КИБЕРПРОТЕКТ

КИБЕР
Бэкап Облачный

Версия 26.07

Проектирование и типовое
развёртывание частного облака

Редакция: 01.09.2026

Оглавление

Введение

В данном руководстве описано проектирование и типовое развёртывание частного облака на основе Кибер Бэкапа Облачного в закрытом или открытом контуре.

При развёртывании частного облака на основе Кибер Бэкапа Облачного все инфраструктурные компоненты находятся в зоне ответственности эксплуатирующей организации, что обеспечивает полный контроль над системой защиты данных.

Архитектура Кибер Бэкапа Облачного

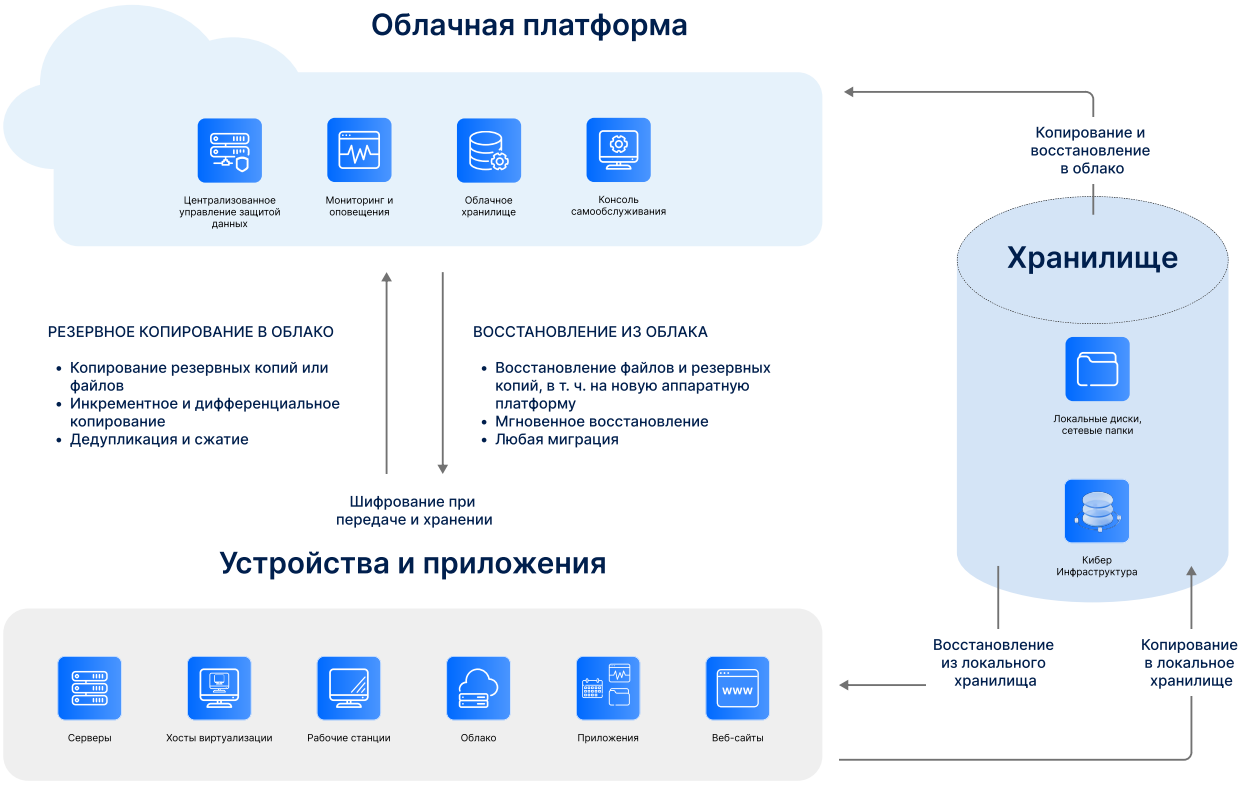
Архитектурно Кибер Бэкап Облачный основан на взаимодействии облачной платформы, агентов и хранилища резервных копий.

Облачная платформа реализует службы резервного копирования и восстановления, а также предоставляет веб-интерфейс управления (портал управления). С помощью портала управления обеспечиваются: настройка резервного копирования, управление учётными записями, мониторинг параметров и формирование отчётов. Подробнее о портале управления см. в Руководстве администратора компании.

Агенты резервного копирования устанавливаются на объекты рабочих нагрузок, с которых будут создаваться резервные копии (серверы, хосты виртуализации, рабочие станции и пр.). Агенты обеспечивают как создание резервной копии, так и восстановление из неё. После создания резервная копия передаётся в хранилище резервных копий.

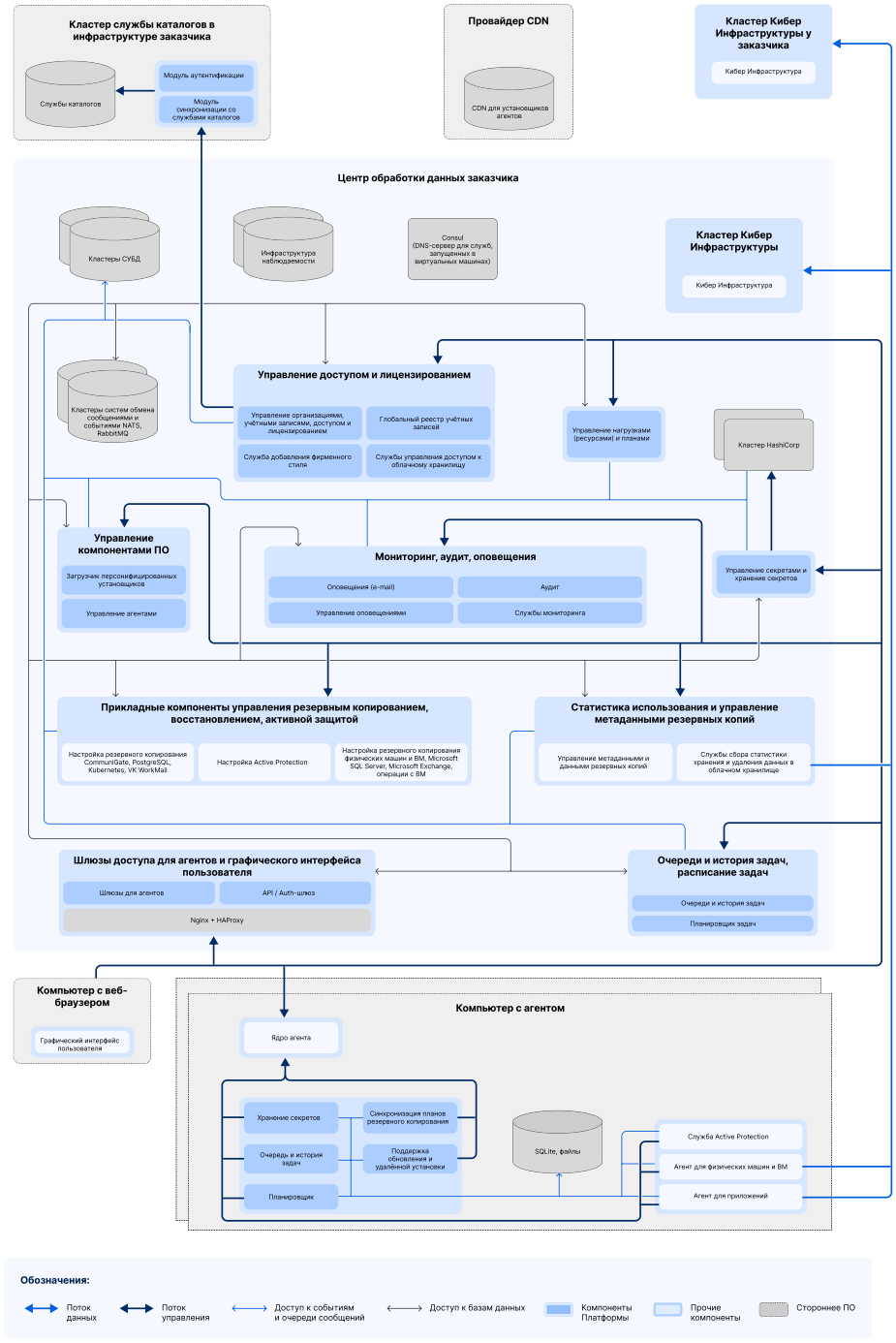
Хранилище резервных копий может быть как локальным, так и облачным или распределённым. Хранение резервных копий обеспечивается программно определяемым хранилищем Кибер Инфраструктуры.

Схема архитектуры Кибер Бэкапа Облачного приведена на рисунке.



Функциональная схема Кибер Бэкапа Облачного

Функциональная схема взаимодействия компонентов Кибер Бэкапа Облачного приведена на рисунке.



Функционирование части компонентов Кибер Бэкапа Облачного реализовано с использованием Kubernetes 1.24. Остальные компоненты функционируют в составе виртуальных машин.

Описание компонентов приведено в таблице.

Категория	Наименование	Описание
Управление доступом и лицензированием	Управление организациями, учётными записями, доступом и лицензированием	• Аутентификация пользователя в облаке, включая двухфакторную аутентификацию (2FA); • множественная аутентификация с использованием одного набора учётных данных (SSO); • реализация OAuth2 Device Flow; • API для конфигурирования тенантов и пользователей; • API для конфигурирования политик доступа; • API для конфигурирования лицензий и продуктов; • API для управления учётными записями внутренних служб и агентов, а также API ключей; • API для ручного и автоматического лицензирования, проверки возможности лицензирования; • отчёты по использованию лицензированных ресурсов и хранилища, отчёты по расписанию.
	Глобальный реестр учётных записей	• API для сопоставления учётной записи пользователя и URL ЦОД; • API для сопоставления ID тенанта и URL ЦОД.
	Служба добавления фирменного стиля	API для управления настройками добавления фирменного стиля.
	Службы управления доступом к облачному хранилищу	• API для получения и работы с сертификатами доступа к облачному хранилищу; • внутренний API, используемый облачным хранилищем для синхронизации CRL.

(продолжается на следующей странице)

(продолжение с предыдущей страницы)

Категория	Наименование	Описание
Управление нагрузками (ресурсами) и планами	Управление нагрузками (ресурсами) и планами	• API для управления нагрузками (ресурсами); • API для управления группами нагрузок; • API для управления политиками; • API для управления применением политик к нагрузкам и их группам, для запуска политик; • проверка политик, синхронизация политик для агентов, расписание политик для централизованных агентов; • отслеживание статуса политик в контексте каждой применённой нагрузки и объединение статусов; • лицензирование функций политик в контексте применённых нагрузок; • API для объединённых видов статусов нагрузок и статусов политик.
Мониторинг, аудит, оповещения	Оповещения (e-mail)	• Получение и подготовка данных для электронных писем; • формирование электронных писем из шаблонов; • отправление электронных писем по отдельным событиям, оповещениям и ежедневным сводкам.
	Управление оповещениями	• Хранилище оповещений; • API для доступа к оповещениям и управления ими.
	Аудит	• Хранилище информации о событиях аудита; • API для поиска по журналу аудита.
	Службы мониторинга	• Получение данных для мониторинга из других служб системы; • хранение информации мониторинга; • серверная часть построения виджетов и отчётов мониторинга по расписанию.
Управление секретами	Управление секретами и хранение секретов	• API для сохранения секретов пользователя; • API для генерации секретов и хэшей с помощью различных алгоритмов.

(продолжается на следующей странице)

(продолжение с предыдущей страницы)

Категория	Наименование	Описание
Управление компонентами ПО	Управление агентами	• API для регистрации и удаления регистрации агентов; • API для конфигурации агентских модулей; • синхронизация конфигураций агентских модулей с агентом; • API для хостов без агентов; • серверная часть графического интерфейса пользователя для конфигурирования удалённой установки агентов.
	Загрузчик персонифицированных установщиков	API для скачивания персонифицированных установщиков.
Очереди и история задач, расписание задач	Очереди и история задач	• API для очереди задач (помещение задачи в очередь, считывание задачи из очереди); • API для управления жизненным циклом задачи и её шагами (активностями); • API для доступа и поиска задач.
	Планировщик задач	• API для планирования задач (для централизованных агентов); • вызов HTTP-оповещений по расписаниям.
Шлюзы доступа для агентов и графического интерфейса пользователя	Шлюзы для агентов	• Приём и поддержание соединений от агентов; • синхронизация с агентами части политик резервного копирования, нагрузок (ресурсов), шагов выполнения задач, метаданных резервных копий; • перенаправление команд и HTTP-запросов от централизованных служб к агентам.
	API / Auth-шлюз	• Управление пользовательскими сессиями для интерфейса веб-консоли резервного копирования; • аутентификация входящих API-запросов (проверка токенов доступа, их обмен, кэширование).

(продолжается на следующей странице)

(продолжение с предыдущей страницы)

Категория	Наименование	Описание
Прикладные компоненты управления резервным копированием, восстановлением, активной защитой	Настройка резервного копирования физических и виртуальных машин, Microsoft SQL Server, Microsoft Exchange, операции с виртуальными машинами	• Проверка политик резервного копирования физических и виртуальных машин, Microsoft SQL Server, Microsoft Exchange; • различные операции с виртуальными машинами, включая восстановление из резервной копии.
	Настройка Active Protection	Проверка политик Active Protection.
	Настройка резервного копирования CommuniGate, PostgreSQL, Kubernetes, VK WorkMail	Проверка политик резервного копирования CommuniGate, PostgreSQL, Kubernetes, VK WorkMail.
Статистика использования и управление метаданными резервных копий	Управление метаданными и данными резервных копий	• API для управления метаданными резервных копий (директории хранения резервных копий, файлы с архивами резервных копий и сами резервные копии); • API для управления данными резервных копий на агентах (в т. ч. перечитать содержимое директории с резервными копиями, удалить файлы с резервными копиями и отдельные резервные копии); • удаление данных пользователя в облачном хранилище при удалении пользователя.
	Службы сбора статистики хранения и удаления данных в облачном хранилище	Вычисление объёмов резервных копий, хранящихся в облачном хранилище, для каждой учётной записи пользователя.

Сетевые соединения

Базовая конфигурация сетевых соединений серверов и кластеров, необходимых для развёртывания Кибер Бэкапа Облачного в частном облаке, зависит от используемого варианта:

- с отдельными кластерами вычислений и хранения резервных копий (рекомендуемый вариант для промышленной эксплуатации);
- с гибридным кластером, совмещающим функции вычислений и хранения резервных копий.

Соответствующие схемы сетевых соединений приведены на рисунках ниже.

Схема для варианта с отдельными кластерами вычислений и хранения резервных копий

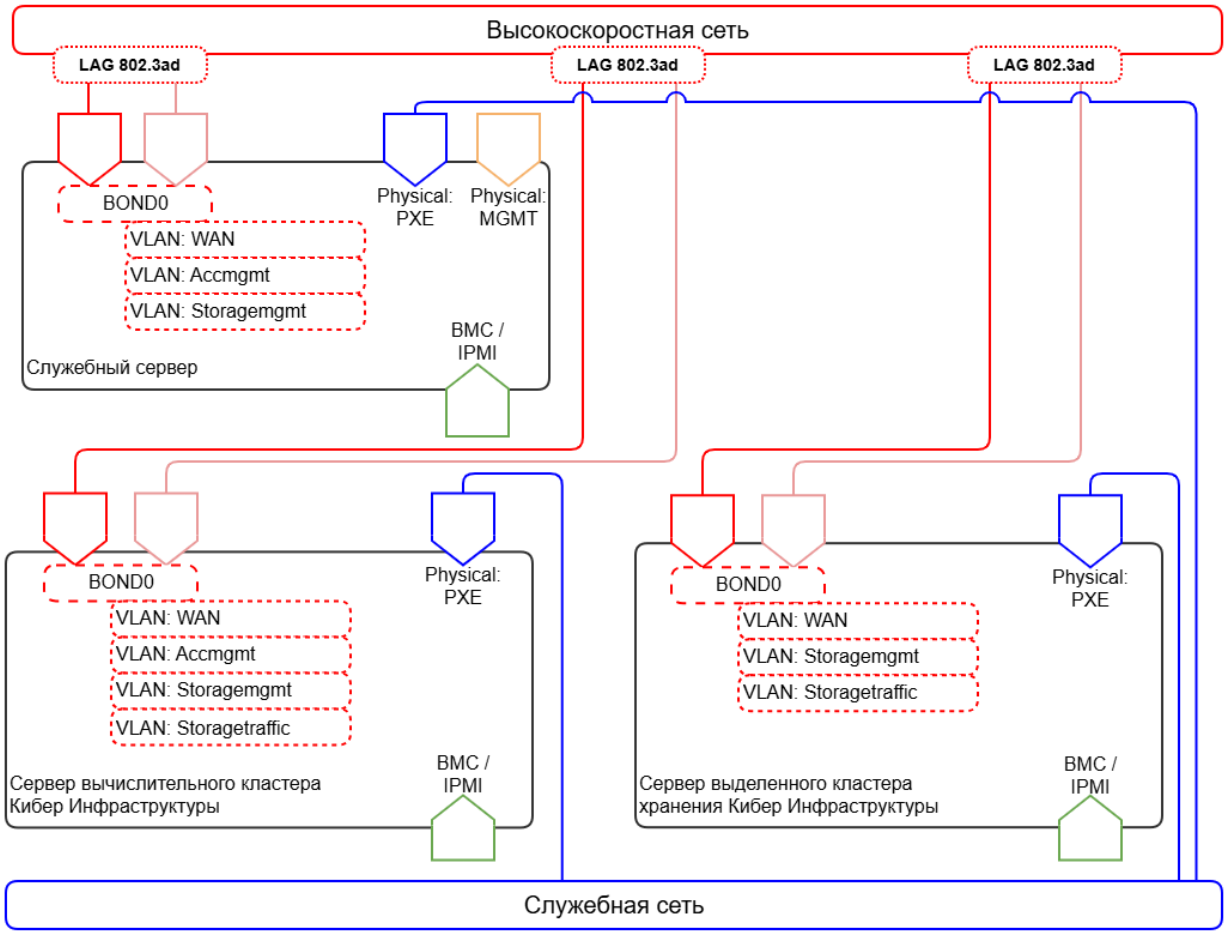
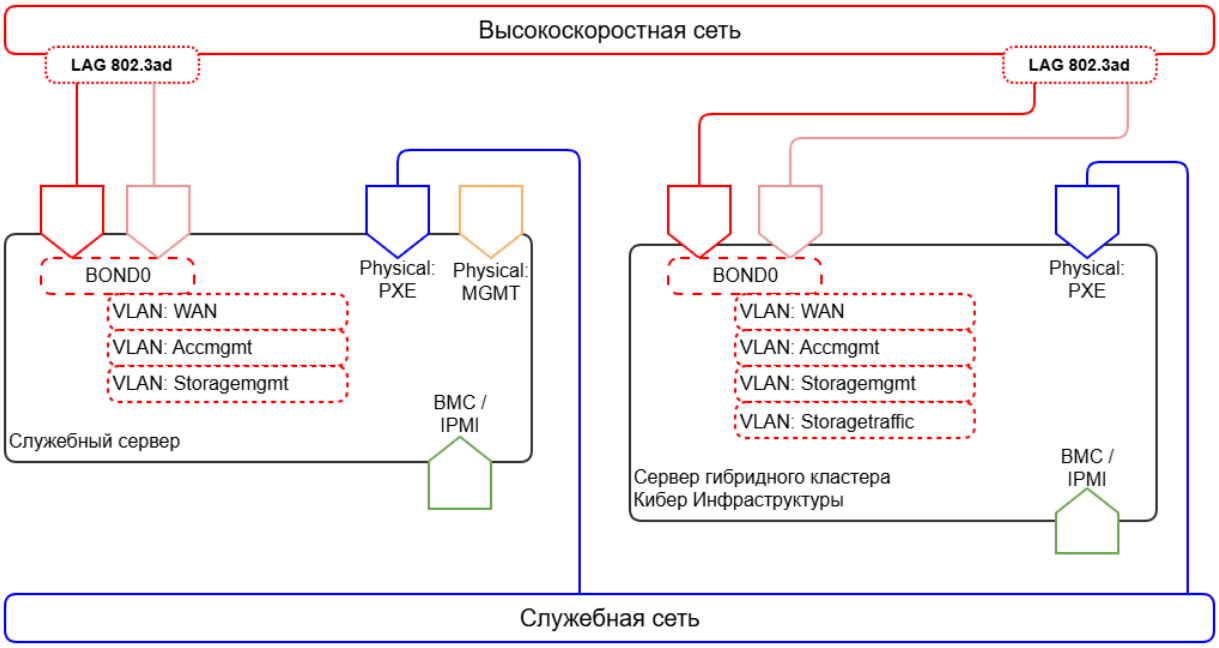


Схема для варианта с гибридным кластером



Описание обозначенных на рисунках элементов схем приведено далее.

Сети

- **Высокоскоростная сеть** — сеть, предназначенная для передачи данных между Кибер Инфраструктурой и Кибер Бэкапом Облачным на высокой скорости (от 10 Гб/с и выше) с минимальными задержками (до 100 мкс).
- **Служебная сеть** — сеть, предназначенная для установки и развёртывания служебного сервера, Кибер Инфраструктуры и других компонентов стенда, а также для управления Кибер Инфраструктурой и служебным сервером при сбоях высокоскоростной сети.

Серверы

- **Служебный сервер** — сервер, предназначенный для размещения служб, необходимых для автоматизации процессов подготовки Кибер Инфраструктуры и Кибер Бэкапа Облачного, хранения данных, используемых в процессах автоматизации, а также для маршрутизации трафика между сетями стенда и других инфраструктурных задач.
- **Сервер вычислительного кластера** — сервер кластера Кибер Инфраструктуры, в котором разворачивается вычислительный кластер (средства виртуализации) и не разворачивается шлюз Backup Gateway.
- **Сервер кластера хранения** — сервер кластера Кибер Инфраструктуры, в котором разворачивается только шлюз Backup Gateway.

- **Сервер гибридного кластера** — сервер кластера Кибер Инфраструктуры, в котором разворачивается и вычислительный кластер (средства виртуализации), и шлюз Backup Gateway.

> **Примечание**
>
> Для эксплуатации в промышленных условиях рекомендуется использовать отдельные кластеры для вычислений и хранения резервных копий вместо гибридного кластера.

Интерфейсы

- **LAG 802.3ad** — объединение физических портов в режиме ”Активный-Активный” на сетевом оборудовании. Параметры объединения:
  - miimon=100;
  - mode=802.3ad;
  - lacp_rate=fast;
  - xmit_hash_policy=layer2+3.
- **Bond0** — группа объединённых физических портов в режиме ”Активный-Активный” в Linux-подобных операционных системах. Параметры объединения:
  - miimon=100;
  - mode=802.3ad;
  - lacp_rate=fast;
  - xmit_hash_policy=layer2+3.

> **Примечание**
>
> Для промышленной эксплуатации стенда в группы объединённых физических портов **LAG 802.3ad** и **Bond0** должно быть включено не менее двух физических портов. Включение в вышеуказанные группы по одному физическому порту допустимо только для тестовых и аналогичных сред.

- **VLAN: WAN** — развёрнутый поверх группового интерфейса **bond0** виртуальный интерфейс в выделенной сети **WAN**. Данная сеть является маршрутизируемой и предназначена для взаимодействия агентов резервного копирования и пользователей веб-консоли с Кибер Бэкапом Облачным.

  В сети **WAN** назначаются IP-адреса:

- служб, принимающих внешние подключения;
- шлюза Backup Gateway;
- внутреннего репозитория;
- служебного сервера.

Для сети **WAN** требуется не менее 30 доступных IP-адресов, не включая служебные (сеть с префиксом 27).

- **VLAN: Accmgmt** — развёрнутый поверх группового интерфейса **bond0** виртуальный интерфейс в выделенной сети **Accmgmt**. Данная сеть предназначена для взаимодействия виртуальных машин Кибер Бэкапа Облачного.

  Сеть **Accmgmt** может быть маршрутизируемой для обеспечения прямого доступа из внутренних сетей к виртуальным машинам Кибер Бэкапа Облачного (например, для обслуживания и диагностики при сбоях). Маршрутизация для данной сети не является обязательной.

  Для сети **Accmgmt** требуется не менее 254 доступных IP-адресов, не включая служебные (сеть с префиксом 24).

- **VLAN: Storagemgmt** — развёрнутый поверх группового интерфейса **bond0** виртуальный интерфейс в выделенной сети **Storagemgmt**. Данная сеть предназначена для взаимодействия управляющих служб кластера Кибер Инфраструктуры (в том числе компонентов управления шлюза Backup Gateway).

  Сеть **Storagemgmt** может быть маршрутизируемой для обеспечения прямого доступа из внутренних сетей к виртуальным машинам Кибер Бэкапа Облачного (например, для обслуживания и диагностики при сбоях). Маршрутизация для данной сети не является обязательной.

  Для сети **Storagemgmt** требуется не менее 254 доступных IP-адресов, не включая служебные (сеть с префиксом 24).

- **VLAN: Storagetraffic** — развёрнутый поверх группового интерфейса **bond0** виртуальный интерфейс в выделенной сети **Storagetraffic**. Данная сеть предназначена только для внутреннего трафика программно определяемого хранилища (SDS) Кибер Инфраструктуры.

  > **Примечание**
  >
  > Интерфейсы в сети **Storagetraffic** настраиваются только на серверах Кибер Инфраструктуры и не настраиваются на служебных серверах.

  Сеть **Storagetraffic** не должна быть маршрутизируемой.

Для данной сети требуется не менее 254 доступных IP-адресов, не включая служебные (сеть с префиксом 24).

> **Примечание**
>
> Количество IP-адресов в сети **Storagetraffic** должно соответствовать количеству IP-адресов в сети **Storagemgmt**.

- **Physical: PXE** — физический интерфейс в выделенной сети **PXE**. Данная сеть предназначена для первичной установки и настройки служебных серверов и серверов Кибер Инфраструктуры.

  Сеть **PXE** может быть маршрутизируемой для обеспечения резервного прямого доступа из внутренних сетей к служебному серверу и серверам Кибер Инфраструктуры. Маршрутизация для данной сети не является обязательной.

  Для данной сети требуется не менее 254 доступных IP-адресов, не включая служебные (сеть с префиксом 24).

- **Physical: MGMT** — физический интерфейс в выделенной сети **MGMT**. Данная сеть используется для подключения к служебному серверу до запуска его автоматической настройки. IP-конфигурация интерфейса **MGMT** может быть получена как через внутренний DHCP-сервер эксплуатирующей организации, так и настроена вручную. Системное наименование данного интерфейса указывается в качестве резервного при заполнении формы первичных настроек стенда.

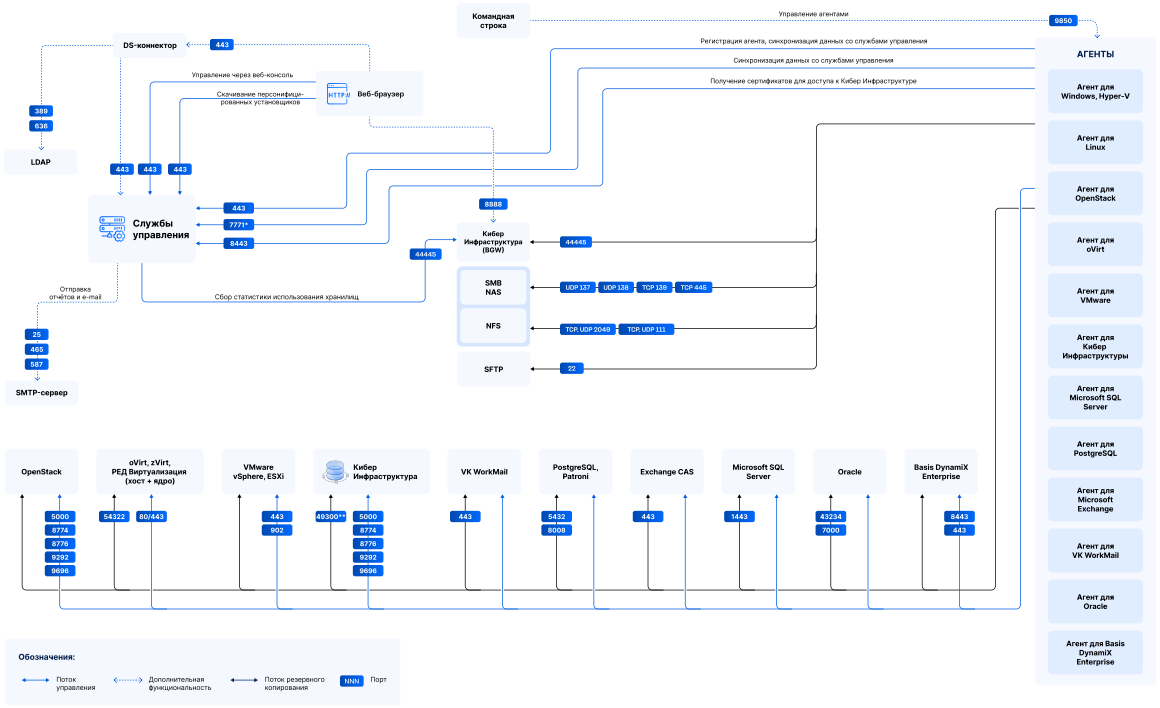
  Интерфейс сети **MGMT** может быть заменён аналогичным интерфейсом в сети **PXE**. В этом случае при заполнении формы первичных настроек стенда укажите системное наименование интерфейса **PXE** в качестве резервного и вручную настройте его IP-конфигурацию.

  > **Примечание**
  >
  > В этой сети интерфейсы настраиваются только на служебных серверах; настройка интерфейсов на серверах Кибер Инфраструктуры не предусмотрена.

- **BMC/IPMI** — интерфейсы серверов для удалённого управления, настраиваются эксплуатирующей организацией. Средства автоматизации установки и настройки служебного сервера, Кибер Инфраструктуры и Кибер Бэкапа Облачного для стендов частного облака не используют эти интерфейсы.

Сетевое взаимодействие

Сетевое взаимодействие основных компонентов Кибер Бэкапа Облачного показано на схеме.



В целях безопасности рекомендуется закрыть все порты, кроме перечисленных ниже.

В таблицах перечислены порты, необходимые для внешнего подключения к компонентам продукта.

Службы управления

Тип	Порт	Источник подключения	Протокол	Описание
Компонент **Службы управления**				
Входящее	443	Веб-консоль Агенты DS-коннектор	TCP	Веб-консоль сервера управления и шлюз API-запросов. Регистрация компонентов. Обмен информацией с агентами.
Входящее	8443	Агенты	TCP	Получение сертификатов для доступа к Кибер Инфраструктуре.

(продолжается на следующей странице)

(продолжение с предыдущей страницы)

Тип	Порт	Источник подключения	Протокол	Описание
Входящее	7771[1]	Агенты	TCP	Шлюз ZeroMQ для подключения и обмена информацией с агентами. Основной трафик от агентов.
Компонент **Агент для Windows/Hyper-V**				
Входящее	9850	Запросы через интерфейс командной строки	TCP	Работа с интерфейсом командной строки.
Компонент **Агент для Linux**				
Входящее	9850	Запросы через интерфейс командной строки	TCP	Работа с интерфейсом командной строки.
Компонент **Агент для виртуальных машин (VMware, oVirt)**				
Входящее	9850	Запросы через интерфейс командной строки	TCP	Работа с интерфейсом командной строки.
Компонент **DS-коннектор**				
Входящее	443	Веб-консоль	TCP	Форма входа через LDAP.

Хранилища

Тип	Порт	Источник подключения	Протокол	Описание
Компонент **Кибер Инфраструктура (BGW)**				
Входящее	8888	Веб-браузер администратора	TCP	Веб-консоль управления.
Входящее	44445	Агенты Сервер управления	TCP	Загрузка и выгрузка резервных копий.
Компонент **Сетевая папка SMB/NAS**				
Входящее	139	Агенты	TCP	Загрузка и выгрузка резервных копий.
Входящее	445	Агенты	TCP	Загрузка и выгрузка резервных копий.
Входящее	137	Агенты	UDP	Загрузка и выгрузка резервных копий.

(продолжается на следующей странице)

[1] Используются порты из диапазона 7771—7780. Количество открытых портов зависит от количества используемых виртуальных машин со службами управления, для каждой из них должен быть открыт свой порт из указанного диапазона. В минимальной конфигурации используется две виртуальные машины со службами управления, для них должны быть открыты порты 7771 и 7772.

(продолжение с предыдущей страницы)

Тип	Порт	Источник подключения	Протокол	Описание
Входящее	138	Агенты	UDP	Загрузка и выгрузка резервных копий.
Компонент **Сетевая папка NFS**				
Входящее	111	Агенты	TCP UDP	Загрузка и выгрузка резервных копий.
Входящее	2049	Агенты	TCP UDP	Загрузка и выгрузка резервных копий.
Компонент **Сетевая папка SFTP**				
Входящее	22	Агенты	TCP	Загрузка и выгрузка резервных копий.

Виртуализация

Тип	Порт	Источник подключения	Протокол	Описание
Компонент **VMware vSphere и ESXi**				
Входящее	902	Агент для VMware	TCP	Управляющие команды от агента.
Входящее	443	Агент для VMware	TCP	Управляющие команды от агента.
Компонент **oVirt, zVirt Engine, РЕД Виртуализация (хост)**				
Входящее	54322	Агент для oVirt	TCP	Передача агенту данных с дисков ВМ при включенном CBT. Передача ядру гипервизора образа виртуального устройства.
Компонент **oVirt, zVirt Engine, РЕД Виртуализация (ядро)**				
Входящее	80	Агент для oVirt	TCP	Управляющие команды от агента.
Входящее	443	Агент для oVirt	TCP	Управляющие команды от агента.
Компонент **OpenStack**				
Входящее	5000	Агент для OpenStack	TCP	Управляющие команды от агента.
Входящее	8774	Агент для OpenStack	TCP	Управляющие команды от агента.
Входящее	8776	Агент для OpenStack	TCP	Управляющие команды от агента.

(продолжается на следующей странице)

(продолжение с предыдущей страницы)

Тип	Порт	Источник подключения	Протокол	Описание
Входящее	9292	Агент для OpenStack	TCP	Управляющие команды от агента.
Входящее	9696	Агент для OpenStack	TCP	Управляющие команды от агента.
Компонент **Кибер Инфраструктура**				
Входящее	5000	Агент для Кибер Инфраструктуры	TCP	Управляющие команды от агента.
Входящее	8774	Агент для Кибер Инфраструктуры	TCP	Управляющие команды от агента.
Входящее	8776	Агент для Кибер Инфраструктуры	TCP	Управляющие команды от агента.
Входящее	9292	Агент для Кибер Инфраструктуры	TCP	Управляющие команды от агента.
Входящее	9696	Агент для Кибер Инфраструктуры	TCP	Управляющие команды от агента.
Входящее	49300[2]	Агент для Кибер Инфраструктуры	TCP	Передача данных с дисков виртуальной машины.
Компонент **Basis DynamiX Enterprise**				
Входящее	443	Агент для Basis DynamiX Enterprise	TCP	Управляющие команды от агента.
Входящее	8443	Агент для Basis DynamiX Enterprise	TCP	Управляющие команды от агента.

Приложения

Тип	Порт	Источник подключения	Протокол	Описание
Компонент **Microsoft Exchange CAS**				
Входящее	443	Агенты для Microsoft Exchange (почтовые ящики)	TCP	Загрузка и выгрузка содержимого почтовых ящиков.
Компонент **PostgreSQL и Patroni**				
Входящее	5432	Агент для PostgreSQL	TCP	Выгрузка содержимого экземпляра БД.
Входящее	8008	Агент для PostgreSQL	TCP	API службы управления кластером PostgreSQL.
Компонент **Почта VK WorkMail**				

(продолжается на следующей странице)

[2] Используются динамические порты из диапазона 49300—65635.

(продолжение с предыдущей страницы)

Тип	Порт	Источник подключения	Протокол	Описание
Входящее	443	Агент для VK WorkMail	TCP	Загрузка и выгрузка содержимого почтовых ящиков и хранилища Диск VK WorkSpace.
Компонент **Microsoft SQL Server**				
Входящее	1443	Агент для Microsoft SQL Server	TCP	Работа с Windows Cluster API (для AAG) или через ODBC.
Компонент **Oracle**				
Входящее	43234	Агент для Oracle	TCP	Работа с Oracle Restore Tool.
Входящее	7000	Агент для Oracle	TCP	Работа с RMAN.

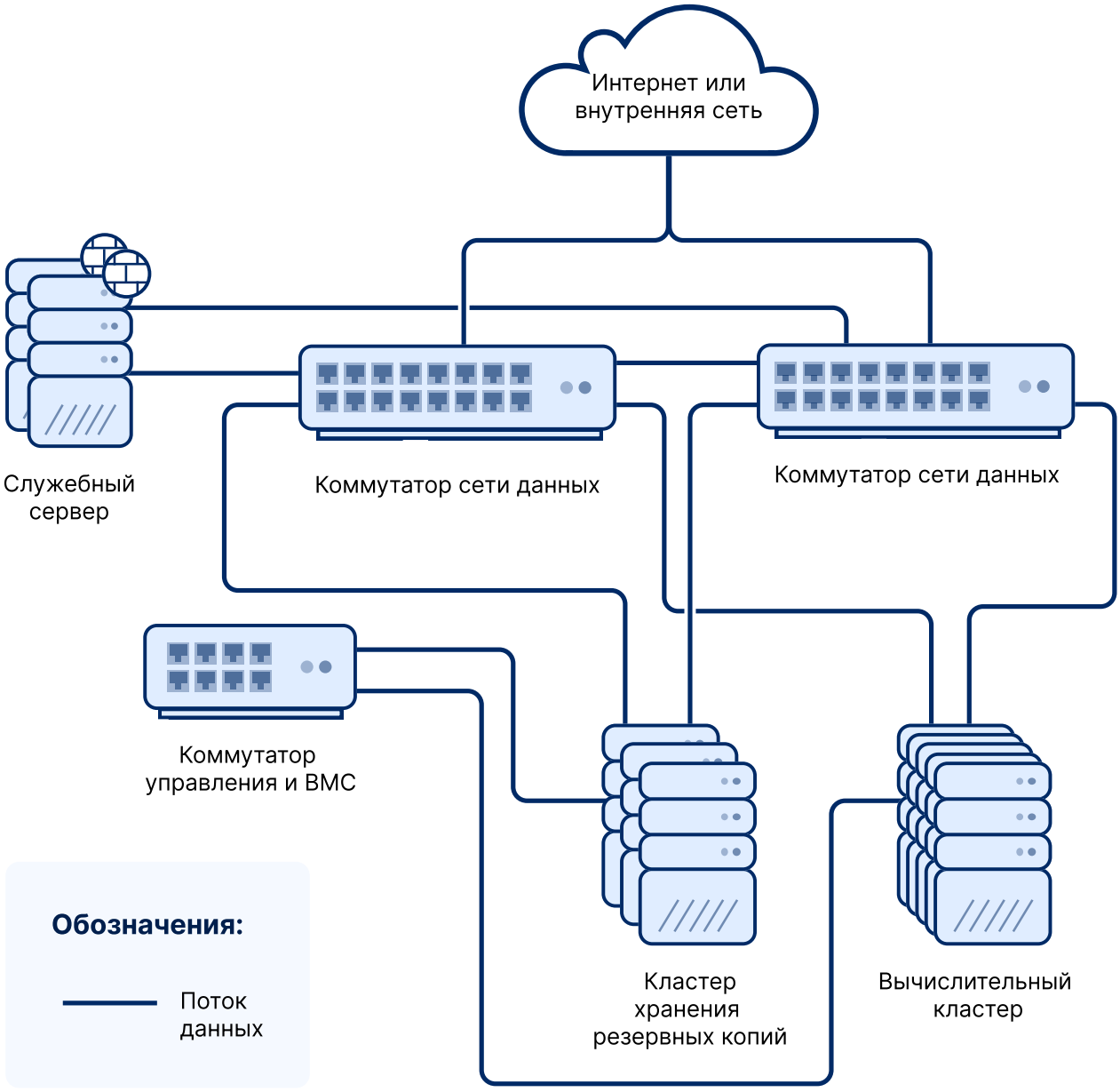
Базовая инфраструктура

Раздельные кластеры вычислений и хранения резервных копий

Состав базовой инфраструктуры для развёртывания частного облака на основе Кибер Бэкапа Облачного с использованием раздельных кластеров вычислений и хранения резервных копий приведён в таблице.

Обозначение	Оборудование	Характеристики	Количество, шт.
Вычислительный кластер	Сервер Yadro VEGMAN R220 G2	• 2x Intel Xeon Gold 6342, • 16x 32 ГБ RAM DDR4-3200 МГц ECC, • 2x M.2 SSD 1024 ГБ, • 8x U.2 SSD 980 ГБ, • Nvidia MCX512A-ACAT.	5
Служебный сервер	Сервер Yadro X3-105	• 1x Intel Xeon 4314, • 4x 16 ГБ RAM DDR4-2667 МГц, • 2x M.2 SSD 1024 ГБ, • 2x SATA SSD 1920 ГБ, • 2x SATA HDD 4 ТБ, • Nvidia MCX512A-ACAT.	2
Кластер хранения резервных копий	См. раздел *Подключение хранилища резервных копий*.		
Коммутатор сети данных		• 10/25G, • LACP, • SFP28+.	2
Коммутатор управления		• 1G BASE-T, • BMC.	1

Схема базовой инфраструктуры частного облака на основе Кибер Бэкапа Облачного с использованием раздельных кластеров вычислений и хранения резервных копий приведена на рисунке.

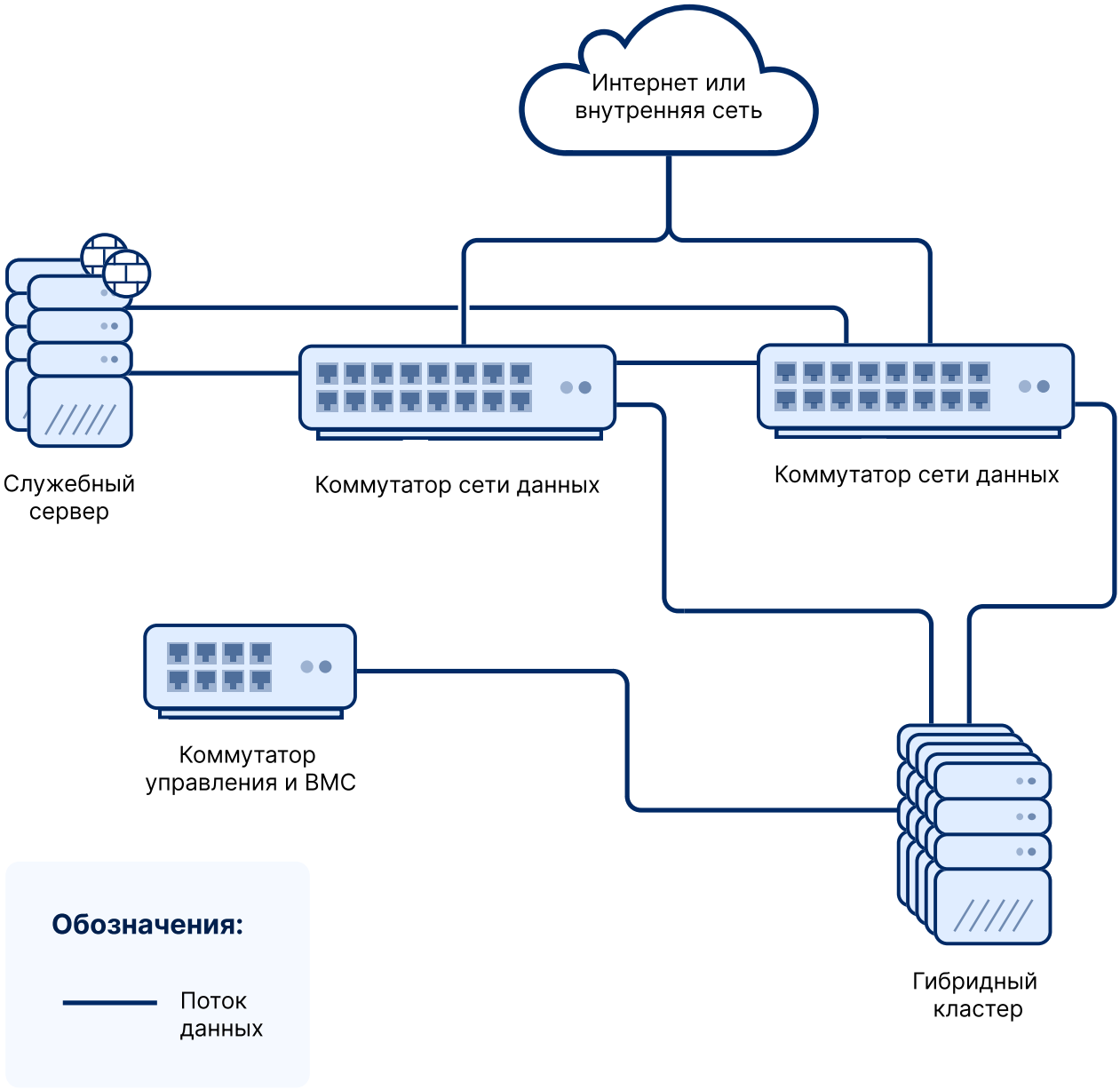


Совмещённое (гибридное) хранение и вычисления

Состав базовой инфраструктуры для развёртывания частного облака на основе Кибер Бэкапа Облачного с использованием гибридного кластера приведён в таблице.

Обозначение	Оборудование	Характеристики	Количество, шт.
Гибридный кластер	Сервер Yadro Vegman R220 G2	• 2x Intel 6342, • 16x 32 ГБ RAM DDR4-3200 МГц ECC, • 2x 512 ГБ M.2 SSD, • 4x 1,92 ГБ U.2 SSD, • 8x 20 ТВ HDD, • Nvidia MCX512A-ACAT.	5
Служебный сервер	Сервер Yadro X3-105	• 1x Intel Xeon 4314, • 4x 16 ГБ RAM DDR4-2667 МГц, • 2x M.2 SSD 1024 ГБ, • 2x SATA SSD 1920 ГБ, • 2x SATA HDD 4 ТБ, • Nvidia MCX512A-ACAT.	2
Коммутатор сети данных		• 10/25G, • LACP, • SFP28+.	2
Коммутатор управления		• 1G BASE-T, • BMC.	1

Схема базовой инфраструктуры частного облака на основе Кибер Бэкапа Облачного с использованием гибридного кластера приведена на рисунке.



Назначение серверов

Функции служебного сервера:

- запуск частного облака на основе Кибер Бэкапа Облачного;
- обновление ПО;
- поддержка функционирования частного облака на основе Кибер Бэкапа Облачного.

Функции сервера вычислительного кластера:

- создание виртуальных машин;
- запуск программных компонентов;

- обеспечение работы компонентов Кибер Инфраструктуры;
- шифрование данных средствами Кибер Инфраструктуры (подробнее см. в Руководстве администратора Кибер Инфраструктуры).

Функции сервера кластера хранения резервных копий:

- хранение резервных копий;
- шифрование данных средствами Кибер Инфраструктуры (подробнее см. в Руководстве администратора Кибер Инфраструктуры).

Серверы кластеров баз данных обеспечивают хранение служебных данных платформы и используются при масштабировании (подробнее см. в разделе *Масштабирование*).

Серверы гибридного кластера выполняют как функции вычислительного кластера, так и функции кластера хранения резервных копий.

Примечание

Для промышленной эксплуатации рекомендуется использовать отдельные кластеры вычислений и хранения резервных копий.

Подключение хранилища резервных копий

Состав кластера хранения резервных копий зависит от целевого объёма полезного места хранилища.

Примечание

Рекомендуемые диски для хранилища резервных копий:

- Western Digital серии Ultrastar DC HC5xx,
- Seagate серии Exos X.

Ниже в таблице приведены примеры конфигурации хранилищ резервных копий и указан ориентировочный размер хранилища для рассматриваемых вариантов.

Вариант	Оборудование	Характеристики	Количество, шт.	Объём места хранения резервных копий (ориентировочно)	Схема кодирования[с. 24, 1]
1	Сервер Yadro X3-205	• 1x Intel Xeon 4314, • 4x 16 ГБ RAM DDR4-2667 МГц, • 2x M.2 SSD 128 ГБ, • 12x SATA HDD 18 ТБ, • Nvidia MCX512A-ACAT.	7[2]	750 ТБ	5+2
2	Сервер Yadro X3-205	• 2x Intel Xeon 4314, • 4x 16 ГБ RAM DDR4-2667 МГц, • 2x M.2 SSD 128 ГБ, • 12x SATA HDD 18 ТБ, • LSI HBA 9300-8e, • Nvidia MCX512A-ACAT.	10	2,4 ПБ	7+2

(продолжается на следующей странице)

(продолжение с предыдущей страницы)

Вариант	Оборудование	Характеристики	Количество, шт.	Объём места хранения резервных копий (ориентировочно)	Схема кодирования[1]
	Дисковый модуль расширения L12	• 12x SATA HDD 18 ТБ в модуле L12	10		
3	Сервер Yadro X3-105	• 2x Intel Xeon 4314, • 8x 16GB RAM DDR4-2667 МГц, • 2x M.2 SSD 256 ГБ, • LSI HBA 9300-8e, • Nvidia MCX512A-ACAT.	10	7,9 ПБ	7+2
	Дисковый модуль расширения L78	• 78x SATA HDD 18 ТБ в модуле L78	10		

[1] Подробнее о схеме кодирования см. в Руководстве администратора Кибер Инфраструктуры.

[2] Для обеспечения оптимального баланса между производительностью, отказоустойчивостью и накладными расходами на хранение данных не рекомендуется использовать меньшее количество узлов. В противном случае достижение оптимальных значений указанных характеристик может быть затруднено или невозможно.

Масштабирование

Масштабирование заключается в добавлении к базовой инфраструктуре дополнительных серверов вычислительного кластера, кластера базы данных Percona или кластера базы данных Patroni для увеличения количества поддерживаемых агентов и учётных записей. Под учётными записями понимаются учётные записи пользователей или тенантов (подробее см. в Руководстве администратора партнёра).

Примечание

В этом разделе под агентами подразумеваются агенты, выполняющие защиту физического сервера. При использовании образа виртуальной машины для работы в среде виртуализации (т. н. virtual appliance) или агента для VK WorkMail или Microsoft Exchange нагрузка на сервер управления больше, чем при использовании агента, выполняющего защиту физического сервера, а количество поддерживаемых агентов при этом — меньше.

Зависимость количества поддерживаемых агентов и учётных записей от конфигурации инфраструктуры частного облака на основе Кибер Бэкапа Облачного приведена в таблице.

Количество серверов, шт.				**Максимальное количество агентов, тыс. шт.**	**Максимальное количество учётных записей, тыс. шт.**
Вычислитель-ный кластер	Служебный сервер	Кластер БД Percona	Кластер БД Patroni		
5	2	—	—	25	25
7	2	—	—	50	50
7	2	3	—	100	100
7	2	3	3	130 - 140	130 - 140
10	2	3	3	200	200

Примечание

При добавлении серверов в кластер базы данных Percona или Patroni требуется миграция баз данных из вычислительного кластера на добавляемые серверы.

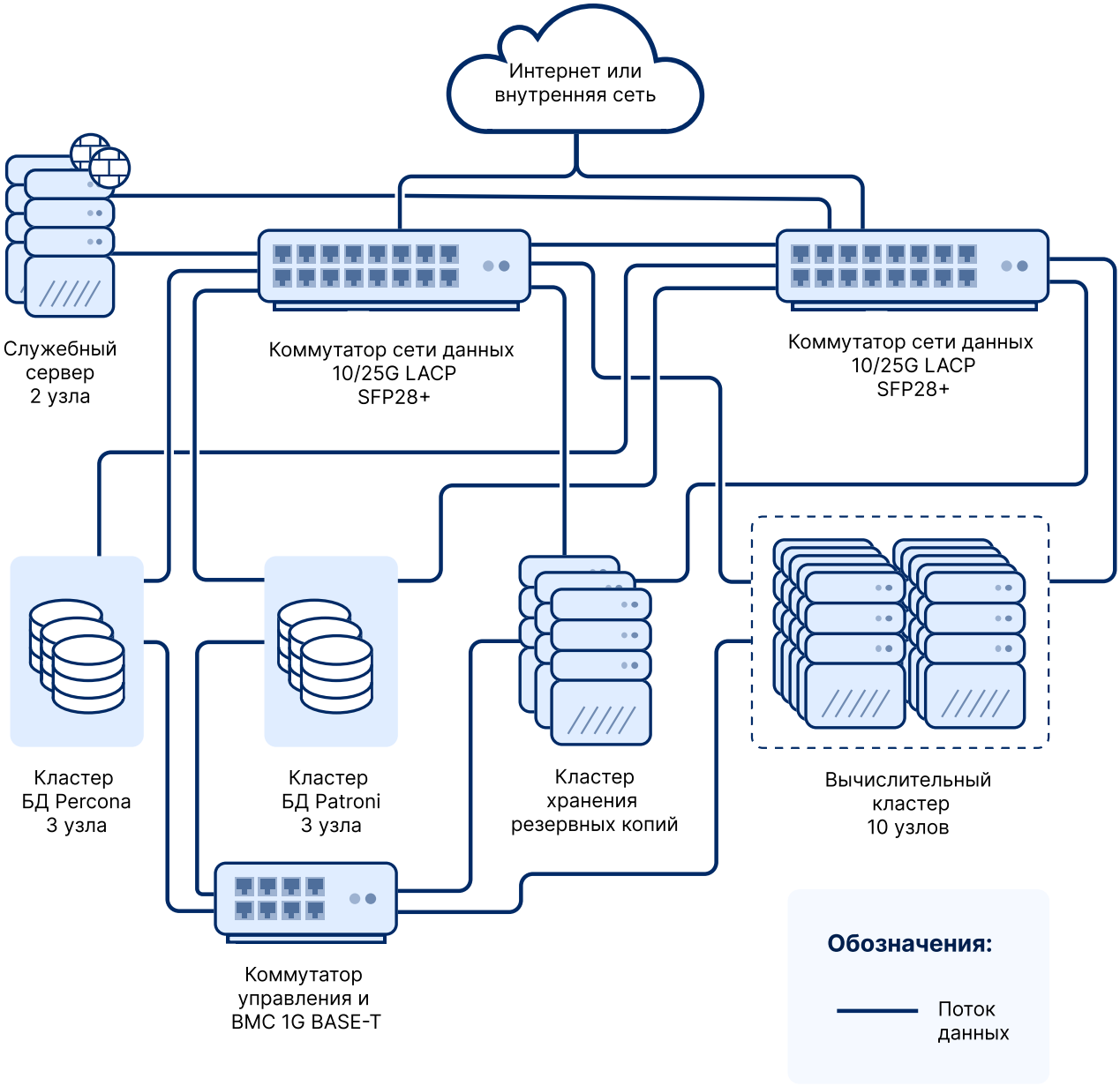
Важно

Масштабирование для поддержки свыше 200 тысяч агентов или учётных записей в рамках одной инфраструктуры не рекомендуется.

Характеристики серверов для кластера базы данных Percona или кластера базы данных Patroni приведены в таблице.

Обозначение	Оборудование	Характеристики	Количество, шт.
Кластер БД Percona	Сервер Yadro VEGMAN R220 G2	• 2x Intel Xeon Gold 6342, • 16x 32 ГБ RAM DDR4-3200 МГц ECC, • 2x M.2 SSD 1024 ГБ, • 8x U.2 SSD 980 ГБ, • Nvidia MCX512A-ACAT.	0 - 3
Кластер БД Patroni	Сервер Yadro VEGMAN R220 G2	• 2x Intel Xeon Gold 6342, • 16x 32 ГБ RAM DDR4-3200 МГц ECC, • 2x M.2 SSD 1024 ГБ, • 8x U.2 SSD 980 ГБ, • Nvidia MCX512A-ACAT.	0 - 3

Схема инфраструктуры частного облака на основе Кибер Бэкапа Облачного для поддержки 200 тысяч агентов и 200 тысяч учётных записей приведена на рисунке.



В случае необходимости поддержки более 200 тысяч агентов или более 200 тысяч учётных записей требуется развёртывание дополнительного стенда. При этом допускается использование стендами общего хранилища резервных копий.