БРЕСТ

ПК СВ «Брест»
Новые возможности и технологии в современной реальности

Арсений Гизатуллин

Руководитель отдела технического presale
Дирекции виртуализации и облачных сервисов

Задачи

- Что требуется реализовать?
- Для каких целей?
- В каком объеме?
- Какие исходные данные?
- Есть ли перспектива масштабирования/аппаратной миграции?
- Имеются ли дополнительные требования?
- Как выглядит вектор развития продукта?

Виртуализация ресурсов

— механизм создания изолированных копий серверов (виртуальных машин) и информационных систем в рамках одной аппаратной платформы с полным сохранением функциональности системы

Назначение виртуализации

- Консолидация серверов или вычислительных ресурсов
- Обеспечение отказоустойчивости сервисов
- Информационная безопасность
- Разработка и тестирование информационных систем
- Предоставление ИТ-услуг

«Брест»– это...

....платформа для организации

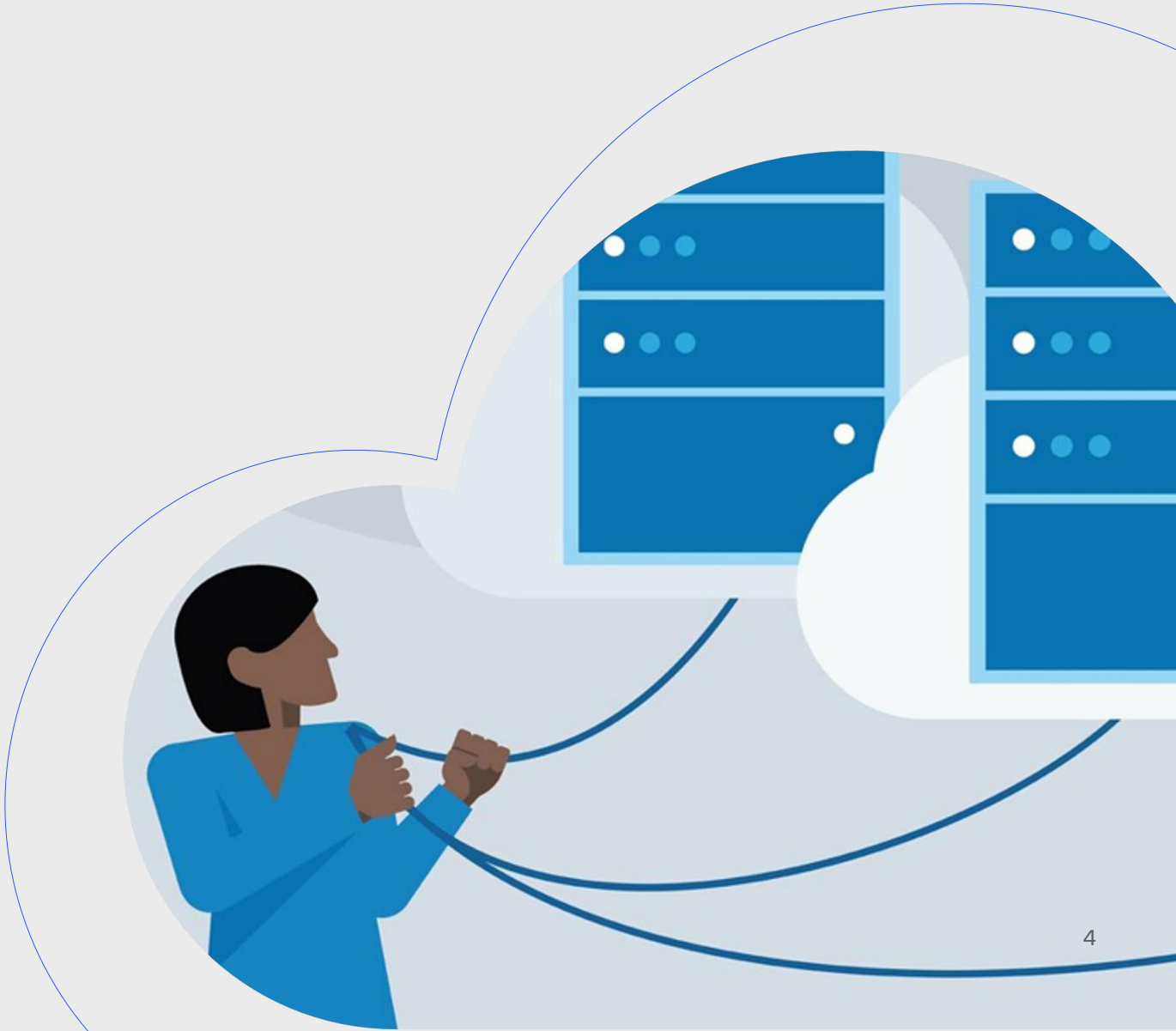
1. VDI-решения (совместно с Termidesk VDI)

2. Виртуальной среды для серверной группировки ОС

3. Готовых сервисов-приложений на базе ВМ

4. Групп ВМ с политиками эластичности под динамические нагрузки

5. Частного облака с мультитенантностью и изоляцией



Совместимость

RuBackup

Профессиональный инструментарий для резервного копирования

TERMIDESK

Инфраструктура виртуальных рабочих мест

БРЕСТ

Программный комплекс средств виртуализации

ASTRA LINUX®

Серверная базовая платформа

ALD Pro

Централизованное управление компьютерами и учетными записями пользователей

Механизмы автоматизированного развертывания

ASTRA AUTOMATION

kaspersky

ideco

s•terra

UserGate

Active Directory

Технологический стек

Виртуализация

1. Libvirt
2. KVM
3. Qemu

Конфигурирование

Ansible

Управление и магазин приложений

OpenNebula

Хранение

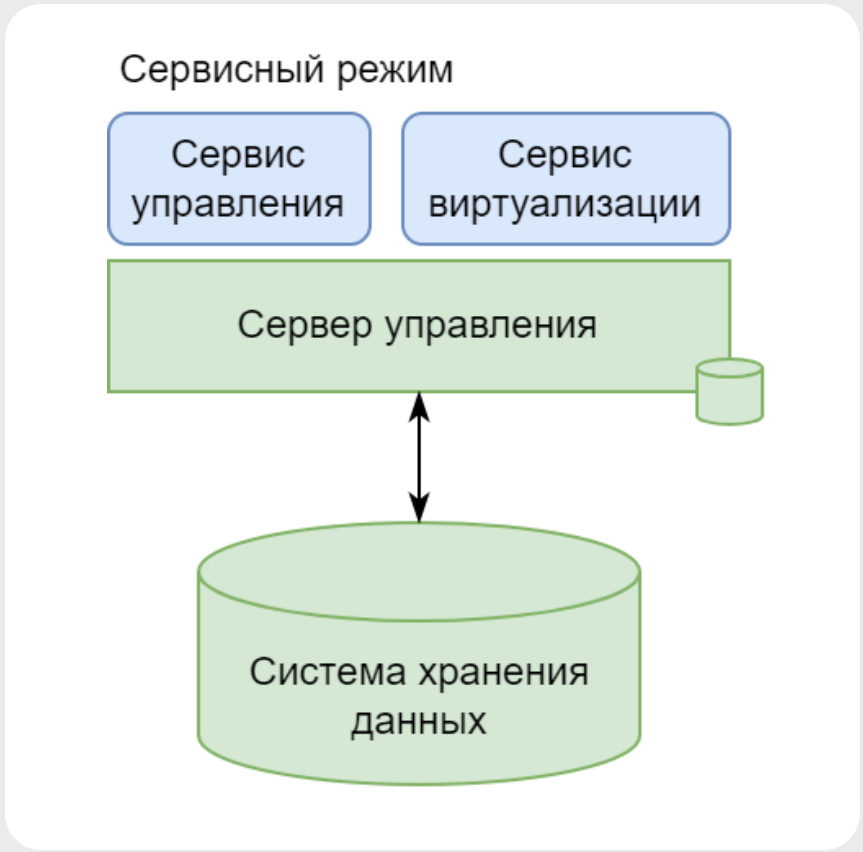
Гиперконвергентное / конвергентное
Ceph-RBD

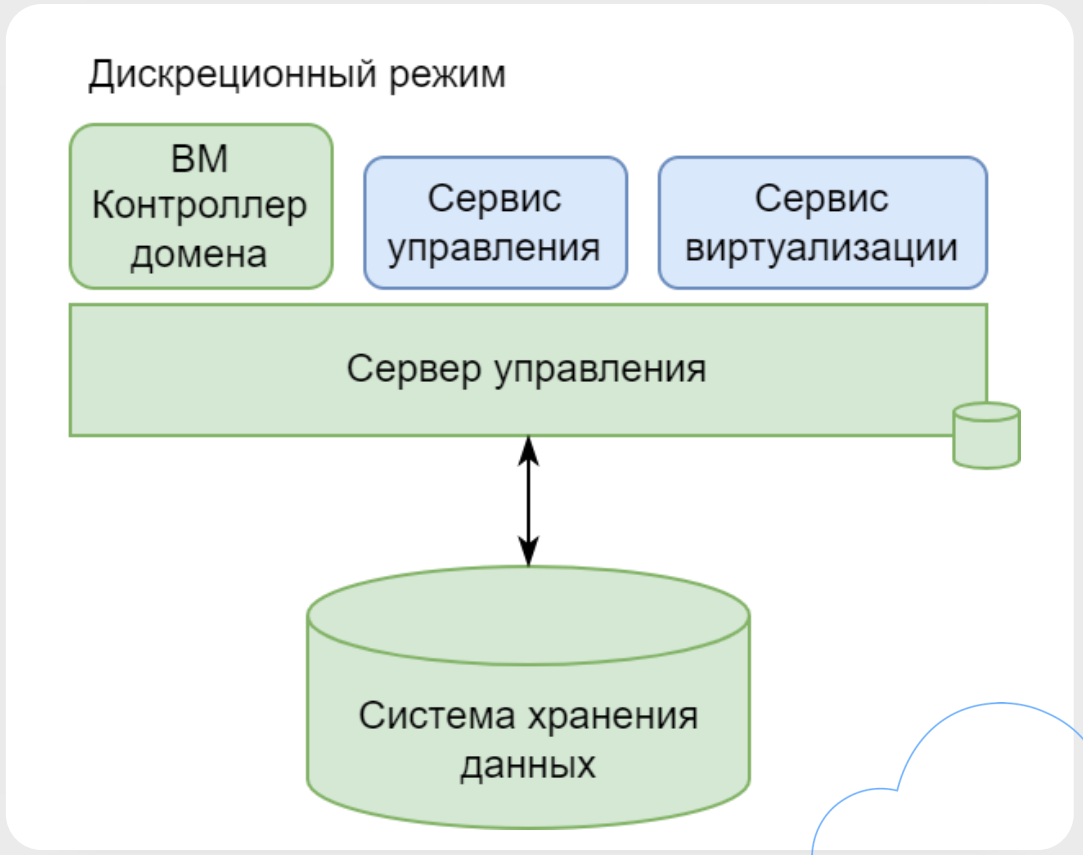
Классические
1. СХД (iSCSI / FC)
2. LVM_LVM/LVM_Thin

Сеть

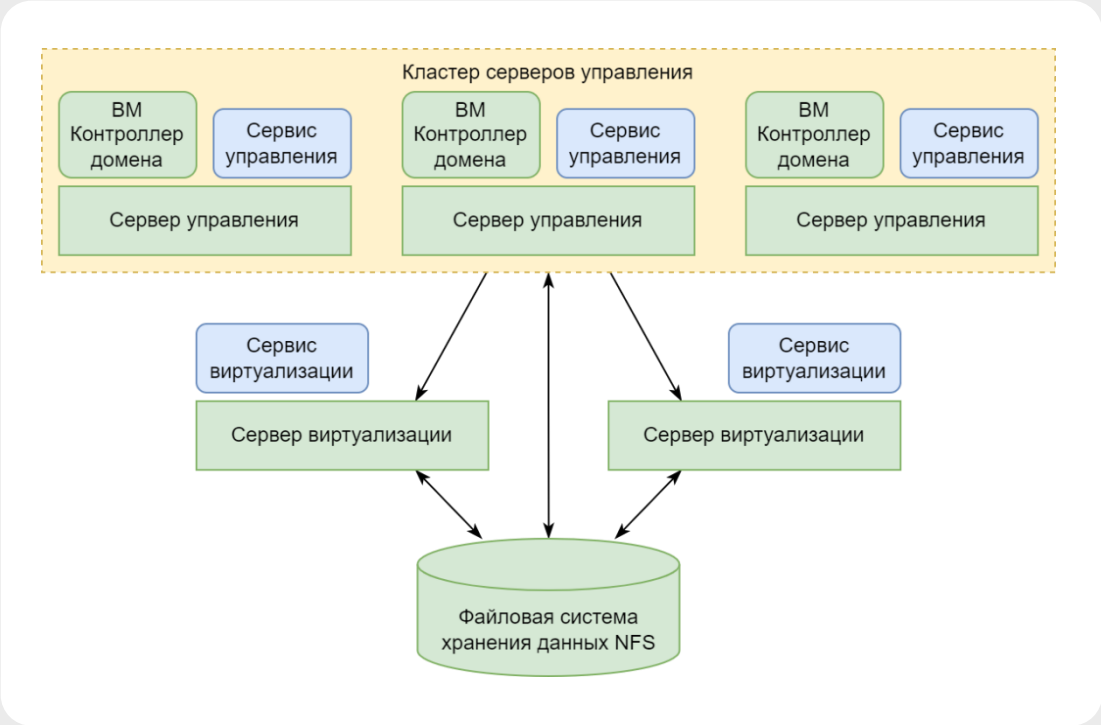
1. Security Groups Bridge (*FW)
2. 802.1Q
3. VXLAN
4. OpenVswitch
5. OpenVswitch-VXLAN

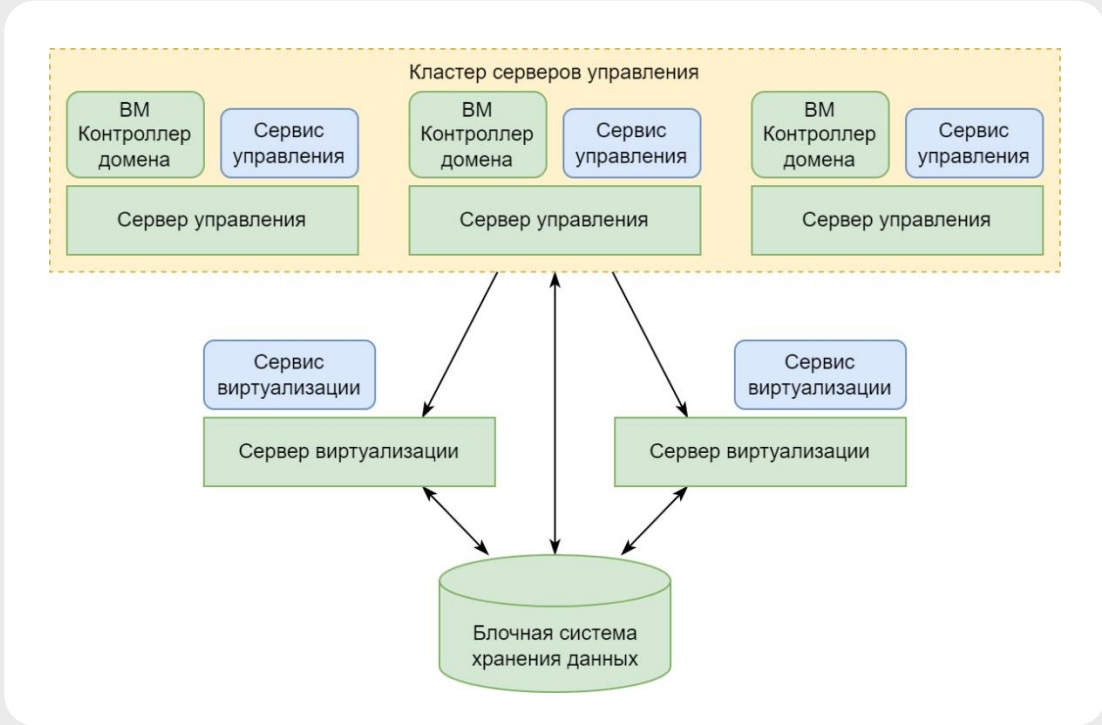
Архитектура продукта
Режимы



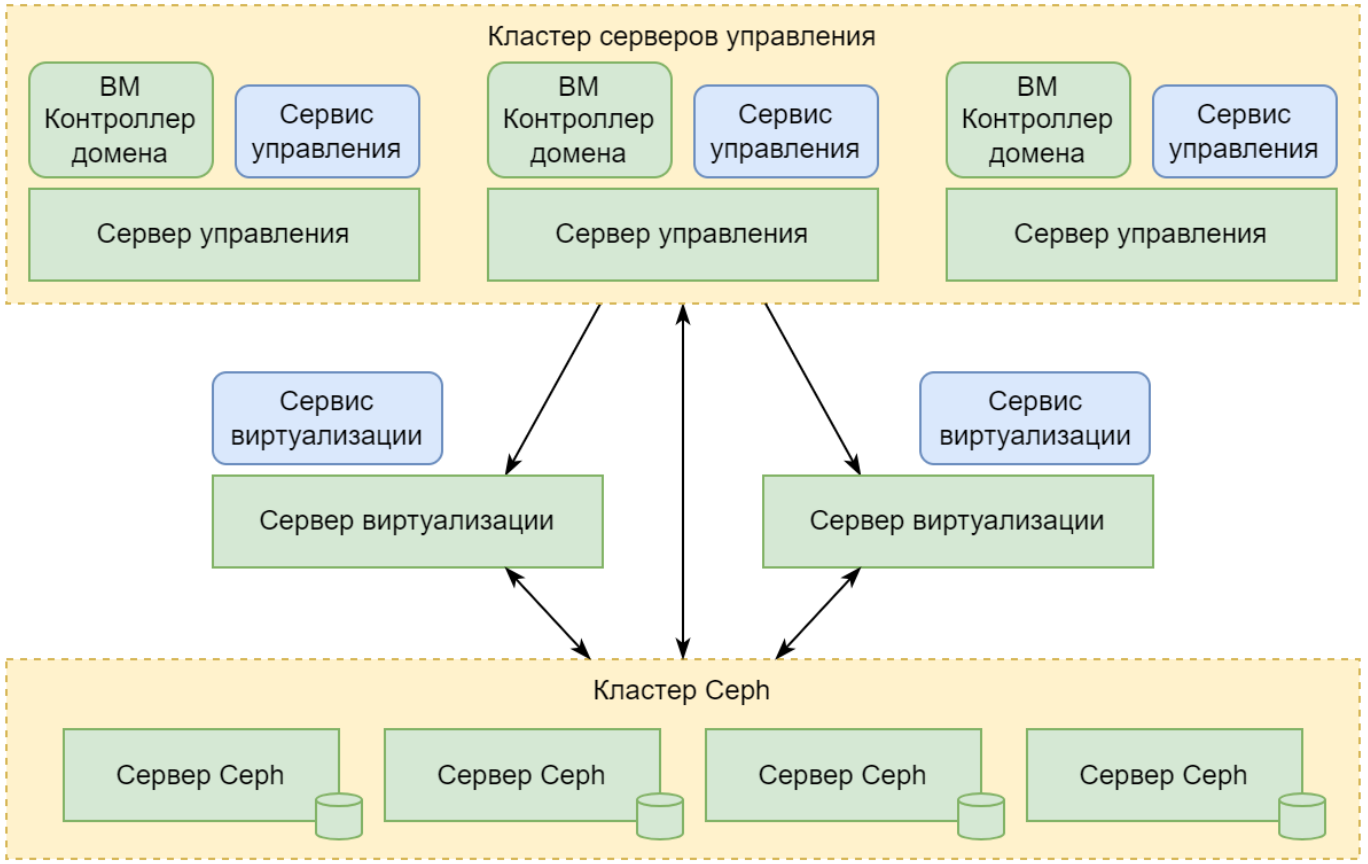


Архитектура продукта Конвергенция – СХД / NFS

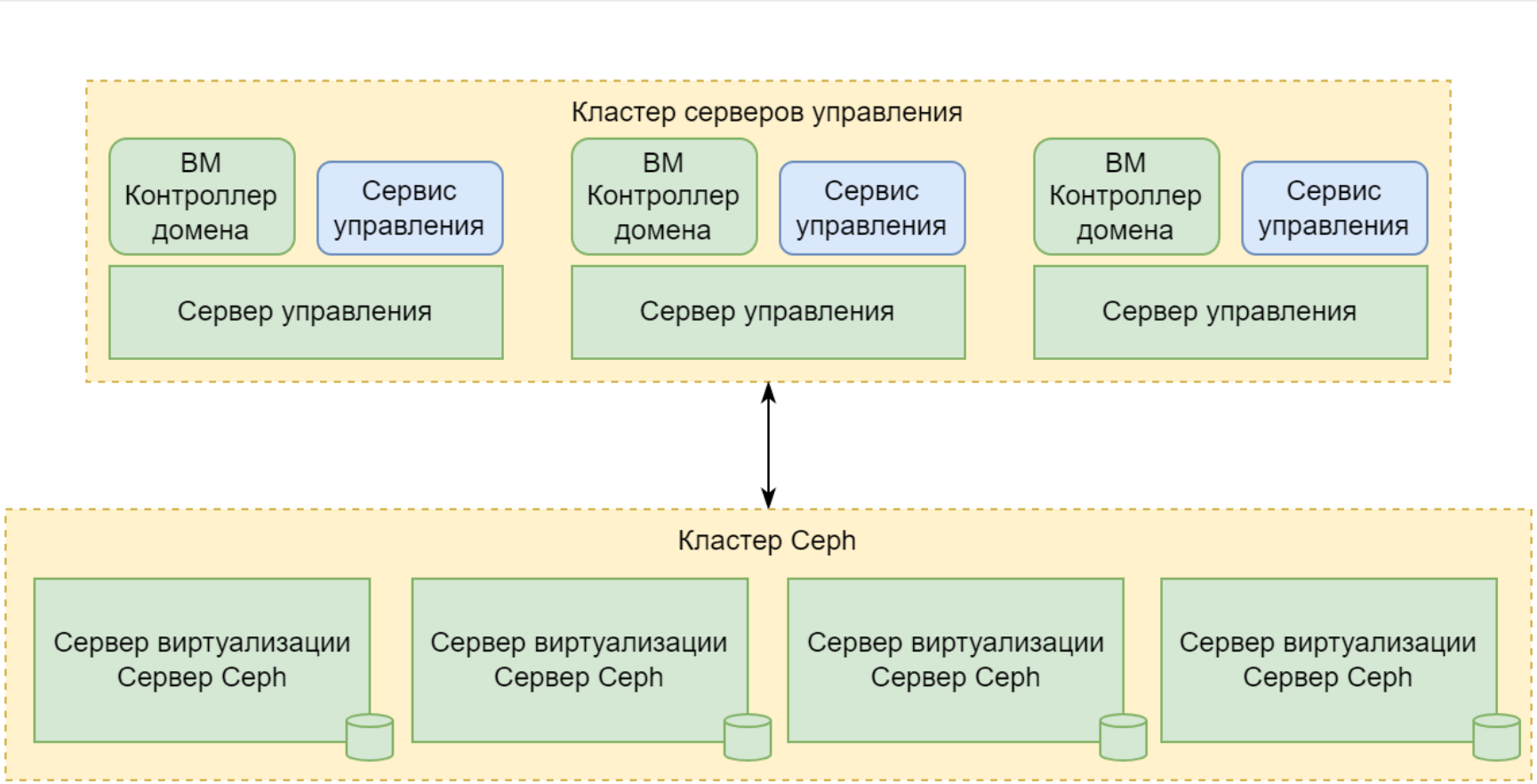




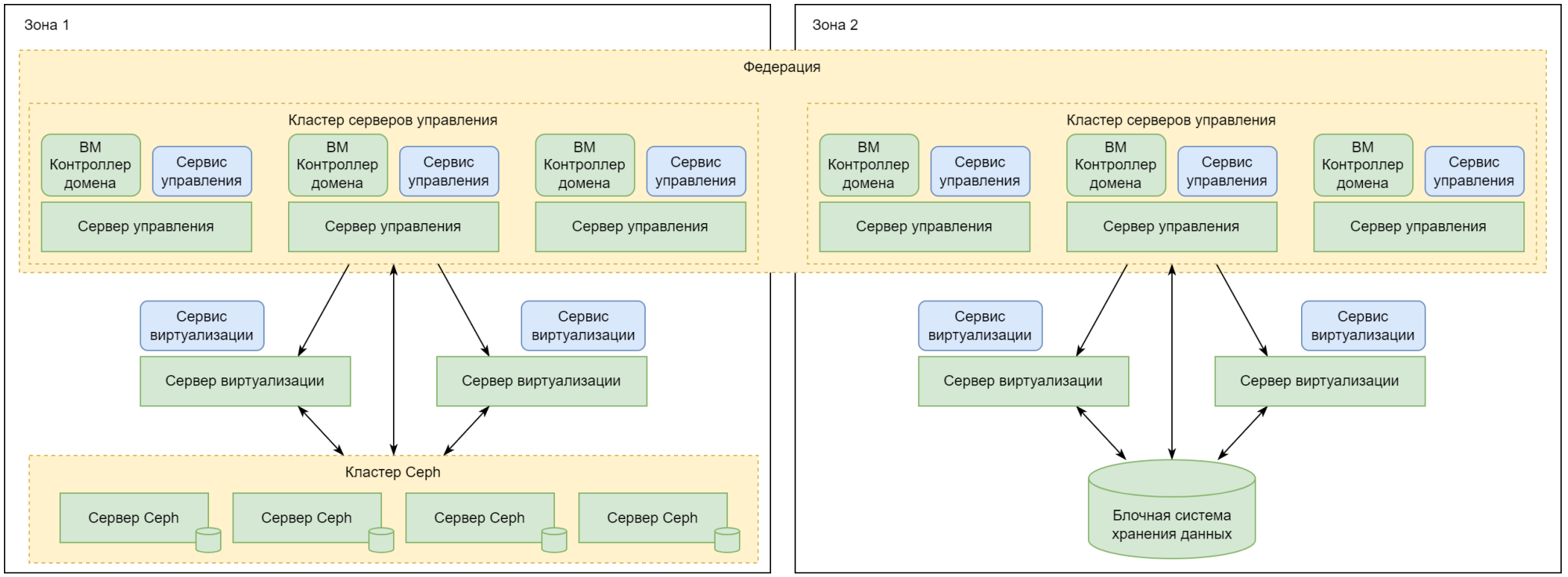
Архитектура продукта Конвергенция – SDS



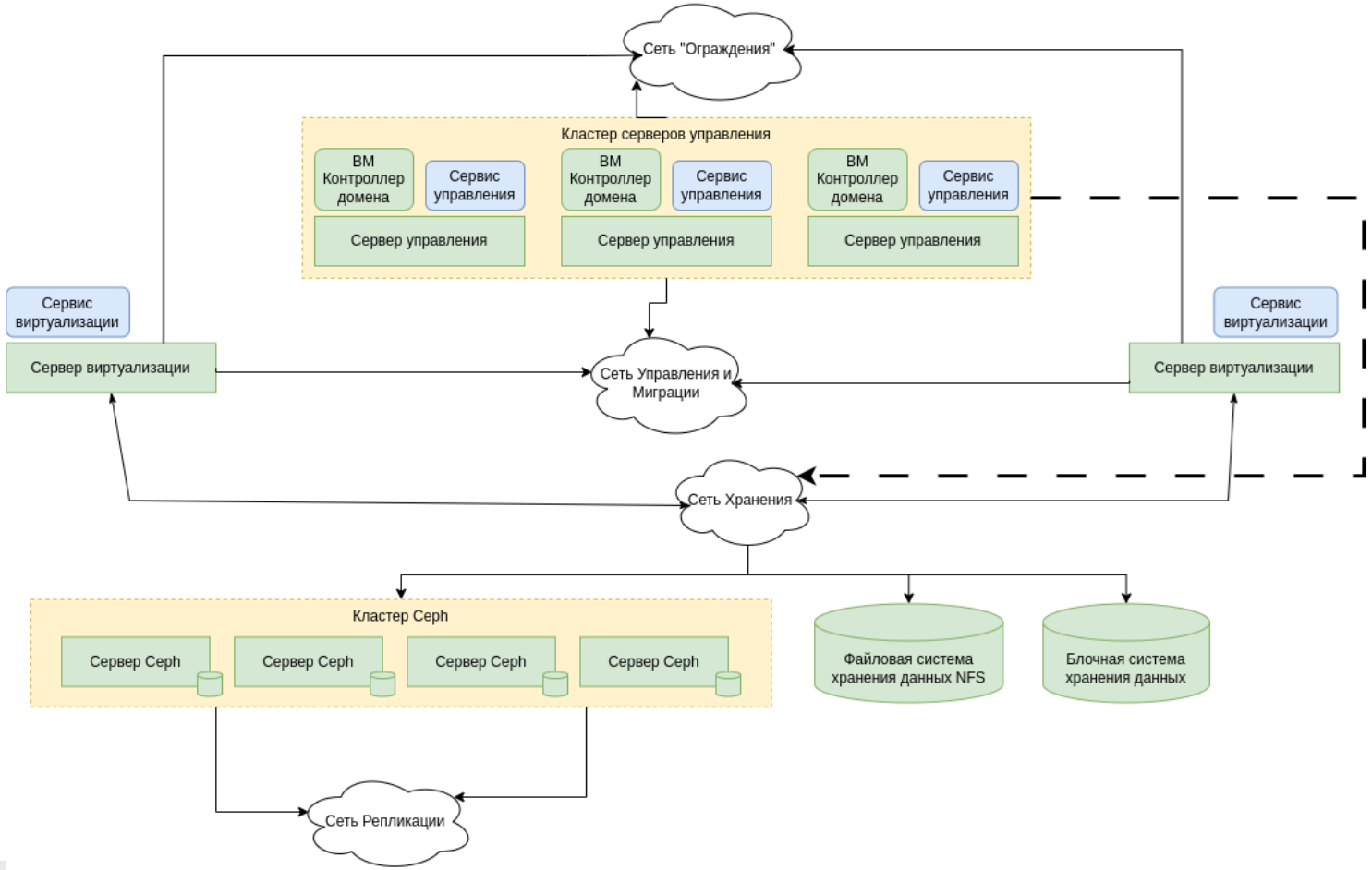
Архитектура продукта Гиперконвергенция



Архитектура продукта Федерация



Архитектура продукта
Схема сети



Ограничения

Один сервер виртуализации

- До 32 сокетов
- Архитектура CPU: AMD 64 and Intel 64
- До 384 ядер ЦПУ, 768 потоков
- До 6 Tb оперативной памяти
- До 150 ВМ
- До 100 дисков

Федерация

- До 16 зон
- До 160 000 виртуальных машин
- До 40 000 серверов виртуализации

Одна виртуальная машина

- До 256 виртуальных CPU (vCPU)
- До 2 Tb оперативной памяти
- До 32 виртуальных сетевых интерфейсов (virtio-nic)
- До 32 устройств PCI
- До 32 виртуальных дисков (virtio-blk)
- До 100 виртуальных дисков (virtio-scsi)

Один управляющий кластер

- До 9 серверов управления (рек.)
- До 1250 подчиненных серверов виртуализации
- До 10 000 виртуальных машин

Методика развертывания

CLI Wizard

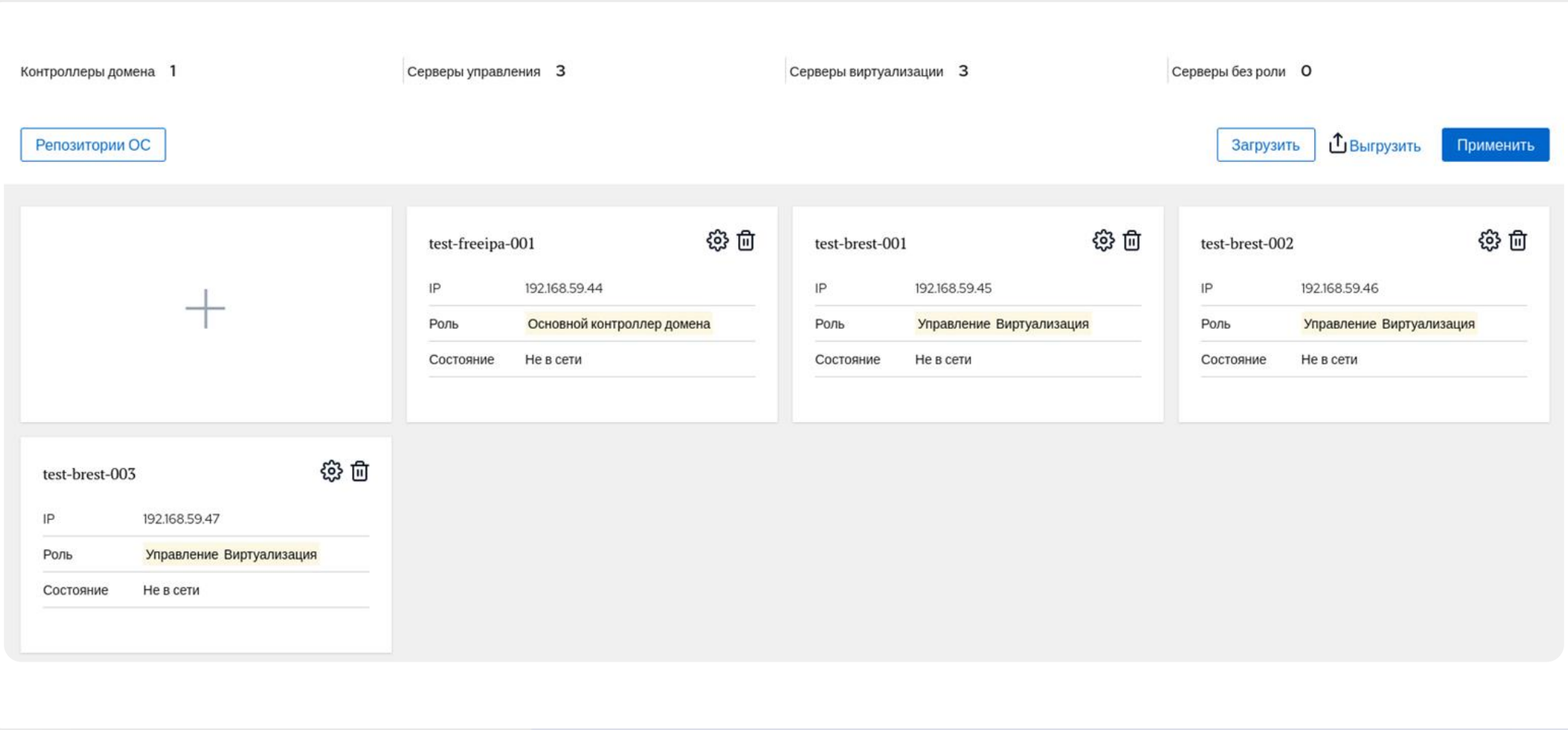
```
Укажите количество серверов (число от 3 до 2N+1): 3
В системе присутствуют следующие интерфейсы:

lo eth0

Укажите интерфейс для плавающего IP-адреса,
предназначенный для синхронизации между нодами:
интерфейс по умолчанию eth0
eth0
Укажите плавающий IP адрес, предназначеный для лидера RAFT,по умолчанию, IP будет 10.10.10.100/24:10.152.0.190/24
Построчно введите имена (hostname) серверов, пример ниже, этот сервер уже введен:
Server01: srv-brest-001
Server02: srv-brest-002
Server03: srv-brest-003
В работу поступили следующие сервера:
srv-brest-001.domain.intra
srv-brest-002.domain.intra
srv-brest-003.domain.intra
Все верно? y/n: y
Начинается настройка RAFT.
Добавляем первый сервер в зону
```

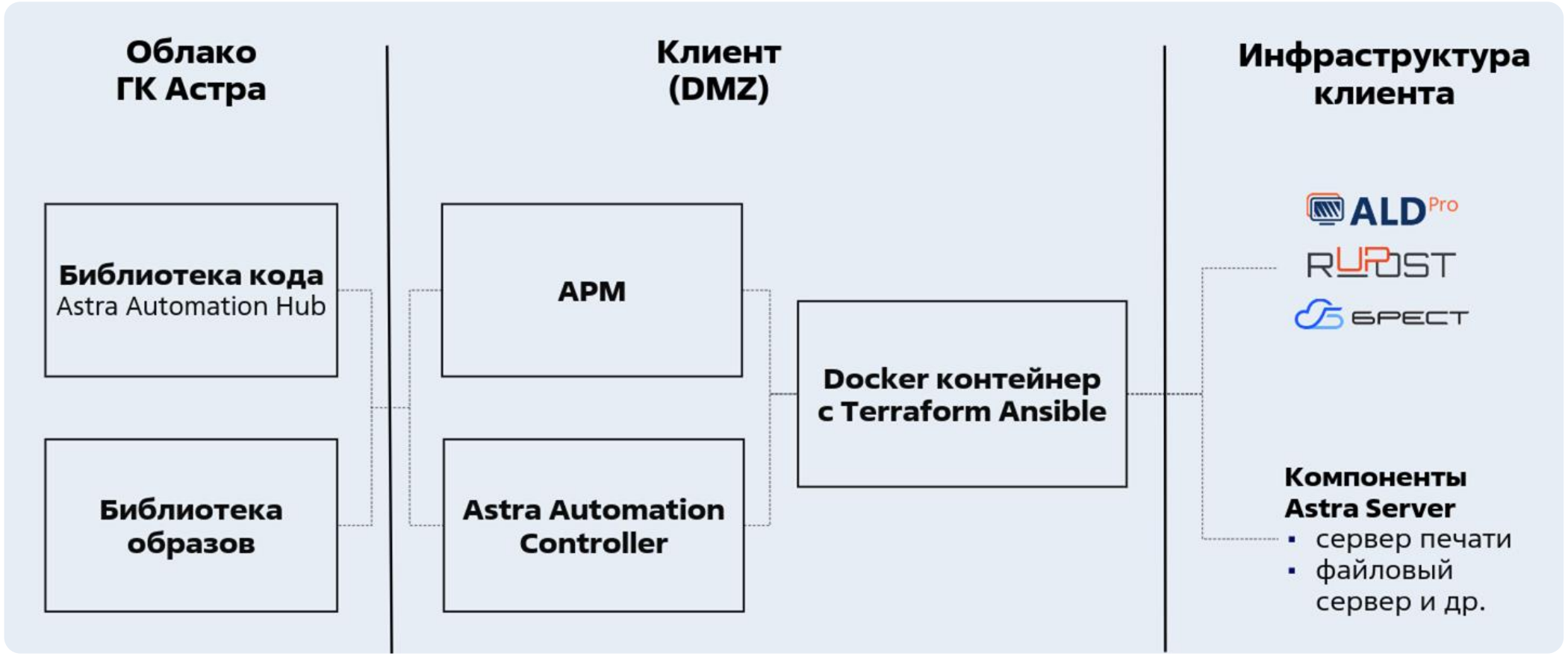
Методика развертывания

КУБ

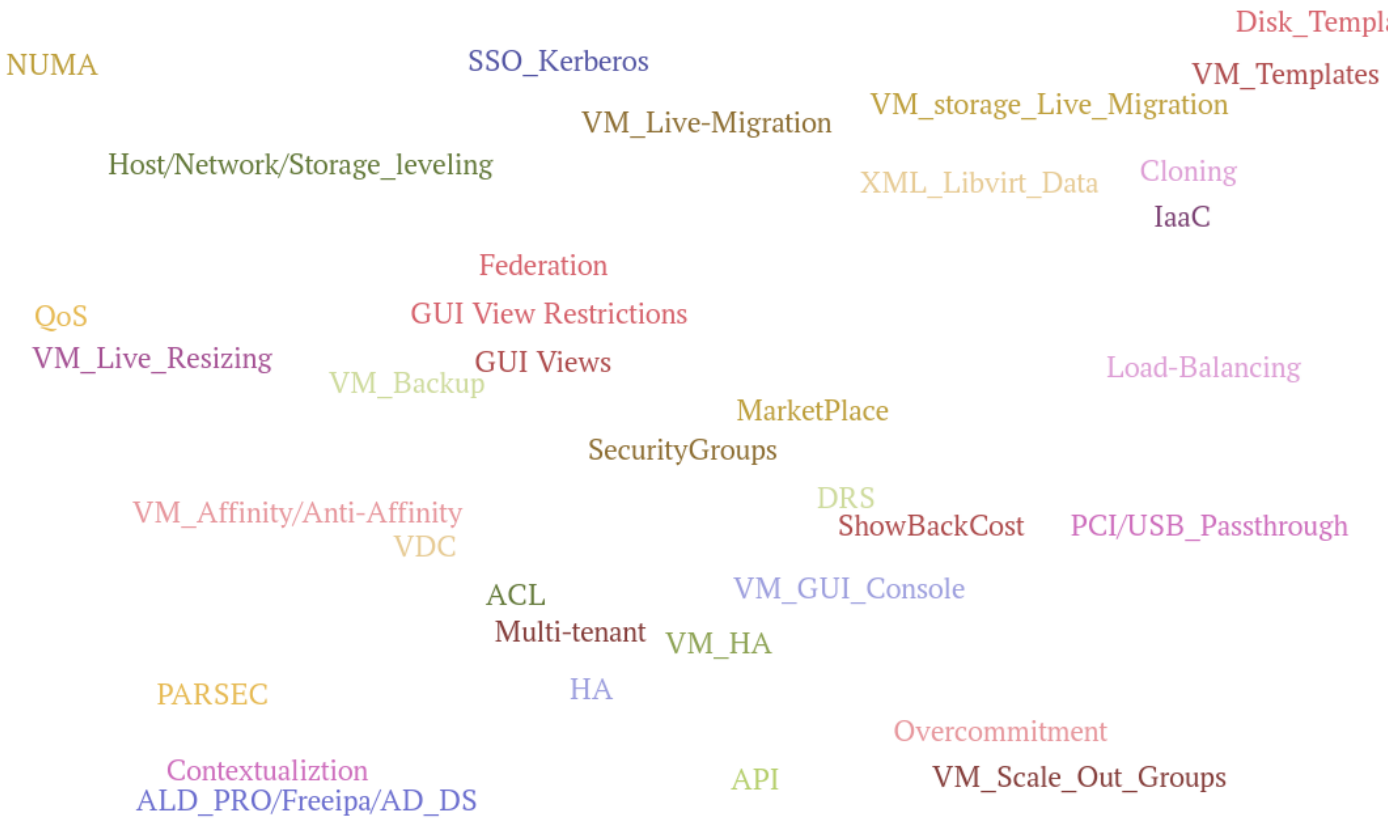


Методика развертывания

IaaS – Astra Automation



Основные функции



Масштабируемость

Кластер управления

- Добавление участников – серверов управления

Хранение:

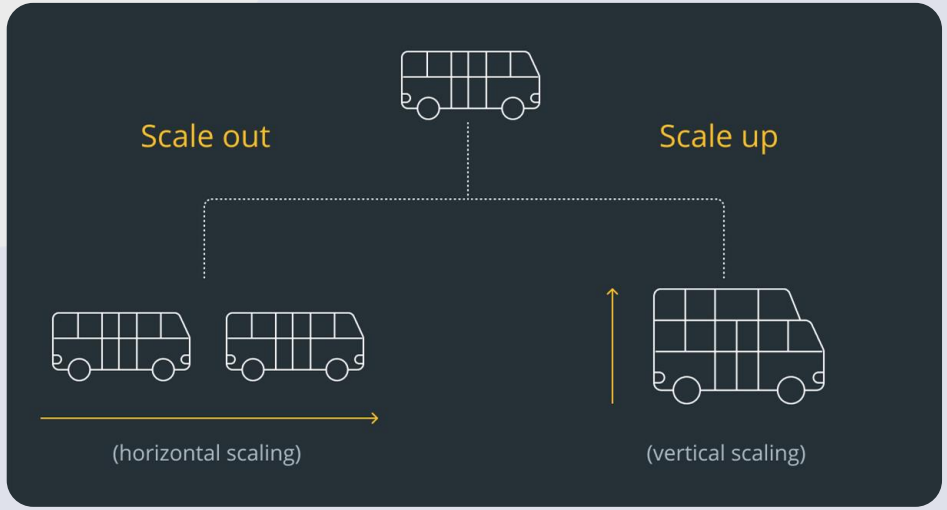
- Добавление LVM PVs и расширение VGs
- Создание новых LVM VGs на базе новых блочных устройств и миграция ВМ
- Добавление Ceph OSD в существующие Pools и их расширение
- Создание новых Pools на базе новых блочных устройств
- Добавление СХД, участников SDS Ceph / новых кластеров SDS Ceph

Вычислительные ресурсы

- Добавление серверов виртуализации
- Увеличение CPU и RAM на текущих серверах

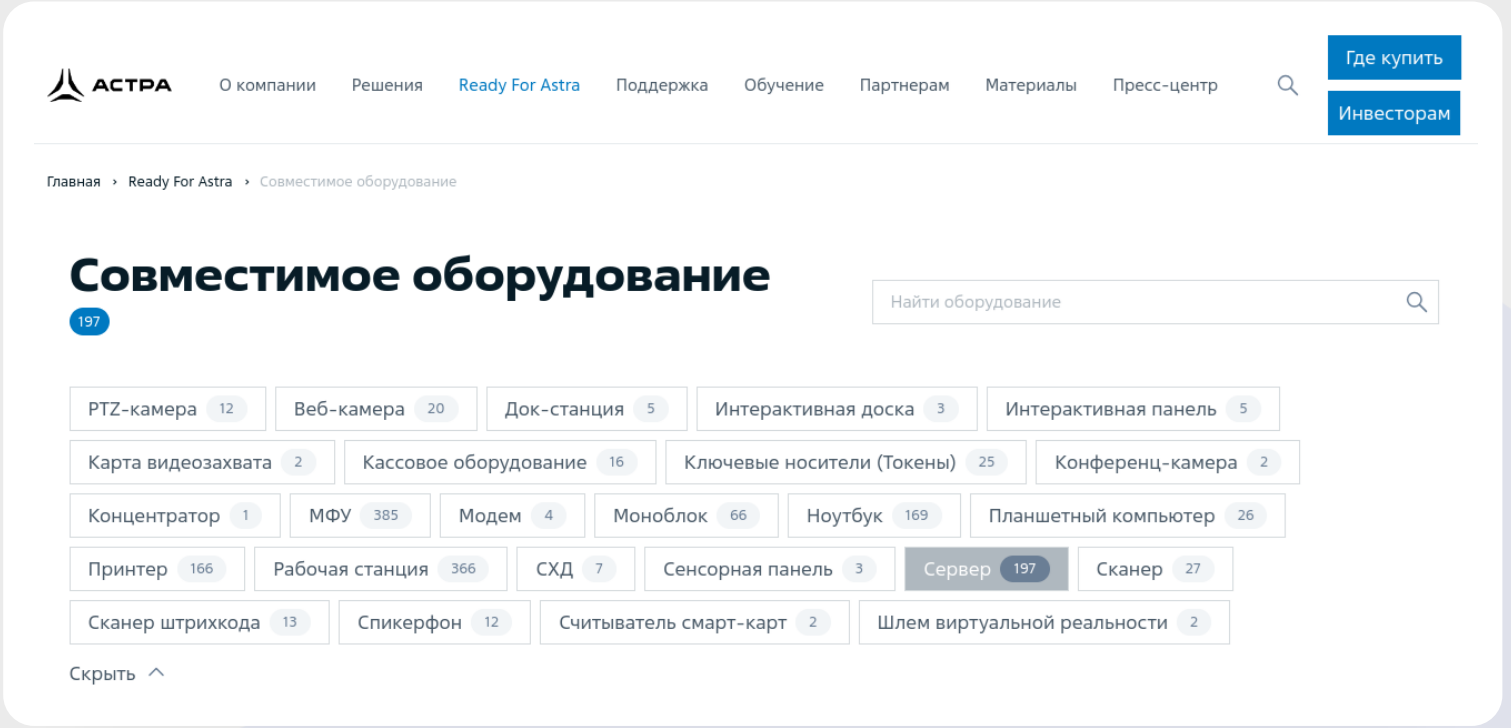
Служба каталогов / DNS/CA

- Добавление реплик – FreeIPA / ALD Pro



Оборудование

1. BMC-модуль (IPMI v.2)
   Контроллеры и адаптеры
   (ОС ALSE)
2. Материнская плата
   (ОС ALSE)
   CPU и инструкции
   (ОС ALSE)



AQUARIUS · YADRO · DELTA SOLUTIONS · TCC · 3LOGIC GROUP · HUAWEI · Atos · SUPERMICRO

Отказоустойчивость

LACP groups – Bonds

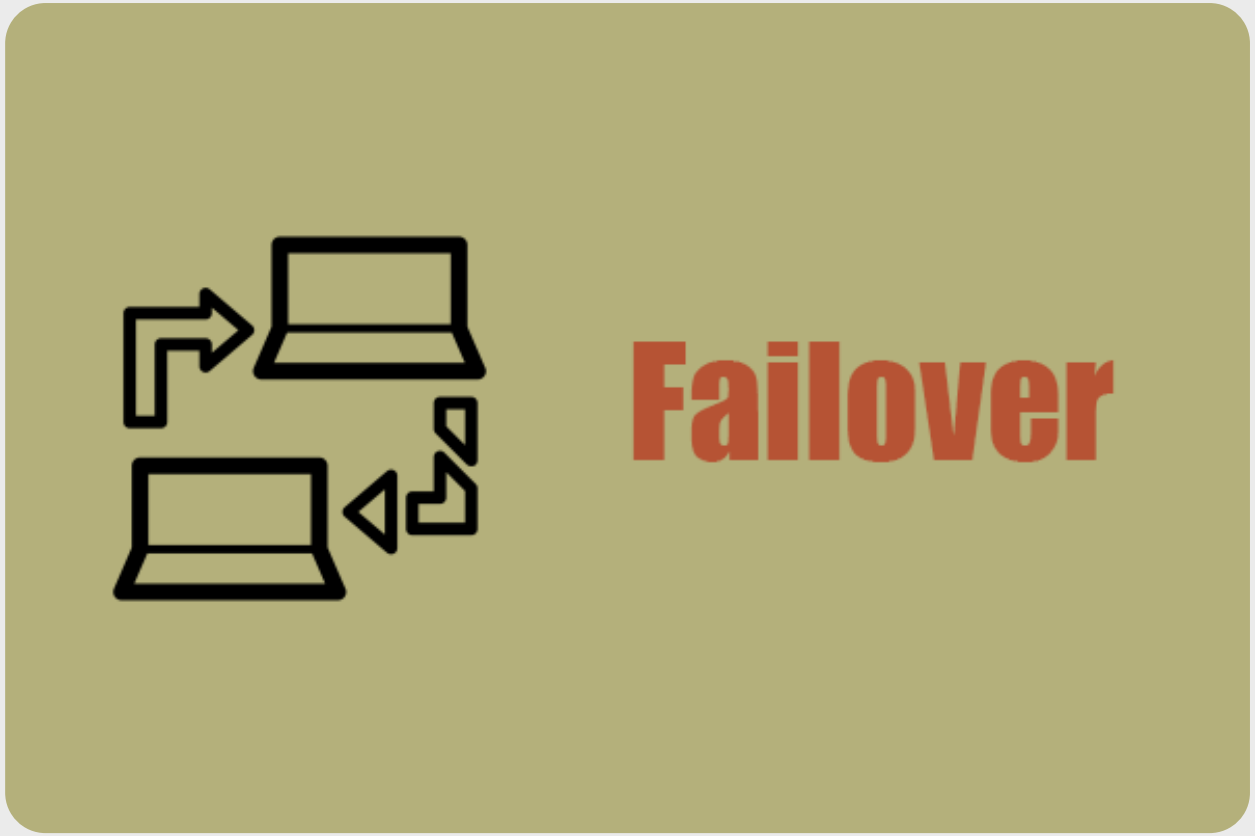
Multipathing

SDS Ceph – кворум мониторов, репликация данных, CRUSH

BM HA – “ограждение” гипервизоров, BMC, кластеры гипервизоров

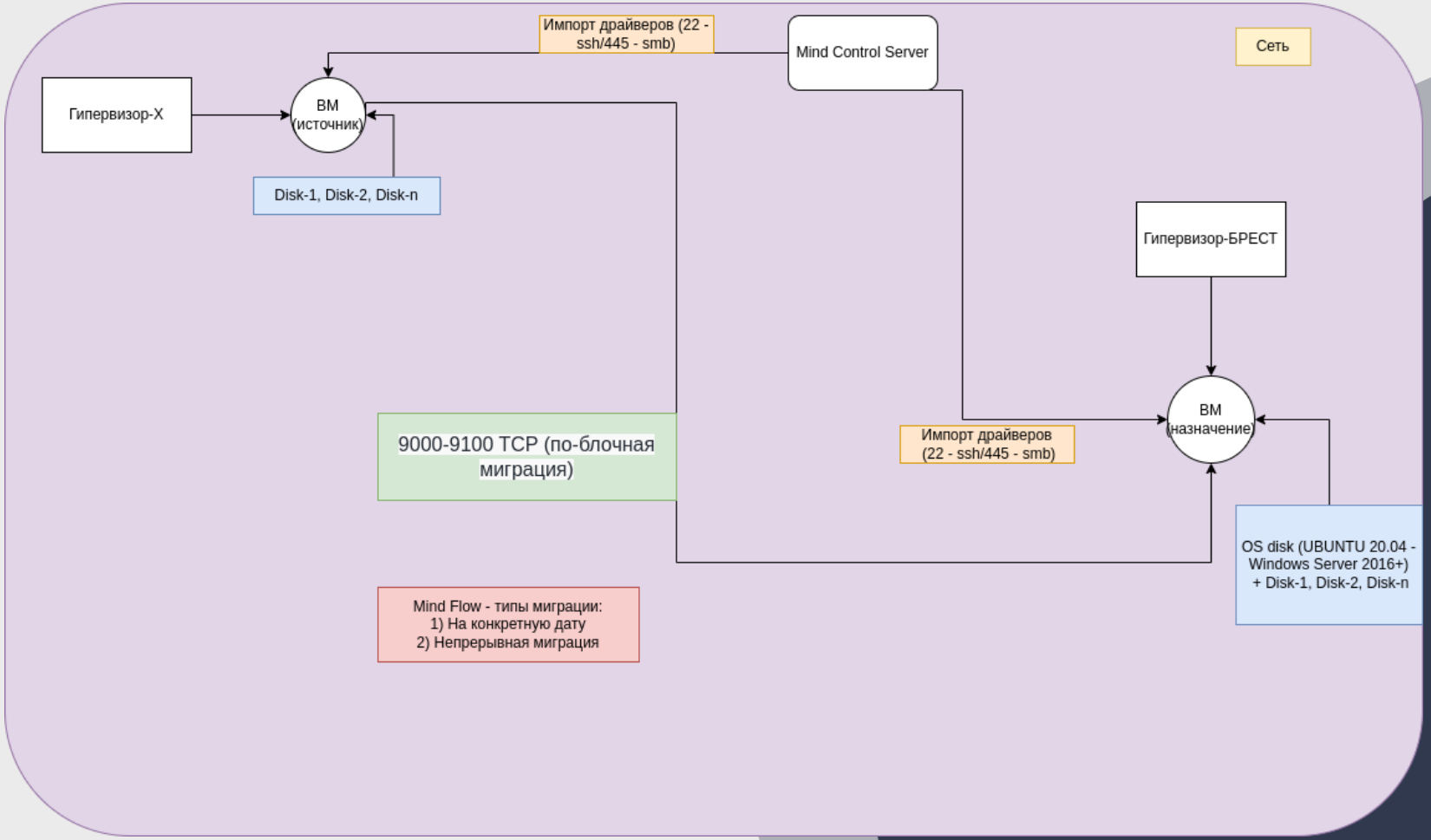
RAFT – кворум серверов управления, “плавающий” VIP, консистентное внесение изменений на большинстве участников

Freeipa / ALD Pro (DC / DNS / CA) – реплики



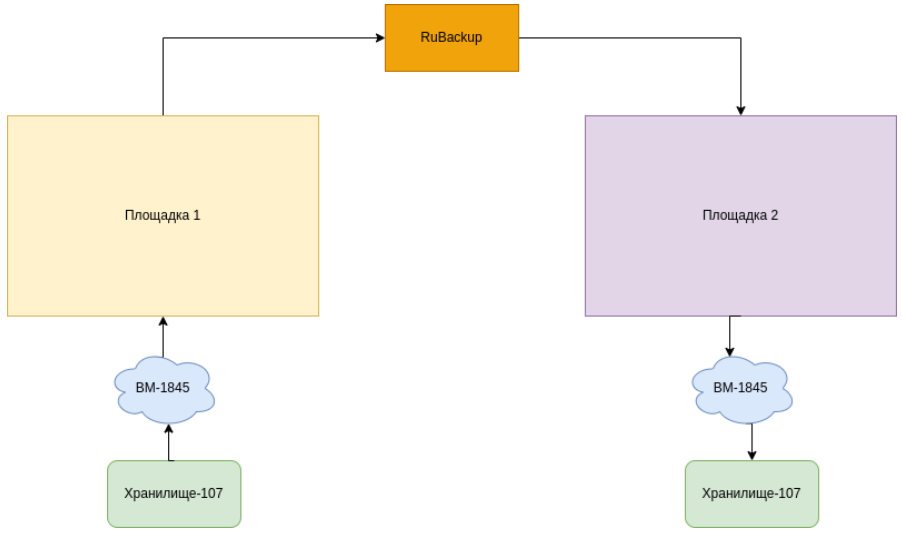
Асинхронная миграция данных на уровне ОС ВМ

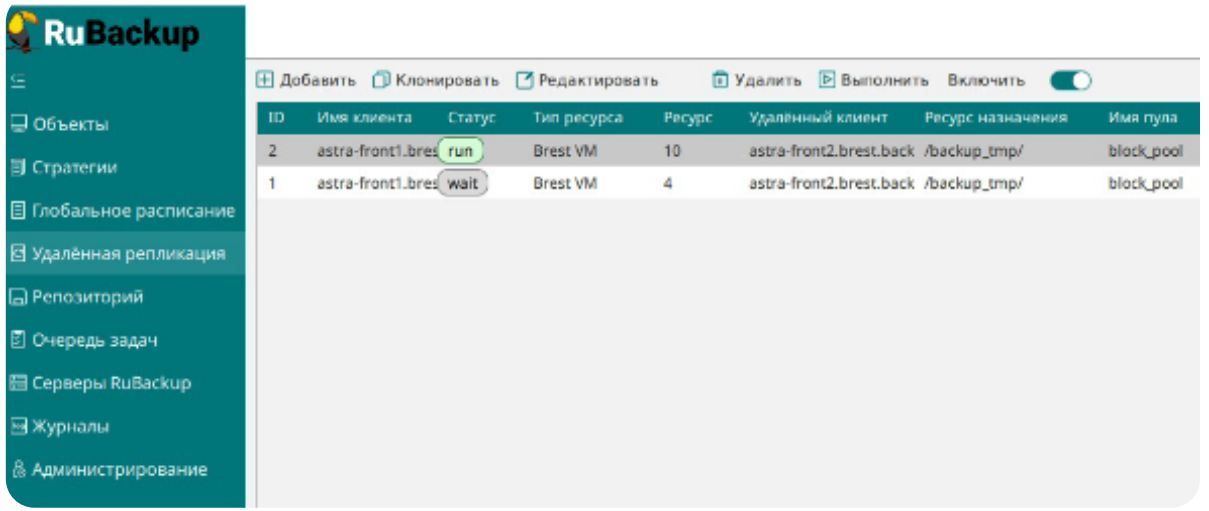
Software Mind – Control & Flow



Асинхронная репликация

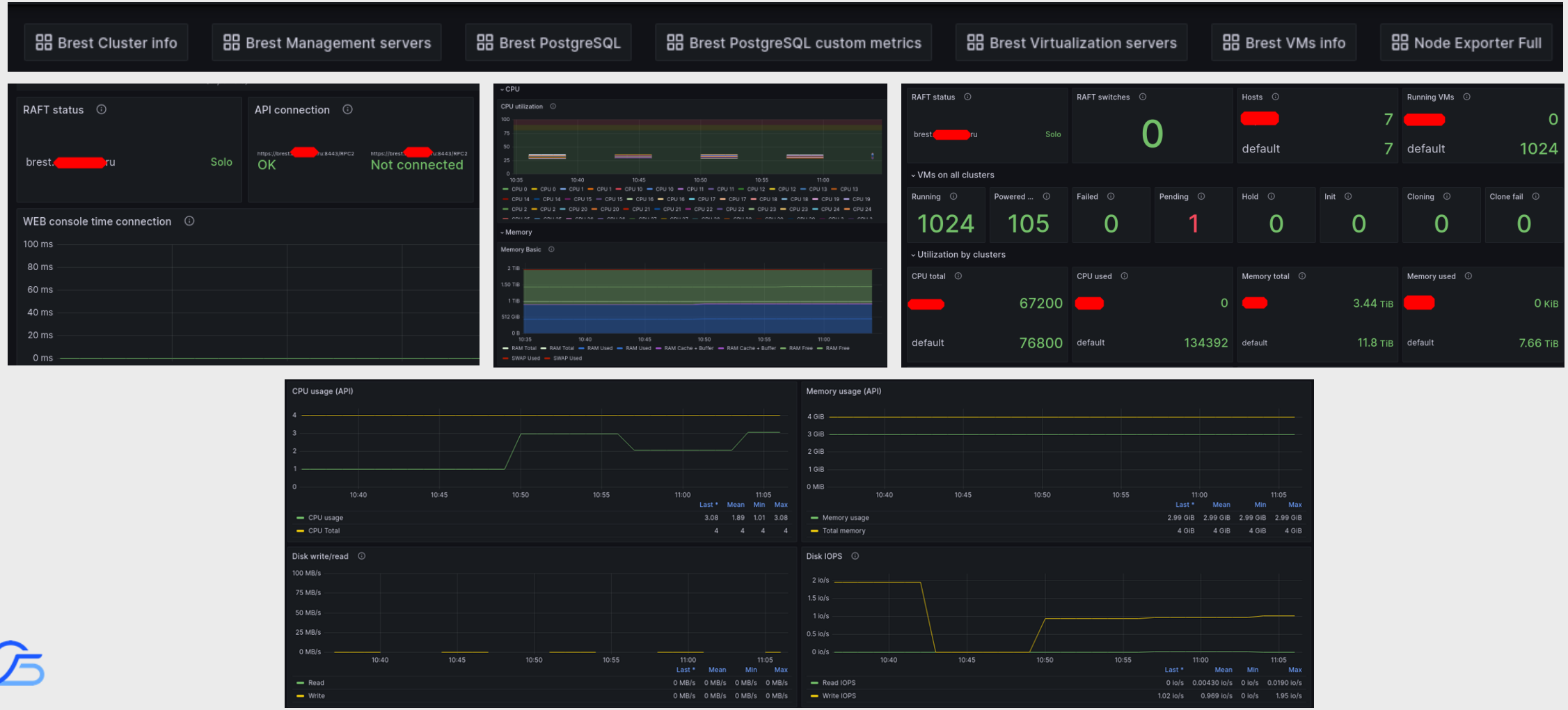
RuBackup





Astra- мониторинг

Prometheus Node Exporter + Prometheus + Grafana



Информационная безопасность

1. СЗИ Parsec (МКЦ и МРД)
2. UEFI bootloader
3. Private RAM & NUMA Core
4. Логирование действий пользователей и администраторов
5. SSL

Сертификация

Сертификация МО и ФСЭК (2 класс) запланирована на конец 2023 – 1 квартал 2024 года

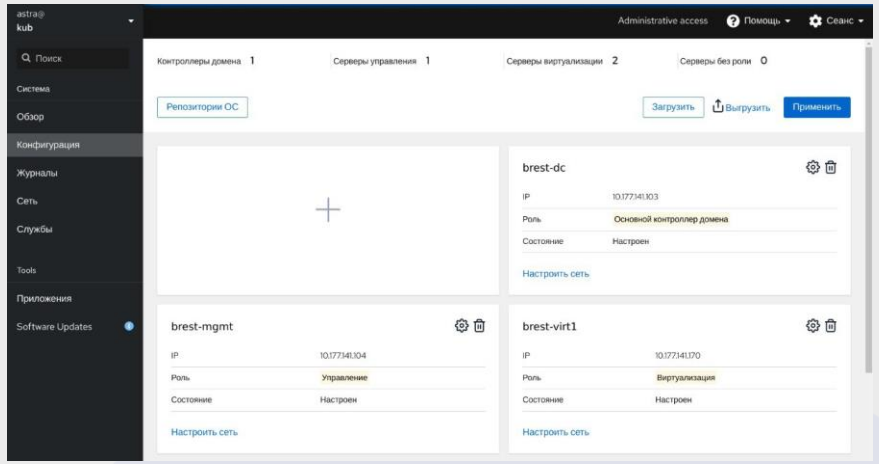
RoadMap 2024

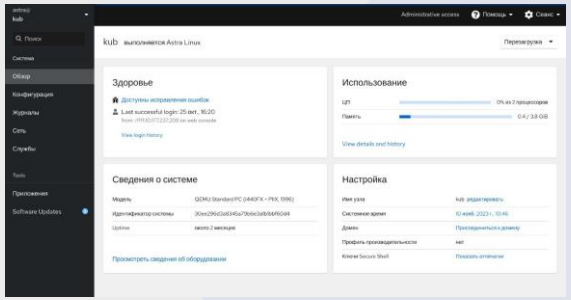
1. Поддержка расширенного мандатного контроля целостности
2. Расширение количества метрик и графиков в интерфейсе управления
3. Extended LVM (thin-диски, снапшоты и миграция ВМ, онлайн-обслуживание хранилища, поддержка МКЦ / МРД)
4. Модуль для sosreport (сбор журналов для техподдержки)
5. Интеграция с BILLmanager
6. NVIDIA vGPU
7. Установка в удаленный ЦОД (КУБ)
8. Новый веб-интерфейс (MVP)
9. Виртуальный маршрутизатор (DHCP, DNS, NAT, S / DNAT, LB-4, ROUTING, HA-VRRP)
10. Универсальный режим работы ПК СВ «Брест»
11. L7-балансировщик нагрузки
12. Интегрированный DNS-сервер
13. Зеркалирование трафика ВМ
14. Интегрированный VPN-сервер
15. OSPF/BGP Edge
16. Журналирование сетевых пакетов ВМ
17. Thick Provisioning для виртуальных дисков

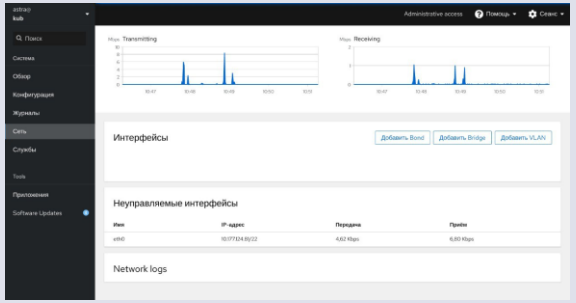
КУБ

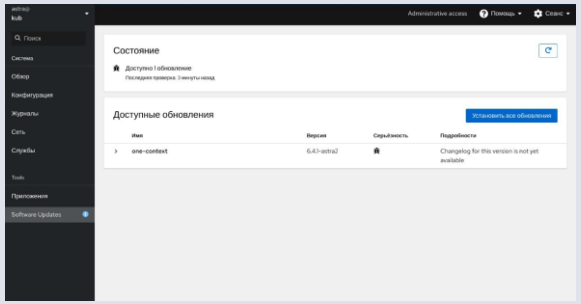
Развитие функционала

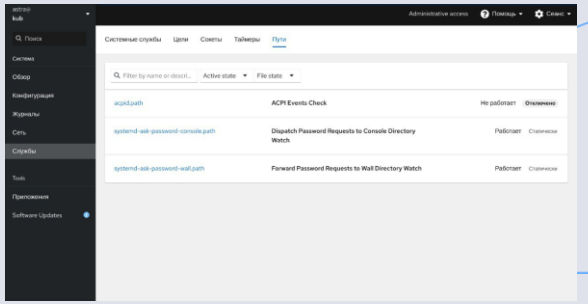
- Обслуживание физической составляющей
- Добавление / удаление серверов-участников кластеров
- Подключение хранилищ
- Централизованное обновление кластеров гипервизоров и управления
- Развертывание SDS Ceph
- Настройка backend-части сетей



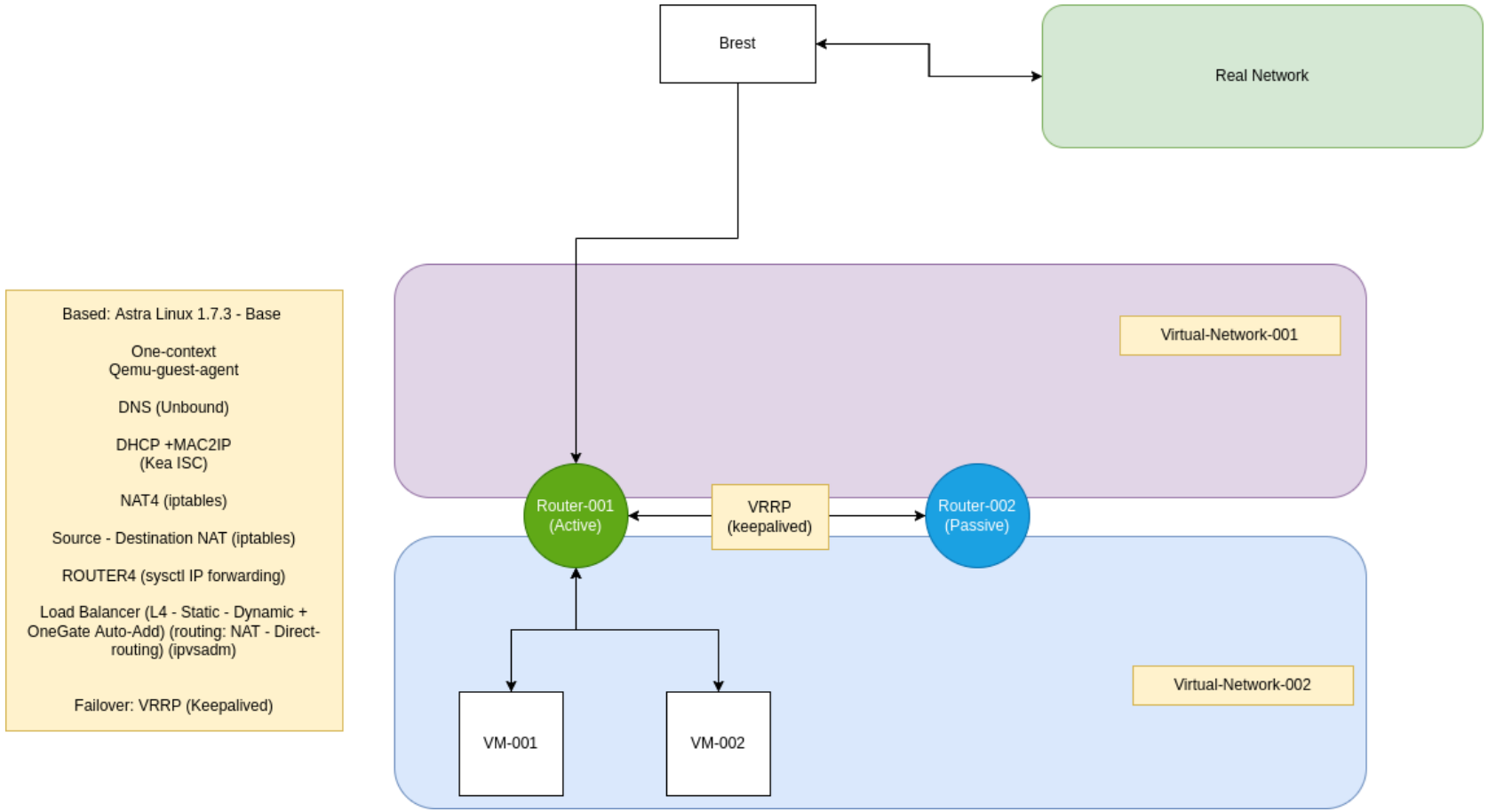






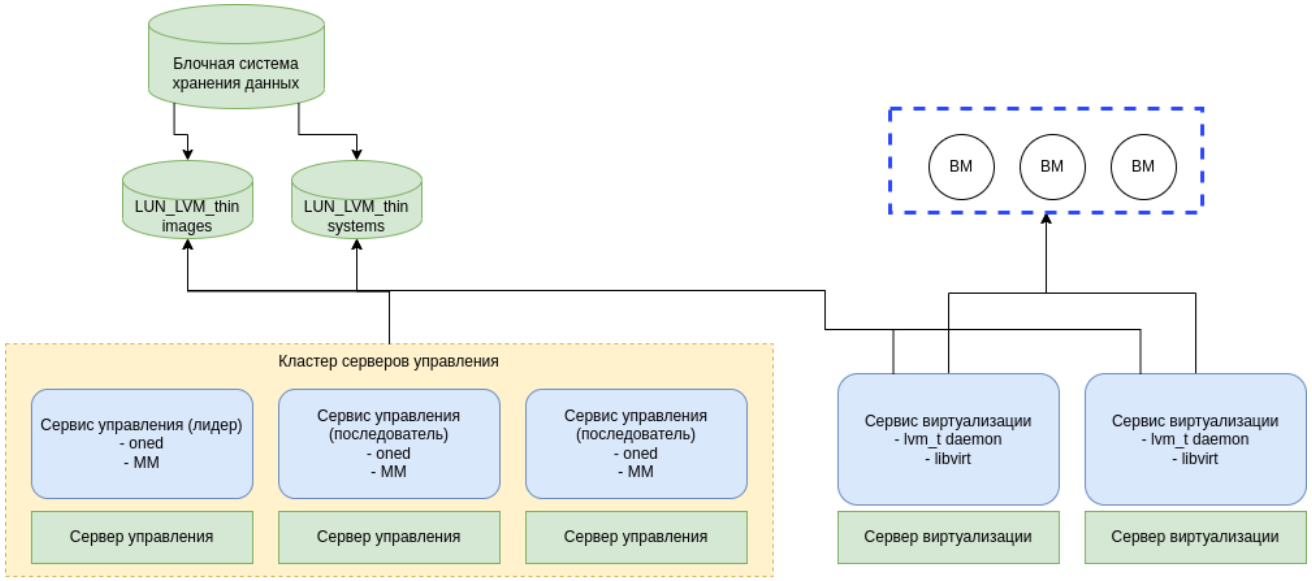


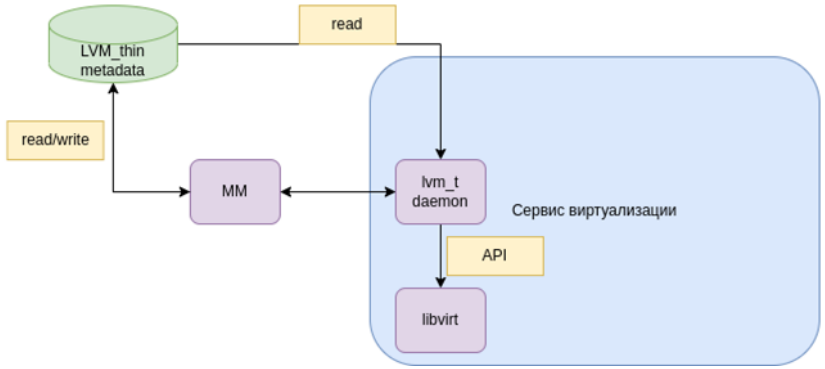
Виртуальный маршрутизатор



Асинхронная репликация

RuBackup





БРЕСТ

Спасибо за внимание!