



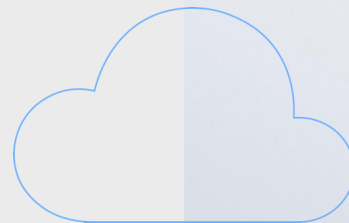
ПК СВ «Брест» Новые возможности и технологии в современной реальности

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?



Назначение виртуализации

Виртуализация ресурсов

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



Консолидация серверов или вычислительных ресурсов



Обеспечение отказоустойчивости сервисов



Информационная безопасность



Разработка и тестирование информационных систем

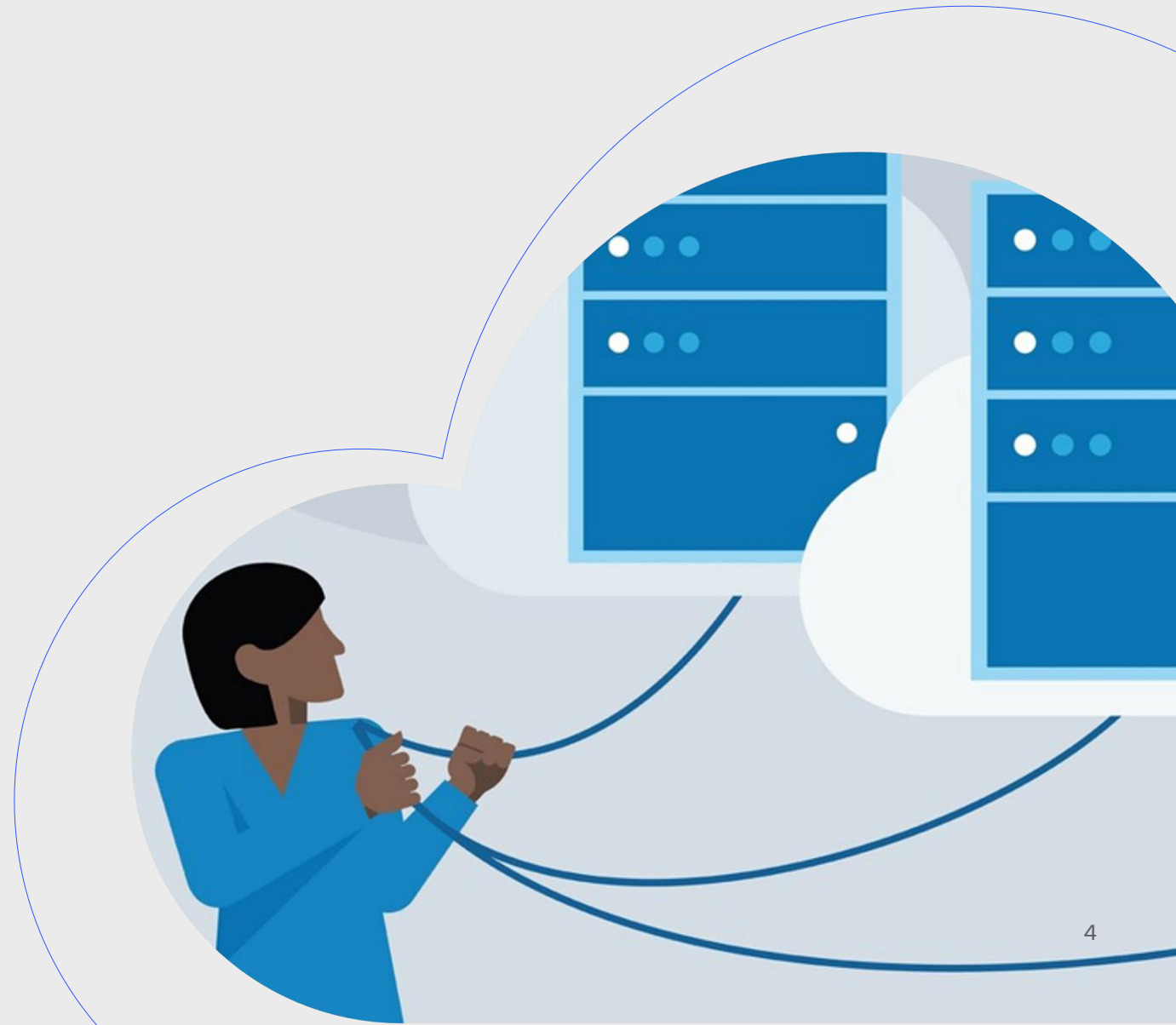


Предоставление ИТ-услуг

«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 VM
4. Групп VM с политиками эластичности под динамические нагрузки
5. Частного облака с мультитенантностью и изоляцией



Совместимость



Профессиональный
инструментарий
для резервного
копирования



Инфраструктура виртуальных
рабочих мест



Программный комплекс средств
виртуализации



Серверная базовая платформа



Централизованное
управление
компьютерами и
учетными записями
пользователей



Active Directory

Механизмы автоматизированного развертывания



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

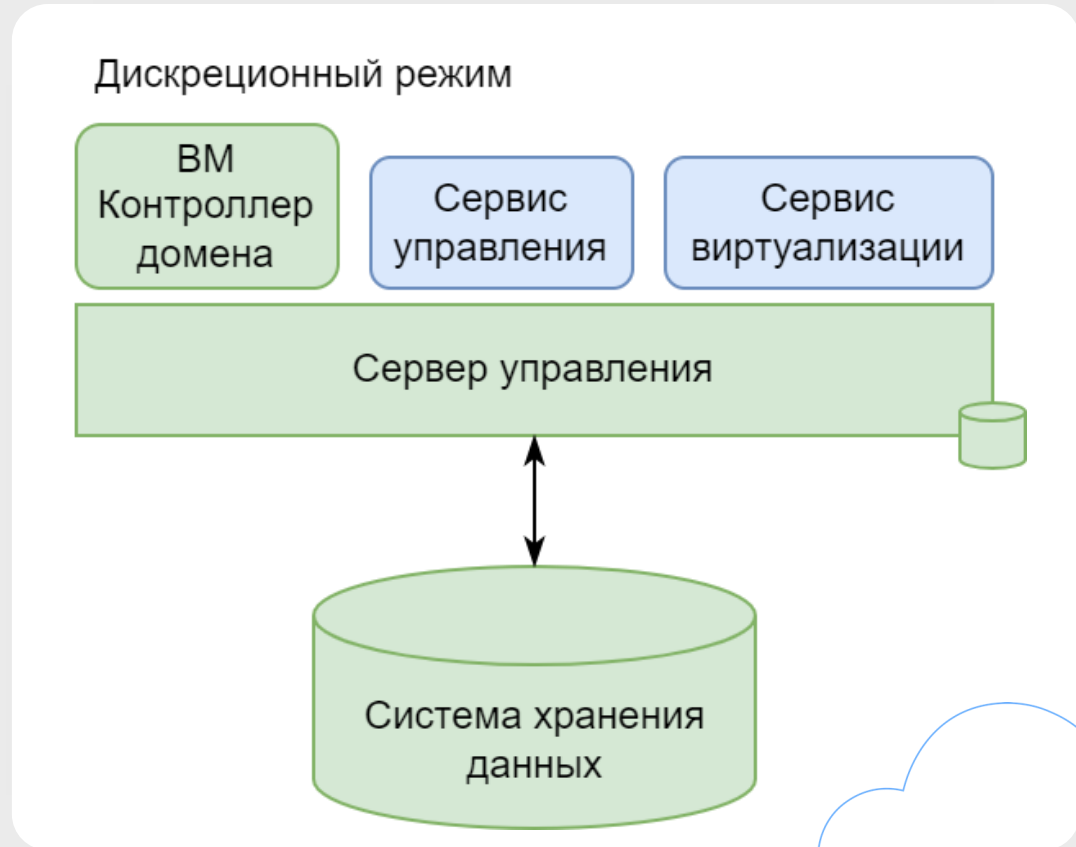
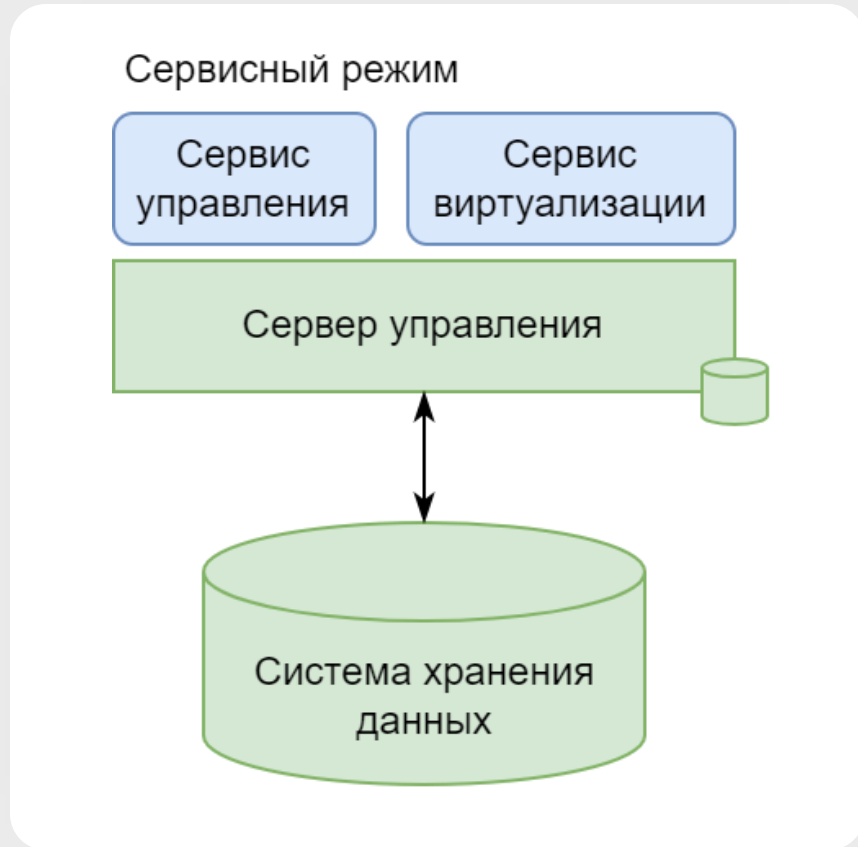
Сеть

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



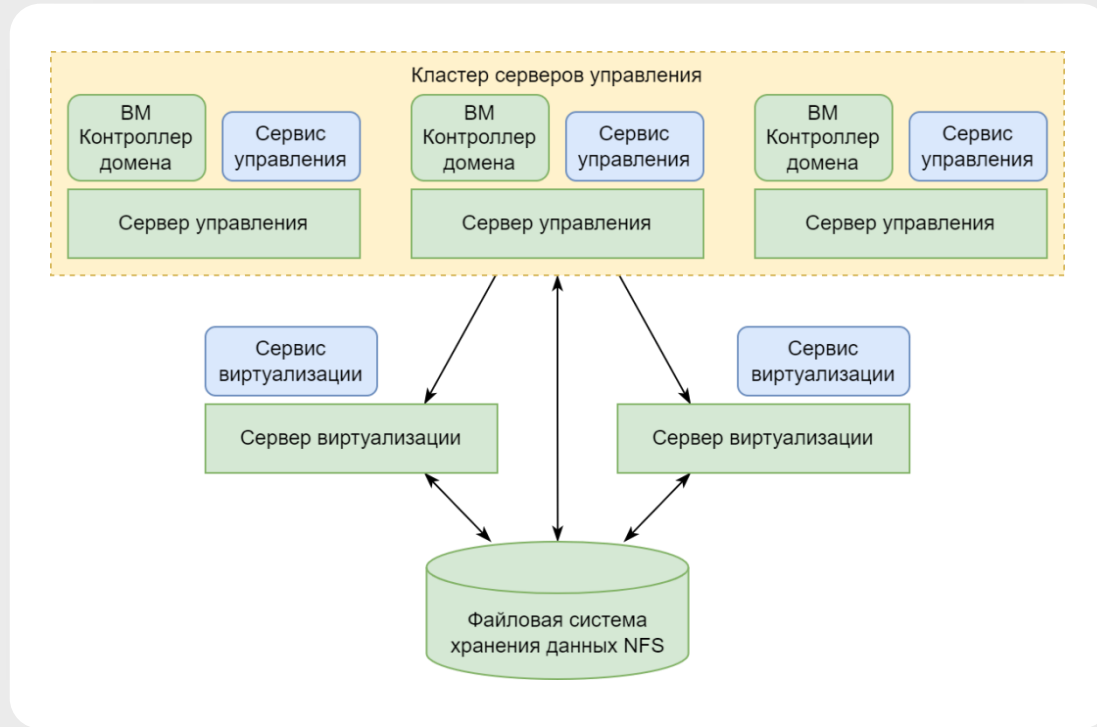
Архитектура продукта

Режимы

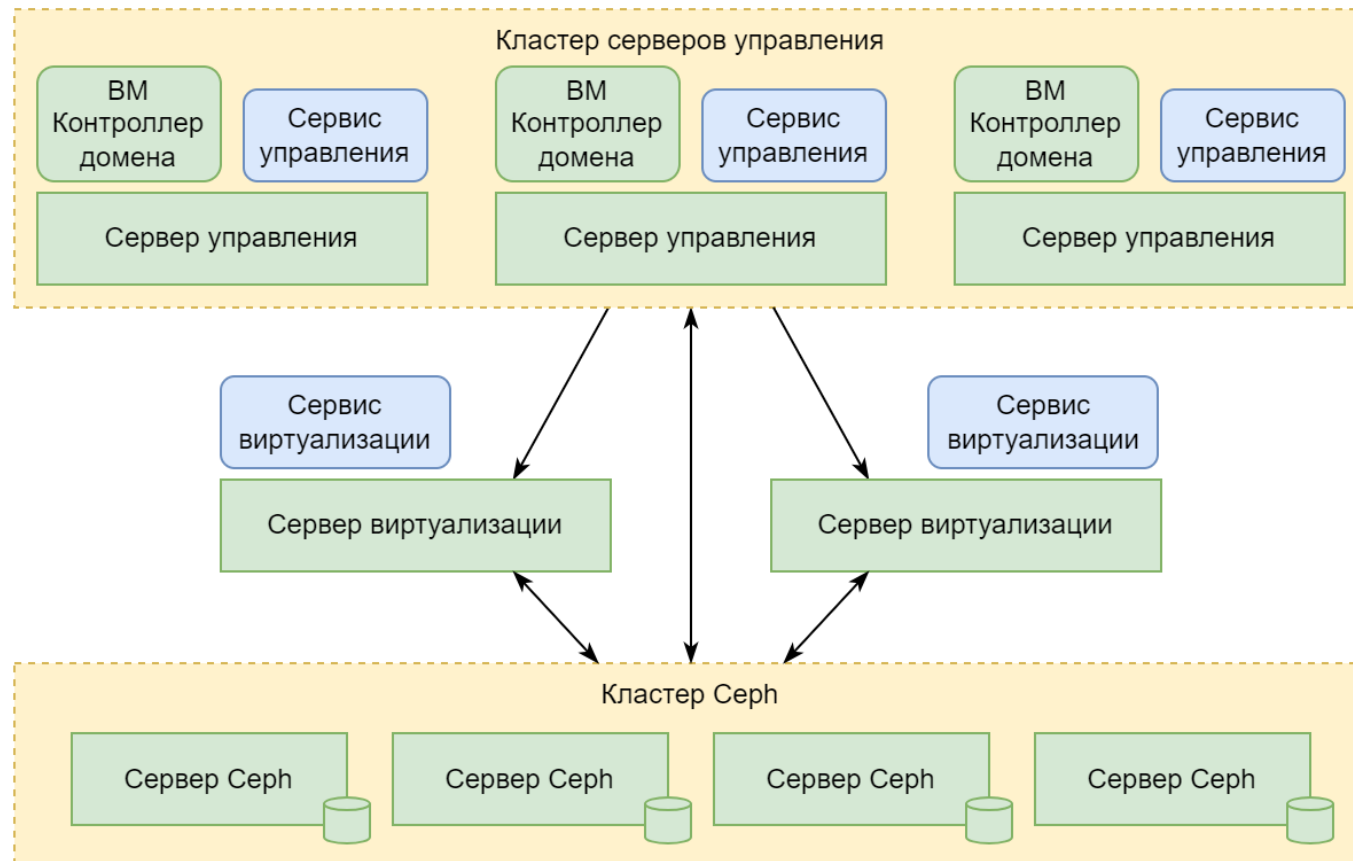


Архитектура продукта

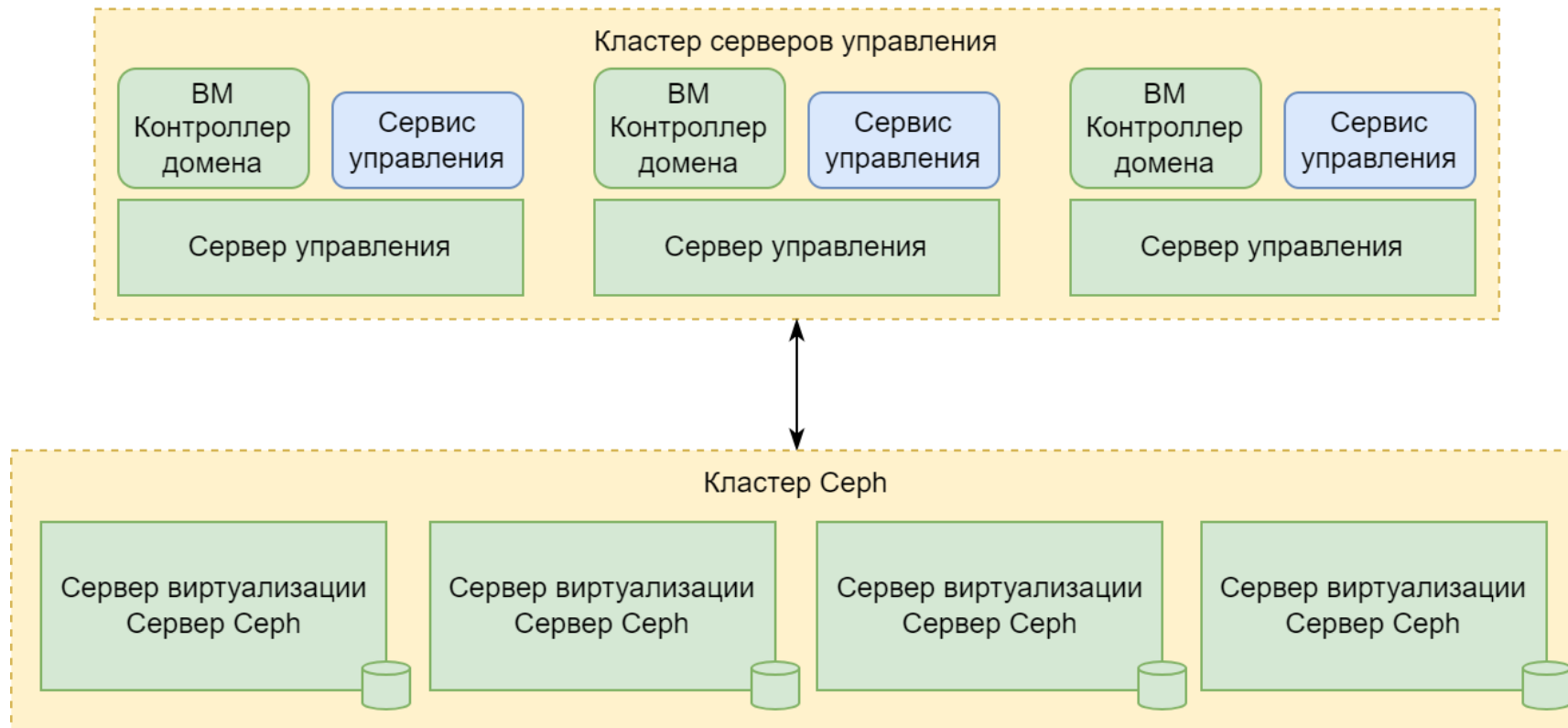
Конвергенция – СХД / NFS



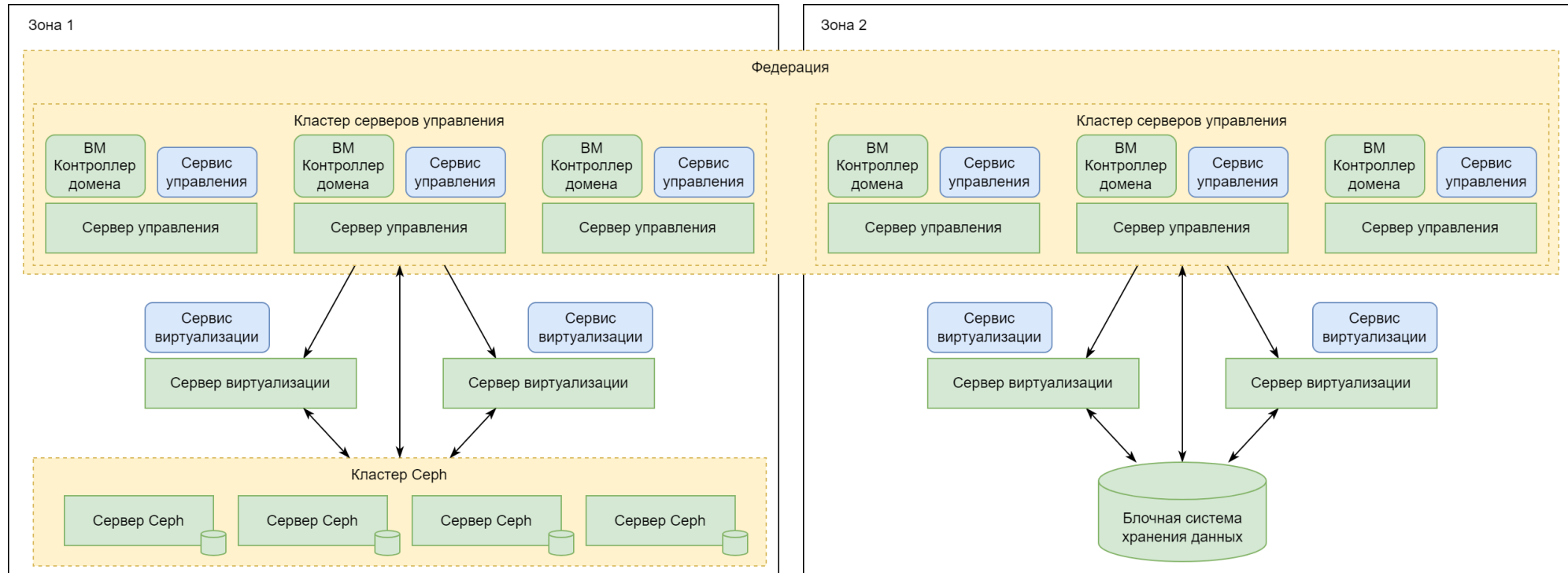
Архитектура продукта Конвергенция – SDS



Архитектура продукта Гиперконвергенция

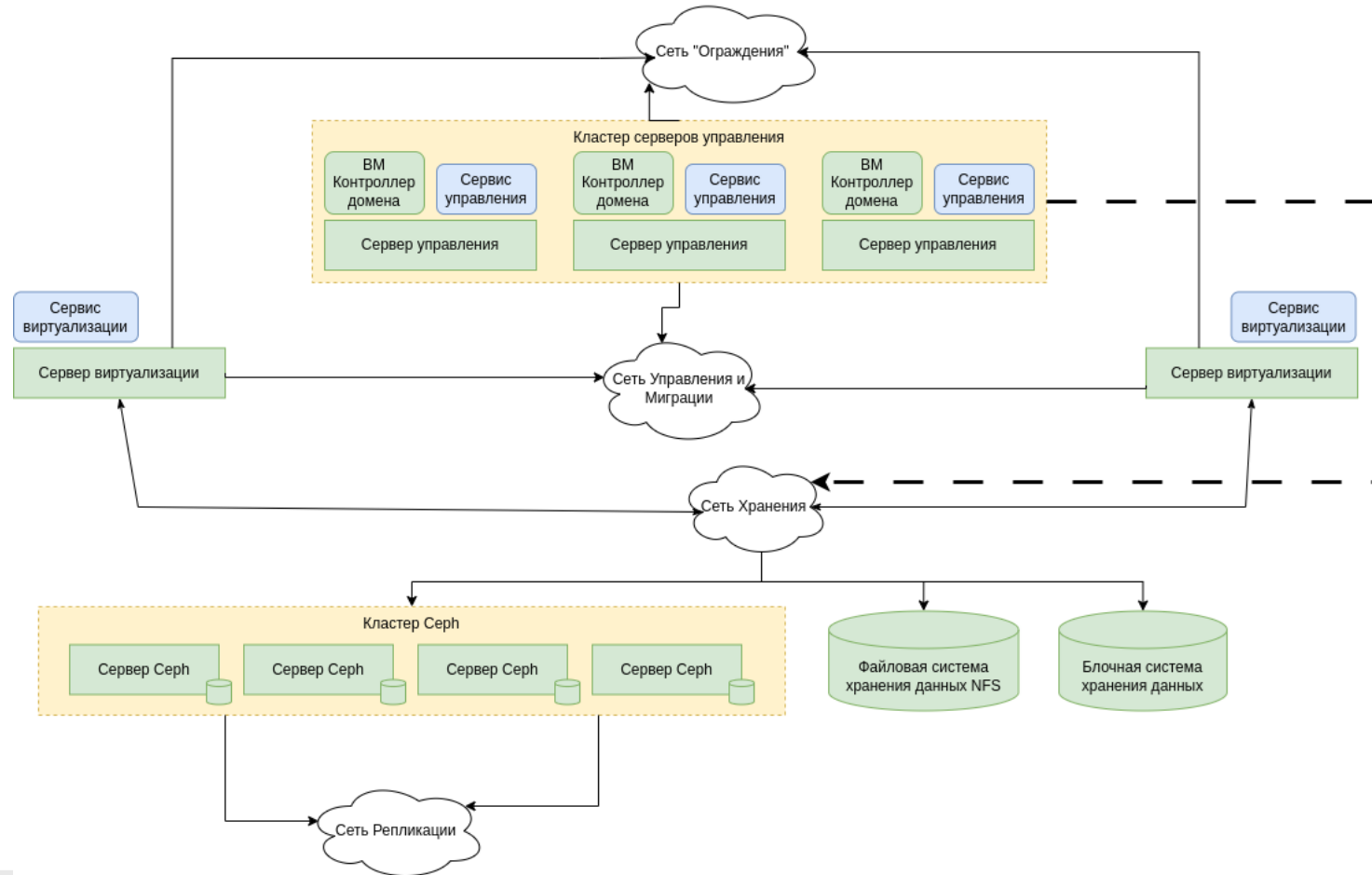


Архитектура продукта Федерация



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 VM
- 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, предназначенный 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
```

I












Методика развертывания

КУБ

Контроллеры домена 1 Серверы управления 3 Серверы виртуализации 3 Серверы без роли 0

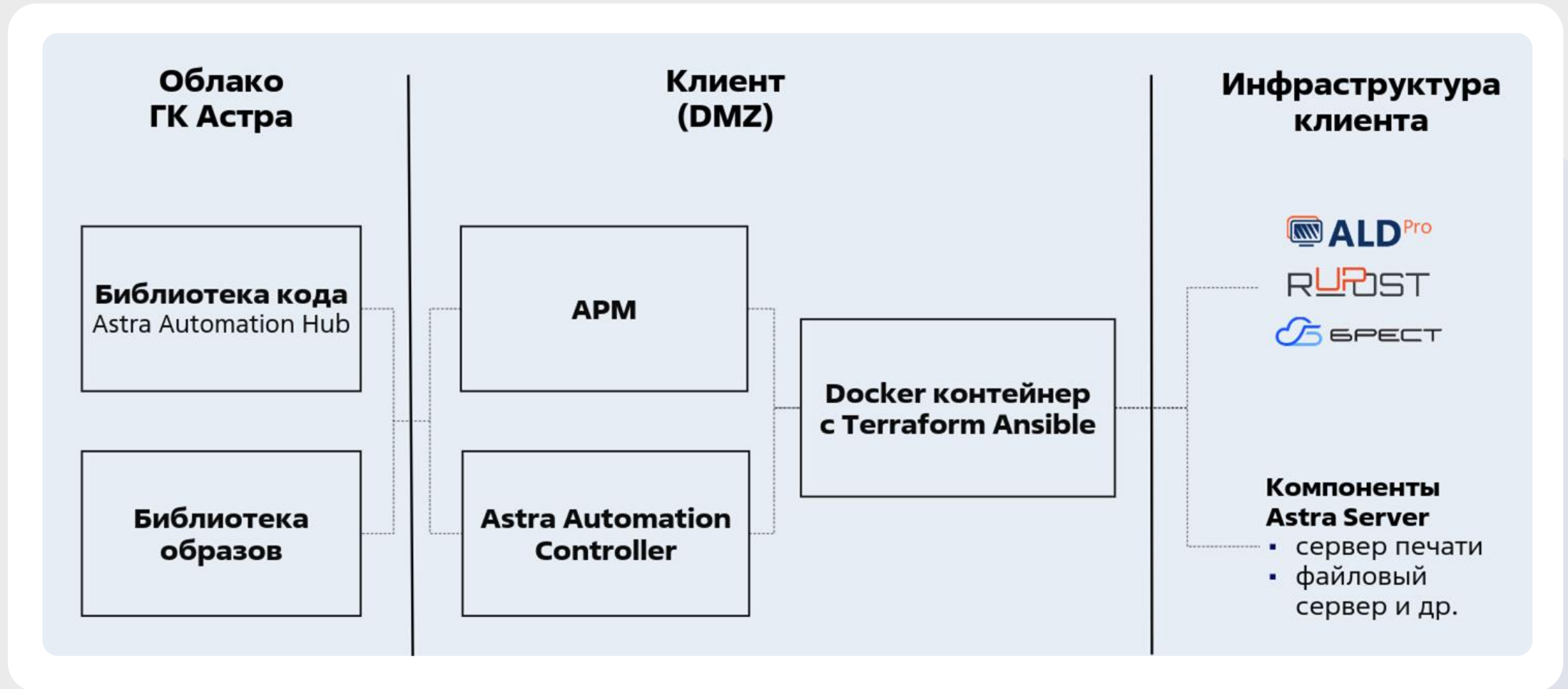
Репозитории ОС Загрузить Выгрузить Применить

	test-freeipa-001   IP 192.168.59.44 Роль Основной контроллер домена Состояние Не в сети	test-brest-001   IP 192.168.59.45 Роль Управление Виртуализация Состояние Не в сети	test-brest-002   IP 192.168.59.46 Роль Управление Виртуализация Состояние Не в сети
	test-brest-003   IP 192.168.59.47 Роль Управление Виртуализация Состояние Не в сети		

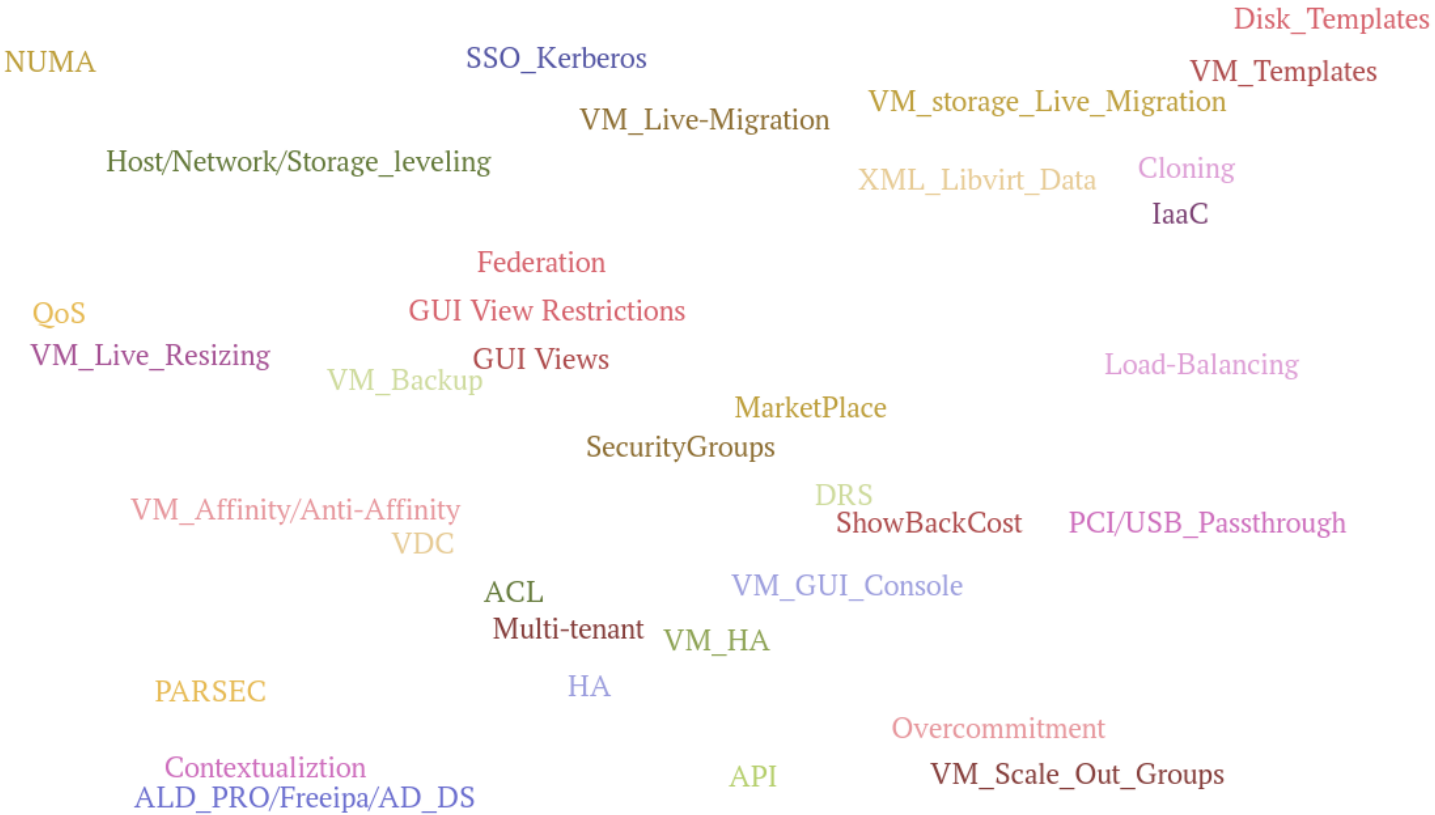


Методика развертывания

IaaS – Astra Automation



Основные функции



Масштабируемость

Кластер управления

- Добавление участников – серверов управления

Хранение:

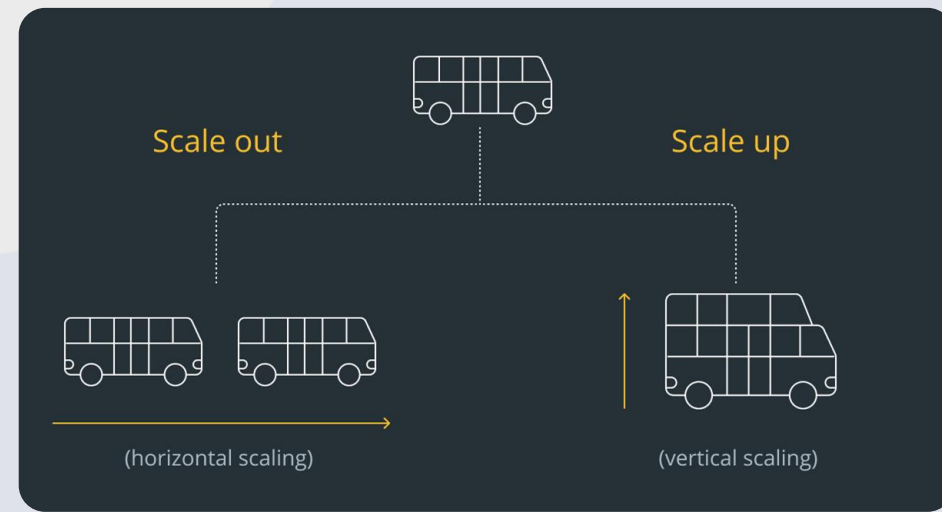
- Добавление LVM PVs и расширение VGs
- Создание новых LVM VGs на базе новых блочных устройств и миграция VM
- Добавление Ceph OSD в существующие Pools и их расширение
- Создание новых Pools на базе новых блочных устройств
- Добавление СХД, участников SDS Ceph / новых кластеров SDS Ceph

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
(OC ALSE)
2. Материнская плата
(OC ALSE)
CPU и инструкции
(OC ALSE)

The screenshot shows the Astra website's 'Compatible Equipment' page. The navigation bar includes 'АСТРА', 'О компании', 'Решения', 'Ready For Astra', 'Поддержка', 'Обучение', 'Партнерам', 'Материалы', 'Пресс-центр', and buttons for 'Где купить' and 'Инвесторам'. The breadcrumb trail is 'Главная > Ready For Astra > Совместимое оборудование'. The main heading is 'Совместимое оборудование' with a count of 197. A search bar is present. Below is a grid of equipment categories with their respective counts:

PTZ-камера 12	Веб-камера 20	Док-станция 5	Интерактивная доска 3	Интерактивная панель 5
Карта видеозахвата 2	Кассовое оборудование 16	Ключевые носители (Токены) 25	Конференц-камера 2	
Концентратор 1	МФУ 385	Модем 4	Моноблок 66	Ноутбук 169
Планшетный компьютер 26	Принтер 166	Рабочая станция 366	СХД 7	Сенсорная панель 3
Сервер 197	Сканер 27	Сканер штрихкода 13	Спикерфон 12	Считыватель смарт-карт 2
Шлем виртуальной реальности 2				

Скрыть ^

AQUARIUS



Atos



Отказоустойчивость

LACP groups – Bonds

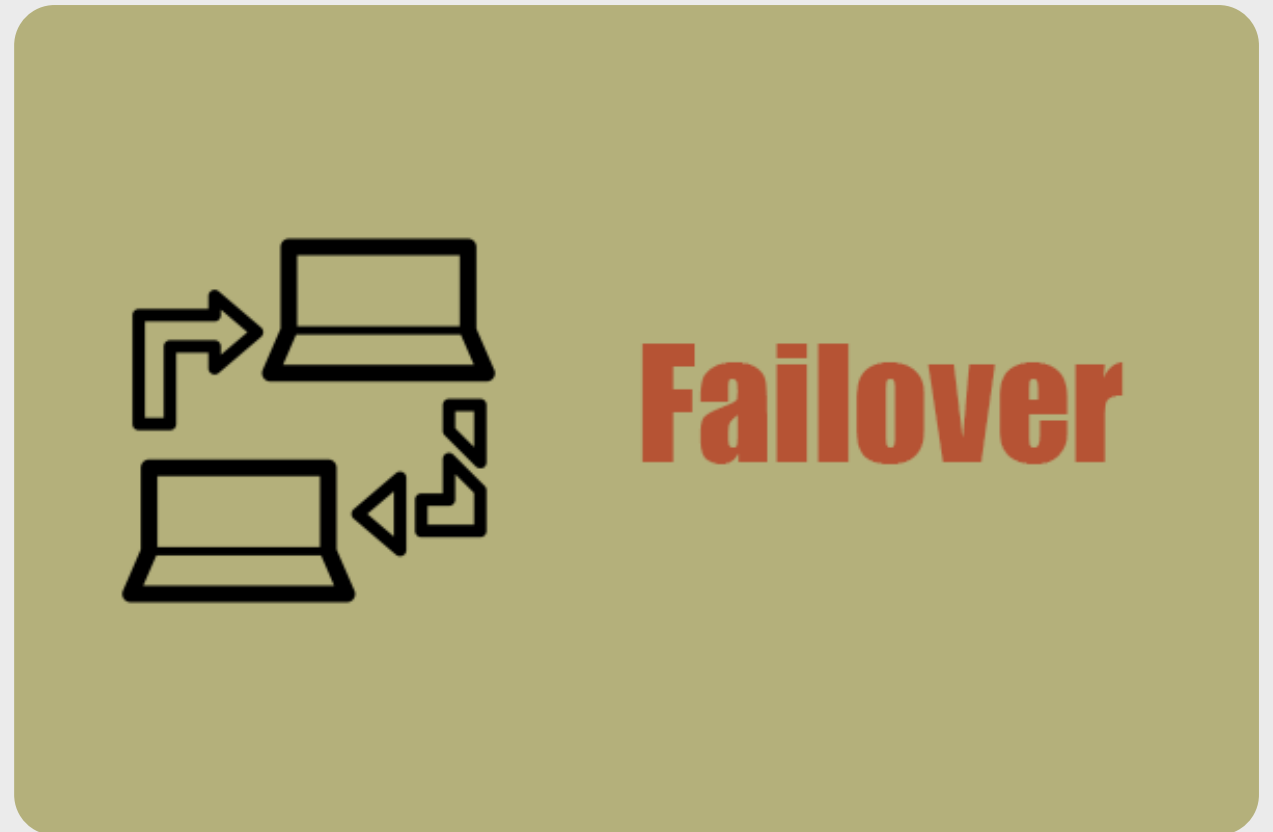
Multipathing

SDS Сeph – кворум мониторов,
репликация данных, CRUSH

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

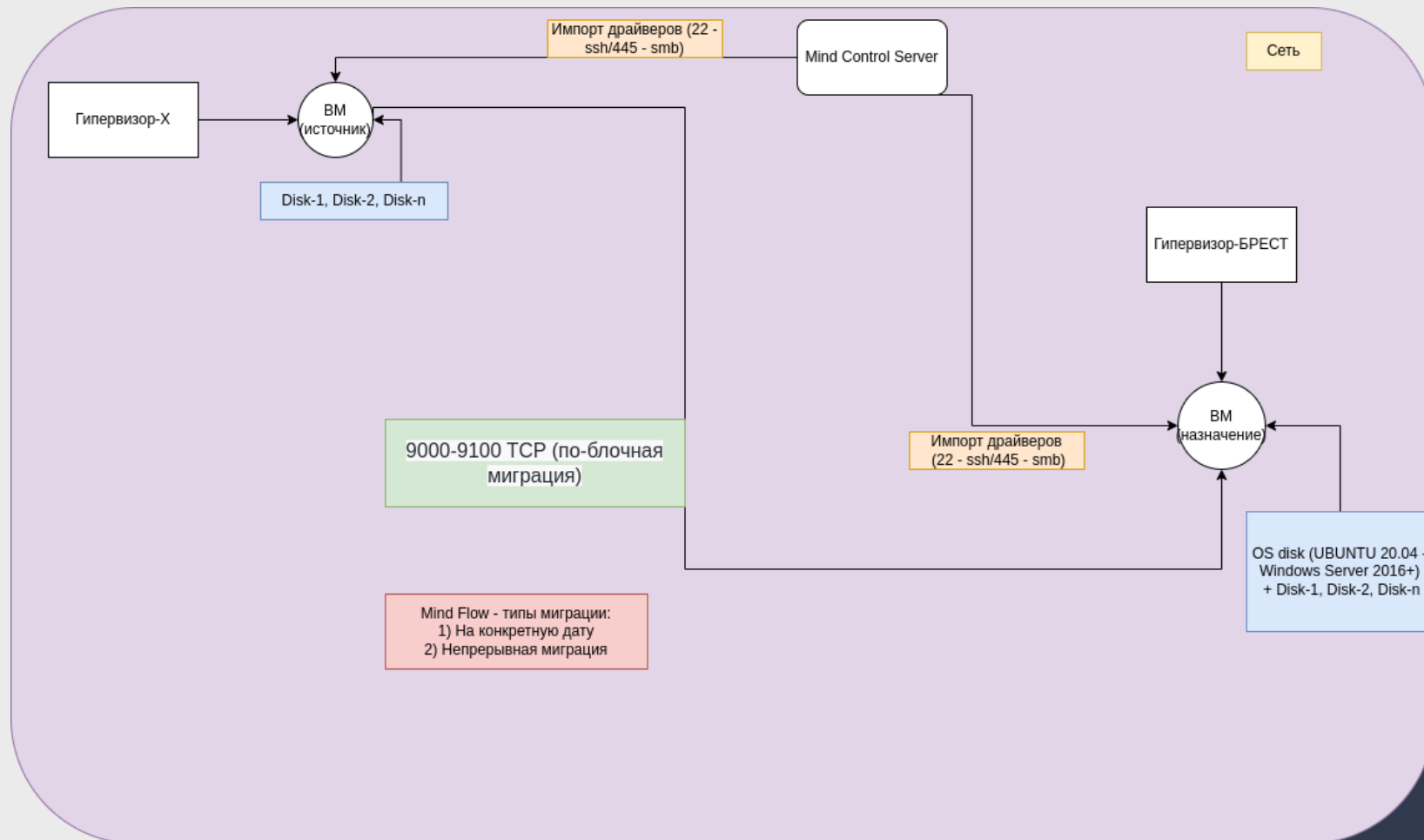
RAFT – кворум серверов управления,
“плавающий” VIP, консистентное
внесение изменений на большинстве
участников

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



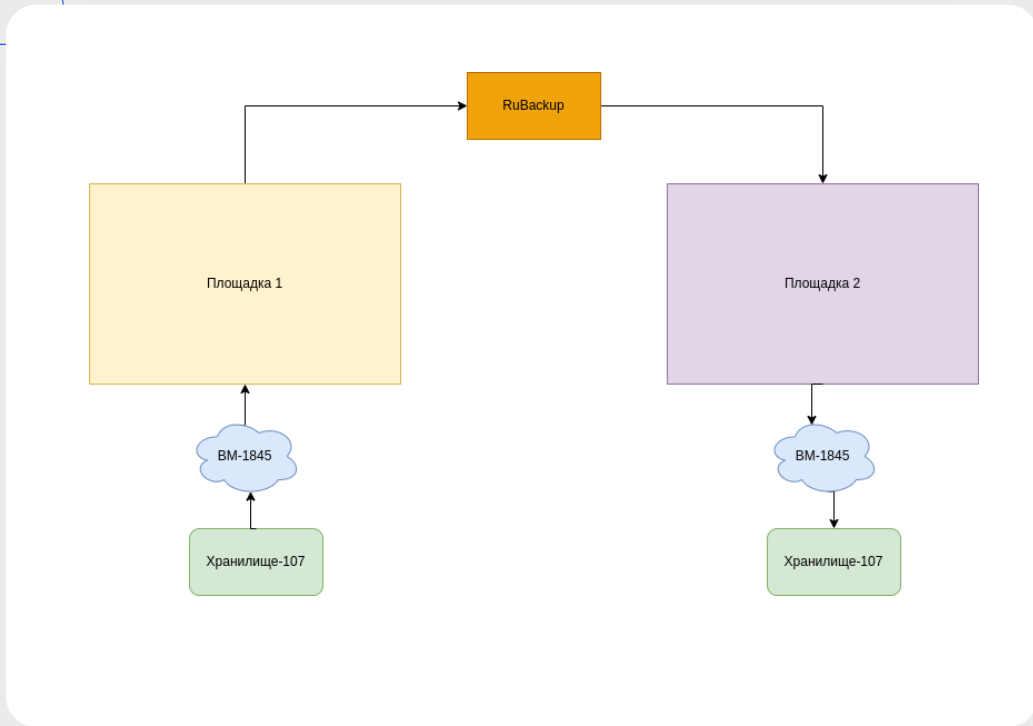
Асинхронная миграция данных на уровне ОС VM

Software Mind – Control & Flow



Асинхронная репликация

RuBackup



RuBackup

Добавить Клонировать Редактировать Удалить Выполнить Включить

ID	Имя клиента	Статус	Тип ресурса	Ресурс	Удаленный клиент	Ресурс назначения	Имя пула
2	astra-front1.bres	run	Brest VM	10	astra-front2.brest.back	/backup_tmp/	block_pool
1	astra-front1.bres	wait	Brest VM	4	astra-front2.brest.back	/backup_tmp/	block_pool

Объекты
Стратегии
Глобальное расписание
Удаленная репликация
Репозиторий
Очередь задач
Серверы RuBackup
Журналы
Администрирование



Astra- МОНИТОРИНГ

Prometheus Node Exporter + Prometheus + Grafana

Brest Cluster info
Brest Management servers
Brest PostgreSQL
Brest PostgreSQL custom metrics
Brest Virtualization servers
Brest VMs info
Node Exporter Full

RAFT status ⊙

brest. [redacted].ru **Solo**

API connection ⊙

https://brest. [redacted].ru:8443/RPC2 **OK**

https://brest. [redacted].ru:8443/RPC2 **Not connected**

WEB console time connection ⊙

~ CPU

CPU utilization ⊙

~ Memory

Memory Basic ⊙

RAFT status ⊙

brest. [redacted].ru **Solo**

RAFT switches ⊙

0

Hosts ⊙

default **7**

Running VMs ⊙

default **7**

1024

~ VMs on all clusters

Running ⊙	Powered ... ⊙	Failed ⊙	Pending ⊙	Hold ⊙	Init ⊙	Cloning ⊙	Clone fail ⊙
1024	105	0	1	0	0	0	0

~ Utilization by clusters

CPU total ⊙	CPU used ⊙	Memory total ⊙	Memory used ⊙
default 67200	default 0	default 3.44 TiB	default 0 KiB
default 76800	default 134392	default 11.8 TiB	default 7.66 TiB

<p>CPU usage (API)</p> <table border="1"> <thead> <tr> <th></th> <th>Last *</th> <th>Mean</th> <th>Min</th> <th>Max</th> </tr> </thead> <tbody> <tr> <td>CPU usage</td> <td>3.08</td> <td>1.89</td> <td>1.01</td> <td>3.08</td> </tr> <tr> <td>CPU Total</td> <td>4</td> <td>4</td> <td>4</td> <td>4</td> </tr> </tbody> </table>		Last *	Mean	Min	Max	CPU usage	3.08	1.89	1.01	3.08	CPU Total	4	4	4	4	<p>Memory usage (API)</p> <table border="1"> <thead> <tr> <th></th> <th>Last *</th> <th>Mean</th> <th>Min</th> <th>Max</th> </tr> </thead> <tbody> <tr> <td>Memory usage</td> <td>2.99 GiB</td> <td>2.99 GiB</td> <td>2.99 GiB</td> <td>2.99 GiB</td> </tr> <tr> <td>Total memory</td> <td>4 GiB</td> <td>4 GiB</td> <td>4 GiB</td> <td>4 GiB</td> </tr> </tbody> </table>		Last *	Mean	Min	Max	Memory usage	2.99 GiB	2.99 GiB	2.99 GiB	2.99 GiB	Total memory	4 GiB	4 GiB	4 GiB	4 GiB
	Last *	Mean	Min	Max																											
CPU usage	3.08	1.89	1.01	3.08																											
CPU Total	4	4	4	4																											
	Last *	Mean	Min	Max																											
Memory usage	2.99 GiB	2.99 GiB	2.99 GiB	2.99 GiB																											
Total memory	4 GiB	4 GiB	4 GiB	4 GiB																											
<p>Disk write/read ⊙</p> <table border="1"> <thead> <tr> <th></th> <th>Last *</th> <th>Mean</th> <th>Min</th> <th>Max</th> </tr> </thead> <tbody> <tr> <td>Read</td> <td>0 MB/s</td> <td>0 MB/s</td> <td>0 MB/s</td> <td>0 MB/s</td> </tr> <tr> <td>Write</td> <td>0 MB/s</td> <td>0 MB/s</td> <td>0 MB/s</td> <td>0 MB/s</td> </tr> </tbody> </table>		Last *	Mean	Min	Max	Read	0 MB/s	0 MB/s	0 MB/s	0 MB/s	Write	0 MB/s	0 MB/s	0 MB/s	0 MB/s	<p>Disk IOPS ⊙</p> <table border="1"> <thead> <tr> <th></th> <th>Last *</th> <th>Mean</th> <th>Min</th> <th>Max</th> </tr> </thead> <tbody> <tr> <td>Read IOPS</td> <td>0 io/s</td> <td>0.00430 io/s</td> <td>0 io/s</td> <td>0.0190 io/s</td> </tr> <tr> <td>Write IOPS</td> <td>1.02 io/s</td> <td>0.969 io/s</td> <td>0 io/s</td> <td>1.95 io/s</td> </tr> </tbody> </table>		Last *	Mean	Min	Max	Read IOPS	0 io/s	0.00430 io/s	0 io/s	0.0190 io/s	Write IOPS	1.02 io/s	0.969 io/s	0 io/s	1.95 io/s
	Last *	Mean	Min	Max																											
Read	0 MB/s	0 MB/s	0 MB/s	0 MB/s																											
Write	0 MB/s	0 MB/s	0 MB/s	0 MB/s																											
	Last *	Mean	Min	Max																											
Read IOPS	0 io/s	0.00430 io/s	0 io/s	0.0190 io/s																											
Write IOPS	1.02 io/s	0.969 io/s	0 io/s	1.95 io/s																											



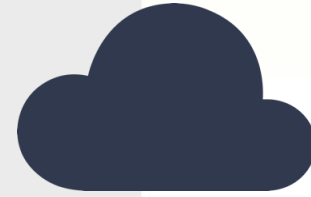
Информационная безопасность

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



CERTIFIED

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 VM, 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 VM
14. Интегрированный VPN-сервер
15. OSPF/BGP Edge
16. Журналирование сетевых пакетов VM
17. Thick Provisioning для виртуальных дисков



КУБ

Развитие функционала



Обслуживание физической составляющей



Добавление / удаление серверов-участников кластеров



Подключение хранилищ



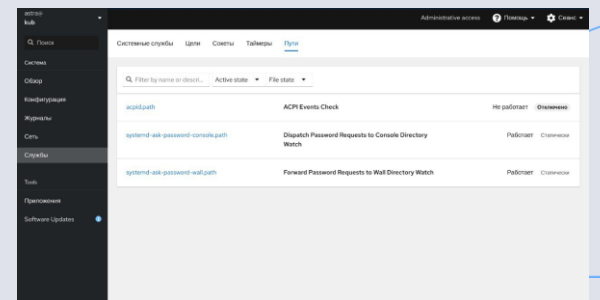
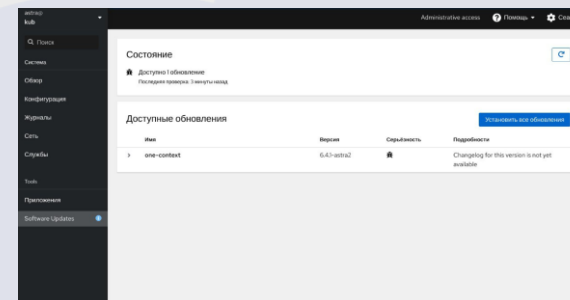
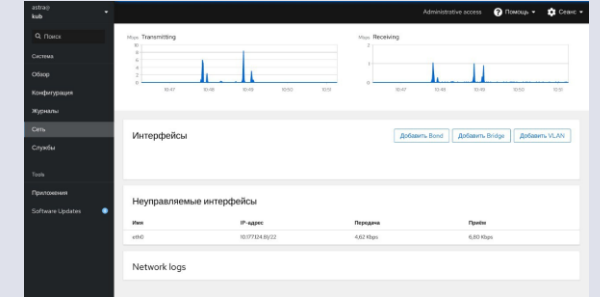
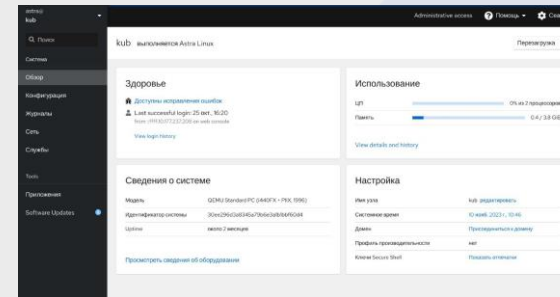
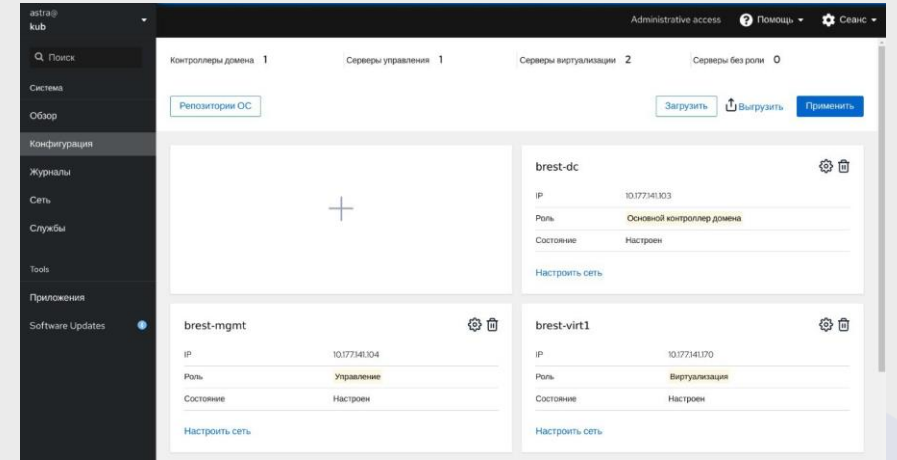
Централизованное обновление кластеров гипервизоров и управления



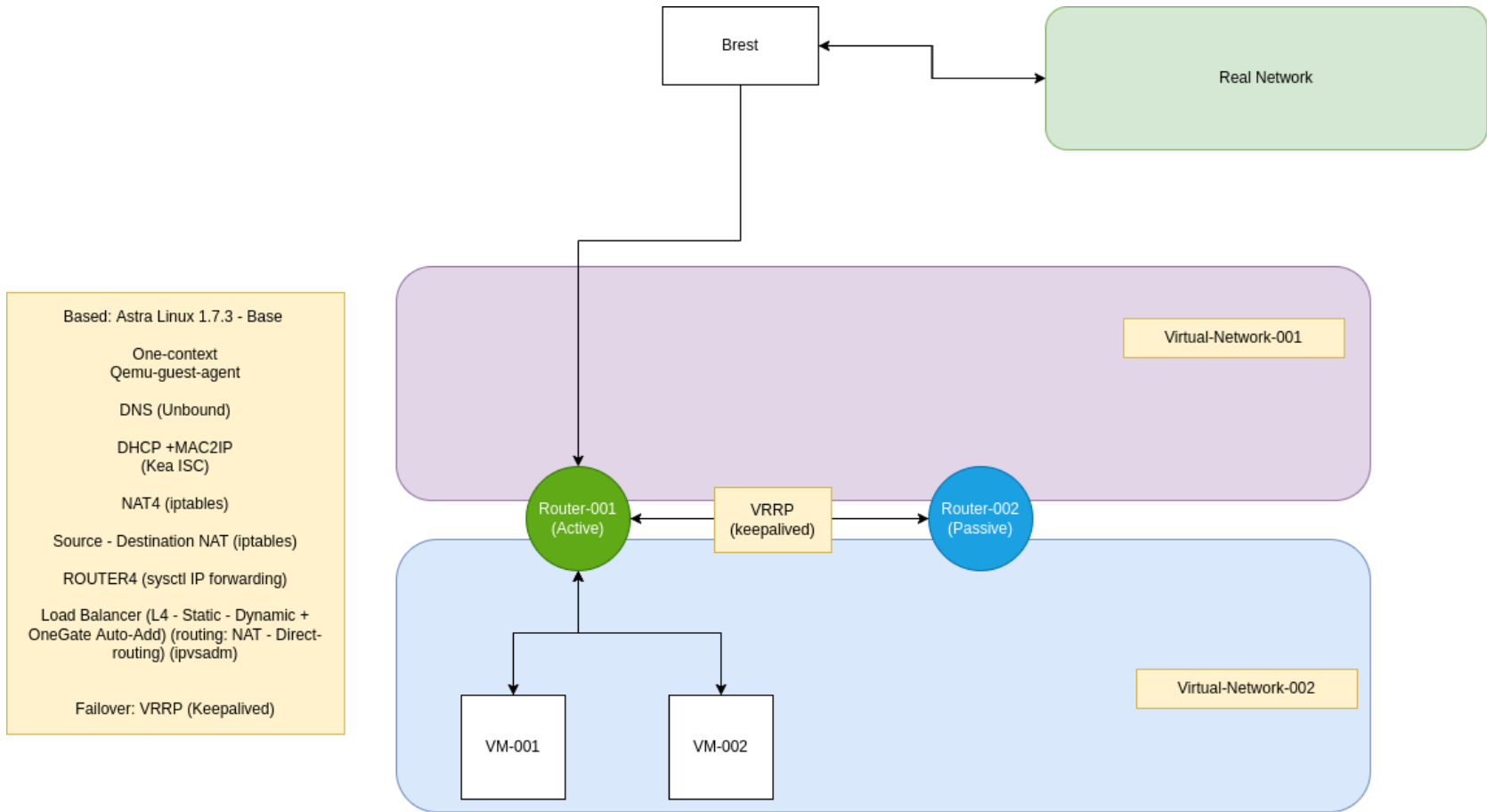
Развертывание SDS Серв



Настройка backend-части сетей

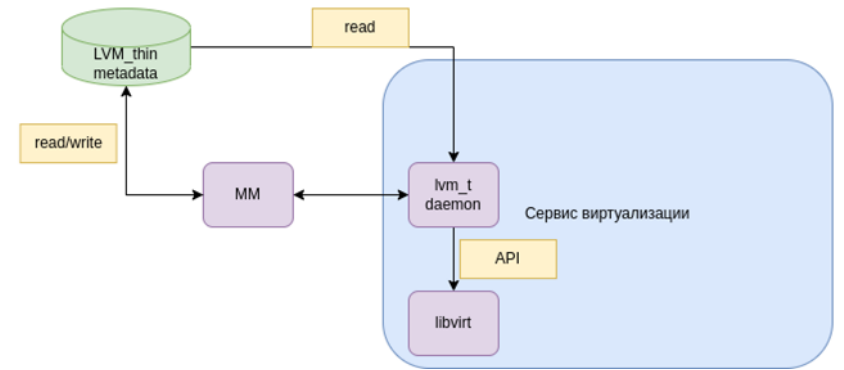
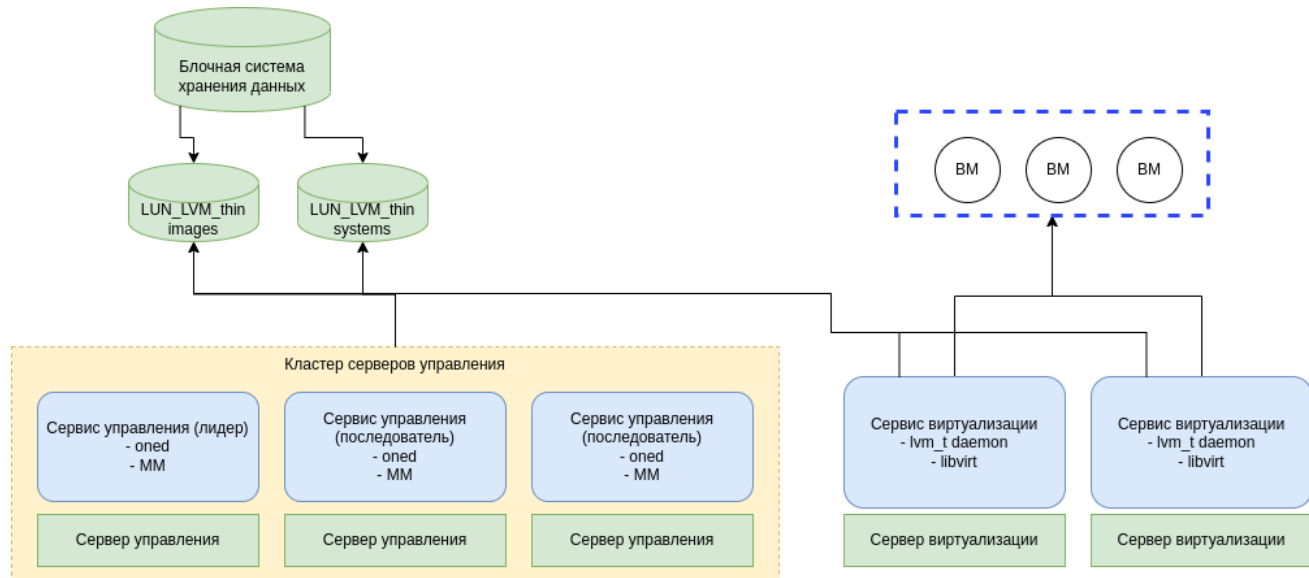


Виртуальный маршрутизатор



Асинхронная репликация

RuBackup



**Спасибо
за внимание!**

