключ клиента Инсталляции В и наоборот.

Итого на Инсталляции А должен быть набор следующих файлов:

- публичный сертификат CA — server.cacert.pem
- публичный сертификат сервера — server.cert.pem
- приватный (секретный) ключ сервера — server.key.pem
- публичный сертификат клиента — client.cert.pem
- приватный(секретный) ключ клиента — client.key.pem
- публичный сертификат CA удаленной инсталляции, которым подписан клиент — client_B.cacert.pem
- публичный сертификат клиента от удаленной инсталляции — client_B.cert.pem
- приватный(секретный) ключ клиента от удаленной инсталляции — client_B.key.pem

Все сертификаты рекомендуется разместить в директории **/opt/certs**.

Шаг 1. Получите tenantID

Перейдите на машину, где развернута Панель администратора VK WorkSpace и проверьте, есть ли в системе tenantID:

```
sudo docker exec -it bizpostgres1 psql pdd_postgres -U postgres
```

Если tenantID есть, в выводе команды будет:

```
SELECT common_tenant.tid
FROM common_tenant
ORDER BY common_tenant.id ASC
LIMIT 1;
```

Если ответ пустой, сгенерируйте новый tenantID, последовательно выполнив команды:

```
sudo docker exec -it bizf1 bash
. env/bin/activate
./manage.py shell
from pdd.common.models import Tenant
t = Tenant(name='test')
# в параметре name укажите название вашей инсталляции на ланитинце (на свое усмотрение)
t.save()
print(t.tid)
```

После команды `print(t.tid)` будет вывод tenantID. Сохраните это значение, оно понадобится вам ниже.

Получите у администратора удаленной инсталляции его tenantID. Он понадобится вам ниже.

> **Важно**
>
> Укажите в параметре name то же имя инсталляции, что и при создании сертификатов

Шаг 2. Включите Федерацию

Перед включением убедитесь, что у вас есть доступ до удаленной инсталляции (см. предусловия).

Чтобы включить Федерацию:

1. Подключитесь к серверу Мессенджер и ВКС.
2. Включите новый метод для отправки сообщений — в конфигурационном файле **/usr/local/nginx-im/html/myteam/myteam-config.json** в поле **message-send-api-enabled** укажите значение true:

   ```
   message-send-api-enabled: true
   ```

3. Для инсталляции на одну виртуальную машину выполните команду:

   ```
   HELMWAVE_USE_LOCAL_REPO_CACHE=true hwup -t godmod
   ```

   Для кластерной инсталляции:

   ```
   HELMWAVE_USE_LOCAL_REPO_CACHE=true HELMWAVE_ENV_NAME=cluster hwup -t godmod
   ```

4. Перезапустите под в технологическое окно (может приводить к сбою в новых подключениях):

   ```
   kubectl delete pods -n vkteams -l app=myteam-admin
   ```

5. Включите сервисы для работы федерации — в файле **/usr/local/etc/k8s/helmwave/projects.yml** удалите или закомментируйте строчки:

   - event-manager
   - federation
   - strimzi-kafka-operator

   ```
   envs:
   all:
       projects:
       disabled:
   #       event-manager:
   #       federation:
   #       strimzi-kafka-operator:
   ```

6. Внесите изменения в файл **/usr/local/etc/k8s/helmwave/store/federation.yml**:

   • В поле **enabled** установите значение true.

   • В поле **mtlsEnabled** установите значение true.

   • В поле **localTenant** укажите tenantID вашей инсталляции из шага 1:

```
enabled: true
mtlsEnabled: true
localTenant: '7BJqEXMGyEL' # вывод команды print(t.tid) из шага 1
```

   • Установите связь с удаленной инсталляцией:

```
- address: 'federation.<домен удаленной инсталляции>:443'
    name: <имя удаленной инсталляции на латинице>
    cert_cn: <имя удаленной инсталляции на латинице>
    ssl_cert: "/opt/certs/client.cert.pem" # публичный сертификат клиента от удаленной
инсталляции
    ssl_key: "/opt/certs/client.key.pem" # приватный (секретный) ключ клиента от
удаленной инсталляции
    cacert: "/opt/certs/client.cacert.pem" # публичный сертификат CA удаленной
инсталляции, которым подписан клиент
    tenants:
    - '<tenantID удаленной инсталляции>' # получите у администратора удаленной
инсталляции
```

Пример файла federation.yml

```
enabled: true
mtlsEnabled: true
localTenant: 7BJqEXMGyEL
instances:
- address: federation.domain.ru:443
    name: remote installation_B
    cert_cn: remote installati_B
    ssl_cert: "/opt/certs/client_B.cert.pem"
    ssl_key: "/opt/certs/client_B.key.pem"
    cacert: "/opt/certs/client_B.cacert.pem"
    tenants:
      - HWqHczeM2P
```

7. В конфигурационном файле **/usr/local/etc/k8s/helmwave/projects/federation/values/fedproxy.yml** пропишите локальный серверный сертификат:

```
grpc:
  server_cert: "/opt/certs/server.cert.pem"
  server_key: "/opt/certs/server.key.pem"
  server_ca: "/opt/certs/server.cacert.pem"
```

8. Включите **event-manager** — в конфигурационном файле **/usr/local/etc/k8s/helmwave/store/event_manager.yml** укажите:

```
enabled: true
```

9. Примените изменения, последовательно выполнив команды под супер пользователем:

```
hwup -t federation
hwup -t event-manager
hwup -t boss
hwup -t front
hwup -t mchat-st
hwup -t istio
hwup --tags apigwv2
```

10. Перезапустите поды сервиса Boss:

```
im_pod_cleaner delete -n vkteams --pod-label app=boss
```

11. Проверьте, что переменная **UC_ALLOW_FAKE_AIMSID** имеет значение «1»:

```
[root@fed1-el7] centos# kubectl exec -n vkteams -it boss-1-dng2p -- bash
[root@boss-1-dng2p oap]# echo 'config {return $UC_ALLOW_FAKE_AIMSID}' | nc 127.0.0.1 4323
boss.onpremise.a-01-1 online; Wed, 15 Oct 2025 15:30:19 MSK
Note: Default privileges 'WMNSD' are in effect
Ok
1
Ok
```

12. В конфигурационном файле сервиса Nomail **/usr/local/etc/nomail-1.conf** укажите для параметра **federation.enabled** значение true:

```
federation.enabled true
```

13. Перезапустите сервис Nomail:

```
systemctl restart nomail-1.service
```

Шаг 3. Добавьте пользователей в Федерацию

Чтобы пользователи из разных инсталляций могли общаться друг с другом, нужно добавить пользователей в белый список.

На обеих инсталляциях нужно:

1. Составить список пользователей, которым разрешено федеративное общение, и запустить команду, которая сформирует файл с белым списком.
2. Передать файл с белым списком в удаленную инсталляцию и получить такой же файл от удаленной инсталляции.
3. Загрузить файлы с белыми списками на каждой инсталляции.

> **Внимание**
>
> Эта процедура должна быть выполнена в обеих инсталляциях, входящих в Федерацию. Без наличия белого списка с обеих сторон и их загрузки в удалённой инсталляции — федеративная коммуникация будет невозможна.

1. Создайте файл с белым списком пользователей

1. Создайте файл whitelist.yaml и наполните его списком пользователей, которым разрешено федеративное взаимодействие с удаленной инсталляцией. Файл выглядит так:

```
remoteTenant: HWqHczeM2P # tenantID удаленной инсталляции
users:
    "i.ivanov@company_domain":
    "n.belov@company_domain":
    "a.petrov@company_domain":
```

   - remoteTenant — tenantID удаленной инсталляции, для которой выбранным пользователям разрешается общение.
   - users — список пользователей. В конце email обязательно ставьте двоеточие. Email в этом случае — это ключ объекта, в котором потом могут быть дополнительные значения.

2. Создайте файл с белым списком — на сервере Мессенджер и ВКС выполните команду:

```
creeper federation whitelist --file=whitelist.yaml --outfile=remote_whitelist.yaml
```

   Команда создает для каждого пользователя федеративный идентификатор (fid). Сгенерированный файл remote_whitelist.yaml имеет следующую структуру:

```
users:
    "i.ivanov@company_domain":
        fid: fid:0/HZnKEBoqDU/100401
    "n.belov@company_domain":
        fid: fid:0/HZnKEBoqDU/100402
    "a.petrov@company_domain":
        fid: fid:0/HZnKEBoqDU/100403
```

3. Передайте файл с белым списком в удаленную инсталляцию.

> **Передача файла в удаленную инсталляцию должна производиться безопасным способом**
>
> Возможные варианты передачи списков email для заведения белого списка:
>
> - Файлы защищены паролем в письме или на физических носителях.
> - Сжатые зашифрованные письма.
> - Предоставление своего SFTP/FTPS.
> - По ссылке с вводом логина и пароля.

2. Загрузите список пользователей от удаленной инсталляции

1. Получите файл remote_whitelist.yaml от удаленной инсталляции.
2. На сервере Мессенджер и ВКС добавьте полученный файл в любую директорию и выполните команду:

```
creeper federation whitelist --file=remote_whitelist.yaml
```

Как создать сертификаты

На рисунке ниже представлена схема взаимодействия между инсталляциями A и B по протоколу mTLS:

Сгенерированные сертификаты и ключи должны быть доступны на чтение/запись только для root-пользователя/сервисов Мессенджер и ВКС в рамках прав доступа файловой системы.

1. Выпустите CA сертификат и ключ, последовательно выполнив команды:

```
# mkdir /root/mtls
# mkdir /root/mtls/private
# mkdir /opt/certs
# openssl genrsa -out /root/mtls/private/cakey.pem 4096
# openssl req -new -x509 -days 3650 -key /root/mtls/private/cakey.pem -out /opt/certs/
server.cacert.pem
```

   Каждая инсталляция Федерации выпускает свой публичный сертификат CA.

2. Выпустите серверный сертификат и ключ:

```
[ req ]
distinguished_name  = req_distinguished_name

[v3_req]
subjectAltName = @alt_names

[alt_names]
DNS.1 = federation.domain.ru # хост удаленной инсталляции

[ req_distinguished_name ]
C  = RU
ST = Moscow
L  = Moscow
O  = CompanyA
CN = <installation_A> # укажите имя локальной инсталляции на латинице
```

3. Перейдите в директорию с сертификатами **/opt/certs** и создайте приватный ключ:

```
# cd /opt/certs
# openssl genrsa -out server.key.pem 4096
```

4. Переподпишите с SNA:

```
# openssl req -new -nodes -out server.csr.pem -keyout server.key.pem -config /root/mtls/
san.cnf -subj "/CN=<company_installation_name>"
```

5. Выпустите сертификат (подпишите у CA):

```
# openssl x509 -req -in server.csr.pem -CA server.cacert.pem -CAkey /root/mtls/private/
cakey.pem  -CAcreateserial -out server.cert.pem -days 365 -extensions v3_req -extfile /
root/mtls/san.cnf
```

6. Проверьте SAN в сертификате:

```
# openssl x509 -in server.cert.pem -noout -text | grep -A1 "Subject Alternative Name"
```

7. Под каждую инсталляцию, с которой устанавливается соединение, выпустите клиентские ключ и сертификат. В CN и SAN добавьте информацию удаленной инсталляции (в которую будете передавать эти сертификаты). В конфигурации сервиса Fedproxy полю **cert_cn** для каждой инсталляции задайте значение соответственно CN клиентских сертификатов:

```
# openssl genrsa -out client.key.pem 4096
# openssl req -new -key client.key.pem -out client.csr.pem -subj "/CN=<имя удаленной
инсталляции>"
# openssl x509 -req -in client.csr.pem -CA server.cacert.pem -CAkey /root/mtls/private/
cakey.pem   -CAcreateserial -out client.cert.pem -days 365   -extfile <(echo
"subjectAltName=DNS:<хост удаленной инсталляции>")
```

   где <имя удаленной инсталляции> — значение параметра **cert_cn** конфигурационного файла federation.yml.

   Пример команды:

```
# openssl genrsa -out client.key.pem 4096
# openssl req -new -key client.key.pem -out client.csr.pem -subj "/CN=installation_B"
# openssl x509 -req -in client.csr.pem -CA server.cacert.pem -CAkey /root/mtls/private/
cakey.pem   -CAcreateserial -out client.cert.pem -days 365   -extfile <(echo
"subjectAltName=DNS:federation.domain.ru")
```

   Полученные сертификаты client.cert.pem, client.key.pem и server.cacert.pem (переименовав в client.cacert.pem) передайте в инсталляцию B.

Технический писатель: Белова Ирина

2 марта 2026 г.