

Белорусский университет информатики и  
радиоэлектроники, кафедра ЭВМ

# Изоляция GRID-задач с помощью LXC

Пынькин Д.А.

# Задачи

Предоставить GRID — задачам отдельное программное окружение

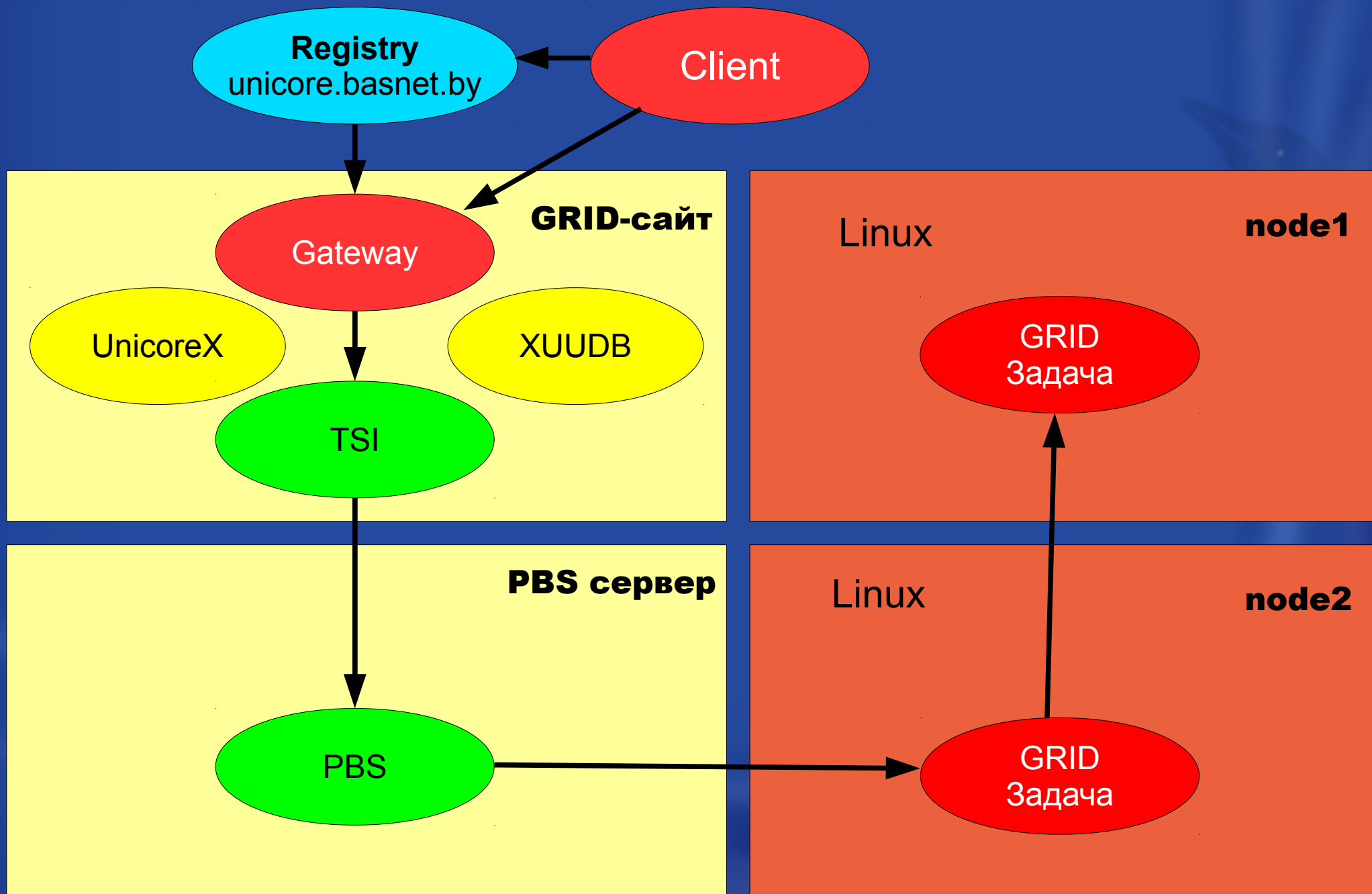
Изолировать влияние GRID — задач на рабочие станции студентов

# Терминология

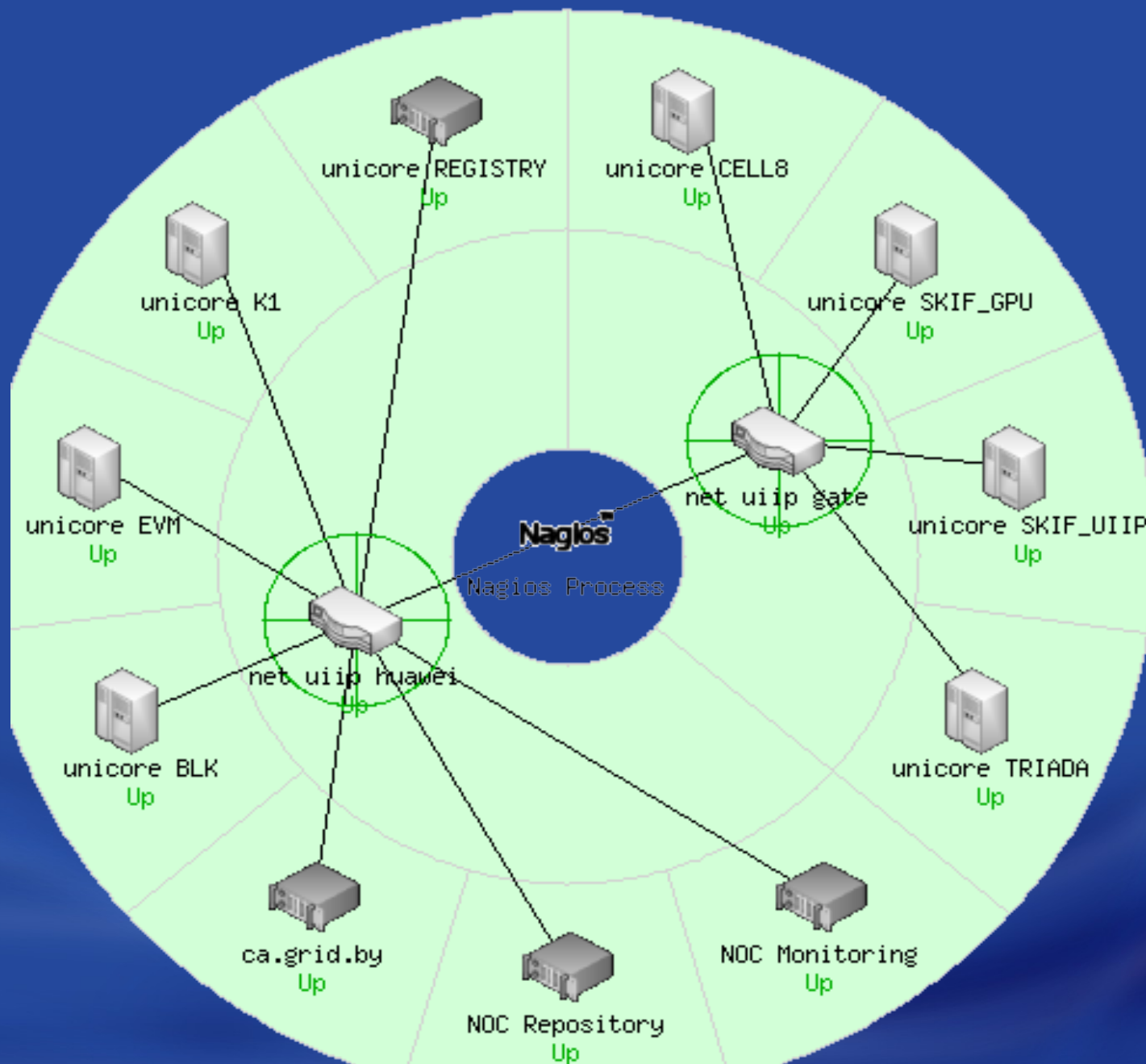
Грид (англ. grid — решётка, сеть) — согласованная, открытая и стандартизованная компьютерная среда, которая обеспечивает гибкое, безопасное, скоординированное разделение вычислительных ресурсов и ресурсов хранения информации, которые являются частью этой среды, в рамках одной виртуальной организации.

«Шланговый кластер» (жарг.) - кластер, собранный без применения спецтехнологий.

# Запуск задачи пользователя на GRID-сайте



# Национальный сегмент GRID



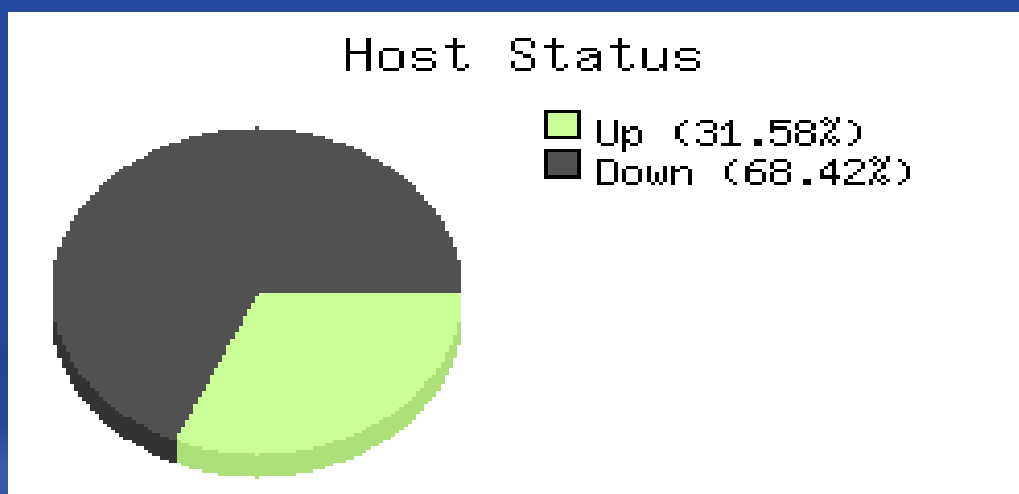
# Кластер БГУИР ЭВМ: немного статистики

При запуске хостов только одной лаборатории:

CPU Total: 42

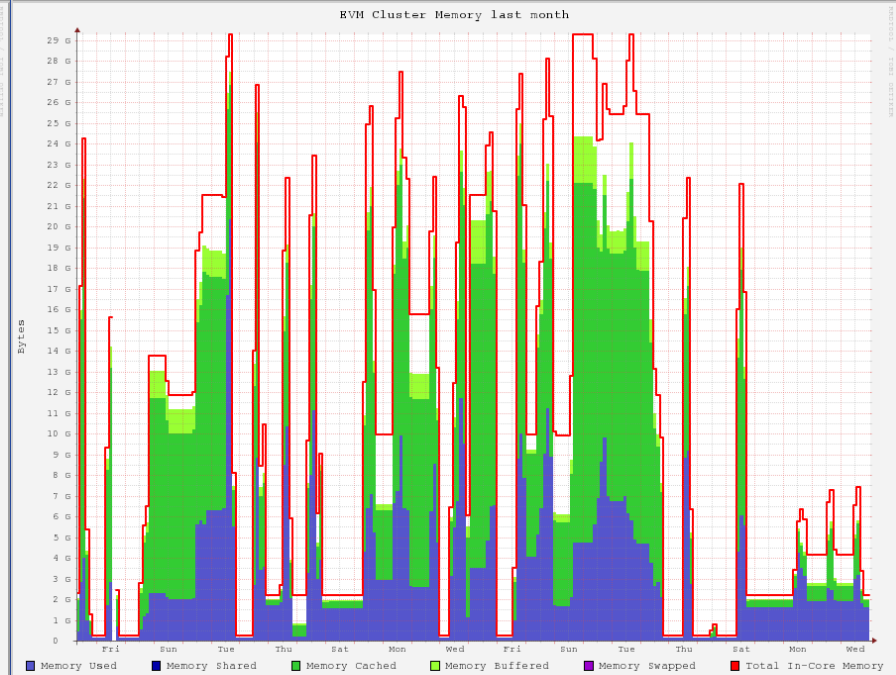
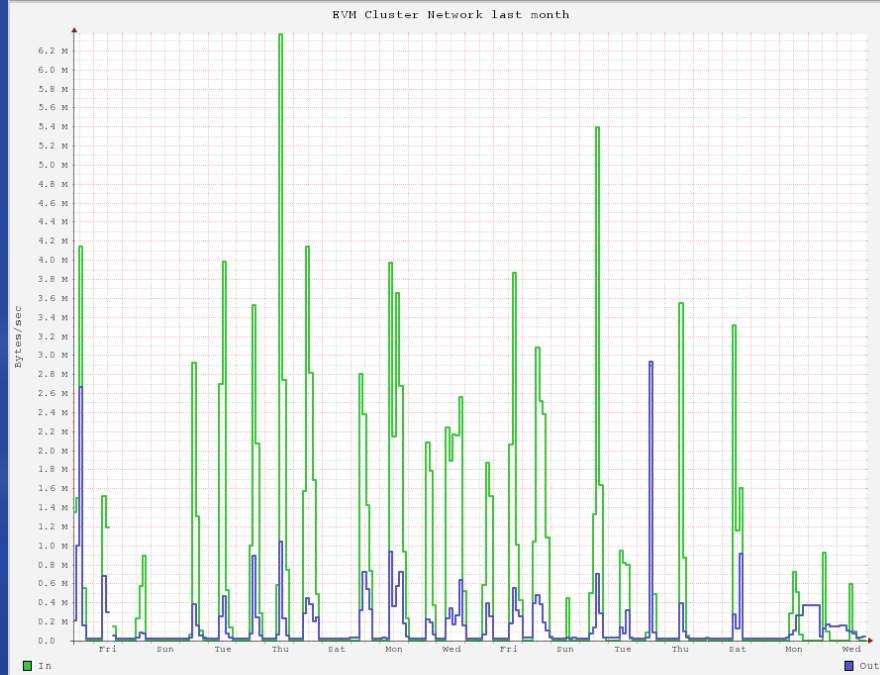
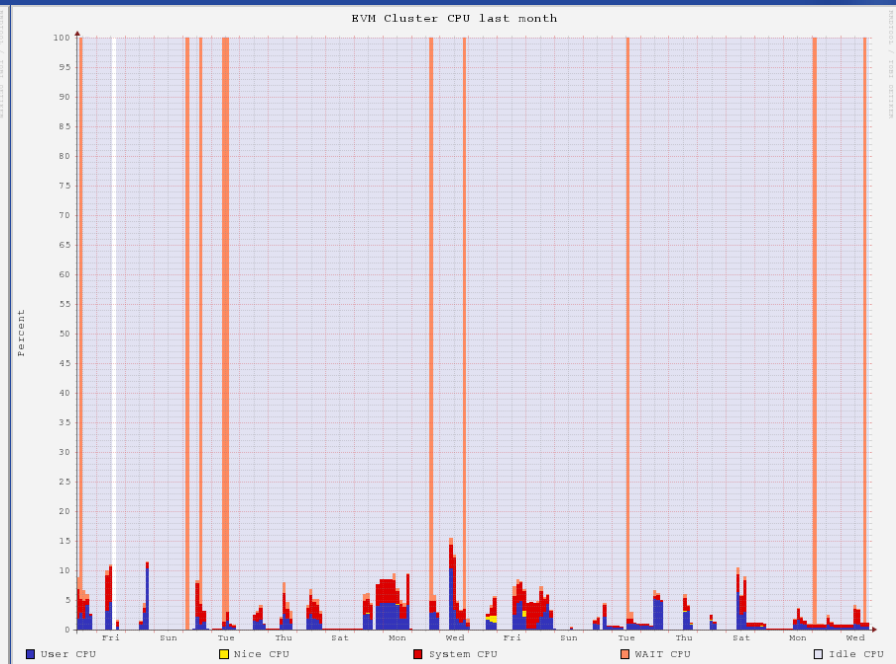
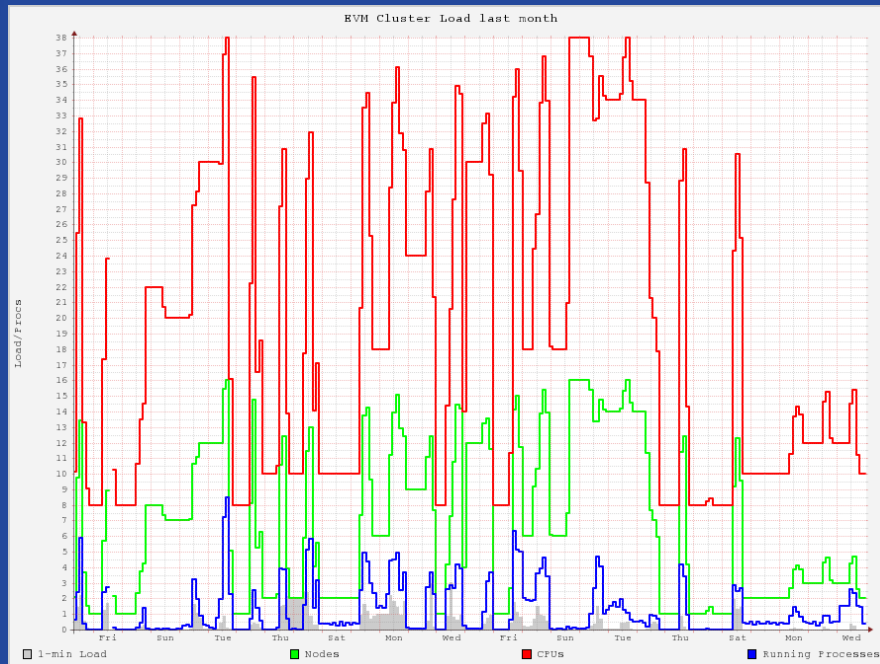
Hosts up: 12

Hosts down: 26





# Кластер БГУИР ЭВМ: немного графиков



# Терминология

Linux Containers (LXC) — виртуализация на уровне операционной системы для запуска нескольких изолированных «контейнеров» на одном физическом хосте.

LXC — это не виртуальная машина!

С помощью LXC можно создавать и управлять виртуальным окружением, с отдельным пространством имен для процессов и сети. Очень похоже на chroot, но дает намного большую изоляцию.



# Linux Control Groups

Изоляция файловой системы

Ограничение подсистемы ввода/вывода

Управление ресурсами памяти

Управление ресурсами процессора

Изоляция сетевой подсистемы

# Linux Kernel

## Control Group support

1. Namespace cgroup subsystem
2. Freezer cgroup subsystem
3. Cpuset support
4. Simple CPU accounting cgroup subsystem
5. Resource counters
6. Group CPU scheduler

## Namespaces support

1. UTS namespace
2. IPC namespace
3. User namespace
4. PID namespace
5. Network namespace

## Security options

File POSIX Capabilities

## Device Drivers

Network device support

Virtual ethernet pair device

# LXC — набор утилит

lxc-create  
lxc-destroy  
lxc-start  
lxc-stop  
lxc-checkpoint  
lxc-freeze  
lxc-unfreeze  
lxc-console  
lxc-execute  
lxc-cgroup  
lxc-setcap

# Кластер БГУИР ЭВМ: особенности

Узлы кластера = рабочие станции студентов

Бездисковая загрузка

Stateless

# Варианты изоляции задачи в LXC

Отдельный контейнер LXC, который запускается при запуске хоста.

Создание контейнера LXC на лету для каждой отдельной задачи.

# Отдельный контейнер LXC

## Плюсы:

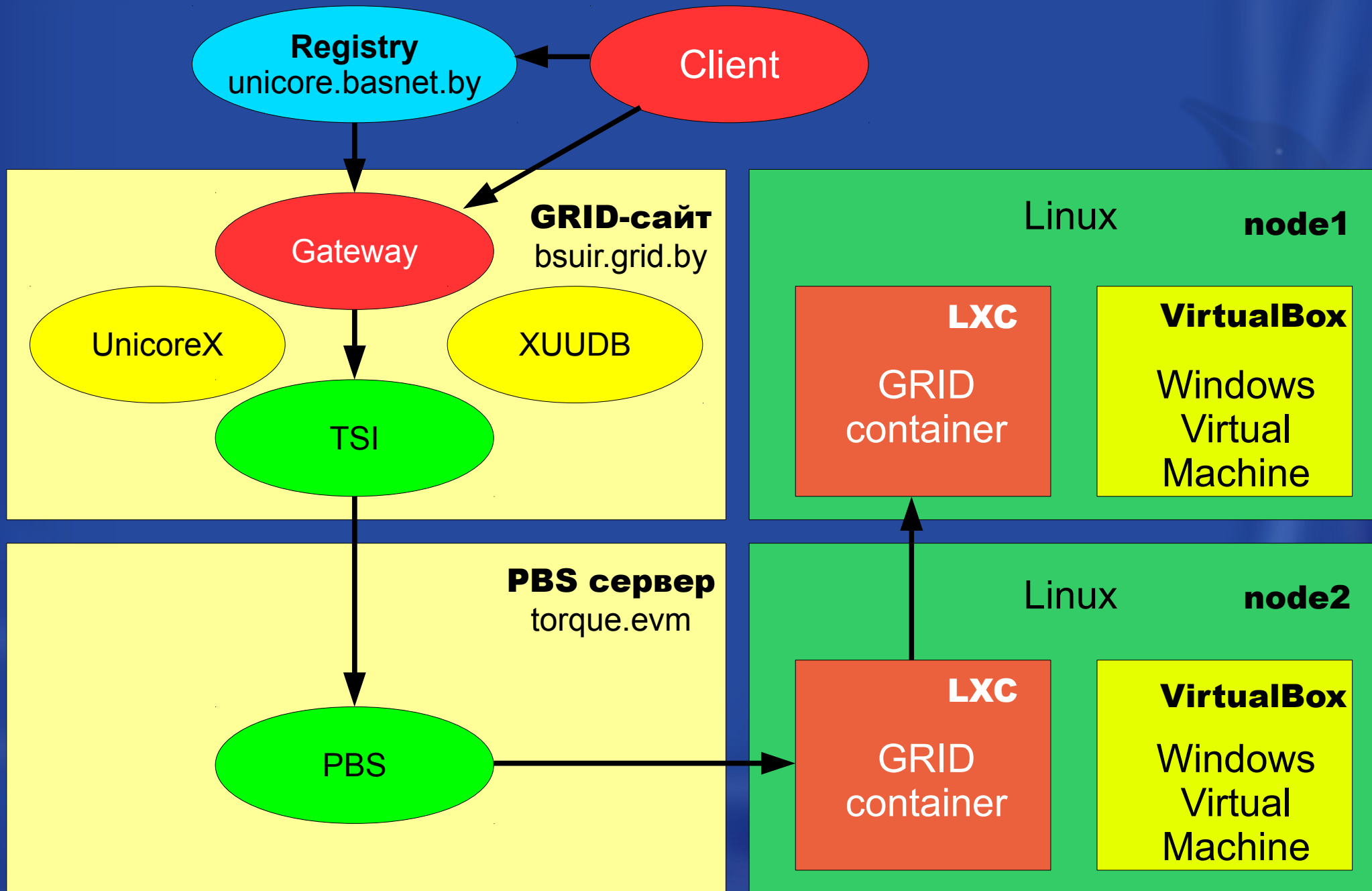
- выделенная вычислительная сеть
- отдельный контейнер для кластерного ПО

## Минус:

- нет изоляции по отдельным задачам



# Запуск GRID-задачи в контейнере



# Конфигурация контейнера

1. ФС контейнера в формате squashfs переводится в режим записи с помощью aufs.
2. Модификация конфигурации sshd для запуска на 222 порту.
3. Модификация конфигурации ssh-клиента для работы с нестандартным портом по умолчанию.
4. Монтирование общих ресурсов.
5. Модификация файла inittab для запуска только 3-х сервисов, необходимых для GRID-задач.

# Результаты

GRID — задачи запускаются в том окружении, которое требуется по условиям вышестоящей организации.

Решена проблема потенциально опасных для кластера задач в безопасной и сильно ограниченной «песочнице».

Есть возможность запускать задачи от разных групп пользователей в различных операционных окружениях и/или предоставляя различные ресурсы.

**Спасибо за внимание!**

Пынькин Денис  
[denis.pynkin@bsuir.by](mailto:denis.pynkin@bsuir.by)