

Архитектура VK Workspace

Архитектура VK Workspace

Оглавление

Введение	3
Термины, определения и сокращения	3
Общее описание архитектуры VK WorkSpace	4
Верхнеуровневое описание компонентов VK WorkSpace	5
Интеграции с внешними системами	6
Описание организации сетевого взаимодействия VK WorkSpace	8
Пропускная способность каналов связи	9
Технические требования	9

Введение

В настоящем документе приведено описание архитектуры продуктов, входящих в состав коммуникационной платформы VK Workspace.

- Почта VK Workspace — электронная почта для обмена сообщениями между сотрудниками внутри и вне компании .
- Календарь VK Workspace — сервис для планирования совместных встреч .
- Диск VK Workspace — облачное хранилище для совместной работы с документами.
- Панель администратора VK Workspace — сервис для управления пользователями, почтой, диском и другими настройками.
- Установщик VK Workspace — сервис для взаимодействия с дистрибутивом.

Данный документ предназначен для технических специалистов, которые внедряют или поддерживают приведенные технологические решения. Документ предполагает наличие технических знаний в области проектирования систем, однако будет полезен и специалистам бизнес-подразделений.

Термины, определения и сокращения

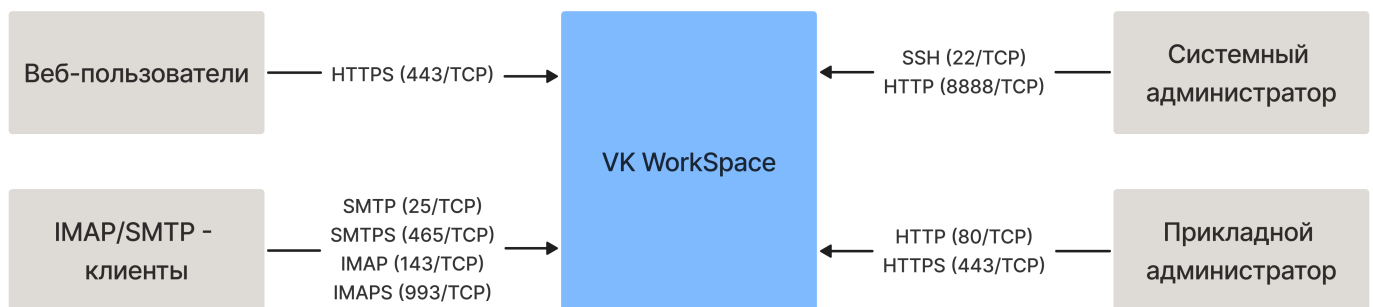
В настоящем документе приняты следующие термины и сокращения:

Термин/ сокращение	Определение
Компонент	Логическая единица обобщающая функциональное назначение в рамках архитектуры платформы VK Workspace. Может включать несколько сервисов
Контейнер	Докер-контейнер — изолированное пространство, которое позволяет запускать приложения с их зависимостями отдельно от основной системы
Сервис	Реализация бизнес-логики
DNS	Domain Name System, компьютерная распределённая система для получения информации о доменах
DLP	Data Loss Prevention — специализированное программное обеспечение, которое защищает конфиденциальную информацию от утраты, утечки или неправомерного использования

Термин/ сокращение	Определение
NTP	Network Time Protocol, протокол сетевого времени
SIEM	Security Information and Event Management, система управления информационной безопасностью и событиями безопасности
SMTP	Simple Mail Transfer Protocol, простой протокол передачи почты
IMAP	Internet Message Access Protocol, протокол прикладного уровня для доступа к электронной почте
WAF	Web Application Firewall — совокупность технологий, направленных на выявление уязвимостей и защиту от сетевых атак на веб-приложения

Общее описание архитектуры VK WorkSpace

Общая схема взаимодействия пользователей с VK WorkSpace:



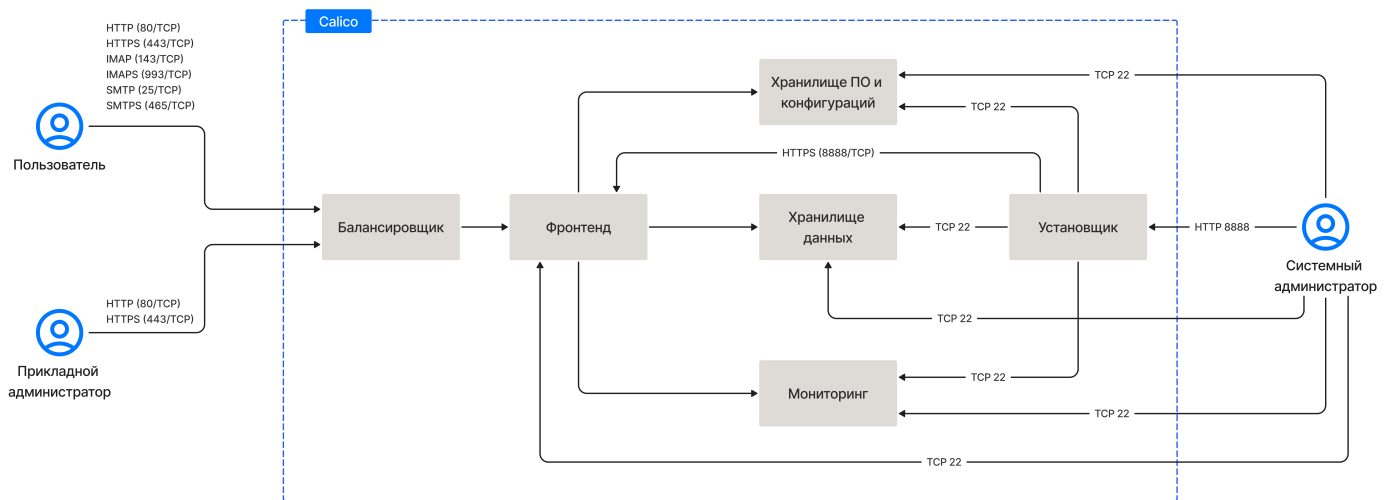
Общее описание взаимодействий приведено в таблице.

Взаимодействие	Описание
Веб-пользователи	Сотрудники могут получить доступ к VK WorkSpace с рабочего места, в рамках корпоративной сети, мобильного устройства и персонального компьютера из внешней сети Internet
Системный администратор	Корпоративный пользователь в зоне корпоративной сети с правом системного администрирования (управление настройками инфраструктуры VK WorkSpace)
Прикладной администратор	Корпоративный пользователь с доступом к Административной панели VK WorkSpace

Взаимодействие	Описание
IMAP/SMTP - клиенты	Используется для взаимодействия с внешними почтовыми серверами для отправки/получения и синхронизации почты

Верхнеуровневое описание компонентов VK WorkSpace

Общая схема компонентов VK WorkSpace:



Общее описание компонентов приведено в таблице:

Компонет	Описание
Балансировщик	Компонент, отвечающий за обработку пользовательских запросов и перенаправление на необходимый фронтенд — Nginx, который может обслужить запросы как HTTP-стека, так и IMAP, SMTP-протоколы (варианты балансировки: Nginx (upstream) и DNS-балансировка)
Фронтенд	Компонент, отвечающий за взаимодействие с пользователями, администраторами и внешними системами
Хранилище ПО и конфигураций	Компонент, отвечающий за хранение образов контейнеров, инфраструктурных данных и настроек сети
Хранилище данных	Компонент, отвечающий за хранение данных пользователей (включая списки пользователей на связанных инсталляциях) и данных Системы
Мониторинг	

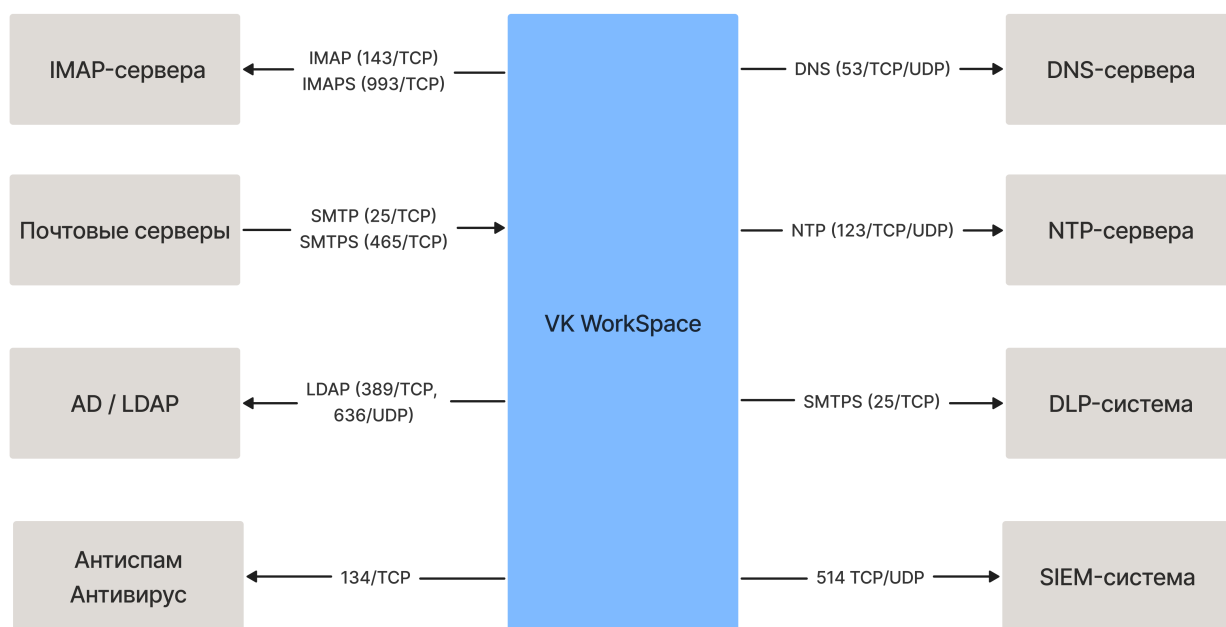
Компонет	Описание
	Компонент, отвечающий за сбор метрик и телеметрии со всех составляющих Системы
Установщик	Компонент, отвечающий за установку решения, реализованный с помощью сервиса <code>onpremise-deployer_linux</code> . Сервис предоставляет веб-интерфейс установщика, используемый как при первичной установке, так и при дальнейшей настройке и обслуживании Системы (обновление лицензии, обновление SSL-сертификатов, включение дополнительных продуктовых опций, настройки компонентов и интеграций)
Calico	Компонент, отвечающий за сетевое взаимодействие между контейнерами системы, расположенными на разных серверах

Интеграции с внешними системами

Платформа VK WorkSpace предоставляет следующие интеграционные возможности:

- Интеграция с внешними почтовыми сервисами по протоколу CalDav.
- Интеграция с IDM-системами: Keycloak 17, Blitz.
- Интеграция с офисным ПО: P7-офис сервер 24.1.
- Интеграция с инструментами антивируса, антиспама, антифишинга: Kaspersky Secure Mail Gateway, KSL и другие.
- Интеграции с DLP-системами: InfoWatch Traffic Monitor.
- Интеграции с LDAP: Microsoft AD, FreeIPA, Samba DC и другие LDAP-совместимые каталоги.
- Интеграции с системами резервного копирования: Кибер Бэкап 17 и другие.

На рисунке приведена общая схема взаимодействий VK WorkSpace с внешними системами.



Общее описание взаимодействий приведено в таблице ниже:

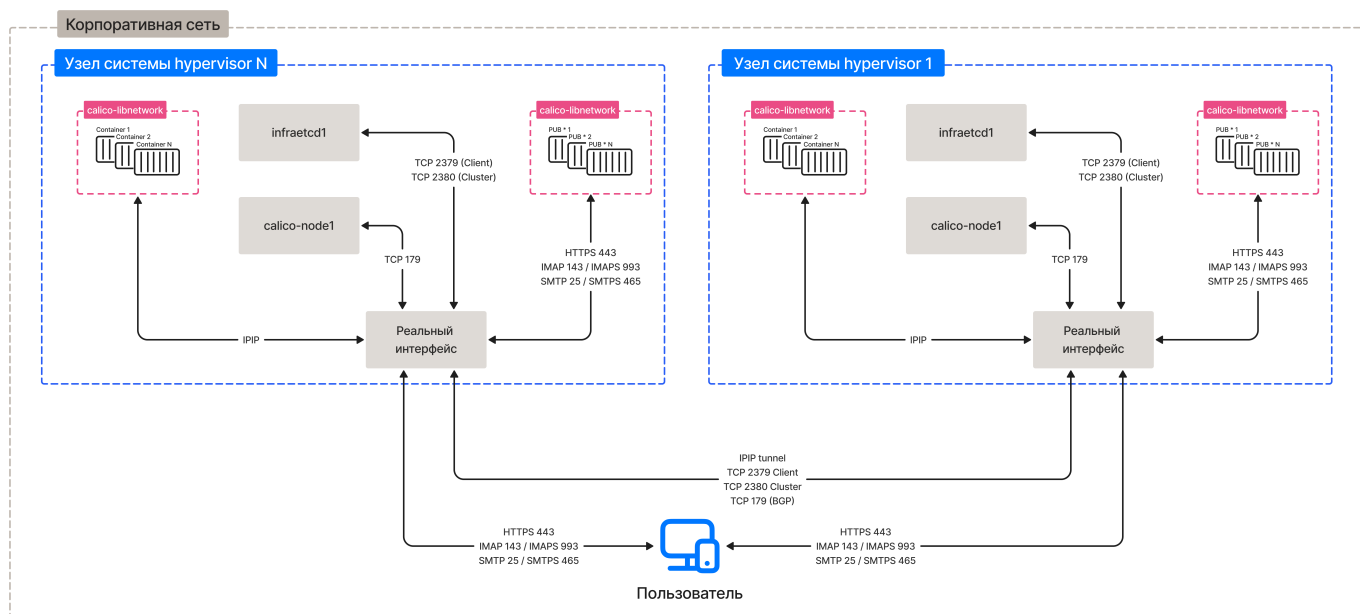
Система	Общее описание взаимодействия
IMAP-сервера	Используется для синхронизации почты по протоколу IMAP. Взаимодействие осуществляется по протоколам TCP (143, 993)
Почтовые серверы	Используется для взаимодействия с внешними почтовыми серверами для отправки/получения почты. Взаимодействие осуществляется по протоколам TCP (25, 465)
AD / LDAP	Используются для аутентификации и авторизации пользователей, осуществляется по TCP (389), UDP (636)
NTP-сервер	Используется для синхронизации времени серверов.
Антиспам, Антивирус	Используется для взаимодействия с инструментами антивируса и антиспама. Взаимодействие осуществляется по протоколу TCP (134).
DLP-система	Используется для передачи информации о событиях информационной безопасности в DLP-систему. Взаимодействие осуществляется по протоколу TCP (25)
SIEM-система	SIEM-система и(или) выделенный сервер для хранения журналов работы системы и данных аудита. Взаимодействие осуществляется по протоколу TCP/UDP (514)
DNS-сервер	Используется для получения информации о доменах. Взаимодействие осуществляется по UDP/TCP 53

Описание организации сетевого взаимодействия VK WorkSpace

VK WorkSpace работает в контейнеризированном окружении в подсети Calico. Взаимодействие между контейнерами осуществляется через закрытые IP-in-IP туннели.

Взаимодействие между контейнерами в рамках одного сервера происходит через оперативную память и производится в доверенной среде.

Общая схема организации сетевого взаимодействия приведена ниже:



Общее описание компонентов, приведенных на схеме:

Компонет	Общее описание
calico-libnetwork	Программно-конфигурируемая виртуальная сеть
calico-node1	Осуществляет маршрутизацию запросов в сети Calico между calico-libnetwork
infraetcd1	Распределенное хранилище настроек Calico
Реальный интерфейс	Физический сетевой порт на сервере

Описание взаимодействий, приведенных на общей схеме сетевого взаимодействия:

Протокол/ порт	Общее описание	Инициатор
TCP 2379	Подключение клиентов (потребителей)	Все машины и контейнеры инсталляции
TCP 2380	Общение между инстансами etcd	Взаимодействие между инстансами etcd
TCP 179	Calico. Работа BGP-сессий	Взаимодействие между всеми серверами системы
TCP 143	Подключение imap-клиентов	Пользователи
TCP 993	Подключение imap-клиентов	Пользователи
TCP 443	Подключение веб-клиентов	Пользователи
TCP 25	Подключение smtp-клиентов	Пользователи
TCP 465	Подключение smtp-клиентов	Пользователи

Сетевая инфраструктура должна обладать достаточной пропускной способностью для обеспечения работоспособности Системы. Также должна быть обеспечена сетевая связанность компонентов Системы.

Пропускная способность каналов связи

Пропускная способность для серверных компонентов кластера не ниже 10ГБит/с .

Пропускная способность для клиентских компонентов определяется экспериментально на уровне протокола IMAP, современного браузера или веб-технологий, исходя из приемлемой скорости для пользователя.

Технические требования

Поддерживаемые операционные системы для установки:

- **Astra Linux SE Опел** — версия 1.7.5+ , версия ядра 5.15.
- **РЕД ОС** — версия 7.3.5, версия ядра 6.1
- **РЕД ОС** — версия 7.3с (сертифицированная), версия ядра — 6.1.

- **MosOS Arbat** — версия 15.4, версия ядра — 5.14

Архитектура системы — **x86_64**.

Обновлять операционную систему можно только на поддерживаемую версию и только после консультации с представителем VK. Список поддерживаемых ОС может быть уточнен в рамках работ по индивидуальному проекту.

Поддерживаемые операционные системы мобильных устройств:

- **iOS** — версия 17;
- **Android** — версии 12-14.

Поддерживаемые клиентские операционные системы:

- **Microsoft Windows 10**: Google Chrome версии 126, Яндекс Браузер версии 24.

Примечание

В операционной системе **Microsoft Windows 10** веб-браузер Microsoft Edge — рекомендуется не использовать.

- **РЕД ОС**: Google Chrome версии 126, Яндекс Браузер версии 24.
- **MacOS**: Safari версии 17.5, Google Chrome версии 126, Яндекс Браузер версии 24.

 17 декабря 2025 г.