UZCLOUD

Что вам не расскажет

ваш провайдер о приватном облаке

набор компромиссов между изоляцией, контролем, ценой и ответственностью

Артем Гринберг
Head of Cloud Products

Кто я

Артем Гринберг

Head of Cloud Products
UzCloud

Telegram: @argrinberg

Более 11 лет в ИТ

Последние 5 лет строил и развивал облачные сервисы

- ➔ Product Lead at Timeweb Cloud
- ➔ Technical Product Manager at MWS
- ➔ Product Manager ML/AI сервисов at HCB

Head of System Analyst, DWH Architect,

Lead Systems Integration

Сейчас в UzCloud отвечаю за развитие облачной инфраструктуры, IaaS- и PaaS-сервисов, а также managed-решений

Что такое private cloud

UZCLOUD

Выделенные ресурсы сами по себе еще не делают сервис private cloud. Нужна именно облачная модель потребления и эксплуатации — три составляющих одновременно.

Exclusive Use — Исключительное использование

Ресурсы предназначены для одной организации. Не обязательно всё физически отдельное, но модель должна быть рассчитана на исключительное использование клиентом — без конкурирующих нагрузок от других арендаторов.

Cloud-модель потребления

Self-service, API, эластичность, измеряемое потребление. Если ресурсы выдаются только через заявку, а масштабирование занимает дни — это уже не полноценный cloud-сценарий, а управляемая виртуализация.

Эксплуатационная модель

Провайдер управляет платформой, клиент — своими сервисами, данными и доступами.
Private cloud — это не только изоляция, но и понятное разделение ответственности между сторонами.

⚠ Выделенные ресурсы сами по себе еще не делают сервис private cloud.
Нужна именно облачная модель потребления и эксплуатации.

Под приватным облаком рынок продает 4 разные модели

UZCLOUD

Провайдеры используют термин «приватное облако» для принципиально разных архитектурных решений. Разница между ними критична для безопасности, производительности и стоимости.

Модель	Что это на самом деле	Ключевой признак	Уровень изоляции
1. VPC в public cloud	Логически изолированная сеть в общем облаке	Изоляция на сетевом уровне	Сеть
2. Dedicated Host / Sole-Tenant	Выделенный физический сервер под ваши VM	Изоляция на host-уровне	Хост
3. Hosted private cloud	Инфраструктура для exclusive use одной организации у провайдера	Single-tenant модель	Вся платформа
4. Hybrid cloud	Связка private + public cloud с управляемой переносимостью	Переносимость и связность	Гибрид

Спросите провайдера: к какой из этих моделей относится ваш контракт?
Ответ определяет реальный уровень изоляции, а не маркетинговое название тарифа.

Если нет self-service и elasticity — это не совсем cloud

UZCLOUD

> Если масштабирование делается тикетом, ресурсы фиксированы,
> а учета нет — это чаще «managed virtualization», а не полноценный cloud.

✅ Полноценный Cloud

- **On-demand self-service**

  Ресурс создается через portal или API без тикетов

- **Rapid elasticity**

  Масштабирование — минуты, а не дни согласования

- **Measured service**

  Прозрачный биллинг по факту потребления
  и/или за выделенный пул

⚠️ Managed Virtualization

- **Ресурсы по тикету**

  Изменение конфигурации требует заявки и ожидания

- **Фиксированные квоты**

  Нет динамического пула — всё заранее выделено и зафиксировано

- **Непрозрачный биллинг**

  Оплата за емкость без фактически выделенного пула

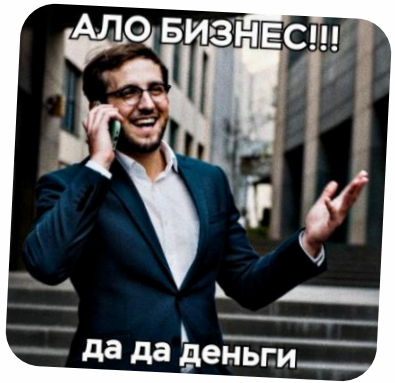
⚠ NIST прямо требует все три характеристики: on-demand self-service, rapid elasticity и measured service.
Отсутствие хотя бы одной из них означает, что вы платите за cloud, но получаете что-то другое.

Если нет self-service и elasticity — это не совсем cloud

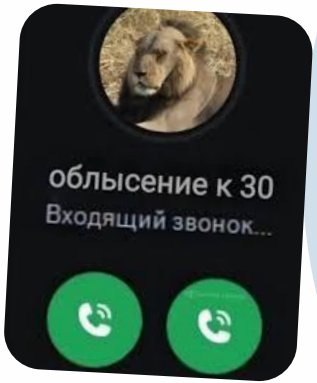
UZCLOUD

> Если масштабирование делается тикетом, ресурсы фиксированы,
> а учета нет — это чаще «managed virtualization», а не полноценный cloud.

✅ Полноценный Cloud



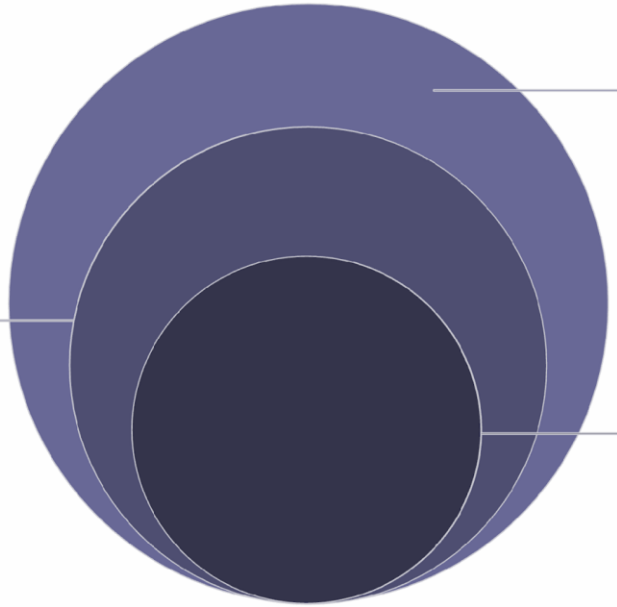
⚠️ Managed Virtualization



⚠ NIST прямо требует все три характеристики: on-demand self-service, rapid elasticity и measured service.
Отсутствие хотя бы одной из них означает, что вы платите за cloud, но получаете что-то другое.

Как выглядит реальная топология hosted private cloud

UZCLOUD



Платформенные сервисы

Виртуализация, compute, сеть, storage, управление

Инфраструктурный слой

Физические серверы, сеть хранения, дата-центр

Ядро: Сайты и регионы

Zones, Regions, DR site — dedicated/shared

Может быть shared: control plane, billing, monitoring, backup plane, storage fabric

Может быть dedicated: физические хосты, сетевые устройства, storage-узлы

Уточняйте: hypervisor-слой, планировщик, узлы Kubernetes

Производительность: vCPU и RAM — только верхушка

UZCLOUD

Провайдеры рекламируют количество ядер и объем памяти, но реальная производительность определяется ресурсами, о которых в описании тарифа часто не говорится.

CPU

Важно не количество vCPU, а политика выделения: overcommit ratio, CPU pinning, NUMA-топология и соседство нагрузок на одном физическом хосте.

RAM

Важно не только сколько памяти, но и как она резервируется: гарантия выделения, overcommit, memory ballooning, reclaim под давлением платформы.

IOPS / Storage

Часто bottleneck живет именно здесь: IOPS-лимиты, latency, burst-политика, классы хранения, ограничения на VM и диск.

Network / Throughput

Сеть — это не только «до 10 Гбит/с»: bandwidth caps, PPS-лимиты, east-west и north-south трафик, oversubscription на уровне фабрики.

Отказоустойчивость: zone ≠ region, SLA ≠ непрерывность

UZCLOUD

SLA на доступность платформы не равен непрерывности вашего приложения.
За gap между этими понятиями отвечаете вы.

Зона отказа

Zone, site и region — это разные failure domains с разным радиусом поражения. Разнесение по зонам уменьшает один тип риска, но не закрывает все сценарии: отказ платформы, storage или control plane может затрагивать несколько зон.

Плановые работы

Плановые работы все равно будут. Нужно понимать: возможны live migration, reboot, redeploy. Важны окна обслуживания, notice time, гарантии по доступности во время maintenance и ограничения по вашей нагрузке.

Disaster Recovery

DR нужно проектировать отдельно — это не опция платформы, а архитектурное решение. Репликация, runbook, порядок переключения, регулярные тесты восстановления, зафиксированные RPO и RTO.

⚠ SLA провайдера покрывает доступность платформы, а не вашего приложения.
RPO и RTO — ваша ответственность, если иное явно не прописано в договоре.

Безопасность и backup: ответственность не исчезает

UZCLOUD

🔒 Провайдер отвечает за:

- Физическую безопасность дата-центра
- Сетевую инфраструктуру и гипервизор
- Базовую доступность платформы и управляемых сервисов
- Патчинг гипервизора и физических хостов

Один провайдер формулирует это как **security of the cloud**. Другой всегда отвечает за underlying infrastructure.

👤 Клиент отвечает за:

- Guest OS: установку, патчи, hardening
- Application software и его конфигурацию
- Firewall rules, security groups, IAM-политики
- Шифрование данных at rest и in transit
- Backup, restore testing, RPO и RTO
- Политики доступа и управление ключами

BIaaS клиент сам планирует и реализует большинство reliability-возможностей.

⊗ Shared responsibility не означает разделенную ответственность поровну.
В IaaS большая часть операционной ответственности остаётся на стороне клиента.

Экономика: скрытые счета приходят за трафик и архитектуру

UZCLOUD

Обычно private cloud сначала сравнивают по стоимости виртуальных машин. Но реальный бюджет растет из совсем других статей — чем ближе к корпоративному уровню надежности, тем меньше доля самих VM в итоговом счете.

Сеть

Internet egress, межзонный и межсайтовый трафик, публичные IP-адреса, балансировщики нагрузки — всё это тарифицируется отдельно.

Надежность

Второй сайт, репликация данных, резервная емкость, snapshots, полноценный DR-контур — резервирование стоит денег.

Операции

Backup, monitoring, logging, SOC, managed services, уровень поддержки — операционные расходы часто недооцениваются на этапе выбора.

Лицензии и сервисы

ОС, базы данных, middleware, панели управления, security tools — лицензионная нагрузка может быть сопоставима со стоимостью инфраструктуры.

Сравнивать нужно не цену VM, а полную стоимость сервиса: compute + storage + network + resilience + operations.

10 вопросов, которые надо задать провайдеру

UZCLOUD

01

Что именно private?

VPC, кластер, host, storage или вся платформа?

02

Логика или физика?

Логическая изоляция или выделенные физические хосты?

03

Виртуализация или bare metal?

Что лежит под вашими VM — гипервизор или просто железо?

04

Какие слои shared?

Control plane, backup plane, monitoring, storage fabric?

05

Гарантии производительности?

Что гарантировано, что best effort?

06

Что при maintenance?

Live migration, reboot или redeploy? Какое notice time?

07

Что реально в SLA?

Платформа, VM, guest OS или только control plane?

08

Кто отвечает за backup?

Restore testing, RPO и RTO — ваши или провайдера?

09

Как считается трафик?

Inter-zone, inter-region и internet egress — тарифы и лимиты?

10

Как выглядит выход?

Миграция образов, данных и т.п.— формат, стоимость, сроки?

Провайдер, который отвечает на все 10 вопросов четко — партнёр. Тот, кто уходит от ответов — риск.

ЗВОНИТЕ АРТЕМУ!

UZCLOUD

Спасибо за внимание!
Вопросы?

UZCLOUD

Артем Гринберг

@argrinberg
a.gavrilov@uzcloud.uz

Телеграм

linkedin