# **Модуль 1**

## **Системне адміністрування і послуги IT – інфраструктури. Вступ**

### **Вступ до курсу**

Перш ніж ми почнемо, хочу привітати вас із тим, що ви дійшли до цього етапу програми. Давайте згадаємо про навички, які ви вже опанували до цього часу. Ви вивчили основи інформаційних технологій: від того, як працює двійкова система та чому важлива підтримка користувачів, до збирання комп’ютера. Ви вивчили основи комп’ютерних мереж і дізналися, як насправді працює Інтернет. Нарешті, ви дізналися про навігацію в операційних системах Windows і Linux і навчилися керувати процесами й програмами в командному рядку, наче професіонали. Молодці!

Перш ніж зануритися в нетрі системного адміністрування й інфраструктури, я, користуючись нагодою, ще раз представлюсь для тих, хто, можливо, не пам’ятає мене з давно минулого 1-го курсу, Мене звати Деван Шрі-Таран. Я працюю у сфері ІТ вже 10 років. Я інженер із корпоративних операцій у Google, де вирішую цікаві та складні проблеми з ІТ. Якщо пригадати, то свій перший досвід роботи з технологіями я отримав приблизно в 9 років, коли мій тато приніс додому перший у нашій сім’ї комп’ютер. Пам’ятаю, як тато тримав дискету й сказав мені, що на ній була гра. На подив свого тата, я якось примудрився скопіювати гру з дискети на жорсткий диск комп’ютера. Хоча зараз це може здатися буденною справою, цей пристрій був для нас тоді абсолютно новим. Звісно, мені подобалися різні ігри, але ще більше я любив копирсатися в комп’ютері, намагаючись змусити його робити те, що я хотів. Хоча та дискета й комп’ютер запалили мою пристрасть до технологій, лише перший досвід роботи справді почав формувати мою кар’єру у сфері ІТ. Одна робота була в роздрібній торгівлі дитячими меблями, а друга – у відділенні пошти, де я допомагав клієнтам відправляти посилки і став ІТ-командою з однієї людини.

Може здатися дивним, що роздрібна торгівля надихнула мою кар’єру. але я зрозумів, що мені подобається спілкуватися з клієнтами, розуміти їх потреби та пропонувати рішення. Свій перший досвід роботи безпосередньо у сфері ІТ я отримав у коледжі під час стажування на фахівця ІТ-підтримки. Там я працював ІТ-консультантом під час виведення з експлуатації цілого середовища. Це був мій перший досвід роботи безпосередньо з великою ІТ-інфраструктурою і вихід із зони комфорту звичайного студента коледжу. Я згадую ці перші кілька своїх робіт не просто так. Цей досвід допоміг сформувати мою кар’єру у сфері ІТ. Тоді я знав, що хочу займатися технологіями, але не міг визначитись, чому саме присвятити свою кар’єру. Перша посада ІТ-фахівця широкого профілю в Google дала мені змогу випробувати себе в різних сферах технологій. Я зрозумів, якою роботою я не хочу займатися, а потім визначив, що саме я точно хотів би робити. Я справжній фанат ІТ-інфраструктури. Ця програма покликана допомогти вам підготуватися до роботи в технічній підтримці, підтримці настільних комп’ютерів чи іншій службі підтримки, але не тільки.

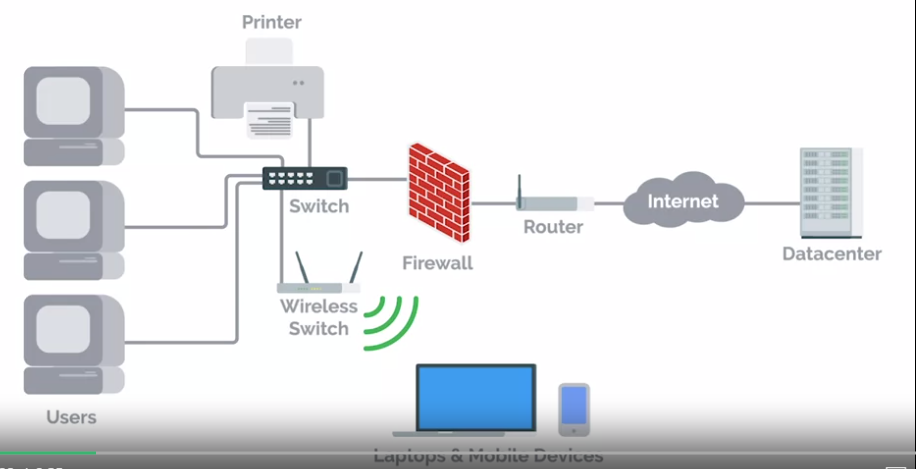
У цьому курсі ми відкриємо ще ширше коло можливостей у сфері ІТ, надавши вам необхідні навички для керування комп’ютерами цілої організації. У невеликій організації вам, можливо, доведеться робити це з першого дня. Але в будь-якому разі, ширший набір навичок виділятиме вас з-поміж інших і підготує до виконання таких завдань у подальшій кар’єрі. На цьому курсі на основі знань, які ви отримали про операційні системи, ви отримаєте навички системного адміністрування. Загалом кажучи, системне адміністрування – це галузь ІТ, що відповідає за підтримку надійних комп’ютерних систем у багатокористувацькому середовищі. Обов’язки в системному адмініструванні можуть частково збігатися з іншими роботами у сфері ІТ, але людина, яка працює лише в цій сфері, є системним адміністратором. Системні адміністратори мають різноманітний набір ролей і обов’язків. Це може бути налаштування серверів, контроль мереж, виділення ресурсів, налаштування комп’ютерів для нових користувачів тощо. Уявляйте, що системний адміністратор – це технічний універсал. Він робить багато різних речей, щоб забезпечувати роботу організації. Це насправді дуже схоже на те, як працюють фахівці з ІТ-підтримки. Ви маєте застосовувати широкий набір технічних навичок у різних ситуаціях, щоб вирішувати проблеми в організації. Завдання із системного адміністрування можуть теж належати до обов’язків фахівця з ІТ-підтримки. Отже, ми представимо вам навички та знання, необхідні для керування організаціями й системами, щоб ви були універсальним фахівцем.

На цьому курсі ви дізнаєтеся, які сервіси використовуються в інфраструктурі. Ви також отримаєте базові знання з використання ПЗ в організації й навчитеся керувати користувачами й комп’ютерами всієї організації за допомогою служб каталогів. Нарешті, ви отримаєте навички, необхідні для резервного копіювання даних організації та їх відновлення в разі аварії. Гаразд, час починати. До справи!

## **Що таке системне адміністрування**

### **Що таке системне адміністрування?**

Перш ніж перейти до визначення адміністрування систем,  слід поговорити, про які саме системи йдеться. Усі процеси в організації не виконуються самі собою. Працівникам потрібні комп’ютери з доступом до Інтернету, щоб взаємодіяти з клієнтами. Сайти організації мають працювати.  Мають спільно використовуватися брандмауери. І ще багато чого.



Усі ці вимоги разом складають ІТ-інфраструктуру організації. ІТ-інфраструктура охоплює програмне й апаратне забезпечення, мережу й сервіси, необхідні для роботи організації в корпоративному ІТ-середовищі. Без ІТ-інфраструктури працівники не змогли б виконувати свою роботу й уся компанія збанкрутувала б, навіть не встигнувши відкритись. Тож організації користуються допомогою так званого системного адміністратора, який керує ІТ-інфраструктурою компанії. Системні адміністратори або, як ми їх звикли називати, "сисадміни" – неоспівані герої будь-якої організації. Вони непомітно працюють, дбаючи про безперебійну роботу ІТ-інфраструктури компанії, постійно борються, щоб запобігати аваріям у сфері ІТ. Звертайте увагу на ту важку роботу, яку виконують системні адміністратори. На знак вдячності сисадмінам весь світ відзначає День вдячності системним адміністраторам. Так, це реальний факт. Але якщо серйозно, то в сисадмінів дуже багато різних обов’язків. Будь-якій компанії, що використовує ІТ, потрібен системний адміністратор або хтось, хто виконуватиме ці обов’язки. Роль сисадміна може варіюватися залежно від розміру організації. Коли організація росте, їй стають потрібні цілі команди сисадмінів. Їхні обов’язки можуть бути розділені між кількома посадами (наприклад: адміністратори мереж і адміністратори баз даних). У таких компаніях, як Facebook і Apple, далеко не одна людина відповідає за ІТ. Але в менших компаніях усією ІТ-інфраструктрою зазвичай керує одна людина. У цьому курсі ми зосередимося на тому, як лише одна людина (тобто ви) може одноосібно керувати ІТ-інфраструктурою. Ви здобуте навички, необхідні для керування організацією з менше ніж 100 працівників як єдиний ІТ-фахівець. Коли ви почнете працювати у великих організаціях, вам знадобиться поглибити знання в системному адмініструванні. Ви маєте здобути навички, які дозволять автоматизувати робочі процеси й керувати конфігураціями чи параметрами автоматично. А зараз ми зосередимося на системному адмініструванні в невеликій організації. На кількох наступних уроках ми детально поговоримо про обов’язки системного адміністратора і як це пов’язано з роботою фахівця з ІТ-підтримки, який займається адмініструванням систем.

### **Повторення про сервери**

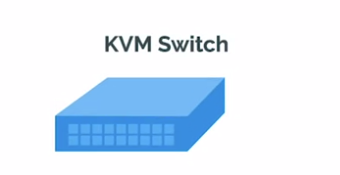
По суті, системний адміністратор відповідає за ІТ-сервіси своєї компанії. Ці ІТ-сервіси потрібні працівникам, щоб ефективно виконувати роботу. Це, зокрема, електронна пошта, сховище файлів, робота сайту тощо. Сервіси мають десь зберігатися, вони не беруться з нізвідки. Здогадаєтесь, де вони зберігаються? Якщо ви відповіли "сервери", ви маєте рацію. Ми говорили про сервери на одному з попередніх курсів, і ви дізналися, що термін "сервер" має кілька значень. На одному з курсів ми говорили, як сервери зберігають вебконтент, який передають на інші комп’ютери. На іншому курсі ми говорили, що сервери можуть бути програмами, які виконують певну функцію. У цьому відео ми поговоримо про сервери докладніше, бо в багатьох випадках системні адміністратори відповідають за обслуговування всіх серверів компанії. Якщо ви працюєте фахівцем з ІТ-підтримки й маєте обов’язки адміністрування систем, вам знадобиться виконувати подібні завдання.

По суті, сервер – це програмне забезпечення або комп’ютер, що надає сервіси іншому ПЗ чи комп’ютерам. Наприклад, вебсервер зберігає та надає клієнтам контент через Інтернет. Доступ до вебсервера можна отримати за допомогою доменного імені, як-от google.com. Вебсервери ми докладно розглянемо пізніше. А зараз розгляньмо деякі інші приклади серверів. Сервер електронної пошти надає сервіс електронної пошти іншим комп’ютерам. SSH-сервер надає SSH-сервіси іншим комп’ютерам тощо. Комп’ютери, що користуються сервісами, які надає сервер, називаються клієнтами. Клієнти запитують сервіси із сервера, а сервери, у свою чергу, у відповідь надають такі сервіси. Сервер може надавати сервіси декільком клієнтам одночасно, а клієнт може використовувати кілька серверів.

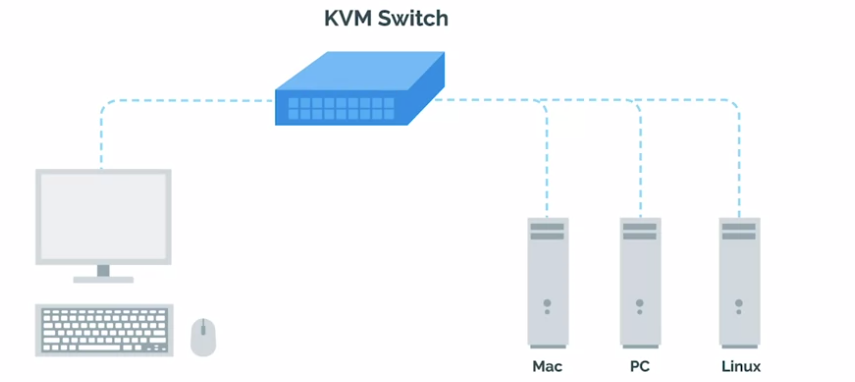
Будь-який комп’ютер може бути сервером. Я можу запустити вебсервер на своєму домашньому комп’ютері, що обслуговуватиме для мене мій особистий сайт. Але я не дуже хочу це робити, тому що мій комп’ютер має бути завжди ввімкнений, щоб мій сайт був постійно доступний. Стандартні сервери в галузі зазвичай працюють у режимі 24/7 і далеко не на таких маленьких пристроях, як мій домашній ноутбук. Вони працюють на дуже потужному й надійному обладнанні. Серверне обладнання може мати багато різних форм. Це можуть бути вертикальні баштові корпуси, дуже подібні до звичайних настільних комп’ютерів. Ці башти можна вмонтувати в шафу або за бажання встановити на стіл. Але що, якщо вам потрібно 10 серверів? Башти б почали займати занадто багато місця. Натомість, ви можете використовувати стійкові сервери, які мають пласку форму й зазвичай встановлюються в серверну стійку шириною 90 дюймів. Якщо вам потрібно ще більше місця, можна використовувати блейд-сервери, які ще тонші, ніж стійкові.



Існують також інші форм-фактори серверів, але це найпоширеніші. Ви можете адаптувати апаратне забезпечення сервера до певних сервісів. Наприклад, на файловому сервері вам потрібно більше ресурсів пам’яті, щоб зберігати більше файлів. А як щодо підключення до наших серверів? Працюючи в невеликій ІТ-організації, ви, мабуть, матимете справу з малою кількістю серверів. Ви ж не хочете мати монітор, клавіатуру й мишу для кожного з цих серверів? На щастя, це й не потрібно завдяки тому, що ми вивчали на попередньому курсі. Ми можемо віддалено підключатися до серверів за допомогою SSH. Однак, ви завжди повинні мати під рукою клавіатуру для монітора. Іноді під час роботи можуть виникати проблеми в мережі, і тоді SSH не зможе працювати. У таких випадках прийнято використовувати так званий KVM-перемикач.



KVM – це абревіатура, що означає "клавіатура, відео та миша". На вигляд KVM-перемикач – це концентратор, до якого можна підключити кілька комп’ютерів і керувати ними за допомогою однієї клавіатури, миші й монітора.



Про використання KVM можна прочитати в наступному довідковому матеріалі. Тепер, коли ми краще розуміємо, що таке сервери та які функції вони виконують, ви можете купувати серверне обладнання й налаштовувати сервіси для своєї організації. А можливо, і ні. Насправді не треба купувати власне серверне обладнання чи навіть підтримувати власні сервіси. У наступному відео ми дізнаємося про нову хвилю в комп’ютерних обчисленнях, яка почала захоплювати світ ІТ, – хмарні обчислення. До зустрічі!

<https://en.wikipedia.org/wiki/KVM_switch>

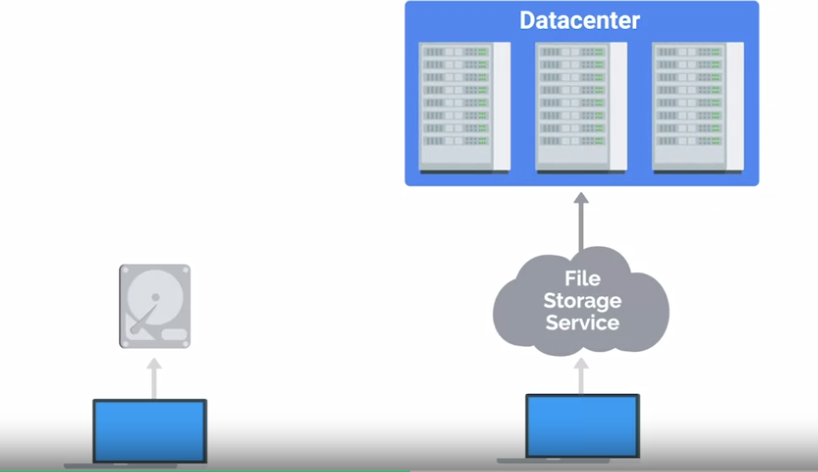
### **Хмара**

О, хмара, чудова чарівна хмара, про яку ви чуєте з новин і яка переміщує дані через пухкі білосніжні вікна в небі. Чарівна хмара розкидала по всьому світу біти даних, неначе краплинки, чи не так? Ні, насправді хмара працює зовсім не так, але вас здивує, як багато людей у це вірять. Без сумніву, ви чули термін "хмара" в новинах або від інших людей. Ваші фото зберігаються в хмарі, електронна пошта зберігається в хмарі. Хмарні обчислення – це концепція, яка дає вам змогу отримувати доступ до даних, користуватися додатками, зберігати файли тощо в будь-якій точці світу, за умови, що у вас є інтернет-з’єднання.

Але хмара – це не щось магічне. Це просто мережа серверів, що зберігають і обробляють наші дані. Можливо, ви вже чули про "центри обробки даних"? Центр обробки даних – це об’єкт, де зберігаються сотні, якщо не тисячі серверів. Компанії з великими обсягами даних мають зберігати свою інформацію в центрах обробки даних. Великі компанії, як-от Google і Facebook, зазвичай мають власні центри обробки даних, бо мільярдам їхніх користувачів потрібен постійний доступ до своїх даних. Менші компанії теж могли б це робити, але зазвичай орендують частину центру обробки даних для своїх потреб.

Коли ви користуєтеся хмарним сервісом, ці дані зазвичай зберігаються в одному чи кількох центрах обробки даних, достатньо великих, щоб зберігати інформацію мільйонів або навіть мільярдів користувачів. Легко зрозуміти, чому хмара стала популярним способом комп’ютерних обчислень за останні кілька років.

Тепер, замість того щоб тримати терабайти пам’яті на ноутбуці, ви можете завантажити свої дані в сервіс зберігання файлів, як-от Dropbox, який зберігає ці дані в керованому об’єкті на кшталт центру обробки даних.



Те саме стосується вашої організації. Замість того, щоб керувати власними серверами, можна використовувати вебсервіси, які роблять усе за вас: оновлюють систему безпеки, надають серверне обладнання, регулярно оновлюють ПЗ тощо. Але кожен із цих варіантів має певні недоліки.

Перший – це вартість. Коли ви купуєте сервер, ви сплачуєте за обладнання наперед. У такому разі ви можете налаштувати свої сервіси, як-от файлове сховище, за потенційно дуже невеликі кошти, адже саме ви ним керуєте. Коли ж ви використовуєте такі вебсервіси, як Dropbox, які пропонують зберігання файлів онлайн, початкові витрати можуть бути невеликими. Але в довгостроковій перспективі витрати можуть зростати, адже ви сплачуєте фіксовану суму щомісяця. Порівнюючи вартість сервісів, завжди враховуйте, скільки коштуватиме підписка кожного користувача у вашій організації. Порівняйте це з вартістю утримання власного обладнання в довгостроковій перспективі та прийміть оптимальне рішення для організації.

Другий недолік – залежність. Ваші дані залежать від цих платформ. Якщо із сервісом виникне проблема, хтось інший відповідатиме за її вирішення, а не ви. Це може коштувати вашій компанії істотної втрати продуктивності й даних. Незалежно від того, який спосіб ви оберете, пам’ятайте, що ви все одно нестимете відповідальність за проблеми в разі неполадок. Якщо в Dropbox виникає проблема з важливими даними користувачів, це й надалі ваша проблема й ви маєте відновити роботу, хай там що. Щоб запобігти виникненню подібної ситуації, можна створити резервну копію критично важливих даних у хмарі й на фізичному диску. Тоді в разі збою однієї із систем у вас буде інший спосіб вирішити проблему.

Незалежно від того, що ви виберете, – фізичні сервери чи хмарні сервіси, – вам слід зважати на ці моменти, плануючи надання послуг вашій компанії.

На кількох наступних уроках ми поговоримо про деякі інші обов’язки системного адміністратора. Спочатку ми розглянемо їх загалом, а пізніше розберемо подробиці.

## **Завдання системного адміністратора**

### **Організаційні політики**

У невеликій компанії зазвичай саме системний адміністратор відповідає за вибір комп’ютерної політики. У великих компаніях із сотнями чи тисячами працівників ці обов’язки зазвичай виконує директор із питань безпеки. Але на менших підприємствах системний адміністратор має ретельно дбати про комп’ютерну безпеку та вирішувати, чи надавати доступ певним користувачам.

Під час налаштування ІТ часто виникає кілька поширених запитань, на які ви маєте відповісти. Чи дозволяти користувачам встановлювати ПЗ? Мабуть, ні. Існує ризик, що користувач може випадково встановити шкідливу програму, про що ми поговоримо на майбутньому курсі з безпеки. Чи повинні користувачі мати складні паролі з певними вимогами? Безумовно, це корисне правило, щоб пароль був складним і містив символи, випадкові числа й літери. Бажано встановити правило, що пароль має складатися з мінімум 8 символів, адже тоді його буде важче зламати. Чи можуть користувачі переглядати сайти, не пов’язані з роботою, як-от Facebook? Це особистий вибір. Деякі організації воліють, щоб працівники використовували свої робочі комп’ютери та мережу виключно для бізнесу, але багато хто дозволяє й інші застосування, щоб працівники могли просувати бізнес чи товари компанії в соціальних мережах, були в курсі поточних подій тощо.

Звісно, таке правило ви можете встановлювати разом із керівництвом своєї організації. Якщо ви видаєте працівнику робочий телефон, чи слід встановлювати пароль на пристрій? Безсумнівно. Люди часто гублять мобільні пристрої. Якщо пристрій буде втрачено або вкрадено, він має бути щонайменше захищений паролем, щоб хтось інший не зміг легко прочитати електронну пошту компанії.

Про вплив і наслідки правил щодо безпеки в організації ми поговоримо на останньому курсі цієї програми, присвяченому безпеці. Це лише кілька запитань, які можуть виникнути стосовно правил безпеки. Усі правила, що встановлюються, мають десь документуватися. Ви вже знаєте з уроку про документацію з першого курсу, що вести належну документацію критично важливо. Якщо ви керуєте системами, ви відповідаєте за документування правил своєї компанії, стандартних процедур тощо. Цю документацію можна зберігати на внутрішньому довідковому сайті, у файловому сервері, в програмному забезпеченні тощо. Найважливіше – це те, що наявність доступної документації правил допоможе працівникам їх вивчати й дотримуватися.

### **Послуги ІТ-інфраструктури**

Ми трохи поговорили про сервіси, які можуть використовуватися в організації, як-от сховище файлів, електронна пошта, вебконтент тощо. Але є й багато інших інфраструктурних сервісів, про які потрібно знати. Як фахівець з ІТ-підтримки, який займається системним адмініструванням, ви відповідатимете за сервіси ІТ-інфраструктури в організації. Увага, спойлер: попереду їх буде ще дуже багато. Як завжди, обов’язково переглядайте уроки, якщо вам потрібно більше часу на засвоєння матеріалу. Рим будувався не один день. Те ж саме стосується фахівців з ІТ-підтримки.

Візьмімо, наприклад, доступ до мережі. Це сервіс, яким потрібно керувати. А як щодо безпечного з’єднання з сайтами й іншими комп’ютерами? Як ви, мабуть, здогадалися, це також сервіс, яким потрібно керувати. Керування сервісами – це не просто їх налаштування. Їх потрібно регулярно оновлювати, усувати вразливості безпеки та дбати про сумісність із комп’ютерами в організації. Пізніше в цьому курсі ми детальніше розглянемо основні інфраструктурні сервіси, з якими ви можете мати справу як фахівець з ІТ-підтримки.

### **Обслуговування користувачів та апаратного забезпечення**

Ще один обов’язок системних адміністраторів – керувати користувачами й апаратним забезпеченням. Системні адміністратори мають уміти створювати нових користувачів і надавати їм доступ до ресурсів своєї компанії. З іншого боку, вони також мають видаляти користувачів з ІТ-інфраструктури, коли ті звільняються з компанії. Вони мають дбати не лише про облікові записи користувачів. Системні адміністратори відповідають також за комп’ютери користувачів. Вони мають дбати про те, щоб користувач міг увійти в систему, а на комп’ютері було потрібне програмне забезпечення, щоб користувач міг ефективно працювати. Системні адміністратори також мають контролювати, щоб обладнання, яке вони надають або налаштовують для користувачів, було певним чином стандартизоване.

На попередньому курсі ми говорили про створення однакових образів комп’ютерів. Це стандартна практика в роботі з багатокористувацькими середовищами. Системні адміністратори мають не лише стандартизувати налаштування комп’ютера, але й визначати життєвий цикл його апаратного забезпечення. Вони часто думають про життєвий цикл апаратного забезпечення комп’ютера в буквальному сенсі. Коли його випущено? Коли його вперше використали? Організація купила його новим або вживаним? Хто його раніше обслуговував? Скільки користувачів працювало на ньому в поточній організації? Що буде з цим комп’ютером, якщо комусь знадобиться новий? Це всі хороші запитання, які слід ставити, думаючи про технології в організації.

Системні адміністратори не хочуть мати в організації 10-річний комп’ютер. А можливо, й хочуть. Навіть з цього приводу вони мають прийняти рішення. Є чотири основні етапи життєвого циклу апаратного забезпечення. **Придбання. На цьому етапі обладнання купується чи знову використовується для працівника**. **Розгортання. Тут обладнання налаштовується, щоб працівник міг виконувати свою роботу**. **Обслуговування. Це етап, на якому оновлюється програмне забезпечення й вирішуються можливі проблеми з апаратним забезпеченням. Списання.**

На цьому останньому етапі обладнання стає непридатним чи непотрібним, і його слід належним чином вилучити з використання. У невеликій організації типовий життєвий цикл обладнання приблизно такий. Спочатку компанія наймає нового працівника. Відділ кадрів просить вас надати йому комп’ютер і налаштувати обліковий запис. Далі ви виділяєте комп’ютер зі своїх запасів або за потреби замовляєте новий. Виділяючи обладнання, вам, можливо, доведеться позначити комп’ютер стікером, щоб користувач завжди знав, що це - майно організації. Далі можна завантажити на комп’ютер базовий образ для використання оптимізованого методу, який ми розглядали в останньому курсі "Операційні системи й ви". Потім ви даєте комп’ютеру ім’я, що містить стандартне ім’я хосту. Це допомагає керувати комп’ютерами. Ми розглянемо це пізніше, коли вивчатимемо служби каталогів.

Щодо самого імені, ми говорили про такий формат, як ім’я користувача-розташування, але можна використовувати й інші імена хостів. Докладніше про це читайте в довідковому матеріалі. Після цього ви встановлюєте на комп’ютер користувача необхідне програмне забезпечення. Потім новий працівник приступає до роботи, а ви оптимізуєте для нього процес налаштування, даючи вказівки, як увійти в новий комп’ютер, отримати електронну пошту тощо. Якщо на комп’ютері виникає помилка обладнання, тобто неполадка, ви вивчаєте її й плануєте наступні дії. Якщо комп’ютер застарів, вам слід визначити, де його утилізувати й де отримати нове обладнання. Нарешті, якщо користувач звільняється, вам потрібно заблокувати його доступ до ІТ-ресурсів і видалити всі дані з комп’ютера, щоб пізніше ви могли надати його комусь іншому.

Завантаження образу, встановлення програмного забезпечення й налаштування нового комп’ютера можуть забирати трохи часу. У невеликій компанії ви не робитимете це часто, тож це не настільки критично. Але у великій компанії ви не впораєтесь із такими тривалими процесами. Вам доведеться опанувати автоматизовані способи виділення нових комп’ютерів, щоб витрачати на це лічені хвилини, а не години.

### **Регулярне технічне обслуговування**

Коли ви керуєте комп’ютерами для компанії, ви не можете їх просто налаштувати й забути. Їх потрібно оновлювати й обслуговувати, щоб на них працювали найновіші й надійні програми. Коли ви робите це для цілого парку комп’ютерів, небажано одразу встановлювати оновлення, щойно вони з’являються. Це б займало забагато часу. Натомість, щоб ефективно оновлювати обладнання й керувати ним, використовується так зване "групове оновлення". Це означає, що приблизно раз на місяць ви встановлюєте на всіх серверах останні оновлення системи безпеки. Ви маєте знайти час, щоб перевести відповідні сервіси в режим офлайн, установити оновлення та переконатися, що вони належно працюють із сервісом. Також не потрібно виконувати оновлення щоразу, коли з’являється нове програмне забезпечення. Натомість, прийнято виконувати групове оновлення для систем безпеки і критично важливих оновлень системи. У курсі щодо безпеки ми докладніше розглянемо методи контролю безпеки, але раджу вам дбати про безпеку системи, регулярно встановлюючи останні оновлення системи безпеки. Підтримувати найвищий рівень безпеки – завжди хороша ідея.

### **Постачальники**

Системні адміністратори в невеликих компаніях працюють не лише з комп’ютерами. Вони мають справу також із принтерами й телефонами. Використовують працівники мобільні чи стаціонарні телефони, їхні телефонні лінії потрібно налаштувати. Принтери досі використовуються в компаніях, тож їх потрібно налаштовувати для роботи. Системні адміністратори можуть відповідати за забезпечення роботи принтерів або, якщо орендується комерційний принтер, вони мають викликати в офіс того, хто може усувати неполадки.

Що робити, якщо в компанії не працює факс?

Якщо ви не знаєте, що таке факс, це зовсім не дивно. Вони поступово відходили в минуле з часу винайдення електронної пошти. Факсимільні апарати досі працюють у компаніях і вони – це справжній головний біль. І за них теж відповідають системні адміністратори. Пристрої для відео- й аудіоконференцій – так, з ними теж доведеться мати справу. На підприємстві системні адміністратори, так чи інакше, мають забезпечувати таке обладнання. Зазвичай вони співпрацюють із постачальниками або іншими компаніями для його придбання.

Налаштування робочих облікових записів за допомогою таких постачальників, як Hewlett Packard, Dell, Apple тощо, зазвичай є вигідним, адже ці компанії можуть пропонувати знижки для бізнесу. Це те, про що має думати системний адміністратор. Якщо просто купувати пристрої на Amazon, це зазвичай неможливо масштабувати. Хоча, якщо буде прийнято таке рішення, сисадмін може вчинити й так.

Системні адміністратори мають зважувати варіанти перед будь-якою покупкою. Вони мають думати про постачання обладнання. Так, якщо певна модель ноутбука більше не використовується, вони мають подумати про відповідний резервний пристрій для організації. Також потрібно враховувати ціну. Щоб установити подібні відносини з постачальником, імовірно, знадобиться формальне схвалення керівника чи когось із начальства.

Системний адміністратор має думати не лише про технічну реалізацію апаратного забезпечення.

Є й багато інших речей.

### **Усунення несправностей і врегулювання проблем**

Ми багато говорили про вирішення проблем на одному з попередніх курсів, але варто зазначити ще раз: якщо ви керуєте всією ІТ-інфраструктурою, вам постійно доведеться вирішувати проблеми й знаходити рішення для своїх ІТ-потреб. Це, ймовірно, займатиме більшу частину вашого часу як фахівця з ІТ-підтримки. Це може бути окремий клієнтський комп’ютер працівника або сервер чи сервіс, що працює не належним чином.

Дехто, починаючи кар’єру в ІТ-підтримці, поглиблює свої знання, щоб стати системним адміністратором. Він переходить від роботи з одним комп’ютером до роботи з багатьма. Щодо мене, я зробив великий стрибок під час стажування на посаді фахівця з ІТ-підтримки в коледжі в лабораторії напівпровідників. Лабораторія зрештою закрилася, і потрібна була допомога зі згортанням середовища. Отже, з роботи в службі ІТ-підтримки я швидко перейшов на рівень помічника адміністратора. Ця можливість стала моїм золотим квитком у світ Active Directory, підмереж і прийняття рішень, що є основою цієї роботи. Сисадмінам доводиться також вирішувати проблеми й визначати їх пріоритетність у більшому масштабі. Якщо сервер, яким керує сисадмін, припиняє надавати сервіси тисячам користувачів, а якась одна людина має проблему з принтером, над чим, на вашу думку, потрібно попрацювати насамперед? Яким би не був сценарій, є дві критично важливі навички, щоб прийняти правильне рішення для користувачів. Ми вже говорили про них в одному з попередніх курсів. Знаєте, які це навички? Перша – вирішення проблем. Постановка запитань, ізолювання проблеми, відстеження симптомів і читання журналів – ось найкращі способи з’ясувати проблему. Можливо, вам доведеться читати журнали з кількох комп’ютерів чи з усієї мережі. Ми трохи говорили про централізоване ведення журналів в останньому курсі на тему "Операційні системи й ви" – "Як стати досвідченим користувачем". Щоб пригадати, як працює централізоване ведення журналу, перегляньте довідковий матеріал. Так чи інакше, друга надважлива навичка, яку ми розглядали, – це обслуговування клієнтів. Демонстрація емпатії, використання правильного тону голосу та правильна поведінка в складних ситуаціях – ці навички вкрай важливі на будь-якій роботі у сфері ІТ. У деяких компаніях сисадміни мають бути доступні цілодобово. Якщо сервер або мережа перестають працювати серед ночі, має бути хтось, хто зможе їх полагодити. Але не хвилюйтеся! Сисадмін не має не спати й бути доступним у режимі 24/7. Він може контролювати сервіс, який сповістить його в разі проблеми. Отже, як контролювати вирішення проблем? Загальноприйнятий спосіб – використання системи запитів або реєстрації помилок. Користувачі можуть надсилати запити на допомогу щодо проблеми, а ви можете відстежувати свою роботу з її вирішення в системі запитів. Це допомагає упорядковувати, визначати пріоритет проблем і документувати вжиті заходи. На цьому курсі ми познайомимось із сервісами, які має забезпечувати системний адміністратор, і з його обов’язками в організації. Я також дам вам кілька порад із вирішення проблем у сфері системного адміністрування. Якщо ви працюєте фахівцем з ІТ-підтримки, системне адміністрування може стати частиною вашої роботи. Тож це допоможе вам осягнути всі аспекти керування ІТ-інфраструктурою в організації. Що якісніше ви підготовлені, то краще.

### **У разі пожежі розбийте скло**

Поговорімо трохи про неприємне, а саме про аварії. Подобається це чи ні, але іноді щось перестає працювати, як би ретельно ви все не спланували. Це відбувається як у малих, так і у великих компаніях. Шанси завжди однакові. Ви не можете передбачити все, але ви можете бути готові виправити помилку. Як?

Дуже важливо забезпечити регулярне резервне копіювання даних компанії в певне місце. Бажано, щоб воно було далеко від поточного місцезнаходження. Що, якщо на вашу будівлю обрушиться буревій і ваші резервні копії зникнуть? У вас більше не буде офісної будівлі, не кажучи вже про те, що ви не зможете відновити свої дані й повернути людей до роботи. Пізніше на цьому курсі ми докладніше обговоримо можливі способи резервного копіювання даних організації та їх відновлення після аварії. Поки що не будемо надто ускладнювати собі життя. Ви вже багато дізналися про ролі й обов’язки системного адміністратора. Дещо з цього може здаватися складною роботою. Дещо навіть може лякати. Нести відповідальність за збереження даних нелегко. Але це престижна роль у сфері ІТ, і ви вже здобуваєте необхідний набір навичок із системного адміністрування, вивчаючи основи ІТ-підтримки. Далі на вас чекає тест.

### **Діон: зустріч із Мішель Обамою**

Мене звати Діон Пол, і я фахівець з операцій у команді з керування ризиками в gTech. gTech означає Google Technical Services. Я не завжди був ІТ-фахівцем. Та чи взагалі можливо знати все в цій сфері? Я для себе усвідомив одне: знань ніколи не буде забагато. Немає межі навчанню. Усе завжди змінюється, особливо у сфері ІТ, тому так важливо постійно вчитися, бути в курсі останніх технологій, куди б це тебе не привело. Я ніколи не перестану вчитися. І я завжди охоче вивчатиму нові речі й застосовуватиму їх у різні способи. Найбільш пам’ятним моментом у моїй кар’єрі було знайомство з тодішньою першою леді Мішель Обамою під час робочої поїздки. Мене вибрали для участі в проєкті в Білому домі з огляду на те, чим займалася моя команда. І нам вдалося не лише залучити її до зйомок у віртуальній реальності, я ще повинен був забезпечити роботу цього обладнання, поставивши його просто перед нею. І цей контент мали побачити мільйони дітей по всьому світу. Можливість керувати камерою з першою леді просто навпроти мене – це момент, який я ніколи не забуду.

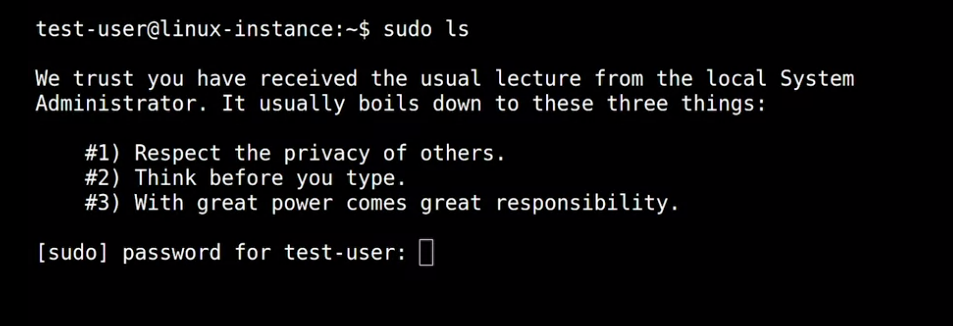
Для мене успіх – це процес. Я визначаю його просто як злагода, перебування в злагоді зі своєю кар’єрою, у злагоді із своєю сім’єю. Неважливо, що це означає для тебе особисто. Мені подобається мати можливість спокійно проводити вихідні, забути про роботу й провести час із сім’єю. А на роботі – це участь у проєктах, які тебе захоплюють, і відчуття, що ти робиш свій внесок у щось вагоме. Але для мене успіх – це процес. І для мене це почуття злагоди з усім, над чим ти працюєш.

## **Застосування змін**

### **Великі можливості – велика відповідальність**

Коли у вас є права адміністратора (на один комп’ютер, парк зі 100 комп’ютерів або хмарний сервіс із тисячами користувачів), вам слід бути обережними й використовувати ці права відповідально. Найголовніше: уникайте використання прав адміністратора для тих завдань, які цього не вимагають. Наприклад, не варто переглядати вебсторінки як адміністратор. Намагайтеся мінімізувати час сеансів із правами адміністратора. Виконайте все, що потрібно, а після цього закрийте сеанс.

У системах Linux ми зазвичай використовуємо команду sudo, щоб виконувати команди від імені адміністратора. Коли ви вперше виконуєте команду sudo на комп’ютері, ви отримуєте таке повідомлення:



Ці принципи застосовуються до будь-яких прав адміністратора, незалежно від операційної системи або служби, за яку ви відповідаєте. Розберімося детальніше, що це все означає. Поважайте конфіденційність інших. Не використовуйте права адміністратора для доступу до приватної інформації, якщо в цьому немає необхідності. Наявність у файловій системі доступу до інформації в основному каталозі користувача не означає, що ви маєте переглядати його особисті файли. Якщо ви адміністратор сервера електронної пошти, це не означає, що ви маєте читати чужу пошту. Те, що ви це можете, не означає, що це треба робити. Навіть якщо у вас є ділові підстави для доступу до певної інформації, обов’язково дотримуйтеся належної процедури або правил доступу до неї. Не використовуйте права адміністратора, щоб обійти будь-які правила.

Думайте, перш ніж натискати клавіші. Коли ви користуєтеся правами адміністратора, ваші дії можуть мати набагато серйозніші наслідки, ніж коли ви дієте як звичайний користувач. Добре подумайте, що хочете зробити, і не поспішайте. Такі помилки, як видалення не того набору файлів, перезавантаження не того комп’ютера або розірвання з’єднання для керування віддаленим комп’ютером, можуть статися через вашу необережність. Щоб привчити себе це робити, записуйте кроки, які плануєте зробити, перш ніж почати діяти. Це корисно з двох причин. Так ви можете планувати заздалегідь і документувати свої дії. Документувати вчинені дії вкрай важливо для використання прав адміністратора. Список виконаних команд дає вам змогу повторювати той самий процес у майбутньому й усувати проблеми, які можуть виникнути пізніше.

У Linux існує команда script. За її допомогою можна реєструвати групу виконаних команд разом із даними, які вони виводять. У Windows Power-Shell є аналогічна команда Start-Transcript. Дані, які виводять ці команди, корисні для автоматизації процедур. Аналогічно, можна використовувати інструмент recordMyDesktop, щоб записувати процес взаємодії з графічним додатком. Про ці інструменти можна почитати в наступному довідковому матеріалі.

Останній принцип використання команди sudo: "Велика сила – то велика відповідальність". Це дещо жартівлива алюзія, але суть її серйозна. Що більше ви можете зробити з правами адміністратора, то більше можете зіпсувати. Ви можете мінімізувати вплив будь-якої помилки (а помилки в цій справі неминучі), якщо будете впевнені, що зможете швидко скасувати зміни, якщо щось піде не так. Для цього можна створити копію стану пристрою перед внесенням змін. Зберігайте конфігурацію в системі керування версіями або документуйте, які дії потрібно виконати, щоб повернутися до попереднього стану. Повернення до попереднього стану називається відкатом. Деякі команди легше відкотити, ніж інші. Наприклад, якщо змінити налаштування конфігурації з true на false, відкатом буде повернення його до true. Але якщо ви видалите файл без збереження резервної копії, відкотити цю дію може бути складно або й геть неможливо. Тож, перш ніж внести зміну, подумайте, до чого вона призведе, і переконайтеся, що у вас є копії всієї інформації, яку можна втратити.

### **Записування виконаних дій**

**Записування виконаних дій**

Коли ви збираєтеся внести зміни на комп’ютері, дуже важливо мати чіткий план того, що ви збираєтеся робити, і записувати дії, які ви вже зробили.

Загальною практикою для системних адміністраторів, які працюють із чергами помилок або системами заявок, є зазначення виконаних команд і отриманих результатів для опрацьованої помилки або заявки. Це варто робити, коли виконуваних команд небагато і вони досить прості.

Однак існують ситуації, коли без попереднього дослідження неможливо визначити, які саме команди знадобляться. У таких випадках вам можуть стати у пригоді команди [script](http://manpages.ubuntu.com/manpages/bionic/man1/script.1.html) для Linux або [Start-Transcript](https://docs.microsoft.com/en-us/powershell/module/microsoft.powershell.host/start-transcript?view=powershell-6) для Windows.

**script**

У разі використання команди script ви можете назвати її так:

script session.log

Після цього контент вашого сеансу буде записано у файл session.log. Якщо ви бажаєте зупинити запис, ви можете написати **exit** або натиснути Ctrl-D. Створений файл буде у форматі ANSI, який міститиме кольори, які відображалися на екрані. Щоб прочитати їх, ви можете використовувати такі команди, як [ansi2txt](http://manpages.ubuntu.com/manpages/bionic/man1/ansi2txt.1.html) або [ansi2html](http://manpages.ubuntu.com/manpages/bionic/man1/ansi2html.1.html), щоб перетворити їх на звичайний текст або HTML відповідно.

**Start-Transcript**

У разі використання команди Start-Transcript ви можете назвати її так:

Start-Transcript -Path C:\Transcript.txt

Контент сеансу буде записано до C:\Transcript.txt. Щоб зупинити запис, потрібно виконати команду **Stop-Transcript**. Створений файл – це звичайний текстовий файл, у якому зберігаються дані про виконані команди та їхні результати.

**Запис графічних сеансів**

Виконання дій системного адміністрування через графічний інтерфейс користувача є менш поширеним (оскільки цю процедуру важче автоматизувати й виконувати дистанційно), але іноді трапляється.

Якщо адміністрування потрібно виконати через графічний інтерфейс, а у вас немає змоги задокументувати послідовність кроків, ви можете скористатися спеціалізованим інструментом, як-от [recordMyDesktop](http://recordmydesktop.sourceforge.net/about.php) для Linux, або типовими інструментами для роботи з відео, як-от [OBS](https://obsproject.com/) або [VLC](https://www.videolan.org/vlc/index.html).

### **Тестування під час техобслуговування недоречне**

Почнімо з визначення того, що ми називаємо "робочим середовищем". У контексті інфраструктури ми називаємо робочим середовищем ті частини інфраструктури, де певні сервіси виконуються й надаються користувачам. Якщо ви є адміністратором сайту, сервери, що доставляють його контент користувачам, називаються робочими серверами. Усередині вашої компанії сервери, що перевіряють паролі користувачів, називаються робочими серверами автентифікації. Ну, ви зрозуміли ідею.

Скажімо, вам потрібно внести важливу зміну у робочу інфраструктуру. Ви можете додати новий сервіс, змінити конфігурації наявного, оновити операційну систему або вимкнути сервіс, який виконується. Як це зробити? Щоб внести ці зміни безпечно, важливо завжди спочатку перевіряти їх у тестовому середовищі. Тестове середовище – це зазвичай віртуальний комп’ютер, на якому працює та сама конфігурація, що й в робочому середовищі, але яка насправді не обслуговує користувачів сервісу. Таким чином, якщо під час розгортання зміни виникає проблема, ви можете усунути її непомітно для користувачів. Якщо ви відповідаєте за важливий сервіс, що має надалі працювати під час зміни конфігурації, радимо мати допоміжний або резервний комп’ютер. Він має бути таким самим, як і робочий, але не отримуватимете трафіку від користувачів без вашого дозволу. У цьому випадку, коли ви протестуєте зміни в тестовому середовищі й будете готові розгорнути їх у робочому середовищі, спочатку застосуйте зміни на допоміжному комп’ютері. Застосувавши зміни, зробіть резервний комп’ютер основним, а потім застосуйте зміни на іншому комп’ютері. Якщо йдеться про великі сервіси, які надають багато серверів, раджу використовувати "канарок". Перш ніж увійти у вугільну шахту, шахтарі запускали туди канарку, яка допомагала виявити токсичні гази. Так само й ви за допомогою невеликої групи серверів можете виявляти потенційні проблеми у великих змінах, запланованих у системі. Коли ви перевірите, що на цих комп’ютерах усе працює як слід, ви зможете розгорнути зміну на решті комп’ютерів. Таким чином, якщо зі зміною виникне проблема, вона вплине лише на певну підгрупу користувачів і ви відкотите зміну, перш ніж її побачать усі.

Тепер, скажімо, вам потрібно внести незначні зміни в робочу інфраструктуру. Чи будете ви вносити їх одразу в робочому середовищі? Ні, вам слід завжди випробувати їх у тестовій інфраструктурі. Неважливо, наскільки незначною може здаватися зміна. Завжди є щось, що може піти не так. Чи потрібні в інфраструктурі основні й допоміжні комп’ютери чи групи "канарок", залежить від розміру сервісу й критичності потенційних збоїв у ньому. Навіть для найменших сервісів ніколи не варто вносити зміни безпосередньо в робочому середовищі. Завжди спершу використовуйте тестовий екземпляр, і лише перевіривши його роботу, розгортайте зміну в робочому середовищі.

### **Оцінювання ризиків**

Ми вже згадували, що зміни слід завжди перевіряти перед розгортанням. Документуйте свої дії та передбачте спосіб відновити попередній стан. Кількість часу й зусиль, які ви витратите на кожен із цих кроків, залежить від ступеня ризику. Ви завжди повинні мати тестовий екземпляр, щоб випробувати зміни. Але додатковий сервер, можливо, і не потрібен, якщо простої не критичні. Отже, як вирішити, скільки часу й зусиль потрібно докласти? Ми можемо оцінити ступінь ризику на основі того, наскільки сервіс важливий для інфраструктури та на скількох користувачів вплине збій у його роботі.

Деякі сервіси критично важливі. У разі збою в системі централізованої автентифікації ніхто не зможе ввійти в систему. Якщо недоступна платіжна система, компанія не зможе отримувати платежі. Якщо ви втратите резервні копії, у вас не буде захисту в разі аварії. Але не всі сервіси критично важливі. Інформаційний сайт не настільки важливий, як сайт інтернет-магазину. Внутрішня система підтримки не настільки важлива, як додаток підтримки клієнтів. Інфраструктура, необхідна для нового встановлення, не настільки ж критична, як та, що забезпечує вхід у наявні комп’ютери. Загалом, що більше користувачів мають доступ до сервісу, то ретельніше слід перевіряти, чи зміни не призводять до збоїв. Що важливіший сервіс для діяльності компанії, то більше ви маєте дбати про його безперервну роботу. Можливо, у вас передбачено угоду про очікуваний рівень доступності сервісу. Наприклад, у багатьох компаніях техобслуговування з простоєм сервісу проводиться на вихідних. У таких випадках угодою передбачено, що основний файловий сервер може не працювати в суботу на час внесення змін. Ці самі критерії можуть визначати пріоритетність вирішення проблем. Якщо проблема перешкоджає людям виконувати свою роботу, пошук рішення для неї матиме вищий пріоритет, ніж усунення незначної прикрості, яка загалом не впливає на роботу.

### **Виправлення неполадок у належний спосіб**

Як фахівцю з ІТ-підтримки вам доведеться часто вирішувати проблеми. Це може бути проблема в комп’ютері користувача, серверу у вашій власній інфраструктурі, фрагменті коду, що працює в хмарі, або десь між ними. То як вам її вирішити?

Скажімо, ви маєте справу з проблемою, яку виявили самостійно або хтось вам про неї повідомив. Перш ніж братися до вирішення, переконайтеся, що ви можете відтворити помилку, бо вам знадобиться протестувати рішення, щоб гарантувати вирішення проблеми. Це називається процедурою відтворення. Це означає, що ви створюєте дорожню карту для відстеження дій, які привели користувача до неочікуваного результату. Наприклад, до потрапляння на сторінку помилки. Плануючи процедуру відтворення, ви маєте відповісти на три запитання: "Які дії ви виконали, щоб сюди потрапити?" "У чому полягає неочікуваний або поганий результат?" "Який результат насправді очікувався?" Скажімо, ви намагаєтеся вирішити проблему, через яку користувач не має доступу до сторінки сайту. У такому разі процедурою відтворення буде перейти на проблемний сайт у браузері. Поганий результат – сторінка помилки, а очікуваний результат – відкриття сайту. Дізнавшись, які дії потрібно відтворити, щоб отримати неочікуваний результат, і яким має бути правильний результат, ви можете спробувати вирішити основну проблему. Пам’ятайте: це завжди потрібно робити в тестовому середовищі, а не в робочому. Обов’язково документуйте всі свої дії та всі висновки. Наявність такої документації може бути безцінною, якщо ви колись знову зіткнетеся з подібними проблемами. У майбутньому ви подякуєте собі за це. Застосувавши виправлення, виконайте ті самі дії, які призводили до помилки. Якщо виправлення спрацювало, ви маєте отримати очікуваний результат. У нашому прикладі зі сторінкою ви можете перевірити рішення, відвідавши сайт. Застосувавши необхідне виправлення, ви маєте побачити контент сайту замість сторінки помилки.

Ого, ми пройшли чимало матеріалу й розглянули багато різних аспектів обов’язків системного адміністратора, зокрема як безпечно застосовувати зміни з належною кількістю зусиль. Далі ви попрактикуєтеся застосовувати ці поняття за допомогою Qwiklabs. У наступному модулі ми поговоримо про технічні деталі сервісів інфраструктури, що використовуються в ІТ. До зустрічі!

## **Знайомство з послугами IT-інфраструктури**

### **Які є послуги ІТ-інфраструктури?**

З поверненням! В останньому модулі ми дізналися, що в системних адміністраторів є багато обов’язків, як-от обслуговування сервісів інфраструктури. Сервіси ІТ-інфраструктури – це те, що дає змогу організації функціонувати. До них належать: підключення до Інтернету, керування мережами шляхом налаштування мережевого обладнання, з’єднання комп’ютерів через внутрішню мережу тощо. На цьому уроці ми дізнаємося про стандартні сервіси ІТ-інфраструктури й про те, що ви маєте знати, щоб почати інтегрувати їх в організацію. Ми також глибше розглянемо кожний сервіс інфраструктури окремо. Ми більше зосередимося на сервісах фізичної інфраструктури, як-от серверах, разом із сервісами мережевої інфраструктури, які забезпечують інтернет-з’єднання в компанії. Одним словом, ми будемо обслуговувати всі потреби в сервісах інфраструктури.

### **Роль послуг IT-інфраструктури в системному адмініструванні**

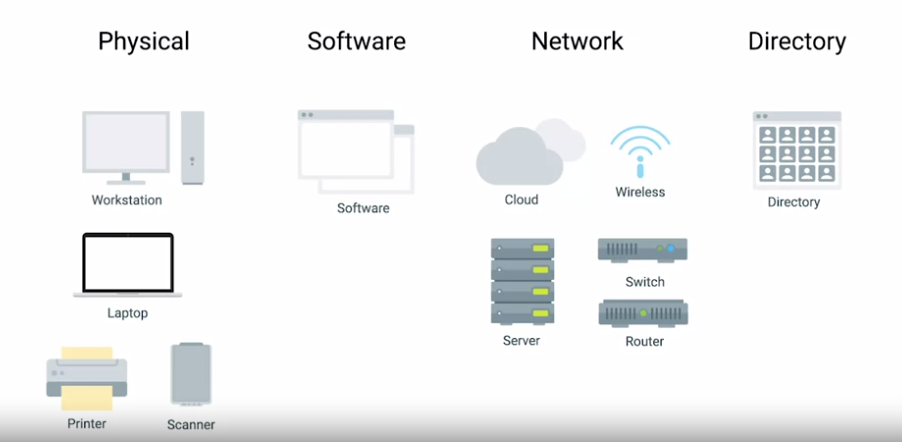
Є багато сервісів ІТ-інфраструктури, які підтримують роботу компанії.  У невеликій компанії за всі ці сервіси може відповідати одна людина. У більших компаніях адміністратори, що допомагають певній команді, можуть керувати одним сервісом. У цьому курсі ми обговоримо, що потрібно для налаштування цих сервісів, якщо ви єдиний ІТ-спеціаліст у компанії. Ми також оглянемо деякі хмарні сервіси, які можна використовувати, якщо ви хочете, щоб вашими сервісами керувала інша компанія.

Нагадаю: як ми вже зазначали раніше, хмарні сервіси – це сервіси, доступні через Інтернет (наприклад, Gmail). Ми можемо отримувати доступ до облікових записів Gmail на будь-якому пристрої, під’єднаному до Інтернету. До кінця цього модуля ви добре розбиратиметеся в тому, які сервіси потрібні для функціональної ІТ-інфраструктури в компанії.

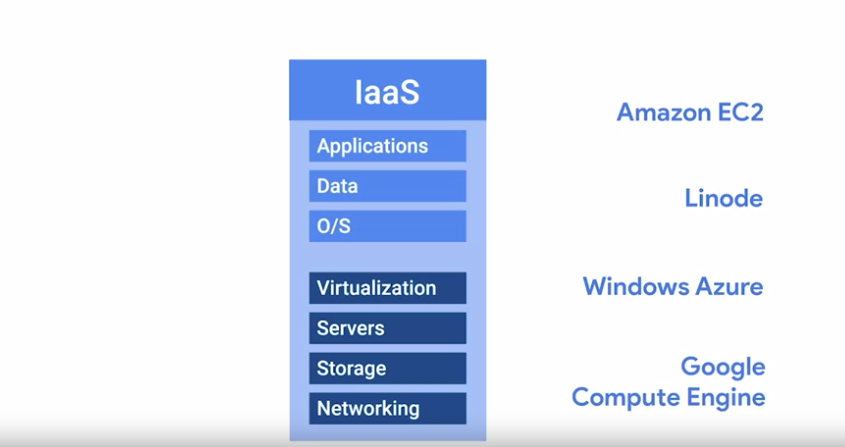
### **Види послуг IT-інфраструктури**

Є багато видів сервісів ІТ-інфраструктури. На цьому уроці ми коротко оглянемо їх усі загалом. На наступних уроках ми докладно розберемось, як налаштовувати й підтримувати ці сервіси. Звучить непогано? Тоді починаймо!

На одному з попередніх уроків ми говорили про компоненти фізичної інфраструктури ІТ-середовища. Згадайте, що ви можете налаштувати різні сервери для роботи своїх сервісів, як-от сервер для сховища файлів.

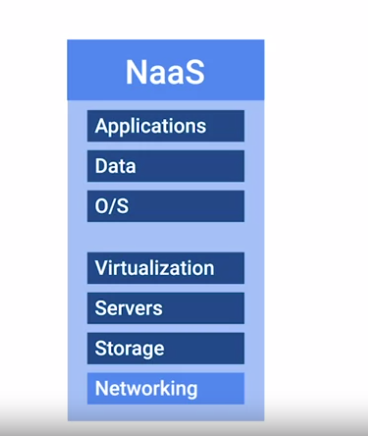


Ви можете придбати або орендувати обладнання для цих серверів і налаштувати й зберігати їх на місці або на іншому об’єкті. По суті, ви керуєте роботою цих серверів від початку до кінця. Є й інший варіант. Якщо ви не хочете відповідати за керування обладнанням і оновлення операційних систем серверів та систем безпеки, можна використовувати хмарну альтернативу для підтримки своєї інфраструктури, яка називається "Інфраструктура як послуга", або IaaS.



Постачальники IaaS надають вам попередньо налаштовані віртуальні комп’ютери, які можна використовувати так само, як фізичний сервер. До популярних IaaS-провайдерів належать Amazon Web Services із сервісом Elastic Compute Cloud (або EC2), Linode, що надає віртуальні сервери, Windows Azure і Google Compute Engine – сервіс, який ви використовували протягом цього курсу. Докладніше про різних IaaS-провайдерів ви можете прочитати в довідковому матеріалі до цього відео.

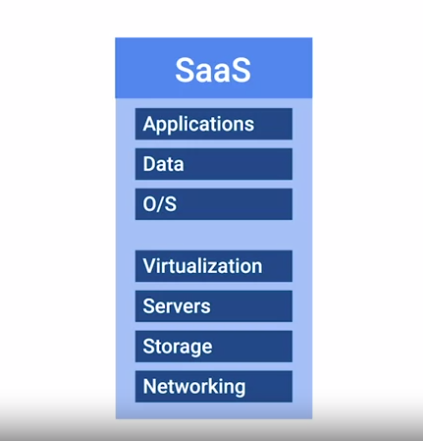
Внутрішня мережа вашої компанії не буде схожа на мережу у вас удома. У вас буде багато комп’ютерів, які мають бути в певній підмережі. Ви маєте призначати їм IP-адреси статично або за допомогою DHCP. Необхідно налаштувати мережеве обладнання. Імовірно, має бути доступний бездротовий Інтернет. Має працювати DNS тощо. Якщо ваша компанія велика, за мережі зазвичай відповідає спеціальна команда. Але в меншій компанії, ймовірно, саме ви відповідатимете за налаштування мережі. Мережа може бути інтегрована в сервіс IaaS-провайдера, але в останні роки в цій сфері також сформувався окремий хмарний сервіс – "Мережа як послуга", або NaaS.



NaaS дає змогу компаніям передоручати керування своїми мережевими сервісами, щоб не мати справу з дорогим мережевим обладнанням. Компаніям також не доводиться налаштовувати власну мережеву безпеку, керувати власною маршрутизацією, налаштовувати WAN і приватні мережі тощо. Більше дізнатися про NaaS-провайдерів ви зможете в довідковому матеріалі.

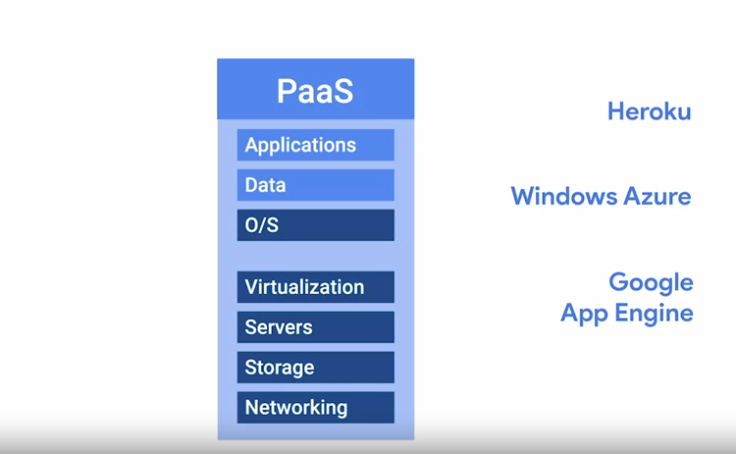
Поговорімо про програмне забезпечення, яке може використовувати ваша компанія. Чи потрібно набирати текст у документах Word, використовувати поштовий клієнт, спілкуватися з іншими людьми, використовувати операційні системи, обробляти електронні таблиці або використовувати інші програми для бізнесу? Б’юся об заклад, що так. Потрібне програмне забезпечення має бути доступне користувачам у компанії.

Ми обговорювали, як встановлювати й обслуговувати програми на комп’ютерах. Вам доведеться мати справу з такими речами, як ліцензії, безпека, оновлення й технічне обслуговування для кожного комп’ютера. Хмарною альтернативою утриманню власного ПЗ є "Програмне забезпечення як послуга", або SaaS. Щоб не встановлювати текстовий процесор на кожному комп’ютері, ви можете використовувати icrosoft Office 365 чи Google G Suite. Обидва ці сервіси, які ви можете купити, дають змогу редагувати документи Word, обробляти електронні таблиці, створювати презентації тощо – і все це в браузері.



Далі, в додатковій статті, ви можете більше дізнатися про SaaS-провайдерів. Деякі компанії мають продукт, створений на основі програмного додатка. У цьому випадку розробники ПЗ повинні мати можливість писати код, складати й оформляти свої програми. По-перше, потрібно встановити певні додатки для середовища програмування. Далі, залежно від продукту, може знадобитися база даних для зберігання інформації. Нарешті, якщо вони надають вебконтент як-от сайт, їм потрібно буде публікувати свій продукт в Інтернеті. Якщо ви організовуєте весь цей процес самостійно, вам може знадобитися налаштувати базу даних і вебсервер. Середовище розробки програм також має бути встановлене на кожному комп’ютері, де це потрібно.

Якщо вам потрібне універсальне рішення для створення й розгортання додатка, ви можете використовувати сервіс "Платформа як послуга", або PaaS. Він містить цілу платформу, що дає змогу писати код, зберігати інформацію в базі даних і надавати додаток – усе на одній платформі. Популярними варіантами PaaS є Heroku, Windows Azure і Google App Engine.



Як ви могли здогадатися, більше про PaaS-провайдерів можна прочитати в довідковому матеріалі. І останній сервіс ІТ-інфраструктури, який ми розглянемо, – це керування користувачами, доступом і авторизацією. Служба каталогів централізовано керує користувачами й комп’ютерами організації, даючи вам змогу додавати, змінювати й видаляти користувачів і комп’ютери.



До популярних служб каталогів, які можна налаштувати, належать Windows Active Directory і OpenLDAP. Ми трохи докладніше поговоримо про них пізніше в цьому курсі. Служби каталогів також можна розгортати в хмарі за допомогою провайдерів сервісів "Каталог як послуга", або DaaS. Як ви здогадалися, прочитати докладніше про DaaS-провайдерів можна в додатковій статті.

Ось, власне, і все. Це був загальний огляд найпопулярніших сервісів інфраструктури, з якими ви зустрінетеся під час адміністрування систем. Хоча хмарні сервіси – це чудовий варіант, дуже важливо, щоб ви розуміли, як працює сервіс та як його обслуговувати, перш ніж звернутися по допомогу до хмарного сервісу. Хоча хмарні сервіси широко використовуються в галузі й мають багато переваг, у них є й певні недоліки. Це, зокрема, періодичні витрати й залежність від постачальника сервісу. Ми розповімо вам про технічні подробиці й реалізацію цих поширених сервісів ІТ-інфраструктури. Ми розглянемо всі питання: від налаштування власного сервера й визначення потрібних додатків для ефективної роботи до того, як створити багато користувачів і впорядкувати мережеві сервіси. До кінця цього курсу ви отримаєте базові знання, необхідні для налаштування ІТ-інфраструктури в невеликій організації.

Послуги фізичної інфраструктури складаються з фізичного апаратного забезпечення, яке організація використовує у своєму ІТ-середовищі.

Мережеві служби складаються з мережевих компонентів, які організація використовує у своєму ІТ-середовищі, це, зокрема, мережеві протоколи, мережеве апаратне забезпечення тощо.

Служби програмного забезпечення складаються з програмного забезпечення, яке організація використовує у своєму ІТ-середовищі.

<https://cloud.google.com/learn/what-is-iaas#:~:text=IaaS%2C%20or%20Infrastructure%20as%20a,way%20requires%20time%20and%20capital>.

<https://en.wikipedia.org/wiki/Network_as_a_service>

<https://www.businessinsider.com/the-most-popular-cloud-apps-used-at-work-2015-8>

<https://www.techradar.com/news/best-paas-provider>

<https://aws.amazon.com/cloud-directory/>

<https://jumpcloud.com/#platform>

<https://www.microsoft.com/en-us/security/business/identity-access/microsoft-entra-id>

### **Як працює платформа Qwiklabs?**

Тепер, коли ми знаємо більше про хмару й сервіси ІТ-інфраструктури, розгляньмо детальніше, що відбувається за лаштунками. Кожне практичне заняття містить складений список дій, які необхідно виконати під час налаштування. Це, зокрема, створення віртуального комп’ютера з певною конфігурацією процесора й пам’яті, та встановлення на ньому певної операційної системи: Windows або Linux. Також указані всі інші хмарні ресурси, необхідні для практичного заняття, як-от додаткові віртуальні диски для віртуального комп’ютера. Під час заняття ви можете отримувати доступ до екземплярів, створених у Qwiklabs, за допомогою SSH або віддаленого робочого столу. Ви можете керувати ними так само, як би ви використовували фізичні комп’ютери з такою операційною системою. Як ви, мабуть, зрозуміли, віртуальна машина поводиться майже так само, як фізичний комп’ютер. Після завершення практичного заняття Qwiklabs видаляє віртуальний комп’ютер. Таким чином, процесор, пам’ять і сховище, які використовувала віртуальна машина, повертаються в пул доступних ресурсів постачальника, щоб їх могли використовувати інші віртуальні машини для інших завдань. Ось і все. Тепер ви краще розумієте, що відбувається за лаштунками, коли ви запускаєте Qwiklabs у наших курсах.

### **Гізер: перша робота у сфері технологій**

Я виросла в маленькому містечку посеред пустелі.  Там особливо не було чим займатися, окрім як читати, грати на комп’ютері та вчитися. І саме там я справді полюбила технології, зрозуміла, як працює комп’ютер, як він виконує свої функції і як я можу змусити його робити щось інше. Коли я вступила до коледжу, то почала вивчати операційні системи Unix. І я вивчила рівно стільки, скільки було потрібно для стажування в місцевого інтернет-провайдера. І я досить сильно хвилювалася, тому що в перший же день стажування, щойно я ввійшла в офіс, мені сказали: "Чудово! Ми дуже раді бачити вас тут.

Ви знаєте Unix, чи не так?" – "Так". "Ось сервер RADIUS, ми хочемо, щоб ви його налаштували. Це потрібно зробити до до кінця тижня". І я сказала: "Як цікаво! Я маю зробити щось, що вплине на наших користувачів, і чомусь навчуся". Була лиш одна проблема. Я не знала, що таке RADIUS, тож це мало стати для мене складним завданням. Мені довелося читати посібники, довідники, а також шукати книжки в бібліотеці.

Мені знадобилося десь три дні, щоб дізнатися, що таке RADIUS і як його налаштувати. Але врешті-решт я дізналася про це більше, ніж будь-хто інший в офісі інтернет-провайдера. Я вважаю, що ці знання й досвід справді допомогли мені стати експертом зі ще більшого кола питань. Це дало мені впевненість, що я можу виконувати таку роботу, і це було справді корисно. Тож врешті-решт я стала системним адміністратором з UNIX і з цього почалася моя кар’єра.

[

## **Послуги фізичної інфраструктури**

### **Серверні операційні системи**

Якщо вам потрібно налаштувати сервер, ви встановлюєте на нього сервіс або додаток, наприклад сервіс зберігання FAS. Мережевий сервер надаватиме ці сервіси комп’ютерам за їх запитом. Можливо, ви думали, що встановите сервіси або використовуватимете ОС, як-от Windows 10. Хоча це теж варіант, але зазвичай в організації сервіси краще встановлювати на серверній операційній системі. Серверні операційні системи – це зазвичай операційні системи, оптимізовані для функцій сервера. Це, зокрема, такі функції, як більша кількість мережевих з’єднань і більший об’єм оперативної пам’яті.

У більшості операційних систем є версії, спеціально розроблені для серверів. У Windows це Windows Server. У Linux багато дистрибутивів мають версії для серверів, як-от Ubunta Server – ОС, оптимізована для серверів. Mac OS також доступна у версії Mac OS Server. Серверні операційні системи зазвичай краще захищені й мають додаткові вбудовані сервіси. Отже, вам не потрібно налаштовувати ці сервіси окремо. Більше про різні серверні операційні системи ви прочитаєте в додатковій статті. А поки що запам’ятайте, що під час встановлення сервісів на сервері слід використовувати спеціальну серверну операційну систему.

<https://phoenixnap.com/kb/server-operating-system>

### **Віртуалізація**

На останньому курсі ми говорили про віртуальні комп’ютери, зокрема, як його налаштувати на персональному комп’ютері. На цьому уроці ми поговоримо про те, чому віртуалізація може бути важливою частиною сервісів інфраструктури й системного адміністрування.

Є два способи виконання сервісів: на виділеному обладнанні або у віртуалізованому екземплярі на сервері. Коли ви віртуалізуєте сервер, ви розміщуєте на одному сервері багато віртуальних екземплярів. Кожен екземпляр містить сервіс. У роботі сервісів на кожній із цих платформ є багато переваг і недоліків. Розгляньмо їх.

Продуктивність. Сервіс, що працює на виділеному обладнанні, матиме вищу продуктивність, ніж сервіс у віртуалізованому середовищі. Це пов’язано з тим, що один сервіс використовує один комп’ютер, на відміну від ситуації, коли його використовують багато сервісів.

Вартість. Серверне обладнання може бути досить дорогим. Якщо ви розміщуєте сервіс на певній частині виділеного обладнання й мусите зробити це ще для 9 сервісів, може набігти солідна сума. Одна з величезних переваг віртуалізації сервісу полягає в тому, що 10 сервісів можуть працювати в 10 різних віртуальних екземплярах – і все на одному фізичному сервері. Ось як ще можна подумати про це. На типовому сервері, на якому працює лише один сервіс, він, імовірно, використовуватиме лише до 10–20% ресурсу процесора. Решта апаратних ресурсів не використовується. Ви можете додати на фізичний сервер ще багато сервісів і все одно мати хороший запас його ресурсів. Дешевше запустити кілька сервісів на одному комп’ютері, ніж багато сервісів на кількох комп’ютерах.

Технічне обслуговування. Сервери потребують технічного обслуговування й регулярного оновлення системи. Іноді для цього сервери потрібно переводити в режим офлайн. Якщо сервіс віртуалізовано, ви можете швидко зупинити його роботу або перенести його на інший фізичний сервер, а тоді проводити обслуговування, скільки буде потрібно.

Віртуалізований сервіс суттєво спрощує обслуговування сервера.

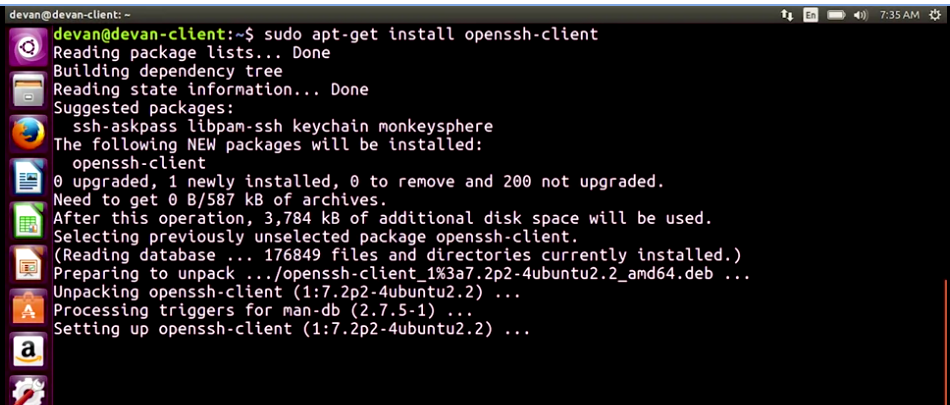
Критичні точки. Якщо ви встановили сервіс на одному фізичному комп’ютері і на цьому комп’ютері виникли проблеми, у вас починаються неприємності. Віртуалізований сервіс можна легко перемістити з фізичного комп’ютера й запустити його резервну копію на іншому комп’ютері. Це можна зробити і з фізичним сервером, але це може бути дорого, якщо у вас багато сервісів. Порада: ви можете запобігти одній критичній точці на фізичному комп’ютері, якщо налаштуєте резервні сервери, тобто дублюватимете їх. Про резервне обладнання ви дізнаєтесь у наступному модулі. Як бачите, використання віртуалізованих сервісів має багато переваг. Просто обов’язково зважте плюси й мінуси візуалізації вашого сервісу та використання виділеного серверного обладнання. Так ви зможете зробити правильний вибір для своєї компанії.

### **Віддалений доступ (повторення)**

Ще один важливий аспект сервісів фізичної інфраструктури – можливість з’єднання з інфраструктурою в будь-якій точці світу. Ми говорили про віддалений доступ на одному з попередніх курсів і використовували його для з’єднання з навчальними комп’ютерами.

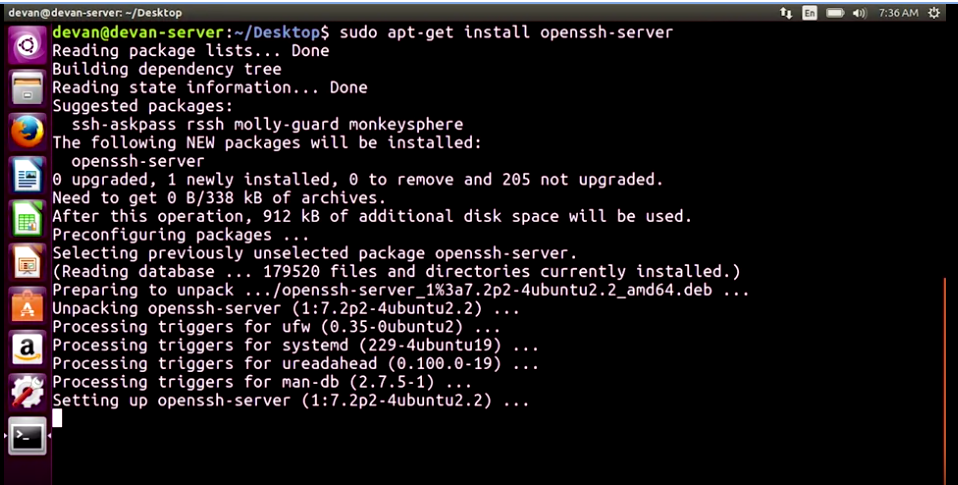
На цьому уроці ми обговоримо, що потрібно для налаштування віддаленого доступу в невеликій організації. Системному адміністратору, як і будь-якому працівнику ІТ-підтримки, важливо мати можливість віддаленого доступу до іншого сервера чи комп’ютера користувача, щоб вирішувати проблеми або проводити обслуговування, де б він не перебував. У Linux найпопулярніший інструмент віддаленого доступу – це OpenSSH.

В останньому курсі ми вже дізналися, як за допомогою SSH під’єднатися до віддаленого комп’ютера, і трохи поговорили про те, що потрібно для налаштування SSH. Але я швидко покажу вам, як це зробити. Щоб за допомогою SSH увійти в інший комп’ютер, потрібно встановити SSH-клієнт на комп’ютері, з якого ви під’єднуєтеся. Потім установіть SSH-сервер на комп’ютері, до якого ви під’єднуєтеся. Більше про OpenSSH ви прочитаєте в наступному довідковому матеріалі. А ми продовжимо дізнаватися, як установити клієнт OpenSSH на комп’ютері. Це надзвичайно просто. Для цього потрібно на клієнтському комп’ютері просто виконати таку команду: sudo apt-get install openssh-client.

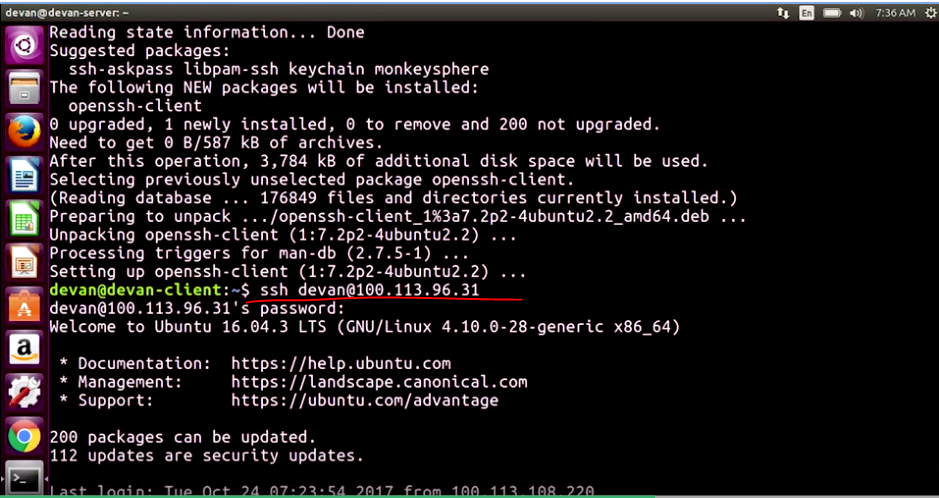


Зараз завантажиться пакет... Чудово! Мій клієнт встановлено. Далі потрібно встановити сервер OpenSSH на комп’ютері, до якого ви хочете отримати доступ. Пам’ятайте, що SSH-сервер – це лише процес, який відстежує вхідні з’єднання SSH. Тож перейдімо на сервер і встановімо сервер OpenSSH.

Отже, я ввожу: sudo apt-get install openssh-server.



Чудово! Схоже, мій сервер тепер працює. Тепер ми повернемося на клієнт і виконаємо тест. Я ввожу команду ssh і свою IP-адресу сервера з моїм іменем користувача. Мене просять ввести пароль, що добре.



Чудово! Отже, як бачите, я під’єднався до свого сервера. Дієвий спосіб це перевірити – відкрити робочий стіл мого сервера й створити там каталог. Тепер, якщо я повернуся на свій сервер, який відкрито в цьому вікні, і перегляну список файлів, то ви побачите каталог test. Ось і все. Тепер ви можете з одного комп’ютера отримувати доступ до іншого. Не надто складно, чи не так?

У Windows теж можна використовувати такі інструменти. Популярним інструментом віддаленого доступу до CLI є WinRM або Putty. Для віддаленого доступу до графічного інтерфейсу популярний інструмент RDP. В останньому курсі ми вже говорили про під’єднання за допомогою Putty. Просто не забудьте встановити SSH-сервер на комп’ютері, до якого під’єднуєтеся. Ми також обговорювали на останньому курсі, як налаштувати RDP. Ви завжди можете переглянути ті уроки, якщо дещо підзабули. Більше про інструменти віддаленого доступу у Windows читайте в довідковому матеріалі. Головне, що слід запам’ятати: такі засоби, як віддалений доступ, допоможуть вам ефективніше керувати фізичною ІТ-інфраструктурою. Спочатку потрібно буде виконати певні налаштування: установити SSH-клієнт, SSH-сервери, дозволити з’єднання з віддаленим робочим столом тощо. Але це принесе вам чимало користі. Далі ми розглянемо мережевий сервіс. До зустрічі!

## **Мережеві служби**

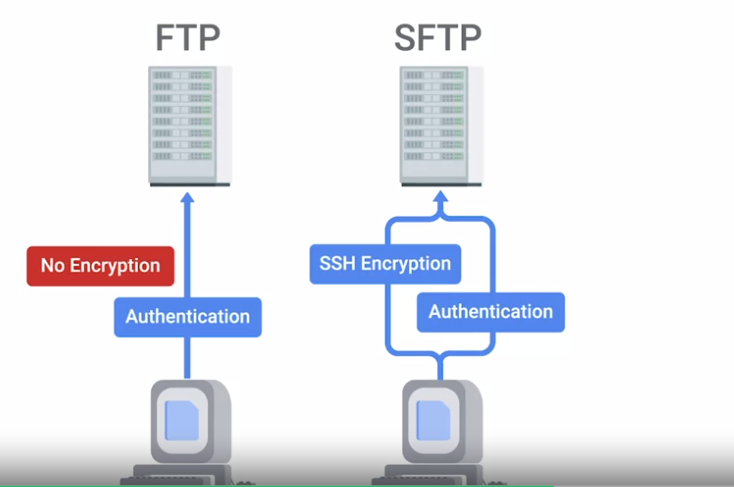
### **FTP, SFTP та TFTP**

Тепер, коли ми трохи більше знайомі з деякими загальними аспектами фізичної інфраструктури, перейдімо до мережевих сервісів. Мережевий сервіс, що зазвичай використовується в організації, – це сервіс передавання файлів. Але навіщо потрібен спеціальний сервіс для передавання файлів?

Так, звісно, ви можете скрізь носити із собою флешку й копіювати файли на кожний комп’ютер, де працюєте, або використовувати засоби віддаленого копіювання з нашого останнього курсу. Або ви можете зберігати величезні файли й передавати їх з одного комп’ютера на інший через Інтернет. Сьогодні використовується кілька сервісів протоколів передавання файлів. Розгляньмо коротко, які вони й що роблять.

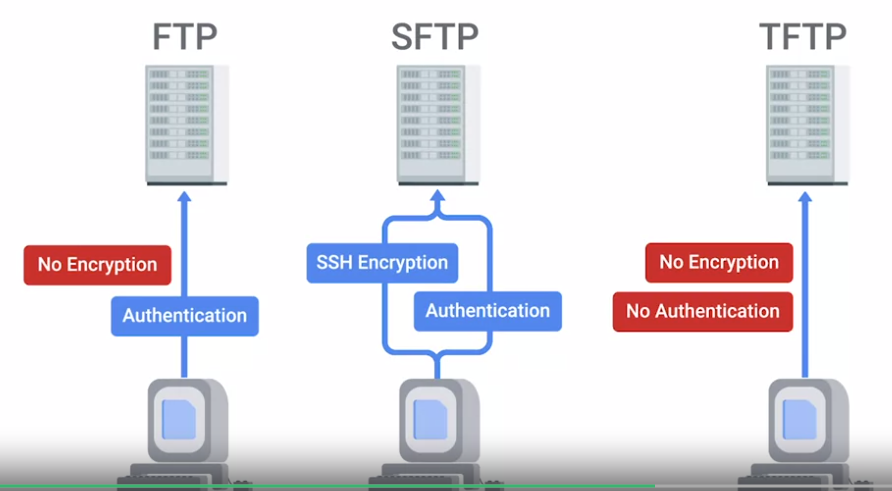
FTP. На другому курсі цієї програми "Основи комп’ютерних мереж" ми згадували про FTP (скорочено від "File Transfer Protocol"). Це застарілий спосіб передавати файли між комп’ютерами через Інтернет, але він досі використовується. Це не надто безпечний спосіб передавання даних, адже він їх не шифрує. Сервіс FTP працює дуже подібно до сервісу rsh. Щоб отримати доступ до FTP-сервера, користувачі мають установити FTP-клієнт. На FTP-сервері ми встановлюємо програмне забезпечення, яке дає нам змогу ділитися інформацією, що зберігається в каталозі на сервері. Сьогодні FTP використовується здебільшого для обміну вебконтентом. Якщо ви користуєтеся послугами хостингу сайту, то можете побачити, що там уже є готове до використання FTP-з’єднання, щоб можна було легко копіювати файли на ваш сайт і з нього.

SFTP. Це захищена версія FTP. Тому є сенс вибрати цей варіант, а не FTP.



Під час процесу SFTP дані надсилаються через SSH і шифруються.

TFTP. Розшифровується як Trivial FTP ("елементарний FTP"). Це простіший спосіб передавання файлів, ніж FTP. На відміну від FTP, сервіс TFTP не вимагає автентифікації користувача, тому всі файли, які ви зберігаєте тут, мають бути звичайними й не потребувати захисту.



Найчастіше TFTP використовується для розміщення інсталяційних файлів. Один зі способів завантаження комп’ютера, який ми ще не розглянули, – це PXE або PXE Boot, що означає "виконання до завантаження". Сервіс дає змогу завантажувати програмне забезпечення, доступне через мережу. Типове використання для організації, що хоче встановлювати ПЗ через мережу, – зберігати інсталяційні файли операційної системи на TFTP-сервері. Так, коли ви завантажуєте мережу, ви можете автоматично запускати засіб встановлення. Це набагато ефективніше, ніж завжди носити із собою флешку з образом операційної системи. Докладніше про PXE Boot ви прочитаєте в наступному довідковому матеріалі.

Залежно від своїх потреб, ви можете обрати один із зазначених сервісів передавання файлів. Раджу ознайомитися з популярними FTP-клієнтами в довідковому матеріалі. Якщо ви просто хочете безпечно обмінюватися файлами між комп’ютерами й мати зручний каталог, де у вас буде доступ до всіх спільних файлів замість передавання їх на ваш комп’ютер, вам краще звернути увагу на мережеві сервіси зберігання файлів. Про них ми поговоримо в наступному модулі.

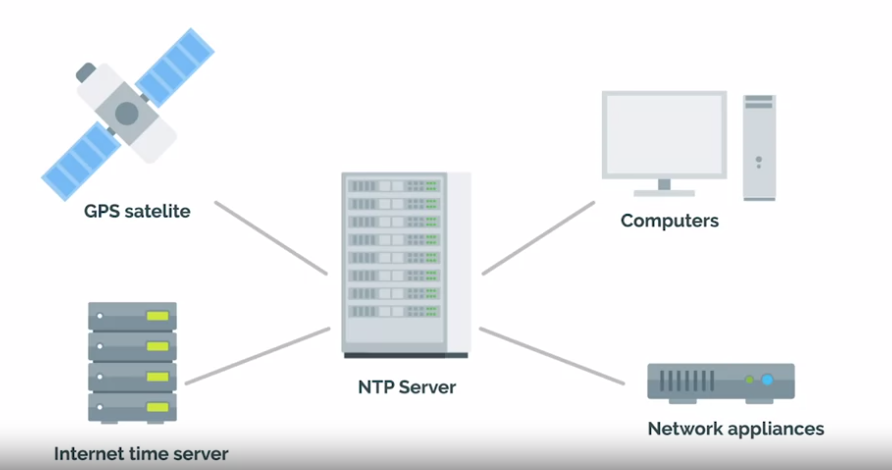
<https://en.wikipedia.org/wiki/Preboot_Execution_Environment>

<https://en.wikipedia.org/wiki/Comparison_of_FTP_client_software>

### **NTP**

Одним із найстаріших інтернет- протоколів, що досі використовуються, є мережевий протокол часу, або NTP. Він забезпечує синхронізацію годинників на комп’ютерах, під’єднаних до мережі. Ви, напевне, бачили реалізацію NTP у своєму особистому житті, якщо колись були в аеропорту. В аеропортах діють синхронізовані системи годинників, і в багатьох із них використовується NTP. Це пов’язано з тим, що інформація, яку ви бачите на екрані відправлення та прибуття, має відповідати часу, який команда керування аерорухом бачить для літаків. Якби тільки NTP міг вирішити проблему із затримками рейсів.

У світі ІТ комп’ютерам потрібен точний час по всій мережі з багатьох причин. Деякі сервіси безпеки, як-от Kerberos і протокол автентифікації в мережі, залежать у своїй роботі від узгодженості значень часу по всій мережі. Докладніше про це ви дізнаєтеся в майбутньому курсі з ІТ-безпеки. Важливо забезпечувати узгоджений і точний час на всіх комп’ютерах компанії. У питанні узгодженості часу ви не можете покладатися лише на обладнання, тому варто налаштувати NTP-сервер. Фхівець ІТ-підтримки або системний адміністратор може робити це для організації різними способами. Можна використовувати локальний або загальнодоступний NTP-сервер. Щоб налаштувати локальний NTP-сервер, можна встановити його програмне забезпечення на сервер керування. Потім ви встановлюєте NTP-клієнти на комп’ютери й повідомляєте їм, з яким NTP-сервісом їм слід синхронізувати свій час.



Це чудовий варіант, адже ви можете керувати процесом від початку до кінця. Інший спосіб налаштування NTP – за допомогою загальнодоступного NTP-сервера. Загальнодоступними NTP-серверами керують інші організації, з якими клієнтські комп’ютери з’єднуються, щоб синхронізувати час. Це чудовий спосіб використовувати NTP без виділеного NTP-сервера. Але якщо у вас великий парк із тисяч комп’ютерів, краще використовувати власні NTP-сервери. Ще один ефективний спосіб – застосовувати власний NTP-сервер, замість того щоб використовувати загальнодоступний. У цьому разі не треба під’єднувати всі клієнти до загальнодоступного сервера й вимірювати синхронізацію часу. Незалежно від того, чи ви використовуєте власний чи загальнодоступний NTP-сервер, NTP – це важливий мережевий сервіс, який обов’язково слід інтегрувати у свій комп’ютерний парк.

### **Служби підтримки мережі (повторення)**

Є кілька мережевих сервісів, які використовуються всередині ІТ-середовища компанії, щоб покращувати продуктивність працівників, конфіденційність і безпеку. Вони досить поширені, але рідко використовуються в невеликих організаціях. Ми говорили про ці сервіси в другому курсі про мережі, але давайте трохи пригадаємо. Я впевнений, що ви зіткнетеся з ними на певному етапі вашої ІТ-кар’єри.

Існують мережі інтранет і проксі-сервери. Інтранет – це внутрішня мережа всередині компанії. Вона доступна, якщо ви під’єднані до мережі компанії. Мережі інтранет можуть надавати широкий спектр інформації й призначені для підвищення продуктивності шляхом надання працівникам кращого способу обміну інформацією. Це можна собі уявити як сайт компанії, доступний лише для людей у мережі компанії. На цьому сайті може централізовано зберігатися документація, команди можуть публікувати актуальні новини, працівники можуть спілкуватися на форумах тощо. Мережі інтранет найчастіше створюються на великих підприємствах і можуть бути дуже цінним засобом підвищення продуктивності працівників. **Іншим популярним внутрішнім сервісом підтримки є проксі-сервер**. Проксі-сервер виступає посередником між мережею компанії та Інтернетом. Він отримує мережевий трафік і передає цю інформацію в мережу компанії. Тому зберігається конфіденційність трафіку мережі компанії від Інтернету. Інтернет отримує трафік через проксі-сервер, але він не знає, звідки той походить. Він знає лише проксі. За допомогою проксі-серверів також можна відстежувати й реєструвати дії у внутрішній мережі компанії. Їх можна налаштувати так, щоб доступ до певних сайтів блокувався. Проксі-сервери корисні для забезпечення конфіденційності та безпеки в Інтернеті, а також регулювання доступу в компанії. На кількох наступних уроках ми поговоримо про, мабуть, найважливіші мережеві сервіси – DNS і DHCP.

### **DNS**

Ми детально розглянули DNS (або систему доменних імен) у курсі про мережі. Якщо ви дещо забули, обов’язково перегляньте той матеріал. У двох словах, DNS – це сервіс, який зіставляє зрозумілі людині імена з IP-адресами. Це важливий мережевий сервіс, який потрібно налаштувати й використовувати, керуючи ІТ-інфраструктурою компанії. Якщо не налаштувати його правильно, ніхто не зможе отримувати доступ до сайтів за назвою. Нам насправді не потрібно думати про DNS на персональних комп’ютерах. Коли ви під’єднуєте новий комп’ютер до Інтернету й починаєте вводити вебадресу, цей сервіс працює автоматично. Вам не потрібно вводити IP-адресу тощо, але залаштунками виконується певний процес. Під час під’єднання до мережі ви використовуєте адресу DNS-сервера, надану маршрутизатором, до якого ви підключені. Він оновлює налаштування мережі, щоб використовувалась адреса цього сервера (зазвичай, це DNS-сервер інтернет-провайдера). З нього ви можете отримати доступ практично до будь-якого сайту. Тож навіщо налаштовувати власний DNS-сервіс, якщо він працює автоматично? На це є дві причини.

По-перше, якщо ви використовуєте вебсервіс, як-от сайт, вам треба повідомити Інтернету, за якою IP-адресою доступний цей сайт. Для цього потрібно налаштувати DNS. Друга причина полягає в тому, що ви, ймовірно, хочете працювати на сервері чи комп’ютерах користувачів дистанційно. Теоретично віддалений доступ до них можна було б отримати через IP-адресу, але можна використовувати зручне для запам’ятовування ім’я хосту. Для цього потрібно за допомогою DNS зіставити IP-адресу з іменем хосту. На наступних кількох уроках ми розглянемо, що потрібно для налаштування DNS для сайтів і внутрішніх мереж.

### **DNS для вебсерверів**

Ви, мабуть, пам’ятаєте, що ми можемо використовувати вебсервер для зберігання й надання контенту клієнтам, яка запитують наші сервіси. Імовірно, ми зберігатимемо контент сайту на нашому вебсервері. Щоб клієнти могли відкрити сайт, ми маємо налаштувати DNS, щоб вони могли просто ввести URL-адресу й знайти його.

Отже, поговорімо про те, як налаштувати DNS для сайту. По-перше, нам потрібне доменне ім’я. Ми можемо придбати доменне ім’я на кшталт SettingUpDNSIsFun.example.com. Такі доменні імена продають компанії, що називаються реєстраторами доменів, як, наприклад, GoDaddy.com або BluHost.com. Отримавши доменне ім’я, ми вказуємо його для файлів нашого сайту. Файли сайту можна зберігати в хмарному сервісі хостингу, або ми можемо самостійно керувати ними й зберігати їх на власних серверах.

Зазвичай реєстратори доменів також надають послуги хмарного хостингу, але можуть стягувати щомісячну плату за розміщення ваших вебфайлів. Порада: щоб не користуватися послугами хмарного хостингу, ви можете використовувати власний вебсервер. Пам’ятайте: розміщення сервісу самостійно й через сторонню компанію завжди мають свої плюси й мінуси. Якщо ви єдиний фахівець з ІТ-підтримки в організації, обов’язково зважте всі варіанти, перш ніж приймати рішення щодо сервісу інфраструктури.

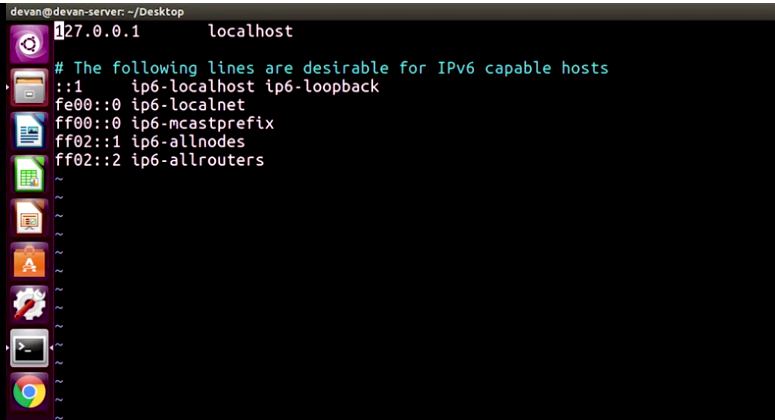
Припустімо, ми хочемо розміщувати файли нашого сайту самостійно. Нам усе одно потрібно вказати наше нове доменне ім’я для місця зберігання вебконтенту. Це можна зробити двома способами. Більшість реєстраторів доменів надають вам налаштування DNS, і ви можете вказати IP-адресу місця зберігання контенту.

Якщо ви вирішили не розміщати DNS через реєстратора доменів, ви маєте налаштувати авторитетний DNS-сервер для свого сайту. Ви, мабуть, пам’ятаєте з 2-го курсу, що авторитетними називають DNS-сервери, які точно знають IP-адресу для доменного імені. Оскільки ми маємо доменне ім’я та розміщуємо вебконтент самостійно, нам варто мати DNS-сервери, які знатимуть цю інформацію.

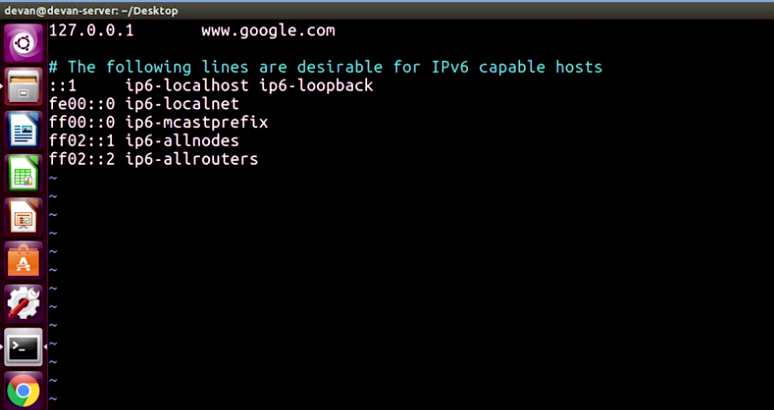
### **DNS для внутрішніх мереж**

Ще одна причина, чому нам бажано мати власні DNS-сервери, – можливість зіставляти внутрішні комп’ютери з IP-адресами. Ми також можемо посилатися на комп’ютер за іменем, а не за IP-адресою. Ми можемо зробити це кількома способами. Перший – за допомогою локального хост-файлу, що містить статичні IP-адреси для зіставлення з іменами хосту. Розгляньмо приклад.

Ми вже вивчали, що хост-файл у побудові мереж дає нам змогу вручну зіставляти IP-адреси з іменами хостів. У Linux хост-файл має назву etc/hosts. Він містить IP-адресу 127.0.0.1, що вказує на ім’я localhost. Це просто посилання на комп’ютер. Localhost зазвичай використовується як спосіб доступу до локального вебсервера. Ми поговоримо про вебсервери в наступному модулі. А поки що не будемо приділяти надто багато уваги localhost. Натомість, якщо змінити зіставлення цієї IP-адреси на www.google.com, зберегти зміну, відкрити браузер і ввести "www.google.com", ми не потрапимо туди. Зараз я це покажу.



Отже, я змінюю localhost на [www.google.com](http://www.google.com). Зберігаю зміну.



Відкриваю браузер, ввожу "www.google.com". Як бачите, нічого не відкривається. Я просто повертаюся на свій локальний комп’ютер. Це тому, що DNS-запит спочатку перевіряє наш файл localhost, а тоді – наші локальні DNS-сервери. Отже, якщо в моєму хост-файлі є запис для google.com, ви перейдете натомість за цією IP-адресою.

Скажімо, я хочу отримати доступ до комп’ютера Наталі за адресою 192.168.15, а її ім’я хосту – catlady.examplecompany.com. Мені доведеться ввести це в хост-файл для кожного комп’ютера в компанії. Цей варіант точно не підходить для масштабування. Гаразд. То який наступний варіант? Ми можемо налаштувати локальний DNS-сервер, де імена всіх комп’ютерів організації будуть зіставлені з їхніми IP-адресами. У такому разі ця інформація зберігатиметься централізовано. Потім ми змінюємо налаштування мережі для всіх комп’ютерів, щоб вони використовували DNS-сервер, а не наданий інтернет-провайдером. Нарешті, розгляньмо один з останніх варіантів DNS, який можна використовувати для внутрішньої мережі. Його можна інтегрувати зі службою каталогів, яка централізовано обробляє інформацію про користувачів і комп’ютери, наприклад Active Directory або LDAP. Коли ми налаштуємо DNS у службі каталогів, у неї автоматично підставляться всі пари зіставлених імен комп’ютерів і IP-адрес. Отже, цю інформацію не знадобиться вводити вручну. Більше про ці служби каталогів ми поговоримо в наступному модулі. Ось і все! Ми в загальних рисах розглянули, навіщо потрібен сервіс DNS і які є варіанти його налаштування. Ми не будемо заглиблюватися в технічні подробиці налаштування DNS-сервера, але, якщо вам цікаво, яке програмне забезпечення DNS можна використовувати, то є кілька ефективних варіантів, як-от Bind або powerDNS.

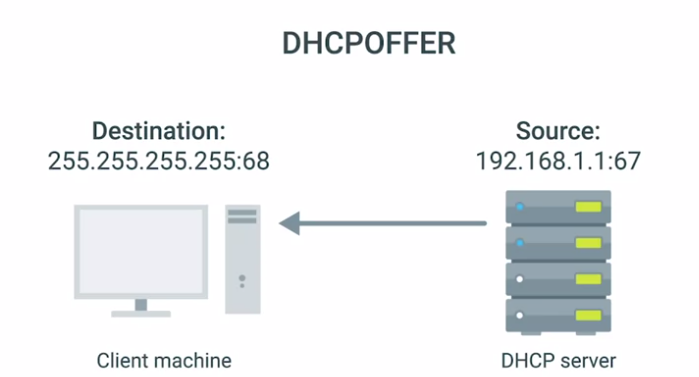
Упевнений, ви здогадалися, де можна більше про них прочитати. Так, у довідковому матеріалі. Ще один аспект DNS, який ми не розглянули, – що робити, якщо ми використовуємо сервіс на кшталт DHCP, де не використовуються статичні IP-адреси. Не хвилюйтеся, ми поговоримо про це на наступному уроці.

<https://blog.dnsimple.com/2015/02/top-dns-servers/>

### **DHCP**

Ще один мережевий сервіс, який полегшить вам роботу в ІТ-підтримці, – це DHCP, або "протокол динамічної конфігурації вузла". Щоб згадати про DHCP, просто перегляньте уроки про DHCP у курсі про мережі.

Коли ви керуєте ІТ-інфраструктурою й хочете під’єднати комп’ютер до мережі, у вас є два варіанти. Ви можете надати йому статичну IP-адресу або IP-адресу, призначену сервісом DHCP. Якщо ви використовуєте статичну IP-адресу, ви маєте контролювати кожну IP-адресу, яку призначаєте комп’ютеру, і вручну вводити її в налаштуваннях мережі. Якщо ви вмикаєте функцію DHCP, IP-адреси комп’ютерам призначатиме DHCP-сервер. Вони отримуватимуть IP-адреси автоматично, і вам не знадобиться встановлювати їх вручну. Якщо ви колись вирішите розширити діапазон IP-адрес, вам теж не знадобиться нічого міняти на клієнтських комп’ютерах. Усе відбудеться автоматично.



Щоб налаштувати DHCP-сервер, потрібно визначити діапазон IP-адрес, у якому ви можете призначати IP-адреси. Якщо ви маєте на меті інтеграцію з DNS, вам знадобиться адреса ваших локальних DNS-серверів. Який шлюз призначити та яку маску підмережі використовувати? Визначившись із програмним забезпеченням DHCP-сервера, налаштуйте параметри на основі цієї інформації. Різні виробники ПЗ для DHCP-серверів пропонують різні набори налаштувань конфігурації, тож вам знадобиться розібратися саме з тим, який ви хочете використовувати. Є багато популярних ПЗ DHCP-серверів, які можна використовувати. У версіях Windows для серверів уже вбудовано DHCP-сервіс, але ви можете більше прочитати про варіанти в довідковому матеріалі.

Якщо ви ввімкнули DHCP-сервер і клієнт налаштований так, щоб отримувати адреси DHCP замість статичних IP-адрес, ваші налаштування DHCP готові для роботи. На останньому уроці ми говорили про зв’язок між DNS і DHCP. Тож тепер у налаштуваннях конфігурації DHCP ми можемо вказати розташування DNS-серверів. Потім два сервери синхронізуються, і, коли DHCP призначить нові адреси, DNS автоматично оновить зіставлення IP-адрес. Це дуже швидкий огляд того, як налаштовуються сервери DHCP. Сподіваюся, тепер ви розумієте, чому DHCP і DNS – це критично важливі мережеві сервіси для вашої організації.

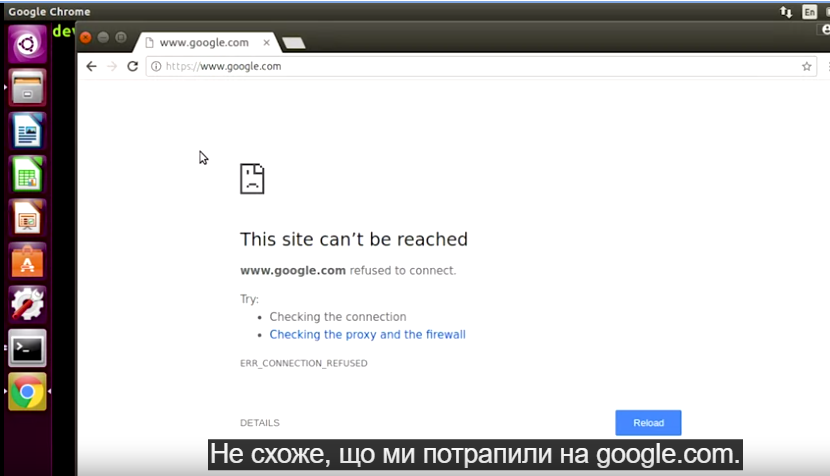
<https://blog.dnsimple.com/2015/02/top-dns-servers/>

<https://en.wikipedia.org/wiki/Comparison_of_DHCP_server_software>

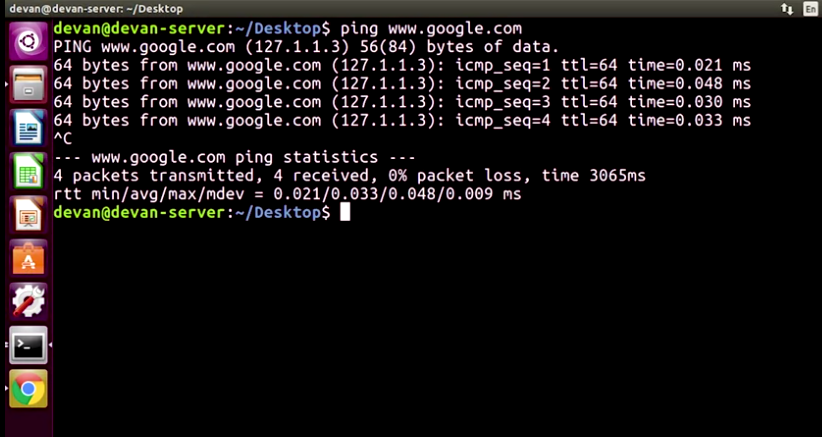
## **Усунення несправностей мережевих служб**

### **Не вдається виконати перетворення імені хосту або доменного імені**

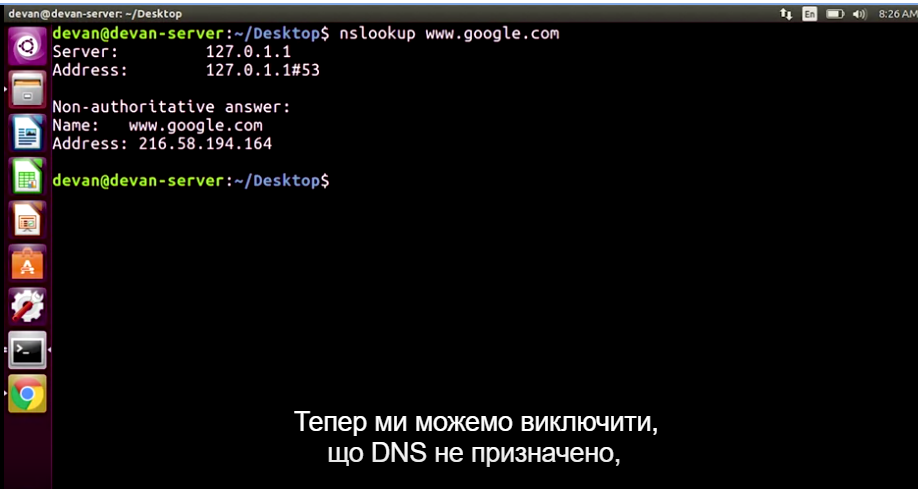
Коли ви працюватимете в ІТ-підтримці, у вас траплятимуться випадки, коли ви не зможете розпізнати або отримати IP-адресу для імені сайту. Цю конкретну проблему може бути складно ідентифікувати. Ви можете просто думати, що мережеве з’єднання не працює. Спробуймо відкрити сайт google.com у браузері. Отже, я відкриваю браузер і переходжу на google.com.



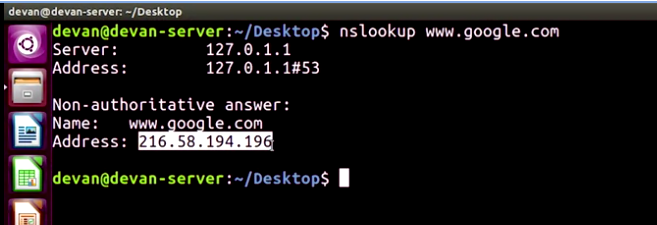
Не схоже, що ми потрапили на google.com. Згадаймо, які інструменти, що ми вивчили в курсі про мережі, можуть нам допомогти. По-перше, якщо не вдається розпізнати доменне ім’я, перевірте, чи працює мережеве з’єднання. Щоб швидко це перевірити, надішліть запит ping на сайт, який точно доступний. Старий перевірений спосіб – надіслати запит ping на www.google.com. У Google дуже рідко трапляються збої, хоча це й не виключено. Отже, я відкриваю термінал і вводжу: ping [www.google.com](http://www.google.com). Схоже, ми отримуємо відповіді.



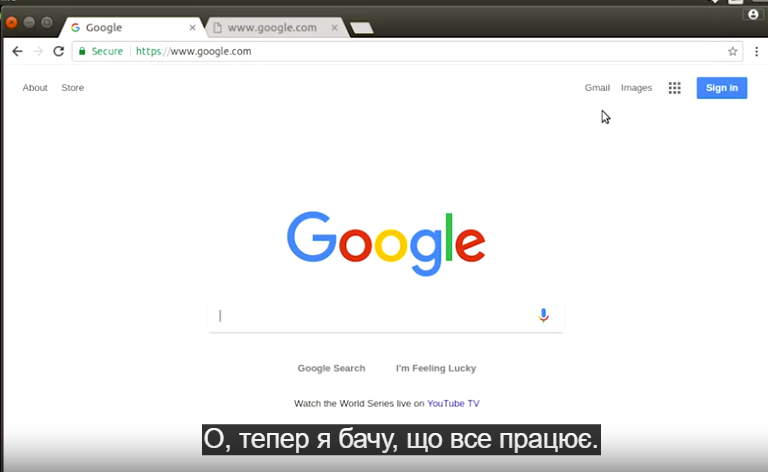
Спробуймо ізолювати іншу проблему – DNS. Щоб переконатися, що DNS-сервер надає вам правильну адресу для google.com, можна використати команду nslookup. Пам’ятайте, що nslookup надає нам сервер імен для імені хосту чи доменного імені. Зараз я зроблю це на своєму терміналі.



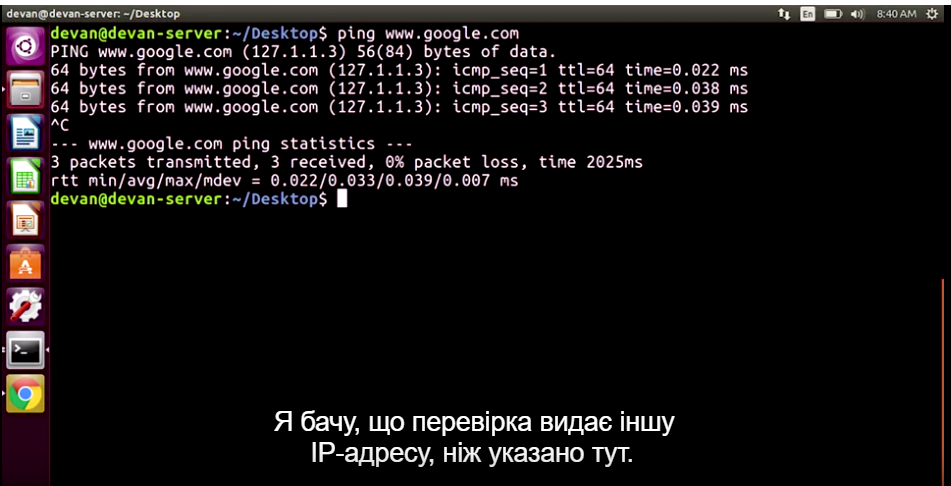
Тепер ми можемо виключити, що DNS не призначено, переконавшись, що ім’я хосту вказує на сервер імен. Якщо скопіювати отриману IP-адресу й вставити її в браузер, вона має видати ім’я сайту якщо DNS працює. Зробімо це. Отже, я копіюю неавторитетну IP-адресу,



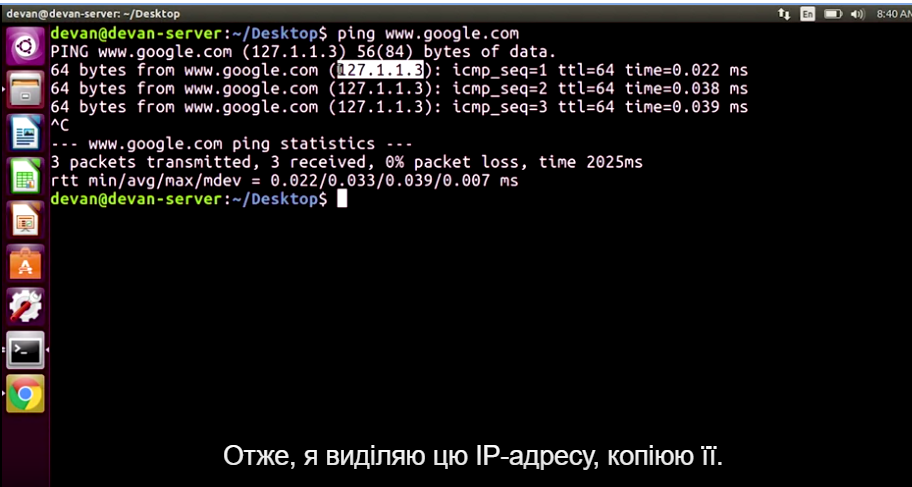
відкриваю браузер. О, тепер я бачу, що все працює.



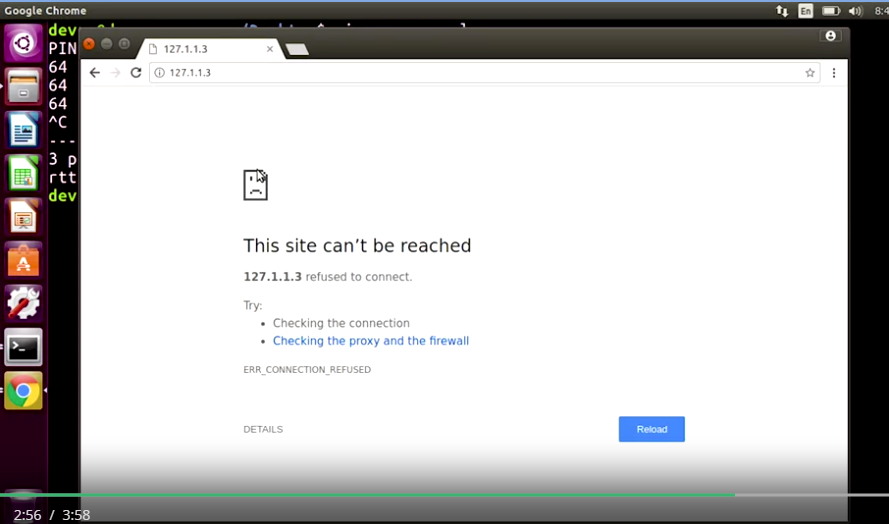
Ммм, що ж відбувається? Схоже, мої налаштування DNS працюють неправильно. Погляньмо ще раз на результати запиту ping. Я відкриваю термінал і вводжу: ping www.google.com.Хм.



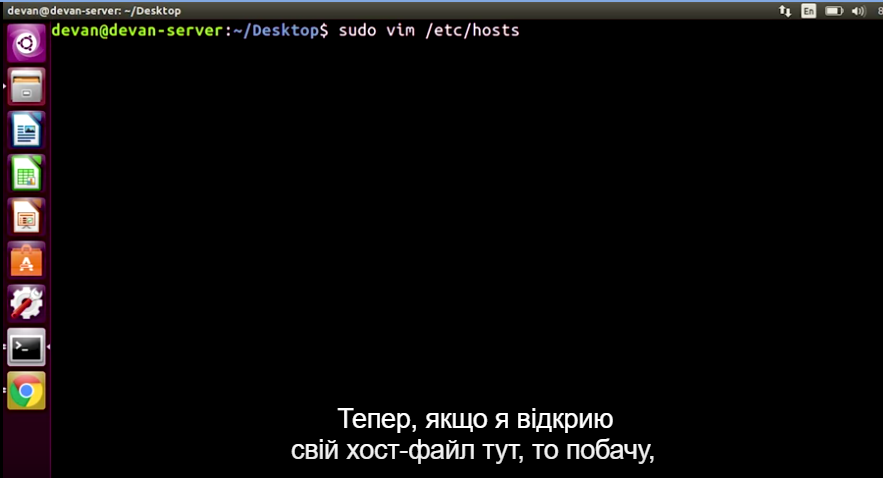
Я бачу, що перевірка видає іншу IP-адресу, ніж указано тут. Якщо я перейду за цією IP-адресою, нічого не відкриється. Отже, я виділяю цю IP-адресу, копіюю її.



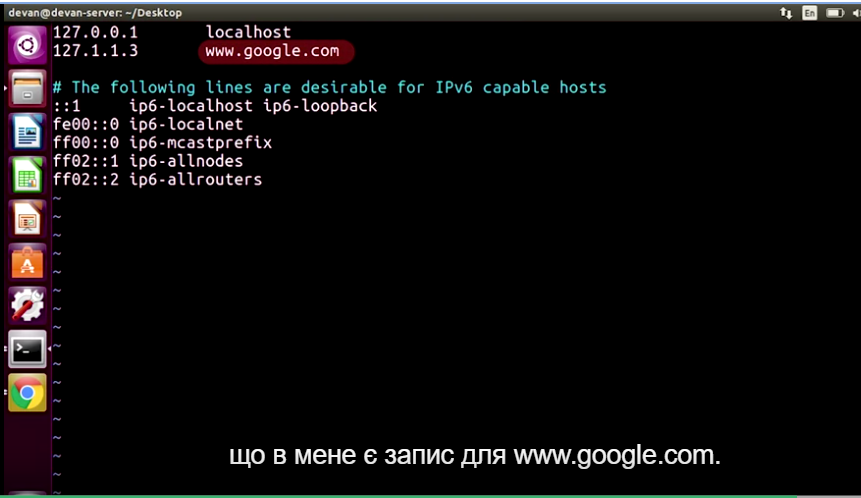
Ха!



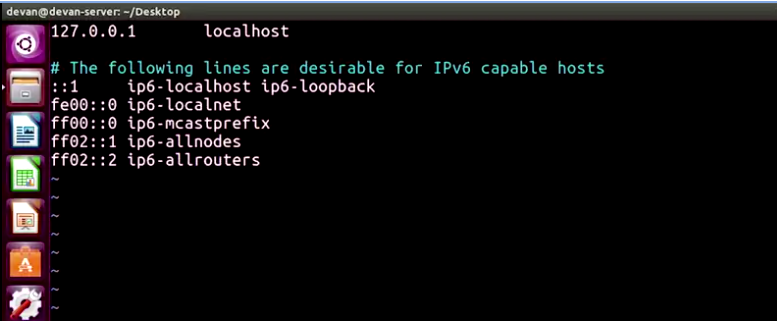
Пам’ятайте, що, коли виконується запит DNS, комп’ютер спочатку перевіряє хост-файл.



Тепер, якщо я відкрию свій хост-файл тут, то побачу, що в мене є запис для www.google.com. І в ньому вказано недійсну IP-адресу.



Якщо я видалю ось цей рядок, де вказано "127.1.1.3",



і збережу цей файл конфігурації, а потім перезапущу браузер і введу "www.google.com", то ось, ми потрапимо куди слід. І правильне налаштування DNS має застосовуватися до www.google.com.

Бувають ситуації, коли навігація в DNS може бути складною, бо на неї можуть впливати багато різних факторів. Але, як і в будь-якому сценарії вирішення проблем, завжди продовжуйте ізолювати проблему, доки не знайдете першопричину. З часом і досвідом ви дізнаєтеся набагато більше про DNS і про те, як вирішувати проблеми з ним на практиці.

## **Керування системними службами**

### **Як системні служби використовуються на практиці**

Ми розглянули багато сервісів:

DNS, DHCP, NTP та інші.

Фахівцю з ІТ-підтримки важливо розуміти,

як працюють програми, що надають ці сервіси.

Тоді ви зможете керувати ними й вирішувати всі можливі проблеми.

Ці програми виконуються як фонові процеси.

Їх ще називають "демонами" або просто "службами".

Це означає, що програмі не потрібно взаємодіяти з користувачем

через графічний інтерфейс або інтерфейс командного рядка,

щоб надавати необхідний сервіс.

Операційна система забезпечує роботу програми.

Кожен сервіс має щонайменше один файл конфігурації,

за допомогою якого ви як системний адміністратор

визначаєте потрібну поведінку сервісу.

Деякі сервіси можуть мати інтерактивні інтерфейси,

у яких користувач може редагувати конфігурацію

та перевіряти поточний статус або історію використання.

Інші сервіси для цього можуть просто використовувати інфраструктуру системи.

У такому разі ви маєте редагувати файли конфігурації самостійно.

Ви маєте знати, як запускати й зупиняти сервіс

і як переглянути його журнали, щоб дізнатися про поточні чи попередні дії.

Зазвичай сервіси налаштовані на запуск під час завантаження комп’ютера.

Отже, у разі збою електроживлення або іншої події,

що призводить до перезавантаження комп’ютера,

не потрібен системний адміністратор, щоб запустити сервіс вручну.

Якщо ви самі хочете вирішувати, коли запускати сервіс,

замість його запуску під час завантаження,

потрібно змінити конфігурацію ПЗ, щоб сервіс запускався, коли ви захочете.

Аналогічно, служби зазвичай налаштовані на перезапуск

у разі неочікуваного завершення роботи.

Якщо ви хочете змінити це налаштування,

може знадобитися змінити конфігурацію системи, яка керує цими параметрами.

Існує багато сервісів,

і кожен може вимагати конкретних знань про те, як його налаштувати

й коли та як його використовувати.

Але загальні концепції керування сервісами та їх налаштування

мало чим відрізняються.

Далі на цьому уроці ми на конкретних прикладах розглянемо,

як це робити у Windows і Linux.