Private Cloud

v.3.0

Описание

VK Cloud

Содержание

Основная информация

Наименование

Полное наименование: Private Cloud.

Условное обозначение: Платформа.

Альтернативное (устаревшее) название, используется в реестре отечественного ПО: Mail.ru Private Cloud Enterprise.

Назначение

Private Cloud — платформа для построения частного облака в крупных компаниях и государственных учреждениях с широким выбором готовых инструментов для ИТ-специалистов со встроенными маркетплейсом приложений.

Платформа обеспечивает выполнение требований информационной безопасности, возможность масштабирования для высоконагруженных сервисов и разворачивается на любом оборудовании с архитектурой x86.

С помощью Private Cloud от VK вы можете создать собственное (частное, корпоративное) облако, для управления виртуальными ресурсами в рамках основных облачных моделей обслуживания:

- IaaS
    - Виртуальные машины.
    - Виртуальные диски.
    - Виртуальные сети.
- PaaS
    - Управляемые базы данных.
    - Кластеры Kubernetes.

- SaaS
    - Маркетплейс облачных приложений.

Пользователи Платформы могут самостоятельно создавать виртуальные ресурсы, в рамках квот проектов, гибко управлять виртуальными ресурсами, а также настраивать планы резервного копирования, шаблоны и образы.

Администраторы Платформы могут управлять пользователями, их доступом, проектами, квотами и балансом каждого из проектов, а также управлять гипервизорами и другими узлами Платформы.

При этом Платформа обеспечивает удобные интерфейсы управления, разграничение прав доступа, логирование, мониторинг, нотификацию, балансировку нагрузки между гипервизорами, отказоустойчивость, а также тарификацию и биллинг использования ресурсов.

Состав и структура

Состав

В состав Платформы входит программное обеспечение (ПО) собственной разработки, а также ПО с открытым исходным кодом.

В основе Платформы лежит программный комплекс с открытым исходным кодом OpenStack, включающий множество различных взаимосвязанных компонентов, многие из которых были доработаны или даже переделаны под нужды Платформы.

Кроме того, в состав платформы входит следующее ПО с открытым исходным кодом:

- Ceph
- Keycloak
- Zabbix
- OpenSearch
- Docker
- Драйвера для Cinder для поддержки различных СХД
- Cloud audit logs
- MiniO
- MariaDB
- Kubernetes
- ClickHouse
- HAProxy
- ZooKeeper
- Kafka
- Consul
- RabbitMQ
- Memcached
- Galera
- Percona Xtrabackup

Структура

Для удобства представления функции системы разделены на следующие функциональные блоки и подсистемы:

- Интерфейсы:
  - Подсистема потребителя облачных услуг.
  - Подсистема администрирования.
  - Подсистема установки и управления конфигурацией.
- Общие подсистемы:
  - Подсистема тарификации и биллинга.
  - Подсистема управления доступом.
  - Подсистема служебных хранилищ.
- Группа подсистем IaaS:
  - Подсистема вычислительных ресурсов.
  - Подсистема хранения данных.
  - Сетевая подсистема.
- Группа подсистем PaaS/SaaS:
  - Подсистема управляемых баз данных.
  - Подсистема управляемых контейнеров.
  - Подсистема облачных приложений.

Интеграция с внешними системами

Платформа поддерживает различные решения по интеграции в ИТ-инфраструктуру Заказчика. В том числе решения по интеграции со следующими системами:

- LDAP(S) сервера;

- SIEM;
- CMDB;
- DNS.

Интеграционные решения описаны в документации с указанием протоколов и общих подходов для их использования.

Потребительские характеристики

Надёжность

Архитектура Платформы позволяет обеспечивать высокую надёжность и отказоустойчивость Платформы и управляемых ею вычислительных ресурсов. При наличии достаточного количества аппаратных ресурсов Платформа может продолжать работату даже в условиях выхода из строя отдельных аппаратных узлов.

При необходимости могут быть настроены схемы обеспечения катастрофоустойчивости и восстановления при авариях.

Производительность

Высокая производительность вычислительных ресурсов достигается за счёт использования виртуализации на основе QEMU + KVM.

Платформа позволяет эффективно распределять нагрузку, балансируя и распределяя её между отдельными узлами. Благодаря этому имеется возможность масштабировать Платформу для решения задач практически любого масштаба.

Имеется возможность реализации High-IOPS и LLD дисковых подсистем и соответствующей их тарификации.

Платформа позволяет гибко настраивать функцию oversell для различных типов ресурсов, а также вручную или автоматически перераспределять нагрузку между узлами платформы для наилучшей производительности.

Безопасность

Платформа обладает множеством встроенных функций и механизмов безопасности.

Доступ пользователей настраивается при помощи ролевой модели управления доступом, позволяя задать различный уровень привилегий пользователю в рамках разных проектов. При этом

функции администрирования платформы недоступны пользователям даже при некорректных настройках доступа.

Основные события безопасности записываются в журналы и доступны для просмотра администраторами Платформы.

Возможна поставка Платформы в сертифицированном по требованиям ФСТЭК России варианте.

Разработчик Платформы — ВК Цифровые технологии — Ведущая российская IT-компания с безупречной репутацией.

Адаптируемость

Платформа построена на базе отечественных разработок и открытого ПО. На эксплуатацию и поддержку платформы не влияют никакие внешние факторы, кроме законодательства Российской Федерации. Это позволяет проще находить квалифицированных специалистов для обеспечения эксплуатации частного облака, построенного на базе Платформы и делает маловероятной проблему vendor lock.

Поддержка Платформы непрерывно осуществляется Разработчиком и организациями-партнёрами на территории Российской Федерации.

Платформа имеет Roadmap развития в долгосрочной перспективе. При этом у организаций, эксплуатирующих Платформу, имеется возможность влиять на этот Roadmap, исходя из своих интересов.

Исходные коды многих компонентов платформы доступны, что позволяет проще выполнять отладку и работы по интеграции со смежными системами даже без привлечения разработчика Платформы.

Имеется возможность протестировать основные технологии, используемые в Платформе при помощи публичного облака VK Cloud, имеющего общую технологическую базу с Платформой.

Описание функциональных возможностей

Подсистема потребителя облачных услуг

Подсистема потребителя облачных услуг предназначена для предоставления всех необходимых интерфейсов управления для конечных пользователей Платформы.

Она позволяет пользователям создавать виртуальные вычислительные ресурсы и управлять ими в рамках своих проектов в соответствии с имеющимися полномочиями.

Подсистема включает следующие основные сервисы:

- Портал самообслуживания — веб портал для пользователей.
- Сервис IaC — сервис Terraform, позволяющий создавать и управлять ресурсами при помощи подхода Infrastructure as Code.
- API/CLI Gateway — консольный и REST API интерфейсы для пользователей. Позволяют пользователям автоматизировать выполнение типичных операций по работе с Платформой.

Подсистема администрирования

Подсистема администрирования предназначена для предоставления основных интерфейсов, позволяющих администрировать систему.

Подсистема администрирования включает следующие сервисы:

- Портал администратора — отдельный веб-портал для администраторов Платформы.
- Сервис мониторинга — веб-портал мониторинга на основе Zabbix и соответствующие инструменты сбора данных.
- Сервис логирования — веб-портал журналирования OpenSearch и соответствующие инструменты сбора журналов.

- Журнал аудита — встроенный в Портал самообслуживания механизм отслеживания действий пользователей.

Подсистема установки и управления конфигурацией

Подсистема установки и управления конфигурацией Платформы предназначена для автоматизации процессов развёртывания Платформы в новом окружении, а также процессов обновления конфигурации или компонентов Платформы.

Подсистема вычислительных ресурсов

Подсистема вычислительных ресурсов (далее — ПВР) предназначена для управления виртуальными машинами (ВМ). Обеспечивает размещение ВМ на вычислительных узлах, а также функции управления жизненным циклом ВМ, возможность использования шаблонов/типов ВМ, образов дисков, настраивать агрегацию вычислительных узлов, правила распределения нагрузки, миграцию ВМ, резервное копирование и восстановление.

ПВР поддерживает следующие типы гостевых ОС:

- Microsoft Windows Server 2012 R2, 2016, 2019.
- Debian 10.X.
- CentOS 7.X, 8.X.
- Ubuntu Linux 18.X, 19.X, 20.X, 22.X.
- FreeBSD 10.3.
- RHEL 7.X, 8.X.
- openSUSE 42.3.

В состав дистрибутива Платформы входят дистрибутивы следующих гостевых операционных систем:

- CentOS 7.X.

- Ubuntu Linux 22.X.

Подсистема хранения данных

Подсистема хранения данных (далее — ПХД) является средством оркестрации конечных решений по блочному хранению данных. При помощи неё реализуется возможность создавать и управлять жизненным циклом виртуальный дисков.

ПХД поддерживает следующие типы конечных устройств по блочному хранению данных:

- SDS CEPH (программно-определяемое хранилище CEPH).
- iSCSI-хранилище.
- FC-хранилище.

ВАЖНО

Для хранилищ FC и iSCSI не гарантируется поддержка всех видов дисковых подсистем. В некоторых случаях может потребоваться доработка.

> ПХД поддерживает созданием моментальных снимков (snapshot) и клонирование виртуальных дисков, а также увеличение их объёма без перерыва в обслуживании.

Подсистема служебных хранилищ

Подсистема служебных хранилищ предназначена для ведения каталога образов ВМ, хранения секретов и ключей, а так же предоставления сервиса удалённого файлового хранилища.

Сетевая подсистема

Сетевая подсистема отвечает за управление всеми аспектами виртуальной сетевой инфраструктуры и обеспечивает управление жизненным циклом публичных и приватных сетей, подсетей,

виртуальных маршрутизаторов, сетевых интерфейсов виртуальных машин, групп безопасности и балансировщиков нагрузки.

Сетевая подсистема включает в себя следующие сервисы:

- Сервис программно-определяемой сети, позволяющий создавать сети и подсети с поддержкой VXLAN, DVR, NAT, DNS, DHCP.
- Сервис программной фильтрации пакетов, позволяющий гибко настраивать фильтрацию пакетов на основе групп безопасности.
- Сервис дополнительных утилит, позволяющий использовать Floating IP и балансировщики нагрузки с поддержкой протколов HTTP, HTTPS, TCP, TCP+Procy protocol и политик Round Robin, Least connection, Source IP, а также VRRP и тегов.

Подсистема управляемых баз данных

Подсистема управляемых баз данных (далее — ПУБД) предназначена для автоматизации развёртывания СУБД (DBaaS).

ПУБД позволяет развёртывать экземпляры слудующих СУБД:

- MySQL версии 5.7.
- PostgreSQL версий 11-13 в конфигурациях Single, Master-slave и Кластер.
- MongoDB версии 4.
- Redis версии 5.

ПУБД также позволяет создавать кластера СУБД и настраивать их топологию, вертикально масштабировать инстансы СУБД, управлять пользователями, подключаться к инстансам по SSH. ПУБД обеспечивает поддержку расширений и флагов, а также резервное копирование и восстановление.

Подсистема управляемых контейнеров

Подсистема управляемых контейнеров предназначена для автоматизации управления кластерами вычислительных контейнеров Kubernetes.

Подсистема управляемых контейнеров позволяет управлять жизненным циклом кластеров Kubernetes, поддерживает разные режимы развёртывания, вертикальное и горизонтальное масштабирование и систему мониторинга на базе Prometheus.

Подсистема облачных приложений

Подсистема облачных приложений предназначена для автоматизации развертывания в Платформе облачных приложений (SaaS).

Подсистема облачных приложений позволяет использовать удобный веб-интерфейс (Маркетплейс) для автоматизированной установки и настройки облачных приложений по шаблонам с возможностями их масштабирования. Поддерживаются следующие типы виртуальных устройств:

- Виртуальные машины.
- Блочные устройства.
- Сети.
- Сетевые порты.

Подсистема тарификации и биллинга

Подсистема тарификации и биллинга (далее — ПТБ) предназначена управления тарифами и учёта потребления ресурсов Платформы.

Потребление ресурсов Платформы учитывается с точностью до минуты по модели «Pay-As-You-Go» (биллинг по факту использования).

ПТБ позволяет настраивать тарифы для следующих основных типов ресурсов:

- vCPU.
- Высокопроизводительные CPU.
- RAM.
- HDD.
- Диски файловых хранилищ NFS/CIFS.
- High-IOPS SSD.
- SSD.

Кроме того, ПТБ позволяет управлять квотами (доступными ресурсами) проектов:

- Виртуальные машины.
- vCPU.
- RAM.
- Диски.
- Размер дисков.
- Диски High-IOPS SSD.
- Размер High-IOPS SSD.
- IP-адреса.
- Порты.
- Маршрутизаторы.
- Балансировщики.

- Группы безопасности.
- Правила безопасности.
- Файловые хранилища NFS/CIFS.
- Размер файловых хранилищ NFS/CIFS.
- Снимки файловых хранилищ NFS/CIFS.
- Размер снимков файловых хранилищ NFS/CIFS.
- Сети файловых хранилищ NFS/CIFS.
- Сети (networks).
- Подсети (subnets).

ПТБ обеспечивает возможность выгрузки отчётов по потреблению за отчётный период в формате xlsx.

Подсистема управления доступом

Подсистема управления доступом (далее — ПУД) предназначена для идентификации и аутентификации пользователей и администраторов Платформы, а также управления их учётными записями.

ПУД позволяет:

- Безопасно выполнять идентификацию и аутентификацию пользователей.
- Управлять учётным записями.
- Задавать требования к аутентификаторам учётных записей.
- Реализовать ролевую модель управления доступом.
- Защиту от различного вида атак.
- Интеграцию со службами LDAP(S).