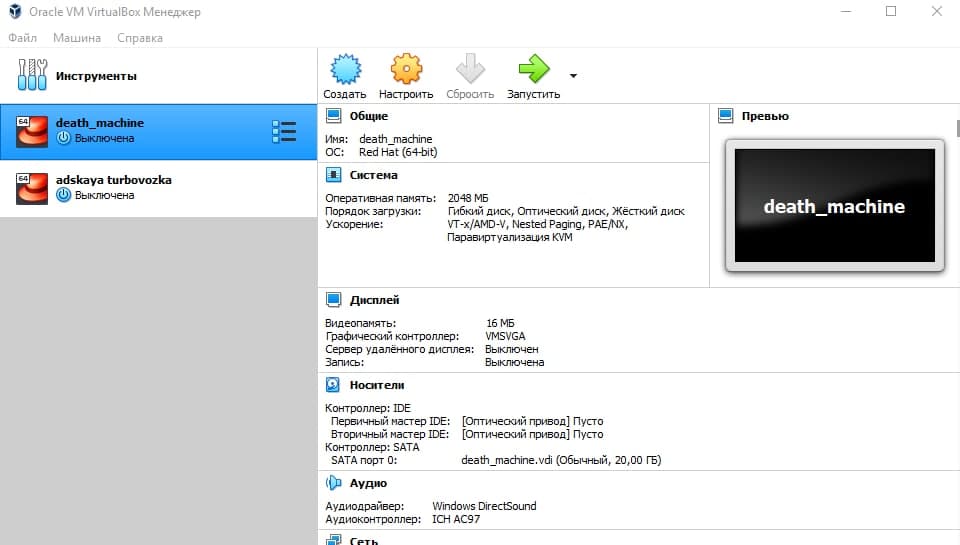
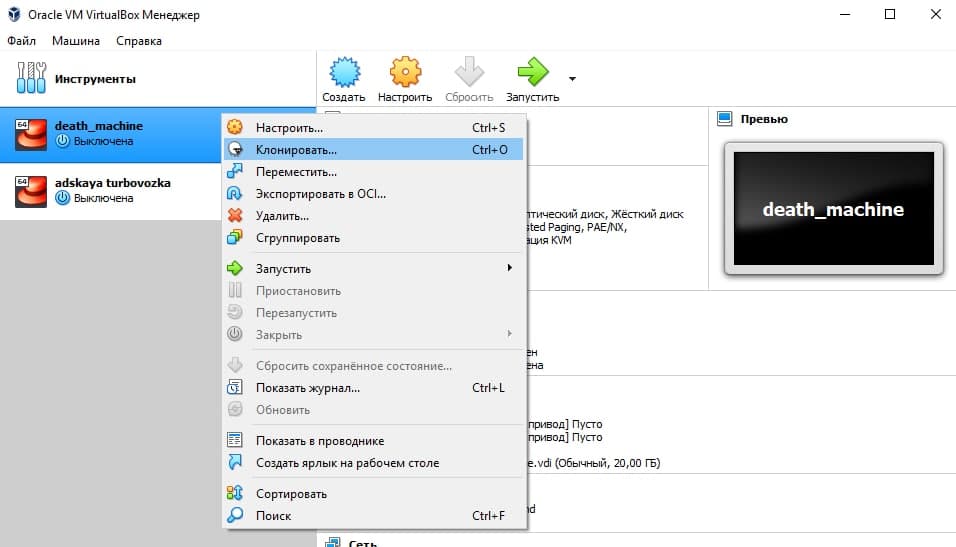
­­­­­­­­­­КСМ93б Марчук Олексій Сергійович

Work-case 3

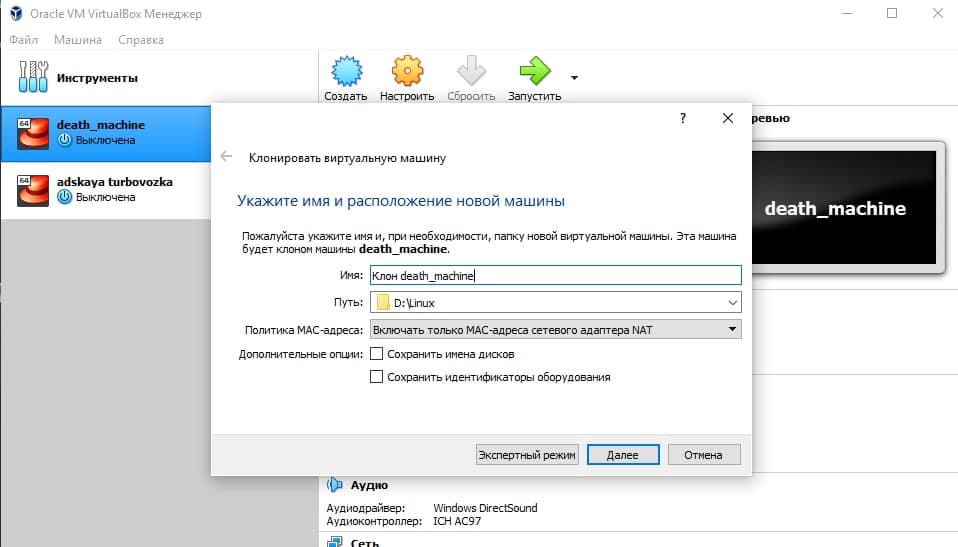
Для створення повної копії існуючої машини небхідно виконати наступні дії:



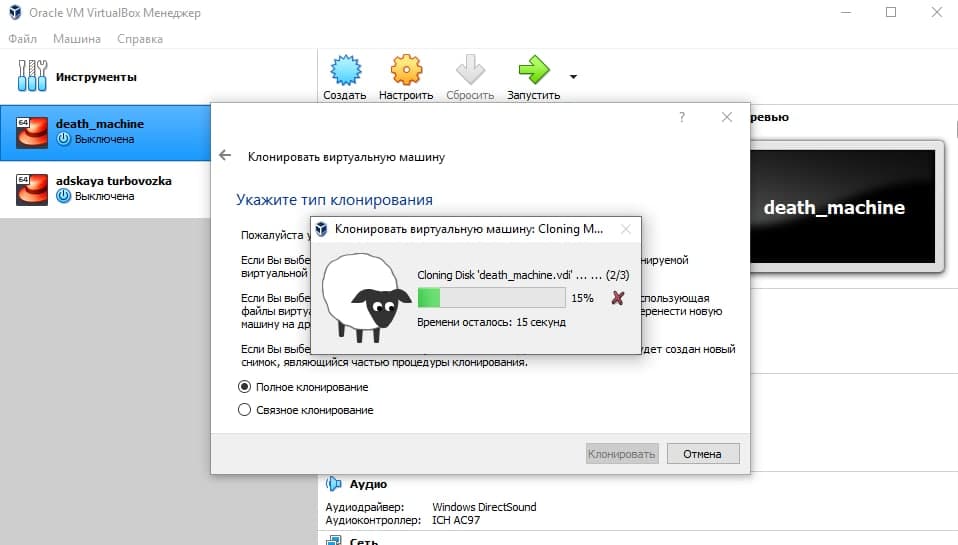
Відкриваємо середовище VirtualBox.



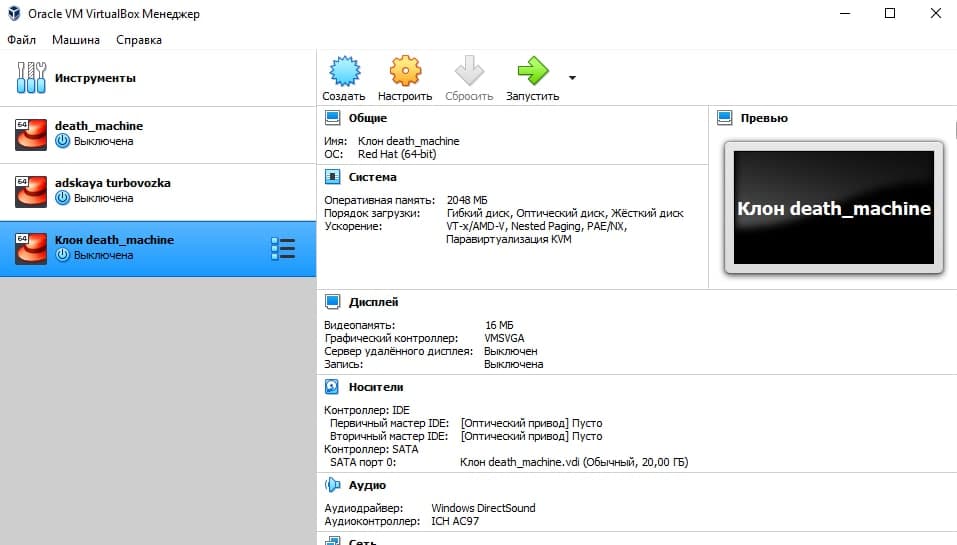
Нажимаємо правою кнопкою мищі на машину яку хочемо скопіювати і вибираємо кнопку «Копіювати».



Вводимо ім’я машини та вибираємо шлях де буде створена копія.

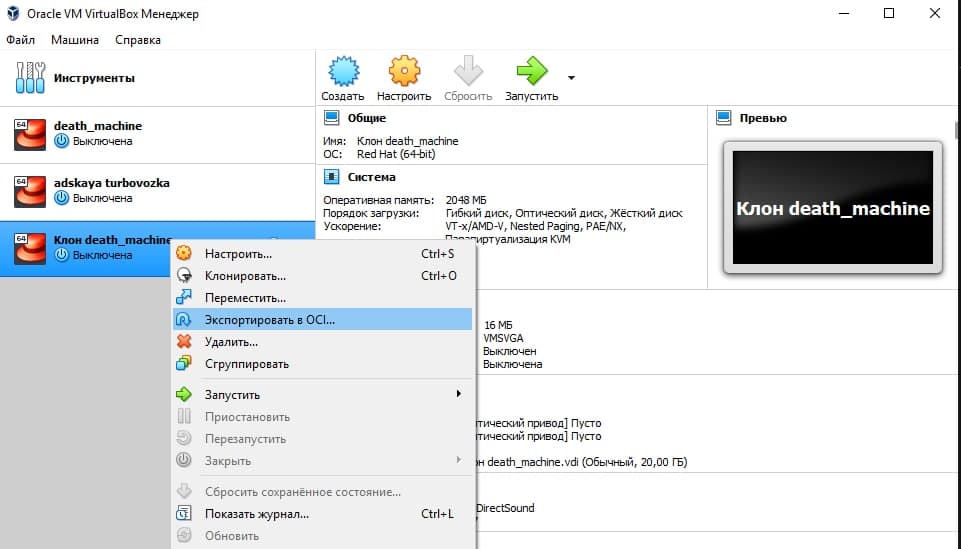


Вибираємо повне копіювання.

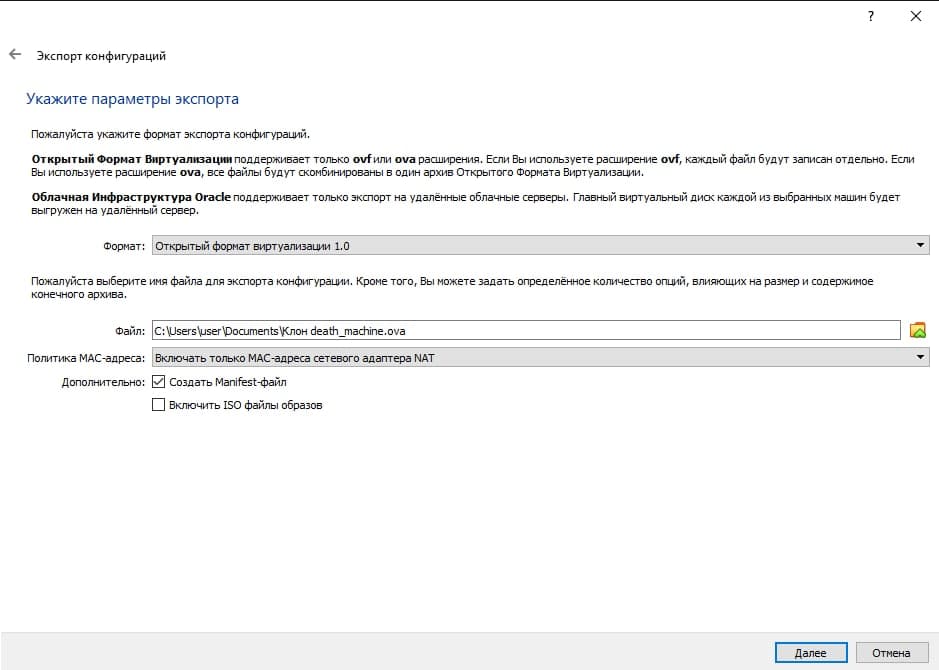


Копія створена.

Для експорту:



Правою кнопкою на потрібну машину, вибрати «експорт».



Налаштувати небхідні параметри.

**Трансляція мережевих адрес (NAT)**

Протокол NAT дозволяє гостьовій операційній системі виходити в Інтернет, використовуючи при цьому приватний IP, який не доступний з боку зовнішньої мережі або для всіх машин локальної фізичної мережі. Таке мережеве налаштування дозволяє відвідувати web-сторінки, завантажувати файли, переглядати електронну пошту. І все це, використовуючи гостьову операційну систему. Однак, ззовні неможливо безпосередньо з'єднатися з такою системою, якщо вона використовує NAT.

Принцип трансляції мережевих адрес полягає в наступному. Коли гостьова ОС відправляє пакети на конкретну адресу віддаленої машини в мережі, сервіс NAT, що працює під VirtualBox, перехоплює ці пакети, витягує з них сегменти, що містять адресу пункту відправки (IP-адреса гостьової операційної системи) і здійснює їх заміну на IP- адреса машини-хоста. Потім знову упаковує їх і відправляє за вказаною адресою.

Наприклад, у вашій домашній локальній мережі хост та інші фізичні мережеві пристрої мають адреси в діапазоні, що починається з 192.168.х.х. У VirtualBox адаптери, що працюють за протоколом NAT, мають IP-адреси в діапазоні, що починається з 10.0.2.1 і закінчується 10.0.2.24. Такий діапазон називається підмережею. Як правило, цей діапазон не використовується для присвоєння адрес пристроям в основній мережі, тому така система недоступна ззовні з боку хоста. Гостьова ОС може виконувати оновлення програмного забезпечення та web-серфінг, але залишається невидимою для решти "учасників".

У посібнику VirtualBox цей момент описаний докладніше:

"У режимі NAT гостьовому мережному інтерфейсу присвоюється за замовчуванням IPv4 адреса з діапазону 10.0.х.0/24, де х позначає конкретну адресу NAT-інтерфейсу, що визначається за формулою +2. Таким чином, х дорівнюватиме 2, якщо є тільки один активний NAT-інтерфейс: У цьому випадку гостьова операційна система отримує IP-адресу 10.0.2.15, мережному шлюзу призначається адреса 10.0.2.2, серверу імен (DNS) призначається адреса 10.0.2.3." (Oracle Corporation, 2012, Розділ 9).

Протокол NAT корисний у тому випадку, коли немає різниці в тому, які IP-адреси використовуватимуть гостьові ОС на віртуальній машині, оскільки всі вони будуть унікальними. Однак, якщо потрібно налаштувати перенаправлення мережного трафіку, або ж розширити функціональність гостьової ОС, розгорнувши на ній web-сервер (наприклад), необхідні додаткові налаштування. У режимі NAT також недоступні такі можливості, як надання спільного доступу до папок та файлів.

**Мережевий міст (Bridged)**

У з'єднанні типу "Мережевий міст" віртуальна машина працює так само, як і решта комп'ютерів у мережі. У цьому випадку адаптер виступає в ролі моста між віртуальною та фізичною мережами. З боку зовнішньої мережі є можливість безпосередньо з'єднуватися з гостьовою операційною системою.

Адаптер у режимі "Мережевий міст" підключається, минаючи хост, до пристрою, який розподіляє IP-адреси всередині локальної мережі для всіх фізичних мережевих карток. VirtualBox з'єднується з однією із встановлених мережевих карток і передає пакети через неї безпосередньо; виходить робота мосту, яким передаються дані. Як правило, адаптер у моделі "Мережевий міст" отримує стандартну адресу з діапазону 192.168.х.х від роутера. Тому віртуальна машина в мережі виглядає так, ніби це звичайний фізичний пристрій, який не відрізняється від інших.

**Віртуальний адаптер хоста (Host-only)**

При підключенні типу "Віртуальний адаптер хоста" гостьові ОС можуть взаємодіяти між собою та з хостом. Але все це тільки всередині самої віртуальної машини VirtualBox. У цьому режимі адаптер хоста використовує свій власний, спеціально для цього призначений пристрій, який називається vboxnet0. Також їм створюється підмережа і призначаються IP-адреси мережевим картам гостьових операційних систем. Гостьові ОС що неспроможні взаємодіяти з пристроями, що у зовнішньої мережі, оскільки де вони підключені до неї через фізичний інтерфейс. Режим "Віртуальний адаптер хоста" надає обмежений набір служб, корисних для створення приватних мереж під VirtualBox для гостьових ОС.

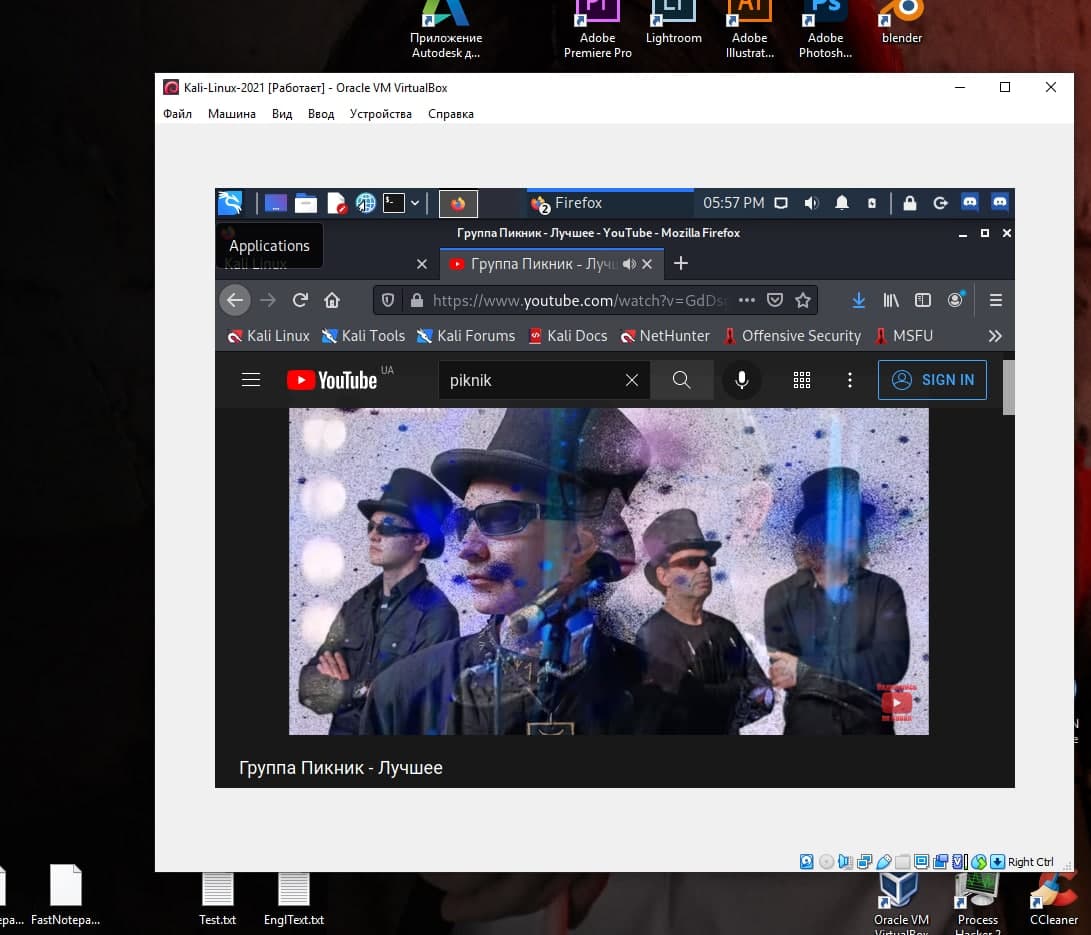
На відміну від інших продуктів віртуалізації, адаптер, що працює під протоколом NAT у VirtualBox, не може виступати в ролі сполучного моста між мережевим пристроєм за умовчанням на хостах. Тому неможливий прямий доступ ззовні до машин, "захованих" за NAT - ні до програм, що працюють на них; ні до даних, що знаходяться на самих хостах.

**Внутрішня мережа (Internal Network)**

Якщо на практиці вам знадобиться налагодити взаємозв'язок між декількома гостьовими операційними системами, що працюють на одному хості та можуть спілкуватися лише між собою, тоді можна скористатися режимом "Внутрішня мережа". Звичайно, для цієї мети можна використовувати режим "Мережевий міст", але режим "Внутрішня мережа" має більшу безпеку. У режимі "Мережевий міст" усі пакети надсилаються та виходять через адаптер фізичної мережі, встановлений на машині-хості. У цьому випадку весь трафік може бути перехоплений (наприклад, шляхом встановлення сніфера пакетів на машині-хості).

Внутрішня мережа, згідно з керівництвом VirtualBox, є "програмною мережею, яка може бути видима для вибірково встановлених віртуальних машин, але не для додатків, що працюють на хості або на віддалених машинах, розташованих ззовні". Така мережа є набором з хоста і кількох віртуальних машин. Але жоден з перелічених вище пристроїв не має виходу через фізичний мережевий адаптер - він повністю програмний, що використовується VirtualBox як мережевого маршрутизатора. Загалом виходить приватна локальна мережа лише для гостьових операційних систем без доступу до Інтернету, що робить її максимально безпечною. Можливе застосування такої мережі – надсекретний сервер із клієнтами, призначений для розробки; тестування систем на проникнення або будь-які інші цілі, що мають створення внутрішньої мережі для команд-розробників або організацій. Це ідеальний спосіб для блокування оточення від неавторизованої установки програмного забезпечення, завантаження чи закачування файлів, відвідування сервісів типу Facebook у робочий час.

Отже, ми розглянули різні типи мережевих з'єднань. Кожен з них має власні налаштування і призначений для певних цілей. Повернемося до того моменту, звідки все почалося – створення віртуального сервера для розгортання на ньому CMS Wordpress та його тестування.



Для передачі інформації між машиною-хостом та віртуальною машиною можна використати наступні типи організації мережевих з’єднань:

* Мережевий міст (Bridged);
* Віртуальний адаптер хоста (Host-only);
* Внутрішня мережа (Internal Network).