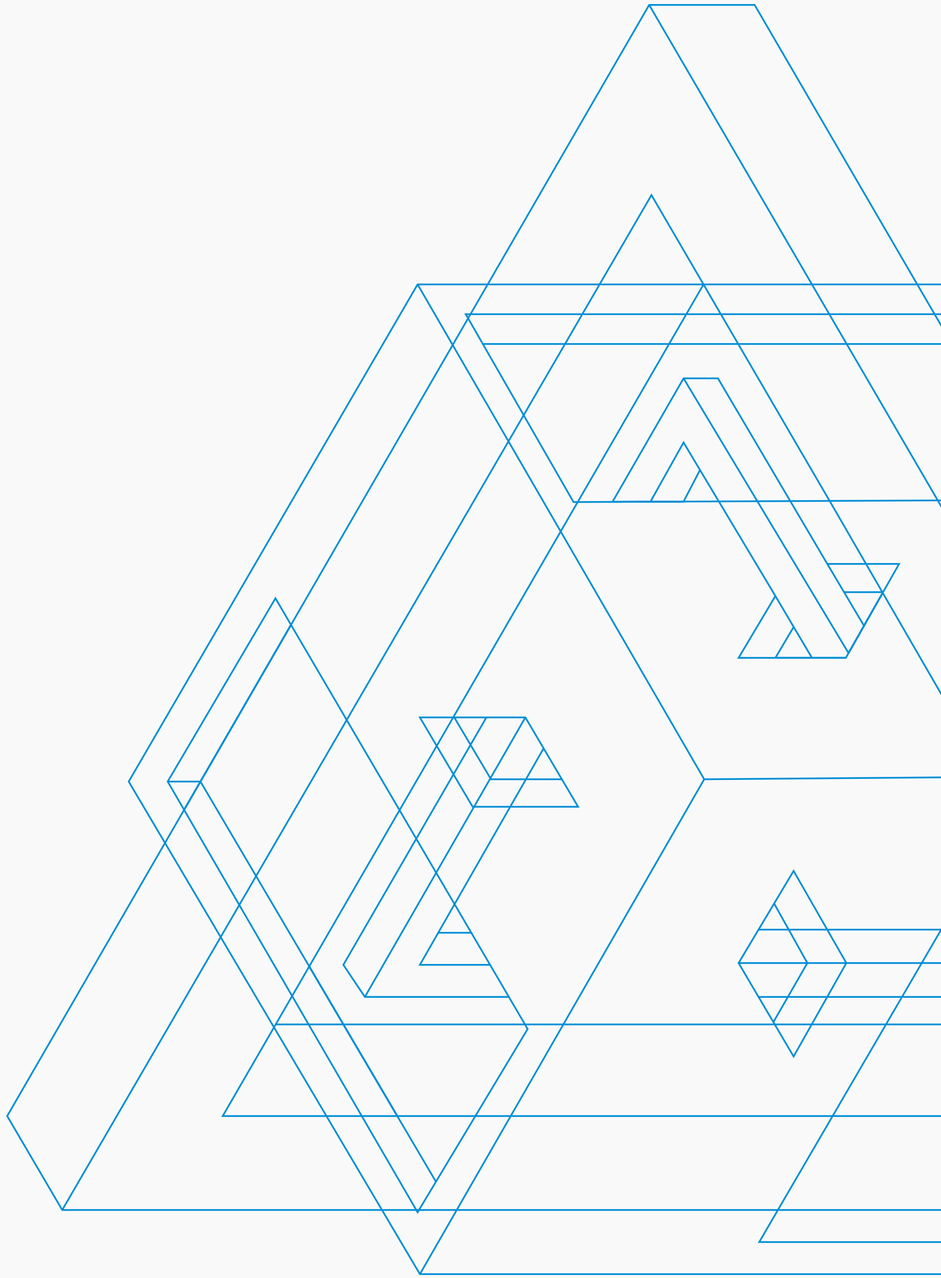
Техническая презентация продуктов АО «БФГ»

ПК «Звезда»: СВ «Звезда» · Прокуратор · Сфера · VDI Звезда · Рефлект · РСХД «Шторм»



Проблематика

Необходимость импортозамещения



Согласно указу Президента РФ № 166 об использовании технологически независимых компонентов в критической инфраструктуре страны, а также в связи с санкциямии ограничениями лицензирования (например, уход VMware, Microsoft и Red Hat) компаниям приходится искать альтернативу решениям виртуализации

Риски блокировки и обновлений



Использование иностранных гипервизоров может привести к:

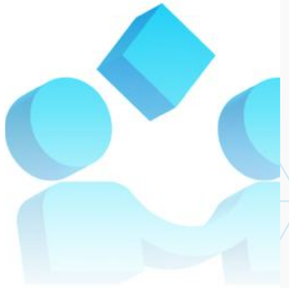
- Блокировке активаций или подписок
- Невозможности обновления и устранения уязвимостей
- Юридическим рискам при эксплуатации нелицензионного ПО

Обеспечение цифрового суверенитета и безопасности



- Критически важные данные государства и бизнеса должны размещаться в инфраструктуре, полностью контролируемой внутри страны
- Отечественные платформы могут проходить сертификацию ФСТЭК и ФСБ, что является ключевым требованием для госорганов и госкорпораций

Кадровая переориентация



- Персонал, привыкший к интерфейсу VMware/ Hyper-V, нуждается в переобучении
- Рынок испытывает нехватку квалифицированных специалистов, работающих с новыми российскими продуктами виртуализации

Угрозы применения импортных технологий в КИИ

Реальность

- Отечественные серверные платформы продолжают использовать процессоры **Intel** и **AMD**
- Значительная часть аппаратной базы серверной инфраструктуры зависит от зарубежных производителей компонентов **Samsung, Western Digital, Adata, Toshiba** и т.д.
- Многие существующие решения виртуализации построены на базе зарубежных open-source и коммерческих платформ **(oVirt, OpenNebula, OpenStack, Citrix Xen)**

Риски

- Закладки и уязвимости в чужом ПО и «железе»
- Зависимость от иностранных технологий
- Зависимость от иностранных обновлений и лицензий
- Возможность кибератак через скрытые механизмы

Пример

Кибератака на «Аэрофлот» – в цепочке использовался продукт на базе oVirt (США)

Вывод

Такие системы не являются доверенными, нарушают Указ №166 и угрожают нацбезопасности

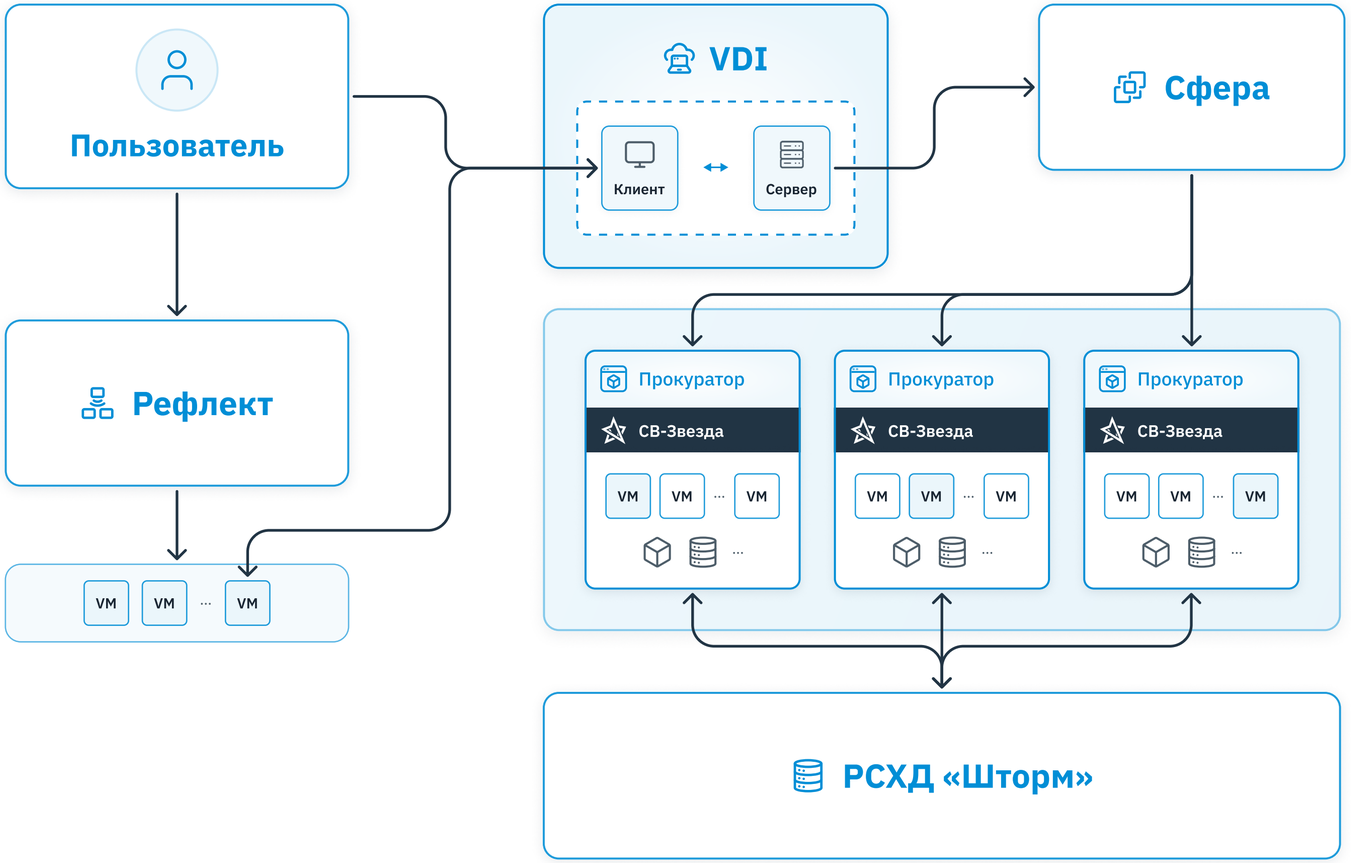
Экосистема продуктов компании АО «БФГ»



Экосистема продуктов компании АО «БФГ»

Полный стек решений для построения, управления и эксплуатации виртуальной инфраструктуры

Каждый продукт решает специфическую задачу, вместе они создают единый стек виртуализации, готовый к масштабированию и поддержке критичных бизнес-процессов



Компоненты ПК «Звезда»

СВ «Звезда»
Гипервизор 1-го типа

Прокуратор
Система управления гипервизором

Сфера
Система оркестрации виртуальной инфраструктуры

VDI «Звезда»
Платформа виртуальных рабочих мест

РЕФЛЕКТ
Протокол доставки рабочего стола

РСХД «Шторм»
Распределённая система хранения данных

Экосистема продуктов компании АО «БФГ»

Полный стек решений для построения, управления и эксплуатации виртуальной инфраструктуры

Сфера

Уровень управления всей инфраструктуры

- Единая аутентификация
- RBAC и роли
- Политики доступа
- Аудит и журналирование

Логическая структура инфраструктуры

Зоны → Датацентры → Кластеры

Прокураторы

Управление физическими хостами в составе кластеров

- Прокуратор (хост 1)
- Прокуратор (хост 2)
- Прокуратор (хост 3)
- Прокуратор (хост N)

Прокураторы (хосты)

В Сфере может быть один или несколько Прокураторов

Ресурсы каждого Прокуратора

- Виртуальные машины
- Сети
- Хранилища
- Бэкапы

В каждой категории может быть несколько объектов (например, несколько ВМ, сетей, хранилищ и бэкапов).

Решение ПК «Звезда»

Единая экосистема решений для виртуализации, управления инфраструктурой и построения отказоустойчивых ИТ-сред



Почему решение ПК «Звезда» надежно для заказчика

Российская разработка

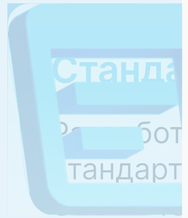
Российская разработка АО «БФГ» с полным контролем кода и возможностью адаптации под задачи заказчика

Реестр российского ПО

Решение включено в Реестр Минцифры России №16845

Стандарты и сертификация

Разработано по группе стандартов РБПО. Сертификат СВЗ №4934 от 05.05.2025



Базовая виртуализация

Единая экосистема управления серверами и ЦОДами: гипервизор, VDI, хранилище данных и смежные компоненты

Снижение рисков открытого кода

Решение развивается с 2009 года, без уязвимостей и рисков, связанных с «чужим» кодом

Восстановление после инцидентов

Возможность оперативного восстановления ИТ-инфраструктуры после сбоев с гарантированным SLA

Сегментация инфраструктуры

Функционал «папок» создан как часть архитектуры и упрощает управление виртуальной средой

Масштаб эксплуатации

Под управлением ПК «Звезда» сегодня работает около 500 тыс. виртуальных машин

Совместимость с ОС и платформами

Поддерживаются известные базовые операционные системы, включая основные российские, и стандартные серверные платформы

Интеллектуальная балансировка

Автоматическое распределение виртуальной инфраструктуры для стабильной работы и оптимального использования ресурсов

Оптимизация под высокие нагрузки

Собственные специализированные компоненты повышают эффективность использования серверного оборудования

Промышленная надежность и высокий уровень ИБ

Надежность и масштабирование

Отказоустойчивая архитектура

Архитектура решения продолжает работать при любом сценарии

Масштабирование до десятков тысяч ВМ

Поддерживается гибкое масштабирование инфраструктуры до десятков тысяч виртуальных машин в кластере

Стабильная работа при перегрузках

Система сохраняет качество работы при переподписке до 6:1 и выше, в зависимости от конфигурации серверного оборудования

Ускоренное расширение инфраструктуры

Реализована технология быстрого масштабирования без перестройки архитектуры

Кластер высокой доступности

Работа в HA-кластере до 256 узлов

Информационная безопасность

Сертифицированный гипервизор ФСТЭК

Гипервизор 1-го типа сертифицирован ФСТЭК России №4934 от 05.05.2025 как средство защиты информации

Соответствие требованиям регуляторов

Поддержка требований КИИ до 1-й категории значимости, ИСПДн до 1 уровня, ГИС и АСУ ТП до 1 класса защищенности

Усиленная защита на уровне архитектуры

Встроенные параметры ИБ реализованы на архитектурном уровне платформы

Защищенная аппаратная сеть

Взаимодействие ВМ через защищенную аппаратную сеть без программной эмуляции

Аппаратное усиление изоляции ВМ

Возможно дополнительное усиление ИБ за счёт аппаратной реализации (ПАК «Звезда»), радикально повышающей защищённость ИТ-инфраструктуры за счёт аппаратной изоляции между ВМ с использованием отечественного интерконнекта «Альфа», сертифицированного ФСТЭК, и обеспечивающей возможность взаимодействия ВМ через защищённую аппаратную сеть без программной эмуляции.

Безопасное использование гостевых систем

Возможность безопасной работы с несертифицированными гостевыми ОС и ПО

Виртуализация и управление инфраструктурой



Собственный стек управления виртуализацией

Отказ от промежуточного слоя libvirt обеспечивает прямое управление гипервизором, ресурсами и жизненным циклом ВМ

Традиционный подход с libvirt

Промежуточный слой управления

Платформа управления
oVirt / OpenNebula / другие решения

↓

libvirt
Универсальный API для управления гипервизорами

↓

QEMU / KVM
Гипервизор и механизм виртуализации

↓

Виртуальные машины
Гостевые ОС и приложения

Библиотека и API для управления различными гипервизорами через единый интерфейс

VS

Архитектура виртуализации ПК «Звезда»

Прямое управление без промежуточных слоев

Прокуратор
Управление инфраструктурой и виртуальными ресурсами

↓

Собственный драйвер управления
Прямое управление QEMU/KVM без libvirt

↓

QEMU / KVM
Гипервизор и механизм виртуализации

↓

Виртуальные машины
Гостевые ОС и приложения

Прямой контроль над гипервизором, ресурсами и жизненным циклом ВМ без промежуточных слоев

Плюсы libvirt

- Универсальность API
- Быстрая интеграция
- Большая экосистема

Минусы libvirt

- Дополнительный слой
- Ограничения API
- Сложная отладка

Плюсы нативного подхода

- Прямое управление API
- Максимальный контроль
- Оптимизация задержек

Минусы нативного подхода

- Выше стоимость разработки
- Поддержка драйверов
- Больше ответственности

Вывод ПК «Звезда» сохраняет проверенный и производительный гипервизор QEMU/KVM, но использует собственный механизм управления вместо libvirt для максимального контроля и эффективности

Подробное описание преимуществ использования собственного драйвера управления виртуализацией

Плюсы libvirt

- **Универсальность:** единый API для разных гипервизоров
- **Быстрая интеграция:** готовые инструменты и поддержка
- **Большая экосистема:** широкое сообщество и совместимость
- **Совместимость:** поддерживается большинством open-source платформ

Минусы libvirt

- **Избыточная универсальность:** Библиотека проектировалась как универсальный слой управления различными гипервизорами, что увеличивает сложность интеграции для специализированных решений.
- **Ограниченная адаптация под собственную архитектуру:** Реализация специфических сценариев (нестандартные типы хранилищ, сетевые механизмы, собственные сервисы управления) требует дополнительных слоёв интеграции и обходных решений.
- **Архитектурные ограничения:** Развитие платформы ограничивается возможностями и архитектурой libvirt, а внедрение новых функций зависит от поддержки в библиотеке.
- **Ограниченная оптимизация под конкретную платформу:** Libvirt разрабатывался как универсальная библиотека и не оптимизирован под требования отдельных коммерческих решений, что усложняет глубокую интеграцию с их архитектурой.
- **Дополнительные накладные расходы:** Промежуточный слой увеличивает количество компонентов, участвующих в обработке команд управления и взаимодействии с гипервизором.

Плюсы нативного подхода

- Прямое управление ВМ без промежуточных слоёв.
- Максимальный контроль над ресурсами (CPU, память, сеть, хранилища).
- Более глубокая телеметрия и наблюдаемость.
- Тесная интеграция с Sphere, HA, DRS, Live Migration и другими компонентами.
- Независимость от внешнего API и roadmap сторонних проектов.
- Оптимизация производительности и поведения под собственную платформу.
- Расширенные возможности для проектирования бэкапов

Минусы нативного подхода

- **Выше стоимость разработки:** требуется собственная разработка и поддержка драйвера.
- **Необходимо самостоятельно поддерживать драйвер** и обеспечивать его стабильность.
- **Больше ответственности за совместимость версий QEMU/KVM.**
- **Требуется собственная экспертиза** и компетенции команды.

Типичные сценарии

- Реализация поддержки нескольких типов хранилищ (NFS, FC, iSCSI, SDS) требует дополнительных адаптеров и слоёв интеграции
- Интеграция собственных механизмов HA, DRS и мониторинга ограничивается архитектурой libvirt.
- Добавление новых возможностей управления QEMU/KVM требует учёта ограничений универсального API.

Многоуровневая архитектура управления виртуальной инфраструктурой ПК «Звезда»

Экосистема ПК «Звезда» построена по принципу иерархического управления, где каждый уровень решает свои задачи и взаимодействует с соседними уровнями, обеспечивая надежную, масштабируемую и безопасную работу инфраструктуры

Собственный драйвер управления обеспечивает взаимодействие между уровнями виртуализации, управления хостами и централизованной оркестрацией

Сфера
Система оркестрации виртуальной инфраструктуры

→ Управление кластерами, ресурсами, политиками размещения и пользователями

Прокуратор
Управление единичным хостом

→ Выполнение операций жизненного цикла ВМ, управление сетями, хранилищами и ресурсами отдельных серверов

Собственный драйвер управления ВМ
Прямое взаимодействие с QEMU/KVM без промежуточных слоёв

→ Прямое взаимодействие с QEMU/KVM и управление виртуальными машинами без промежуточных слоёв

СВ «Звезда»
Гипервизор QEMU/KVM на базе собственной разработки

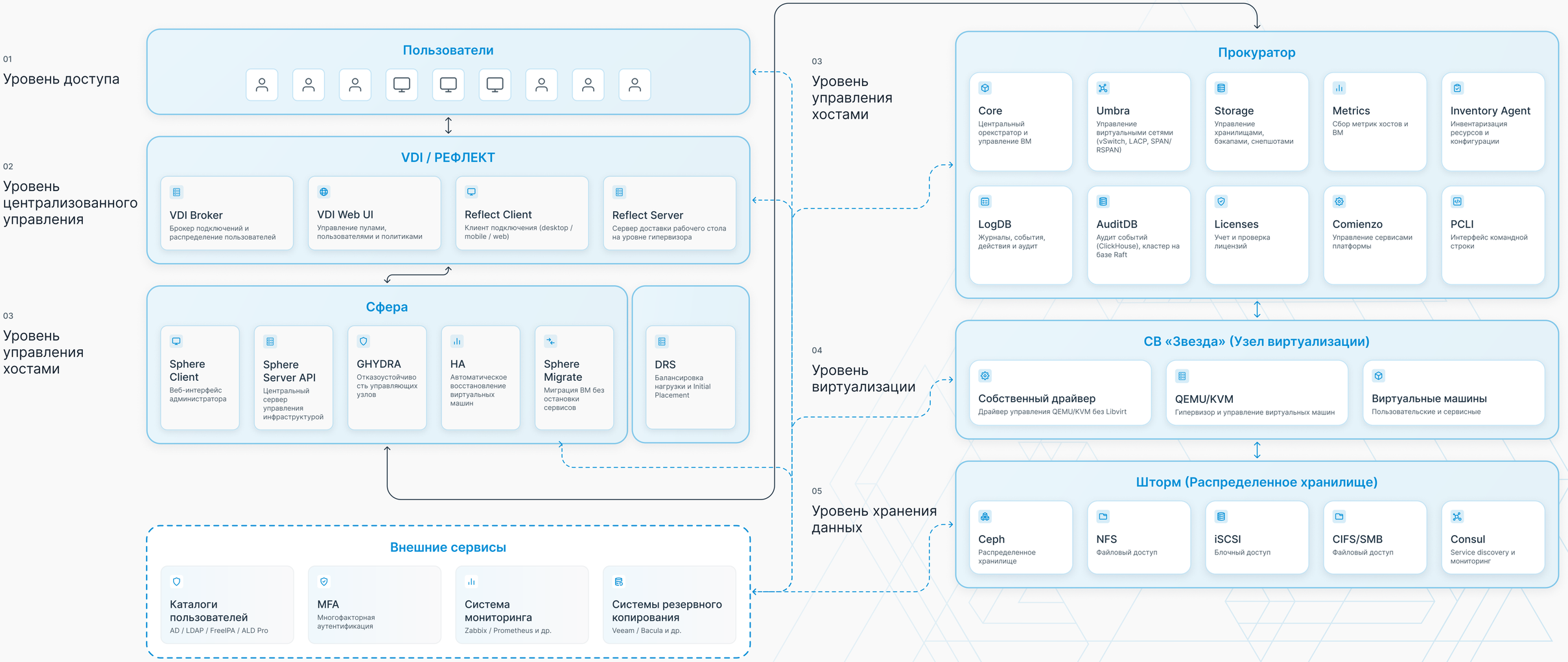
→ Исполнение виртуальных машин и предоставление вычислительных ресурсов

Виртуальные машины
Гостевые ОС и приложения

→ Исполнение пользовательских приложений, сервисов и информационных систем

Компонентная многоуровневая архитектура ПК «Звезда»

Логические уровни взаимодействия инфраструктуры



СВ «Звезда»



СВ-Звезда

Современный гипервизор 1 типа

Назначение

Единая гипервизор-платформа, обеспечивающая базовые механизмы для управления и функционирования:

- ВМ
- Ресурсов хоста
- Информационной безопасности

Функционал

- **Создание и управление ВМ и контейнерами:** полный цикл работы с виртуальными средами
- **Эффективное распределение** CPU, памяти, хранилищ и сетевых устройств между ВМ
- **Базовый слой** для работы сервисов управления, автоматизация и предоставления виртуальных рабочих мест
- **Ролевой доступ:** гибкое управление правами пользователей (администраторы, разработчики, security-специалисты)
- **Журналирование и аудит:** детальная регистрация всех событий безопасности
- **Интерфейс:** текстовый (TUI) и консольный, с поддержкой графического установщика
- Решает задачи **изоляции, контроля доступа, обеспечения целостности и соответствия требованиям ФСТЭК**



СВ-Звезда

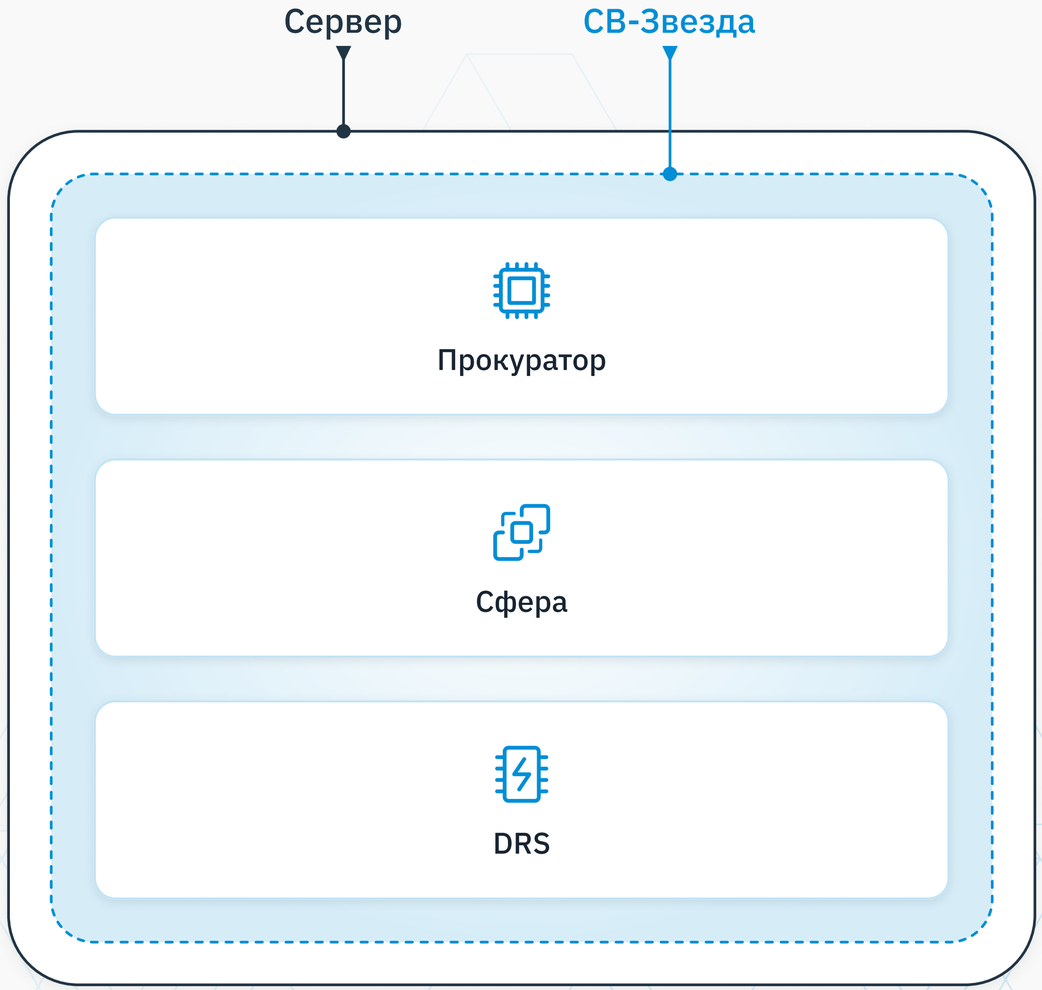
Современный гипервизор 1 типа

Технические особенности

- **Интеграции:** Kubernetes, OVS, iSCSI, NFS, CIFS/SMB, Fibre Channel
- **Протоколы:** VLAN, VXLAN, SPICE, HTML, GRE, Geneve
- **Безопасность:** IMA-подпись контейнеров и исполняемых файлов и библиотек, auditd, изоляция через namespaces/cgroups
- **Масштабируемость:** до 4096 процессоров, 256 ТБ ОЗУ, 32 ТБ на ВМ

Преимущества

- **Безопасность:** соответствует приказам ФСТЭК №187 и №118
- **Надёжность:** контроль целостности, изоляция ВМ, защита памяти
- **Гибкость:** поддержка множества ОС, сетевых протоколов, современных серверных платформ и широкого набора оборудования
- **Удобство:** резервное копирование, снимки состояния, миграция ВМ



Прокуратор



Прокуратор

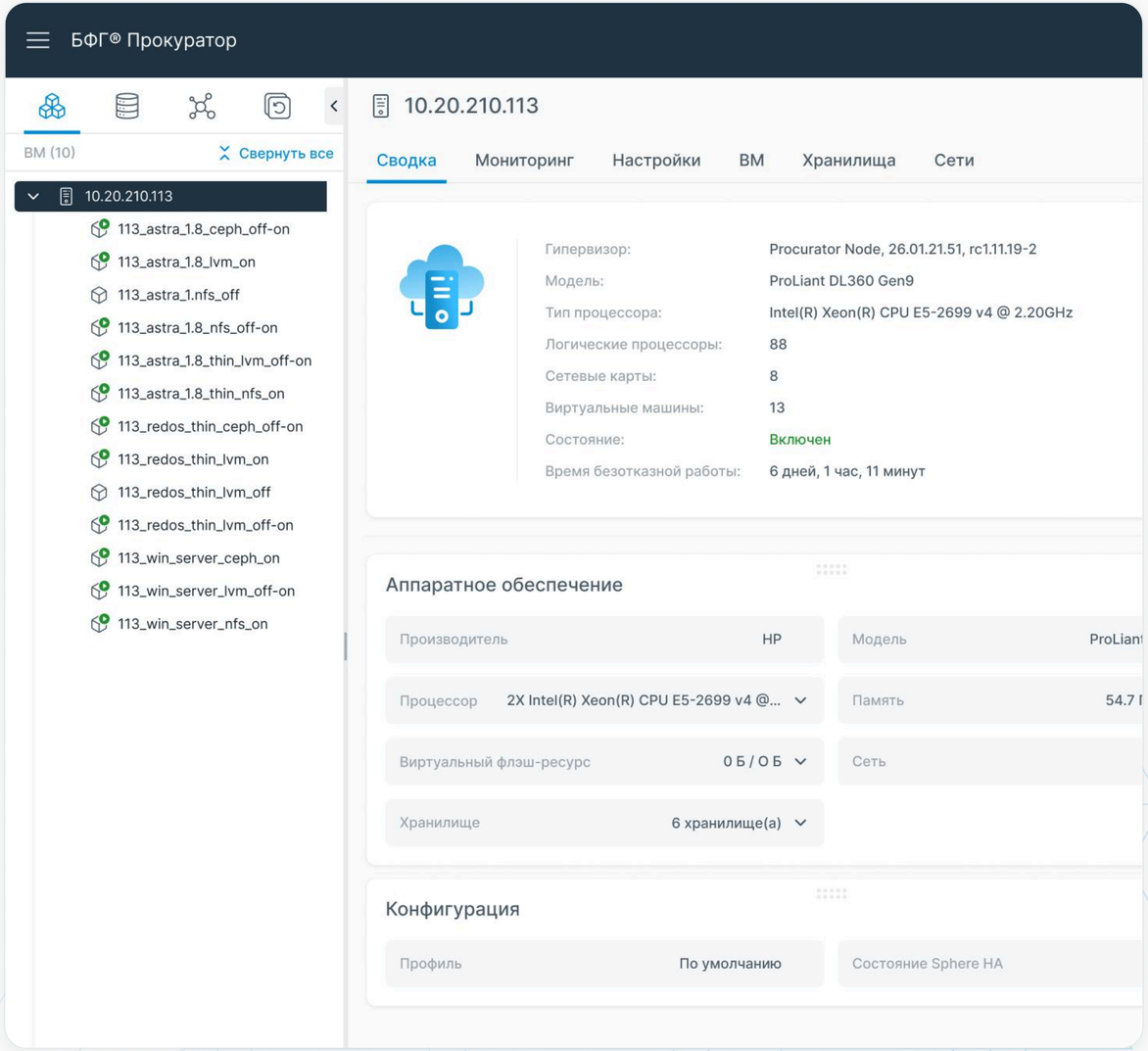
Система управления виртуализацией единичного хоста

Назначение

Единая платформа для управления гипервизором. Позволяет запускать несколько сотен изолированных ВМ на одном физическом сервере, распределяя ресурсы (CPU, RAM, диски, сеть) с использованием встроенной системы резервного копирования

Функционал

- **Управление ВМ:** создание, настройка, клонирование, миграция, управление питанием
- **Работа с хранилищами:** поддержка локальных, NFS, SMB, iSCSI, FC-хранилищ, тонкое provisioning
- **Сетевые настройки:** виртуальные коммутаторы, VLAN, агрегация интерфейсов, настройка безопасности, зеркалирование (SPAN)
- **Резервное копирование и восстановление:** полные копии
- **Мониторинг и отчетность:** встроенные инструменты мониторинга производительности, интеграция с Zabbix и GLPI
- **Интерфейс:** веб-интерфейс на русском языке с возможностью переключения на английский, включая навигационное меню, панель управления задачами, мониторинг в реальном времени и доступ к документации



Прокуратор

Система управления виртуализацией единичного хоста

Преимущества

- Полный контроль над жизненным циклом ВМ
- Собственные сервисы управления виртуализацией, сетями, мониторингом и аудитом без зависимости от внешних систем управления
- Конфигурация сетей, хранилищ и ВМ сохраняется и восстанавливается сервисами платформы

Технические особенности

- **Интеграции:** поддержка протоколов SNMP, SSH, CLI, CIM, API, интеграция с Zabbix, GLPI
- **Стандарты:** поддержка NFS, iSCSI, Fibre Channel, VLAN, LACP, SPICE, Reflect
- **Безопасность:** встроенные СЗИ, аудит событий
- **Производительность:** поддержка до 255 vCPU на ВМ, горячее добавление ресурсов, балансировка нагрузки

Создание ВМ
Создание новой виртуальной машины или из шаблона

↓

Настройка ресурсов
Выделение CPU, RAM, дисков, сетей и других ресурсов

↓

Запуск
Запуск виртуальной машины на хосте

↓

Мониторинг
Непрерывный сбор метрик и контроль состояния

↓

Snapshot / Clone
Создание снимков состояния или клонирование ВМ

↓

Backup
Резервное копирование данных ВМ

↓

Live Migration
Миграция ВМ между хостами без остановки работы

↓

Удаление
Безопасное удаление ВМ и освобождение ресурсов

Архитектура Прокуратора

Набор специализированных сервисов для управления вычислительными ресурсами, сетями, хранилищами и ВМ

Назначение сервисов

Comienzo
Контроль состояния сервисов платформы и управление их жизненным циклов

CORE
Управление:
- ВМ
- Дисками (от Storage)
- Сетями (от Umbra)
- Метриками (от Metrics)

Umbra
Управление виртуальными сетями, порт-группами и сетевыми политикам

Storage
Управление хранилищами, виртуальными дисками и снапшотами ВМ

Metrics
Сбор и предоставление метрик хостов и ВМ

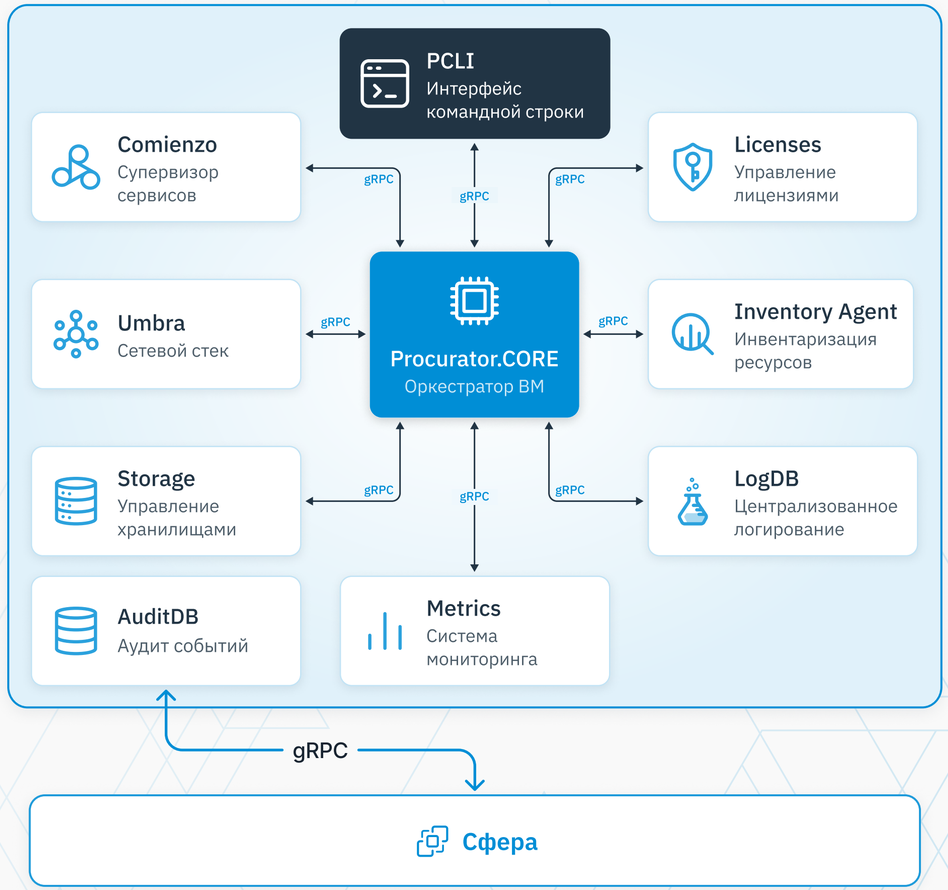
LogDB
Хранение журналов событий, действий пользователей и системных операций

Licenses
Учет, контроль и проверка лицензий

Inventory Agent
Инвентаризация ресурсов, конфигураций и объектов виртуальной инфраструктуры

PCLI
CLI-управление системой с помощью текстовых команд

AuditDB
Хранение и предоставление данных аудита безопасности для Сферы



Comienzo

Сервис управления жизненным циклом компонентов Прокуратор

Назначение

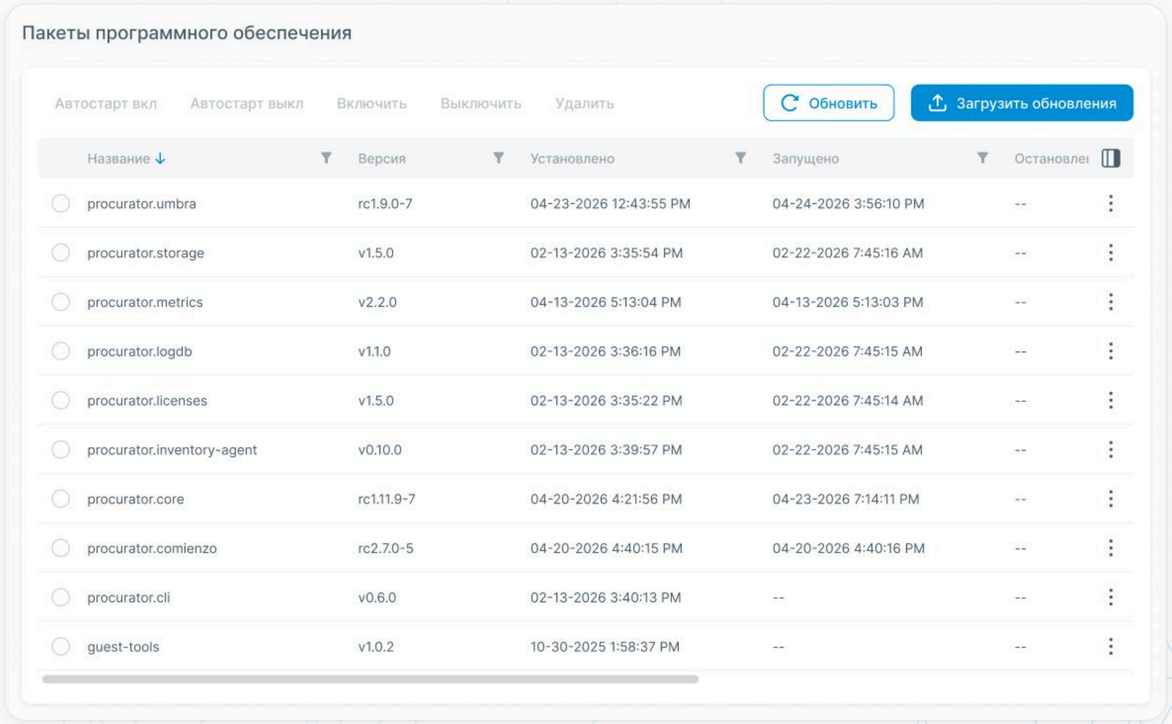
Управление запуском, состоянием, обновлением и восстановлением сервисов

Ключевые функции

- **Безопасность:** Генерация локальных сертификатов и учётных данных для сервисов
- **Надежность:** Контроль состояния сервисов и автоматический перезапуск при сбоях
- **Управление компонентами:** Установка, обновление, удаление и управление компонентами

Почему является базовым сервисом

- **Инициализирует и запускает все сервисы** (как systemd в Linux)
- **Контролирует их работоспособность и обеспечивает восстановление после сбое**



Umbra

Единый контроль сетей: коммутаторы, портовые группы, SysX

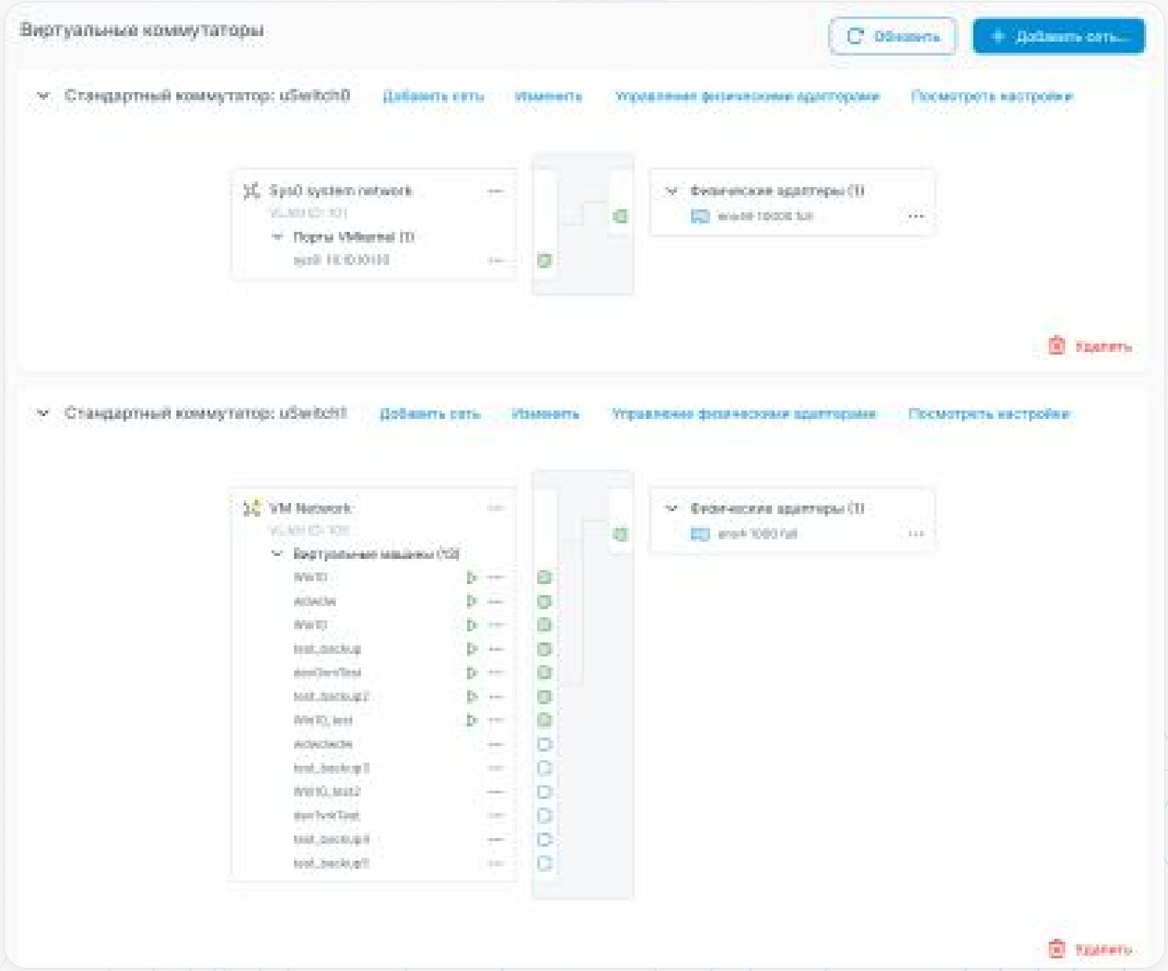
Назначение

Централизованное управление виртуальной сетевой инфраструктурой

- Создание и управление виртуальными коммутаторами (vSwitch)
- Настройка портовых групп (Port Groups) и VLAN 802.1Q
- Подключение физических сетевых адаптеров и управление их конфигурацией

Сетевые возможности

- Агрегация каналов (LACP) для повышения пропускной способности и отказоустойчивости
- DHCP-сервер для автоматической выдачи сетевых параметров
- Зеркалирование трафика (SPAN) для анализа и диагностики
- Балансировка и управление трафиком (Load Balancing, Traffic Shaping)
- Сетевой мониторинг и диагностика состояния виртуальной сети



Storage

Управление конфигурацией хранилищ

Назначение

Управление подключением, конфигурацией и использованием систем хранения данных

Основные типы хранилищ

Тип хранилища	Протокол/ Технология	Использование
Локальное	sStorm, dStorm	Для standalone-хостов
Блочное (SAN)	iSCSI, Fibre Channel	Enterprise-хранилища
Файловое (NAS)	NFS v3/v4.1	Общие хранилища для ВМ

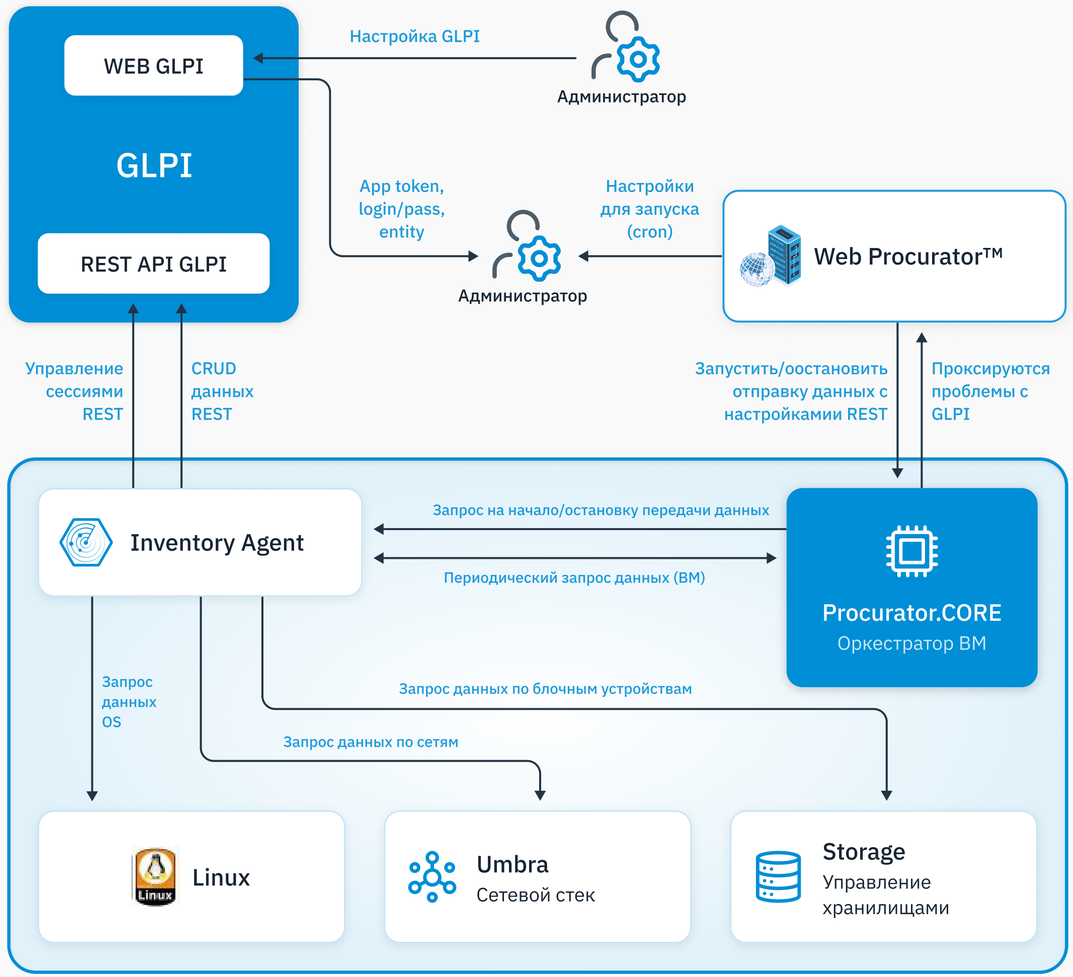
Инструменты управления (встроенный веб-интерфейс)

- **Создание/расширение датасторов**
- **Настройка multipathing**
  Подключение новых систем хранения
  Мониторинг состояния подключённых хранилищ

Ключевые компоненты

- VMkernel Storage Stack (базовый драйвер):
  - Поддержка многопутевого доступа (MPIO)
  - Аппаратное ускорение (VAAI: XCOPY)
- Системные службы:
  - Hostd (управление датасторами)
  - vpxa (интеграция с Sphere)

Inventory Agent



Как работает

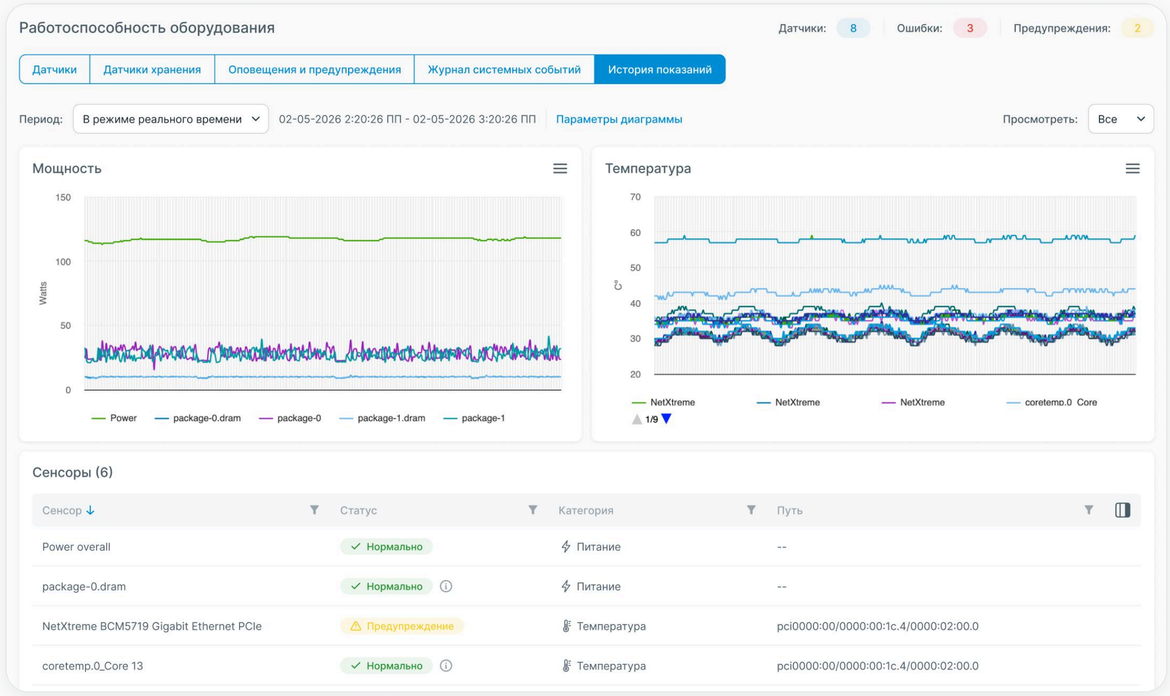
1. Связь с GLPI
2. Конвертация данных из формата Procurator в формат GLPI
3. Управление данными о хосте с Procurator (crud) в GLPI
4. Запрос к Core с требованием отправлять профильные данные
5. Сбор данных с заданной периодичностью с Core, Storage, Umbra и OS
6. Следит, чтобы информация о хосте была актуальной

Metrtics

Система мониторинга

Назначение

Система мониторинга, обеспечивающая сбор, хранение и предоставление эксплуатационных метрик виртуальной инфраструктуры



Цели

- Автоматический сбор, хранение и визуализация метрик производительности.
- Отправка выбранных метрик во внешнюю систему мониторинга Zabbix.
- Предоставление интерфейсов (gRPC и REST) для запросов исторических данных и интеграции с другими сервисами платформ Procurator и Sphere.

Ключевые функции

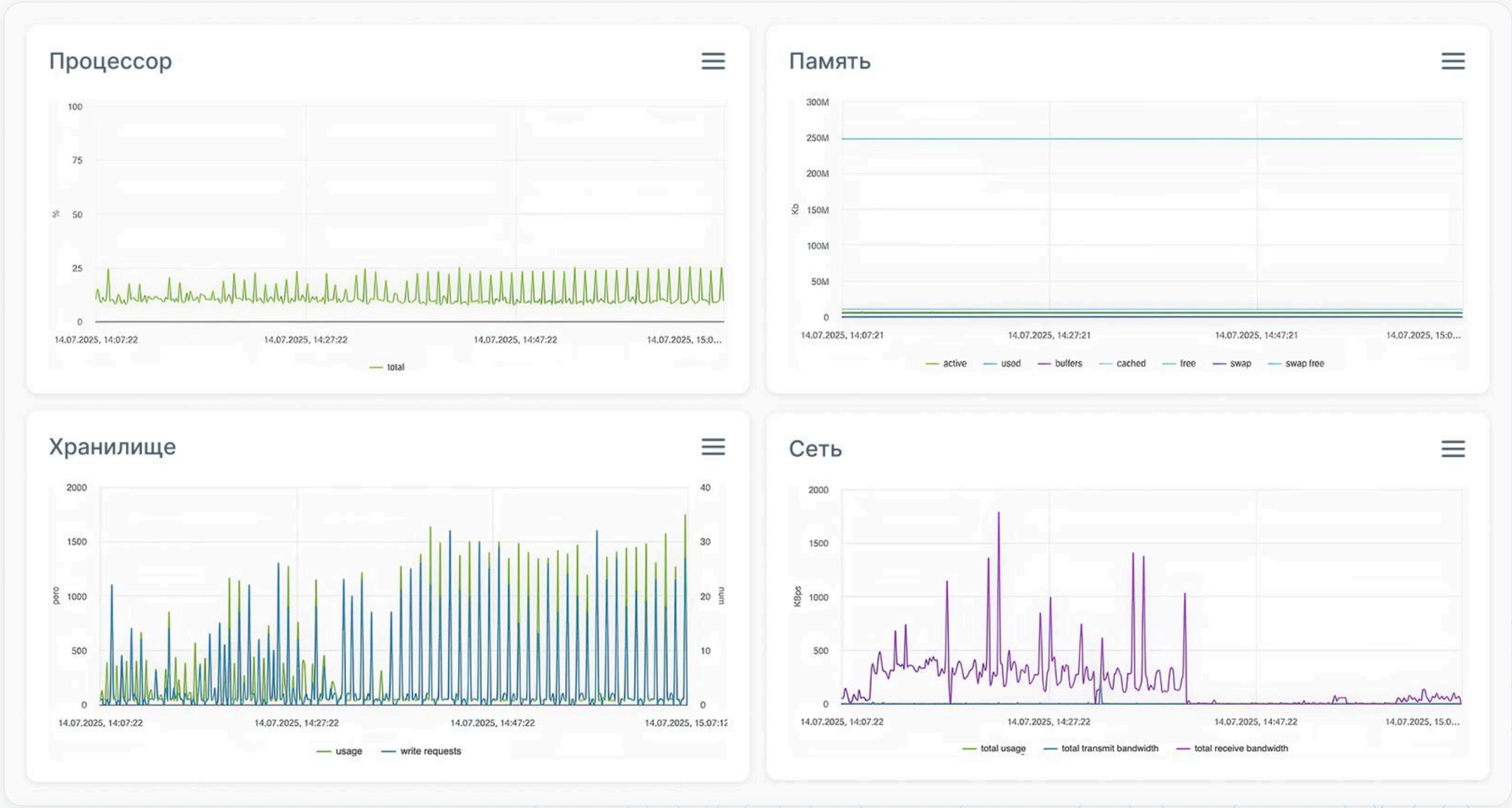
- Непрерывный сбор метрик хоста (CPU, RAM, сеть, диски, LVM, NFS, датчики).
- Непрерывный сбор метрик ВМ (CPU, RAM, сеть, диски, Spice сессии).
- Отложенная инициализация подсистемы виртуальных машин (ожидание получения актуального списка ВМ).
- Локальное хранение временных рядов на базе Prometheus TSDB (встроенная).
- Избирательная отправка метрик в Zabbix.
- Сбор алертов по сенсорам дисков, мониторинг энергопотребления и температуры.

Metrtics

Система мониторинга

Полный перечень собираемых метрик

- CPU
- RAM
- Сеть
- Диски
- LVM
- NFS
- Датчики
- ВМ CPU
- ВМ RAM
- ВМ Сеть
- ВМ Диски
- Spice-сессии



Metrtics

Система мониторинга

Управление и конфигурирование

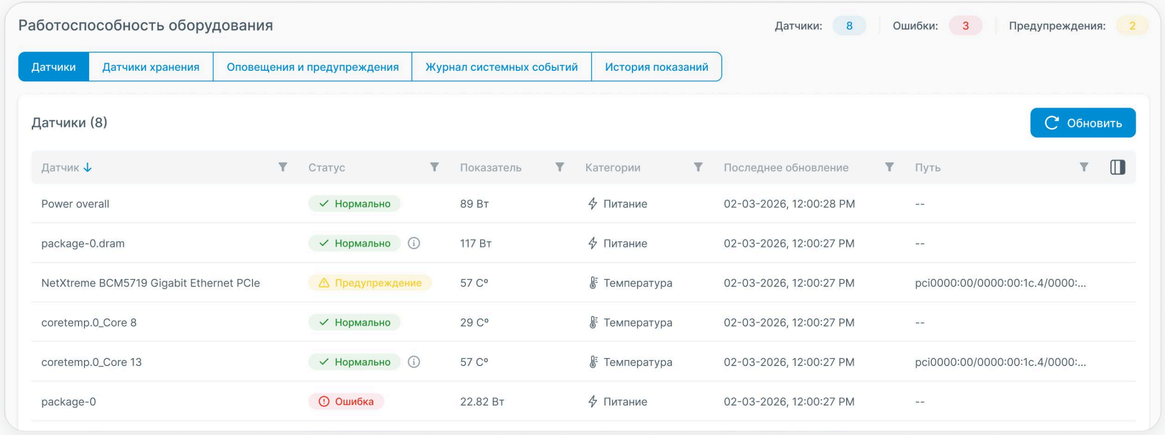
Система поддерживает гибкую настройку интервалов сбора данных, сроков хранения и отправляемых метрик. Конфигурация осуществляется через файлы конфигурации и переменные окружения

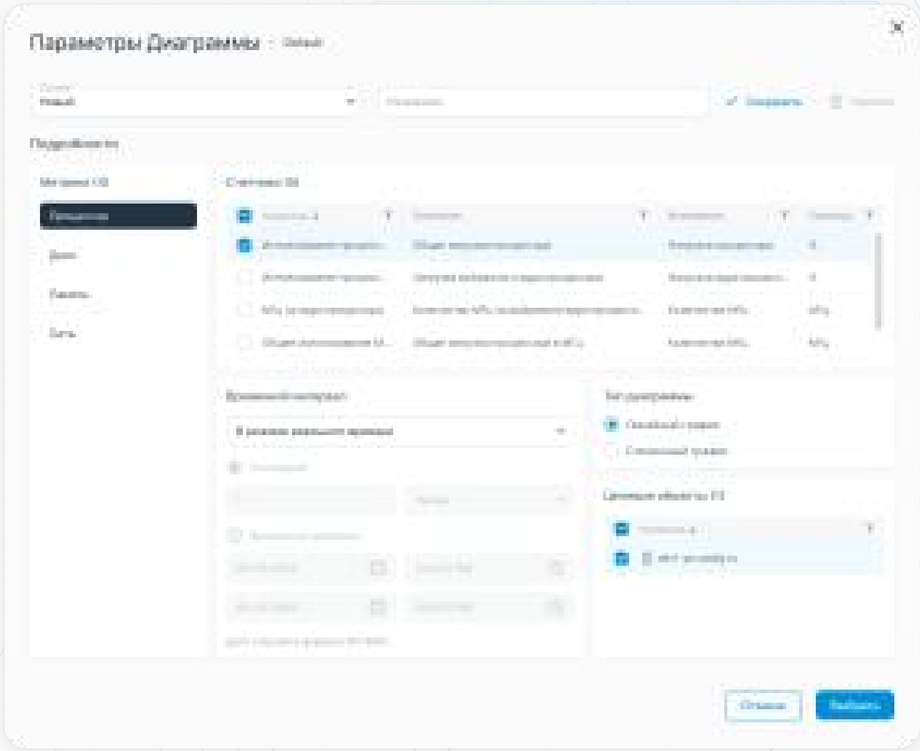
Procurator.metrics

Обеспечивает надежный и подробный мониторинг аппаратных и виртуальных ресурсов хоста с возможностью глубокой интеграции в существующие системы мониторинга и инфраструктурные сервисы

Алерты и мониторинг

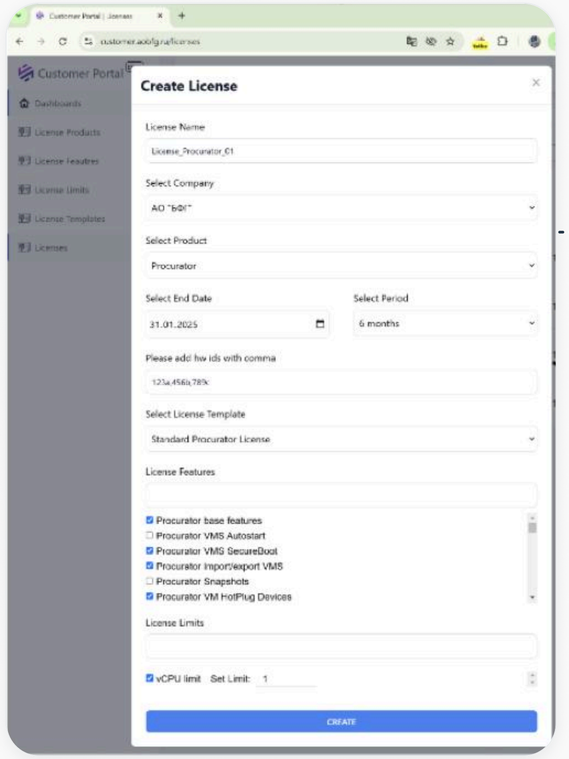
Система способна собирать и обрабатывать алерты с датчиков дисков, мониторить температуру оборудования и энергопотребление, и передавать эту информацию во внешние системы.





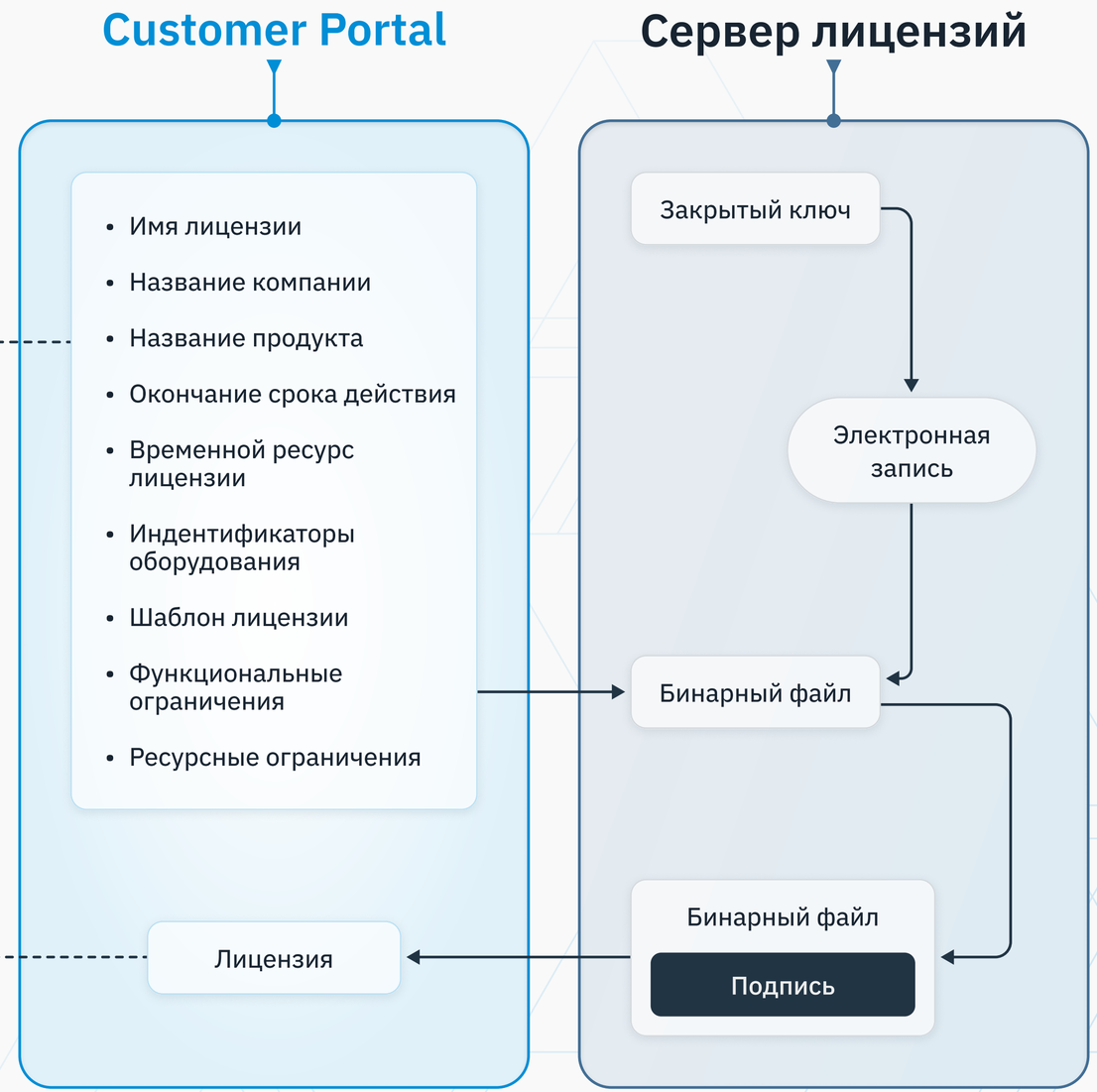
Licenses

Хранит список доступных лицензий, полученных следующим образом



License

eNpcxy9LBGEcxPHvoGg4yxUFu1Xu9_zdK5s0mSyCbNS6sGBQECxaDKLJJCIIW0T1gjaDbOLYpskiFkGe6H0YmBn-08141WMM2QRZaYcslIvIErKMrEI2RQ45Qy4gF5FH3pAvMyGfUUARRUPRoZhQyQQlh1JAqfyMMqrQFDFrb-njpF5ZWLx8_myPx8PZ-cVps9-3T_1dXJ7_Gb6722rz6uFr7u10571-1Pbrwcv61v312mj_J1cbUZ_AGAA_-MJSOO



Logdb

Журнал безопасности – Всё, что делает пользователь в Core, попадает в LogDB

Назначение

Централизованное логирование действий пользователей из Core для аудита и анализа

UI

Фильтрация, группировка, детализация событий

Что хранит

Уникальный ID, дата/время, тип события, логин, уровень лога (инфо/ошибка и т.д.), описание, устройство (IP, браузер), причины ошибок

Гарантия отслеживания

Core не работает без записи в LogDB

Особенности

- **Иерархия событий:** каскадные логи (связанные действия группируются)
- **Гибкий поиск:** простой + комбинированный по всем полям
- **Хранение:**
  - **По умолчанию** – бессрочно
  - **С настройкой интервала** – старые логи сжимаются в *.qz



Pcli

Инструмент автоматизации – Мощный инструмент для DevOps и админов, позволяющий заменить рутинные задачи

Назначение

Автоматизация управления Procurator, BM через PowerShell, Bash.

Что умеет

- Управление виртуальными машинами (создание, запуск, снапшоты)
- Настройка хостов, сетей, хранилищ
- Использование для массовых операций при помощи скриптов

Как работает

- **Установка модуля**
- **Подключение к Procurator: host<IP> – password - user**
- **Выполнение команд: pcli.command, network.nic, system.license**

Преимущества

- Кроссплатформенность (Windows, Linux, macOS)
- Интеграция с CI/CD



Сфера



Сфера

Единая точка централизованного управления виртуальной инфраструктурой

Функционал

Управление инфраструктурой:

Централизованное создание и управление дата-центрами, кластерами, хостами, сетями и хранилищами (NFS, iSCSI, Fibre Channel, Storm) через веб-интерфейс

Виртуализация рабочих нагрузок:

Полный жизненный цикл ВМ: создание, клонирование, снапшоты, бэкапы, «горячее» добавление ресурсов (vCPU, память, диски) и миграция между хостами без простоя

Ресурсная оптимизация:

DRS - балансировка нагрузки и оптимизация распределения ресурсов виртуальной инфраструктуры

Отказоустойчивость:

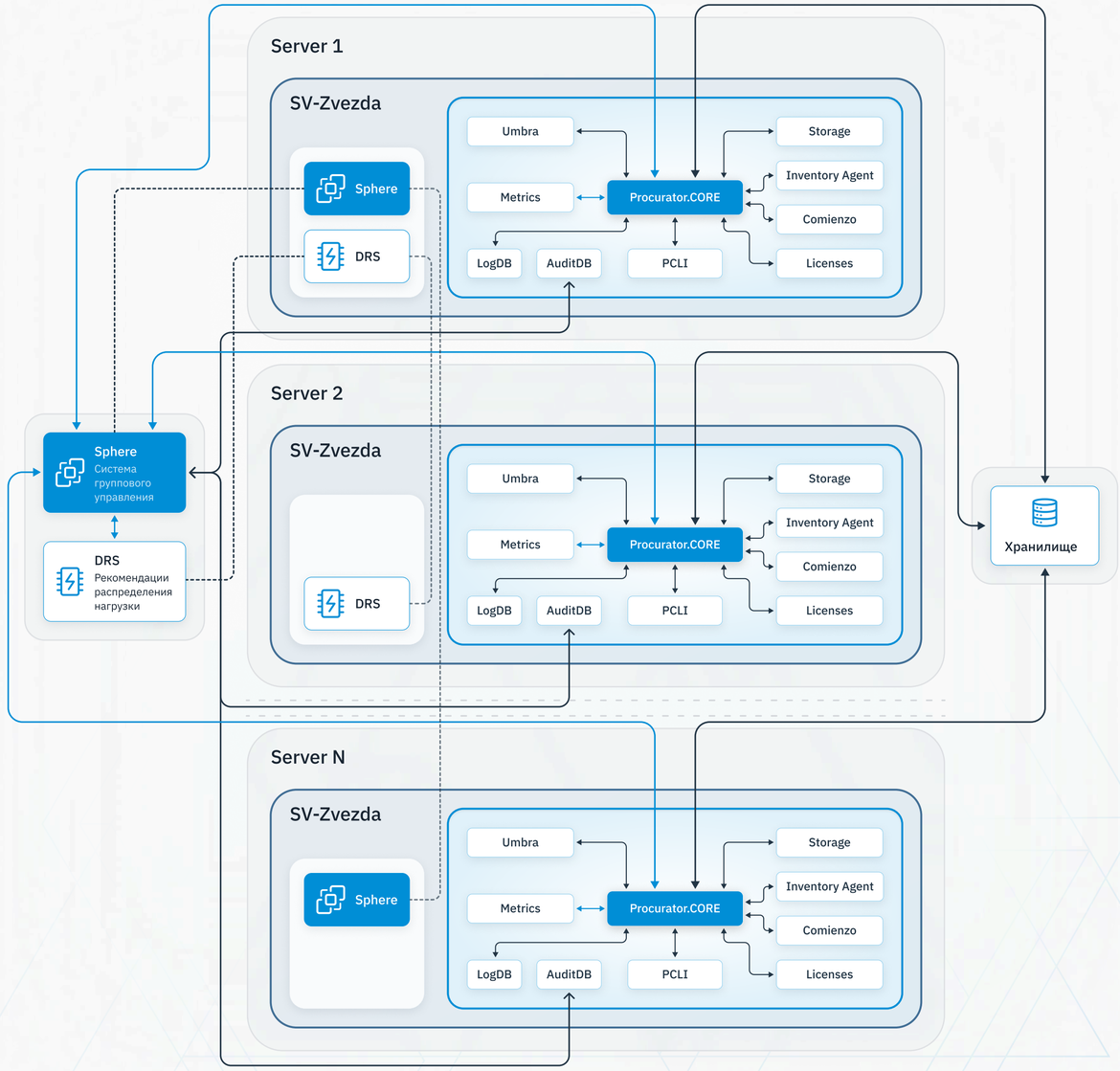
Живая миграция и автовосстановление ВМ

Безопасность и контроль доступа:

Детальное ролевое управление доступом (RBAC), двухфакторная аутентификация, аудит событий, изоляция хостов и поддержка отечественных ОС (Astra Linux, ALT, РЕД ОС)

Мониторинг и аналитика:

Дашборды в реальном времени для отслеживания нагрузки на CPU, память, диски и сеть как на уровне кластеров и хостов, так и отдельных ВМ



Сфера

Единая точка централизованного управления виртуальной инфраструктурой

Преимущества

Централизованное управление

Единая точка управления дата-центрами, кластерами, хостами, сетями и хранилищами через удобный веб-интерфейс. Снижение операционных затрат и упрощение администрирования

Масштабируемость

Платформа рассчитана на крупные инфраструктуры и обеспечивает высокую плотность размещения виртуальных машин

Высокая доступность

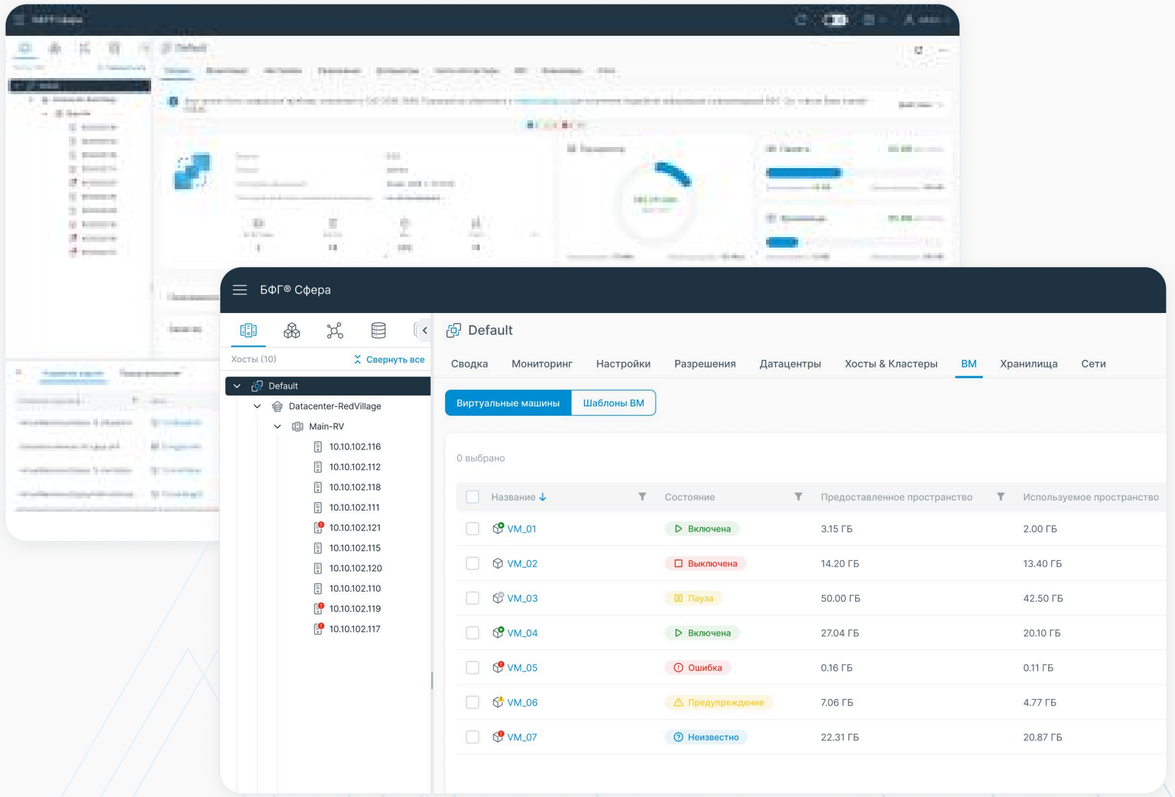
Технология HA-кластеров автоматически восстанавливает виртуальные машины на исправных узлах при сбоях, минимизируя простой критичных сервисов

Интеллектуальная оптимизация ресурсов

DRS анализирует состояние кластеров и вырабатывает рекомендации по оптимальному размещению виртуальных машин для сбалансированного использования ресурсов

Знакомый интерфейс

Интуитивно понятный интерфейс, логика работы и терминология близки VMware vCenter, что ускоряет адаптацию администраторов и не требует переобучения персонала



256
узлов в кластере

>10 000
виртуальных машин

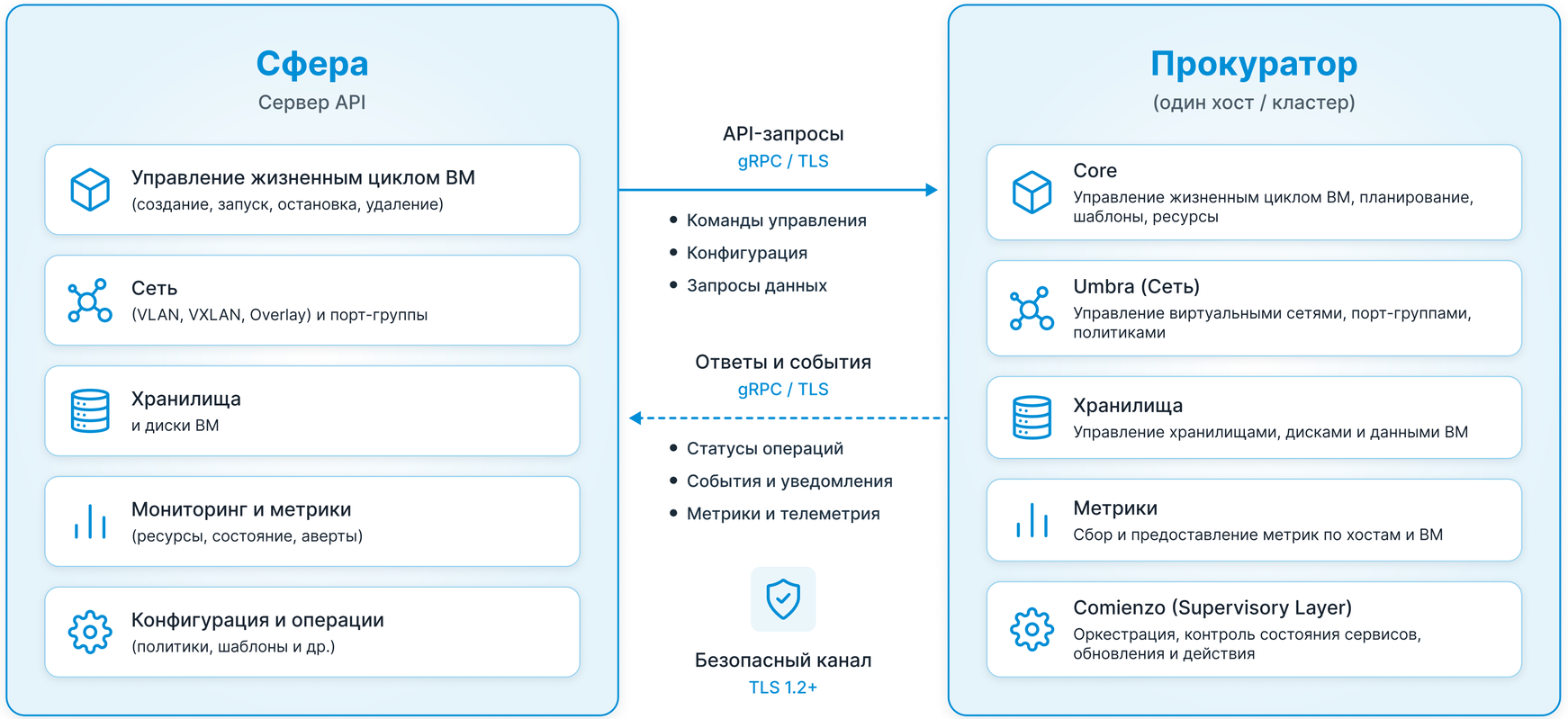
255
vCPU на ВМ

36 ТБ
оперативной памяти на ВМ

Архитектура взаимодействия Сферы и Прокуратора

Сфера использует сервисную API-архитектуру для централизованного управления компонентами виртуализации, сети, хранения и мониторинга

Сфера Server API централизованно управляет одним или группой Прокураторов



Ключевой принцип

Сфера Server API — единая точка входа. Все командыи данные проходят только через API

Взаимодействие Сферы и Прокуратора



Многоуровневая отказоустойчивая архитектура ПК «Звезда»

Отказоустойчивость на всех уровнях: управление, вычисления, балансировка и хранение данных



GHYDRA

Защита системы управления от отказа узлов управления

HA

Защита виртуальных машин при отказе хоста

DRS

Балансировка нагрузки и миграция ВМ при перегрузке

Шторм

Защита данных при отказе дисков или узлов хранения

Отказ Sphere

Ghydra выбирает новый управляющий узел

Отказ хоста

HA автоматически восстановливает ВМ на другом узле

Перегрузка хоста

DRS выполняет миграцию ВМ для балансировки нагрузки

Отказ диска или узла хранения

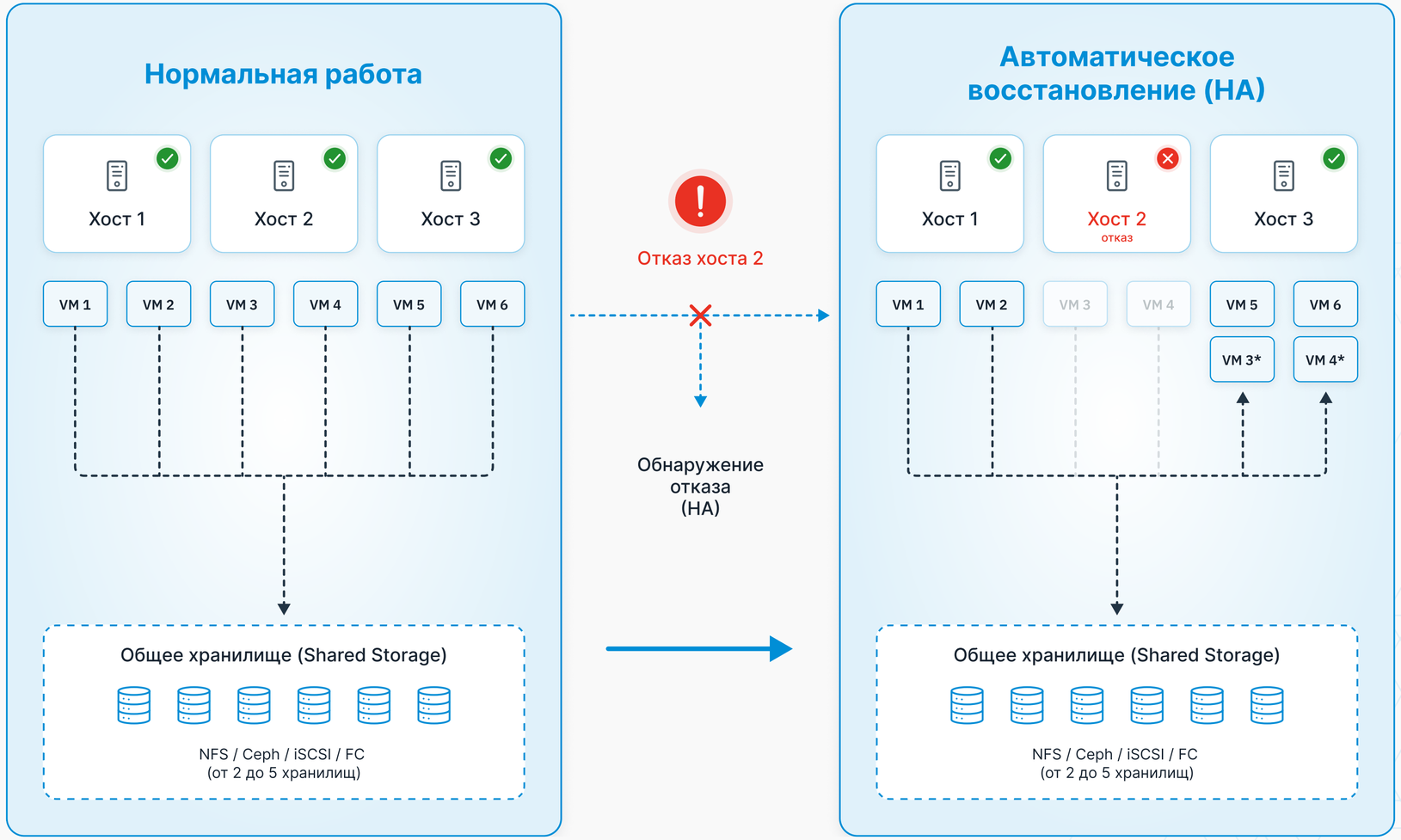
Шторм вобеспечивает сохранность данных и доступность сервисов

Отказоустойчивость



Сервис отказоустойчивости ВМ (HA)

Автоматическое восстановление ВМ обеспечивает непрерывность работы сервисов при отказах хостов и сбоях инфраструктуры



Как работает

1. **Мониторинг**
   Сервис непрерывно контролирует состояние хостов и сети
2. **Обнаружение отказа**
   При недоступности хоста HA фиксирует сбойи инициирует процедуру восстановления
3. **Выбор узла назначения**
   Выбирается оптимальный доступный узел с учётом ресурсов CPU и RAM
4. **Восстановление ВМ**
   ВМ автоматически перезапускается на другом узле с использованием общего хранилища
5. **Продолжение работы**
   downtime минимален

Сервис отказоустойчивости ВМ (HA)

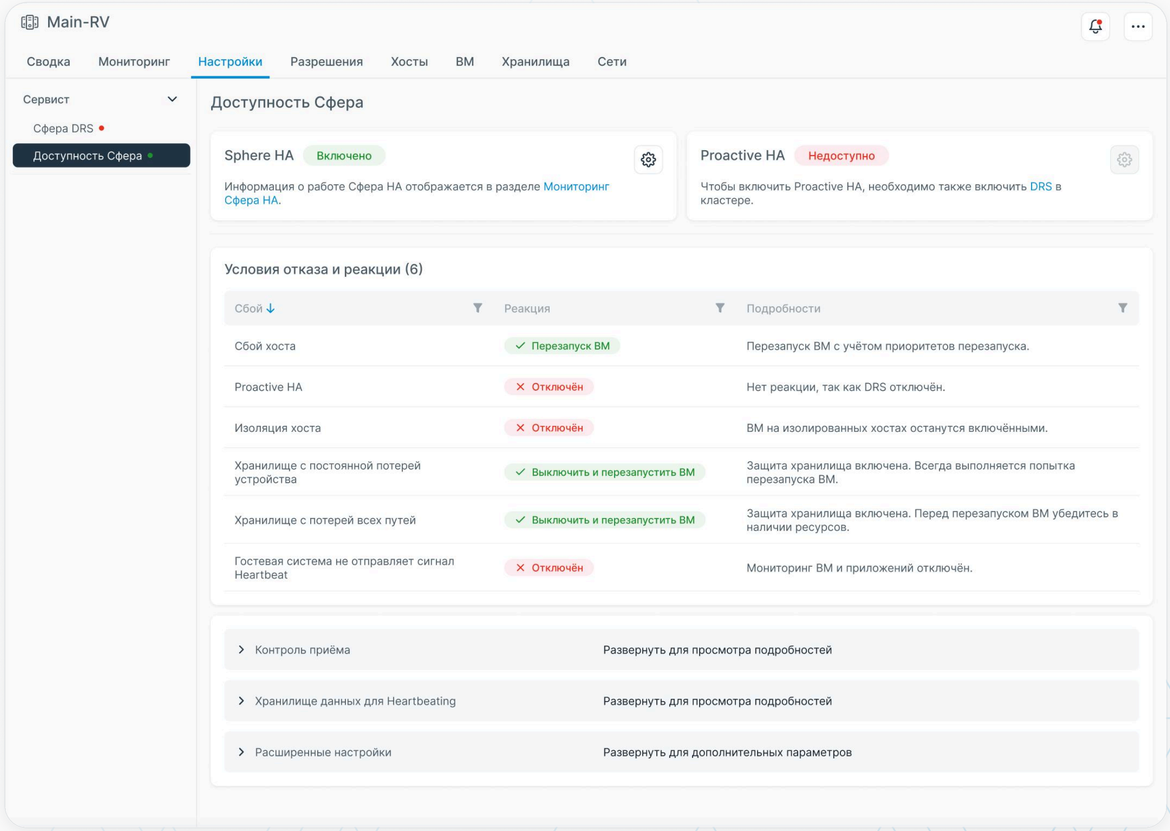
Автоматическое восстановление ВМ обеспечивает непрерывность работы сервисов при отказах хостов и сбоях инфраструктуры

Технические особенности

- Работа в кластерах на базе GHYDRA
- Использование общего хранилища (shared storage)
- Автоматическое определение отказов (heartbeat, health-checks)
- Быстрый перезапуск ВМ (restart)
- Сохранение сетевых настроек и конфигурации ВМ
- HA гарантирует отсутствие Split-brain
- Если Сфера собрана в Гидру, при смене Сферы-лидера процесс восстановления ВМ HA происходит дольше

Результат работы - высокая доступность ВМ

- Автоматическое восстановление ВМ на работоспособных узлах кластера при отказе хоста
- Минимизация влияния аппаратных и программных сбоев на работу ВМ
- Снижение рисков простоя сервисов и потери доступности приложений



GHYDRA

Обеспечение отказоустойчивой архитектуры Sphere

Роль GHYDRA

GHYDRA защищает управляющий контур Sphere от сбоев и обеспечивает отказоустойчивую работу управляющих компонентов

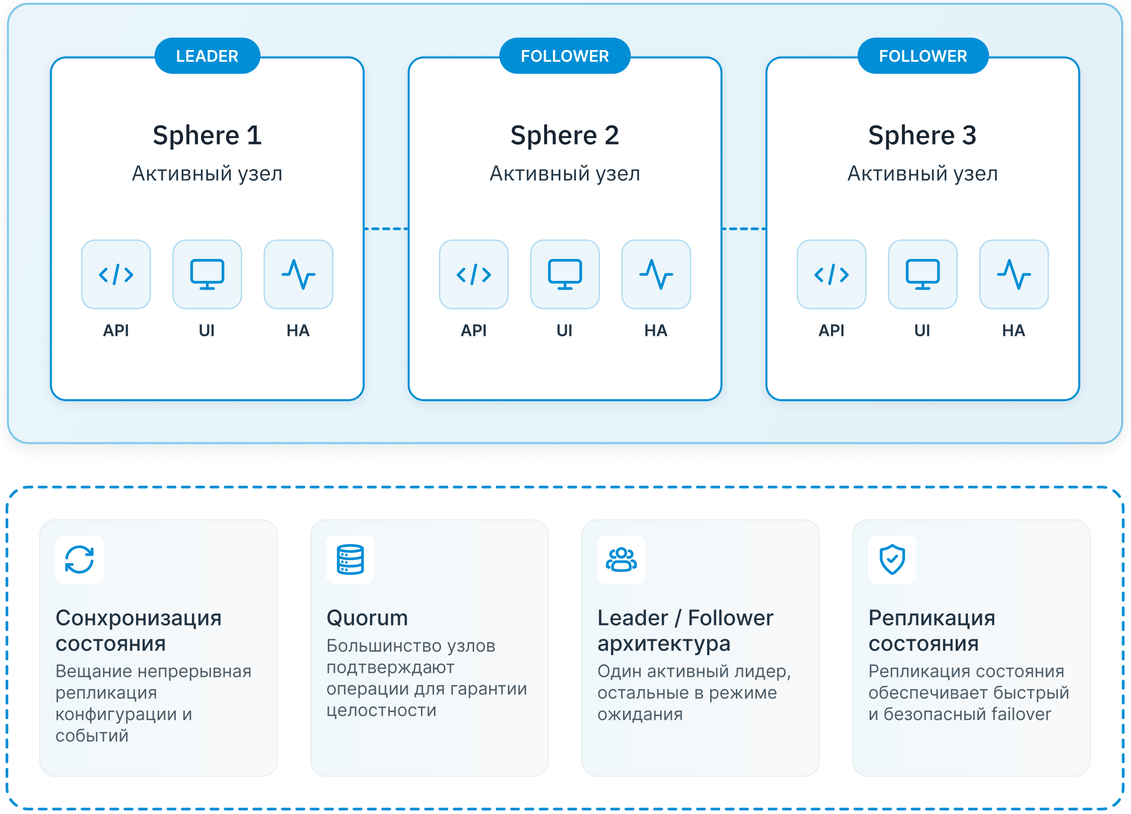
Что остается доступным

- API и SDK Sphere
- Web UI и административный доступ
- Управление кластерами и хостами
- Политики доступа и аутентификацию
- DRS и распределение ресурсов
- HA и управление отказами хостов
- Live Migration и задачи миграции
- Оркестрацию и интеграции с внешними системами

Что НЕ делает GHYDRA

- Не перезапускает виртуальные машины (это роль HA)
- Не балансирует ресурсы (это роль DRS)
- Не выполняет миграцию (это роль Sphere.Migrate)
- Не хранит данные пользователей
- Не выполняет задачи внутри ВМ

GHYDRA Cluster - управляющие узлы Sphere

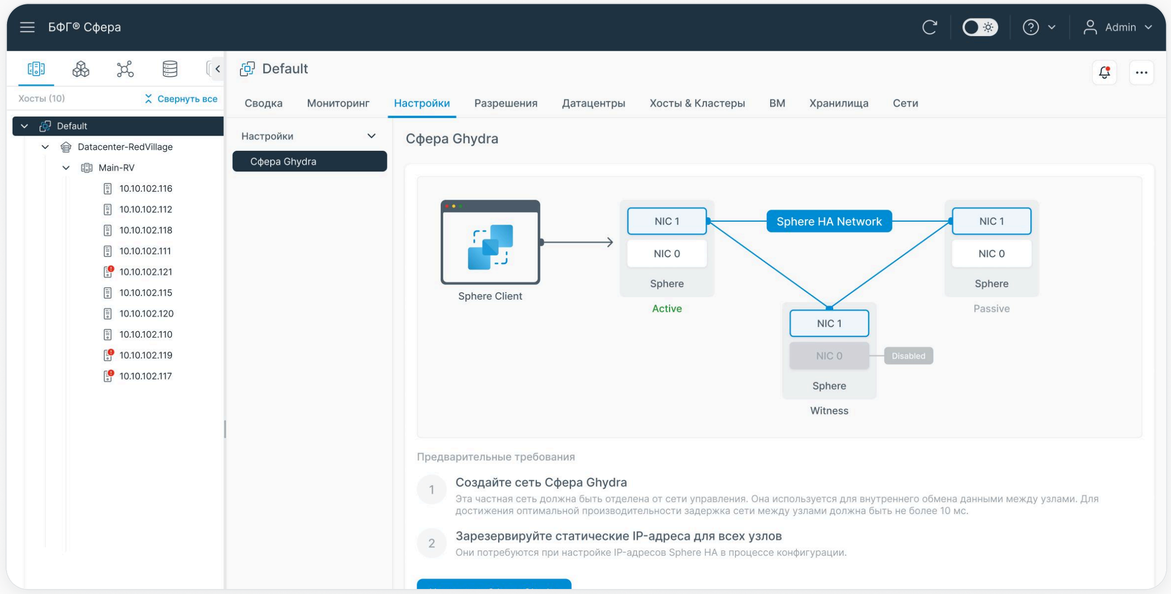


GHYDRA - автоматический failover

При отказе активного узла управление автоматически передаётся другому узлу кластера без потери доступности сервисов

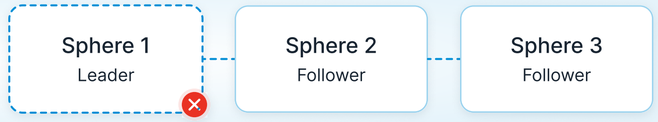
Результат работы GHYDRA

- Непрерывное управление
- Минимальное время переключения
- Автоматический failover без ручного вмешательства
- Сервисы и инфраструктура остаются доступными



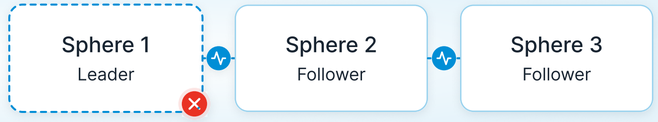
1. Отказ Leader

Активный узел (Leader) становится недоступным из-за сбоя.



2. Обнаружение отказа

Оставшиеся узлы обнаруживают потерю доступности через heartbeat и таймауты



3. Election (выбор нового Leader)

Узлы проводят выборы нового лидера на основе quorum-механизма



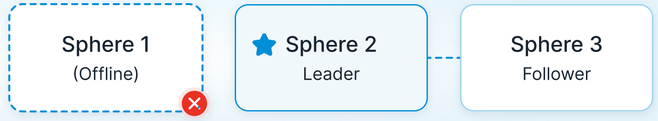
4. Назначение нового Leader

Выбранный узел становится новым Leader и принимает управление кластером.



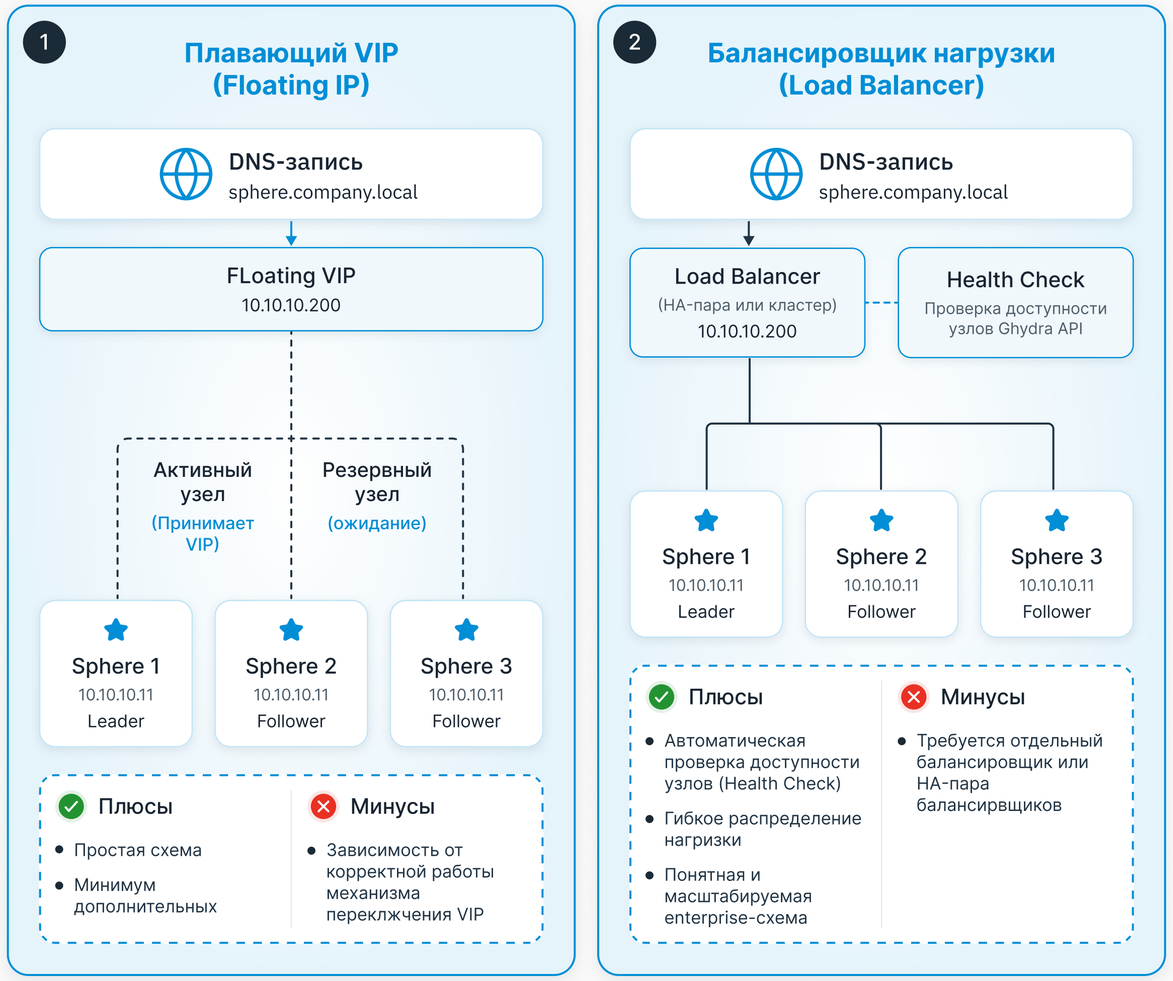
5. Продолжение работы

Сервисы продолжают работы без перерывов. Управление и доступность сохранены.



DNS-доступ к кластеру GHYDRA

DNS должен указывать не на конкретный узел Sphere, а на отказоустойчивую точку входа, чтобы управление оставалось доступным при отказе узла



Рекомендация

DNS-запись (например, sphere.company.local) должна указывать на единую точку входа: Floating VIP или балансировщик нагрузки.

Привязка DNS к конкретному узлу Sphere не рекомендуется, так как при отказе этого узла управление станет недоступным.

Куда указывать DNS

- Администраторы (Web UI, API)
- Интеграции и внешние системы
- Автоматизация и скрипты

DRS



Цикл работы и логика принятия решений

DRS регулярно анализирует состояние кластера и принимает решения о миграции ВМ

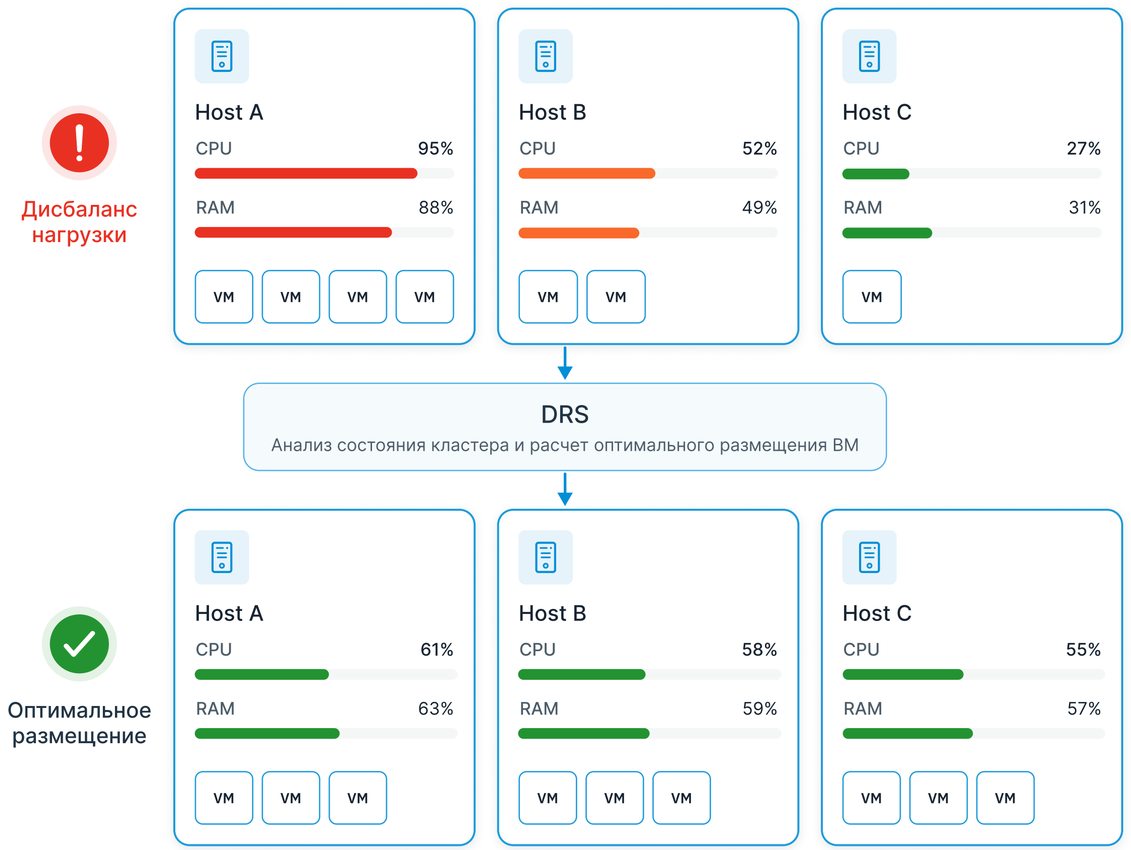
Основные функции

1. **Анализ состояния кластера по расписанию**
   Периодический сбор данных о хостах, ВМ и нагрузке
2. **Выявление дисбаланса ресурсов**
   Определение узлов с перегрузкой и неэффективным использованием
3. **Расчёт оптимального размещения ВМ**
   Выбор лучших целевых узлов для каждой виртуальной машины
4. **Запуск миграции**
   Формирует команды на миграцию и контролирует процесс
5. **Повышение эффективности использования ресурсов**
   Выравнивание нагрузки и увеличение плотности размещения ВМ

Принципы работы DRS

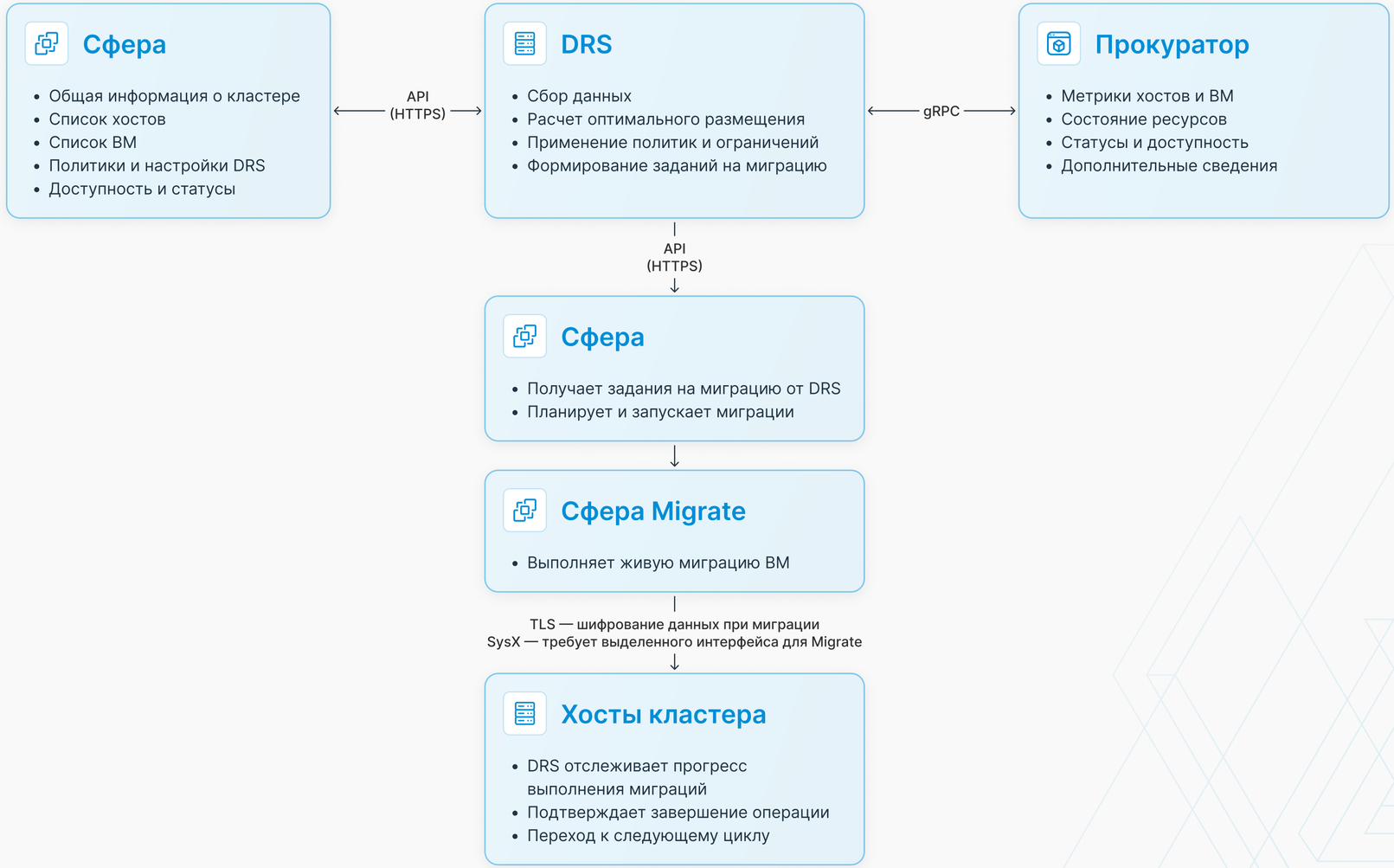
1. **Автономность**
   Работает автоматически по заданному интервалу
2. **Уровень агрессивности миграции**
   - Высокая — частые миграции при малых улучшениях
   - Средняя — миграции при заметных улучшениях
   - Низкая — допускаются большие отклонения
3. **Политики размещения**
   - Равномерное распределение - балансировка нагрузки между всеми хостами
   - Плотное размещение - максимальная загрузка минимального числа хостов

Кластер виртуализации



Цикл работы и логика принятия решений

DRS регулярно анализирует состояние кластера и принимает решения о миграции ВМ



Что проверяет DRS

1. Какие кластеры нужно обслуживать
2. Появились ли новые кластеры
3. Изменились ли политики размещения
4. Изменился ли уровень агрессивности миграции
5. Изменились ли параметры работы

Учитываемые ресурсы

1. Используются (сейчас):
   - CPU
   - RAM
2. Собираются, но не участвуют в расчете:
   - Disk I/O (метрики)
   - Network (метрики)
3. Учитываются при расчете:
   - Reservation (резерв)
   - Limit (ограничение)

Условие для миграции: Типы процессоров ВМ должны быть совместимы

Оптимизация ресурсов: математическая основа и области применения

DRS использует методы решения задач оптимального размещения ресурсов.Аналогичные подходы применяются в логистике, робототехнике, складских системах и облачных платформах.

Математическая основа

Σ

Multidimensional Bin Packing Problem

Многомерная задача упаковки в контейнеры

- Каждая ВМ — это объект с набором требований (CPU, RAM и др.)
- Каждый хост — контейнер с ограниченной ёмкостью
- Задача — разместить все ВМ в контейнерах так, чтобы минимизировать отклонение от цели (политики)

Математические термины, используемые в DRS

- Задача размещения ресурсов (Resource Placement Problem)
- Оптимизационная задача (Optimization Problem)
- Многомерная задача упаковки в контейнеры (Multidimensional Bin Packing)
- Распределение рабочей нагрузки (Workload Distribution)
- Консолидация ресурсов (Resource Consolidation)
- Ограничения (Constraints)
- Правила совместимости (Compatibility / Rules)
- Резервирование ресурсов (Resource Reservation)
- Лимиты ресурсов (Resource Limits)
- Ограничения размещения (Affinity / Anti-Affinity Rules)

Области применения

- **Логистика и транспорт**
  Оптимизация распределения грузов по транспортным средствам с учётом вместимости, ограничений и маршрутов
- **Складская логистика**
  Размещение товаров на складе с учётом объёмов, зон хранения и ограничений по вместимости.
- **Робототехника и производственные системы**
  Назначение задач роботам и оборудованию с учётом их возможностей и ограничений.
- **Облачные и IT-инфраструктуры**
  Размещение и балансировка нагрузок для эффективного использования ресурсов и повышения отказоустойчивости.
- **Другие области**
  Телеком, энергетика, планирование ресурсов, финансовые расчёты и др.

Преимущества DRS

- Эффективное использование CPU, RAM и других ресурсов
- Снижение перегрузок и повышение стабильности системы
- Автоматическая адаптация к изменениям нагрузки
- Масштабируемость на кластерах любого размера
- Надёжность решений - математические модели и алгоритмы обеспечивают сбалансированные и предсказуемые решения

Доступ и аутентификация



Централизованное управление доступом и аутентификацией

Сфера и Прокуратор обеспечивают единую модель аутентификации и ролевого доступа для всей среды виртуализации ПК «Звезда»

Возможности платформы

Единая аутентификация

Поддержка интеграции с AD, ALD Pro,OpenLDAP, FreeIPA, Samba

Аудит

Журналирование всех действий пользователей

Централизованное применение политик

- Единые политики доступа на уровне: кластеров, хостов, ВМ, сетей и хранилищ
- Наследование и переопределение прав

Ролевое управление доступом (RBAC)

- Гибкая модель ролей и привилегий
- Разделение обязанностей и минимизация рисков

Безопасность и надежность

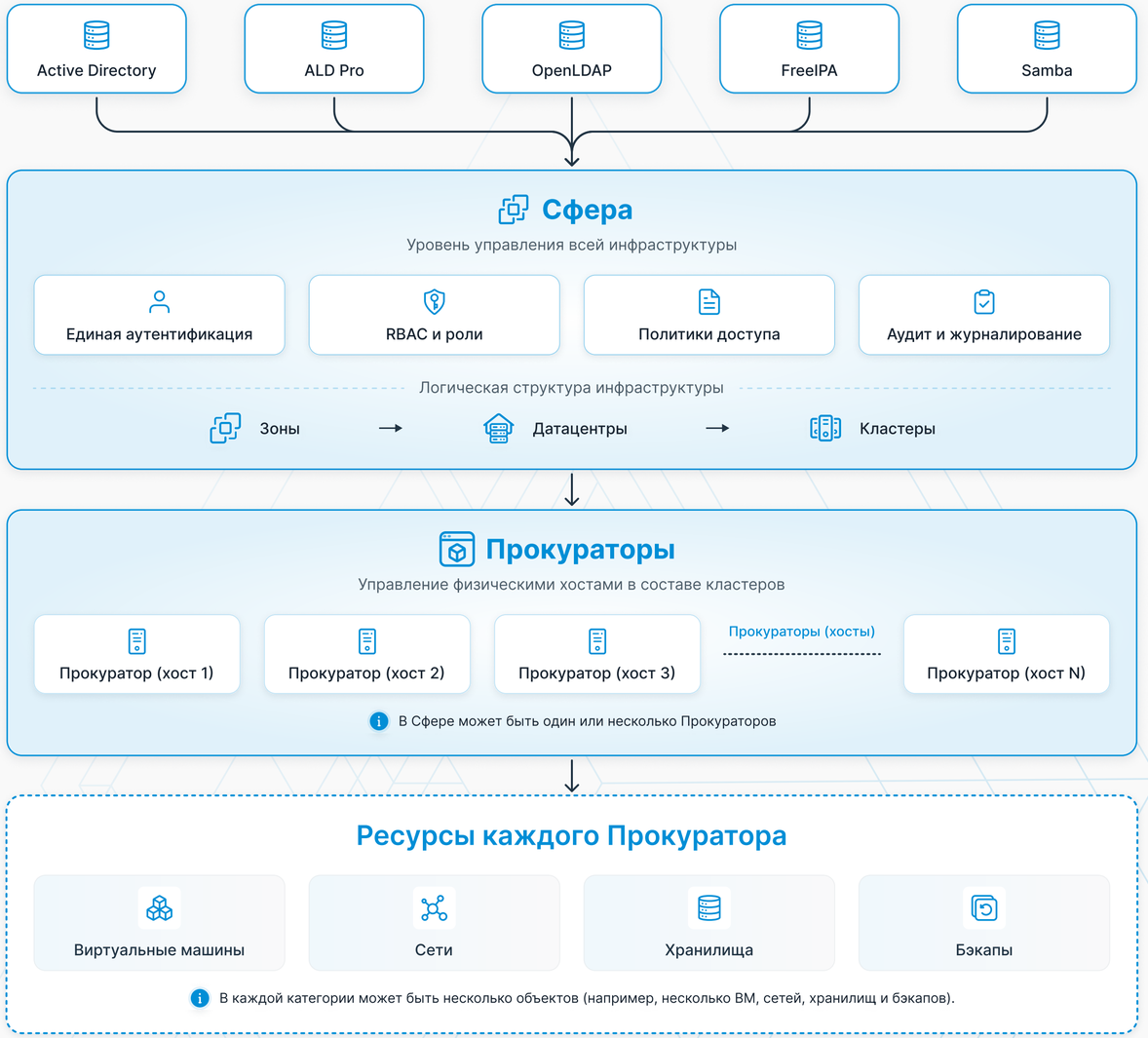
- Шифрование каналов и безопасные протоколы
- Защита от несанкционированного доступа
- Двухфакторная аутентификация

Операционная эффективность

Упрощение администрирования и снижение трудозатрат

Масштабируемость

Поддержка роста инфраструктуры без усложнения управления



Двухфакторная аутентификация пользователей

Безопасный доступ к платформе Сфера

Пользователь
Инициирует вход в систему

↓

Логин и пароль
Ввод логина и пароля

↓

LDAP / AD / FreeIPA/ALDPro/Samba
Проверка логина и пароля через корпоративный каталог (Identity Provider).

↓

Сфера
После успешной проверки запрашивается второй фактор — одноразовый код (TOTP).

↓

Google Authenticator / Яндекс Ключ / TOTP-приложение
Генерация 6-значного кода в приложении пользователя

↓

Подтверждение входа
Пользователь вводит код из приложения в Сфере

↓

Доступ к платформе
Успешная аутентификация и доступ к ресурсам

Ключевые возможности

- встроенная двухфакторная аутентификация в Сфере
- поддержка TOTP (6-значный код)
- совместимость с Google Authenticator и Яндекс Ключ
- подключение через QR-код
- обновление кода каждые 30 секунд

Важно

- Проверка логина и пароля выполняется через LDAP/AD/FreeIPA/ALDPro/Samba
- Проверка OTP-кода выполняется средствами Сферы

Политика безопасности и восстановление доступа

Защита учетных записей и управление двухфакторной аутентификацией в Sphere

Резервные коды восстановления

Подключение 2FA
Пользователь сканирует QR-код и подтверждает активацию

→

Выдача кодов
Система выдает 6 одноразовых резервных кодов в открытом виде

→

Хранение в Sphere
Коды сохраняются в зашифрованном виде (Hash + Salt)

→

Использоване
При утрате доступа к приложению код используется однократно

Важно
Двухфакторная аутентификация значительно снижает риск несанкционированного доступа к учетным записям и защищает критически важные ресурсы платформы.

Механизм защиты

- Секреты TOTP и резервные коды хранятся в виде Hash + Salt
- TOTP-код действителен в течение 30 секунд
- Резервные коды используются однократно
- Требуется синхронизация времени через NTP-сервер
- Все операции 2FA выполняются внутри Sphere

Обязательная двухфакторная аутентификация (2FA)

Включении политики
Администратор включает обязательную 2FA для всех пользователей

↓

Grace Period
У новых пользователей отсчет начинается с момента создания учетной записи. У существующих - с первого входа после включения политики.

↓

Уведомление
В течении примерно 7 дней на веб-интерфейсе отображается уведомление «Подключите 2FA»

↓

Блокировка
Если пользователь не подключил 2FAв течении Grace Period - учетная запись блокируется

Административные возможности

Блокировка
Администратор может включить обязательную 2FA через политики безопасности

Сброс 2FA
Администратор может снять двухфакторную аутентификацию для конкретного пользователя при утрате доступа

Контроль соблюдения
Система отслеживает статус 2FA, уведомляет пользователей и обеспечивает соблюдение политик безопасности

Требования

Синхронизация времени
Для корректной работы TOTP необходимо, чтобы время на сервере Sphere и устройстве пользователя совпадало.

Рекомендуется использовать единый NTP-сервер для всей инфраструктуры

Важно Двухфакторная аутентификация значительно снижает риск несанкционированного доступа к учетным записям и защищает критически важные ресурсы платформы.

- Защита от компрометации пароля
- Соответствие требованиям ИБ и стандартам
- Контроль и гибкое управление доступом пользователей

Резервное копирование и снимки состояния ВМ



Резервное копирование и снимки состояния ВМ

Обеспечение защиты виртуальной инфраструктуры без использования внешних backup-решений

Основные возможности

Собственный Full Backup

- встроенный механизм резервного копирования
- создание полных резервных копий ВМ
- централизованное управление backup-операциями
- хранение резервных копий в выделенном backup-хранилище

Восстановление виртуальных машин

- восстановление ВМ из резервной копии
- минимизация downtime
- восстановление отдельных ВМ и сервисов

Snapshot-механизмы

- создание снимков состояния ВМ
- фиксация состояния памяти, дисков и конфигурации

Перспективы

До конца 2026 года планируется добавление функционала:

- дифференциальный и инкрементальный backup
- API для интеграции с внешними backup системами

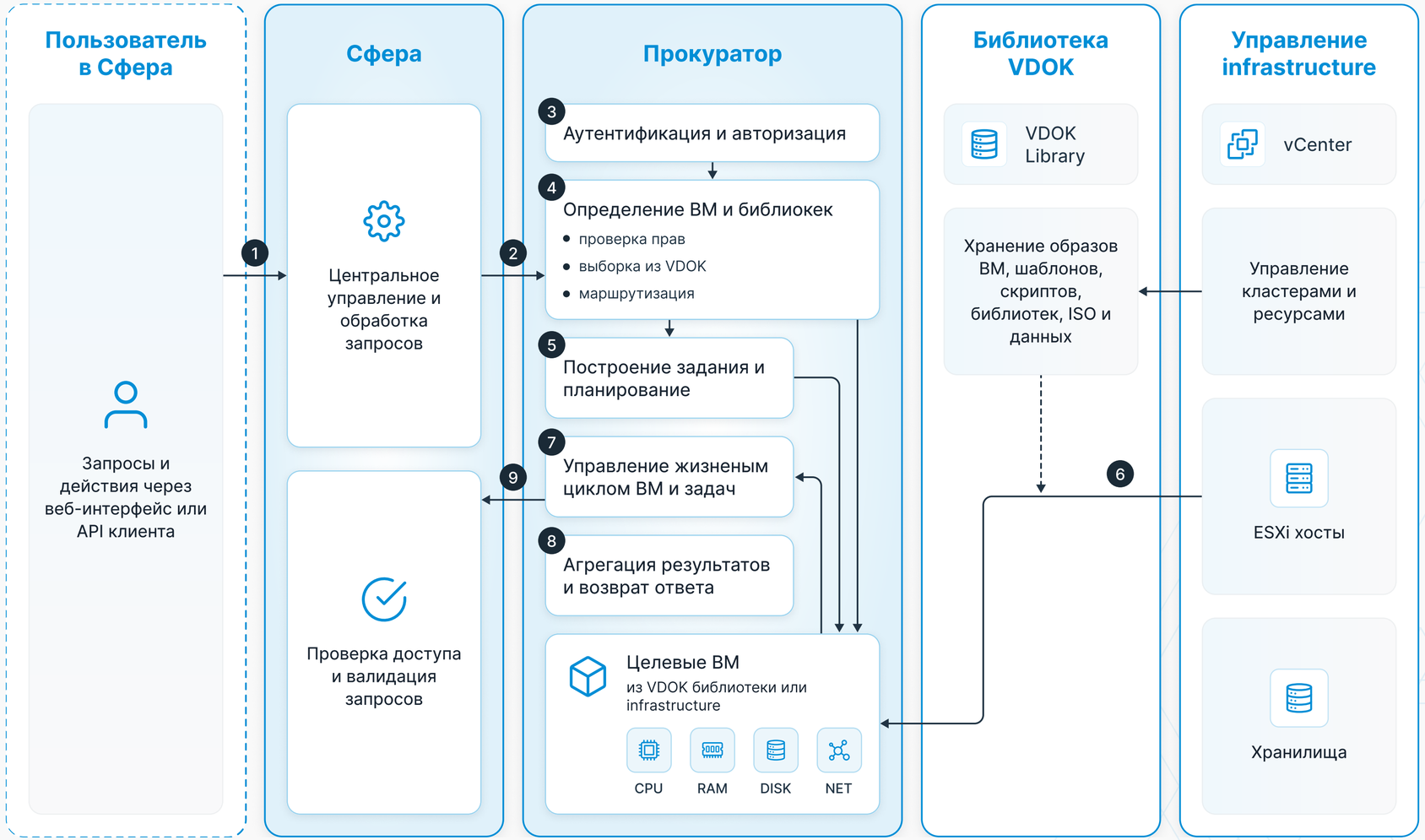


Инфраструктурные возможности платформы



Миграция ВМ из VMware

Перенос ВМ с минимальным временем простоя за счет нативных механизмов VMware и библиотеки VDDK



Как работает

1. Пользователь создаёт запрос на миграцию в Sphere
2. Sphere передаёт задание на миграцию Прокуратору
3. Прокуратор получает задание на миграцию от Sphere
4. Прокуратор создаёт целевую ВМ на платформе ПК «Звезда»
5. Прокуратор обращается к библиотеке VDDK
6. VDDK копирует данные из VMware и переносит их в целевую ВМ
7. Прокуратор контролирует процесс миграции и получает статусы от VDDK
8. Прокуратор формирует итоговый статус и отчёт для Sphere
9. Отображение результата миграции

Проверка миграции проводилась для VMware версий 7 и 8
Шифрование при миграции происходит на стороне VMware библиотекой VDDK

VDI-платформа



VDI-решение

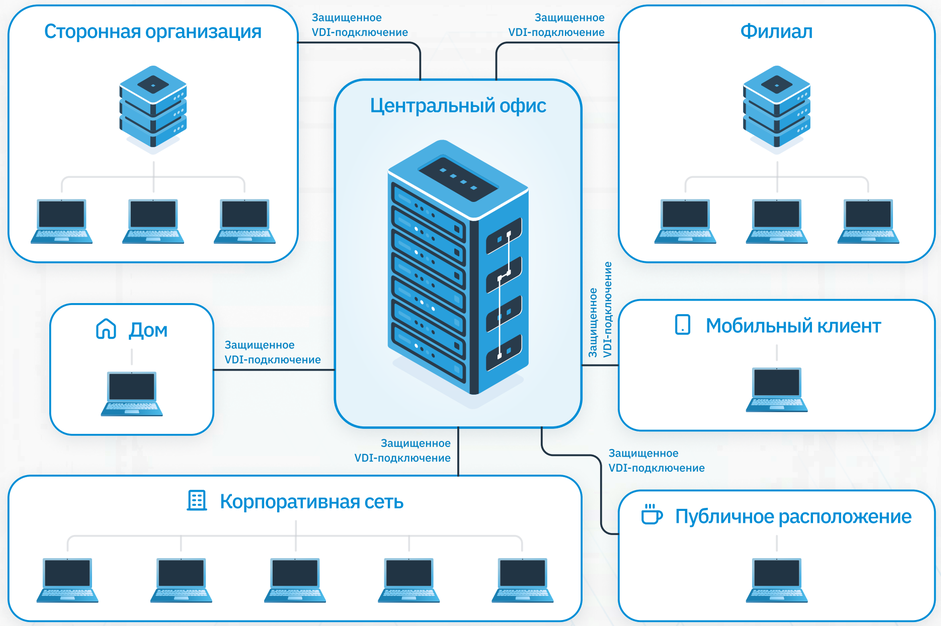
Безопасность, экономия и простота для удалённой работы

Назначение

- **Безопасный доступ** к корпоративным ресурсам из любой точки
- **Сохранность данных** – информация остаётся внутри инфраструктуры предприятия
- **Обеспечить привычные инструменты** – сотрудники работают в знакомой среде

Функционал

- Интеграция с **Active Directory, LDAP, SAML, RADIUS, Azure AD**
- **Автоматическое создание и управление ВМ**
- **Настройка пулов услуг, мониторинг использования, логирование**
- **Упрощает администрирование и масштабирование** рабочих мест
- **Интерфейс**: веб-панель управления с разделением прав доступа, вкладками для поставщиков услуг, аутентификаторов, мониторинга и журналов



Критерий	VDI	Обычные ПК
Безопасность	Данные в ЦОД	Риск утечки с устройств
Управление	Единый центр	Локальная поддержка
Стоимость	Экономия на железе	Затраты на ремонт/апгрейд
Гибкость	Работа с любого устройства	Привязанность к ПК

VDI-решение

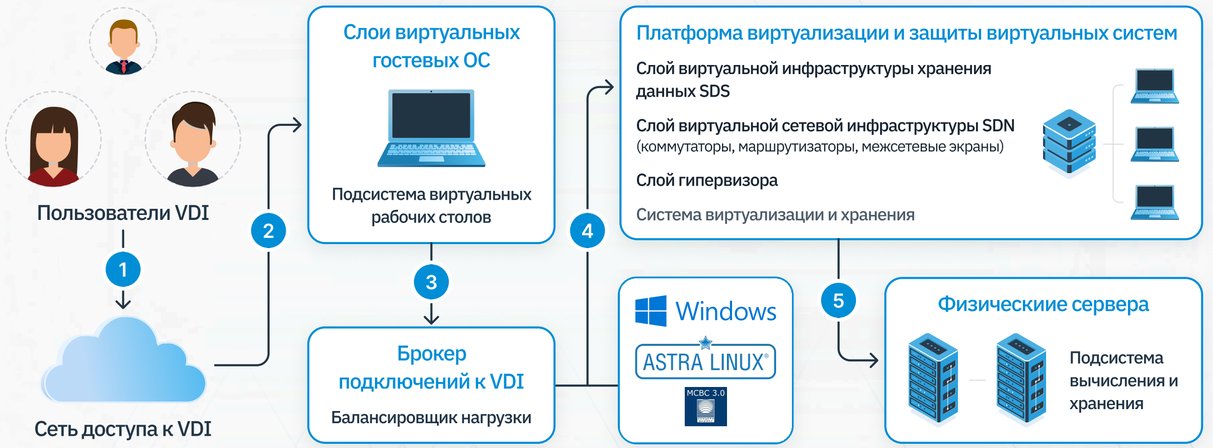
Безопасность, экономия и простота для удалённой работы

Как работает

1. Пользователи подключаются к инфраструктуре VDI через защищённую сеть доступа
2. Сессии виртуальных рабочих столов предоставляются через брокер подключений VDI с механизмами балансировки нагрузки.
3. Пулы виртуальных рабочих столов функционируют в изолированных средах гостевых операционных систем.
4. Платформа виртуализации и безопасности обеспечивает централизованное управление инфраструктурой, SDS, SDN и сервисы гипервизора.
5. Физические серверы предоставляют вычислительные и storage-ресурсы для работы VDI-инфраструктуры

Возможности

- Поддержка 3D-графики
- Работа с периферийными устройствами
- Доступ к графическому ускорению ВМ
- Клиенты для x86, ARM и Эльбрус
- Поддержка NVIDIA и AMD
- Поддержка клиентских устройств на архитектурах x86, ARM и Эльбрус (E2K)

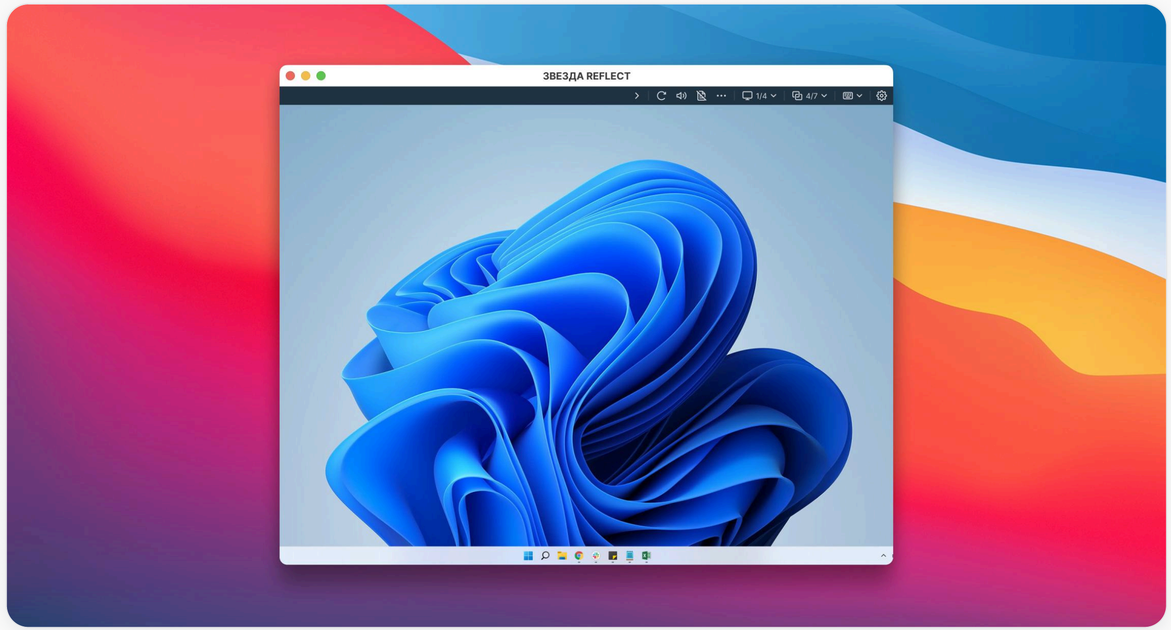


VDI-решение

Безопасность, экономия и простота для удалённой работы

Технические особенности

- **Интеграции:** LDAP/LDAPS, RADIUS
- **Протоколы:** RDP, NX, PCoIP, SSH, HTTPS, SPICE, «Reflect»
- **Безопасность:** SSL/TLS, Multi-Factor Authentication, изоляция сессий, контроль доступа
- **Масштабируемость:** поддержка кластеров, динамическое выделение ресурсов



Преимущества

- **Единый корпоративный АРМ под централизованным управлением** ИТ-службы
- Доступ к рабочему месту из **любой точки** и с **различных типов устройств**
- **Снижение затрат** на инфраструктуру и поддержку рабочих мест
- **Высокая доступность и надёжность** за счёт централизованного управления и быстрого восстановления ВМ
- **Гибкая аутентификация и контроль доступа** (MFA, корпоративные каталоги пользователей)
- **Поддержка графически нагруженных** рабочих мест
- **Удобство:** единая точка управления разнородной виртуальной инфраструктурой
- **Широкая поддержка** платформ виртуализации
- **Поддержка статических и динамических пулов** виртуальных рабочих мест для различных сценариев эксплуатации

VDI-решение

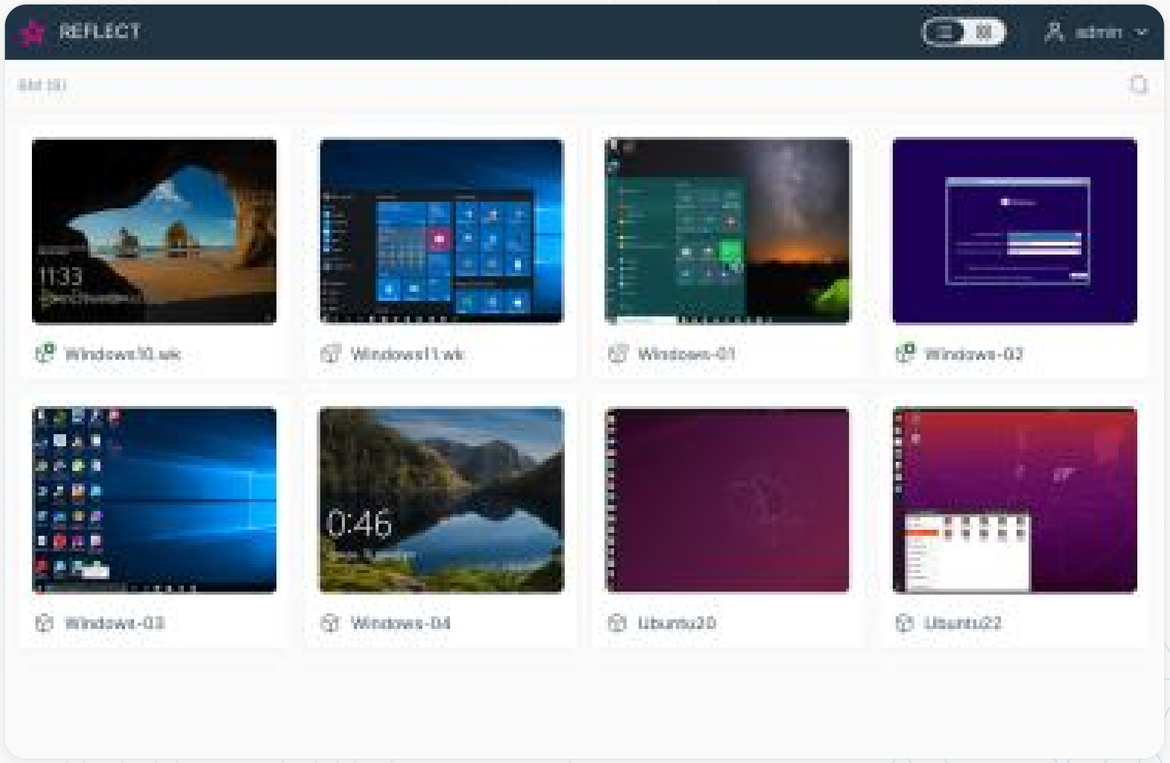
Безопасность, экономия и простота для удалённой работы

Назначение

Безопасный доступ к графическому окружению ВМ с поддержкой 3D-графики, стриминга и периферии

Ключевые функции

- Доступ к **графической оболочке ВМ** (включая 3D-ускорение)
- Поддержка **периферийных устройств** (мышь, клавиатура, USB)
- **Кроссплатформенность**:
  - Десктоп: Windows, Linux, macOS
  - Мобильные ОС: Android, iOS, Aurora
  - Веб-браузер
- **Поддержка архитектур**: x86, ARM, Эльбрус



Компоненты «Reflect»

Reflect Клиент (десктоп/мобильный/веб)

- Пользовательская точка входа
- Режим аппаратного ускорения и режим SPICE (fallback)
- Поставляется в виде дистрибутива для установки на клиентское устройство (веб-клиент доступен по умолчанию)

Reflect Сервер

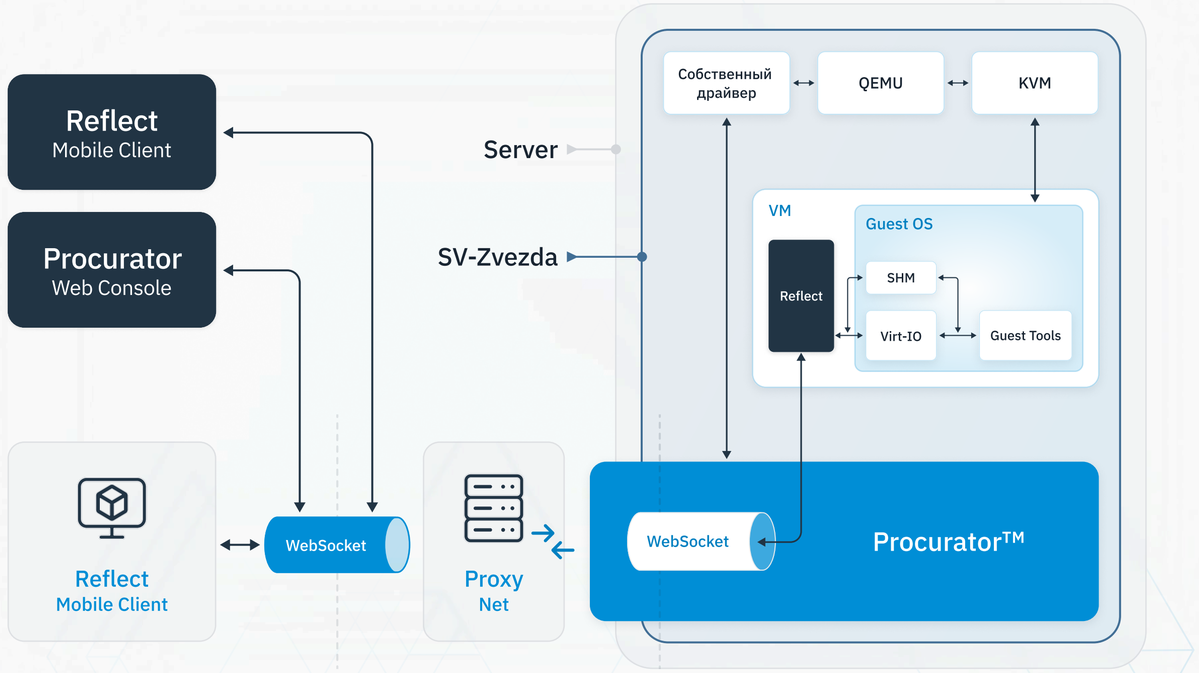
- Ядро протокола
- Реализация функционала на уровне гипервизора
- Поставляется в виде приложения для ОС «Звезда»

Reflect Драйвер

- Сторонний драйвер для гипервизора + утилиты для автоматизации управления через Прокуратор. Например, драйвер NVIDIA vGPU
- Поставляется в виде приложения для ОС «Звезда»

Procurator Desktop Agent

- Набор гостевых утилит
- Реализация функционала на уровне гостевой ОС (Windows/Linux)
- Поставляется в виде дистрибутива для установки в гостевую ОС

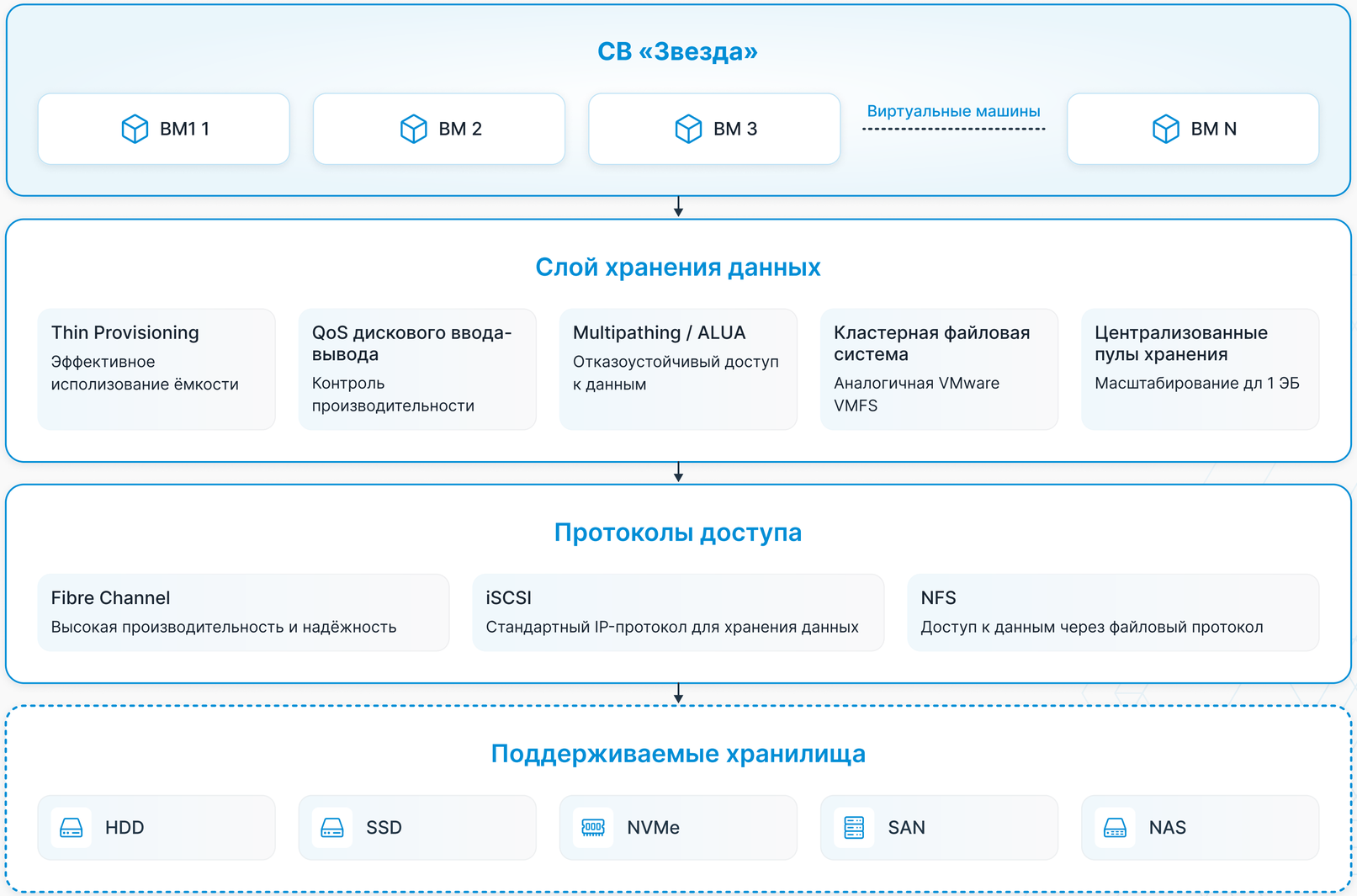


Storage



Возможности хранения для виртуализации

Единая подсистема хранения для размещения виртуальных машин, образов, шаблонов и резервных копий.



Ключевые возможности

Централизованные пулы хранения
Масштабирование емкости до 1 ЭБ

Размещение ВМ на локальных и внешние СХД
Гибкость и выбор оптимального хранилища

Поддержка SAN и NAS
Интеграция с существующей инфраструктурой

Thin Provisioning
Динамическое выделение ресурсов по мере необходимости

Отказоустойчивый доступ
Multipathing и ALUA обеспечивают непрерывность работы

QoS дисковой подсистемы
Контроль нагрузки и приоритизация важных операций

РСХД Шторм

Единое хранилище для виртуальной среды

Ключевые возможности для виртуализации

- Отказоустойчивое распределённое хранилище
- Поддержка всех типов ВМ
- Высокая доступность (автоматический failover при сбоях узлов)
- Динамическое масштабирование (добавление дисков и узлов без downtime)

Архитектурные компоненты

- **Ceph** – распределение пользовательских данных по дискам
- **iSCSI/NFS/CIFS/S3/RBD** – совместимостьс любыми гипервизорами
- **Consul** – сервис-дискавери и мониторинг состояния кластера
- **NTP** – гарантия безопасности данных при чтении и записи

Как РСХД Шторм работает с ВМ (интеграция с гипервизорами)



Как работает

1. Данные разбиваются на объекты и распределяются по OSD-узлам
2. Обновление состояния ряда параметров и настроек посредством Consul
3. NTP – обеспечение синхронизации времени между узлами для обеспечения безопасности данных кластера
4. Доступ через стандартные протоколы (S3/NFS/CIFS/iSCSI)

РСХД Шторм

Единое хранилище для виртуальной среды

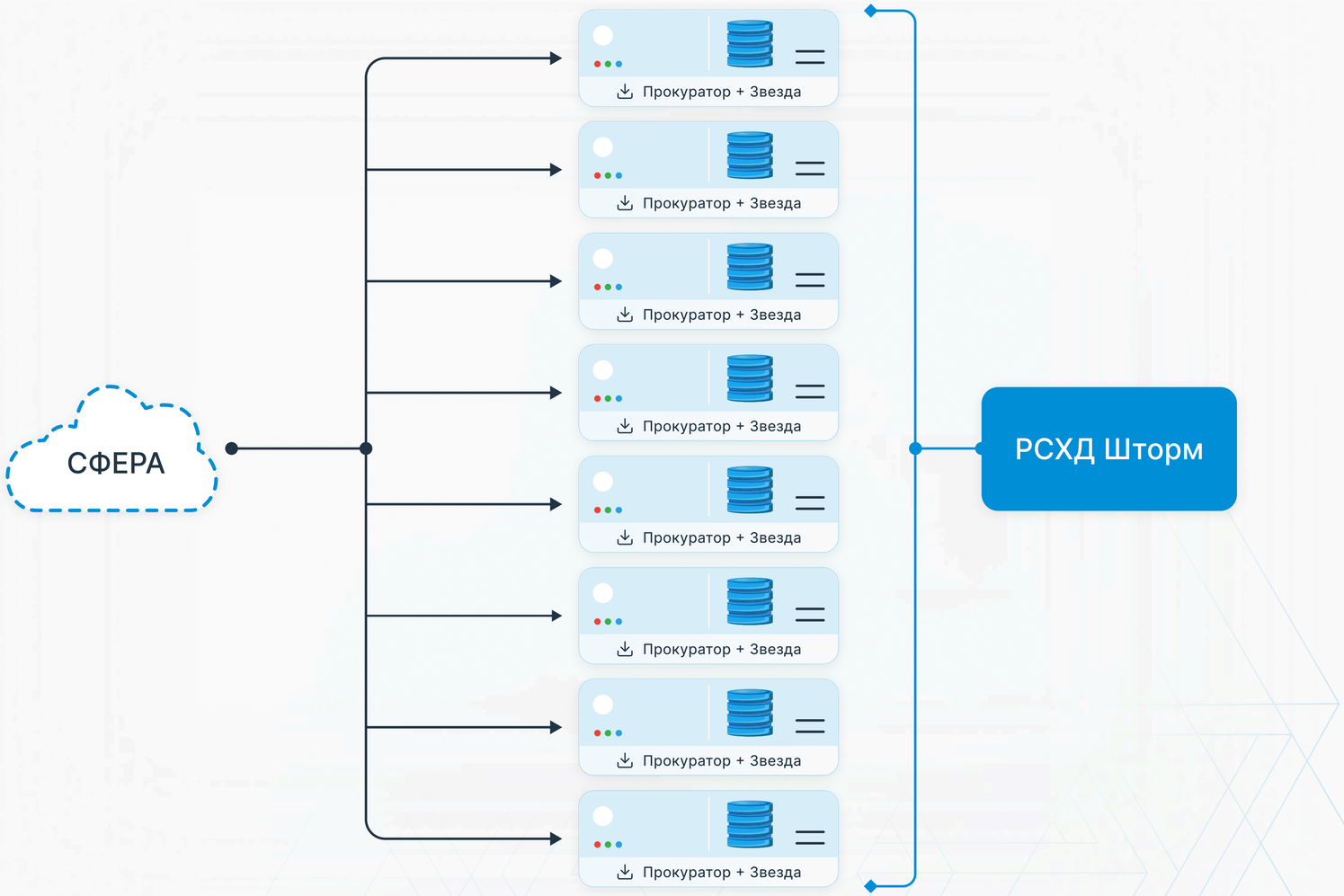
Функционал

1. **Отказоустойчивая кластерная архитектура**
   Данные сохраняются и остаются доступны даже при отказе узлов или дисков

2. **Удобное управление топологией**
   Для лучшего распределения данных

3. **Управление через удобный веб-интерфейс**
   Единая точка контроля и мониторинга

4. **Настройка репликации на уровне пула**
   Основное и минимальное число копий (минимум 1, максимум 5)



РСХД Шторм

Единое хранилище для виртуальной среды

Преимущества

- **Раннее обнаружение проблем:** уведомления о заполнении дисков и других событиях
- **S.M.A.R.T.-проверки** дисков с уведомлениями о поломках
- **Роль «Наблюдатель»** — безопасный доступ к мониторингу без права изменений
- **Лёгкое горизонтальное масштабирование** кластера через мастер развёртывания
- **Быстрый старт** – простое развертывание за счёт мастера и готовых пресетов сервисов (RBD, файловые сервисы, S3)
- **Гибкие правила репликации:** отдельные пулы под кэш, резервное хранение и другие сценарии
- **Прозрачность:** легко понять, какие диски использует каждый пул
- **Тонкая настройка весов дисков** для дополнительного контроля распределения
- **Гибкая настройка экспортируемых директорий**, прав доступа и пользователей
- **Поддержка IP-диапазона** для распределения между узлами и бесперебойного доступа к CIFS
- **Файловая система с «макетами»:** разные типы данных — в разных пулах
- **Встроенный бенчмарк:** массовая запись/чтение с параллельным сбором метрик; результат — в таблице
- **Кэш опережающей записи** для оптимизации дисковых операций
- **Повышенная производительность** за счет архитектурных решений (равномерное распределение хранения, использование tiring, наличие кэша)

Технические особенности

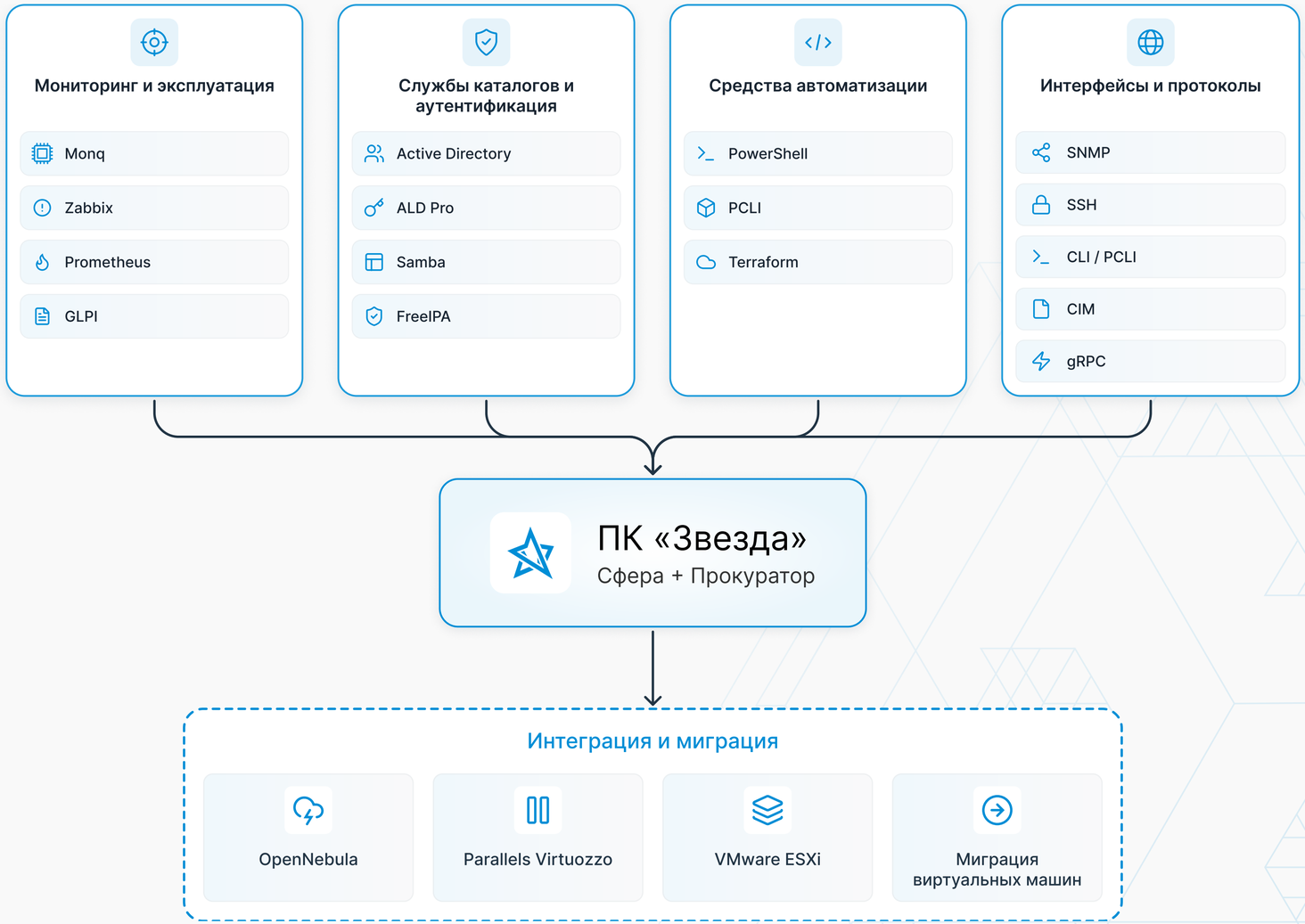
- **Erasure Coding:** экономия пространства за счёт CPU/времени, гибкая конфигурация чанков данных и контрольных чанков
- **Упрощённое создание таргетов:** TPG, ACL, Portal, LUN — из веб-интерфейса
- Гибкое управление службами на узлах (S3, iSCSI, NFS, CIFS, RBD) для повышения отказоустойчивости API
- Возможность работы в защищенной среде гипервизора «Звезда»
- Опционально создаются: пул RBD для iSCSI, стандартная файловая система и пулы под NFS/CIFS, конфигурация RGW для S3
- Встроенное сжатие (lz4, zstd, zlib, snappy) и режимы применения для экономии места

Интеграции



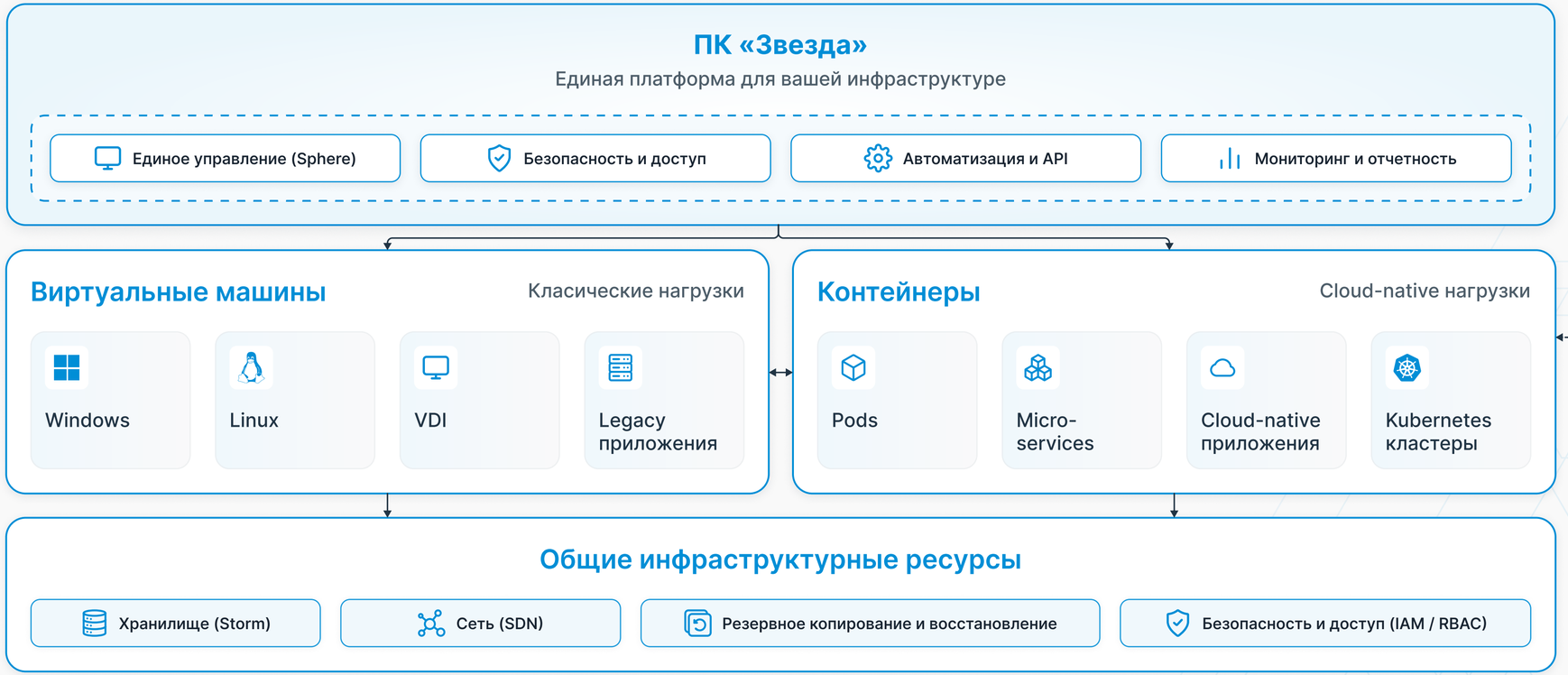
Интеграция и автоматизация

Открытая экосистема для интеграции с корпоративными сервисами, системами мониторинга и автоматизации



Контейнеризация и cloud-native приложения

ПК «Звезда» обеспечивает совместное использование виртуальных машин и контейнеризированных приложений в единой, безопасной и управляемой инфраструктуре



Интеграция со «Штурвал»

(Kubernetes-платформа)

Подключение Kubernetes-кластеров к инфрасктруктуре ПК «Звезда»

- Управление контейнерными нагрузками из единой точки
- Использование общих ресурсов вычислений, сети и хранения
- Единые политики безопасности и контроля доступа (RBAC)
- Открытый API для интеграции с внешними системами

Возможности решения

- ВМ и контейнеры в одной инфраструктуре
- Единые политики безопасности и дсотупа
- Общие вычислительные, сетевые и хранилищные ресурсы
- Поддержка современных cloud-native приложений и микросервисов
- Интеграция с Kubernetes-платформами (Штурвал)
- Высокая отказоустойчивость и масштабируемость

Единая платформа - единые преимущества | ПК «Звезда» помогает быстро внедрять современные приложения, оптимизировать ресурсы и обеспечивать надёжную работу ИТ-инфраструктуры любой сложности.

DeepMail



Почтовая система «DeepMail»

Открытая экосистема для интеграции с корпоративными сервисами, системами мониторинга и автоматизации

Удобство использования

- **Облачный** WebDAV клиент
- Календари и планировщики задач с функцией **«free/busy»**
- Поисковая **многоуровневая** система
- **Встроенный инструмент** для работы с офисными документами
- **Аудио- и видеосообщения** как вложения письма

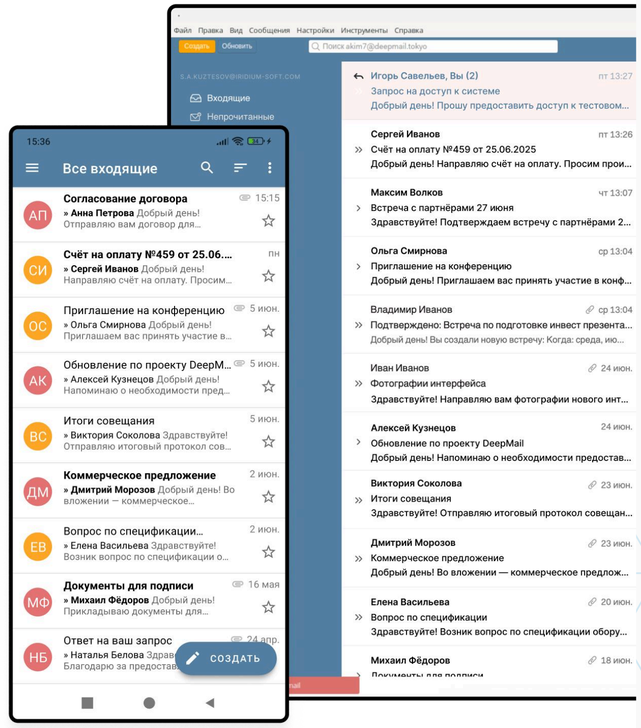
Безопасность

- **Функции криптозащиты PKI** (шифрование, электронная подпись)
- **Защита от утечки** данных DLP
- Встроенная **защита от спама**
- Встроенный **антивирус**

Механизмы снижения нагрузки на архитектуру

- **Балансировщик** нагрузки HA-proxy
- Разделение вложений **с большим объемом**
- **Хранение файлов** в виде ссылок
- **Функция дедупликации и сжатий** почтовых ящиков, контактови событий

Почтовый сервер-клиент, обеспечивающий полноценное и безопасное управление корпоративными коммуникациями через почту, календари, задачи и адресные книги

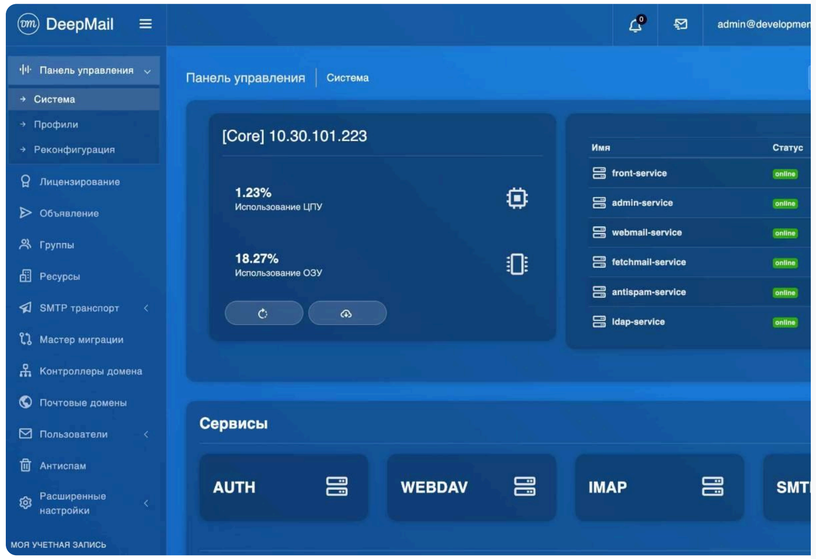


Почтовая система «DeepMail»

Открытая экосистема для интеграции с корпоративными сервисами, системами мониторинга и автоматизации

Сервер корпоративного уровня

- Современное решение для управления почтой, календарями и адресными книгами
- Поддержка до миллиона активных пользователей одновременно



Гибкая интеграция и масштабируемость

- Поддержка контроллеров доменов (SambaDC, ALD Pro, MS AD, FreeIPA)
- Развертывание в кластере
- Использование нескольких контроллеров домена, учетных записей сторонних серверов
- Работа с несколькими хранилищами, настройка релейных доменов
- Возможность интеграциис мессенджером,SIP-телефониейи информационными каналами

Гибкая настройка групповых политик

- Поддержка общих почтовых ящиков
- Использование групп рассылки (алиасов)
- Делегирование прав на отправку почты
- Поддержка групповых календарей
- Делегирование почтовых папок, календарей, адресных книг и задач

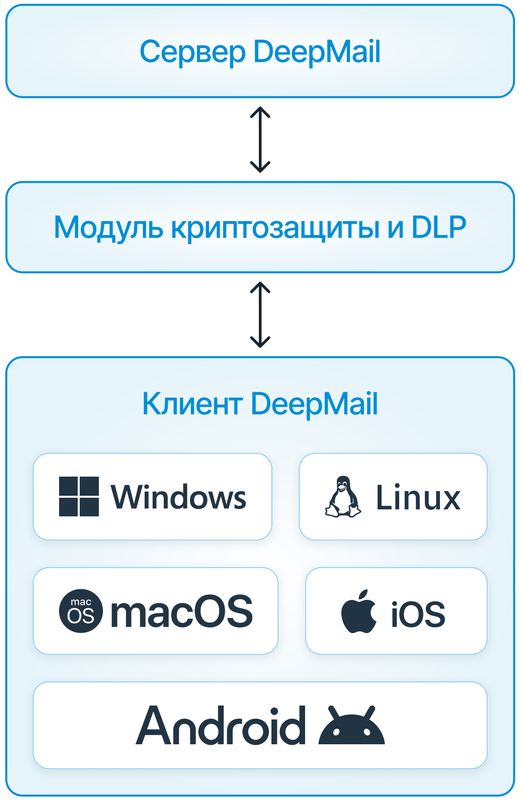
Поддержка почтовых сервисов и перенос данных

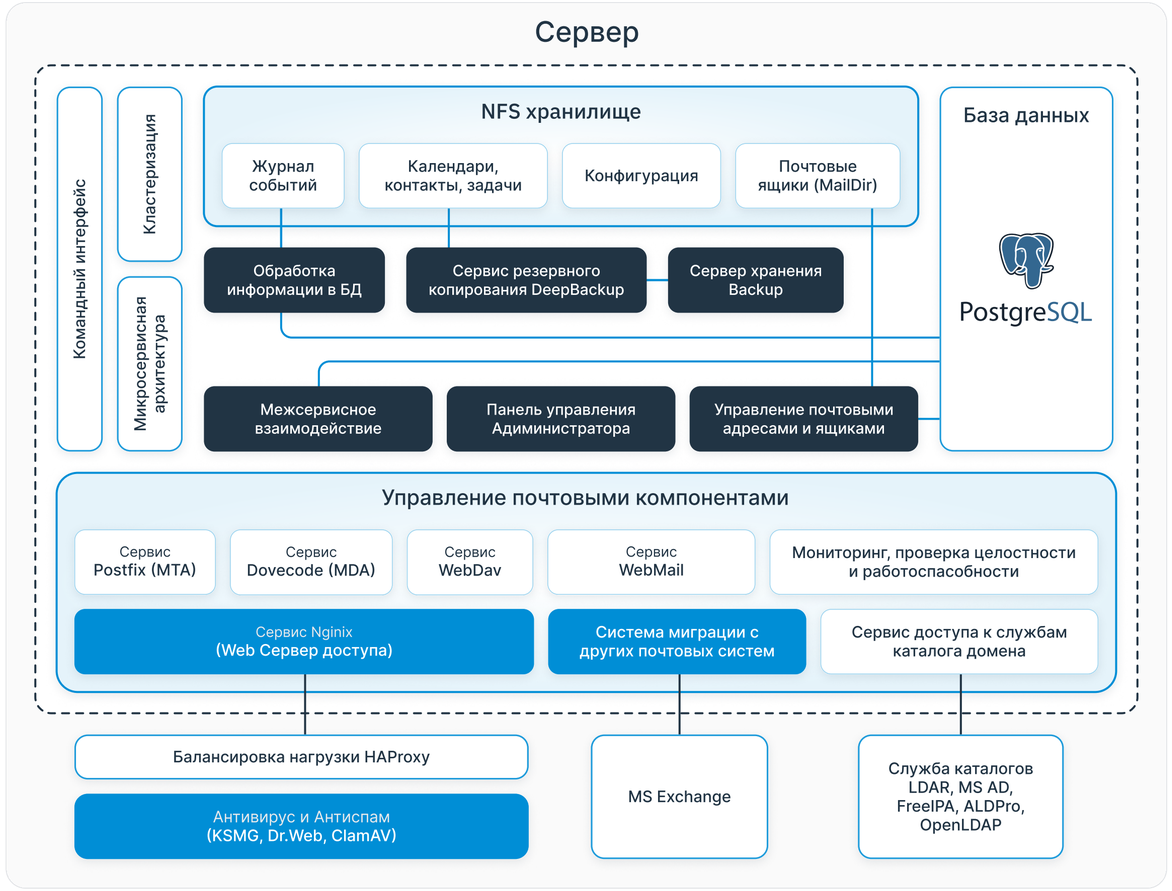
- Поддержка Microsoft Exchange Server и других сервисов (Gmail, iCloud, Outlook.com, Yahoo!, Hotmail, Mail.ru, Yandex и др.)
- Перенос почты из различных систем (Microsoft Outlook, Windows Mail, Mozilla Thunderbird, The Bat, MBOX и др.)

Архитектура DeepMail

Открытая экосистема для интеграции с корпоративными сервисами, системами мониторинга и автоматизации

Общая структура





Архитектура кластера DeepMail

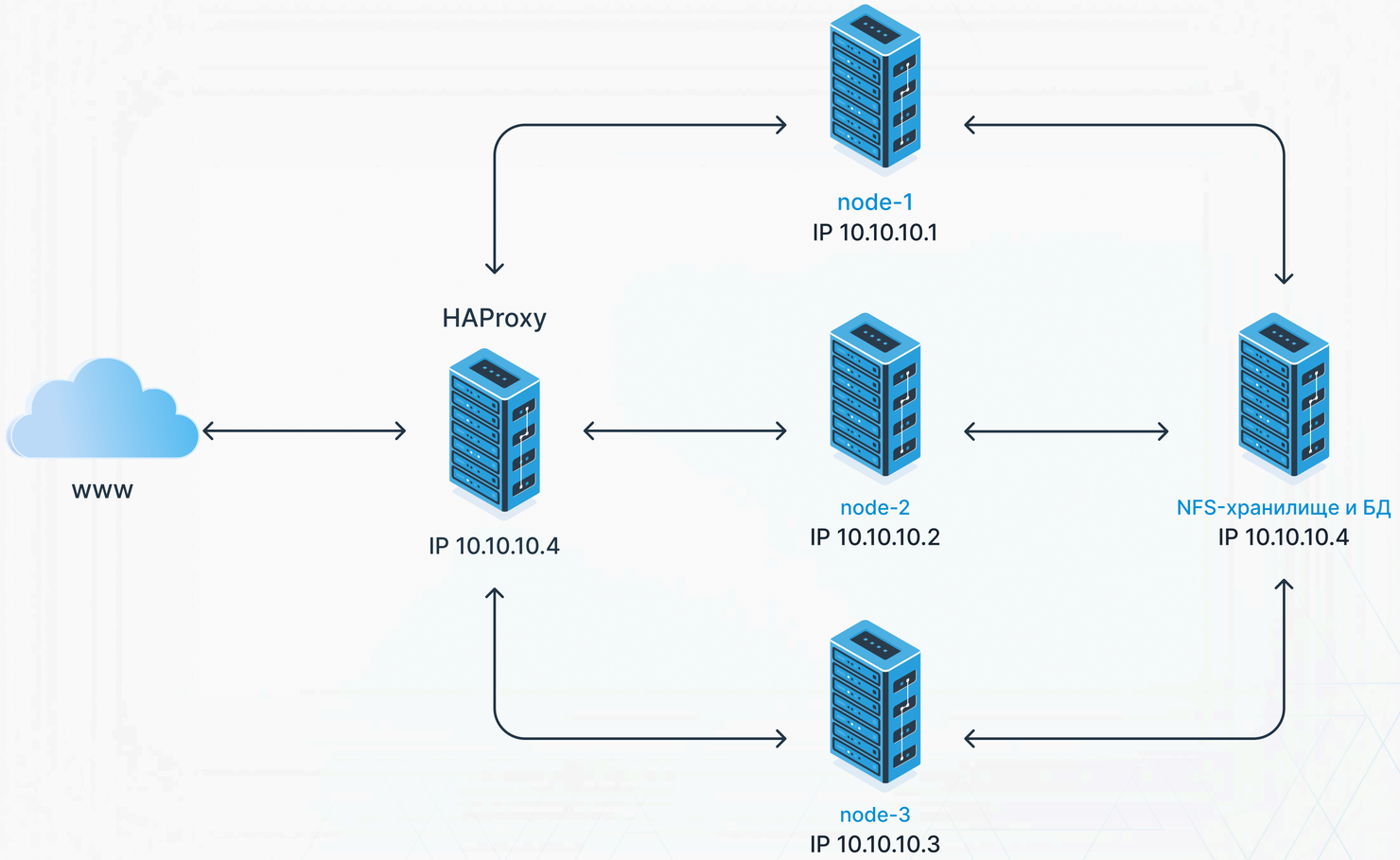
Обеспечивает отказоустойчивую работу почтовой системы за счет распределения сервисов между несколькими узлами, использования балансировщика нагрузки HAProxy и централизованного хранения данных на NFS-хранилище

Отказоустойчивый почтовый кластер с единой точкой входа

- Балансировщик нагрузки HAProxy обеспечивает единую точку входа пользователей
- Почтовые сервисы работают на трех узлах кластера (node 1–3)
- Узлы взаимодействуют между собой для обеспечения отказоустойчивости и синхронизации данных.
- Почтовые данные и база данных размещаются на выделенном NFS-хранилище
- Отказ отдельного узла не приводит к остановке работы системы

Ключевые преимущества

Архитектура позволяет масштабировать систему, выполнять обслуживание отдельных узлов без остановки сервиса и повышать доступность почтовой инфраструктуры



Основные сервисы сервера «DeepMail»

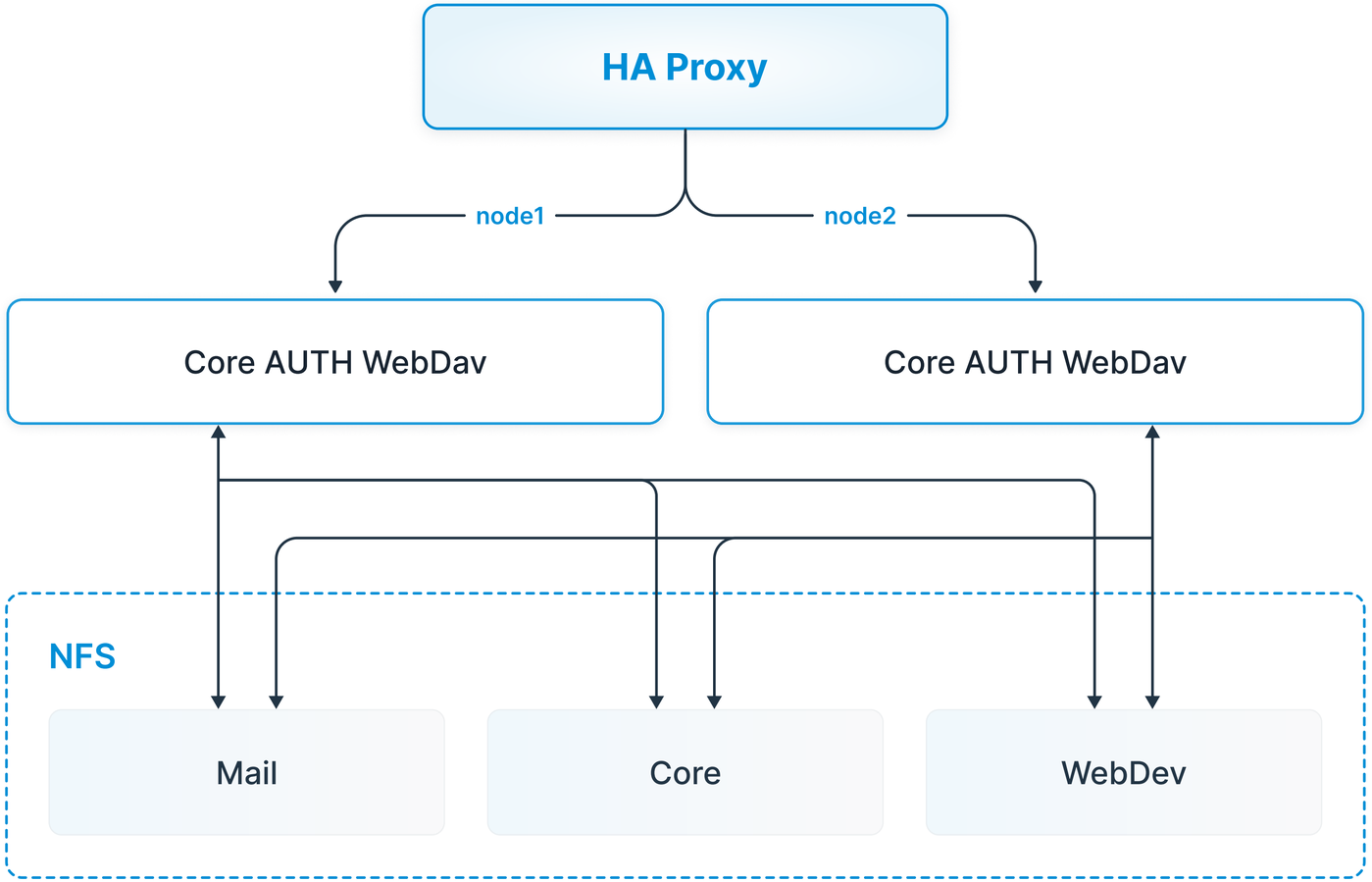
Обеспечивает отказоустойчивую работу почтовой системы за счет распределения сервисов между несколькими узлами, использования балансировщика нагрузки HAProxy и централизованного хранения данных на NFS-хранилище

Сервисы

- Core — координирует процессы работы с письмами, пользователями и календарями
- SMTP — отправка и получение почты
- IMAP — доступ к почтовым ящикам
- Auth — аутентификация пользователей
- WebDav — доступ и управление календарями, задачами и адресными книгами

Для отдельного сервиса используется только соответствующее хранилище в NFS

- Core Storage — хранит конфигурационные файлы, настройки, журналы внутренних процессов и ключи DKIM
- WebDav Storage — контакты и календари
- Mail Storge — почта, флаги и сортировки сообщений, папки, индексы сообщений и папок



Спасибо за внимание!

Наш сайт

Дистрибутив

aobfg.ru

info@aobfg.ru

+7 (495) 120-65-09

Технический пример развёртывания инфраструктуры

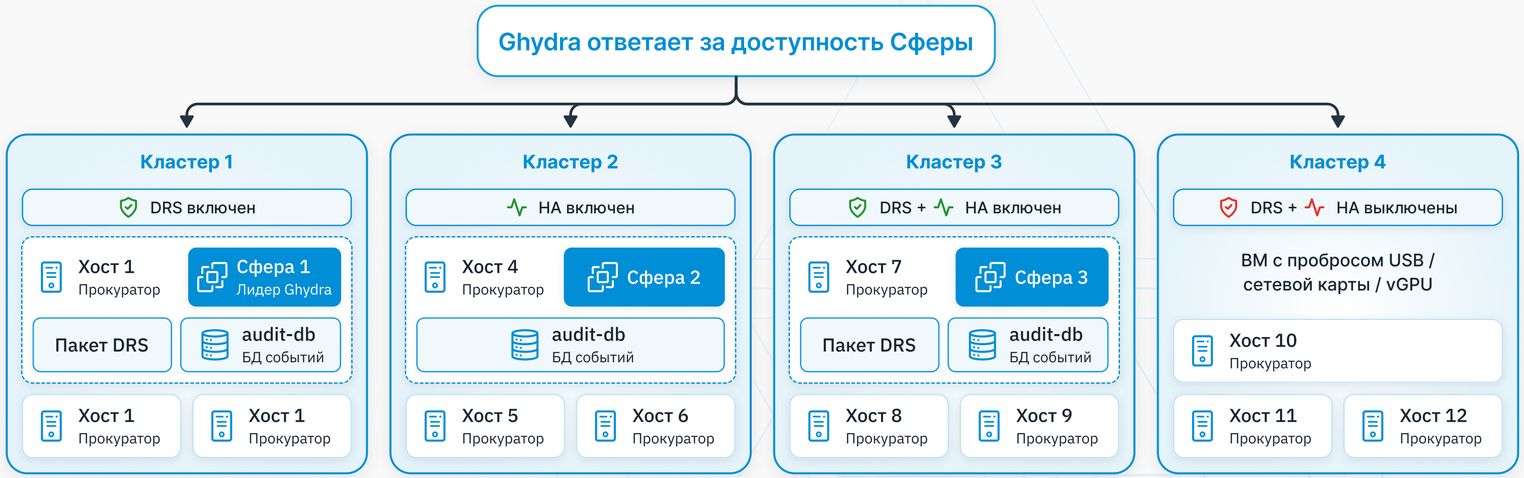


Схема виртуализации: 12 хостов/4 кластера

Обеспечивает отказоустойчивую работу почтовой системы за счет распределения сервисов между несколькими узлами, использования балансировщика нагрузки HAProxy и централизованного хранения данных на NFS-хранилище

Схема

- Сфера собрана в Гидру
- DRS и HA работают на уровне кластера
- Пакет DRS установлен только на хостах 1 и 7
- При отказе хоста с лидером Гидра выбирает нового лидера
- В кластере 4 DRS и HA отключены, так как в нем размещаются ВМ с пробросом USB / сетевой карты / vGPU (такие ВМ не могут мигрировать на другие хосты)



Важно для Сферы

- Сфера может быть размещена на хостах в разных кластерах или все узлы Сферы могут быть размещены в одном кластере
- Роли — только лидер и фолловер
- Для гидры обязательно наличие нескольких узлов Сферы: 3 или 5
- Фронтенд поддерживает до 5 узлов Сферы
- На разных узлах используется 3 экземпляра Сферы на хостах1, 4 и 7

Важно для DRS

- DRS отвечает за распределение ресурсов и миграцию ВМ для балансировки нагрузки в кластере
- Чтобы DRS начал работать (если версия Прокуратора без пакета DRS): 1) удалить хост из инвентаря кластера; 2) установить и включить пакет DRS; 3) вернуть хост в кластер.
- Сфера запрашивает список пакетов один раз в 24 часа (Reboot Сферы так же запустит переопрос всех пакетов на хостах)— в момент добавления хоста в кластер. Если в этот момент обнаружен пакет DRS, функциональность DRS становится доступной в системе в целом
- Для работы DRS достаточно одного установленного пакета, но чем больше пакетов DRS в инфраструктуре, тем выше отказоустойчивостьи доступность DRS
- Если все хосты с установленным пакетом DRS недоступны, DRSв системе будет недоступен

Важно для HA (High availability)

- HA отвечает за автоматический перезапуск ВМв рамках кластера
- HA работает только на лидере Гидры; если лидер недоступен, HA запускается на новом лидере
- Если отказ произошёл только у ВМ, но хост остаётся доступным и находится на связи, storage ВМ доступен, HA может перезапустить ВМ на том же хосте
- Сбоем считаются состояния ВМ, отличные от (PowerOn, PowerOff, Suspended, Paused); например: Error, Unknown, Warning
- ВМ переедет, если хост выключился по питанию. HA работает при условии наличия общего / общих хранилищ

Важно для Audit DB

- Audit-db - это обёртка над БД ClickHouse
- Audit-db используется для хранения событий
- должна размещаться на каждом хосте, где установлена Сфера
- База вынесена отдельно, потому что должна уметь собираться в Raft так же, как etcd и NATS в составе Сферы / Гидры
- Любые записи, выполненные через любой экземпляр Сферы, сохраняются и доступныс любой другой ноды

Дорожная карта



Дорожная карта развития 2026–2028

Отечественная платформа виртуализации ПК «Звезда»

Полный отечественный стек виртуализации — переход с VMware без переобучения. Гипервизор сертифицирован ФСТЭК №4934(СЗИ,КИИ до1-й категории)

	Доступно сейчас	2026	2027	2028
Переход с VMware	• Интерфейс как в vCenter — не требуется переобучение • Весь базовый функционал виртуализации • Импорт ВМ, в т.ч. из VMware • Дистрибутивы слицензией на 30 дней в открытом доступе • Инсталляция за 5 минут	• Живая миграция из vSphere	• Перенос нагрузок между площадками без простоя	• Миграция целых ЦОД «под ключ»
Доверенная среда	• Гипервизор 1-го типа сертифицирован ФСТЭК №4934 (СЗИ), КИИ до 1-й кат. • Сертификация по 4 классу защиты • В реестре российского ПО • Доверенная загрузка и контроль целостности • Ролевой доступ (RBAC) и аудит действий • Двухфакторная аутентификация • Шифрование данных при миграции ВМ • Шифрование данных при импорте ВМ из других сред виртуализации	• Антивирус Касперского	• vTPM, российская криптография	• Доверенные вычисления (confidential computing)
Управление уровня vCenter	• Централизованное управление ЦОД, кластерами, сетями, хранилищами • DRS • кластеры до 256 узлов, десятки тысяч ВМ • Жизненный цикл ВМ: клонирование, шаблоны, снапшоты с откатом • Изменение ресурсов ВМ без простоя (hot-add:vCPU,память, диски, сеть) • До 255vCPUи36ТБО3УнаВМ • Мониторинг ресурсов в реальном времени • Централизованное обновление • Папки для группировки объектов инфраструктуры (как в vCenter)	• Система алертов • StorageDRS— автобалансировка ВМ по хранилищам • Правила размещения ВМ(affinity/anti-affinity) • Отчёты и аналитика • Глобальный поискпообъектам инфраструктуры исостояниям • Эталонные профили хостов(HostProfiles) • Пулы ресурсов с квотами (resource pools) • Порядокзапуска (автостарт) ВМ в настройках хоста	• Управление несколькими регионами • Автонастройка гостевых ОС (sysprep, cloud-init) • Группы приложений с порядком запуска (vApps)	• Предиктивная аналитика • Энергонезависимая память для ускорения (PMem)

Дорожная карта развития 2026–2028

Отечественная платформа виртуализации ПК «Звезда»

Полный отечественный стек виртуализации — переход с VMware без переобучения. Гипервизор сертифицирован ФСТЭК №4934(СЗИ,КИИ до1-й категории)

	Доступно сейчас	2026	2027	2028
Непрерывность бизнеса и защита данных	• HA-кластеры и автозапуск согласно политикам DRS • Отказоустойчивость системы управления • Встроенное резервное копирование • Multipathing — отказоустойчивость хранения	• Репликация ВМ • DR/BCDR с тестовыми переключениями • Инкрементальные и дифференциальные бэкапы; копии в S3	• Растянутые (метро) кластеры	• Георазпределённое восстановление между ЦОД • Упреждающая эвакуация с проблемных хостов (Proactive HA) • Fault Tolerance для критичных ВМ
Сеть	• Виртуальные коммутаторы • VLAN (802.1Q) • LACP • Мониторинг трафика • DHCP-сервер • Зеркалирование трафика	• Программно-определяемые сети (Distributed Switch) • Встроенный экран для каждой ВМ, zero-trust (микросегментация, аналог NSX) • 100 Гбит/с сети	• dge-сервисы: балансировка, NAT, VPN, firewall (аналог NSX) • Сеть с низкими задержками, RDMA (RoCE)	• Дальнейшее развитие SDN
Хранилище	• РСХД «Шторм» (распределённое хранилище) • Локальные и внешние: HDD/SSD/NVMe, SAN/NAS • Протоколы: iSCSI, FC, NFS • LVM (Thin Provisioning) • Отказоустойчивый доступ к СХД (Multipathing, ALUA) • Файловая система аналогичная VMFS • Централизованные пулы до 1 ЭБ • QoS дискового ввода-вывода (SIOC)	• QoS • Настройка и оптимизация распределенного хранилища через веб	• Дедупликация и сжатие • Политики хранения • NVMe over TCP	• Аппаратное ускорение хранения (VAAI) • Интеграция с СХД на уровне ВМ (vVols/VASA)
Рабочие места (VDI)	• VDI: 3D-графика, стриминг, периферия • Безопасный доступ к графическому окружению ВМ • Клиенты для всех платформ (x86, ARM, Эльбрус) • Поддержка лицензий NVIDIA и AMD	• Развитие и оптимизация VDI • Оптимизация доставки изображения рабочего стола • Адаптивное качество трансляции	• Развитие и оптимизация VDI	• Развитие и оптимизация VDI

Дорожная карта развития 2026–2028

Отечественная платформа виртуализации ПК «Звезда»

Полный отечественный стек виртуализации — переход с VMware без переобучения. Гипервизор сертифицирован ФСТЭК №4934(СЗИ,КИИ до1-й категории)

	Доступно сейчас	2026	2027	2028
Автоматизация	• PowerShell • pcli (аналог ESXi CLI) • Terraform	• PowerShell для оркестратора уровня ЦОД • Расширение функционала pcli • Полный публичный API (gRPC)	• Автосценарии по событиям (policy-based automation) • Планировщик задач • Ansible	• Дальнейшее развитие
Интеграции	• Протоколы: SNMP, SSH, CLI, CIM, gRPC • Мониторинг: Monq, Zabbix, Prometheus, GLPI • Клиентское GUI-приложение для подключения к ВМ • Службы каталогов: AD, ALD Pro, Samba, FreeIPA • Миграция ВМ с платформ на базе OpenNebula, Parallels (Virtuozzo)	• API для систем бэкапа • Интеграция с внешними бэкап-системами • Совместимость с опенсорс-платформами (в обе стороны) • Миграция ВМ с Microsoft Hyper-V	• Совместимость с опенсорс-платформами (в обе стороны)	• Партнёрская экосистема и маркетплейс интеграций
Облака		• Интеграция с внешними облачными системами • Начало собственной разработки	• Аналог Cloud Director (портал самообслуживания, мультитенантность)	• Развитие облачной платформы
Аппаратная поддержка	• Клиенты «Спектр» / VDI на Эльбрус (x86, ARM, E2K) • MVP с отечественным интерконнектом «Альфа»	• MVP платформы виртуализации на Эльбрус • Продакшен-версия интеграции с интерконнектом «Альфа»	• Продакшен-версия на Эльбрус • 80 Гбит/с с интерконнектом «Альфа»	• Развитие и оптимизация