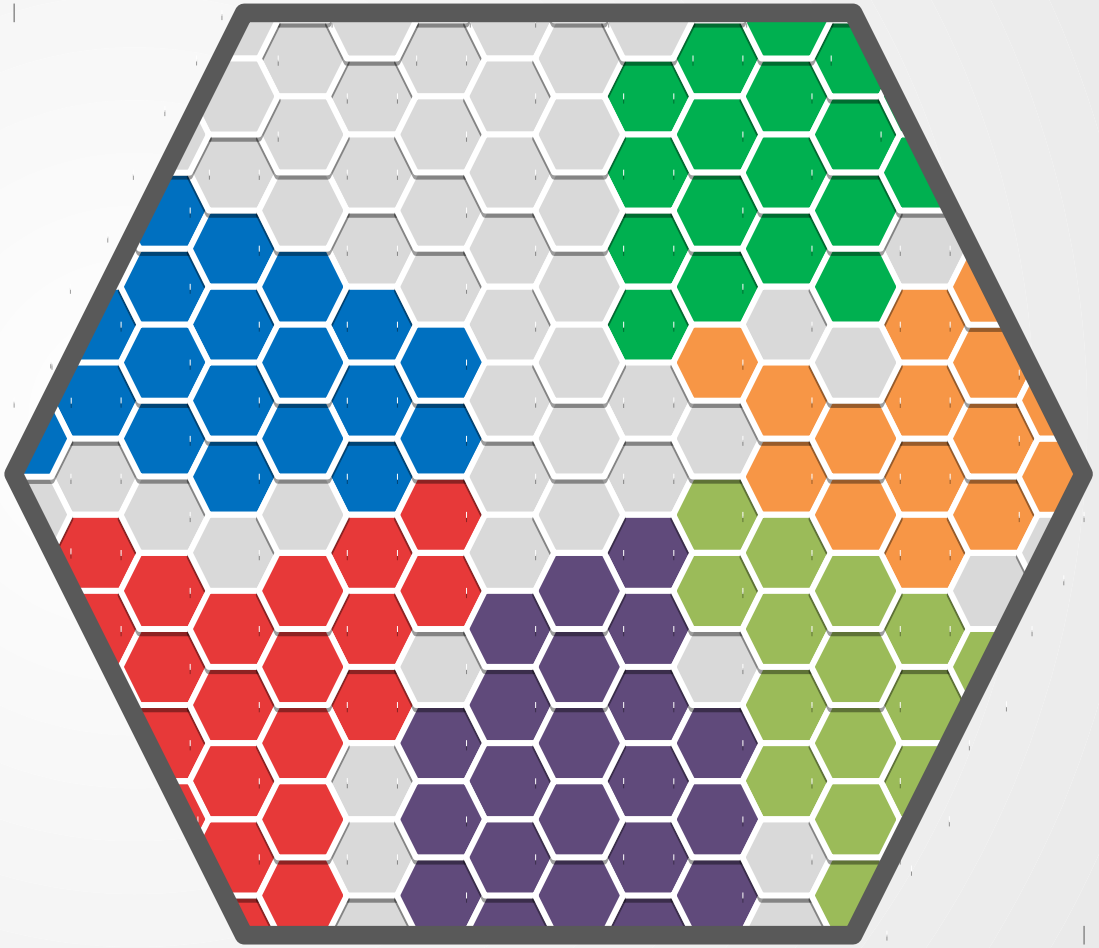
Защищенная облачная платформа

«Глобус»



Лаборатория 50

http://лаборатория50.рф

team@lab50.net

Общие сведения

Комплекс современных программных решений российской разработки для построения эффективной ИТ-инфраструктуры

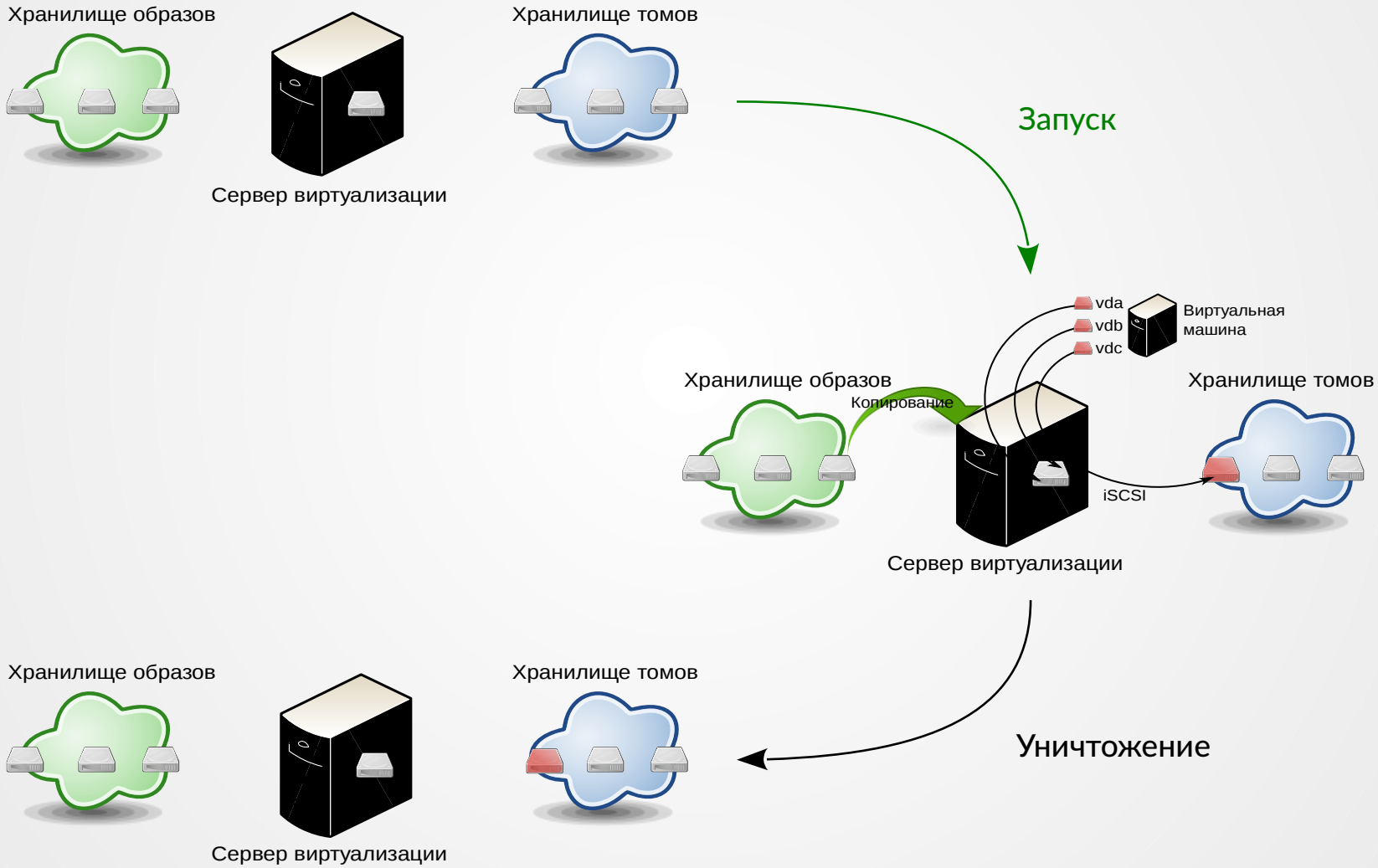
- АС с требованиями НДВ 2 и НСД 1Б ФСТЭК и Минобороны России
- Основана на свободном ПО OpenStack®
- Работает в среде ОС «Astra Linux Special Edition»
- Интеграция с «Astra Linux Special Edition»
- Разработка в тесном контакте с НПО «РусБИТех» с 2010 года

Технологии

Виртуализация вычислительных ресурсов:

- виртуальные машины
  - Линукс (Астра, МСВС), Windows, QNX/КПДА
- сети и маршрутизаторы
  - IPv4, VLAN и GRE, программные брандмауэры
- ресурсы хранения данных
  - постоянные тома

Как это работает



Компоненты

Глобус

облачная платформа

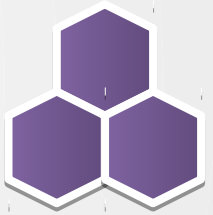
- Служба безопасности
- Менеджер виртуальных машин
- Реестр образов
- Оператор блочных устройств
- Сетевой интегратор

Гипервизор аппаратной виртуализации

QEMU/KVM

Распределенная отказоустойчивая файловая система

GlusterFS



Программный коммутатор

Open vSwitch

Безопасность

- Интеграция с комплексом средств защиты ОС «Astra Linux Special Edition»
- Аутентификация пользователей через Astra Linux Directory
- PARSEC для защиты виртуальных машин
- Интеграция в панель управления безопасности

Удаленное подключение

- Браузер (встроен в Астру)
- Протокол VNC
- Протокол SPICE
  - несколько мониторов
  - проброс USB-накопителей
  - драйвера для Linux, Windows
- Возможность авторизации по Kerberos (SASL)

Функциональность

- Виртуализация
  - до 160 ядер ЦП, 2 ТБ ОЗУ
  - «горячая миграция»
- Распределённая система хранения данных
  - реконфигурация «на лету»
  - петабайтная ёмкость
  - снимки
  - отказоустойчивость
- Поддержка широкого перечня оборудования

Разграничение доступа

Объекты

- Доменные пользователи
- Проекты
- Роли

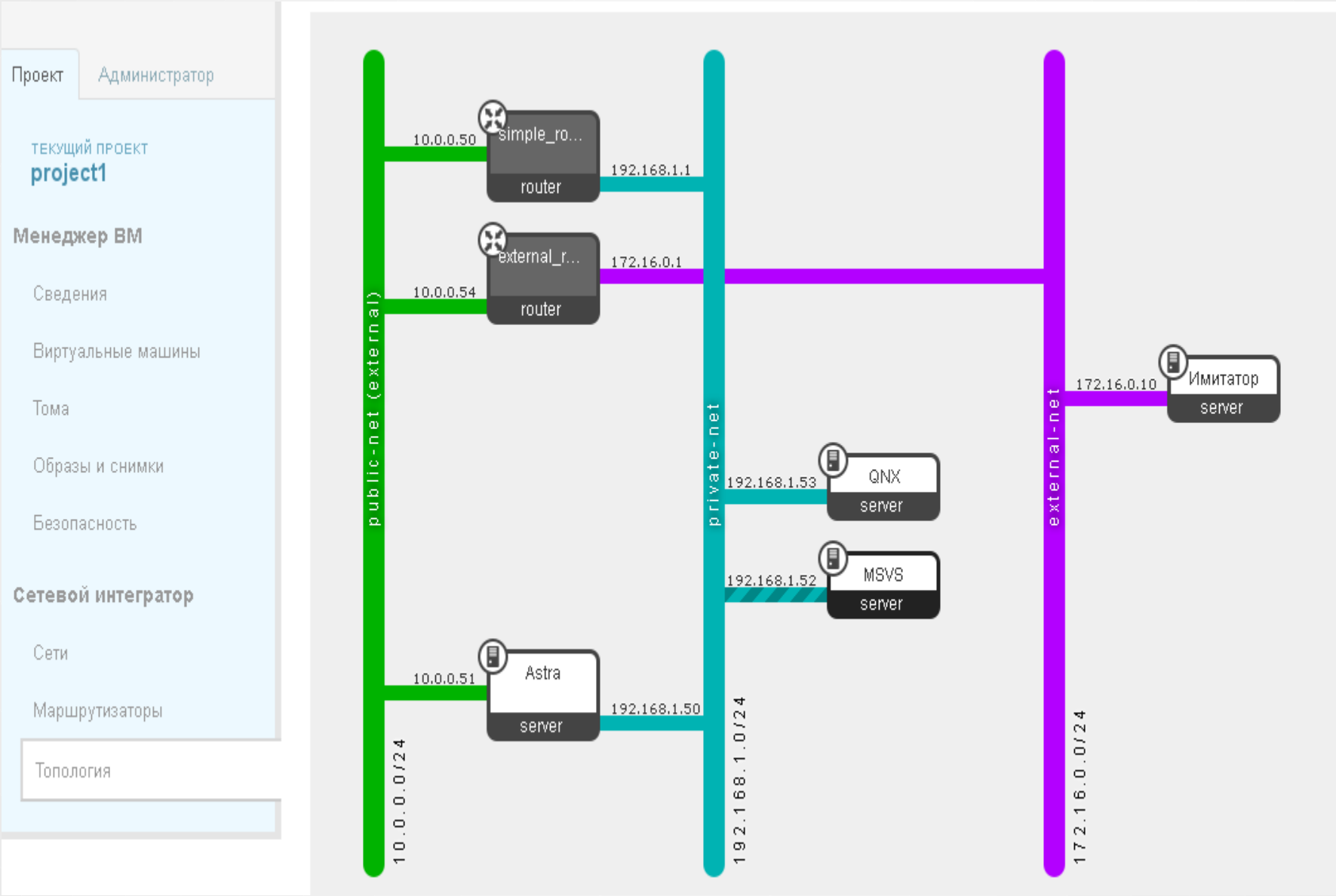
Принципы

- Ресурсы принадлежат проектам (квоты)
- Разграничение по проектам (+мандатный доступ)
- Полномочия на основе роли в проекте
- Независимо для каждого компонента по функциям

Сетевой интегратор

- **Изолированные сети**
  - на физическом уровне: VLAN или GRE
- **Внешние сети**
  - привязывается к физической сети
- **Закрытые (в проекте) или общедоступные**
- **Маршрутизация между сетями**
- **Независимый доступ из вне к любой ВМ через «плавающие IP»**
- **Виртуальный экран**

Сетевая топология



Возможности для стендов

- Работа в кооперации по защищенным каналам
- Параллельная работа К/А или подразделений над одной системой
- Универсальность и модернизационный потенциал
- База для испытательных стендов и комплексных тренажеров

Лицензирование

- Неограниченное количество ВМ и пользователей
- Управляющий сервер
- Наращиваемое количество серверов виртуализации
- Всё, кроме кластерной файловой системы