

вводный курс в Proxmox VE

 selectel.ru/blog/magic-of-virtualization-intro

15 февраля 2018 г.

Магия виртуализации: вводный курс в Proxmox VE



Николай Рубанов Старший технический писатель

15 февраля 2018

Сегодня речь пойдет о том, как быстро и достаточно просто на одном физическом сервере развернуть несколько виртуальных серверов с разными операционными системами. Любому системному администратору это позволит централизованно управлять всей IT-инфраструктурой компании и экономить огромное количество ресурсов. Использование виртуализации помогает максимально абстрагироваться от физического серверного оборудования, защитить критичные сервисы и легко восстановить их работу даже [...]



Сегодня речь пойдет о том, как быстро и достаточно просто на одном физическом сервере развернуть несколько виртуальных серверов с разными операционными системами. Любому системному администратору это позволит централизованно управлять всей IT-инфраструктурой компании и экономить огромное количество ресурсов.

Использование виртуализации помогает максимально абстрагироваться от физического серверного оборудования, защитить критичные сервисы и легко восстановить их работу даже в случае очень серьезных сбоев.

Без всякого сомнения, большинству системных администраторов знакомы приемы работы с виртуальной средой и для них эта статья не станет каким-либо открытием. Несмотря на это, есть компании, которые не используют гибкость и скорость работы виртуальных решений из-за недостатка точной информации о них. Мы надеемся, что наша статья поможет на примере понять, что гораздо проще один раз начать использовать виртуализацию, чем испытывать неудобства и недостатки физической инфраструктуры.

К счастью, попробовать как работает виртуализация достаточно просто. Мы покажем, как создать сервер в виртуальной среде, например, для переноса CRM-системы, используемой в компании. Практически любой физический сервер можно превратить в виртуальный, но вначале необходимо освоить базовые приемы работы. Об этом и пойдет речь ниже.

Как это устроено

Когда речь идет о виртуализации, многим начинающим специалистам сложно разобраться в терминологии, поэтому поясним несколько базовых понятий:

- **Гипервизор** – специальное программное обеспечение, которое позволяет создавать виртуальные машины и управлять ими;
- **Виртуальная машина (далее VM)** – это система, представляющая собой логический сервер внутри физического со своим набором характеристик, накопителями и операционной системой;
- **Хост виртуализации** — физический сервер с запущенным на нем гипервизором.

Для того чтобы сервер мог работать полноценным хостом виртуализации, его процессор должен поддерживать одну из двух технологий – либо Intel VT, либо AMD-V. Обе технологии выполняют важнейшую задачу — предоставление аппаратных ресурсов сервера виртуальным машинам.

Ключевой особенностью является то, что любые действия виртуальных машин исполняются напрямую на уровне оборудования. При этом они друг от друга изолированы, что достаточно легко позволяет управлять ими по отдельности. Сам же гипервизор играет роль контролирующего органа, распределяя ресурсы, роли и приоритеты между ними. Также гипервизор занимается эмуляцией той части аппаратного обеспечения, которая необходима для корректной работы операционной системы.

Расширенные возможности

Внедрение виртуализации дает возможность иметь в наличии несколько запущенных копий одного сервера. Критический сбой или ошибка, в процессе внесения изменений в такую копию, никак не повлияет на работу текущего сервиса или приложения. При этом также снимаются две основные проблемы –

масштабирование и возможность держать «зоопарк» разных операционных систем на одном оборудовании. Это идеальная возможность совмещения самых разных сервисов без необходимости приобретения отдельного оборудования для каждого из них.

Виртуализация повышает отказоустойчивость сервисов и развернутых приложений. Даже если физический сервер вышел из строя и его необходимо заменить на другой, то вся виртуальная инфраструктура останется полностью работоспособной, при условии сохранности дисковых носителей. При этом физический сервер может быть вообще другого производителя. Это особенно актуально для компаний, которые используют серверы, производство которых прекращено и потребуется осуществить переход на другие модели.

Теперь перечислим самые популярные гипервизоры, существующие на текущий день:

- VMware ESXi
- Microsoft Hyper-V
- Open Virtualization Alliance KVM
- Oracle VM VirtualBox

Они все достаточно универсальны, однако, у каждого из них имеются определенные особенности, которые следует всегда учитывать на этапе выбора: стоимость развёртывания/обслуживания и технические характеристики. Стоимость коммерческих лицензий VMware и Hyper-V весьма высока, а в случае возникновения сбоев, решить проблему с этими системами собственными силами очень непросто.

KVM же напротив, полностью бесплатен и достаточно прост в работе, особенно в составе готового решения на базе Debian Linux под названием Proxmox Virtual Environment. Именно эту систему мы можем порекомендовать для первоначального знакомства с миром виртуальной инфраструктуры.

Установка Proxmox VE

Данная процедура чаще всего не вызывает никаких вопросов. Скачиваем актуальную версию образа с [официального сайта](#) и записываем его на любой внешний носитель с помощью утилиты [Win32DiskImager](#) (в Linux используется команда dd), после чего загружаем сервер непосредственно с этого носителя. Наши клиенты, арендующие у нас выделенные серверы, могут воспользоваться двумя еще более простыми путями – просто смонтировав нужный образ непосредственно из KVM-консоли, либо [используя наш PXE-сервер](#).

Программа установки имеет графический интерфейс и задаст всего лишь несколько вопросов.

1. Выбираем диск, на который будет выполнена установка. В разделе «Options» можно также задать дополнительные параметры разметки.



2. Указываем региональные настройки.



Proxmox VE Installer

Location and Time Zone selection

The Proxmox Installer automatically makes location based optimizations, like choosing the nearest mirror to download files. Also make sure to select the right time zone and keyboard layout.

Press the Next button to continue installation.

- **Country:** The selected country is used to choose nearby mirror servers. This will speedup downloads and make updates more reliable.
- **Time Zone:** Automatically adjust daylight saving time.
- **Keyboard Layout:** Choose your keyboard layout.

Country

Time zone

Keyboard Layout

Abort

Next

3. Указываем пароль, который будет использоваться для авторизации суперпользователя root и E-mail адрес администратора.



Proxmox VE Installer

Administration Password and E-Mail Address

Proxmox Virtual Environment is a full featured highly secure GNU/Linux system based on Debian.

Please provide the *root* password in this step.

- **Password:** Please use a strong password. It should have 8 or more characters. Also combine letters, numbers, and symbols.

- **E-Mail:** Enter a valid email address. Your Proxmox VE server will send important alert notifications to this email account (such as backup failures, high availability events, etc.).

Press the Next button to continue installation.

Password

Confirm

E-Mail

Abort

Next

4. Указываем сетевые настройки. FQDN обозначает полностью определенное имя домена, например, node01.yourcompany.com.



Proxmox VE Installer

Management Network Configuration

Please verify the displayed network configuration. You will need a valid network configuration to access the management interface after installation.

Afterwards press the Next button to continue installation. The installer will then partition your hard disk and start copying packages.

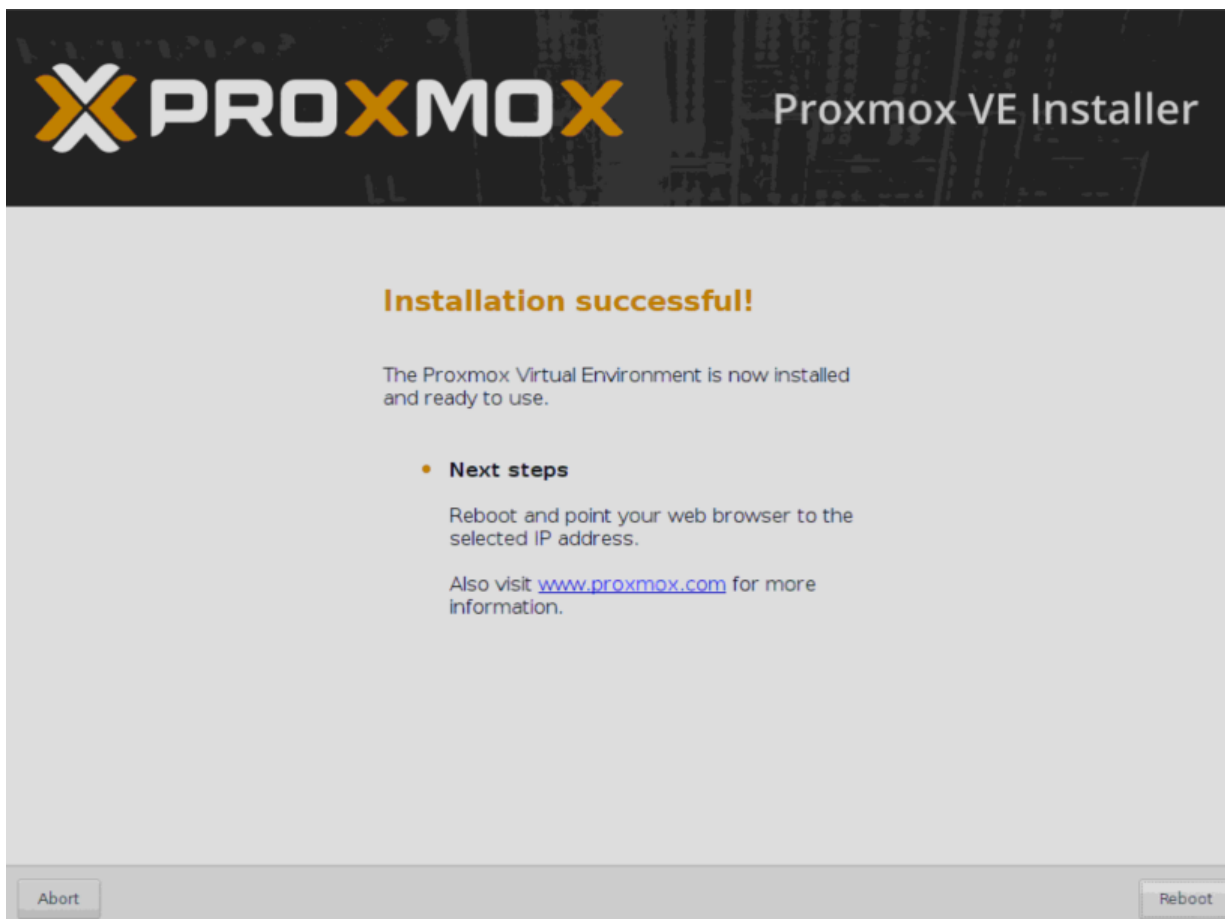
- **IP address:** Set the IP address for the Proxmox Virtual Environment.
- **Netmask:** Set the netmask of your network.
- **Gateway:** IP address of your gateway or firewall.
- **DNS Server:** IP address of your DNS server.

Management Interface:	enp4s0f0 - 0c:c4:7a:33:1f:b6 (igb) ▼
Hostname (FQDN):	Домен полностью
IP Address:	IP-адрес сервера
Netmask:	Маска подсети
Gateway:	Основной шлюз
DNS Server:	Адрес DNS-сервера

Abort

Next

5. После завершения установки, сервер можно отправить в перезагрузку с помощью кнопки Reboot.



Веб-интерфейс управления станет доступен по адресу:

`https://IP_адрес_сервера:8006`

Что нужно сделать после установки

Есть несколько важных вещей, которые следует выполнить после установки Proxmox. Расскажем о каждой из них подробнее.

Обновить систему до актуальной версии

Для этого зайдём в консоль нашего сервера и отключим платный репозиторий (доступен только тем, кто купил платную поддержку). Если этого не сделать — apt сообщит об ошибке при обновлении источников пакетов.

1. Открываем консоль и редактируем конфигурационный файл apt:

```
nano /etc/apt/sources.list.d/pve-enterprise.list
```

2. В этом файле будет всего одна строка. Ставим перед ней символ «#», чтобы отключить получение обновлений из платного репозитория:

```
#deb https://enterprise.proxmox.com/debian/pve stretch pve-enterprise
```

3. Сочетанием клавиш Ctrl+X выполняем выход из редактора, отвечая «Y» на вопрос системы о сохранении файла.

4. Выполняем команду обновления источников пакетов:

```
apt update
```

5. Обновляем все пакеты:

```
apt -y upgrade
```

Позаботиться о безопасности

Мы можем порекомендовать установить популярнейшую утилиту Fail2Ban, защищающую от атак методом перебора паролей (брутфорс). Принцип ее работы заключается в том, что если злоумышленник превысит определенное количество попыток входа за указанное время с неверным логином/паролем, то его IP-адрес будет заблокирован. Срок блокировки и количество попыток можно указать в конфигурационном файле.

Исходя из практического опыта, за неделю работы сервера с открытым ssh-портом 22 и внешним статическим IPv4 адресом, было более 5000 попыток подобрать пароль. И около 1500 адресов утилита успешно заблокировала. Для выполнения установки приводим небольшую инструкцию:

1. Открываем консоль сервера через веб-интерфейс или SSH.

2. Обновляем источники пакетов:

```
apt update
```

3. Устанавливаем Fail2Ban:

```
apt install fail2ban
```

4. Открываем конфигурацию утилиты на редактирование:

```
nano /etc/fail2ban/jail.conf
```

5. Изменяем переменные **bantime** (количество секунд на которые будет блокироваться злоумышленник) и **maxretry** (количество попыток ввода логина/пароля) для каждого отдельного сервиса.

6. Сочетанием клавиш Ctrl+X выполняем выход из редактора, отвечая «Y» на вопрос системы о сохранении файла.

7. Перезапускаем службу:

```
systemctl restart fail2ban
```

Проверить статус работы утилиты, например, снять статистику блокировок заблокированных IP-адресов с которых были попытки перебора паролей SSH, можно одной простой командой:

```
fail2ban-client -v status sshd
```

Ответ утилиты будет выглядеть примерно так:

```
root@hypervisor:~# fail2ban-client -v status sshd
INFO    Loading configs for fail2ban under /etc/fail2ban
INFO    Loading files: ['/etc/fail2ban/fail2ban.conf']
INFO    Loading files: ['/etc/fail2ban/fail2ban.conf']
INFO    Using socket file /var/run/fail2ban/fail2ban.sock
Status for the jail: sshd
|- Filter
|  |- Currently failed: 3
|  |- Total failed:    4249
|  `-- File list:      /var/log/auth.log
`- Actions
   |- Currently banned: 0
   |- Total banned:    410
   `-- Banned IP list:
```

Аналогичным способом можно закрыть от подобных атак Web-интерфейс, создав соответствующее правило. Пример такого правила для Fail2Ban можно найти в [официальном руководстве](#).

Начало работы

Хочется обратить внимание на то, что Proxmox готов к созданию новых машин сразу после установки. Тем не менее, рекомендуем выполнить предварительные настройки, чтобы в дальнейшем системой было легко управлять. Практика показывает, что гипервизор и виртуальные машины стоит разнести по разным физическим носителям. О том, как это сделать и пойдет речь ниже.

Настроить дисковые накопители

Следующим этапом следует настроить хранилище, которое можно будет использовать для сохранения данных виртуальных машин и резервных копий.

ВНИМАНИЕ! Приведенный ниже пример дисковой разметки можно использовать только для тестовых целей. Для эксплуатации в реальных условиях мы настоятельно рекомендуем использовать программный или аппаратный RAID-массив, чтобы исключить потерю данных при выходе дисков из строя. О том, как правильно приготовить дисковый массив к работе и как действовать в случае аварийной ситуации мы расскажем в одной из следующих статей.

Предположим, что физический сервер имеет два диска — `/dev/sda`, на который установлен гипервизор и пустой диск `/dev/sdb`, который планируется использовать для хранения данных виртуальных машин. Чтобы система смогла увидеть новое хранилище, можно воспользоваться самым простым и эффективным методом — подключить его как обычную директорию. Но перед этим следует выполнить

некоторые подготовительные действия. В качестве примера посмотрим, как подключить новый диск **/dev/sdb**, любого размера, отформатировав его в файловую систему **ext4**.

1. Размечаем диск, создавая новый раздел:

```
fdisk /dev/sdb
```

2. Нажимаем клавишу **o** или **g** (разметить диск в MBR или GPT).

3. Далее нажимаем клавишу **n** (создать новый раздел).

4. И наконец **w** (для сохранения изменений).

5. Создаем файловую систему **ext4**:

```
mkfs.ext4 /dev/sdb1
```

6. Создаем директорию, куда будем монтировать раздел:

```
mkdir /mnt/storage
```

7. Открываем конфигурационный файл на редактирование:

```
nano /etc/fstab
```

8. Добавляем туда новую строку:

```
/dev/sdb1          /mnt/storage      ext4              defaults          0                0
```

9. После внесения изменений сохраняем их сочетанием клавиш **Ctrl + X**, отвечая «Y» на вопрос редактора.

10. Для проверки, что все работает, отправляем сервер в перезагрузку:

```
shutdown -r now
```

11. После перезагрузки проверяем смонтированные разделы:

```
df -h
```

Вывод команды должен показать, что **/dev/sdb1** смонтирован в директорию **/mnt/storage**. Это значит, что наш накопитель готов к работе.

Добавить новое хранилище в Proxmox

Авторизуемся в панели управления и заходим в разделы «Датацентр» → «Хранилище» → «Добавить» → «Директория».

В открывшемся окне заполняем следующие поля:

- **ID** — название будущего хранилища;

- **Директория** — /mnt/storage;
- **Содержимое** — выделяем все варианты (поочередно щелкая на каждом варианте).

Добавить: Директория

ID: Узлы:

Директория: Включить: ☒

Содержимое: Общедоступно: ☐

Макс. резерв. копий:

Добавить

После этого нажимаем кнопку «Добавить». На этом настройка завершена.

Создать виртуальную машину

Для создания виртуальной машины выполняем следующую последовательность действий:

1. Определяемся с версией операционной системы.
2. Заранее закачиваем ISO-образ.
3. Выбираем в меню «Хранилище» только что созданное хранилище.
4. Нажимаем «Содержимое» → «Загрузить».
5. Выбираем из списка ISO-образ и подтверждаем выбор нажатием кнопки «Загрузить».

После завершения операции образ будет отображен в списке доступных.

Создаем нашу первую виртуальную машину:

1. Нажимаем «Создать VM».
2. Заполняем поочередно параметры: «Имя» → «ISO-Image» → Размер и тип жесткого диска → Количество процессоров → Объем оперативной памяти → Сетевой адаптер.
3. Выбрав все желаемые параметры нажимаем «Завершить». Созданная машина будет отображена в меню панели управления.
4. Выбираем ее и нажимаем «Запуск».
5. Переходим в пункт «Консоль» и выполняем установку операционной системы точно таким же образом, как и на обычный физический сервер.

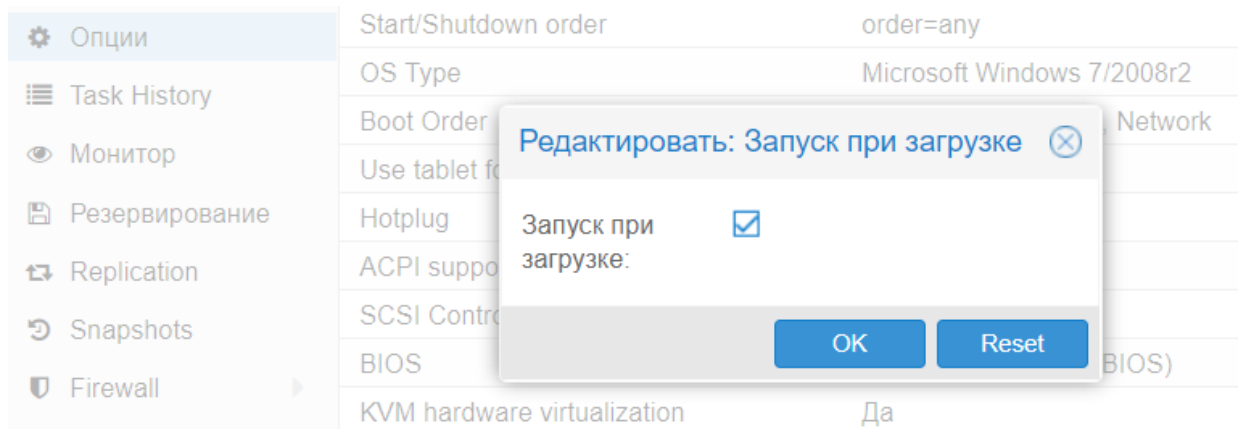
Если необходимо создать еще одну машину — повторяем вышеуказанные операции. После того как все они будут готовы, с ними можно работать одновременно, открывая несколько окон консоли.

Настроить автозапуск

По умолчанию Proxmox автоматически не запускает машины, но это легко решается буквально двумя щелчками мыши:

1. Щелкаем по названию нужной машины.
2. Выбираем вкладку «Опции» → «Запуск при загрузке».
3. Ставим галочку напротив одноименной надписи.

Теперь, в случае перезагрузки физического сервера, VM будет запущена автоматически.



Для продвинутых администраторов имеется еще и возможность указать дополнительные параметры запуска в разделе «Start/Shutdown order». Можно явным образом указать в каком порядке следует запускать машины. Также можно указать время, которое должно пройти до старта следующей VM и время задержки выключения (если операционная система не успеет завершить работу, гипервизор принудительно ее выключит через определенное количество секунд).

Заключение

В этой статье были изложены основы того, как можно начать работать с Proxmox VE и мы надеемся, что она поможет начинающим специалистам сделать первый шаг и попробовать виртуализацию в действии.

Proxmox VE — это действительно очень мощный и удобный инструмент для любого системного администратора; главное не бояться экспериментировать и понять, как это действительно работает.

Если у вас появились вопросы, добро пожаловать в комментарии.