



OTUS

ОНЛАЙН-ОБРАЗОВАНИЕ

Онлайн-образование



Не забудьте включить запись!





Меня хорошо видно && слышно?

Ставьте +, если все хорошо
Напишите в чат, если есть проблемы

Правила вебинара



Активно участвуем



Задаем вопрос в чат или голосом



Off-topic обсуждаем в Slack #канал группы или #general



Вопросы вижу в чате, могу ответить не сразу



Виртуализация

Викирюк Павел

Системный инженер

Маршрут вебинара

Виртуализация



Технологии виртуализации



Proxmox

1 Понять, что такое виртуализация, различать виды виртуализации

2 Узнать о типах гипервизоров и различиях между ними

3 Узнать об основных механизмах и технологиях виртуализации

4

Познакомиться с системой виртуализации Proxmox

5

Понять принципы работы сети в виртуальном коммутаторе Proxmox

6

Познакомиться с механизмами кластеризации в Proxmox

СМЫСЛ | Зачем вам это уметь

1 Чтобы иметь возможность сделать выбор среди технологий и механизмов виртуализации

2 Чтобы представлять как развернуть и эксплуатировать виртуальную инфраструктуру

3 Чтобы понимать основные моменты при работе с системой Proxmox



Виртуализация: основы и назначение

Виртуализация: основы и назначение

Виртуализация — предоставление набора вычислительных ресурсов или их логического объединения, абстрагированное от аппаратной реализации, и обеспечивающее при этом логическую изоляцию друг от друга вычислительных процессов, выполняемых на одном физическом ресурсе

<https://ru.wikipedia.org/wiki/Виртуализация>

Виртуализация: основы и назначение

Основные термины:

Хост (хост-машина) - физический сервер, ресурсы которого используются, чтобы развернуть несколько независимых друг от друга виртуальных сред

Гипервизор (англ. hypervisor) — программа, которая обеспечивает одновременное, параллельное выполнение нескольких операционных систем на одном и том же хост-компьютере

Виртуальная машина (гостевая система) - эмуляция аппаратного обеспечения некоторой платформы, которая использует ресурсы **хост-машины** и работает по управлению **гипервизора**

The image features a blue-toned aerial view of a city skyline, likely New York City, with numerous skyscrapers. A semi-transparent blue band with a white network pattern of dots and lines runs horizontally across the middle of the image. The title text is centered within this band.

Типы гипервизоров

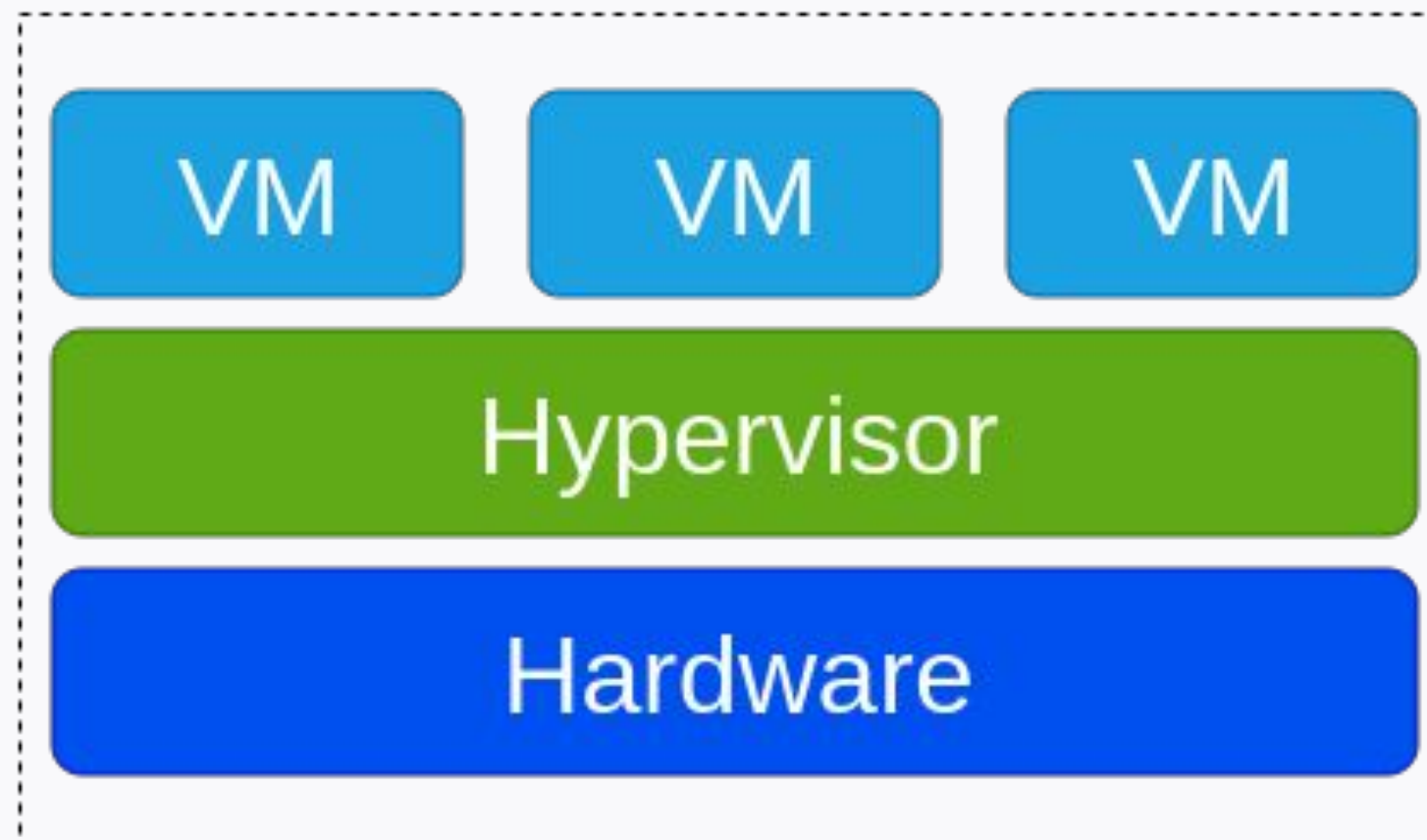


Вопрос к аудитории:

Какие типы гипервизоров вы знаете?

Типы гипервизоров

Гипервизоры первого типа (type 1)



Типы гипервизоров

Гипервизоры первого типа (type 1)

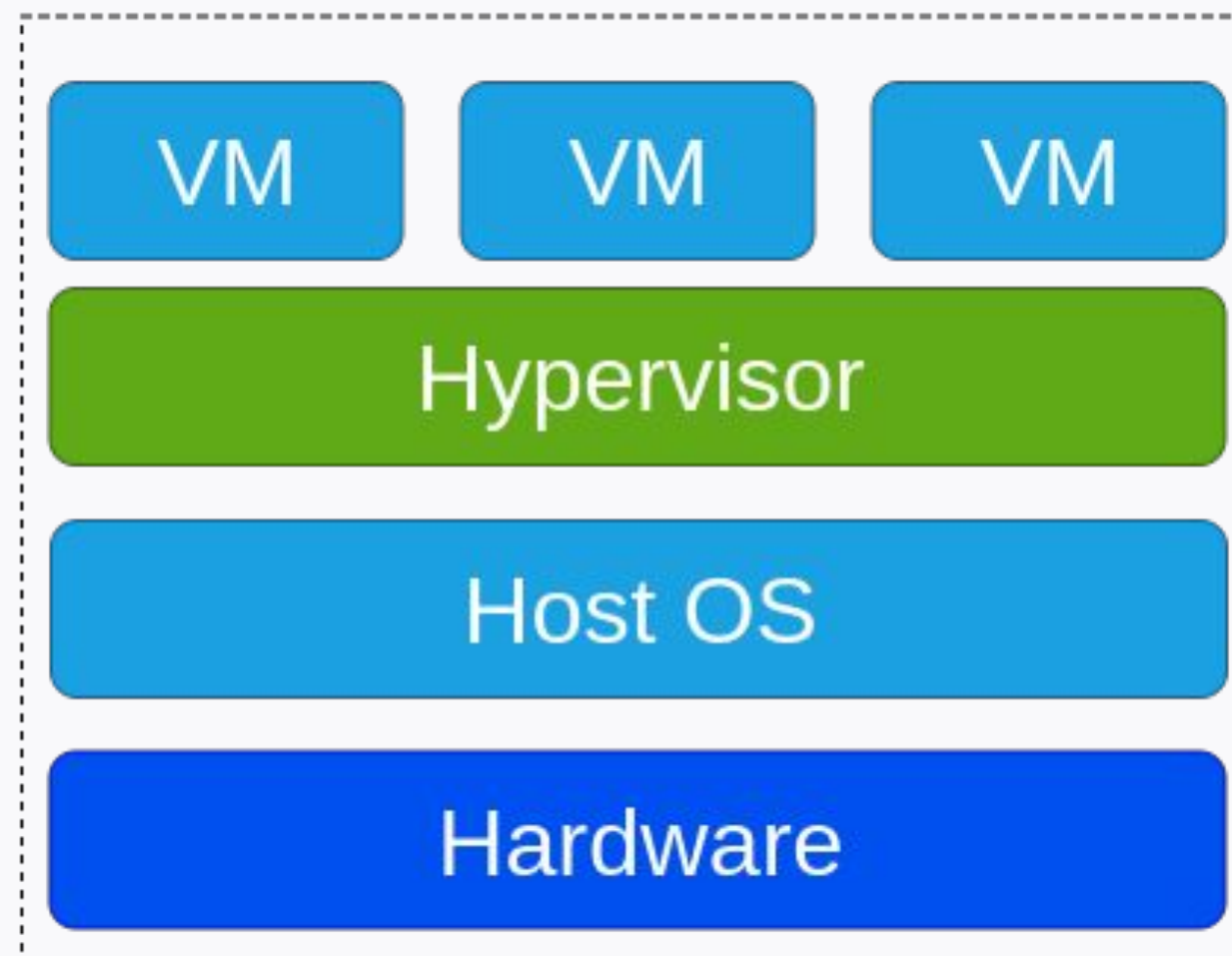
- **запускается непосредственно на железе**
- является компактной ОС (“тонкий гипервизор”)
- размер кода в тонком гипервизоре на два порядка меньше обычной ОС
- управляет набором ресурсов хост-машины
- обладает механизмами безопасности

Примеры продуктов:

- Xen
- VMware ESXi
- Hyper-V

Типы гипервизоров

Гипервизоры второго типа (type 2)



Типы гипервизоров

Гипервизоры второго типа (type 2)

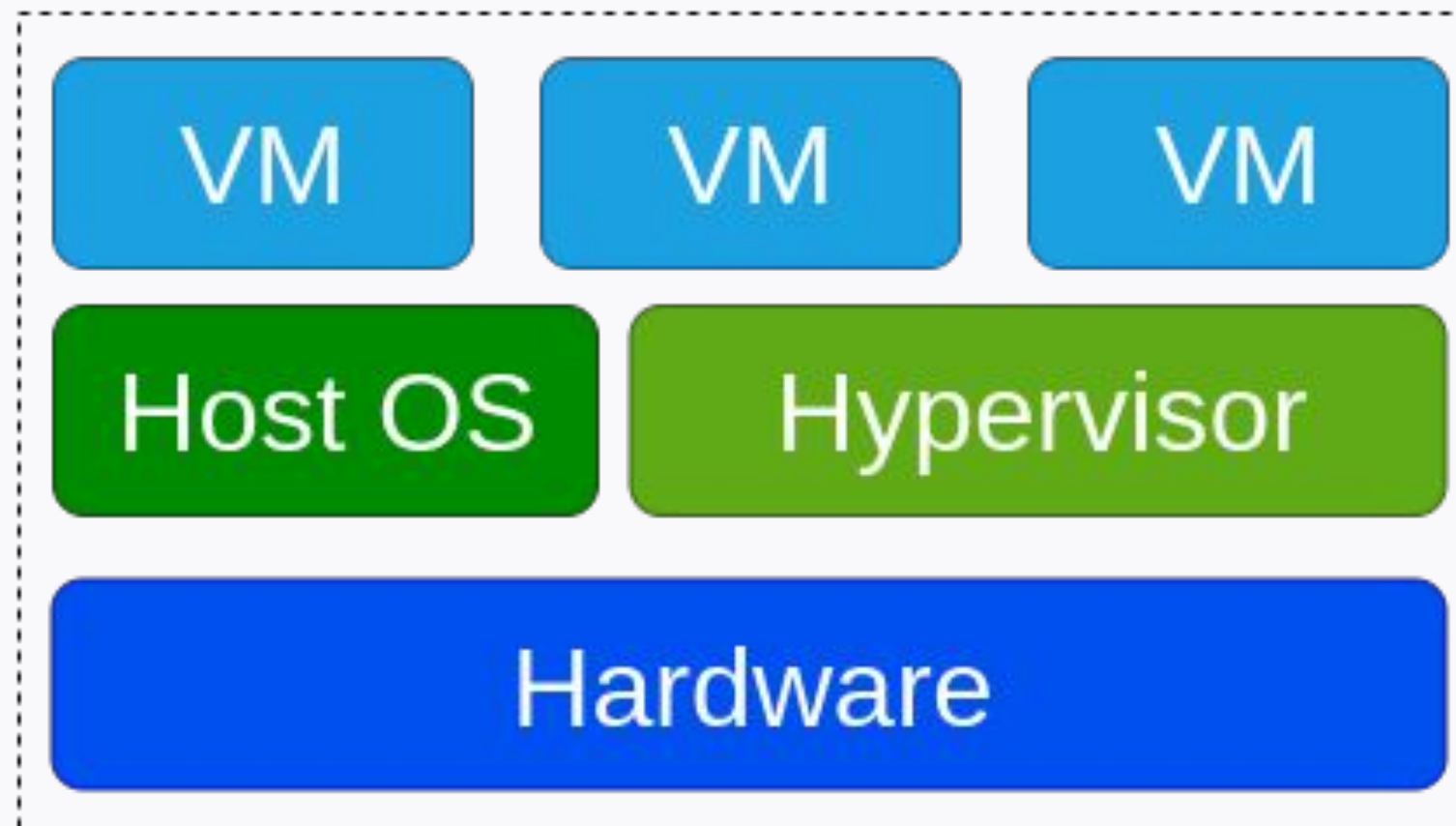
- **запускается поверх ОС хост-машины**
- является программным слоем поверх ОС
- управляет гостевыми ОС
- эмуляцией и управлением физическими ресурсами в этом случае занимается ОС хост-машины
- обладает механизмами безопасности

Примеры продуктов:

- KVM
- VMware Workstation
- Hyper-V
- Oracle Virtualbox
- Proxmox

Типы гипервизоров

Гибридные гипервизоры (type 1+)



Типы гипервизоров

Гибридные гипервизоры (type 1+)

- тонкий гипервизор контролирует процессор и память и управляет служебной ОС
- служебная ОС управляет доступом гостевых систем к физическому оборудованию

Примеры продуктов:

- Xen
- Hyper-V
- VMware Workstation

The image features a central horizontal band with a blue-to-green gradient. Overlaid on this band is a network of white lines connecting various points, resembling a data or communication network. The background of the entire image is an aerial view of a city skyline, with numerous skyscrapers and buildings. The color palette is dominated by shades of blue and green, giving it a technological and urban feel.

Ваши вопросы?

Маршрут вебинара

Виртуализация



Технологии виртуализации



Proxmox



Технологии виртуализации



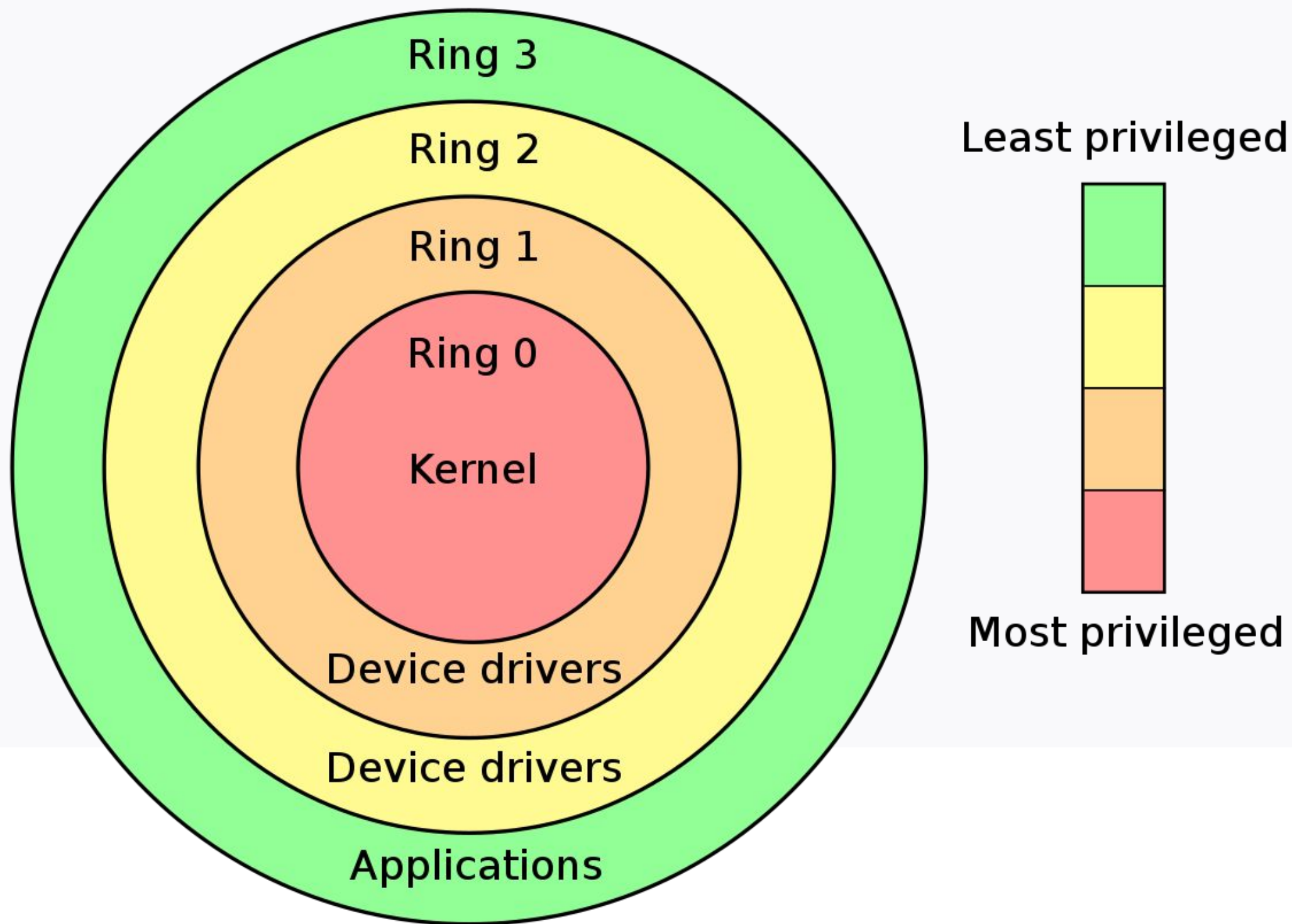
An aerial view of a city skyline, likely New York City, with a blue overlay and a network pattern of lines and dots. The text is overlaid on this image.

Вопрос к аудитории:

**Какие технологии виртуализации
вы знаете?**

Технологии виртуализации

Кольца защиты



Технологии виртуализации

Кольца защиты

- концепция изначально появилась в ОС Multics для мейнфрейма GE645 (1967 года) с частично программной реализацией, и полностью аппаратной уже в 1970 году в системе Honeywell 6180
- в первом кольце, работают менее важные процессы, как например драйверы устройств
- в самом последнем кольце работают пользовательские приложения
- изначально колец защиты было 8
- в данный момент используются только 4
- основной принцип: изнутри наружу **можно**, снаружи внутрь **нельзя**

Технологии виртуализации

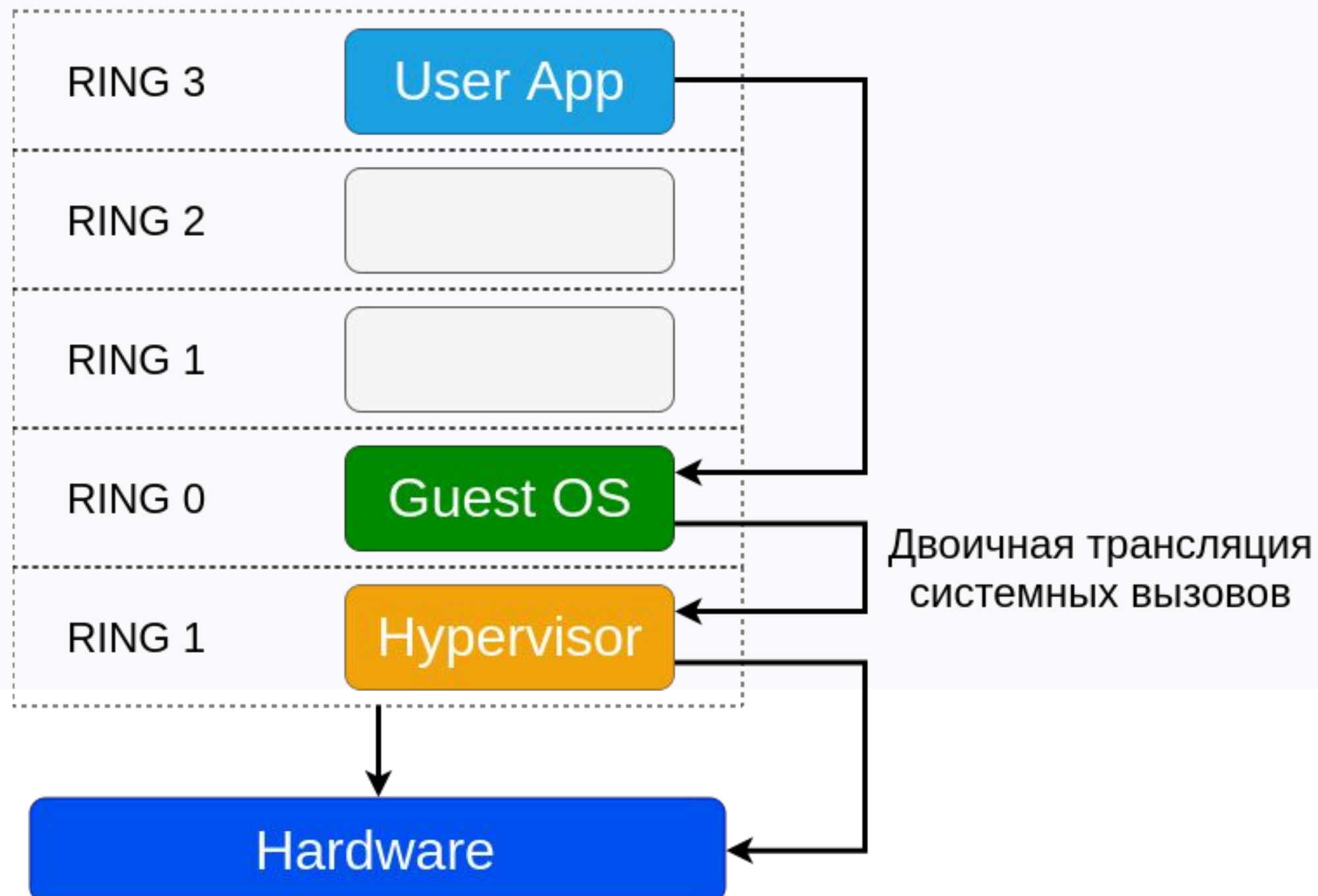
Полная виртуализация (full virtualization)

- полная симуляция базового оборудования
- гостевая ОС не подозревает о запуске в виртуальной среде
- полная изоляция гостевых ОС
- обеспечивает запуск любой ОС на любом процессоре
- упрощает разработку платформ виртуализации
- требует дополнительных технологий (Intel VT-x, AMD-V)
- возможное увеличение быстродействия платформы
- накладные расходы на эмуляцию оборудования

Технологии виртуализации

Типы полной виртуализации:

Software assisted - Full Virtualization (BT - Binary Translation)



Технологии виртуализации

Типы полной виртуализации:

Software assisted - Full Virtualization (BT - Binary Translation)

- эмулирует оборудование, используя программный набор инструкций
- из-за двоичной трансляции Software assisted часто критикуют за проблемы с производительностью

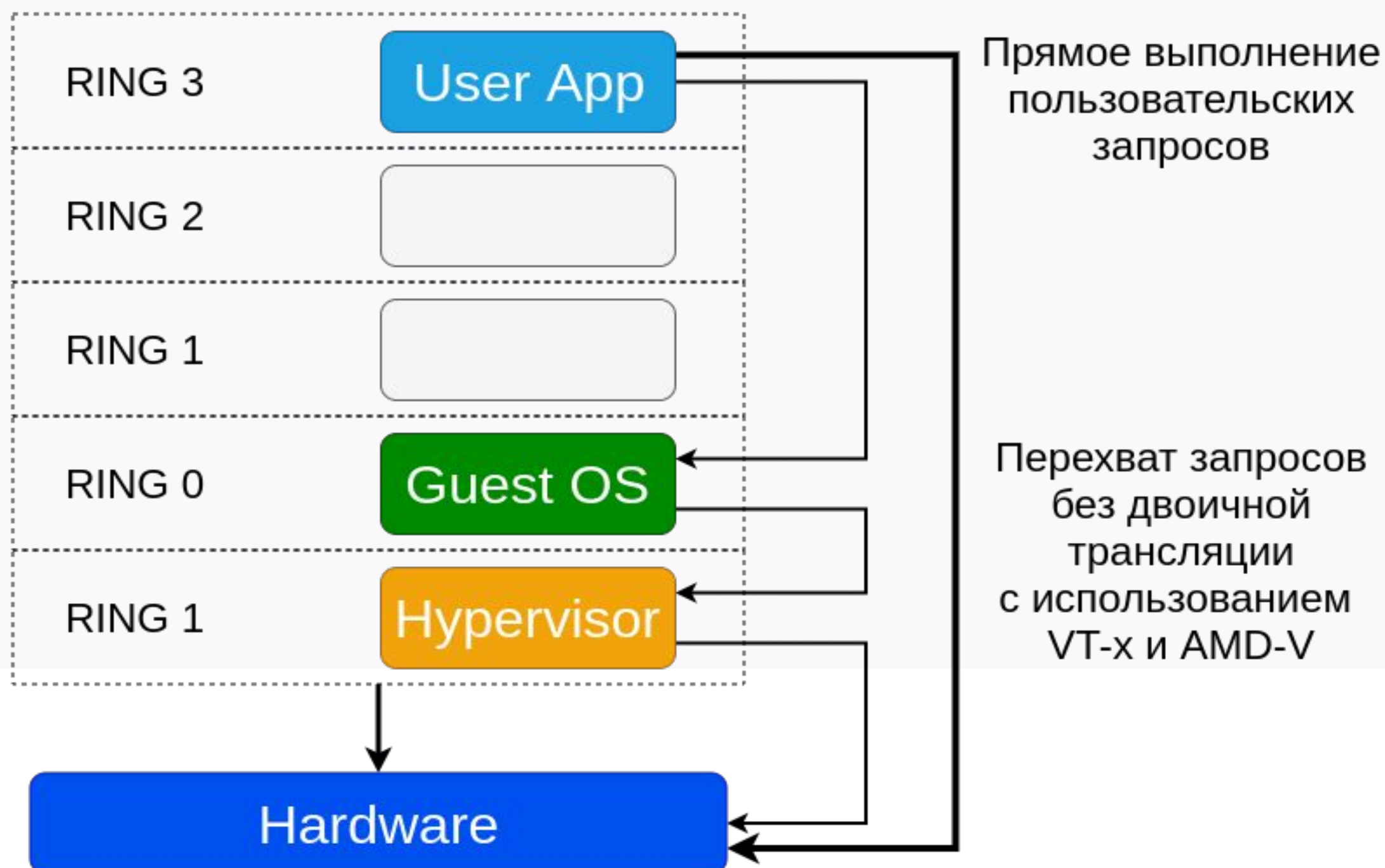
Примеры продуктов:

- VMware workstation (для 32х гостевых ОС)
- Virtual PC
- VirtualBox (для 32х гостевых ОС)
- VMware Server

Технологии виртуализации

Типы полной виртуализации:

Hardware-Assisted – Full Virtualization (VT)



Технологии виртуализации

Типы полной виртуализации:

Hardware-Assisted – Full Virtualization (VT)

- устраняет двоичную трансляцию и напрямую работает с оборудованием
- использует для работы технологии Intel VT-x и AMD-V

Примеры продуктов:

- VMware ESXi
- KVM
- Hyper-V
- Xen

Технологии виртуализации

Типы полной виртуализации:

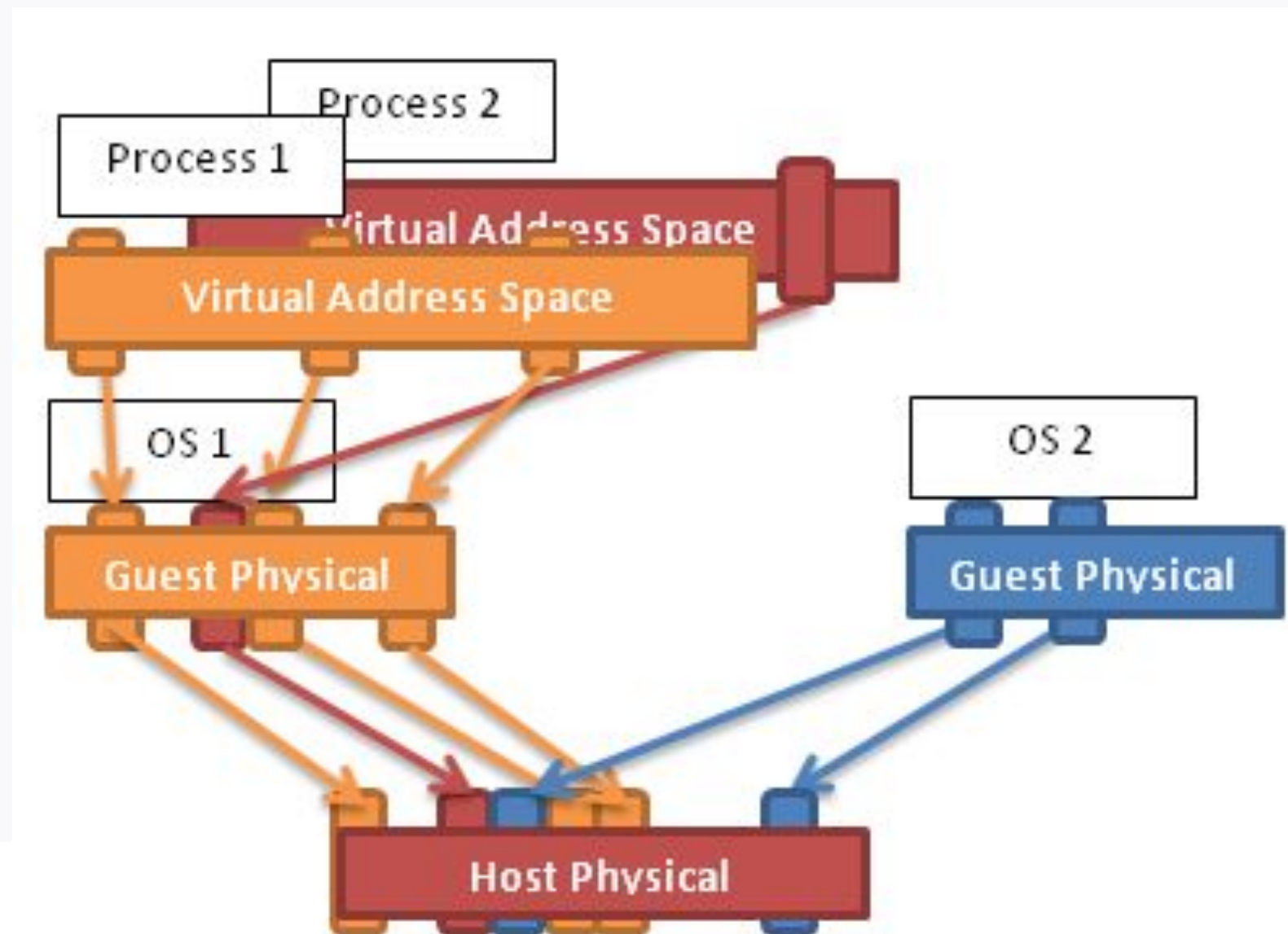
SLAT (англ. Second Level Address Translation), также известный как вложенный пейджинг, представляет собой технологию виртуализации с аппаратным обеспечением, которая позволяет избежать накладных расходов, связанных с управляемыми программным обеспечением таблицами теневых страниц.

- версия технологии в процессорах Intel называется **EPT (Extended Page Tables)**, версия в процессорах AMD - **RVI (Rapid Virtualization Indexing)**
- повышает производительность работы с памятью гостевых систем за счет устранения трансляции адресов памяти

Технологии виртуализации

Типы полной виртуализации:

SLAT (англ. **Second Level Address Translation**)



Технологии виртуализации

Типы полной виртуализации:

SLAT (англ. **Second Level Address Translation**)

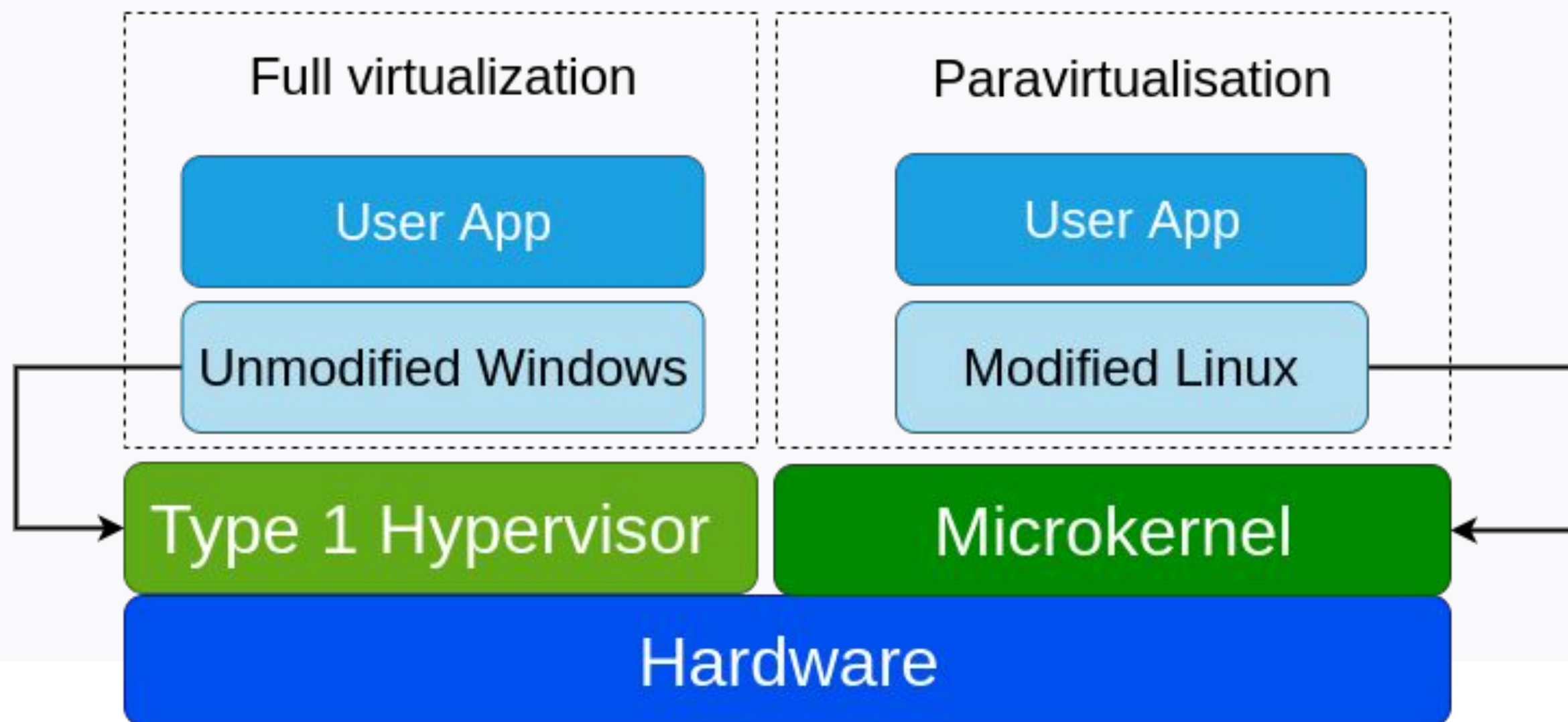
Поддержка гипервизорами:

- Hyper-V для Windows Server 2008 R2, Windows 8 и выше
- KVM, начиная с версии 2.6.26 ядра Linux
- Parallels Desktop для Mac, начиная с версии
- VirtualBox, начиная с версии 2.0.0
- VMware ESX, начиная с версии 3.5
- Xen, начиная с версии 3.2.0

Технологии виртуализации

Паравиртуализация:

Paravirtualization



Технологии виртуализации

Паравиртуализация:

Paravirtualization

- используется модификация ядра гостевой ОС для взаимодействия с гипервизором через API-интерфейс
- взаимодействие с оборудованием происходит с использованием драйверов
- более высокая производительность

Примеры продуктов:

- Xen
- KVM
- Oracle VM

The image features a central horizontal band with a blue-to-green gradient. Overlaid on this band is a network of white lines connecting various points, resembling a data or communication network. The background of the entire image is an aerial view of a city with numerous skyscrapers, rendered in a monochromatic blue and green color palette.

Ваши вопросы?



NUMA



An aerial view of a city skyline, likely New York City, with a blue overlay and a network pattern of lines and dots. The text is overlaid on this image.

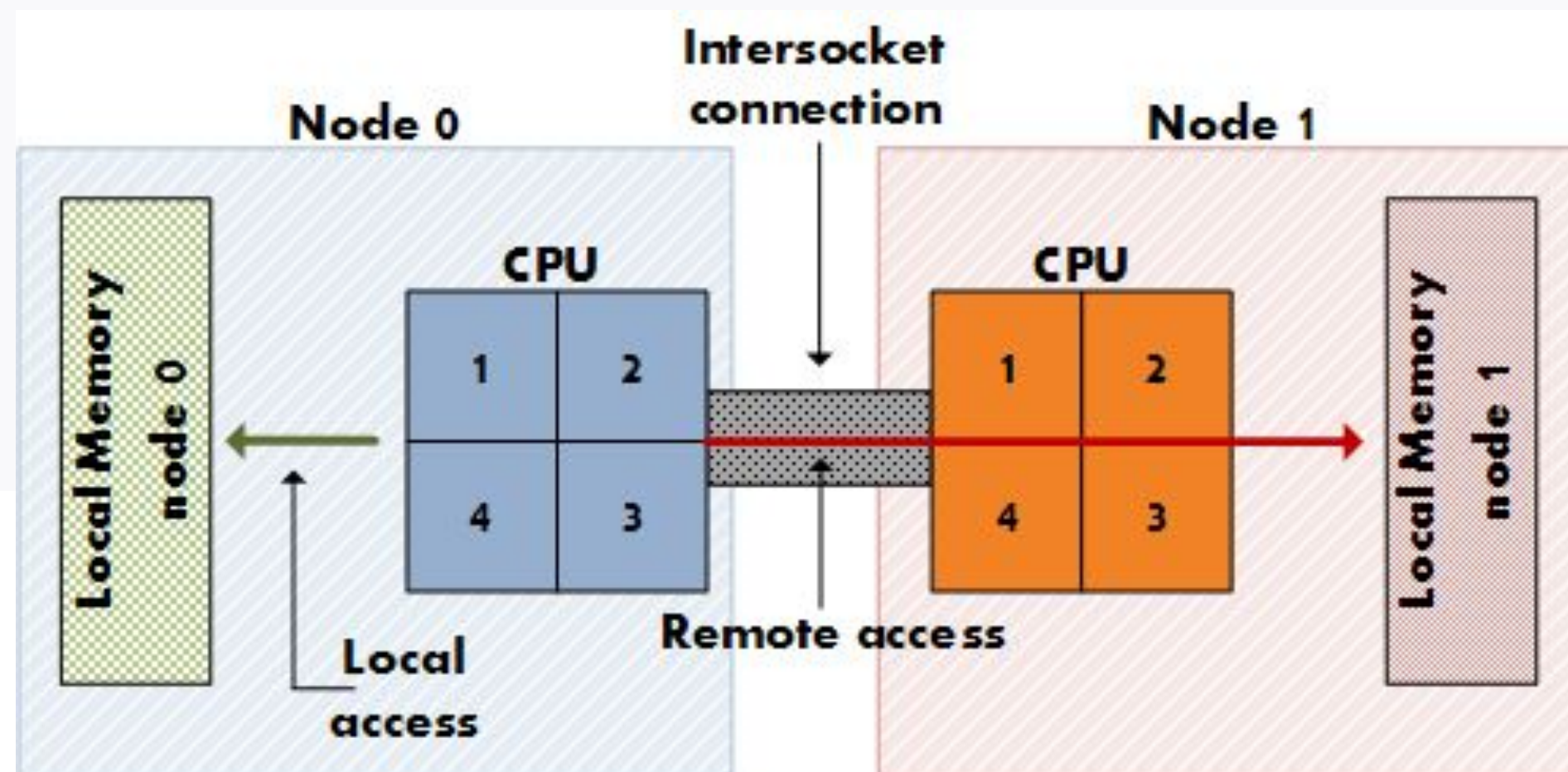
Вопрос к аудитории:

Знаком ли вам механизм NUMA?

NUMA

NUMA (Non-Uniform Memory Access) - или архитектура с **неравномерной памятью**) - схема реализации компьютерной памяти, используемая в мультипроцессорных системах, когда время доступа к памяти определяется её расположением по отношению к процессору

https://ru.wikipedia.org/wiki/Non-Uniform_Memory_Access



NUMA (Non-Uniform Memory Access)

Особенности архитектуры:

- имеет смысл **только** для мультипроцессорных систем
- у каждого процессора есть “локальная” память
- процессор и подключенная к нему память объединяются в узел NUMA
- приоритетно ОС обращается к “локальной” памяти, но может обращаться к “удаленной” с помощью **QPI (QuickPath Interconnect)** шины
- производительность обращений напрямую зависит от расположения памяти относительно процессора

NUMA

NUMA (Non-Uniform Memory Access)

Контроль и настройка обращений:

С помощью пакета `numactl`

Просмотр статистики обращений к нодам NUMA в системе

```
numastat -c qemu-kvm
```

NUMA

NUMA (Non-Uniform Memory Access)

Контроль и настройка обращений:

С помощью пакета **numactl**

Просмотр статистики обращений к нодам NUMA в системе

```
numastat -c qemu-kvm
```

Пример привязки виртуальной машины к конкретной NUMA ноде

```
numactl --membind=0 qemu-kvm -name testvm1 -m 4096 -smp 4 -drive  
file=/var/lib/libvirt/images/testvm1.qcow,if=virtio,media=disk -vnc :5  
-monitor stdio
```

The image features a central horizontal band with a blue-to-green gradient. Overlaid on this band is a network of white lines connecting various points, resembling a data or communication network. The background of the entire image is an aerial view of a city skyline, with numerous skyscrapers and buildings. The color palette is dominated by shades of blue and green, giving it a technological and urban feel.

Ваши вопросы?



libvirt

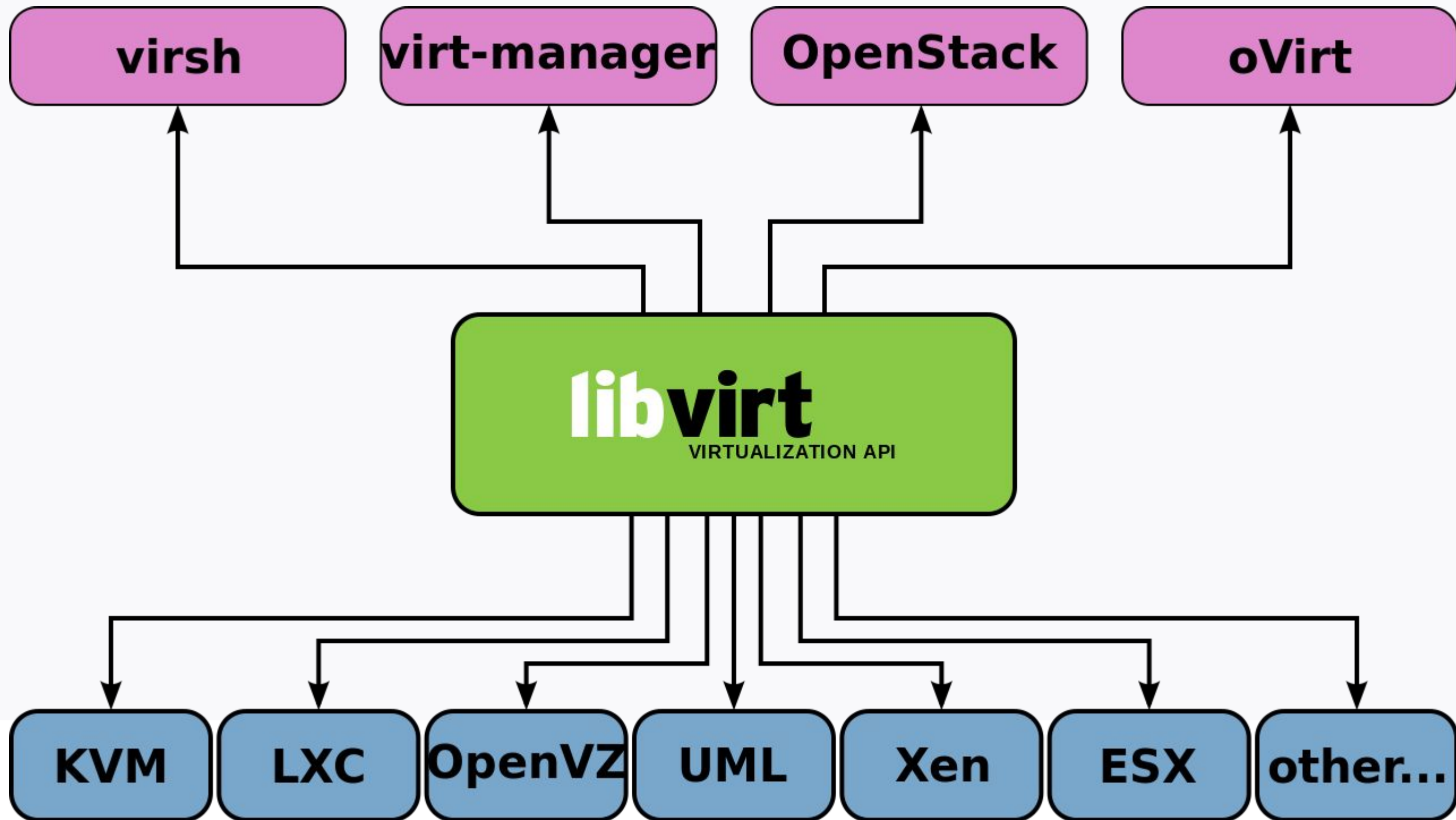


An aerial view of a city skyline, likely New York City, with a blue overlay and a network pattern of dots and lines. The text is overlaid on this image.

Вопрос к аудитории:

Что такое libvirt и для чего он?

libvirt



libvirt - это демон и API, с помощью которого пользовательские интерфейсы осуществляют управление гипервизорами

Поддерживаемые гипервизоры:

- LXC
- OpenVZ
- QEMU (KVM)
- Xen
- VirtualBox
- VMware ESXi, VMware Workstation, VMware Player
- Hyper-V

libvirt - это демон и API, с помощью которого пользовательские интерфейсы осуществляют управление гипервизорами

Поддерживаемые пользовательские интерфейсы:

- virsh
- virt-manager
- oVirt
- mist.io

libvirt - это демон и API, с помощью которого пользовательские интерфейсы осуществляют управление гипервизорами

Особенности:

- создание, редактирование, запуск и остановка виртуальных машин
- просмотр статистики и производительности
- управление как локальным, так и удаленными гипервизорами

The image features a central horizontal band with a blue-to-green gradient. Overlaid on this band is a network of white lines connecting various points, resembling a data or communication network. The background of the entire image is an aerial view of a city skyline, with numerous skyscrapers and buildings. The color palette is dominated by shades of blue and green, giving it a modern, technological feel.

Ваши вопросы?

The image features a blue-tinted aerial view of a city skyline, likely New York City, with numerous skyscrapers. A semi-transparent blue band with a white network diagram pattern (nodes and connecting lines) runs horizontally across the middle of the image. The text "Nested virtualization" is centered within this band in a white, sans-serif font.

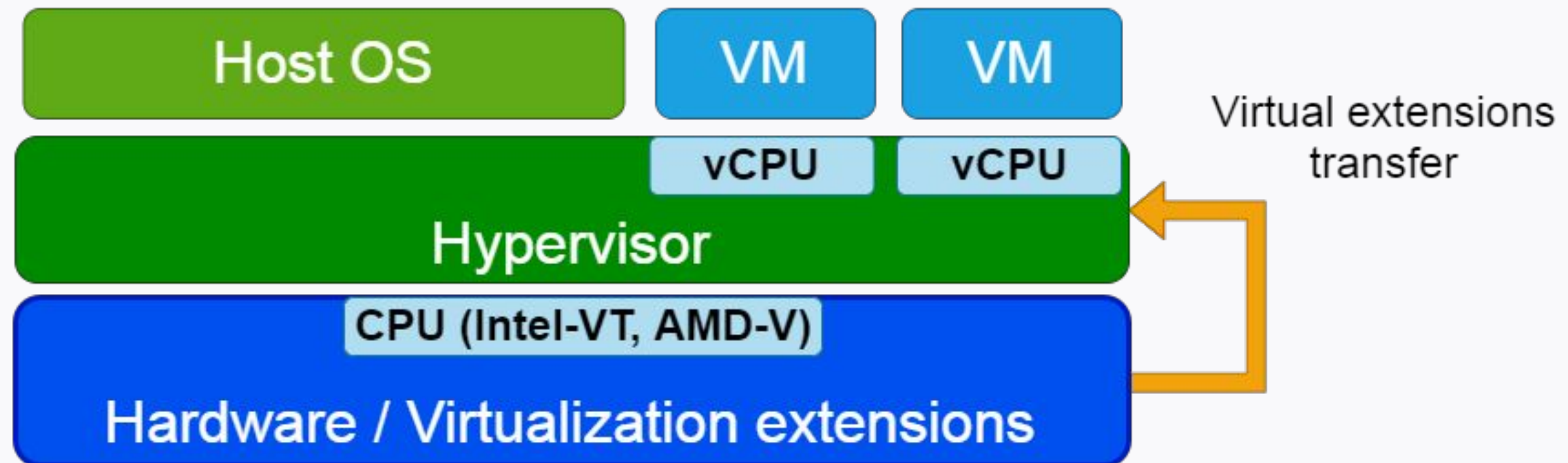
Nested virtualization



Вопрос к аудитории:

**Наступали ли вы на грабли с
вложенной виртуализацией?**

Nested virtualization



Nested virtualization

Nested virtualization - вложенная виртуализация. По сути возможность запуска гипервизора с поддержкой аппаратной виртуализации в виртуальной среде

Особенности:

- передача инструкций аппаратного процессора виртуальным процессорам гостевых систем
- требуется поддержка этого режима гипервизором
- потенциально низкая производительность и стабильность

Спектр применения:

- тестовые и лабораторные стенды
- продакшн-среда облачного хостинг-провайдера

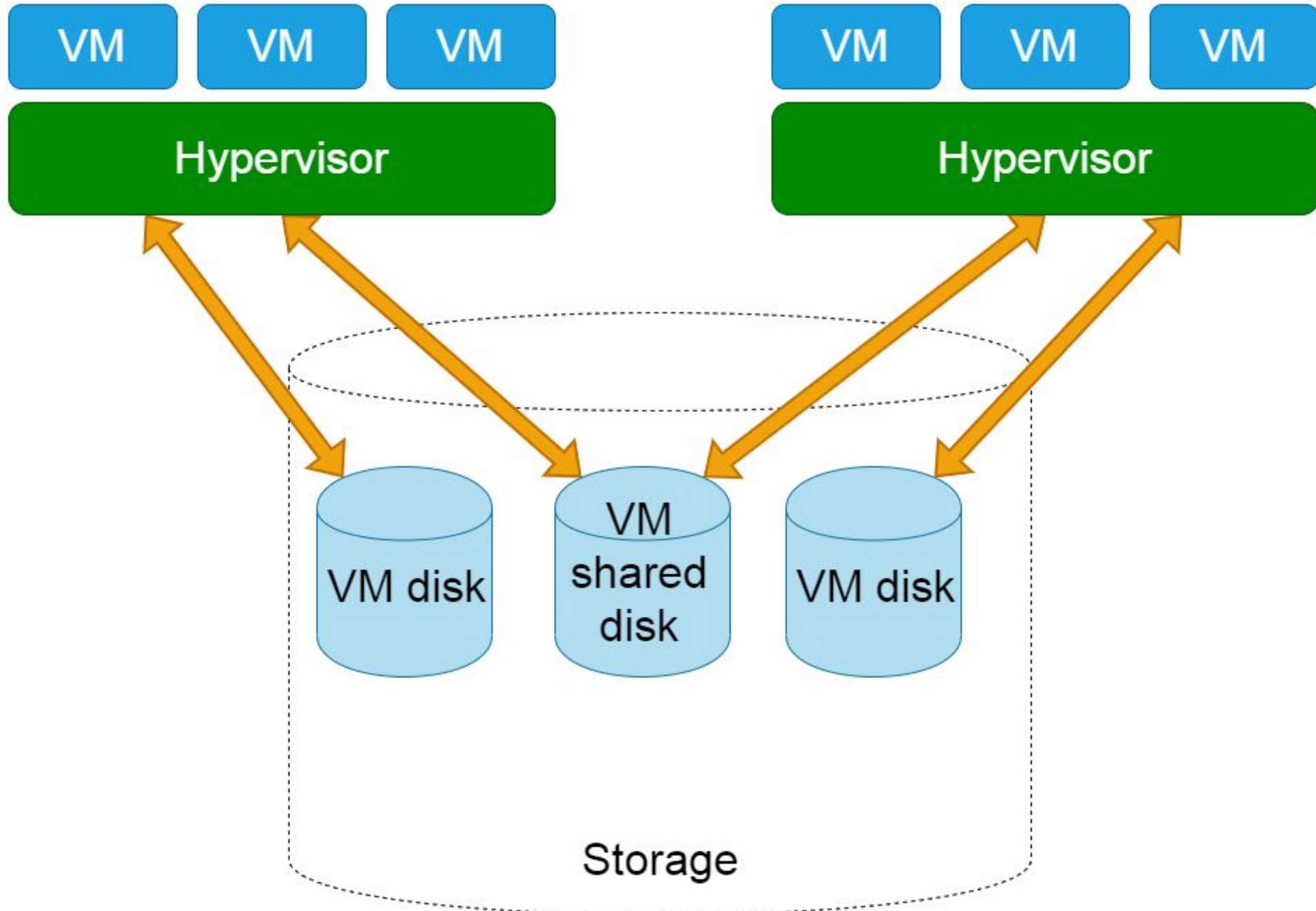
The image features a central banner with a blue-to-green gradient background. Overlaid on this banner is a faint, light-colored network of interconnected nodes and lines, resembling a digital or data network. The text "Ваши вопросы?" is centered in a large, white, bold font. The background of the entire image is an aerial view of a city skyline, with various skyscrapers and buildings, rendered in a monochromatic blue and green color palette.

Ваши вопросы?

The image features a blue-tinted aerial view of a city skyline, likely New York City, with numerous skyscrapers. A semi-transparent blue band with a white network pattern of dots and lines runs horizontally across the middle of the image. The text "Shared disk" is centered within this band in a white, sans-serif font.

Shared disk

Shared disk



Shared disk

Shared disk - это диск виртуальной машины, который располагается в общем хранилище (**storage**) и допускает одновременную запись (или чтение) на него сразу нескольких виртуальных машин

Технология **shared disk** применяется для развертывания отказоустойчивых кластеров

Например в гипервизорах **VMware ESXi** эта технология называется **Multi-writer**

libvirt в свою очередь тоже позволяет добавить флаг **<shareable/>** в конфигурацию виртуальной машины, который определяет возможность записи на диск этой машины другими виртуальными машинами

Shared disk

Технологии **shared disk** накладывают определенные ограничения, например:

- отсутствие возможности онлайн-миграции виртуальной машины между гипервизорами
- обязательное наличие кластерной файловой системы с автоматической синхронизацией (GFS или OCFS)
- отсутствие возможности расширить объем диска без выключения виртуальной машины

The image features a central horizontal band with a blue-to-green gradient. Overlaid on this band is a network of white lines connecting various points, resembling a data or communication network. The background of the entire image is an aerial view of a city with numerous skyscrapers, tinted in shades of blue and green.

Ваши вопросы?



Templates



Templates

Template (шаблон) - полностью подготовленный образ операционной системы, который можно использовать для развертывания виртуальных машин

- создать шаблон можно с помощью клонирования уже развернутых виртуальных машин
- скорость развертывания виртуальных машин из шаблонов характеризуется разработчиками Proxmox термином "молниеносно", то есть очевидно очень высокая
- нельзя создать шаблон из виртуальной машины, диск которой содержит **снапшоты**

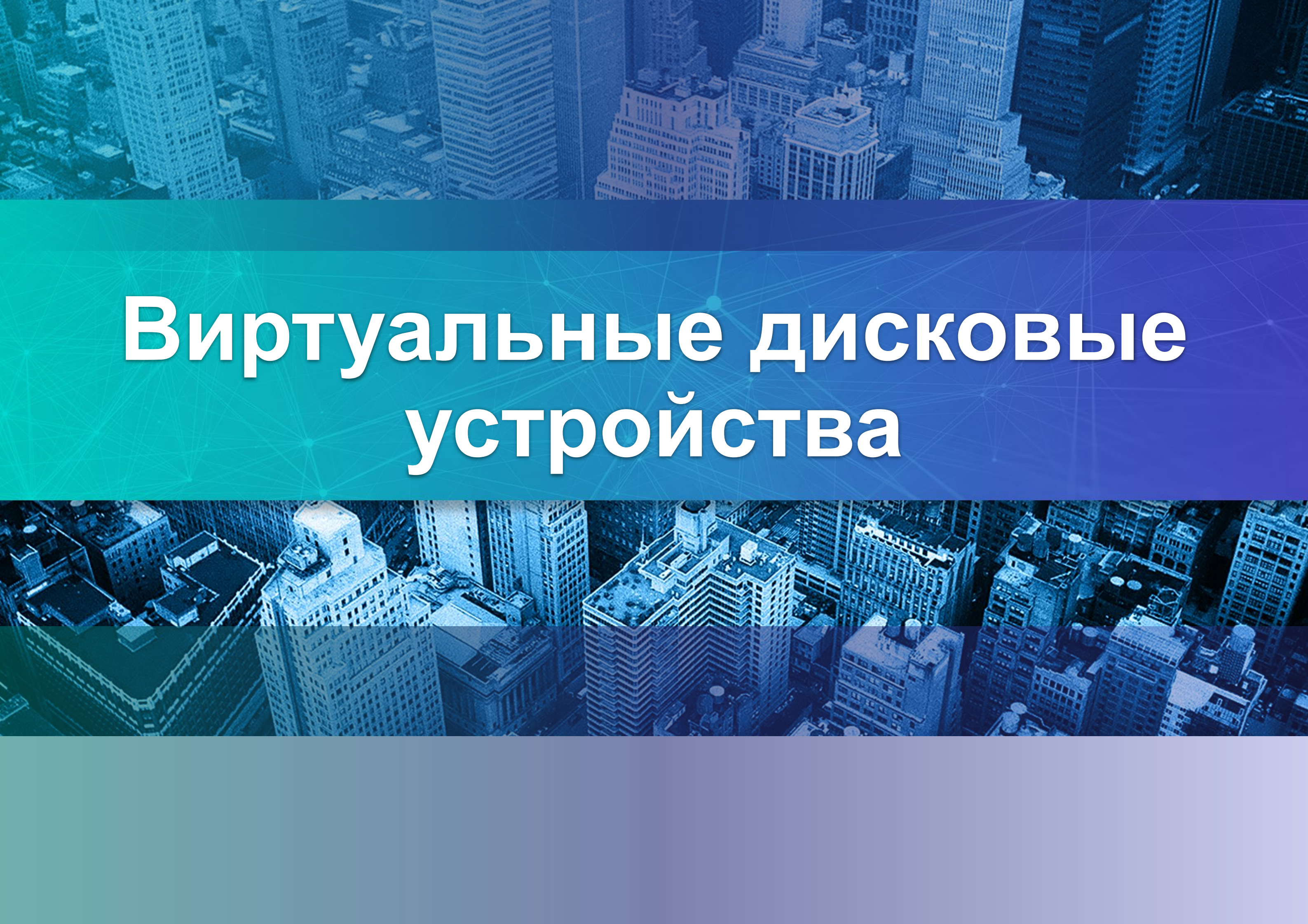
Виды клонов виртуальных машин в Proxmox:

Linked Clone - линкованный клон виртуальной машины, требует меньше дискового пространства, но не может быть запущен без доступа к базовому шаблону, из которого был создан

Full Clone - полный клон виртуальной машины, это полностью независимая копия виртуальной машины, которая занимает аналогичный объем дискового пространства

The image features a central horizontal band with a blue-to-green gradient. Overlaid on this band is a network of white lines connecting various points, resembling a data or communication network. The background of the entire image is an aerial view of a dense city skyline, with numerous skyscrapers and buildings. The color palette is dominated by shades of blue and green, giving it a technological and urban feel.

Ваши вопросы?

The image features a blue-tinted aerial view of a city skyline, likely New York City, with numerous skyscrapers. A semi-transparent blue band with a white network pattern of dots and lines runs horizontally across the middle of the image. The title text is centered within this band.

Виртуальные дисковые устройства

Виртуальные дисковые устройства

Основные форматы виртуальных дисков:

RAW

- наиболее быстрый формат
- универсальный, поддерживается многими гипервизорами
- можно нативно монтировать в среде ОС Linux
- занимает строго заданный объем дискового пространства в момент создания
- не поддерживает снапшоты
- позволяет легко переносить диски машин

Виртуальные дисковые устройства

Основные форматы виртуальных дисков:

QEMU image format (qcow2)

- занимает только тот объем, который занимают данные на виртуальном диске
- требует дополнительного драйвера для монтирования в среде ОС Linux
- поддерживает снапшоты
- производительность сравнительно более низкая (по сравнению с другими форматами дисков)
- позволяет легко переносить диски машин

Виртуальные дисковые устройства

Основные форматы виртуальных дисков:

LVM

- максимальная производительность
- снапшоты средствами LVM, упрощенные бэкапы
- меньшая гибкость дискового пространства
- усложняет процесс переноса дисков машин

Виртуальные дисковые устройства

Основные форматы виртуальных дисков:

LVM thin

- LVM выделяет дисковое пространство целиком при создании тома
- LVM thin вместо этого выделяет блоки по мере их записи

Виртуальные дисковые устройства

Основные форматы виртуальных дисков:

VMDK

- по своему структурному содержанию полностью отражает реальный диск
- является индексированным и документированным
- в основном используется в гипервизоре VMware ESXi
- поддерживается многими другими гипервизорами, например: QEMU, Proxmox, Virtualbox

Виртуальные дисковые устройства

Типы виртуальных дисков:

Thick Provision Lazy Zeroed

- при создании блоки **не очищаются** от данных, которые могли быть в этих блоках ранее
- все пространство диска сразу выделяется при его создании
- при первом обращении происходит очистка диска, что приводит к снижению производительности на первом этапе
- короткое время создания диска

Thick Provision Eager Zeroed

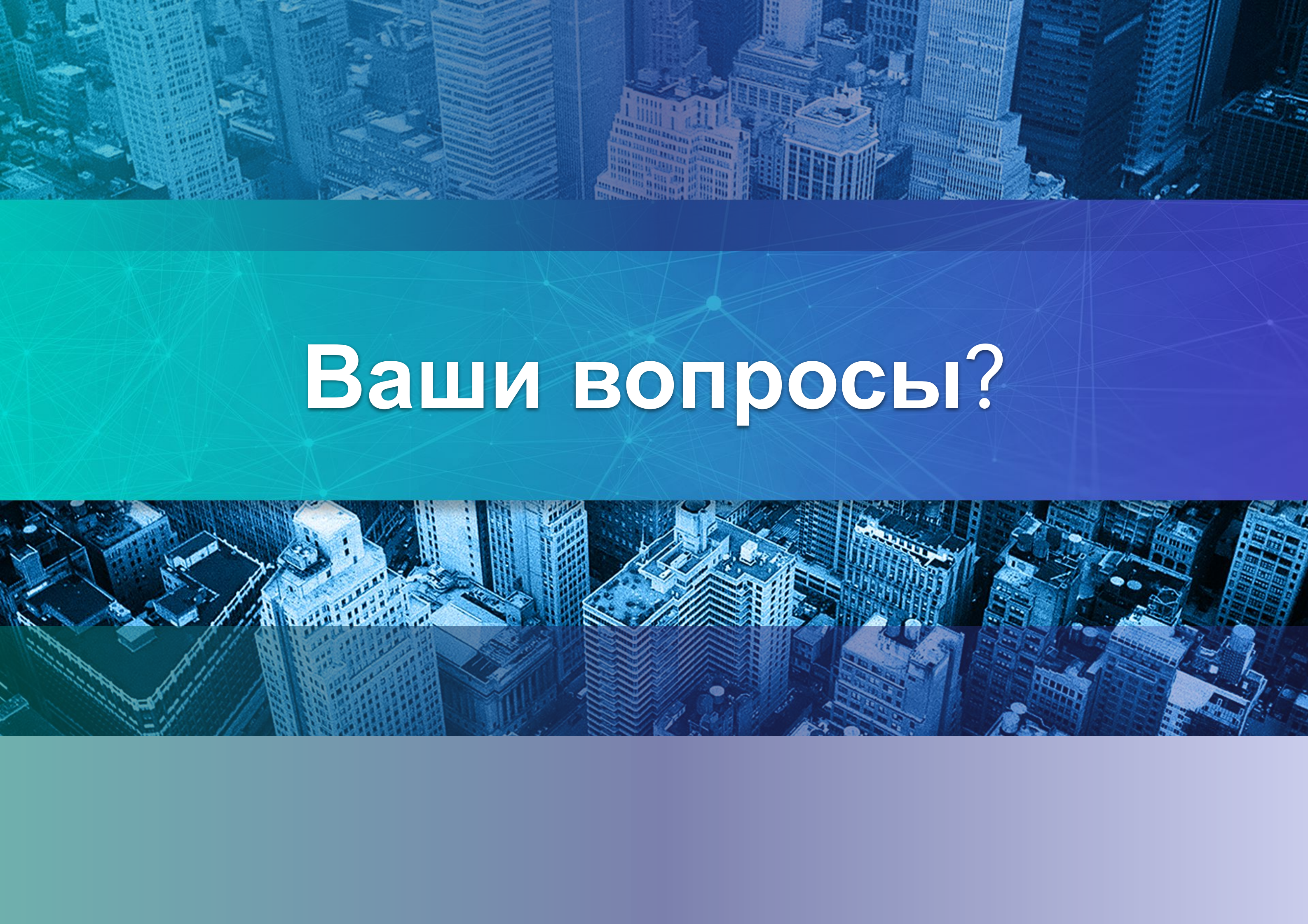
- при создании блоки **очищаются от данных**
- нет потери производительности на очистку блоков
- более долгое время создания

Виртуальные дисковые устройства

Типы виртуальных дисков:

Thin Provision

- при создании занимают минимальный объем и увеличиваются вместе с объемом данных на них
- производится очистка данных в выделяемых блоках
- меньшая производительность
- большая гибкость с точки зрения организации дискового пространства

The image features a central horizontal band with a blue-to-green gradient. Overlaid on this band is a network of white lines connecting various points, resembling a data or communication network. The background of the entire image is an aerial view of a city with numerous skyscrapers, rendered in a monochromatic blue and green color palette.

Ваши вопросы?

The image features a central horizontal band with a blue-to-green gradient. Overlaid on this band is a network of white lines connecting various points, resembling a data or communication network. The background of the entire image is an aerial view of a city skyline, with numerous skyscrapers and buildings. The color palette is dominated by shades of blue and green, with the text 'Overbooking' in white.

Overbooking

Overbooking

Овербукинг (overbooking) или **оверселлинг (overselling)** - в общем случае это продажа услуг поставщиком сверх тех объемов, которые он может предоставить.

Применительно к **виртуализации** - это продажа вычислительных мощностей в объемах больших, чем может предоставить серверное оборудование

О каких ресурсах речь?

В первую очередь это процессор и память, дисковое пространство и пропускная способность канала

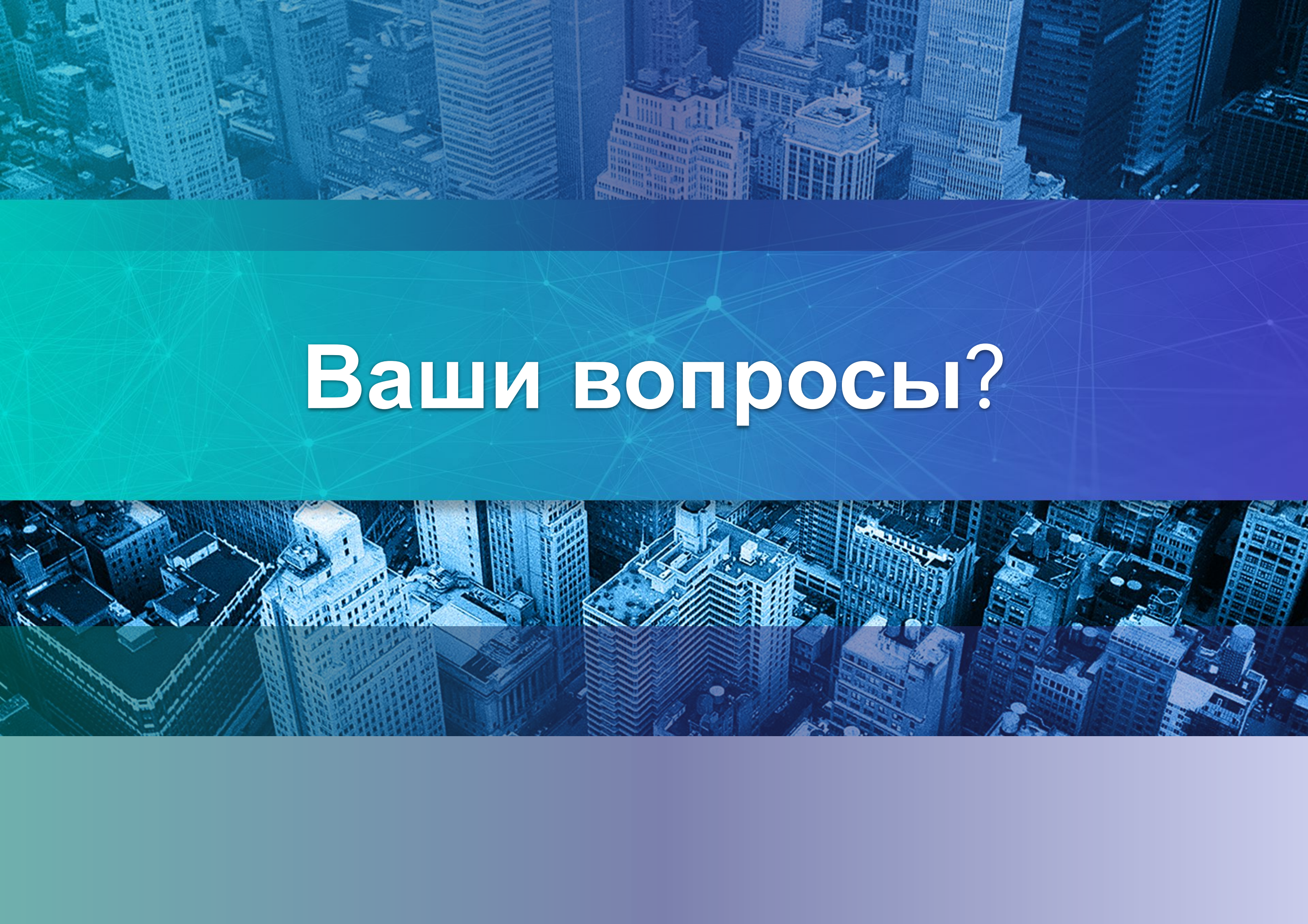
Overbooking

В чем это может выражаться?

Например в случае нехватки памяти для гостевых систем, гипервизор подключает swap, что резко снижает производительность гостевых систем и повышает дисковую активность на самом гипервизоре

Что такое Stolen CPU?

В общем случае на гостевой системе это количество времени, которое виртуальный сервер ждет процессорных ресурсов от гипервизора. Чем ближе этот показатель к нулю - тем лучше. Если steal time больше нуля и более 1% - значит соседняя гостевая система (или процессы на гипервизоре) занимают большое количество процессорного времени

The image features a central horizontal band with a blue-to-green gradient. Overlaid on this band is a white network of lines and dots, resembling a data or communication network. The background of the entire image is an aerial view of a city skyline, with buildings rendered in shades of blue and green. The text "Ваши вопросы?" is centered in the middle of the image in a bold, white, sans-serif font.

Ваши вопросы?

Маршрут вебинара

Виртуализация



Технологии виртуализации

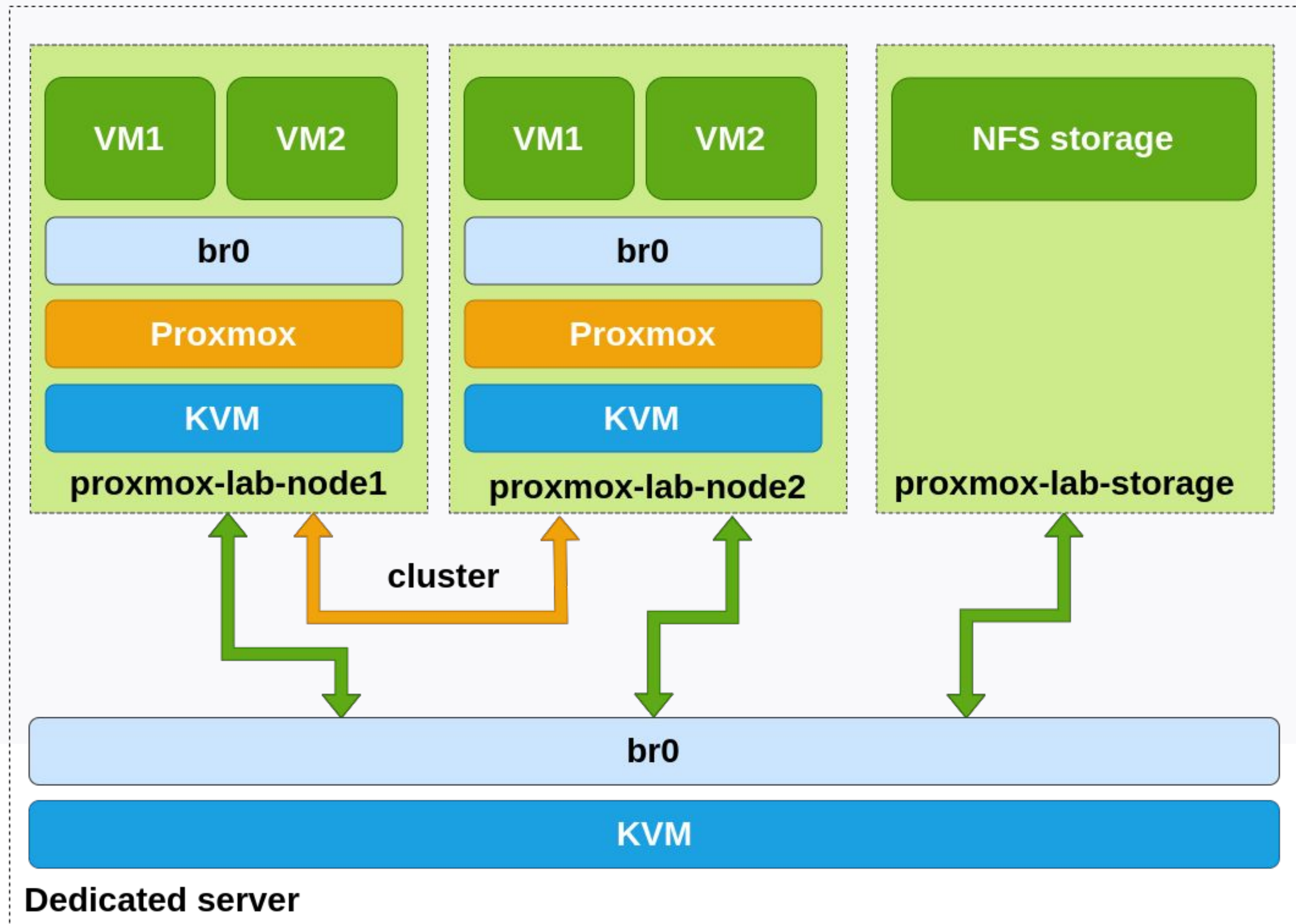


Proxmox



Схема тестового стенда

Схема тестового стенда





Proxmox



Proxmox Virtual Environment (Proxmox VE) - система виртуализации с открытым исходным кодом, основанная на Debian GNU/Linux. Разрабатывается австрийской фирмой Proxmox Server Solutions GmbH

https://ru.wikipedia.org/wiki/Proxmox_Virtual_Environment

Гипервизоры:

- KVM
- LXC

Управление:

- веб-интерфейс
- CLI интерфейс
- API (https://pve.proxmox.com/wiki/Proxmox_VE_API)

Proxmox Virtual Environment (Proxmox VE) - система виртуализации с открытым исходным кодом, основанная на Debian GNU/Linux. Разрабатывается австрийской фирмой Proxmox Server Solutions GmbH

https://ru.wikipedia.org/wiki/Proxmox_Virtual_Environment

Варианты авторизации:

- PAM
- LDAP
- двухфакторная авторизация

Кластеризация:

- возможность объединять от 2 до 32 нод в один кластер
- централизованное управление кластером из веб-интерфейса одной ноды
- живая миграция и бэкап виртуальных машин

Хранилища:

- GlusterFS
- iSCSI
- LVM
- LVM thin
- NFS
- RBD
- ZFS, ZFS over iSCSI
- CEPH



ProxmoX: установка

Proxmox: установка

Варианты установки Proxmox:

1. Установка из iso-образа с официального сайта

- установка образа на базе Debian и самого гипервизора
- удобный интерфейс
- минимум вопросов при установке

2. Установка дистрибутива Debian на сервер и Proxmox из официального репозитория

- больше действий
- больше гибкость и выбор версии дистрибутива Debian при установке

Proxmox: установка

Нюансы в процессе установки:

Включить пропуск пакетов в ядре хостовой системы:

```
sysctl -w net.ipv4.ip_forward=1
```

В файле /etc/hosts требуется следующая строка:

```
192.168.1.20 proxmox1.local proxmox1 pvelocalhost
```

Отключение сообщения об отсутствии подписки в веб-интерфейсе:

```
sed -i.bak "s/data.status !== 'Active'/false/g" \  
/usr/share/javascript/proxmox-widget-toolkit/proxmoxlib.js && \  
systemctl restart pveproxy.service
```

Proxmox: установка

Платная подписка:

- доступ к Enterprise репозиторию со стабильными версиями пакетов
- поддержка через портал клиента (от 3 обращений в год и более, зависит от уровня подписки)
- возможность удаленной поддержки через ssh

The image features a central banner with a blue-to-green gradient background. Overlaid on this banner is a faint, light-colored network of interconnected nodes and lines, resembling a digital or data network. The text "Ваши вопросы?" is centered in a large, white, bold font. The background of the entire image is an aerial view of a dense city skyline, with various skyscrapers and buildings, rendered in a monochromatic blue and green color palette.

Ваши вопросы?

The image features a background of a city skyline, likely New York City, with numerous skyscrapers. The color palette is dominated by shades of blue and green. A semi-transparent network of white lines and dots is overlaid on the cityscape, particularly concentrated in the central area where the text is located. The text 'Proxmox: KSM и Ballooning' is written in a clean, white, sans-serif font, centered horizontally across the middle of the image.

Proxmox: KSM и Ballooning

Proxmox: KSM и Ballooning

KSM (Kernel Samepage Merging) – технология позволяющая уменьшить расход оперативной памяти за счет нахождения одинаковых страниц и их последующего объединения

Преимущества:

- уменьшает вероятность использования swap
- дает возможность использовать больший, чем физически имеющийся на хост-машине, объем памяти

Недостатки:

- нет смысла использовать, если памяти на хост-машине достаточно для всех гостевых систем
- для работы технологии будут задействованы дополнительные процессорные ресурсы хост-машины

Прохтох: KSM и Ballooning

Ballooning - технология, которая позволяет гостевой системе динамически менять использование памяти, удаляя неиспользуемую память

В процессе используется драйвер, который способен вытеснять неиспользуемую память, путём захвата адресного пространства. Захваченная память может быть отдана другим гостевым системам

The image features a central banner with a blue-to-green gradient background. Overlaid on this banner is a faint, light-colored network of interconnected nodes and lines, resembling a digital or data network. The text "Ваши вопросы?" is centered in a large, white, bold font. The background of the entire image is an aerial view of a city skyline, with buildings rendered in shades of blue and green, matching the banner's color scheme.

Ваши вопросы?



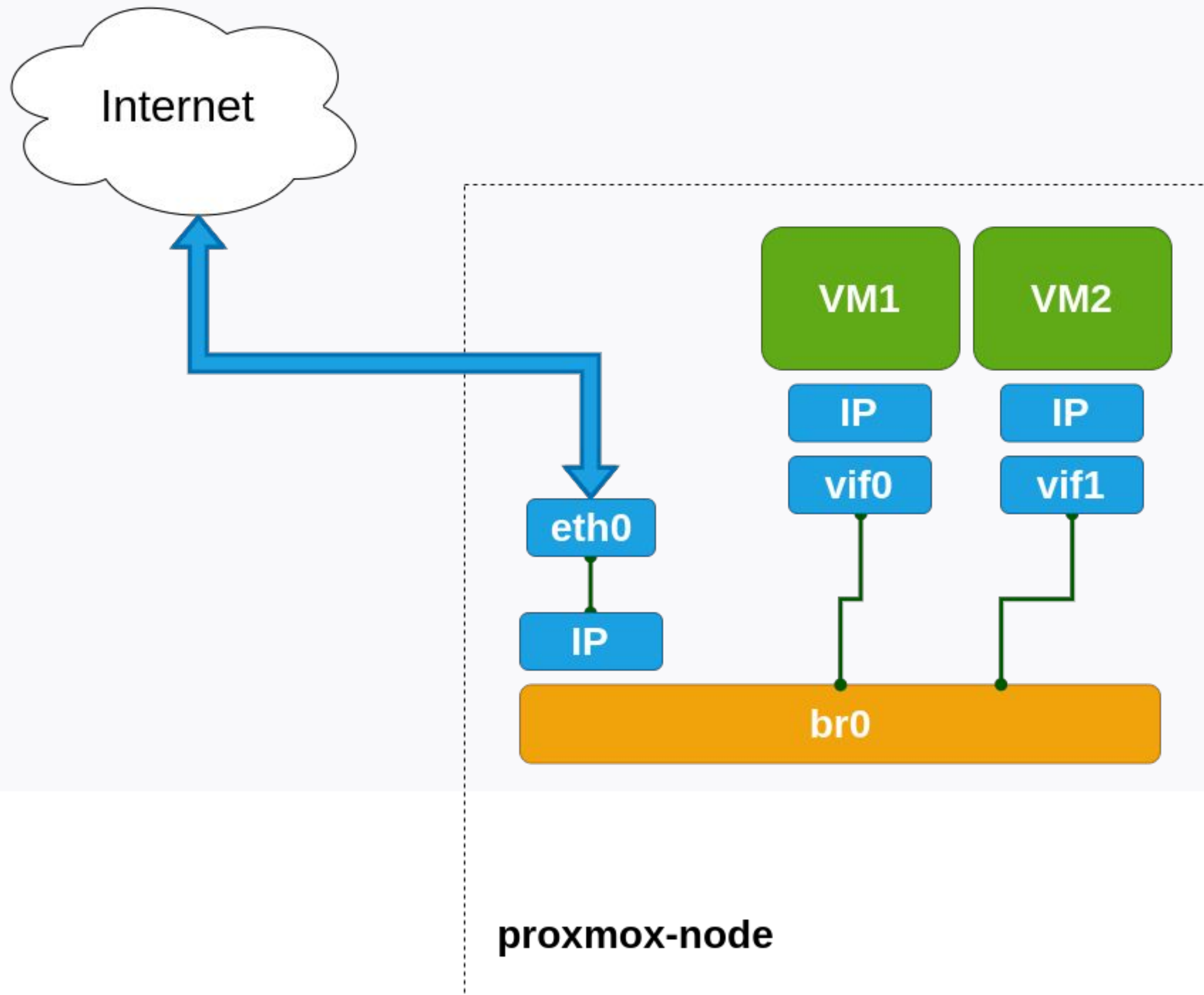
Proxmox: настройка сети



Bridge



Proxmox: настройка сети



Proxmox: настройка сети

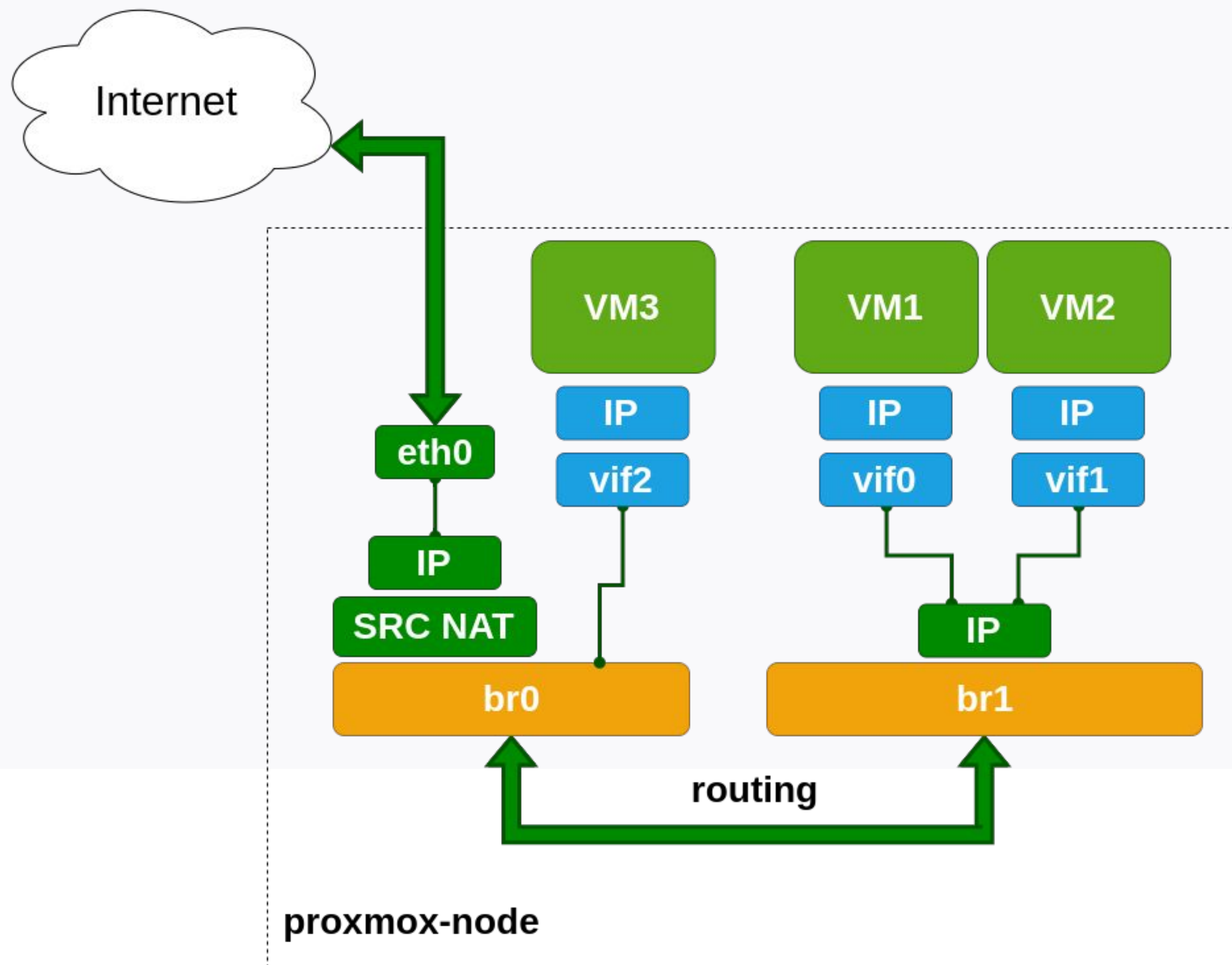
Подключение виртуальных машин через bridge-интерфейс с использованием публичных ip адресов:

- возможность настройки публичных ip адресов на интерфейсах виртуальных машин
- удобный доступ к сервисам в гостевых системах
- необходимость настройки фаерволла непосредственно в гостевых системах для обеспечения безопасности

The image features a background of a city skyline, likely New York City, with numerous skyscrapers. The color palette is dominated by shades of blue and green. A network of white lines and dots is overlaid on the image, suggesting a digital or network theme. The text "Bridge NAT" is centered in the middle of the image in a white, sans-serif font.

Bridge NAT

Proxmox: настройка сети



Proxmox: настройка сети

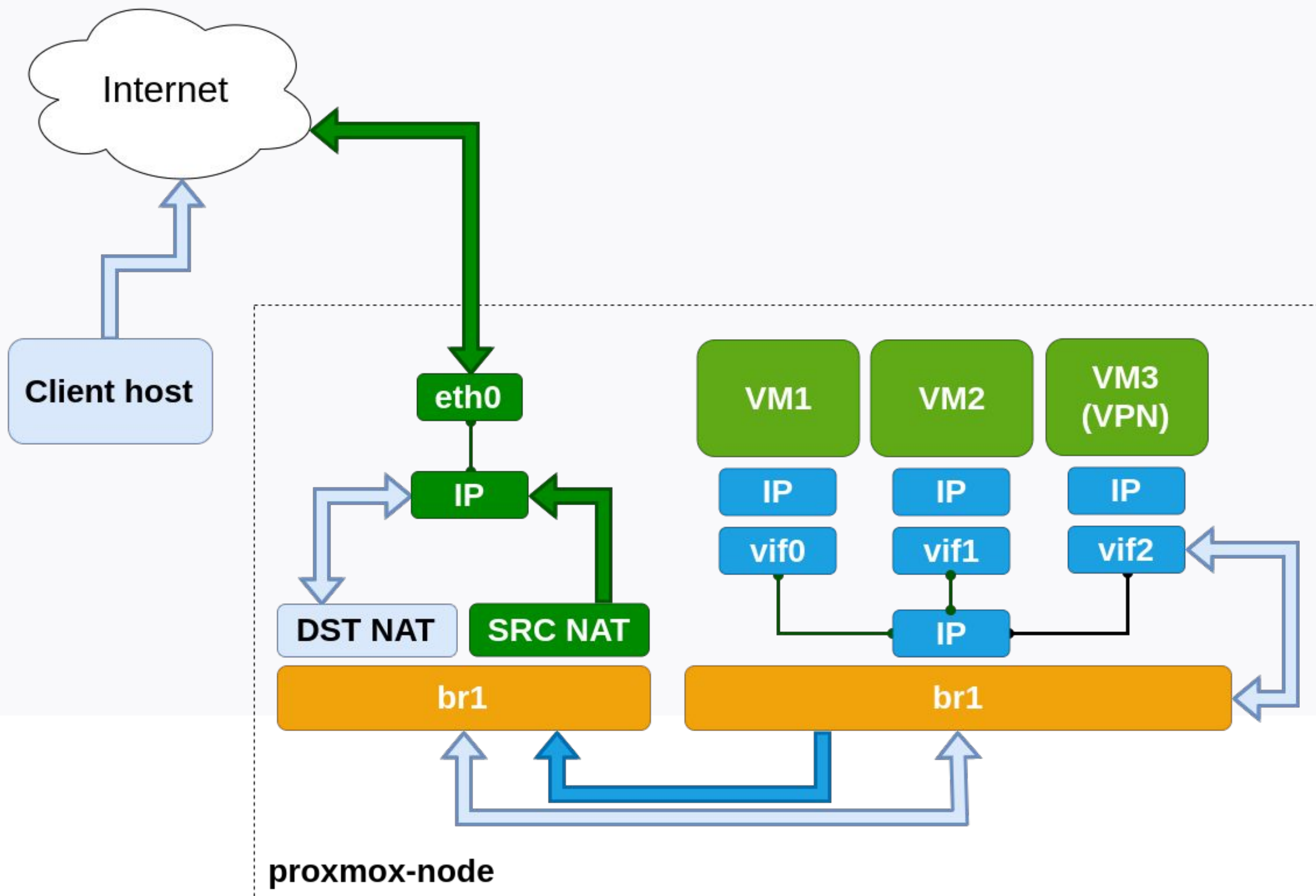
Подключение виртуальных машин в серую сеть на bridge-интерфейсе:

- отсутствие необходимости использовать публичные ip адреса (экономия реальных адресов)
- отсутствие необходимости в настройке файрволла в гостевых системах (нет прямого доступа извне)
- более сложный механизм доступа к сервисам гостевых систем (прокси или DNAT на хост-машине)
- более сложные условия администрирования гостевых систем

The image features a background of a city skyline, likely New York City, with numerous skyscrapers. The image is overlaid with a semi-transparent blue and green gradient. A network of white lines and dots is visible, suggesting a digital or network theme. The text "Bridge NAT VPN" is centered in the middle of the image in a white, sans-serif font.

Bridge NAT VPN

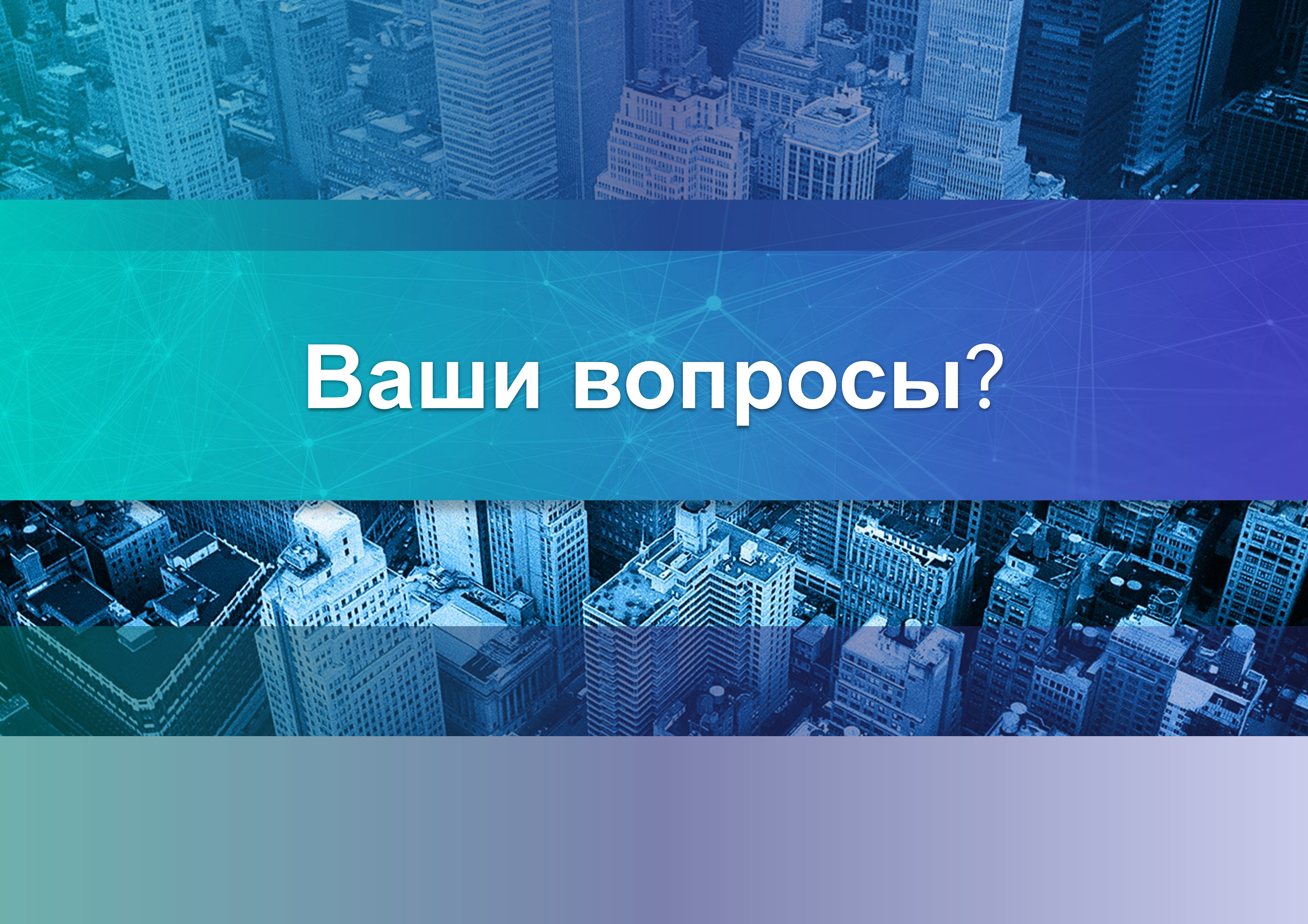
Proxmox: настройка сети



Proxmox: настройка сети

Подключение виртуальных машин в серую сеть на bridge-интерфейсе (использование VPN для доступа):

- использование DNAT для доступа к VPN и гостевым системам
- более простой механизм доступа к сервисам и администрированию гостевых систем (по сравнению с предыдущей схемой)
- зависимость от работы и правил NAT

The image features a central horizontal band with a blue-to-green gradient. Overlaid on this band is a network of white lines connecting various points, resembling a data or communication network. The background of the entire image is an aerial view of a city skyline, with numerous skyscrapers and buildings. The color palette is dominated by shades of blue and green, giving it a modern, technological feel.

Ваши вопросы?

The image features a blue-tinted aerial view of a city skyline, likely New York City, with numerous skyscrapers. A semi-transparent blue band with a white network diagram pattern (nodes and connecting lines) is overlaid across the middle of the image. The title "Snapshots and backups" is written in white, sans-serif font within this band.

Snapshots and backups

An aerial view of a city skyline, likely New York City, with a blue overlay and a network pattern of lines and dots. The text is overlaid on this background.

Вопрос к аудитории:

**В чем разница между снимком
и бэкапом?**

The image features a central horizontal band with a blue-to-green gradient. Overlaid on this band is a faint, white network of interconnected nodes and lines, resembling a data or social network. The background of the entire image is an aerial view of a city skyline, with numerous skyscrapers and buildings. The color palette is dominated by shades of blue and green, giving it a technological or digital feel.

Snapshots

Снапшот (snapshot) - снимок состояния гостевой системы

- сохраняет память (опционально), конфигурацию и состояние всех виртуальных дисков гостевой системы
- во время отката (**rollback**) к какому-то снапшоту происходит восстановление памяти, конфигурации и состояния данных на дисках
- сделать снапшот можно не останавливая работу виртуальной машины
- можно сохранить несколько снапшотов и откатиться позже к любому из них

The image features a central horizontal band with a blue-to-green gradient. Overlaid on this band is a network of white lines connecting various points, resembling a data or communication network. The background of the entire image is an aerial view of a city skyline, with numerous skyscrapers and buildings. The color palette is dominated by shades of blue and green, giving it a technological and digital feel.

Backups

Резервное копирование (backup) - процесс создания резервной копии гостевой системы, которая содержит конфигурацию гостевой системы и все данные с ее дисков:

Алгоритмы сжатия:

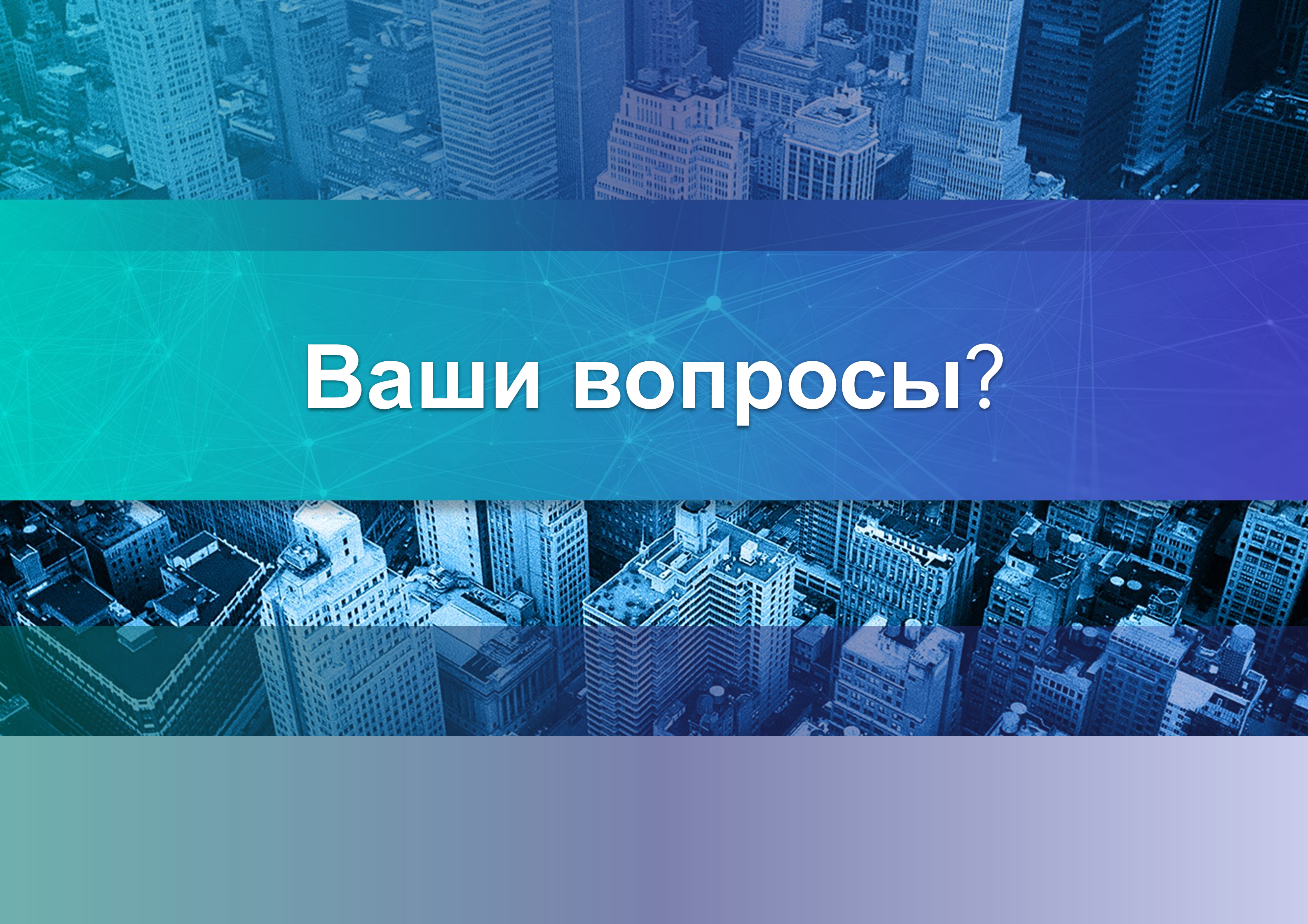
- LZ0
- GZIP

Режимы архивирования:

- **snapshot**
 - не требует остановки виртуальной машины
 - низкая скорость бэкапа
 - низкая надежность бэкапа (блокировки файлов в файловой системе)

Режимы архивирования:

- **suspend**
 - не требует остановки виртуальной машины
 - требует постановки машины на “паузу” (suspend) с сохранением состояния оперативной памяти и стартом с того же состояния
- **stop**
 - требует отключения виртуальной машины
 - после завершения процесса создания бэкапа машина запускается автоматически
 - самый надежный метод создания бэкапов

The image features a central horizontal band with a blue-to-green gradient. Overlaid on this band is a network of white lines connecting various points, resembling a data or communication network. The background of the entire image is an aerial view of a city skyline, with numerous skyscrapers and buildings. The color palette is dominated by shades of blue and green, giving it a modern, technological feel.

Ваши вопросы?

The image features a central horizontal band with a blue-to-green gradient. Overlaid on this band is a faint, white network diagram consisting of interconnected nodes and lines. The background of the entire image is an aerial view of a city skyline, with buildings rendered in shades of blue and green. The text 'LXC в Proxmox' is centered within the gradient band in a white, sans-serif font.

LXC в Proxmox

LXC (англ. Linux Containers) – система виртуализации на уровне операционной системы для запуска нескольких изолированных экземпляров операционной системы Linux на одном узле. LXC не использует виртуальные машины, а создает виртуальное окружение с собственным пространством процессов и сетевым стеком

<https://ru.wikipedia.org/wiki/LXC>

Особенности:

- все экземпляры LXC используют один экземпляр ядра ОС
- LXC основана на технологиях ядра Linux **cgroups** и **namespaces**
- сетевая конфигурация построена с использованием bridge-интерфейсов хост-машины
- контейнеры можно запускать как от пользователя root, так и от непривилегированного пользователя

Где брать образы для LXC-контейнеров?

Можно здесь: <https://us.images.linuxcontainers.org>

А можно прямо из веб-интерфейса Proxmox или его командной строки.

Обновляем данные репозитория:

```
pveam update
```

Смотрим доступные образы:

```
pveam available --section system
system    alpine-3.10-default_20190626_amd64.tar.xz
system    alpine-3.9-default_20190224_amd64.tar.xz
system    archlinux-base_20190924-1_amd64.tar.gz
system    centos-6-default_20191016_amd64.tar.xz
system    centos-7-default_20190926_amd64.tar.xz
system    centos-8-default_20191016_amd64.tar.xz
system    debian-10.0-standard_10.0-1_amd64.tar.gz
system    debian-8.0-standard_8.11-1_amd64.tar.gz
```

LXC в Proxmox

Скачиваем нужный образ в хранилище **local**:

```
pveam download local centos-8-default_20191016_amd64.tar.xz
```

Скачиваем нужный образ в хранилище **NFS_storage**:

```
pveam download NFS_storage centos-8-default_20191016_amd64.tar.xz
```

The image features a central horizontal band with a blue-to-green gradient. Overlaid on this band is a white network of lines and dots, resembling a data or communication network. The background of the entire image is an aerial view of a city skyline, with buildings rendered in shades of blue and green. The text "Ваши вопросы?" is centered in the network band.

Ваши вопросы?

The image features a blue-tinted aerial view of a city skyline, likely New York City, with numerous skyscrapers. A semi-transparent blue band with a white network pattern of dots and lines runs horizontally across the middle of the image. The text 'Кластер Proxmox' is centered within this band in a white, bold, sans-serif font.

Кластер Proxmox

Кластер Proxmox

Перед развертыванием кластера Proxmox:

1. Каждая нода должна резолвить соседнюю, для этого файл /etc/hosts приводим к следующему виду:

```
192.168.1.20 proxmox1.local proxmox1 pvelocalhost  
192.168.1.21 proxmox2.local proxmox2
```

2. Для работы сервиса corosync на всех нодах должны быть доступны UDP порты 5404 и 5405

3. Дата и время должны быть синхронизированы

4. Будет использоваться ssh туннель на порту 22 между нодами

5. Для построения высокодоступного и отказоустойчивого кластера нужны как минимум три ноды с одинаковыми версиями Proxmox

Кластер Proxmox

Перед развертыванием кластера Proxmox:

6. Разработчики Proxmox рекомендуют использовать аппаратные сетевые интерфейсы для пропуска трафика внутри кластера, особенно если речь идет про shared storage

7. При введении новой ноды в кластер нужно быть готовым ввести пароль пользователя root в процессе

Кластер Proxmox

Развертывание кластера Proxmox:

Инициализируем кластер на мастер-ноде (192.168.1.20):

```
proxmox create <имя кластера>
```

Присоединяем вторую ноду к кластеру (192.168.1.21):

```
proxmox add 192.168.1.21
```

Смотрим статус кластера на мастер-ноде:

```
proxmox status
```

Кластер Proxmox

Удалить ноду из кластера:

```
pvestm delnode 192.168.1.21
```

Остановка сервисов Proxmox на сломанной ноде:

```
systemctl stop pvestatd.service  
systemctl stop pvedaemon.service  
systemctl stop pve-cluster.service  
systemctl stop corosync  
systemctl stop pve-cluster
```

Очистка базы данных с информацией о кластере:

```
sqlite3 /var/lib/pve-cluster/config.db  
delete from tree where name = 'corosync.conf';  
.quit
```

Кластер Proxmox

Удаляем файлы сервисов из кластерной файловой системы, для этого сначала переводим ее в standalone режим:

```
proxmoxfs -l
```

Затем удаляем файлы:

```
rm /etc/pve/corosync.conf  
rm /etc/corosync/*  
rm /var/lib/corosync/*  
rm -rf /etc/pve/nodes/*
```

The image features a central horizontal band with a blue-to-green gradient. Overlaid on this band is a network of white lines connecting various points, resembling a data or communication network. The background of the entire image is an aerial view of a city skyline, with numerous skyscrapers and buildings. The color palette is dominated by shades of blue and green, giving it a modern, technological feel.

Ваши вопросы?


Рефлексия



Назовите 3 момента, которые вам запомнились в процессе занятия



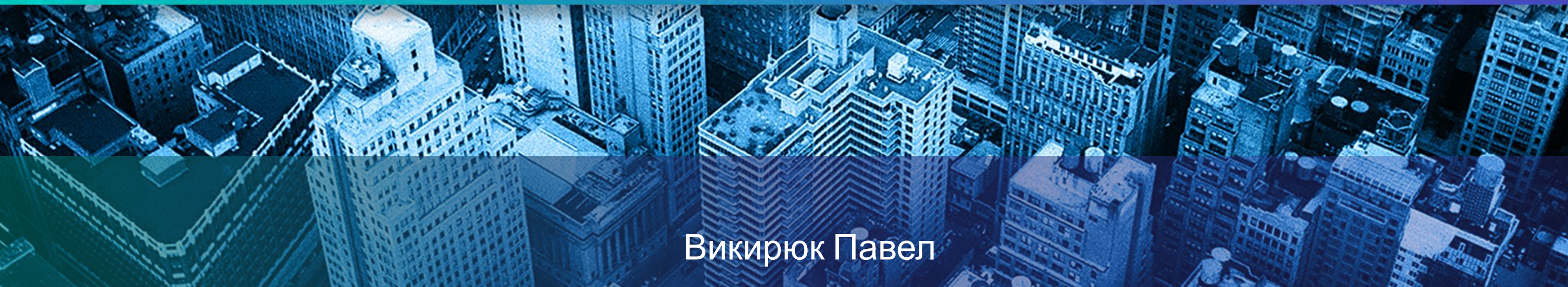
Что вы будете применять в работе из сегодняшнего вебинара?



Заполните, пожалуйста,
опрос о занятии по ссылке в чате



Спасибо за внимание!
Приходите на следующие вебинары



Викирюк Павел

Системный инженер