Міністерство освіти і науки України
Міжнародний гуманітарний університет
Кафедра комп’ютерної інженерії та інноваційних технологій

СИСТЕМНЕ АДМІНІСТРУВАННЯ КОМП'ЮТЕРНИХ МЕРЕЖ

Конспект лекцій
для здобувачів вищої освіти,
які навчаються за спеціальностями
галузі «Інформаційні технології»

Одеса 2025

Лекція 1.Основи адміністрування та керування в комп'ютерних системах та мережах (КСМ)

1. Мета та завдання курсу. Основні поняття. Функції адміністратора КСМ

Метою викладання дисципліни «Адміністрування комп'ютерних систем та мереж» є: формування знань, що дозволяють застосовувати сучасні технології в комп'ютерних системах на етапах від проектування до експлуатації, узагальнення теоретичних знань на конкретних прикладах середовищ систем і сервісів, формування у студентів спеціальних знань у галузі керування сучасними системами і створення програмного забезпечення.

Завданнями викладання даної дисципліни є:

- ознайомлення з принципами роботи систем адміністрування та керування в інформаційних системах.
- вивчення програмної структури, функцій, спеціальних і загальної процедур адміністративного керування.
- визначенні місця досліджуваних процесів і апаратури серед інших технічних систем.

Навіщо потрібно системне адміністрування

Системне адміністрування необхідно, оскільки нам потрібні комп'ютери та мережі. Комп'ютери відіграють в нашому житті зараз значно важливішу роль, ніж раніше. Що сталося?

Широке поширення Інтернету, внутрішніх мереж і світова орієнтація на інтернет-технології визначили залежність компаній від комп'ютерів.

Інтернет працює за принципом 24/7 (24 години на добу, 7 днів на тиждень), і нестабільна робота тут неприпустима. Обробка замовлень може йти щодня безперервним потоком непомітно для користувачів. Однак від інтернет-систем очікують безперешкодної доступності в будь-який час з будь-якого місця. Нічні перерви на профілактику стали небаченою розкішшю.

Інформаційна система (англ. Information system) – сукупність організаційних і технічних засобів для збереження та обробки інформації з метою забезпечення інформаційних потреб користувачів. Для існування цивілізації необхідний обмін інформацією – передача знань, як між окремими членами і колективами суспільства, так і між різними поколіннями. Інформаційна система може існувати і без застосування комп'ютерної техніки – це питання економічної необхідності.

Комп'ютерна система – означає будь-який пристрій або групу взаємно поєднаних або пов'язаних пристроїв, один чи більш з яких, відповідно до певної програми, виконує автоматичну обробку даних (рис.1.1).

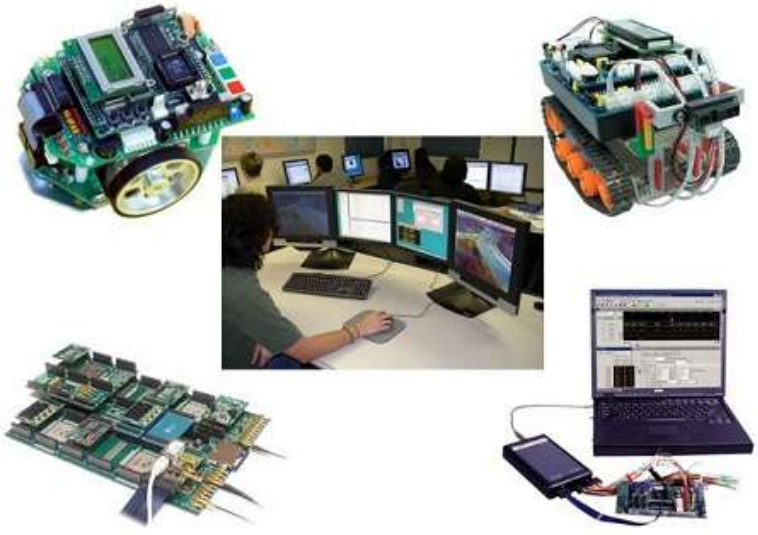


Рис. 1.1 – Різноманітні варіанти комп'ютерної системи

Комп'ютерна мережа – це система розподіленої обробки інформації між комп'ютерами за допомогою засобів зв'язку (рис. 1.2). Комп'ютерна мережа являє собою

сукупність територіально рознесених комп’ютерів, здатних обмінюватися між собою повідомленнями через середовище передачі даних.

Рис. 1.2 – Схематичне представлення комп’ютерної мережі

Адміністратор комп’ютерної системи або **системний адміністратор** (від англ. system administrator, systems administrator) – працівник, посадові обов’язки якого передбачають забезпечення роботи комп’ютерної техніки, комп’ютерної мережі і програмного забезпечення в організації. Системний адміністратор може бути працівником підрозділу інформаційних технологій або окремою штатною одиницею в залежності від розміру організації (рис 1.3).

Рис. 1.3 – Системний адміністратор в обчислювальному центрі

Системний адміністратор – **не розробник програмного забезпечення**. Зазвичай він не зобов’язаний писати прикладні чи системні програми. Однак, сисадмін повинен розуміти призначення і поведінку програмного забезпечення у випадку його розгортання чи застосування, пошуку помилок в програмах, а отже знати декілька мов програмування, щоб використовувати їх для написання скриптів (сценаріїв), які дозволяють автоматизувати рутинні завдання.

Якщо ви попросите шістьох системних адміністраторів описати свою роботу, ви отримаєте шість різних відповідей. Роботу системного адміністратора складно якось визначити, оскільки вона занадто різноманітна. системний адміністратор відповідає за комп'ютери, мережі та за людей, які їх використовують.

Системний адміністратор може відповідати за обладнання, операційні системи, програмне забезпечення, конфігурацію, додатки і безпеку. Від системного адміністратора залежить, наскільки ефективно інші люди використовують свої комп'ютери і мережі.

Час від часу системному адміністратору доводиться бути консультантом з бізнес-процесів, корпоративним віщуном, сторожем, розробником програм, інженером-електриком, економістом, психіатром, телепатом і навіть барменом.

Тому в різних компаніях посаду системного адміністратора може називатися по-різному. Іноді їх називають адміністраторами мереж, системними архітекторами, системними інженерами, системними програмістами, операторами і т. д.

В СРСР вживались назви системний інженер (відповідав за апаратне забезпечення ЕОМ), системний програміст («генерував» операційні системи, відповідав за системне програмне забезпечення), «системщик» – неофіційна назва цих двох професій.

Типові (функції) обов'язки системного адміністратора:

*****з точки зору адміністрування комп'ютерних систем

- підготовка і збереження резервних копій даних, їх періодична перевірка і знищення;
- встановлення і конфігурування оновлень операційної системи і прикладного програмного забезпечення;
- встановлення і конфігурування нового апаратного і програмного забезпечення;
- створення і підтримка в актуальному стані файлу облікових записів користувачів;
- підтримання інформаційної безпеки в організації;
- документування своєї роботи;
- усунення неполадок в комп'ютерній системі.

*****з точки зору адміністрування комп'ютерних мереж

- планування мережі;
- встановлення та налаштування мережевих вузлів;
- встановлення та налаштування мережевих протоколів;
- встановлення та налаштування мережевих служб.
- адміністрування служб каталогів (Novell NDS, Microsoft Active Directory);
- адміністрування служб обміну повідомленнями (системи електронної пошти);
- адміністрування служб доступу до баз даних;
- пошук несправностей;
- моніторинг мережевих вузлів та трафіку;
- забезпечення захисту даних.

День системного адміністратора, також відомий, як день сисадміна – неофіційне професійне свято системних адміністраторів, котре прийнято відзначати кожну останню п'ятницю липня. Метою свята є вияв поваги до роботи системних адміністраторів. Традицію святкування було започатковано 28 липня 2000 року Тедом Кекатосом (Ted Kekatos).

2. Основні принципи адміністрування комп'ютерних систем та мереж

1. Простота означає, що саме лаконічне рішення проблеми – це саме краще рішення. Це допомагає зберегти систему простою для розуміння і знижує кількість складних міжкомпонентних взаємодій, здатних перетворити налагодження в жах.

2. Ясність означає, що рішення має бути зрозумілим, щоб можна було його легко пояснити учасникам проекту або навіть стороннім. Ясність допомагає спростити зміни системи, а також її обслуговування і налагодження. В світі системного адміністрування краще написати п'ять рядків зрозумілого коду, ніж один рядок, незбагненного ні для кого, крім вас.

3. Універсальність означає, що рішення не повинно бути застосоване тільки в одному окремому випадку. Рішення повинні використовуватися повторно.

Використання відкритих, стандартних, незалежних від постачальника (розробника) протоколів робить системи більш гнучкими і дозволяє спростити
взаємозв'язок між програмними пакетами, тим самим поліпшивши обслуговування.

4. Автоматизація має на увазі заміну людської праці програмами. Автоматизація критично важлива. Вона підвищує однотипність і розширеність системи, полегшує навантаження адміністратора і позбавляє від утомливих повторюваних задач, надаючи системному адміністратору більше часу на поліпшення обслуговування.

5. Взаємодія з потрібними людьми може вирішити більше проблем, ніж програми або обладнання. Вам треба взаємодіяти з іншими системними адміністраторами і з вашими користувачами. Ви зобов'язані бути ініціатором взаємодії. Взаємодія гарантує, що всі працюють для досягнення одних і тих же цілей. Через неправильну взаємодію люди стають засмученими і роздратованими. Також в поняття взаємодії входить документація. Документація спрощує підтримку, обслуговування та модернізацію системи. Ефективна взаємодія і хороша документація також спрощують передачу проектів та обслуговування наступнику при переході на іншу роботу або іншу посаду.

6. Першочергове рішення базових проблем означає, що ви будуєте корпоративну мережу на надійному рівні, виявляючи і вирішуючи базові проблеми перш, ніж почнете боротися з проблемами більш високого рівня.

Першочергове вирішення базових проблем дозволяє значно спростити впровадження додаткової функціональності і робить служби більш стійкими до збоїв. Повноцінна базова інфраструктура може бути неодноразово вдосконалена для розвитку корпоративної мережі з відносно малими зусиллями.

Ці принципи універсальні. Вони грунтуються на всіх рівнях системи. Вони застосовуються до фізичних мереж і комп'ютерного обладнання. Вони застосовуються до всіх операційних систем у корпоративній мережі, всіх використовуваних протоколів, всього програмного забезпечення і всіх служб. Вони застосовуються в університетах, некомерційних організаціях, урядових мережах, в компаніях і на сайтах інтернет-послуг.

3. Практичні поради системним адміністраторам

Що робити якщо:

1. Необхідно впоратися з частими збоями в роботі комп'ютерів

- Використовуйте тимчасові прийоми для усунення помилок і повідомте користувачам, що це тимчасові заходи.
- Встановіть істинну причину збоїв.
- Усуньте справжню причину, а не симптоми.
- Якщо основна причина полягає в обладнанні, придбайте краще обладнання.
- Якщо основна причина полягає в умовах, поліпшите фізичні умови для вашого обладнання.
- Переустановіть систему.
- Навчіть ваших системних адміністраторів ефективніше використовувати інструменти діагностики.
- Якнайшвидше запустіть виробничу систему. Не варто грати в діагностичні гри з виробничими системами. Для цього існують лабораторії і заздалегідь оголошені профілактичні перерви (які, як правило, влаштовуються у вихідні або пізно ввечері).

2. Які робочі інструменти повинні бути у кожного системного адміністратора:

- Ноутбук із засобами мережевої діагностики, такими як мережевий аналізатор пакетів, DHCP-клієнт в режимі розширеного виводу, TELNET / SSH-клієнт з шифруванням, TFTP-сервер і т. д., а також провідна і беспровідна мережа Ethernet.
- Програмний емулятор терміналу і послідовний кабель. Ноутбук може зіграти роль послідовної консолі в екстрених ситуаціях, наприклад при збої консольного сервера, збої в консолі обчислювального центру або при необхідності отримати доступ до сервера за межами обчислювального центру.
- Додатковий комп'ютер або сервер для експериментів з новими конфігураціями.
- Портативний принтер для ярликів.
- КПК або неелектронний органайзер.
- Набір викруток всіх розмірів, що використовуються для комп'ютерів.
- Кабельний тестер.
- Пристрій для обтиску кабелю.
- Патч-кабелі різної довжини, в тому числі один або два 30-метрових. вони можуть бути корисні в самих непередбачуваних ситуаціях.
- Компактний цифровий фотоапарат. При необхідності можна відправити в службу підтримки знімок, який допоможе розшифрувати незрозумілі повідомлення в консолі, визначити номер моделі або стане підтвердженням ушкоджень.
- Портативний жорсткий диск з підключенням через USB / FireWare.

- Рація для підтримки зв’язку в будівлі.
- Шафа з робочими інструментами та комплектуючими.
- Високошвидкісний зв’язок з будинками співробітників відділу та необхідні засоби зв'язку.
- Бібліотека зі стандартним набором довідників за технологіями, з якими працюють системні адміністратори.
- Членство в професійних співтовариствах, таких як USENIX і LOPSA.
- Найрізноманітніші ліки від головного болю. Дуже складно вирішувати серйозні проблеми, якщо болить голова.
- Роздрукований та поміщений в рамку «Етичний кодекс системних адміністраторів».
- Стратегічний запас чіпсів (тільки для екстрених ситуацій).

3. Необхідно забезпечити повернення робочого інструменту

- Спростіть процес повернення робочих інструментів. На кожен з них наклейте ярлик з написом «Повернути [кому]».
- Якщо хтось щось у вас бере певну річ, відкрийте заявку в службі підтримки та закрийте її тільки після того, як вам повернуть вашу річ.
- Змиріться з тим фактом, що ваші речі можуть вам і не повернути. Навіщо засмучуватися через ситуацію, яку ви не в силах контролювати?
- Створіть загальну базу інструментів і складіть графік відповідальних осіб, які стежитимуть за наявністю необхідних інструментів і відстежуватимуть боржників.
- У вас завжди повинні бути запасні набори комп’ютерних викруток. Якщо хто-небудь попросить у вас одну викрутку, посміхніться і дайте відповідь: «Ні, але можете взяти в подарунок весь набір». Зворотно набір не беріть.
- Не давайте викрутки тим, хто відповідає тільки за програмне забезпечення. Чемно поцікавтесь, для чого їм потрібна викрутка, і все зробіть самі. Це заощадить вам час на виправлення чужих помилок.
- Якщо ви відповідаєте лише за програмне забезпечення, користуйтесь викруткою тільки під наглядом дорослих.
- У вас повинен бути запас недорогих наборів для ремонту окулярів.

4. Для чого потрібна документація та письмові інструкції:

- Якісна документація описує, для чого і як все робиться.
- Якщо все робиться правильно і все «просто виходить», навіть ви забудете подробиці, коли необхідно буде виправити або вдосконалити створені проекти.
- Вона дозволяє піти у відпустку.
- Можна зайнятися більш цікавими проектами, замість того щоб робити одне і те ж, будучи єдиною людиною, розуміючою принцип роботи створеного проекту.
- Щоб не справляти враження, ніби ви «придумуєте все на ходу».
- Інші люди не вміють читати ваші думки.

5. Хочеться позбутися від страждання при виконанні «цього жаху»

- Не виконуйте «цей жах».
- Автоматизуйте процеси, що виконують «цей жах».

6. Необхідно уникнути стресу

- Візьміть нарешті відпустку (триденні вихідні відпусткою не рахуються)!
- Нехай ваша відпустка буде достатньо тривалою, щоб за цей час точно з’ясувалося, яка інформація недостатньо документована. Краще відкладіть рішення проблем до вашого повернення через кілька днів, ніж через перевтому потрапити під автобус.
- Здійснюйте прогулянки. На деякий час спробуйте змінити обстановку.
- Не снідайте за своїм робочим столом.
- Не забувайте, що в житті є не тільки робота.
- Раз на тиждень або на місяць ходіть до масажиста.
- Запишіться на заняття йогою або медитацією.

Контрольні запитання:

1. Опишіть мету та завдання курсу «Адміністрування комп’ютерних систем та мереж».

2. Дайте визначення понять «Інформаційна система», «Комп'ютерна система», «Комп'ютерна мережа».
3. Хто такий «Системний адміністратор»?
4. «Що робити якщо…» поради системним адміністраторам.
5. Назвіть основні принципи адміністрування комп'ютерних систем та мереж.

Лекція 2. Робочі станції, сервери та обчислювальні центри

1. Робочі станції

Робоча станція (англ. *workstation*) – комплекс апаратних і програмних засобів, призначених для вирішення певного кола завдань (рис. 2.1).

Рис. 2.1 – Xerox Alto став в 1973 р. першим комп'ютером, який використовував графічний інтерфейс користувача з маніпулятором типу «миша» та мережу Ethernet

Робоча станція як місце роботи фахівця являє собою повноцінний комп'ютер або комп'ютерний термінал (пристрої введення-виведення, відокремлені і часто віддалені від керуючого комп'ютера), набір необхідного ПЗ, за необхідності доповнюються допоміжним обладнанням: принтер, зовнішній пристрій зберігання даних на магнітних та / або оптичних носіях, сканер штрих – коду тощо (рис. 2.2).

У радянській літературі також використовувався термін АРМ (**автоматизоване робоче місце**), але в більш вузькому сенсі, ніж «робоча станція» (вирішує конкретне коло завдань).

Також терміном «**робоча станція** (**клієнт**)» позначають стаціонарний комп'ютер у складі локальної обчислювальної мережі (ЛОМ) по відношенню до сервера, це комп’ютер який використовує ресурси сервера (на робочих станціях користувачі вирішують прикладні завдання (працюють з базами даних, створюють документи, роблять розрахунки, грають у комп'ютерні ігри. Сервер обслуговує мережу і надає власні ресурси всіх вузлів мережі, в тому числі і робочим станціям).

Рис. 2.2 – Робоча станція на три монітори

Існують досить стійкі **ознаки конфігурацій** робочих станцій, призначених для вирішення певного кола завдань, що дозволяє підрозділити їх на окремі професійні підкласи:

- мультимедіа і, зокрема, комп'ютерна графіка та обробка зображень, відео, звуку, розробка комп'ютерних ігор;
- різні інженерні, архітектурні (в тому числі містобудівні) та інші САПР, ГІС, польова робота і геодезія і т. д.;
- наукові та інженерно - технічні обчислення;
- професійні, для біржового інтернет-трейдингу.

Кожен такий підклас може мати властиві йому особливості та унікальні компоненти: великий розмір монітора або декілька моніторів (САПР, біржа), швидкодіюча відеокарта (кінематограф (у тому числі анімація), комп'ютерні ігри), великий обсяг накопичувачів даних (фотограмметрія, анімація), наявність професійного сканера (фотографія), захищене використання (військове застосування, експлуатація в польових умовах) і т.д.

2. Сервери та серверне обладнання

Сервер (англ. server від to serve – служити) апаратне забезпечення, виділене і / або спеціалізоване для виконання на ньому сервісного програмного забезпечення (у тому числі серверів тих чи інших завдань).

У комп'ютерній термінології термін може стосуватися окремого комп'ютера чи програми.

Сервер як комп'ютер – це комп'ютер у локальній чи глобальній мережі, який надає користувачам свої обчислювальні і дискові ресурси, а так само доступ до встановлених сервісів; найчастіше працює цілодобово, чи у час роботи групи його користувачів.

Сервер як програма – програма, що надає деякі послуги іншим програмам (клієнтам). Зв'язок між клієнтом і сервером зазвичай здійснюється за допомогою передачі повідомлень, часто через мережу, і використовує певний протокол для кодування запитів клієнта і відповідей сервера. Серверні програми можуть бути встановлені як на серверному, так і на персональному комп'ютері, щоразу вони забезпечують виконання певних служб (наприклад, сервер баз даних чи веб-сервер).

Сервери розміщуються у спеціально обладнаних приміщеннях, званих серверними кімнатами (рис. 2.3).

Рис. 2.3 – Серверна кімната Хемніцького технологічного університету.

Головною ознакою серверів є здатність машини чи програми переважну кількість часу працювати автономно, без втручання людини реагуючи на зовнішні події відповідно до встановленого програмного забезпечення.

Деякі сервісні завдання можуть виконуватися на робочій станції паралельно з роботою користувача. Таку робочу станцію умовно називають **невиділеним сервером.**

Перші сервери з'явилися в середині 1960-х років. У цей час сервери були дуже великими і складними машинами, які могли б обслуговувати тільки висококваліфікований персонал.

Роль – це функція сервера. Один сервер може відігравати декілька ролей одночасно. При реєстрації адміністратора на сервері майстер «Manage Your Server» допомагає додати нові ролі або змінити існуючі.

В залежності від функціонального призначення розрізняють файлові сервери (англ. File server), проксі-сервери, FTP-сервери, Web-сервери, DNS-сервери, SQL-сервери, термінальні сервери, інтернет-сервери, радіус-сервери та інші. Ці всі ролі можуть встановлюватися як на одну фізичну машину так і окремо на різні (**спеціалізовані сервери**).

Додавання ролі **файлового сервера** оптимізує сервер для підтримки спільних папок і зберігання файлів.

Сервери друку використовуються для надання та управління доступом до принтерів.

Поштовий сервер – дозволяє обслуговувати базові поштові скриньки користувачів і дозволяє приймати та відправляти пошту з сервера.

Після інсталяції ролі **термінального сервера**, ви можете дозволити користувачам підключатися до сервера і запускати на ньому програми так, як ніби ці програми були інстальовані на робочій станції клієнта.

Контролер домену містить базу даних Active Directory. Контролери домену надають служби аутентифікації для користувачів і комп'ютерів, а також керують доступом до мережевих ресурсів.

Сервер DNS дозволяє перетворювати доменні імена (FQDN) в адреси IP.

Сервер DHCP дозволяє клієнтам отримувати свій IP за потребою.

Ігровий сервер – програмний компонент обчислювальної системи, що забезпечує зв'язок між різними клієнтами, надаючи їм можливість комунікації один з одним в рамках програмної оболонки конкретної гри.

Сервер додатків – роль сервера в сімействі продуктів Windows Server, яка поєднує в собі різноманітні серверні технології (Internet Information Services (IIS), Microsoft .NET Framework).

Проксі-сервер

На проксі-сервері автоматично зберігається деякий час вся інформація, яка через нього проходить. Якщо проксі-сервер виявить запит даних, вже наявних в нього, то саме ця копія буде направлена користувачеві.

Крім того, включення проксі-сервера в настройки Інтернет-браузеру дозволяє підвищити швидкість перегляду мережі. Це пов’язано з тим, що багато файлі вже не доводиться отримувати з Мережі: швидкість завантаження файлів з проксі-сервера, розташованого зазвичай «поблизу» користувальницького комп’ютера, вище швидкості отримання даних з віддалених хостів. Крім того, сучасні проксі-сервери мають розвинені засоби управління трафіком: на них можна блокувати вміст за тими чи іншими критеріями, нарізати смуги пропускання для користувачів і т. д.

Особливості серверного обладнання

- *надійність* – серверне обладнання найчастіше призначене для забезпечення роботи сервісів в режимі 24/7, тому часто комплектується дублюючими елементами, що дозволяють забезпечити «п'ять дев'яток» (99,999%; час недоступності сервера або простою системи складає менше 6 хвилин на рік). *Напр.* гаряче підключення і заміна (англ. Hot-swap) критично важливих компонентів, використання жорстких дисків у складі масиву RAID.
- *розміри та інші деталі зовнішнього виконання* – сервери (і інше устаткування), яке потрібно встановлювати на деяке стандартне шасі (наприклад, так звані блейд-сервери) створюються стандартних розмірів і комплектуються необхідними кріпильними елементами.
- *ресурси* – за ресурсами (частота і кількість процесорів, кількість пам'яті, кількість і продуктивність жорстких дисків, продуктивність мережевих адаптерів) сервери спеціалізуються у двох протилежних напрямках – нарощуванні ресурсів та їх зменшенні (збільшується площа та продуктивість – зменшується площа, енергоспоживання). Спочатку сервери у продажу йдуть в базовій комплектації, але з закладеним потенціалом до «апгрейду» – апаратна масштабованість.

Блейд-сервери (англ. blade – лезо) – комп'ютерні сервери з компонентами, встновленими в стійці для зменшення займаного простору (рис. 3.4). Називають також ультракомпактними серверами.

Стійка – шасі для блейд-серверів, що надає їм доступ до загальних компонентів, наприклад, блоків живлення та мережевих контролерів.

Рис. 2.4 – Блейд-сервери в стійці

Блейд-сервер являє собою «урізаний» сервер з модульною конструкцією. Це зводить до мінімуму використання фізичного простору і енергії. У блейд-сервері деякі компоненти відсутні для економії місця, що зводить до мінімуму споживання енергії. В той же час вони мають всі пристрої, щоб вважатися комп'ютером. Блейд-стійка, яка може містити кілька блейд-серверів, виконує такі функції, як електроживлення, охолодження, мережеві функції, функції різних з'єднань та управління.

В стандартних серверних стійках мінімальний розмір сервера прийнято називати 1U або 1 юніт (19 дюймів в ширину x 1,75 дюйма у висоту). Як правило, такі стійки вміщають 42 юніта обладнання, тобто максимум 42 сервера. Використання блейд-серверів дозволяє обійти це обмеження не виходячи за розміри стандартів стійки і розмістити до 100 серверів в кожній.

RAID (англ. redundant array of independent disks – надлишковий масив незалежних дисків) – масив з декількох дисків (запам'ятовуючих пристроїв), керованих контролером, пов'язаних між собою швидкісними каналами передачі даних які сприймаються зовнішньою системою як єдине ціле. Залежно від типу використовуваного масиву може забезпечувати різні ступені відмовостійкості і швидкодії. Служить для підвищення надійності зберігання даних і / або для підвищення швидкості читання / запису.

Кластер – це декілька незалежних обчислювальних машин, що використовуються спільно і працюють як одна система для вирішення тих чи інших задач, наприклад, для підвищення продуктивності, забезпечення надійності, спрощення адміністрування тощо (рис. 2.5). Обчислювальний кластер потрібен для збільшення швидкості обрахунків за допомогою паралельних обчислень.

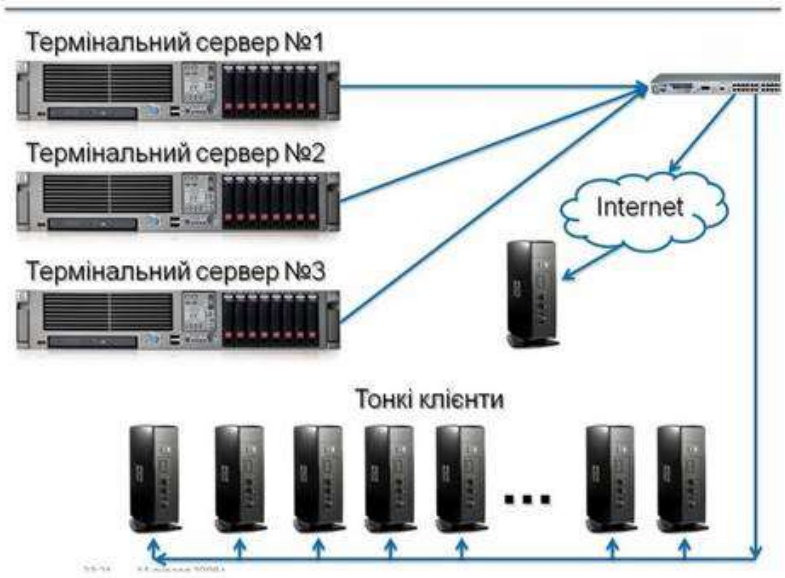


Рис. 2.5 – Термінальний кластер

Мейнфрейм (англ. Mainframe) – даний термін має два основні значення:

- велика універсальна ЕОМ – високопродуктивний комп'ютер із значним обсягом оперативної і зовнішньої пам'яті, призначений для організації централізованих сховищ даних великої місткості і виконання інтенсивних обчислювальних робіт.
- комп'ютер з архітектурою IBM System/360, 370, 390, zSeries (рис. 2.6).

Історію мейнфреймів прийнято відлічувати з появи в 1964 році універсальної комп'ютерної системи IBM System/360, на розробку якої корпорація IBM витратила $5 млрд. Сам термін «мейнфрейм» походить від назви типових процесорних стійок цієї системи. В 1960-х – початку 1980-х років System/360 була беззастережним лідером на ринку. Її клони випускалися в багатьох країнах, у тому числі – в СРСР (серія ЄС ЕОМ).

Мейнфрейми IBM використовуються в більш ніж 25 000 організаціях по всьому світу (без урахування клонів). Близько 70% всіх важливих бізнес-даних зберігаються на мейнфреймах.

Рис. 2.6 – Типовий сучасний мейнфрейм

На початку 1990-х почалася криза ринку мейнфреймів, пік якої припав на 1993 рік. Багато аналітиків заговорили про повне вимирання мейнфреймів, про перехід від централізованої обробки інформації до розподіленої (за допомогою персональних комп'ютерів, з'єднаних дворівневою архітектурою «клієнт-сервер»). Багато хто став

сприймати мейнфрейми як вчорашній день обчислювальної техніки, вважаючи Unix- і PC-сервери більш сучасними і перспективними.

Згідно з одним із прогнозів Gartner Group, останній мейнфрейм передбачалося усунути в 1993 році. Термін цього прогнозу давно закінчився, а ринок мейнфреймів залишається стабільним, і їх продажі щорічно ростуть.

На відміну від робочих станцій, призначених для одного користувача, від сервера залежить безліч користувачів. Отже, головним пріоритетом для них стає надійність і безперебійна робота. До сервера можуть підключатися сотні, тисячі або навіть мільйони користувачів. Всі зусилля з підвищення продуктивності або надійності наштовхуються на бар'єр величезної кількості користувачів. Сервери розраховуються на більш тривалий час роботи, ніж робочі станції, що також має на увазі додаткові витрати.

Устаткування, що продається як сервер, якісно відрізняється від устаткування, купленого для індивідуальної робочої станції. У серверного обладнання інші можливості, а при його розробці враховується інша економічна модель. Сервери розміщують в обчислювальних центрах з контрольованим мікрокліматом і з обмеженим доступом до серверного обладнання.

Купуйте для серверів серверне обладнання

Часто робляться спроби заощадити за рахунок покупки персонального комп'ютера і установки на нього серверного програмного забезпечення. Таке рішення може допомогти на короткий термін, але це не кращий вибір для довгострокових або великих проектів, які мають бути надійніше карткового будиночка. Серверне обладнання зазвичай коштує дорожче, але додаткові можливості виправдовують вкладення. Ось деякі з цих можливостей:

Розширюваність. Як правило, в серверах більше фізичного простору для жорстких дисків і більше слотів для карт розширення і центральних процесорів або вони оснащені роз'ємами з високою пропускною здатністю для підключення спеціалізованих периферійних пристроїв (рис. 2.7).

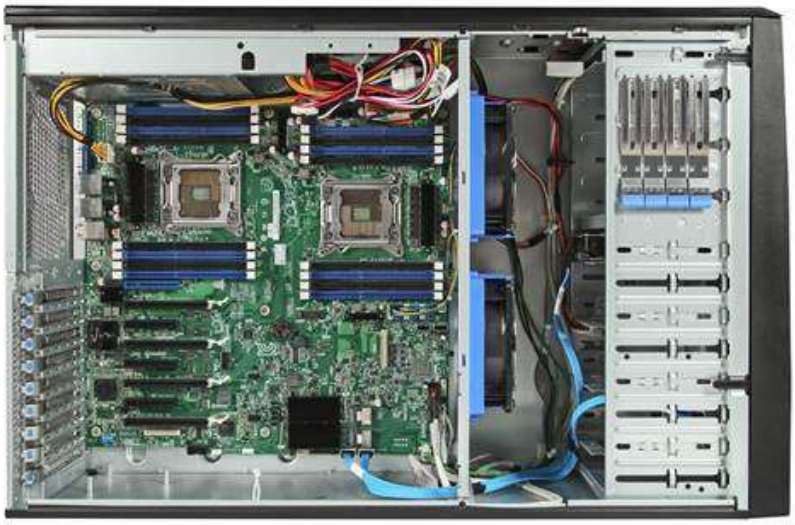


Рис. 2.7 – Сервер із двома сокетами

Велика продуктивність центральних процесорів. Сервери часто обладнують декількома ЦП, а також сервери володіють додатковими можливостями обладнання, такими як багатоступенева перевірка процесорів і динамічний розподіл ресурсів між ЦП і т.д.

Високопродуктивні системи обміну інформацією (введення-виведення). Сервери, як правило, більш продуктивні в плані обміну інформацією (введення-виведення), ніж клієнти. Можливості введення-виведення часто пропорційні кількості користувачів, що виправдовує застосування швидкісних підсистем вводу-виводу.

Можливості модернізації. Сервери частіше модернізують, а не просто замінюють, вони призначені для зростаючих потреб. На серверах, як правило, мається можливість додавати процесори або замінювати окремі процесори на більш швидкі, що не вимагає додаткових апаратних змін.

Можливість монтування в стійку. Сервери повинні мати можливість встановлення в стійки. Якщо настільний комп'ютер може розміщуватися в пластмасовому корпусі обтічної

форми, сервер повинен мати прямокутну форму для ефективного використання простору в стійці. Всі кришки, які потрібно знімати при ремонті, повинні зніматися без необхідності вилучення сервера зі стійки. Ще важливіше те, що сервер повинен бути сконструйований з урахуванням охолодження і вентиляції при монтуванні в стійку. Система, у якої вентиляційні отвори розташовані тільки з одного боку, не зможе підтримувати свою температуру в стійці так само добре, як система з наскрізною вентиляцією від передньої панелі до задньої.

Не потрібно доступ з бічних сторін. Комп'ютер має бути простіше ремонтувати і обслуговувати, якщо він встановлений в стійку. Виконання цих завдань не повинне вимагати доступу до бічних стінок машини. Всі кабелі повинні бути ззаду, а всі відсіки приводів і дисків - спереду. Існують відсіки для DVD-приводів, розташовані збоку, а це свідчить про те, що при конструюванні можливість установки в стійку не враховувалася.

Доповнення для підвищеної надійності. Багато серверів володіють додатковими можливостями, що підвищують надійність, такими як дубльовані джерела живлення, RAID, кілька мережевих карт і компоненти з підтримкою «гарячої» заміни.

Альтернативні варіанти управління. В ідеалі сервери повинні мати підтримку функцій віддаленого управління, таких як доступ через послідовний порт, який може бути використаний для діагностики та вирішення проблем, щоб відновити збійну машину. Деякі сервери також постачаються з вбудованими датчиками температури та іншими апаратними засобами моніторингу, які можуть генерувати оповіщення при виявленні проблем.

Зокрема, вплив ринку змушує постачальників покращувати сервери, щоб було можливо розміщувати більше одиниць в **колокейшн-центрах** - орендованих обчислювальних центрах, де оплата йде за одиницю площі.

Вибирайте постачальників, відомих надійністю продукції

Дуже важливо вибирати постачальників, продукція яких відома своєю надійністю. Деякі постачальники економлять за рахунок використання компонентів споживчого класу, інші використовують компоненти, які відповідають певним стандартам наприклад військовим.

Реальні витрати на серверне обладнання

Щоб мати уявлення про додаткові витрати на сервери, ви повинні знати, з чого складається ціна комп'ютера.

У більшості постачальників є три серії продукції: для дому, для бізнесу і серверне обладнання. Домашня серія зазвичай продається за найменшою початковою ціною, так як клієнти найчастіше приймають рішення про покупку на підставі рекламованої ціни. Доповнення і можливість розширення в майбутньому доступні за вищою ціною. При описі компонентів використовуються загальні технічні характеристики, такі як розширення екрана, замість зазначення конкретного виробника та моделі відеокарти.

Персональні комп'ютери для бізнесу зазвичай розробляються з урахуванням загальних витрат протягом усього терміну їх служби. Початкова закупівельна ціна вища, ніж для домашніх комп'ютерів, адже серія для бізнесу повинна довше не старіти. Компаніям невигідно утримувати велику кількість запасних компонентів, не кажучи вже про вартість навчання техніків з ремонту для кожної моделі.

Серверні серії зазвичай орієнтовані на найкраще співвідношення собівартості і продуктивності. Наприклад, файловий сервер може конструюватися з розрахунком на мінімальну вартість продуктивності по тесту SPEC SFS9731 в перерахунку на закупівельну ціну кожної машини.

Сервери коштують дорожче і з інших причин. Корпус, який зручніше для обслуговування, може бути дорожче у виробництві. Існують обмеження на розташування відсіків для дисководів та інших панелей, доступ до яких має бути тільки з певного боку, - це має на увазі, що їх не можна розмістити так, щоб здешевити конструкцію.

Невірно вважати, що сервери дорожче настільних комп'ютерів, так як це порівняння об'єктів різного роду. Розуміння цієї відмінності моделей ціноутворення допомагає в обговоренні, коли потрібно обґрунтувати гадану дорожнечу серверного устаткування. Крім того, простій сервера обходиться значно дорожче простою настільного комп'ютера.

Забезпечення цілісності даних

На серверах зберігаються критично важливі дані і унікальні конфігурації, які повинні бути захищені.

Розміщення серверів в обчислювальному центрі

Сервери повинні встановлюватися в умовах з надійними енергопостачанням, протипожежним захистом, мережею, охолодженням і фізичної безпекою

Філії та навіть деякі компанії не завжди достатньо великі, щоб мати обчислювальні центри. Проте у всіх має бути виділена кімната або шафа, що забезпечують як мінімум фізичну безпеку, джерело безперебійного живлення (кілька дрібних або один великий) і достатнє охолодження. Краще придбати шафу для телекомунікаційної апаратури з хорошим охолодженням, що закривається на замок дверцятами, ніж робити розрахунок заробітної плати на сервері, що стоїть у когось під столом.

Конфігурація клієнт-серверної ОС

Сервери необов'язково повинні працювати під управлінням тих же ОС, що і їх клієнти. Сервери можуть бути зовсім іншими. Для різних випадків підходять різні варіанти. Наприклад, веб-серверу не потрібно працювати під керуванням тієї ж ОС, що і у клієнтських машин. Клієнти і сервер повинні лише використовувати однаковий протокол. На однофункціональних мережевих спеціалізованих пристроях часто буває встановлена міні-ОС з програмним забезпеченням, мінімально достатнім для виконання єдиної функції (файл-сервер, веб-сервер, поштовий сервер).

Ще один цікавий момент, характерний для серверної ОС, – орієнтованість на перспективу. При установці Solaris 2.x ви можете відзначити, що цей вузол мережі – сервер, на якому встановлені всі програмні пакети, тому що бездискові клієнти або машини з малим об'ємом жорстких дисків можуть використовувати NFS для завантаження необхідних пакетів з сервера. З іншого боку, серверна конфігурація при установці Red Hat Linux – це мінімальний набір пакетів, що припускає, що вам потрібна тільки базова установка, поверх якої ви встановите спеціалізовані програмні пакети, необхідні для створення служб. У зв'язку із зростанням обсягу жорстких дисків останній підхід став більш поширеним.

Забезпечення віддаленого доступу через консоль

Консоль (зазвичай – монітор / клавіатура / миша) і участь людини необхідні серверам тільки на стадії первинної настройки, при апаратно-технічному обслуговуванні та управлінні в нештатних ситуаціях (штатно, більшість серверів управляються віддалено). Для нештатних ситуацій сервери зазвичай забезпечуються одним консольним комплектом на групу серверів (з комутатором, наприклад KVM-перемикачем, або без такого).

Для серверів необхідна можливість віддаленого обслуговування. У минулому для кожного сервера в машинному залі була передбачена власна консоль: клавіатура, відеомонітор або консольний вивід на друк і, можливо, миша. У міру того як системні адміністратори встановлювали все нове обладнання в машинному залі, відмова від цих консолей дозволила звільнити значний простір.

Перемикач KVM (рис. 2.8) – пристрій, що дозволяє декільком машинам використовувати одну клавіатуру, відеоекран і мишу (KVM). Наприклад, можна встановити три сервера і три консолі в одну телекомунікаційну стійку. Однак завдяки комутатору KVM для цієї стійки достатньо тільки однієї клавіатури, монітора і миші. Таким чином, в ту ж стійку можна встановити більшу кількість серверів. Можна заощадити ще більше місця, якщо встановити один комутатор KVM на ряд стійок або на весь обчислювальний центр. Однак більші комутатори KVM, як правило, надмірно дорогі. Можна звільнити ще більше простору за допомогою IP-KVM, тобто KVM, в яких немає ні клавіатури, ні монітора, ні миші. Досить просто підключитися до консольного серверу KVM по мережі з програмного клієнта на іншій машині. Це можна зробити навіть з ноутбука в кафе, якщо ноутбук підключений через VPN до вашої мережі.

Рис. 2.8 – Електронний KVM-перемикач на 4 пристрої

Послідовні консолі і перемикачі KVM дають таку перевагу: вони дозволяють вам керувати системною консоллю, якщо відеосистема не працює або якщо система в несправному стані. Наприклад, певні операції можна виконувати тільки при перезавантаженні системи. Серед них натискання певних клавіш для виходу в меню BIOS. Зрозуміло, для IP-KVM вимагається працездатна мережу між вами і консоллю IP-KVM, але інша мережа необов'язково повинна працювати.

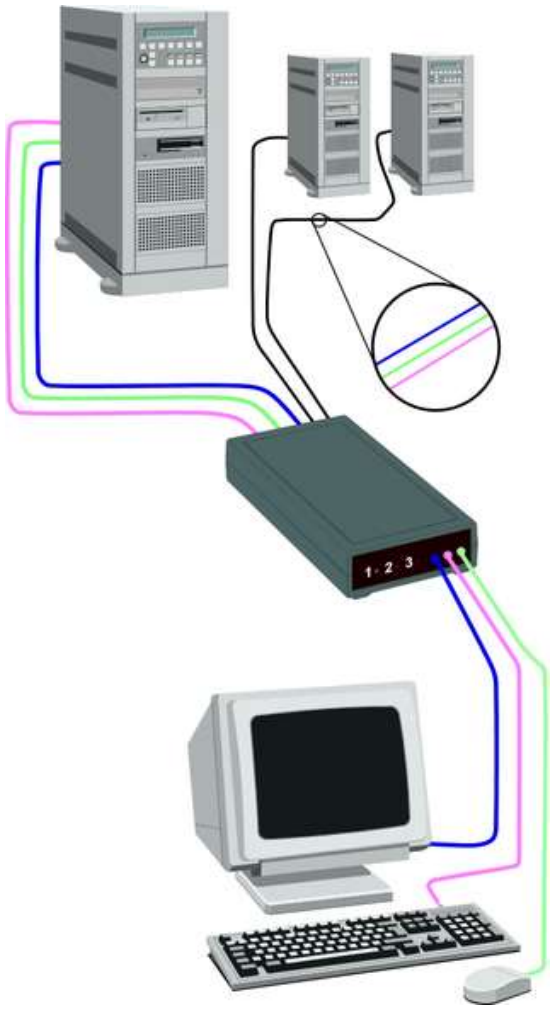


Рис. 2.9. Схема підключення декількох комп'ютерів до одного робочого місця за допомогою KVM-перемикача

Однак у віддаленого доступу є очевидні обмеження через те, що окремі завдання (включення і виключення живлення, завантаження змінних носіїв, заміна несправного обладнання) вимагають присутності людини біля машини. Черговий оператор або доброволець, готовий допомогти, може стати очима і руками віддаленого фахівця. Деякі системи дозволяють віддалено включати і вимикати окремі роз'єми живлення, що, в свою чергу, дозволяє віддалено проводити повне перезавантаження. Однак заміна обладнання і раніше залишається завданням для досвідчених професіоналів.

Не варто очікувати, що системні адміністратори будуть весь день проводити в машинному залі. Робота системних адміністраторів в машинному залі шкідлива і для залу, і для адміністраторів. Робота безпосередньо в машинному залі рідко відповідає вимогам ергономіки для клавіатури і миші та вимогам умов праці, таким як рівень шуму. Перебувати в холодному машинному залі шкідливо для здоров'я. Системним адміністраторам потрібно створити умови, які максимально поліпшують продуктивність праці, а це найпростіше здійснити в офісах. На відміну від машинного залу, в офісі простіше розмістити таке важливе обладнання для системного адміністратора, як довідкова література, ергономічна клавіатура, телефони, холодильники і стереосистеми.

Віддзеркалення завантажувальних дисків

Завантажувальний диск, або диск з операційною системою, як правило, найважче замінити в разі його пошкодження. Тому необхідно дотримуватися особливих заходів безпеки, щоб прискорити процес відновлення. Для завантажувального диска кожного сервера необхідно створити дзеркальний диск. Це означає, що встановлено два диска і при будь-якому оновленні основного диска тут же оновлюється і другий. Якщо один з дисків відмовить, система автоматично переключиться на працездатний диск. Більшість операційних систем дозволяють зробити це програмно, а багато контролери жорстких дисків роблять це на апаратному рівні. Цей метод називається RAID (рис. 2.9).

З роками вартість жорстких дисків значно знизилася, і ця колись надто дорога можливість стала більш доступною. В ідеалі всі диски повинні віддзеркалюватись, або бути захищені RAID-схемою. Однак, якщо ви не можете собі цього дозволити, створіть дзеркало хоча б для завантажувального диска.

Рис. 2.9 – Апаратний RAID масив

Компоненти, що підтримують «гарячу» заміну

Резервні компоненти повинні підтримувати «гарячу» заміну. «Гаряча» заміна мається на увазі можливість відключити і замінити компонент під час роботи системи. Як правило, компоненти слід замінювати тільки при відключеній системі. Можливість «гарячої» заміни аналогічна зміні покришки в той момент, коли автомобіль мчить по шосе. Дуже зручно, коли не доводиться зупинятися, щоб усунути звичайну проблему.

«Гаряче» підключення або «гаряча» заміна

Завжди звертайте увагу, на зазначення на ярлику компонента можливості «гарячого» підключення (hot plug). Це означає, що заміна компонента під час роботи системи безпечна для електроніки, однак цей компонент може бути розпізнаний тільки після наступного перезавантаження системи. Або, що ще гірше, підключити компонент можна до працюючої системи, але система буде тут же перезавантажена, щоб розпізнати цей компонент. А це значно відрізняється від «гарячої» заміни.

Повна надмірність, або n + 1

Надмірність n + 1 відноситься до систем, які спроектовані таким чином, що система продовжує функціонувати навіть після збою одного з компонентів. Прикладом такої системи є RAID-масиви, які продовжують повноцінно функціонувати навіть після виходу з ладу одного з дисків, або комутатор Ethernet з додатковою багатовхідною системою комутації, який дозволяє передавати трафік навіть після збою одного з сегментів системи комутації.

Навпаки, при повній надмірності два повних набори обладнання об'єднані в відмовостійку конфігурацію. Перша система забезпечує виконання служби, а друга в повній готовності взяти на себе роботу при збої першої системи. Перемикання на резервні потужності може здійснюватися вручну (хтось помічає збій в першій системі і активує другу) або автоматично (друга система відстежує роботу першої системи і сама активується при її відмові).

Якщо n дорівнює або більше 2, n + 1 вигідніше, ніж повна надмірність. Користувачі зазвичай воліють використовувати цей метод через його економічність.

Як правило, надмірність n + 1 використовується тільки для серверних підсистем, а не для всіх видів компонентів. Завжди перевіряйте, чи не намагається постачальник вам продати систему з надмірністю n + 1, де резервними є тільки деякі частини системи. Який зиск в автомобілі з додатковими покришками, якщо зламається двигун?

Роздільні мережі для адміністративних функцій

Додаткові мережеві інтерфейси на серверах дозволяють створити роздільні адміністративні мережі. Наприклад, часто створюють окрему мережу для резервного копіювання та моніторингу. Резервне копіювання вимагає високої пропускної здатності, і

відділення цього трафіку від основної мережі означає, що резервне копіювання не заважатиме користувачам працювати з мережею.

Альтернатива: безліч недорогих серверів

Професіонали рекомендують не економити на серверному обладнанні, так як підвищення швидкодії і надійності коштує додаткових витрат.

Однак все частіше ми стикаємося із зустрічною думкою, відповідно до якої краще використовувати декілька недорогих однакових серверів, які будуть давати збої частіше. Якщо ви вмієте непогано справлятися зі збоями, така стратегія буде для вас більш вигідною.

Запуск крупної веб-ферми потребує використання декількох резервних серверів. Всі ці сервери повинні бути налаштовані абсолютно однаково - шляхом автоматичного встановлення. Якщо кожен веб-сервер здатний обробляти 500 запитів в секунду, вам знадобиться десять серверів, щоб обробляти 5000 запитів в секунду, які, як ви припускаєте, надходитимуть від користувачів Інтернету. Механізм розподілу навантаження може розподіляти навантаження серед серверів. Але що найкраще, системи розподілу навантаження можуть автоматично визначати машини, в роботі яких стався збій. Якщо один сервер «падає», механізм розподілу навантаження розподіляє запити між рештою робочими серверами і користувачі продовжують отримувати доступ до сервісу. При цьому завантаження кожного сервера підвищується на одну десяту, але це краще простою в роботі.

Сервер – це обладнання. **Сервіс** – це функція, яку надає сервером. Сервіс може бути скомпонований на декількох серверах, які працюють спільно один з одним.

Запасні елементи

Постарайтеся придбати запасні частини до обладнання, яке купуєте. Зазвичай сервісні контракти після 3-4 років експлуатації стають дуже дорогими, а придбати деталі стає неможливим, оскільки вони перестають випускатися у зв'язку з переходом на нові моделі. Наприклад, для серверів необхідно придбати запасні жорсткі диски та блоки живлення. Ці деталі найчастіше відмовляють під час експлуатації.

Вибір процесора

Сервери початкового рівня вибираються зазвичай з x86-процесорами. Для більш потужних систем можливе використання процесорів іншої архітектури, але цей вибір зазвичай диктується додатком (завдання SAP зазвичай реалізують на потужних обчислювальних процесорах серії Power, сервери баз даних Oracle оптимізовані під власні сервери з процесорами архітектури RISC і т. Д.).

Число ядер, частота і т. д. вибирається на основі вимог проекту. У разі планування віртуалізації необхідно покращувати конфігурацію приблизно на 20%.

Вибір материнської плати

Сервер повинен бути укомплектований системою out-of-band-управління. Ця система дозволяє за допомогою окремого мережевого інтерфейсу моніторити стан сервера, вмикати і вимикати його, програмно віддалено монтувати образи CD / DVD і т. д. Зазвичай серверні плати включають дану опцію за замовчуванням, але є моделі, в яких вона є додатковим компонентом.

Вибір дисків

Бажано зберігати й обробляти дані на спеціалізованих пристроях – системах зберігання даних (СЗД). На ринку представлено багато моделей таких пристроїв, доступних або дорогих, з більшим чи меншим функціоналом.

Можна купити платформу з великим числом жорстких дисків і встановити на неї програмне забезпечення серверів зберігання даних (у тому числі, і безкоштовне). Варіантів багато, в будь-якому випадку перехід на СЗД дозволить більш раціонально використовувати дисковий простір і підвищити надійність системи. Якщо дані будуть зберігатися локально, то спочатку потрібно встановити в сервер максимальне число дисків. Це підвищить продуктивність дискової підсистеми. При цьому потрібно продумати, як будуть сформовані масиви. Зазвичай створюють RAID (Redundant Array of Independent Disks – надлишковий (резервний) масив незалежних дисків) 5-го рівня з усіх дисків сервера, який потім розбивають (або не розбивають) на декілька логічних. Це найекономічніший варіант відмовостійкого масиву, але не найоптимальніший. Наприклад, тип масиву повинен бути різним для розміщення журналів сервера баз даних і для файлів самої бази.

Вибір пам'яті

Часто фахівці намагаються доповнити рекомендовану конфігурацію системи модулями оперативної пам'яті. Бажання зрозуміле, але не слід випускати з уваги той факт, що швидкість роботи з пам'яттю може залежати від її конфігурації – числа встановлених модулів. Легко може виявитися так, що, додавши нові модулі пам'яті, ви одночасно знизили вдвічі швидкість обміну даними з нею.

Сумісність компонентів

І останнє. Всі компоненти сервера повинні бути сумісні. Врахувати всі вимоги, щоб виключити помилки, досить складно. Тому вендори пропонують спеціальні конфігуратори, за допомогою яких можна сформувати бажаний сервер. Цими конфігураторами користуються самі фахівці вендорів, також вони доступні і для пересічних покупців.

3. Обчислювальні центри

Цей розділ присвячений створенню **обчислювального центру** – місця, в якому знаходяться машини, що оперують загальними ресурсами. Однак обчислювальний центр – не просто кімната з серверами. Як правило, обчислювальний центр оснащений системами охолодження, регулювання вологості, електроживлення та протипожежними системами. Всі ці системи – частина вашого обчислювального центру. За теорією ви повинні зібрати всі найбільш важливі компоненти в одному місці, а потім стежити, щоб це місце було досить надійним.

Дата-центр (англ. Data center, Центр зберігання та обробки даних (ЦЗОД), центр Обробки даних (ЦОД) – спеціалізований технічний майданчик для розміщення інформації в мережі Інтернет, підключений до неї в автономну систему (або мережі в її складі) по множині каналів зв'язку.

Ці приміщення відповідають різним умовам і трохи відрізняються один від одного. Найчастіше обчислювальні центри – це окремі будівлі, побудовані спеціально для обчислювальних і мережевих операцій. **Машинний, або комп'ютерний, зал** – менш значне приміщення, можливо, переобладнане із звичайного офісного. Найменші приміщення подібного типу часто жартівливо називають **комп'ютерними комірками** .

Основи

На перший погляд може здатися, що створити обчислювальний центр досить просто. Потрібен тільки великий зал зі столами, стійками або сітчастими стелажами – і все! Насправді основи створення гарного, надійного обчислювального центру, який дозволить системним адміністраторам працювати ефективніше, значно складніше. Для початку вам знадобиться вибрати серверні стійки і мережеві кабелі, підготувати живлення, яке подаватиметься до обладнання; буде потрібно серйозне охолодження і потрібно продумати систему пожежогасіння. Крім того, ви повинні грунтовно спланувати стійкість приміщення до стихійних лих. Правильна організація залу має на увазі продуману розводку кабелів, службу консолей, позначку ярликами, наявність інструментів, запасних частин, робочих місць і місць паркування для пересувних пристроїв. Також вам знадобиться опрацювати механізми безпеки обчислювального центру і продумати способи транспортування обладнання в зал і з залу.

Розміщення

По-перше, вам потрібно вирішити, де буде розміщуватися обчислювальний центр.

Якщо це буде центральний вузол для офісів по всьому світу або в межах географічного регіону, то спочатку доведеться вибрати місто і будівлю в цьому місті. Коли будівля вибрано, необхідно вибрати відповідне місце всередині будівлі. На всіх цих етапах при прийнятті рішення слід приймати до уваги стихійні лиха, типові для цього регіону.

Крім того, ви повинні бути готові до того, що чийсь екскаватор випадково пошкодить ваші лінії енергопостачання і зв'язку, незалежно від того, наскільки добре ви захиститеся від стихійних лих

Приклад: бункери – самі захищені обчислювальні центри

Доступ

Місцеві закони в деякій мірі визначають доступ в ваш обчислювальний центр і, наприклад, можуть вимагати наявності як мінімум двох виходів або пандусів для інвалідних колясок, якщо у вас настелений фальшпол. Крім цих міркувань, ви повинні продумати, як будете переміщати стійки та обладнання в зал.

Деякі елементи обладнання можуть бути ширше стандартних дверних прорізів, так що вам можуть знадобитися більш широкі двері. Якщо у вас подвійні двері, переконайтеся, що між ними немає стояка.

В одній з молодих компаній Силіконової долини не було завантажувальної платформи. Одного разу до них прийшла велика партія серверів, які довелося залишити на вулиці біля будівлі, бо не було можливості вивантажити їх з вантажівки прямо в будівлю. Частина серверів була на піддонах, які доводилося розбирати і по частинах переносити до входу в будівлю. Інші, досить дрібні частини відвозили в будівлю по пандусу для інвалідних колясок. Але деякі частини були настільки великими, що жоден з цих способів не підходив і їх перевозили по сталевому пандусу в гараж; там їх втискували в невеликий підйомник і піднімали на рівень поверху, де знаходився комп'ютерний зал.

На щастя, справа була влітку в Каліфорнії і під час цього тривалого процесу не почався дощ.

Безпека

Обчислювальний центр повинен бути фізично захищений настільки, наскільки це можливо зробити, не перешкоджаючи роботі системних адміністраторів. Доступ повинен надаватися тільки тим, чиї обов'язки того вимагають: технікам з обслуговування апаратури, операторам резервних копій на стримерах, мережевим адміністраторам, фахівцям з матеріальної частини та техніки безпеки, а також обмеженому числу керівників. Відповідальний за пожежну безпеку і, в деяких випадках, аварійні бригади, приписані до цієї зони, повинні призначатися з тих, у кого вже є доступ.

Електрика та охолодження

Енергопостачання та охолодження обчислювального центру безпосередньо взаємопов'язані. Обладнання працює від електрики, охолодження бореться із теплом, виділеним апаратурою при її роботі. При дуже високій температурі обладнання може працювати з помилками або навіть згоріти.

Як правило, на кожен ват, споживаний вашим обладнанням, вам доведеться витратити щонайменше 1 ват на охолодження. Тепло, що виділяється устаткуванням, що споживають 10 кВт, зажадає системи охолодження на 10 кВт (насправді швидше 11 або 12 кВт, враховуючи неефективність системи). Це закони термодинаміки. Значить, половина вашого рахунку за електрику йде на охолодження, а половина – на живлення обладнання. Крім того, це означає, що апаратура, яка споживає менше електроенергії, економить її вдвічі більше за рахунок меншої потреби в охолодженні.

Електроживлення обчислювального центру має бути згладженим, або стабілізованим, щоб захистити обладнання від стрибків і спадів напруги, звичайних в електричній мережі.

Системи пожежогасіння

Настійно рекомендується встановити в обчислювальному центрі систему пожежогасіння, навіть якщо цього не вимагають місцеві законодавчі акти.

Блоки живлення, диски і т.д. можуть випадково перегоріти або спалахнути. При проблемах з електропроводкою може виникнути іскра, яка підпалить знаходяться поблизу матеріали.

Стійки

Устаткування в обчислювальному центрі, як правило, кріпиться в стійки. На перший погляд стійки грають не таку вже важливу роль. Це всього лише металевий прокат і болти. Однак насправді стійки грають настільки важливу роль, що визначають практично всі інші аспекти обчислювального центру. Для обчислювального центру стійки – те ж саме, що хребет для вашого організму. Хребет визначає загальну форму, впливаючи на всі інші аспекти. Кожен вид стійок призначений для певної мети. Деякі більше підходять для серверів, а інші – для мережевого обладнання.

Укладання кабелю

При придбанні стійки завжди продумуйте укладку кабелів. Загалом, рекомендується відразу придбати інструменти для укладання кабелів. Щоб визначити, що саме вам необхідно, продумайте, яким чином ви збираєтеся прокладати проводку у своєму обчислювальному центрі. Обміркуйте можливість горизонтального і вертикального укладання кабелів. Кабелі, належним чином укладені між стійками і всередині них, дозволять працювати ефективно, не зачіпаючи при цьому інше обладнання.

Розплутування кабелів – досить непроста справа. Крім того, воно завжди супроводжується відключенням апаратури. Якщо ви не забезпечите належне управління кабелями, люди почнуть підключати обладнання, як їм заманеться. В результаті з'ясується,

що не вийде витягнути несправний пристрій із стійки, щоб замінити його, чи не відключивши при цьому три інших критично важливих пристрої, які не мають нічого спільного з потрібною вам машиною.

Проводка

В обчислювальному центрі тримати проводку в порядку досить складно.

Однак при плануванні центру у вас є кілька способів, за допомогою яких ви полегшите системним адміністраторам задачу з підтримки проводки в пристойному стані.

Приховати безлад – не означає усунути його. Якщо безладу не видно, це не значить, що він не відіб'ється на роботі системних адміністраторів. Фальшпол допоможе приховати неохайні кабелі, які будуть плутатися як попало. Витягуючи той чи інший кабель з-під підлоги, ви виявите, що він заплутався серед інших кабелів. Можливо, і витягнути його буде не так просто. Це призведе до того, що кабелі будуть просто залишати на місці, щоб розібратися з ними «пізніше, коли буде час».

Поради по патч-кабелям

Короткі мережеві кабелі, які використовуються для з'єднання машини з мережею, а також з'єднання двох патч-панелей або патч-панелі з машиною, називаються патч-кабелями. Як правило, довжина таких кабелів становить 1, 2 або 3 м.

Маркування

Грамотне маркування та ярлики необхідні для безвідмовної роботи обчислювального центру. Всі пристрої повинні мати ярлики як на лицьовій, так і на задній панелі. На цих ярликах повинне бути присутнім повне ім'я пристрою, який вказано в корпоративному просторі імен і в системі консольного сервера.

Робоче місце

Ще один важливий аспект будь-якого обчислювального центру – легкий доступ до робочого місця, обладнаному достатньою кількістю розеток і антистатичною поверхнею, де системний адміністратор може виконувати роботу з машинами: встановлювати пам'ять, диски і процесори на нове обладнання перед його установкою або вирішувати ту чи іншу апаратну проблему.

В ідеалі робоче місце повинно знаходитися поряд з обчислювальним центром, але не всередині нього. Таким чином, воно не буде використовуватися як тимчасова стійка і не стане створювати безлад в обчислювальному центрі.

В таких робочих місцях скупчується багато пилу, особливо якщо там розпаковується нове обладнання. Дуже важливо не допускати появи пилу в обчислювальному центрі.

Інструменти і запаси

В обчислювальному центрі завжди повинен бути повний запас різних кабелів, інструментів і запасних деталей. Це простіше сказати, ніж зробити.

У великому відділі системного адміністрування доводиться постійно відслідковувати наявність запасних частин і матеріалів. Самі системні адміністратори повинні стежити за тим, щоб потрібні запаси не закінчувались, а якщо закінчувалися, то рідко і ненадовго. Системний адміністратор, який помітив, що в обчислювальному центрі закінчуються певні запаси або необхідно використати велику кількість того чи іншого обладнання, повинен повідомити про це співробітнику, який несе відповідальність за відстеження запасних деталей і матеріалів.

Щоб використовувати всі можливості обчислювального центру, необхідно все правильно спроектувати з самого початку. Якщо ви знаєте, що належить зі будівлю нового обчислювального центру, варто все підготувати заздалегідь і зробити грамотно.

Контрольні запитання:

1. Охарактеризуйте термін «робоча станція».
2. Розкажіть про додаткові можливості розширюваності серверів.
3. Вибір та покупка серверного обладнання.
4. Відмінність робочої станції від сервера.
5. Дата-центр та його особливості.

Лекція 3. Структура комп'ютерної мережі

1. Мережоутворююче (переферійне) обладнання.

Периферійний пристрій (периферійне обладнання) – частина технічного забезпечення, конструктивно відокремлена від головного блоку обчислювальної системи.

Периферійні пристрої мають власне керування і функціонують за командами центрального процесора. Периферійні пристрої призначені для зовнішньої обробки даних, що забезпечує їх підготовку, введення, зберігання, керування, захист, вивід та передачу по каналах зв'язку.

Лінія зв'язку – це обладнання, за допомогою якого здійснюється об'єднання комп'ютерів у мережу. Лінії зв'язку залежно від середовища передачі даних поділяються на:

- повітряні – традиційно по таких проводах передають телефонні або телеграфні сигнали, але за відсутності інших можливостей ці лінії використовуються також і для передачі комп'ютерних даних;
- кабельні – представляє складну конструкцію, яка складається із провідників; використовуються такі типи: вита пара, коаксіальний кабель, волоконно-оптичний кабель;
- радіоканали наземного та супутникового зв'язку – створюються за допомогою передавача і приймача радіохвиль.

Комунікаційне або мережеве обладнання – це периферійні пристрої, що здійснюють перетворення сигналів, які використовуються у комп'ютері, на сигнали, що передаються через лінії зв'язку, і навпаки. Такими пристроями є мережеві адаптери, модеми та ін.

Використовуючи лінію зв'язку і мережевий адаптер можна побудувати найпростішу мережу, але надійність і продуктивність такої мережі буде невисокою. Суттєво покращити характеристики мережі дозволять наступні мережеві пристрої:

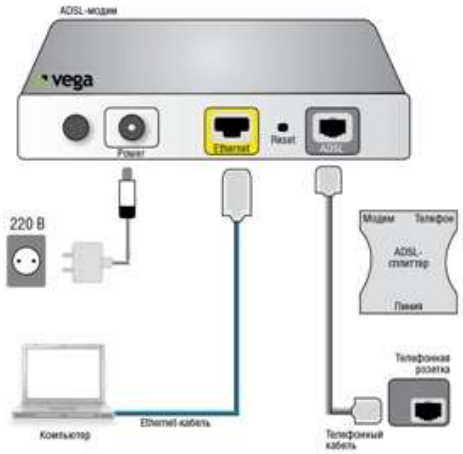
- **комутатори** (англ. Switch – перемикач) – обладнання, яке призначене для об'єднання декількох комп'ютерів комп'ютерної мережі у межах одного сегмента мережі. Комутатор може мати різну кількість портів (зазвичай від 8 до 32);

Комутатор D-link

- **концентратори** – об'єднуючий компонент, до якого підключаються всі комп'ютери в мережі. Нині майже не використовуються – їх змінили комутатори, які виділяють кожен підключений пристрій в окремий сегмент;
- **мости** – це пристрої, що з'єднують дві мережі, які побудовані за різними технологіями. Міст виконує перерозподіл інформаційних потоків між мережами;
- **повторювач** – мережевий пристрій, який відновлює сигнали, спотворені при передачі;
- **маршрутизатор** (роутер) – мережеве обладнання, яке на основі інформації про топологію мережі і визначених правил приймає рішення про пересилання пакетів мережевого рівня між різними сегментами мережі. Маршрутизатор визначає оптимальний маршрут передачі даних. Він допомагає зменшити навантаження мережі, завдяки поділу на домени, а також завдяки фільтрації пакетів.

Маршрутизатор Microtic

- **модем** Модем (Modem – скорочення від модулятор-демодулятор). Пристрій зв'язку для перетворення сигналу за допомогою процесів модуляції (зміна параметрів електромагнітного коливання за законом інформаційного повідомлення) та протилежному йому – демодуляції, що дозволяє комп'ютеру передавати дані по телефонній лінії; він є пристроєм узгодження у телекомунікаційних системах, системах автоматичного керування тощо. Стосовно застосування модемів у комп'ютерній техніці, то модеми поділяють на внутрішні (що встановлюються усередині системного блока) та зовнішні (що встановлюються ззовні системного блока).



ADSL модем в роботі

Захищена телекомунікаційна шафа (антивандальна шафа) (англ. Protective cabinet) – телекомунікаційний шафа, для розміщення та захисту телекомунікаційного обладнання (серверів, маршрутизаторів, комутаторів, модемів, телефонних станцій, елементів оптичних кросових систем) в місцях загального доступу – коридорах, горищах, сходових клітинах під'їздів, підвалах – де можливо розкрадання, пошкодження або підміна обладнання сторонніми особами.

Захищена телекомунікаційна шафа з сейфовими дверима

2. Кабельні мережі

Інформаційна система підприємства розпочинається із з’єднань між різними пристроями. Від якості цих каналів зв’язку не в останню чергу залежить стабільність і надійність роботи бізнес-додатків.

Структурована кабельна система (СКС) – ієрархічна кабельна система, що включає в себе всі необхідні пасивні компоненти для створення середовища передачі інформації: телекомунікаційні кабелі, з’єднувальні патч-корди (кроссовери), пасивне комутаційне обладнання.

Вита пара

Вита, звита, скручена або кручена пара (англ. twisted pair) – вид мережевого кабелю, з однією або декількома парами ізольованих провідників, скручених між собою (з невеликою кількістю витків на одиницю довжини) для зменшення взаємних наведень при передачі сигналу і покритих пластиковою оболонкою (рис. 3.1). Використовується для побудови мереж у багатьох технологіях, наприклад, Ethernet, ARCNet і Token ring. Останнім часом, завдяки своїй дешевизні й легкості установки, є найпоширенішим для побудови локальних мереж.

Кабель приєднується до мережевих пристроїв за допомогою з'єднувача 8P8C.

Позначення 8-позиційних модульних вилок, із зазначенням не тільки кількості позицій (цифра перед символом P, position), але й кількості контактів (цифра перед символом C, contacts). Вилки 8P8C прийнято називати роз'ємами RJ-45, хоча це помилкове найменування. Спочатку так називалися вилки 8P2C – 8-позиційні, оснащені тільки центральними контактами 4, 5.

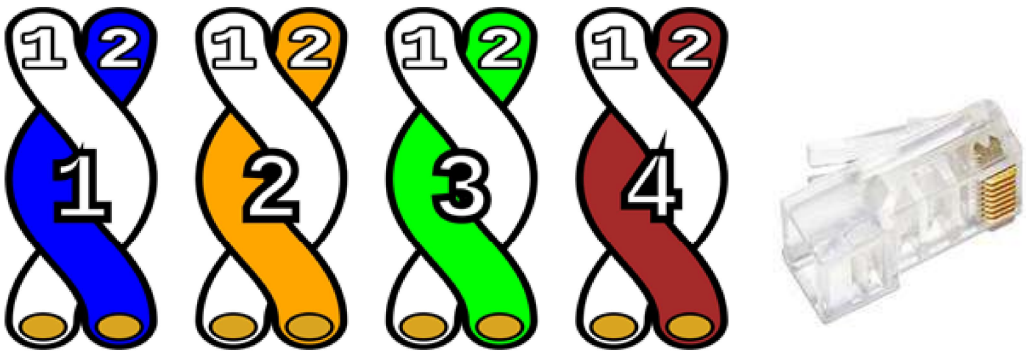


Рис.3.1 – Вита пара та з’єднувач 8P8C

Підтримує передачу даних на відстань до 100 метрів. На більших відстанях сигнал через загасання не розпізнається; якщо передача даних на більшу відстань все ж таки

необхідна, потрібно скористатися повторювачем, або ж задіяти волоконно-оптичний або коаксіальний кабель.

Категорії кабелю вита пара

Існує декілька категорій кабелю вита пара, які нумеруються від CAT1 до CAT7. Кабель вищої категорії зазвичай містить більше пар дротів і кожна пара має більше витків на одиницю довжини. Категорії неекранованої витої пари описуються в стандарті EIA/TIA 568 (Американський стандарт проводки в комерційних спорудах).

- *CAT1* – телефонний кабель, всього одна пара. В США використовувався раніше, і провідники були скручені між собою. Використовується тільки для передачі голосу або даних за допомогою модему.
- *CAT2* – старий тип кабелю з 2-х пар провідників, підтримував передачу даних на швидкостях до 4 Мбіт/с, використовувався в мережах token ring і ARCNet. Зараз іноді зустрічається в телефонних мережах.
- *CAT3* – 2-парний кабель, використовувався для побудові локальних мереж 10BASE-T і token ring, підтримує швидкість передачі даних тільки до 10 Мбіт/с. На відміну від попередніх двох, відповідає вимогам стандарту IEEE 802.3. Також дотепер зустрічається в телефонних мережах.
- *CAT4* – кабель складається з 4-х скручених пар, використовувався в мережах token ring, 10BASE-T, 10BASE-T4, швидкість передачі даних не перевищує 16 Мбіт/с, зараз не використовується.
- *CAT5* – 4-парний кабель, це і є те, що зазвичай називають кабель «вита пара». Завдяки високій швидкості передачі (до 100 Мбіт/с при використанні 2 пар і до 1000 Мбіт/с при використанні 4 пар) є найпоширенішим мережевим носієм, що використовується в комп'ютерних мережах дотепер. Для прокладки нових мереж користуються дещо вдосконаленим кабелем CAT5e, який краще пропускає високочастотні сигнали.
- *CAT6* – Застосовується в мережах Fast Ethernet і Gigabit Ethernet, складається з 4 пар провідників і здатний передавати дані на швидкості до 10000 Мбіт/с. Доданий до стандарту в червні 2002 року, пропускає сигнали частотою до 200МГц. Існує категорія CAT6e, в якій збільшена частота сигналу, що пропускається, до 500МГц. За даними IEEE, 70% встановлених мереж у 2004 році використовували кабель категорії CAT6, проте, можливо, це просто данина моді, бо й кабелі CAT5 і CAT5e цілком справляються в мережах 10GBASE-T.
- *CAT7* – Специфікація на цей тип кабелю поки що не затверджена, швидкість передачі даних – до 10000 Мбіт/с, частота сигналу, що пропускається, до 600–700 Мгц. Кабель цієї категорії екранований.

Кабельну мережу можна віднести до певної категорії, тільки якщо при її створенні використані елементи (розетки, роз’єми, кабелі і т. д.), Що задовольняють вимогам даної або вищої категорії, а проектування та монтаж виконані відповідно до вимог стандартів (обмеження на довжину, число точок комутації і т. д.).

В даний час більшість експлуатованих кабельних систем відносяться до категорії 5, яка допускає передачу даних по мережі зі швидкістю до 100 Мбіт/с. Категорія 5e вводить невеликі додаткові обмеження, які дозволяють використовувати канали передачі даних з гігабітними мережевими картами. На практиці акуратно виконана проводка на елементах категорії 5 дозволяє здійснювати передачу на швидкості до 1 Гбіт/с.

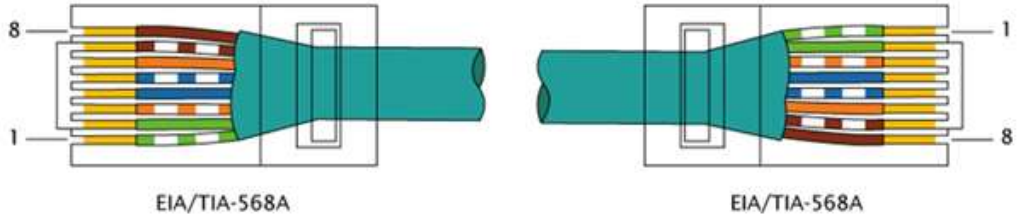
Схема обтискання кабелю CAT5

Для того, щоб комп'ютерна мережа працювала правильно, прокладаючи кабель, необхідно з'єднати відповідні контакти на роз'ємах 8P8C (який помилково ще називають RJ-45) у певному порядку і з одного, і з іншого кінця. Цю послідовність позначають кольорами проводів; при достатньому знанні можна скласти послідовність на власний розсуд, проте це може стати джерелом плутанини у великих мережах. Тому при прокладанні витої пари користуються двома стандартними схемами обтискання проводів на роз'єми:

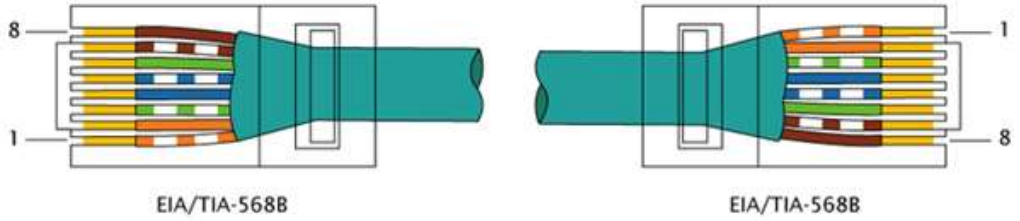
- прямий порядок обтискання (патч-корд) – для з'єднання мережевої карти з комутатором або концентратором;
- перехрещений (кросований, кроссовер) з інвертованою розводкою контактів роз'ємів. Застосовується для з'єднання двох комп'ютерів і для з'єднання деяких старих моделей концентраторів та комутаторів.

Прямий кабель (straight through cable)

Існує два стандартних варіанти обтискання прямого кабелю:
Варіант за стандартом EIA/TIA-568A (часто позначають просто 568A):



Варіант за стандартом EIA/TIA-568B – застосовується найчастіше

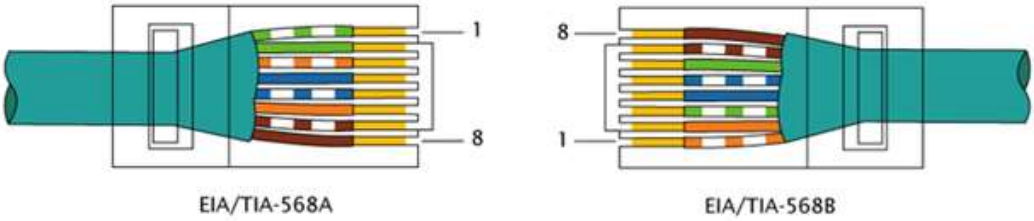


На практиці застосовуються два варіанти розшивки кабелю – A і B. B – використовується в основному в країнах Америки, інший – A – в країнах Європи. Варіанти відрізняються тільки «заміною місцями» зеленої і помаранчевої пар.

Перехресний кабель (crossover cable)

Використовується для з'єднання однотипного обладнання (наприклад, комп'ютер-комп'ютер).

Схема обтискання для 100 МБіт/с



Для передачі сигналів на лініях зв’язку 100 Мбіт/с використовуються тільки дві пари із чотирьох (в Gigabit Ethernet на швидкості 1000 Мбіт/с задіяні всі чотири пари), що наявні в кабелі. Хоча це і не дозволяється стандартами, адміністратор може задіяти вільні пари, наприклад, використовувати середні контакти (пара блакитний – біло-блакитний провод) під телефон, а коричневу пару в якості заміни однієї з сигнальних при виявленні обриву в кабелі. Слід враховувати, що для живлення пристроїв поверх мережі Ethernet (**PoE**) використовується центральна пара провідників і що в гігабітних каналах задіяні всі провідники.

Сучасні моделі комутаторів володіють можливістю визначення типу розшивки кабелю і автоматично перемикаються на потрібний варіант. У моделей, які випускалися раніше такої функції немає, тому, наприклад, для з’єднання двох таких пристроїв між собою також необхідно використовувати crossover-кабель. На деяких моделях є або кнопка перемикання типу одного з портів, або два роз’єми для одного порту, відповідних тому чи іншому варіанту підключення (званих MDI і MDIX).

Розміри сегментів мережі на витій парі

Довжина кабелю від одного елемента активного обладнання до іншого, наприклад від комп’ютера до комутатора, в мережі Ethernet не повинна перевищувати 100 м. Зазвичай стандартами передбачена максимальна довжина самого кабелю 90 м, а 10 м відводиться на сполучні кабелі. На практиці довжина патч-кордів зазвичай становить 1 м і більше. Зверніть увагу, що не має сенсу застосовувати саморобні короткі патч-корди, наприклад, для підключення сервера до патч-панелі, якщо обидва ці елементи розташовані поруч («фірмові» кабелі не можуть бути коротше ~ 60 см). При малій довжині кабелю зростає рівень перешкод, що виникають при відображенні високочастотних сигналів від

точки з’єднання кабелю і розетки. Це може призвести до збільшення кількості помилок в лінії.

Для локальної 10-мегабітної мережі, побудованої на концентраторах, існує «правило 5/4»: між будь-якими двома мережевими пристроями повинно бути не більше 5 сегментів мережі з чотирма концентраторами (хабами). Ця вимога обмежує розмір мережі діаметром 500 м, побудованої на концентраторах і з використанням витої пари. Обмеження на довжини обумовлено самою природою Ethernet, принципами, на яких будується така мережа, і не залежить від вдосконалення елементної бази.

Хоча в 100-мегабітній мережі зазвичай використовуються тільки комутатори, на практиці в ряді організацій експлуатуються і концентратори. Стандартом передбачено в цьому випадку використання максимум двох концентраторів з відстанню між ними не більше 5 м.

Варіанти виконання СКС

Кабельна система підприємства може бути виконана різними способами: за технологією прихованої проводки, в накладних каналах, в просторі під фальшстелею або над навісною стелею і т. д. Власними силами прокладка кабелів зазвичай виконується без трудомістких будівельних робіт – в накладних каналах, при цьому переходи між окремими приміщеннями здійснюються або через отвори в стінах, або над накладною стелею коридору.

Складові лінії

Стандарти СКС не передбачають можливості складання ліній передачі даних з декількох ділянок. Це означає, що з’єднання комп’ютера з комутатором має складатися з патч-корду, інформаційної розетки, кабелю, комутаційної панелі (на яку «розшитий» кабель), патч-корду до роз’єму на комутаторі. Якщо з яких-небудь причин довжини кабелю недостатньо (кабель пошкоджений або співробітнику виділено інше місце), то нарощувати його не можна.

Однак на практиці досить часто доводиться стикатися з необхідністю подовження кабелю. Ні в якому разі не рекомендуючи застосовувати на практиці вишесказане, мушу зазначити, що на 100-мегабітних мережах кабелі цілком задовільно функціонують при наявності скрутки (або, що ще краще, паяного з’єднання) двох частин. При цьому слід мінімізувати довжину ділянки кабелю, на якому порушений крок кручений пари. І, оскільки якість контактів скрутки може істотно знизитися через деякий проміжок часу через вплив зовнішніх умов (наприклад, окислення під впливом вологи), слід подбати про надійну ізоляцію такого з’єднання.

Прокладка силових кабелів

Кожне робоче місце користувача повинно бути обладнане розеткою електроживлення із заземленням та інформаційними розетками. У невеликих організаціях зазвичай використовують розетки існуючої електропроводки. При цьому слід враховувати, що відстань між силовою та інформаційною розетками одного робочого місця за стандартом не повинна перевищувати 1 м. Крім того, з метою зниження рівня перешкод і підвищення пожежобезпеки в стандартах визначається мінімальна відстань між силовим та інформаційними кабелями: вона залежить від споживаної потужності, але зазвичай можна орієнтуватися на значення в 10-15 см. На практиці рідко вдається витримати такі відстані, тому, щоб мінімізувати вплив силового кабелю, часто використовують спеціальні кабелі з екрануванням. При розміщенні великої кількості користувачів в приміщенні, не обладнаному достатньою кількістю силових розеток, часто здійснюється проводка силових та інформаційних кабелів до робочого місця в одному каналі. Відповідно до стандарту, якщо обидва кабелі прокладаються в загальному каналі, то повинна бути передбачена суцільна перегородка між силовими та інформаційним відсіками.

Волоконно-оптичні мережі

Оптичне волокно – нитка з оптично прозорого матеріалу (скло, пластик), яка використовується для перенесення світла всередині себе за допомогою повного внутрішнього відображення.

При побудові кабельної системи підприємства часто виникає необхідність підключення пристроїв, рознесених на великі відстані (100 і більше метрів). У цьому випадку успішно застосовуються волоконно-оптичні лінії зв’язку. Зазвичай одне волокно кабелю використовується для передачі сигналу, інше – для прийому. Існує обладнання, що дозволяє за рахунок використання різних діапазонів випромінювання передавати і

приймати дані по одному волокну, але воно застосовується не часто: зазвичай оптичні кабелі проектуються з великим запасом по числу волокон.

Рис. 3.4 – Волоконно-оптичний кабель

Оптичні волокна можуть бути одномодовими і багатомодовими. Діаметр серцевини одномодових волокон становить від 7 до 10 мікрон. Багатомодові волокна відрізняються від одномодових діаметром серцевини, який складає 50 мікрон в європейському стандарті і 62.5 мікрон в північноамериканському і японському стандартах.

При відстанях 100-200м застосовуються багатомодові оптичні кабелі. Вартість прокладки й експлуатації такої лінії практично порівнянна з вартістю лінії на витій парі. При довжинах з'єднань понад 200м використовується одномодовий оптичний кабель. Відповідне обладнання (приймачі і передавачі оптичного сигналу) за вартістю в кілька разів дорожче, ніж моделі для багатомодового кабелю.

Якщо відстань, на яку передбачається передавати дані, вимірюється десятками кілометрів, то необхідно використовувати передавачі підвищеної потужності (вони присутні в лінійках продукції практично всіх виробників).

Експлуатація волоконно-оптичних каналів зв'язку вимагає підвищеної акуратності з боку користувачів. Не допускається різко згинати кабель, слід оберігати оптичні поверхні від засмічення (не чіпати їх руками, завжди закривати кінці кабелю і гнізда в модулі підключення спеціальними заглушками і т. д.). У разі пошкодження кабелю зазвичай потрібне запрошення монтажних фірм, оскільки придбання обладнання для пошуку та визначення місць несправності (рефлектометри і т.д.) доступно тільки спеціалізованим організаціям.

Основне застосування оптичні волокна знаходять як середовища передачі на волоконно-оптичних телекомунікаційних мережах різних рівнів: від міжконтинентальних магістралей до домашніх комп'ютерних мереж. Застосування оптичних волокон для ліній зв'язку обумовлено тим, що оптичне волокно забезпечує високу захищеність від несанкціонованого доступу, низьке загасання сигналу при передачі інформації на великі відстані і можливість оперувати з надзвичайно високими швидкостями передачі. Вже до 2006-го року була досягнута частота модуляції 111 ГГц, в той час як швидкості 10 і 40 Гбіт/с стали вже стандартними швидкостями передачі по одному каналу оптичного волокна. При цьому кожне волокно, використовуючи технологію спектрального ущільнення каналів може передавати до декількох сотень каналів одночасно, забезпечуючи загальну швидкість передачі інформації, яка обчислюється Терабітами в секунду. Так, до 2008 року була досягнута швидкість 10,72 Тбіт/с, а до 2012 – 20 Тбіт/с. Останній рекорд швидкості – 255 Тбіт/с.

Коаксіальний кабель

Коаксіальний кабель – електричний кабель із співвісними провідниками.
Основне призначення коаксіального кабелю – передача сигналу в різних областях техніки. Сучасний кабель складається з центрального провідника, оточеного шаром діелектрика, зовнішня поверхня якого покрита обплетенням або фольгою (другим провідником) і захисною оболонкою з пластику, що захищає кабель від дії навколишнього середовища.

Для підключення кабельного Інтернету використовується коаксіальний телевізійний кабель, через який одночасно може передаватися відеосигнал і здійснюватися Інтернет-з'єднання. Останній стандарт Docsis 3.0 дозволяє збільшити швидкість Інтернету до 150 Мбіт / с.

3. Бездротові мережі

Стандарти бездротової мережі

В даний час пристрої для бездротової мережі випускаються на основі декількох стандартів, деякі параметри яких показано на рис. 3.6.

Wi-Fi, WiFi (від англ. Wireless Fidelity) – мережа, що належить Wi-Fi Alliance. Загальновживана назва для стандарту бездротового (радіо) зв'язку передачі даних, який об'єднує декілька протоколів і ґрунтується на сімействі стандартів IEEE 802.11 (Institute of Electrical and Electronic Engineers – міжнародна організація, що займається розробкою стандартів у сфері електронних технологій). Найвідомішим та найпоширенішим на сьогодні є протокол IEEE 802.11g, що визначає функціонування бездротових мереж.

Встановлення Wireless LAN рекомендувалось там, де розгортання кабельної системи було неможливим або економічно недоцільним. Нині в багатьох організаціях використовується Wi-Fi, оскільки при певних умовах швидкість роботи мережі вже перевищує 100 Мбіт/с. Користувачі можуть переміщуватися між точками доступу по території покриття мережі Wi-Fi.

Таблиця 1 Порівняльна характеристика основних стандартів

Стандарт	802.11a	802.11b	802.11g	802.11i	802.11n
Частота (GHz)	5.150-5.350 5.470-5.850	2.400-2.483	2.400-2.483	2.400-2.483	2.400-2.483
Дальність (м)	10-100	30-300	30-300	30-300	50-400
Швидкість (Мбит/с)	54	11	54	108	540
Технології шифрування	WEP	WEP	WEP WPA WPA2	WEP WPA WPA2 AES	WEP WPA WPA2 AES

Стандарт	IEEE 802.11a	IEEE 802.11b	IEEE 802.11g	IEEE 802.11n
діапазон частот, ГГц	5.15-5.25 5.67-5.85	2.4-2.483	2.4-2.483	2.4-2.483 5.15-5.25 5.67-5.85
Доступ до радіоканалу	CSMA-CA	CSMA-CA	CSMA-CA	CSMA-CA
Кількість абонентів на один канал	50	10	50	більше 100
Максимальна швидкість обміну даними	54Мбіт/с	11 Мбіт/с	54Мбіт/с	480 Мбіт/с
Метод модуляції	OFDM	DSSS, FHSS	OFDM	BPSK, QPSK,
Дальність дії в приміщенні	10-20	20-100	20-50	10-20

Рис. 3.6 – Основні стандарти бездротової мережі

The Wi-Fi Alliance є всесвітнім, неприбутковим промисловим об'єднанням понад 300 компаній з метою сприяння росту бездротових локальних мереж (WLAN). Маючи на меті покращення роботи користувачів з бездротовими переносними, мобільними, та розважальними пристроями, програми тестування та сертифікації Wi-Fi Alliance гарантують WLAN продукції на основі специфікації IEEE 802.11. З часу запровадження програми сертифікації Wi-Fi Alliance у березні 2000 року, понад 4000 продуктів отримали позначку Wi-Fi CERTIFIED™, що стимулює ширше використання Wi-Fi продуктів та послуг на ринках для споживачів і підприємств.

Wi-Fi Alliance володіє торговою маркою Wi-Fi. Виробники можуть використовувати цю торговельну марку для сертифікованої продукції, яка була протестована на сумісність.

Проектування бездротової мережі підприємства

За допомогою бездротових технологій можна з'єднувати комп'ютери (за принципом «точка – точка»), окремі сегменти мереж і т. д. Найбільш часто в локальних мережах пристрої бездротового доступу ставляться в якості точки доступу (Wireless Access Point, AP). У цьому випадку персональні комп'ютери підключаються до точки доступу, через які здійснюють доступ як в локальну мережу організації, так і в Інтернет, при цьому точка доступу виступає аналогом концентратора локальної мережі.

Після вибору стандарту бездротової мережі слід визначити зони покриття. Одна стандартна точка доступу «покриває» зону радіусом близько 75-100 м. Хоча існують різні оцінки для розрахунків діаграм зон покриття, ці величини істотно залежать від конкретних умов: планування приміщень, матеріалу стін і т. д. Кращим способом є проведення тестових вимірів на місцевості з використанням відповідного обладнання.

На кількість встановлюваних точок доступу будуть впливати також вимоги до швидкості передачі даних. Зазначені на рис. 3.6 значення швидкості передачі даних є максимальними, а смуга пропускання ділиться між усіма пристроями, які підключені до даного каналу. Також слід враховувати, що швидкість передачі даних знижується на максимальних відстанях при слабкому рівні сигналу. Встановлення додаткових точок доступу дозволить розподілити між ними користувачів і підвищити швидкість обміну даними. У зв'язку з цим зазвичай рекомендується встановлювати одну точку доступу приблизно на 10 клієнтів, хоча технічна межа підключень бездротових пристроїв, як правило, становить не одну сотню систем. Бездротові рішення можуть допомогти з'єднати, наприклад, дві будівлі. Для цього створені спеціалізовані бездротові мости і спрямовані антени.

Безпека бездротової мережі

Точку доступу можна порівняти з концентратором локальної мережі, який поставлений в загальнодоступне приміщення. Будь-хто може «підключитися» до даного сегменту і прослуховувати передану інформацію. Тому правильному налаштуванні підключення клієнтів необхідно приділити особливу увагу.

Шифрування трафіку бездротової мережі

Для захисту переданої по бездротовій мережі інформації всі дані шифруються. Історично перший стандарт безпеки для Wi-Fi – протокол WEP (Wired Equivalent Privacy або Wireless Encryption Protocol, протокол шифрування безпровідного зв'язку) – передбачає шифрування за допомогою статичного ключа, відомого як користувачу, так і адміністратору точки доступу. На жаль, у практичній реалізації цього документа були знайдені помилки, які дозволяють за короткий час (порядку декількох годин) обчислити даний ключ.

Тому протоколи WEP, навіть із збільшеною довжиною ключа, не можуть вважатися безпечними при створенні корпоративної бездротової мережі.

Якщо застосовані при створенні бездротової мережі пристрої не підтримують нових протоколів безпеки, то адміністратори можуть захистити передану інформацію шляхом створення віртуальних приватних мереж (VPN) поверх бездротових каналів зв'язку.

Новий стандарт безпеки WPA, WPA2 (Wi-Fi Protected Access) передбачає як використання динамічних (змінюваних) ключів шифрування, так і аутентифікацію користувача при вході в бездротову мережу. Проектуючи бездротовий сегмент мережі, слід купувати тільки пристрої, що задовольняють даному стандарту.

Аутентифікація за допомогою перевірки MAC-адрес пристроїв, що підключаються до даного пункту доступу. У цьому випадку адміністратор вручну повинен налаштувати для кожної точки доступу відповідний список MAC-адрес пристроїв, яким дозволено бездротове підключення.

Спосіб не може вважатися безпечним, оскільки MAC-адреси легко визначаються при прослуховуванні бездротового сегмента, а «підміна» MAC-адреси не представляє ніякої складності навіть для не зовсім досвідченого користувача.

4. Побудова топології існуючої СКС

Для усунення несправностей ліній зв'язку необхідно знати, як з'єднане активне обладнання, до якого порту підключений конкретний комп'ютер. Адміністратор повинен мати комплект документації, в якій були б описані лінії зв'язку, наведені кабельні журнали (крім тих таблиць, які зазвичай наклеюються на комутаційні шафи), зберігалися б результати приймальних тестів і відомості про проведені ремонти і т. д

Відомості про топології реальної мережі, інформацію про порти і підключене до них устаткування можна зібрати автоматично, якщо структурована кабельна мережа (СКС) побудована на керованих комутаторах.

Інвентаризація фізичних каналів зв'язку

Інвентаризація кабельної інфраструктури є однією з найскладніших завдань при наявності розгалуженої мережі підприємства. У кращому випадку у адміністратора є кабельні журнали, в яких наведено перелік кабелів і списки з'єднань, виконаних на комутаційних панелях. Часто ці списки не актуальні, а реальні підключення знає тільки сам адміністратор.

Якщо у адміністратора немає повної інвентаризації, починаючи від розташування кабелів, призначення портів комутаційних панелей і закінчуючи списком встановленого

програмного забезпечення, то на усунення пошкоджень, від яких ніхто не застрахований, може знадобитися тривалий проміжок часу, протягом якого підприємство буде нести збитки через ненадання послуг інформаційною системою. Чим більш докладно буде складена відповідна документація, чим ретельніше вона підтримується в актуальному стані, тим легше зорієнтуватися в аварійній ситуації.

Існують спеціальні програми, що ведуть облік робочих місць, сполучних кабелів та іншого обладнання, які дозволяють у разі потреби швидко вивести всю інформацію про шляхи з'єднання точки «А» і точки «Б», а саме: номер розетки, кабель, номери комутаційних панелей і портів , на які розділені кабелі, та інша інформація.

Контрольні запитання:

1. Вита пара як вид мережевого кабелю, основні характеристики.
2. Побудова СКС на основі витої пари.
3. Яке Ви знаєте мережоутворююче обладнання?
4. Характеристика Wireless LAN.
5. Проектування бездротової мережі підприємства.

Лекція 4. Вибір операційної системи та програмного забезпечення

1. Вибір операційної системи

Вихованні на домашніх Windows-робочих станціях, багато користувачів намагаються перенести свої знання тільки однієї операційної системи в реальне життя. Однак сучасні системи, як правило, об'єднують рішення на різних операційних середовищах. У першу чергу враховуються питання продуктивності, фактори надійності, економічні аспекти рішень і т. д.

Windows-системи відрізняються зручним для користувача інтерфейсом, широким спектром прикладних програм, великою армією розробників. У результаті Windows фактично є домінуючою програмою на кінцевих користувацьких місцях, особливо в організаціях і підприємствах, де виконувані операції не завжди чітко фіксовані (рис. 4.1).

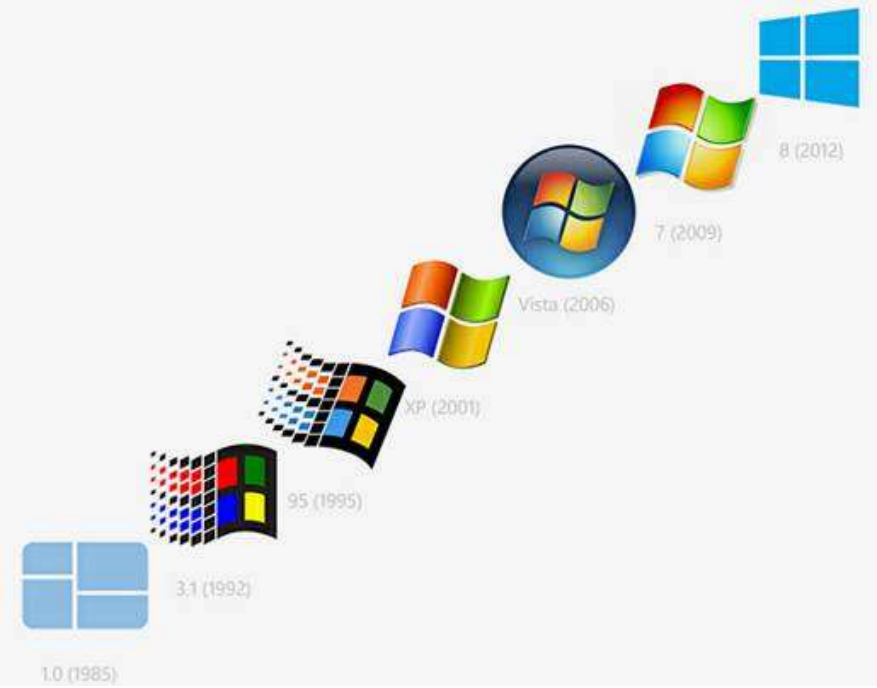


Рис. 4.1 – Логотипи різноманітних версій операційної системи Windows

У той же час більшість офісних завдань, що вирішуються на комп'ютерах, відносяться до роботи з документацією, електронною поштою, серфінгом Інтернету. Ці завдання чудово вирішуються і в безкоштовних додатках, за які не потрібно платити ліцензійні відрахування. Тому в організаціях, у яких починають рахувати гроші і оцінювати ефективність роботи, поступово починають впроваджуватися рішення на відкритих кодах і на персональних робочих місцях. *Якщо говорити про безкоштовні операційні системи, то в першу чергу слід назвати проект Ubuntu Linux, в рамках якого виходять як серверні версії, так і десктопні (рис. 4.2).*

Рис. 4.2 – Логотип проекту Ubuntu Linux

Ці операційні системи підтримуються крупними компаніями: OEM-партнерами є ARM, Asus, Dell, Hewlett Packard, Lenovo, багато компаній розробляють прикладне програмне забезпечення і т. д. Група розробників постійно випускає оновлення, рішення для покращення безпеки, гарантується технічна підтримка спеціальних серверних версій протягом тривалого терміну експлуатації (5 років) і т. д.

Принципового значення вибір того чи іншого дистрибутива не має, головне – загальна спрямованість процесу на неухильне розширення рішень відкритого коду.

Інформатизація все більше приходить і на виробництво. У виробничих інформаційних системах експлуатуються «важкі» додатки, історично створені для Unix-систем (рис. 4.3). На середніх підприємствах такі рішення переходять на ту чи іншу версію Linux. Серед найбільш відомих можна згадати HP AIX, Oracle Solaris, RedHat.

Рис. 4.3 – Логотип Unix-систем

* nix-системи відрізняються, насамперед, надійністю і стабільністю роботи, можливостями тонкого налаштування. Додатки, будучи запущені, не переривають роботи протягом багатьох місяців.

Позначення UNIX-подібної операційної системи, яка утворилася під впливом UNIX, іноді скорочується до позначення « nix-система».*

Вартість

Вибір операційної системи, в тому числі, залежить і від її вартості та вартості обслуговування.

Абстрактної вартості операційної системи та програмного забезпечення не існує. У кожному конкретному випадку вона повинна оцінюватися для умов конкретного підприємства. Не вірте тому, що адміністратора Linux треба навчати, а адміністратор Windows вже підготовлений «за замовчуванням». На первинному рівні адміністрування будь-який фахівець, що має деяке знайомство з інформаційними системами, досить швидко зможе почати керувати як Linux, так і Windows. А якщо виникає необхідність серйозної підготовки, то без навчання не обійтися як одному, так і іншому фахівцеві.

Для оцінки: в зарубіжних проектах на вартість супроводу програмного забезпечення закладаються суми, приблизно в розмірі 1/5 загальної вартості продукту.

Відкриті стандарти

На практиці більшість інформаційних систем включає в себе комп'ютери з різними операційними системами і прикладними програмами. На кожній дільниці застосовується найбільш оптимальне рішення. Гарантом їх працездатності є єдині стандарти взаємодії.

Сторінка Інтернету може бути переглянута в будь-якому браузері – Firefox, Internet Explorer, Opera і т.д. Відсутні проблеми взаємної аутентифікації користувачів Windows – Linux. У Windows реалізований відкритий стандарт Kerberos, а для взаємодії по протоколах NTLM і т. д. є безкоштовний продукт Samba, що входить до складу всіх дистрибутивів Linux. Об'єднання каналів при передачі інформації здійснюється на основі стандарту 803.2ad незалежно від конкретної моделі мережного обладнання, встановленого в мережі передачі даних. Документи, підготовлені в MS Office, відкриваються в OpenOffice (безкоштовна офісна система, призначена для Linux), і навпаки.

Подібних прикладів можна навести безліч.

У той же час багато фірм пропонують власні унікальні технології для реалізації в інформаційній системі. Застосовувати їх чи ні – серйозна проблема в кожному конкретному випадку. Якщо ви використовуєте унікальну технологію, то зазвичай отримуєте більш високу продуктивність, ніж при типовому рішенні, але опиняєтеся прив'язаними до конкретного вендора. При цьому перспектива подальшої підтримки технічної частини рішення, виробником часто буває не очевидною, якщо, звичайно, очистити пропозиції від рекламних слоганів.

У кожному разі потрібно орієнтуватися в першу чергу на використання рішень, описаних у відкритих стандартах. І тільки в разі неможливості такого вибору застосовувати пропрієтарні технології та розробки.

Пропрієтарним (від англ. proprietary – приватний, патентований) називають програмне забезпечення, що є власністю автора, зберігає за собою монопольне право на використання, поширення, копіювання та аналогічні операції. Пропрієтарне програмне забезпечення також може мати відкритий (опублікований) код, але його ліцензія включає контроль власника над продуктом.

Вендор (від англ. vendor – продавець, торговець) – юридична або фізична особа, яка є постачальником товарів і послуг, об'єднаних торговою маркою.

Сертифікація системних адміністраторів

Якщо якийсь час назад часто зустрічалися трудові династії, то зараз зміна роботи через 2-3 роки стала реальним способом збільшення заробітної плати. При цьому посередниками між працівниками та роботодавцями виступають кадрові агентства, а працівник найчастіше оцінюється тільки за формальними ознаками.

Майже повсюдно підбором і прийомом персоналу займаються менеджери, які не є фахівцями з кадрової роботи, а оцінюють «паперову» складову резюме.

Оскільки такі «правила гри» реально існують, то системному адміністраторові слід не забувати під час своєї роботи отримувати необхідні сертифікати. Якщо керівництво погоджується оплатити курси навчання, на яких готують до здачі іспиту на такі сертифікати, – добре. В іншому випадку слід знайти власні кошти для оплати сертифікації в якій-небудь області.

Сертифікат – те ж, що і права на водіння автомобіля. Він не підтверджує, що ви добре водите машину, проте є документом, який свідчить на вашу користь. Хоча – за даними спеціалізованих досліджень – довіра до сертифікатів з боку лінійних керівників на Заході падає, для більшості співробітників кадрових служб кількість наявних у вас сертифікатів пропорційно можливості позитивного рішення, тоді як їх відсутність може стати приводом для відмови.

І навпаки, наявність сертифіката часто аж ніяк не свідчить про рівень фахівця. Наприклад, автору неодноразово доводилося відмовляти в прийомі на роботу особам, які надавали численні сертифікати, але в процесі співбесіди не підтверджують зазначені в них практичні навички управління системою.

Вибір вендора

Особисто я рекомендую всім купувати обладнання середнього цінового діапазону. Топові моделі зазвичай володіють функціоналом, який не буде затребуваний під час експлуатації. Найдешевші – часто працюють не так стабільно, як хотілося б. Цей принцип можна поширити і на вибір вендора. Як правило, інформацію про ранжирування вендорів отримати достатньо легко. І краще вибирати знову ж фірми з середини списку. Найбільш відомі вендори часто завищують вартість обладнання, користуючись популярністю своєї марки. Слід не піддаватися на рекламні обіцянки: великі компанії виділяють на маркетингові цілі досить істотний відсоток від вартості обладнання.

2. Вибір програмного забезпечення

В основу роботи комп'ютерів покладено програмний принцип керування, який полягає в тому, що комп'ютер виконує дії за заздалегідь заданою програмою. Цей принцип забезпечує універсальність використання комп'ютера: у певний момент часу розв'язується задача відповідно до вибраної програми. Після її завершення у пам'ять завантажується інша програма і т.д.

Програма – це запис алгоритму розв'язання задачі у вигляді послідовності команд або операторів мовою, яку розуміє комп'ютер. Кінцевою метою любої комп'ютерної програми є керування апаратними засобами.

Для нормального розв'язання задач на комп'ютері потрібно, щоб програма була налагоджена, не потребувала дороблень і мала відповідну документацію. Тому стосовно роботи на комп'ютері часто використовують термін **програмне забезпечення (software)**, під яким розуміють сукупність програм, процедур і правил, а також документації, що стосуються функціонування системи оброблення даних.

Програмне та апаратне забезпечення у комп'ютері працюють у нерозривному зв'язку та взаємодії. Склад програмного забезпечення обчислювальної системи називається **програмною конфігурацією.** Між програмами існує взаємозв'язок, тобто багато програм працюють, базуючись на програмах нижчого рівня. Міжпрограмний інтерфейс – це розподіл

програмного забезпечення на декілька пов'язаних між собою рівнів. Рівні програмного забезпечення являють собою піраміду, де кожен вищій рівень базується на програмному забезпеченні попередніх рівнів. Схематично структура програмного забезпечення наведена на рис. 4.4.

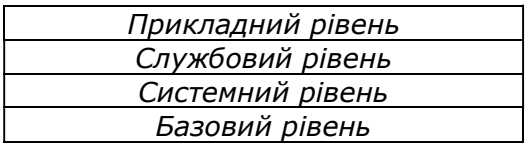


Рис. 4.4. Програмне забезпечення

Базовий рівень

Цей рівень є найнижчим рівнем програмного забезпечення. Відповідає за взаємодію з базовими апаратними засобами. Базове програмне забезпечення міститься у складі базового апаратного забезпечення і зберігається у спеціальних мікросхемах постійного запам'ятовуючого пристрою (ПЗП), утворюючи базову систему введення-виведення BIOS (EFI). Програми та дані записуються у ПЗП на етапі виробництва і не можуть бути змінені в процесі експлуатації без спеціального обладнання.

Системний рівень

Системний рівень – є перехідним. Програми цього рівня забезпечують взаємодію інших програм комп'ютера з програмами базового рівня і безпосередньо з апаратним забезпеченням. Від програм цього рівня залежать експлуатаційні показники всієї обчислювальної системи. При під'єднанні до комп'ютера нового обладнання, на системному рівні повинна бути встановлена програма, що забезпечує для решти програм взаємозв'язок із цим пристроєм. Конкретні програми, призначені для взаємодії з конкретними пристроями, називають **драйверами**.

Інший клас програм системного рівня відповідає за взаємодію з користувачем. Завдяки йому є можливість вводити дані у обчислювальну систему, керувати її роботою й отримувати результат у зручній формі. Це засоби забезпечення користувацького інтерфейсу, від них залежить зручність та продуктивність роботи з комп'ютером.

Сукупність програмного забезпечення системного рівня утворює ядро операційної системи комп'ютера. **Наявність ядра операційної системи** – є першою умовою для можливості практичної роботи користувача з обчислювальною системою. Ядро операційної системи виконує такі *функції*: керування пам'яттю, процесами введення-виведення, файловою системою, організація взаємодії та диспетчеризація процесів, облік використання ресурсів, оброблення команд і т.д.

Службовий рівень

Програми цього рівня взаємодіють як із програмами базового рівня, так і з програмами системного рівня. Призначення службових програм (утиліт) полягає у автоматизації робіт по перевірці та налаштуванню комп'ютерної системи, а також для покращення функцій системних програм. Деякі службові програми (програми обслуговування) відразу додають до складу операційної системи, доповнюючи її ядро, але більшість є зовнішніми програмами і розширюють функції операційної системи. Тобто, у розробці службових програм відслідковуються два напрямки: інтеграція з операційною системою та автономне функціонування.

Прикладний рівень

Програмне забезпечення цього рівня являє собою комплекс прикладних програм, за допомогою яких виконуються конкретні завдання (від виробничих до творчих, розважальних та навчальних). Між прикладним та системним програмним забезпеченням існує тісний взаємозв'язок. Універсальність обчислювальної системи, доступність прикладних програм і широта функціональних можливостей комп'ютера безпосередньо залежать від типу наявної операційної системи, системних засобів, що містяться у її ядрі й взаємодії комплексу людина-програма-обладнання.

Основні види **мережевого програмного забезпечення**:

- *Аналізатор трафіку, або сніфер* (від англ. to sniff - нюхати) – програма або програмно-апаратний пристрій, призначений для перехоплення і подальшого аналізу, або тільки аналізу мережного трафіку, призначеного для інших вузлів.

- *Робот або бот*, а також інтернет-бот, www-бот тощо (англ. bot, скор. від англ. robot) – спеціальна програма, що виконує автоматично і/або за заданим розкладом які-небудь дії через ті ж інтерфейси, що й звичайний користувач. Людина, що обслуговує сервери, може помістити на сервері файл robots.txt, що містить обмеження, яким зобов'язані підпорядковуватися боти.
- *Операційні системи для комунікаційного обладнання* – спеціальні операційні системи, які потрібні для мережевого обладнання.
- *Системи управління доступом до мережі* – сукупність програмно-апаратних технічних засобів безпеки, що мають на меті обмеження та реєстрацію входу-виходу об'єктів в мережі.

Склад програмного забезпечення типової організації

Будь-яка інформаційна система включає в себе інфраструктурні служби – служби і програми, необхідні для підтримки роботи системи і виконання типових функцій, а також власне «корисне» програмне забезпечення – додатки, що виконують розрахунки з метою забезпечення виробництва даної організації.

Якщо прикладне програмне забезпечення дуже різноманітне і загальні рекомендації дати досить складно, то інфраструктурні рішення багато в чому схожі.

У будь-якій інформаційній системі представлені наступні класи програмного забезпечення:

- операційні системи;
- підсистеми дозволу імен;
- підсистеми авторизації, аутентифікації і контролю доступу;
- служби файлових сервісів;
- засоби доступу до глобальної мережі (Інтернету) і перегляду зовнішніх ресурсів;
- програмне забезпечення захисту хоста (антивірусне ПЗ та ПЗ між мережевих екранів, контролю додатків і т. д.);
- підсистема резервного копіювання;
- програмне забезпечення офісу (текстовий редактор, редактор електронних таблиць і т. д.);
- підсистема обміну повідомленнями електронної пошти.

Базові відомості про роботу в * nix-системах

Інформаційні системи підприємств не обходяться сьогодні без серверів, що працюють на одному з клонів * nix-систем.

Linux-міфи

Безкоштовні операційні системи та прикладні програми є серйозним конкурентом комерційним продуктам. На більшості робочих місць можна безболісно перейти на програми з відкритим кодом. Природно, що навколо цієї проблеми існує багато рекламних спекуляцій, покликаних вселити користувачам і керівникам певні уявлення про «правильний» шлях.

Сучасні операційні системи та прикладні програми, особливо наймасовіші, будуються, насамперед, на стандартах. Як Linux, так і Windows можуть використовувати однакові мережеві протоколи, єдину базу користувачів (сервер з обліковими записами користувачів може бути як на основі Linux, так і Windows) і т. д.

Природно, що повної тотожності різних продуктів бути не може.

Виникаючі проблеми носять, насамперед, психологічний характер. Коли я вирішив змінити оглядач Інтернету (у той час це був вимушений крок, оскільки продуктивності мого комп'ютера не вистачало для роботи в Internet Explorer), то кілька днів мене не покидало почуття дискомфорту і бажання повернутися у звичне середовище. Зараз я вже ні за що не відмовлюся від роботи в Firefox: ця програма мені здається більш зручною і надає великі можливості. Істотно менші незручності були пов'язані з переходом до OpenOffice.

Сьогодні в розпорядженні користувачів велика кількість різноманітних дистрибутивів Linux на будь-який смак. Їх легко знайти і скачати з мережі Інтернет. Дистрибутиви для серверів і робочих станцій відрізняються тільки набором програм, ви легко можете встановити додаткові пакети і використовувати, наприклад, робочу станцію в якості сервера.

Для роботи сервера Linux графічний інтерфейс зайвий. І адміністратори, що мають навіть незначний досвід роботи, намагаються виконувати більшість операцій саме в режимі

командного рядка. Тим не менш, графічний інтерфейс в даній операційній системі також присутній, і ви можете використовувати його для налаштувань так само, як робили це в Windows.

У той же час, використання командного рядка має ряд переваг. По-перше, команди дуже легко автоматизувати, використовуючи пакетні файли.

По-друге, графічний інтерфейс сам може бути причиною помилок, крім того, на оформлення затрачаються серйозні ресурси системи. По-третє, використання текстових файлів конфігурації програм дозволяє дуже легко переносити налаштування з однієї системи на іншу, а для резервування системи в більшості випадків достатньо зберегти кілька текстових файлів.

Кілька моментів, про які слід знати користувачам Linux

В Інтернеті представлений досить великий обсяг документації по налаштуванню Linux, і якщо виникла та або інша проблема, швидше за все, ви знайдете необхідні рекомендації простим пошуком в Мережі. Тут згадаємо тільки кілька основних моментів, які потрібно врахувати адміністраторам, що мають досвід роботи тільки в Windows.

Власне сам Linux – це тільки ядро. Решта – це додатки, служби та демони, які ви встановлюєте. Непарні номери версій – експериментальні, парні (2.8 і т. д.) являють собою стабільні збірки.

У Linux не прийнято зберігати файли «де прийдеться». Є досить чітка структура розміщення інформації, тому, наприклад, всі дані користувача будуть знаходитися тільки в папці відповідного особистого профілю.

При роботі в консолі система дозволяє автоматично доповнювати введення з клавіатури після натискання клавіші <Tab>. Наприклад, якщо потрібно скопіювати файл, то досить набрати команду (cp), перші символи імені файлу і натиснути клавішу <Tab>. Якщо перші символи однозначно визначають ім'я файлу або команди, то система автоматично допише повну назву. В іншому випадку ніяких змін на екрані не буде, а повторне натискання клавіші <Tab> виведе на екран повний перелік імен, що починаються з введених символів.

«У крові» більшості системних адміністраторів живе бажання застосувати нову версію ПЗ відразу ж після його випуску. Бажання зрозуміле, хоча в більшості реальних ситуацій кінцеві користувачі не отримають від такого переходу ніяких додаткових переваг. Подумайте, які нові функції експлуатуються в офісних програмах? Переважній більшості користувачів достатньо тільки тих можливостей, які їм були доступні, наприклад, вже в MS Office 97.

У будь-якому випадку необхідно оцінити вигоди, які ви сподіваєтеся отримати від переходу на нову версію програмного забезпечення, і порівняти їх з витратами на цю операцію (вартість оновлення версій ПЗ, вартість модернізації устаткування і т. д.). Виявляється, що дуже часто можна слідувати старій добрій пораді: **якщо програма працює, то не треба її чіпати**.

Зазвичай, велика кількість версій ПЗ, що одночасно знаходяться в експлуатації, ускладнює роботу адміністратора. Наприклад, необхідно стежити за оновленнями всього парку ПЗ, встановлювати замість одного патча два або три, завантажуючи їх з Інтернету. Але зазвичай серйозних проблем така ситуація не створює.

Контрольні запитання:

1. Що прийнято розуміти під терміном «software»?
2. Назвіть основні рівні та склад програмного забезпечення типової організації.
3. Охарактеризуйте основні клієнтські операційні системи
4. Переваги та недоліки операційних систем Windows та Linux
5. Ваші поради при виборі операційної системи.

Лекція 5. DHCP, DNS, IP та основи адміністрування операційних систем сімейства Microsoft Windows

1. **Протокол DHCP та служба DNS.**

Що таке DNS і навіщо ця служба потрібна?

З чого все починалося.

Що б зрозуміти основне завдання служби DNS ми зробимо короткий екскурс в історію і побачимо як саме життя змусило і підказало створити таку службу, навіть якщо б її і не було б. Коли ще не було мереж природно не було і всяких DNS служб і мережевим адміністраторам не потрібно було собі морочити голову різними протоколами, адресами і мережевими службами.

Але ось настав час, коли саме життя, зажадало об'єднати між собою ЕОМ (електронні обчислювальні машини). Отже, починають з'являтися перші мережі. І як нам розповідають історики мережевого матеріалізму, вважається, що бабусею всіх мереж була мережа ARPANET. Унаслідок того що ЕОМ в мережі було мало, а користувачі мережі того часу як правило були «все в одному флаконі» і мережеві адміністратори і програмісти, тобто на цих машинах і в даній мережі працювали професіонали, імена ЕОМ, а більше того - їх мережеві адреси знали напам'ять.

Спочатку кожен вузол мережі ARPANET мав унікальне ім'я і унікальний номер. Потім мережа стала рости, і настав такий момент, коли кількість ЕОМ в людській пам'яті стало неможливо утримувати. І тоді мережеві розробники придумали такий текстовий файл, який знаходився на кожній машині в мережі або скажімо ЕОМ, в якому напроти імені вузла писалася його IP-адреса. Приблизно в такому вигляді:

IP адреса	-	ІМ'Я ВУЗЛА	ПРИМІТКИ
102.54.94.97		server1.rk.com	# source server
38.25.63.10		xyz.rk.com	# x client host

І отримав назву цей файл **HOSTS**. Ідея полягала в тому, що moycomp – це легко запам'ятовуване ім'я вузла або скажімо вже в термінах DNS **ім'я хоста**, і замість того що б запам'ятовувати різний незв'язаний набір цифр, користувач писав коли хотів звернутися до потрібного хосту його ім'я (в даному прикладі ім'я хоста moycomp). А клієнтський компонент (зараз називається resolver, (така спеціальна програма)) читає цей файл, знаходить ім'я машини, витягує її IP -адресу і виконує пошук за цією адресою. Ось так було на початку. І рудимент даного файлу зберігається досі на всіх версіях операційних систем Windows. Знайти і подивитися на нього ви можете на власні очі на своїй машині за адресою *% SYSTEMROOT %* \ *system32* \ *drivers* \ *etc*, відкривши його за допомогою простого блокнота.

Даний файл – HOSTS тоді заповнювався централізовано (вручну) і користувачі скачували його собі на машину. Але мережа росла і даний файл ставав дуже великим, і головне що при ручному введенні записів відповідності IP адрес імені машини, допускалися помилки. Не потрібно забувати також про те, що конфлікти виникали, коли в мережі з'являлися хости з однаковими іменами.

Коли був прийнятий стандарт TCP/IP як протокол мережі ARPANET, ця організація вирішила також удосконалити систему перетворення імен, і зупинилася на DNS, так як DNS є центральною базою даних, що містить вказівники на децентралізовані бази даних, що включають записи для кожного простору імен.

Розробником цієї системи була така організація як DARPA, яка вирішила, використовували доменну систему імен Берклі (**Berkeley Internet Name Domain, BIND**) в якості програмного забезпечення DNS.

Тобто, як бачите, якщо в двох словах, не від хорошого життя, змушені були створити таку службу, яка **автоматично ставить у відповідність «імені вузла» його IP адресу, назвали цю службу DNS**.

Тепер напишемо таку фразу.

DNS є службою перетворення імені хоста.

Враховуючи все вище сказане, думаю що ця фраза стає в деякій мірі зрозумілою. Ну давайте ще зупинимося на її основної функції – розпізнавання імен.

Наприклад вам треба зайти на якийсь сайт (який природно знаходиться на якомусь комп'ютері, названому сервером, і має свою IP-адресу). Ну самі знаєте що в браузері ви набираєте не IP адресу даного сайту а його ім'я, наприклад ім'я сайту ktpn.lntu.info. Але по суті, в будь-якій мережі комп'ютери звертаються один до одного не по імені а по IP адресі. Так от.... набравши в браузері рядок ktpn.lntu.info ви все ж отримуйте зв'язок з даним сайтом, який знаходиться на певному сервері, який має свій унікальний IP адрес, і якого ви природно не знаєте. Так ось (ще раз).... отримавши таке ім'я як ktpn.lntu.info браузер запитує службу DNS типу – «А не підкажеш, який IP адрес в цього імені». DNS шукає в своїй базі даних який IP адрес відповідає цьому імені. Вона, тобто служба DNS займається питанням перетворення даного імені, то треба розуміти, що даному імені ставиться у відповідність IP адреса, якщо таке поєднання як «ім'я вузла» і його «IP-адреса» не існує в базі DNS, то DNS служба займається опитуванням всіх DNS служб типу «підкажіть чи є у вас такий IP відповідний такому імені як ktpn.lntu.info», отримавши відповідь наш комп'ютер звертається до іншого комп'ютера (сервера) (якого він і шукає по імені), а в нашому випадку до комп'ютера з ім'ям ktpn.lntu.info вже не по імені, а як годиться в мережі за його IP адресою. Ось це і є перетворення імені.

Службою DNS – називається служба, що виконує перетворення символічних даних доменних імен в IP- адреси, у відповідь на запити клієнтів.

Служба DNS ставить відповідно ось такому символічному (букви це в даному випадку символічні дані) доменному імені, наприклад, як «moycomp.rk.com » відповідний йому IP – адрес, наприклад 10.10.10.10.

DNS сервером – називається комп'ютер на якому запушена служба DNS.

DNS клієнтом – називається комп'ютер який звертається до DNS сервера з запитом на дозвіл імені. Клієнт DNS функціонує «прозоро» для користувача. Що значить «прозоро»? Те що користувач не бачить, і не чує, і не відчуває як це відбувається.

У відповідь на свій запит по вирішенню імені клієнт DNS повинен отримати або IP-адресу, або повідомлення про неможливість доступу імені, послану сервером DNS. Далі даний клієнт передає отриману IP-адресу додатку якому потрібен даний IP-ардрес.

Делегування – операція передачі відповідальності за частину дерева доменних імен іншій особі або організації. За рахунок делегування в DNS забезпечується розподільність, адміністрування та зберігання. Технічно делегування виражається у виділенні цієї частини дерева в окрему зону, і розміщенні цієї зони на DNS-сервері (див. нижче), керованому цією особою чи організацією. При цьому в батьківську зону включаються «склеюючі» ресурсні записи (NS і A), що містять покажчики на DNS-сервера дочірньої зони, а вся інша інформація, що відноситься до дочірньої зоні, зберігається вже на DNS-серверах дочірньої зони.

DNS-клієнт (від англ. Domain Name System-client – доменних імен система – клієнт) – програма або модуль в програмі, що забезпечує з'єднання із DNS-сервером для визначення IP-адреси по його доменному імені.

Авторитетність (англ. authoritative) – ознака розміщення зони на DNS-сервері. Відповіді DNS-сервери можуть бути двох типів: **авторитетні** (коли сервер заявляє, що сам відповідає за зону) і **неавторитетні** (англ. Non-authoritative), коли сервер обробляє запит, і повертає відповідь інших серверів. У деяких випадках замість передачі запиту далі DNS-сервер може повернути вже відоме йому (за запитами раніше) значення (режим кешування).

Що таке простір імен DNS.

Основними компонентами простору імен DNS є домени. Домени треба розуміти як групу мережевих хостів (вузлів) об'єднані за деяким логічним принципом. Домени взаємодіють один з одним за допомогою відносин «батько-нащадок», утворюючи тим самим певну ієрархію. Тобто, коли йдеться про ієрархію доменів треба розуміти ставлення «батько-нащадок». Положення домену в ієрархії визначає рівень домену (домен другого рівня, домен третього рівня і т.д. зважаючи на його положення від батьківського домену).

В основі ієрархічної побудови простору імен DNS лежить домен, який називається **кореневим доменом** (rootdomain) (не плутайте з кореневим доменом в Active Directory).

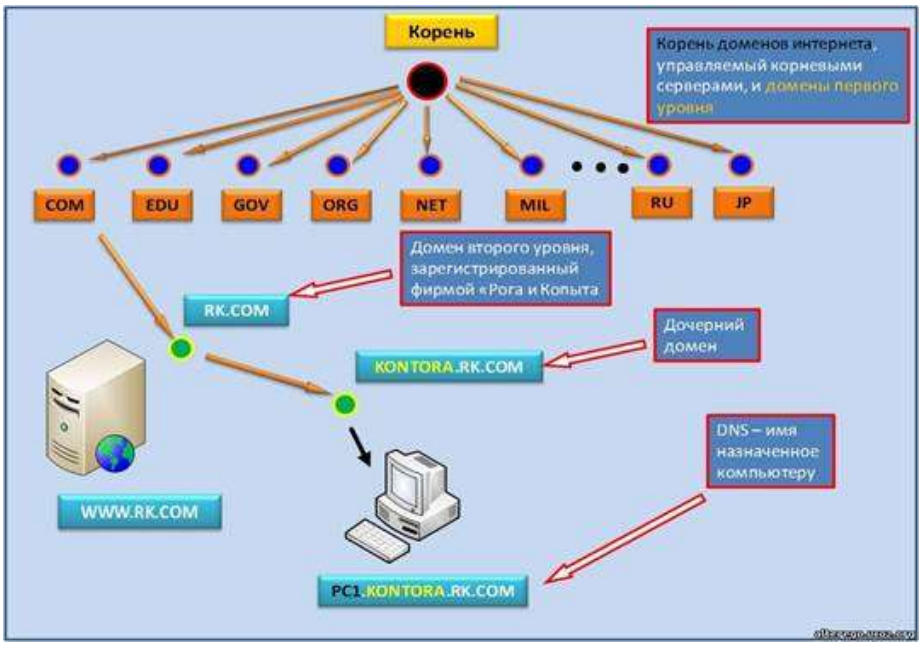


Рис.3. Простір імен DNS

Кореневий домен дотримуючись традицій літератури є як «весільний генерал». Тобто, кореневий домен формальний або чисто символічний, але тим не менше він є прабатьком всіх інших нині існуючих в інтернеті доменів. Або батьком доменів першого рівня таких як *com, edu, org* … та інших, що належать різним організаціям, так само домени належать країнам: *ua, ro, jp*... ну і так далі.

Домени, як ми знаємо виступають в ролі контейнерів. І якщо розглядати це як ієрархію, то в якості листків виступають відомості про ресурси цих доменів. Будь-який об'єкт мережі, який виходячи зі стандартів визначає службу DNS називається хост (host) або хостами.

Будь-який об'єкт простору імен DNS будь-то домен або хост має унікальне ім'я в межах батьківського контейнера.

Імена DNS можуть складатися із символів латинської алфавіту, цифр, і знака «–» тире. Деякі версії DNS в тому числі і DNS Windows Server допускають використовувати в іменах символу підкреслення «_», а також символів у форматі UTF- 8.

Точно ідентифікувати об'єкт можна тільки за допомогою його **«повного доменного імені» FQDN** (Fully Qualified Domain Name).

Повне доменне ім'я хоста утворюється з імені об'єкта і суфікса DNS.

Що таке суфікс DNS? Це всього лише перерахування імен всіх контейнерів (по суті доменів), що знаходяться між безпосередньо ім'ям хоста або об'єкта і коренем простору імен.

Єдиним об'єктом простору імен DNS, що не має ім'я є кореневий домен. Ось так, найголовніший а без імені. Для посилання на нього використовується крапка «.»

І сьогоднішні, сучасні DNS так само представляють, по суті, базу даних з тією ж основною інформацією, яку містив попередник DNS, файл HOSTS. Але на відміну від історичного файлу HOSTS який тримав всю інформацію про всі хости в єдиному файлі, сучасні DNS представляють **розподілену систему зберігання інформації**, або DNS це – розподілена база даних.

Що таке розподілена база даних взагалі ? Це така база даних, яка зберігає інформацію не всю в одному місці, а розподіляє її по різних місцях залежно від якоїсь логіки, яка була внесена при побудові (створенні, проектуванні) даної бази даних. Так от, DNS і є розподілена база даних, і інформація зберігається в різних місцях. І ось чому.

Як ви вже знаєте з попередньої теми – основними компонентами простору імен DNS є домени. Домени взаємодіють один з одним за допомогою відносин «предок-нащадок», утворюючи тим самим певну ієрархію (див. рис. 1). Тобто один домен є «батьком» – решта є «дочірніми» доменами стосовно батьківського.

Наприклад, домен COM – це контейнер. У доменній ієрархії COM, домен першого рівня або TLD. Тоді вирішили – нехай даний контейнер, і зберігає інформацію, про всі об'єкти, що

відносяться до даного контейнера. Наприклад, інформація про зареєстрований домен RK.COM зберігатиметься в домені (контейнері) COM.

Слово «зареєстрованому» – означає що дійсно в інтернеті такому імені як RK.COM «чиновники від інтернету», офіційно присвоїли в суворій відповідності IP-адресу, що б до нього могли звертатися.

Тобто, COM контейнер або домен першого рівня TLD зберігає інформацію про свої дочірні об'єкти, домени другого рівня такі як, наприклад, у нас домен RK.COM домен другого рівня SLD. Тобто логіка, грубо кажучи така - «зробив – зберігай». А от інформація про піддомени, які породив домен UA першого рівня (TLD) зберігає інформацію про всіх його дочірні об'єкти, домени другого рівня (SDL), наприклад edu.ua.

Зони DNS

Ділення доменного простору імен між DNS – здійснюється за допомогою механізму зон (zone).

Зона являє собою базу даних, в якій містяться записи про відповідність (деякої безлічі доменних імен IP адресам). Тобто все як звичайно «ім'я – IP адреса». Кожна зона представляє тільки частину доменного простору імен. Можна сказати ще так: «Зоною – називається частина домену DNS». Чому частина? Ось наприклад, домен RK.COM може містити кілька зон, наприклад зону – KONTORA.RK.COM і зону – BUHGALTERIA.RK.COM. Як правило, термін «зона» використовується для позначення частини домену відносно DNS-сервера або нащадка. Термін «піддомен» використовується для позначення частини домену, що міститься в зоні. При наявності в домені тільки однієї зони використовується будь-який з цих термінів.

Зони слід розглядати як основний адміністративний інструмент, на рівні якого відбувається, як управління простору імен в цілому, так і управління процесом перетворення імен.

Межі зони не визначаються межами домену. Одна зона може включати в себе кілька доменів, в той час як об'єкти, що належать одному домену можуть бути розміщені в декількох зонах. Здійснюючи поділ доменного простору імен на зони системний адміністратор повинен виходити в першу чергу з зручності адміністрування і навантаженням на DNS сервери. Див. рис. 4.

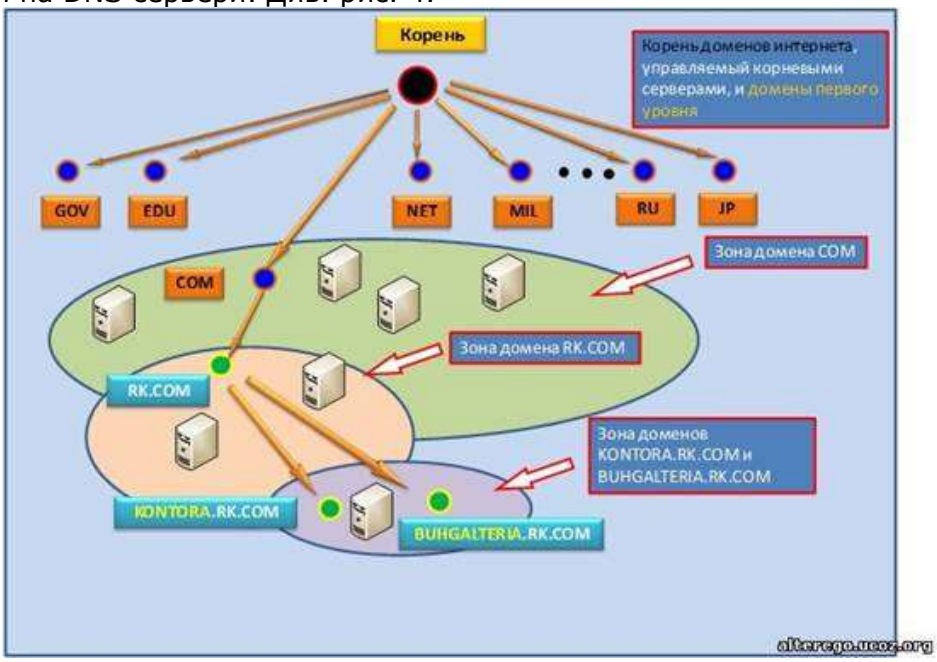


Рис.4. Зони DNS

Параметри TCP / IP-протоколу

Тут і далі ми будемо розглядати характеристики протоколу IPv4.

IP-адреса

Кожен комп'ютер, що працює по протоколу TCP / IP, обов'язково має IP-адреса – 32-бітове число, що використовується для ідентифікації вузла (комп'ютера) в мережі. Адресу

прийнято записувати десятковими значеннями кожного октету цього числа з поділом отриманих значень точками. Наприклад: 192.168.101.36.

IP-адреси унікальні. Це означає, що кожен комп'ютер має своє поєднання цифр, і в мережі не може бути двох комп'ютерів з однаковими адресами. IP-адреси розподіляються централізовано. Інтернет-провайдери роблять заявки в національні центри у відповідності зі своїми потребами. Отримані провайдерами діапазони адрес розподіляються далі між клієнтами. Клієнти самі можуть виступати в ролі інтернет-провайдера і розподіляти отримані IP-адреси між субклієнтами і т. д. При такому способі розподілу IP-адрес комп'ютерна система точно знає «розташування» комп'ютера, що має унікальну IP-адресу; їй достатньо переслати дані в мережу «власника». Провайдер у свою чергу проаналізує пункт призначення і, знаючи, кому віддана ця частина адрес, відправить інформацію наступному власникові піддіапазону IP-адрес, поки дані не надійдуть на комп'ютер призначення.

Для побудови локальних мереж організацій виділені спеціальні діапазони адрес. Це адреси 10.x.x.x, 192.168.x.x, 10.x.x.x, з 172.16.x.x по 172.31.x.x, 169.254.x.x (під «x» мається на увазі будь-яке число від 0 до 254). Пакети, що передаються з зазначених адрес, не маршрутизируются (іншими словами, не пересилаються) через Інтернет, тому в різних локальних мережах комп'ютери можуть мати співпадаючі адреси із зазначених діапазонів. Такі адреси часто називають сірими адресами.

Автоматичне привласнення параметрів IP-протоколу

Як вже зазначалося, параметри IP-протоколу індивідуальні для кожного комп'ютера. Щоб полегшити користувачам їх призначення, були розроблені спеціальні механізми, що дозволяють автоматизувати даний процес.

Сервери DHCP

У локальних мережах адміністратори встановлюють так званий сервер DHCP.

ПРИМІТКА

Адресація APIPA

Для полегшення побудови невеликих мереж передбачена можливість самостійного призначення адрес. Якщо в мережі немає сервера DHCP, а протокол IP встановлений з параметрами автоматичного отримання значень, то Windows присвоїть мережевій платі адреса з діапазону від 169.254.0.1 по 169.254.255.254 (маска під-мережі 255.255.0.0), попередньо перевіривши, чи не використовується вже таку адреса в системі. Даний механізм дозволяє застосовувати IP-протокол в невеликих мережах при мінімальних ручних настройках – комп'ютери побачать один одного в локальній мережі. Природно, що ніяких додаткових параметрів налаштування операційна система в цьому випадку не отримує. Наприклад, вона не буде знати, куди посилати запити, щоб отримати дані з серверів Інтернету.

Використання адреси з зазначеного раніше діапазону (перевіряється командами ipconfig або winipcfg) при наявності в мережі сервера DHCP свідчить або про несправність останнього, або про проблеми кабельного підключення даного комп'ютера.

Порт

При передачі даних крім IP-адрес відправника і одержувача пакет інформації містить в собі номери портів. Порт – це якесь число, яке використовується при прийомі і передачі даних для ідентифікації процесу (програми), який повинен обробити дані. Так, якщо пакет відправлений на 80-й порт, то це свідчить, що інформація призначена для сервера HTTP.

Номери портів з 1-го по 1023-й закріплені за конкретними програмами (так звані well-known-порти). Порти з номерами 1024 – 65 535 можуть бути використані в програмах власної розробки. При цьому можливі конфлікти повинні вирішуватися самими програмами шляхом вибору вільного порту. Іншими словами, порти будуть розподілятися динамічно: можливо, що при наступному старті програма вибере інше значення порту.

Знання того, які порти використовують ті чи інші прикладні програми, важливо при налаштуванні брандмауерів. Частина налаштувань в таких програмах для найбільш популярних протоколів зумовлена, і вам достатньо тільки дозволити / заборонити протоколи, керуючись їх назвами. Проте в деяких випадках доведеться звертатися до технічної документації, щоб визначити, які порти необхідно «відкрити», щоб забезпечити проходження пакетів даної програми.

Побачити, які порти реально задіяні на комп'ютері, можна за допомогою команди *netstat*.

Брандмауер (брандмауер)

Міжмережевий екран (МСЕ), або брандмауер (firewall), – це комплекс технічних, програмних та організаційних заходів з безпечного підключення однієї мережі до іншої. Залежно від розв'язуваних завдань і конфіденційності інформації, що захищається це може бути просто невелика програма, встановлена на комп'ютері, або ж спеціалізовані апаратні засоби, що реалізують вимоги конкретної організації.

Зазвичай за загальними міркувань безпеки в якості брандмауера рекомендується використовувати автономний пристрій. Іншими словами, у разі програмної реалізації брандмауера на цей комп'ютер не слід покладати рішення ніяких інших завдань.

Варіанти міжмережевих екранів

У розпорядженні адміністраторів є як апаратні міжмережеві екрани, так і програмні рішення. Різниця між цими двома варіантами достатньо умовна. Апаратний модуль – це фактично спеціалізована під певне завдання та чи інша обчислювальна система. Зазвичай для нього створюється операційна система (наприклад, IOS у Cisco) або використовується безкоштовна версія Linux.

Програмні варіанти припускають установку на типові операційні системи, наприклад: на Linux, операційні системи від Microsoft і т. П.

У Мережі існує велика кількість програм, призначених для захисту індивідуальних комп'ютерів. Наприклад, можна відзначити такі персональні міжмережеві екрани, як AtGuard, BlackICE Defender, Jammer, Kerio Personal Firewall, Outpost Firewall, Sygate Personal Firewall, Tiny personal firewall, Zone Alarm та ін. Частина цих продуктів – комерційні програми, частина має версії, доступні для безкоштовного використання.

DHCP

Протокол динамічної конфігурації вузла (Dynamic Host Configuration Protocol) – це мережевий сервіс, який дозволяє комп'ютерам в мережі автоматично отримувати налаштування мережі із сервера замість того, щоб налаштовувати кожен мережевий хост вручну. Комп'ютери, налаштовані бути клієнтами DHCP, не управляють тим, які налаштування вони отримають від DHCP сервера, і це налаштування зовсім непомітне для користувача комп'ютера. Стандарт протоколу DHCP був прийнятий у жовтні 1993 року

У загальному випадку **налаштування, передані DHCP сервером** DHCP клієнтам включають:

- *IP адресу і мережеву маску;*
- *IP адреса шлюза;*
- *IP адресу DNS серверів;*

Однак DHCP сервер може також надати такі параметри налаштування, як:

- Ім'я хоста
- Ім'я домена
- Адреса сервера часу
- Адреса сервера друку

Перевага використання DHCP полягає в нестабільності налаштувань мережі, наприклад, зміна адреси DNS сервера потребує змін тільки на DHCP сервері, а всі мережеві хости будуть переналаштовані в момент наступного запиту їх DHCP клієнта до DHCP сервера. Додаткова перевага полягає в простому підключенні нових комп'ютерів до мережі, оскільки не потрібно перевіряти доступність IP адрес. Конфлікти за виділеними IP адресами також мінімальні.

DHCP сервер може **надавати налаштування**, використовуючи такі методи:

- *Виділення уручну (за MAC адресою)*:

Цей метод передбачає використання DHCP для визначення унікального апаратної адреси кожної мережевої карти, підключеної до мережі, і потім тривалого надання незмінній конфігурації кожен раз, коли DHCP клієнт робить запит на DHCP сервер, використовуючи свій мережевий пристрій. Це гарантує, що певну адресу буде автоматично присвоєно цій мережевій картці на основі її MAC адреси.

- *Динамічне виділення (пул адрес):*

При цьому методі, DHCP сервер виділятиме IP адреси з пулу адрес (іноді званим діапазоном або областю) на період часу (або в оренду), який налаштовується на сервері,

або поки клієнт не проінформує сервер, що більше взагалі не потребує адреси. Таким чином, клієнти отримують свої налаштування динамічно за принципом «перший прийшов – перший обслужений». Коли DHCP клієнт відсутній в мережі певний час, адреса вважається простроченою і повертається в пул адрес для використання іншими DHCP клієнтами. Це означає, що адреса орендується або видається на певний період часу. Після закінчення цього періоду клієнт повинен повторно домовлятися про використання адреси з сервером.

- Автоматичне виділення

Використовую цей метод, DHCP автоматично присвоює постійну IP адресу пристрою, вибрану з пулу доступних адрес. Зазвичай DHCP використовується для видачі тимчасового адреси, але DHCP сервер може використовувати нескінченний час оренди.

Два останніх методи можна розглядати, як автоматичні, оскільки DHCP сервер видає адреси без додаткового втручання. Єдина різниця полягає в тому, наскільки часу орендується адреса, іншими словами, коли закінчиться час використання адреси клієнтом.

2. Служба каталогів Active Directory

Що таке Active Directory? Щоб зрозуміти це «поняття», і чому не лише Microsoft але і інші виробники операційних систем зробили таку ж «фішку» у своїх операційних системах (Макінтош використовує «фішку» Open Directory, Novell службу каталогів NDS), розпочнемо з історії.

Припустимо у нас три комп'ютери, три користувачі і один сервер. Поки усе нормально, але ось наша організація розширилася і взяли на роботу ще трьох співробітників, а комп'ютерів доки не купили. Разом у нас є мережа з 3 ПК і 6 користувачів, які доки працюють попарно по двоє на кожному ПК. Вийде така картина як на рис. 1.

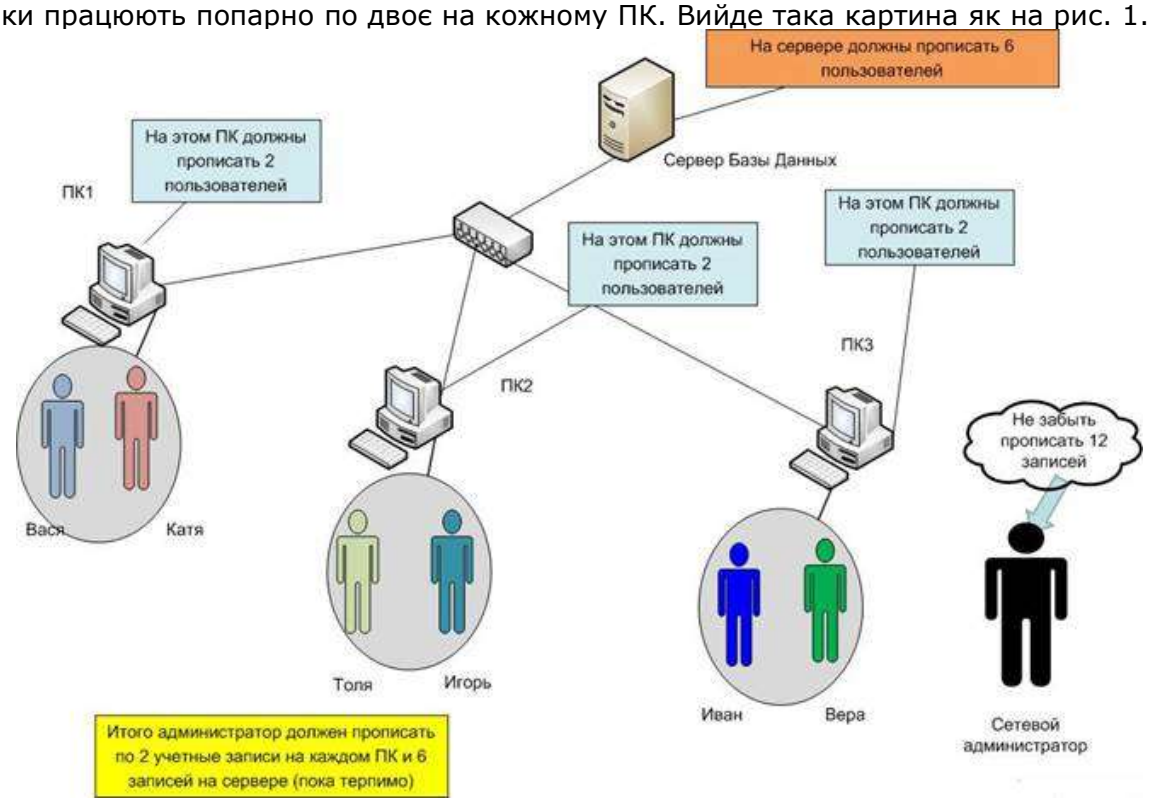


Рис. 1

Тобто, при появі в компанії нових співробітників і з урахуванням того що співробітники строго працюватимуть тільки за тими ПК, які за ними закріплені адміністратор прописує кожного співробітника на відповідному ПК. Виходячи з рис. 1 системний адміністратор прописує на ПК1 облікові записи для користувачів Васі і Каті, на ПК2 – Анатолія і Ігоря, а на ПК3 – Івана і Віри (як він це робить конкретно, ми розглянемо пізніше). І ще йому потрібно прописати цих усіх користувачів у кількості 6 штук на сервері щоб користувачі могли отримати доступ до сервера бази даних. Отже доки терпимо, оскільки користувачів не так вже і багато.

І тільки прописавши користувачів адміністратор, сів попити кави, як нова вказівка від керівництва. Потрібно щоб користувачі не прив'язувались до строго певного комп'ютера, а дозволити їм працювати за будь-яким комп'ютером. І адміністратор опустивши голову, йде і прописує усіх користувачів на усіх комп'ютерах. І якщо раніше, коли за певним комп'ютером працював певний користувач або користувачі, то виходячи з нашої придуманої організації на рис. 1, на кожному комп'ютері було по два облікові записи. Та тепер на кожному комп'ютері мають бути по 6 прописаних користувачів.

Отже, повернемося до нашого адміністратора. Він йде і прописує на кожному ПК усіх співробітників організації. Теж поки що не страшно. А ось вже починаються «сутінки». У нашу організацію узяли на роботу ще співробітників, і купили ще серверів і купу комп'ютерів. Дивіться рис. 2.

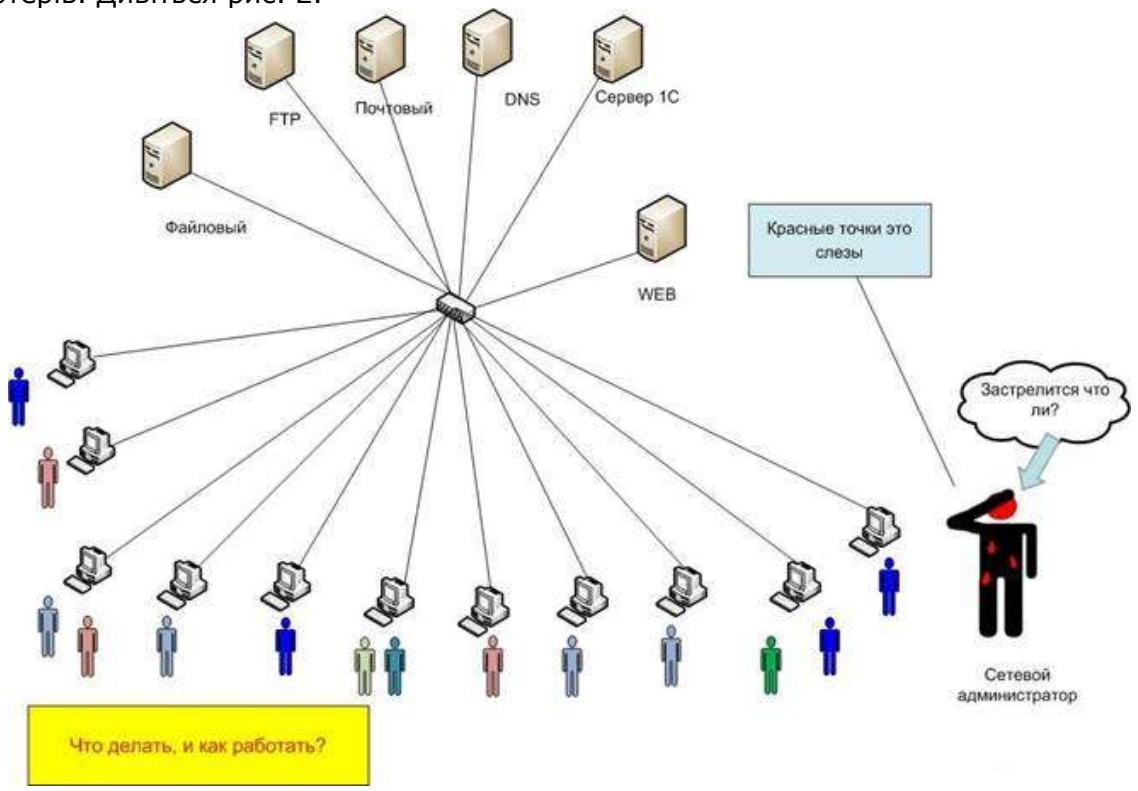


Рис. 2

Тобто саме життя продиктувало необхідність в створення інструменту, який би полегшував роботу користувачів і мережевих адміністраторів в повсякденному житті. Акаунти (облікові записи) стали зберігатися централізовано, тобто в одному місці і відпала необхідність прописувати користувачів на кожному ПК і на кожному сервері в нашій мережі, а користувачам досить один раз зареєструватися в мережі і більше не потрібно це робити на кожному сервері куди він хоче попасти. Краса. Та і взагалі, усе що є у нас в мережі Active Directory зберігає в одному місці, централізовано, а ще дозволяє «пускати» і «не пускати» зухвалих користувачів куди завгодно, і дозволяє так само управляти (адмініструвати) усім, що є у нас в мережі, не витрачаючи додаткові ресурси як у плані узяття на роботу ще адміністраторів, так і в плані купівлі додаткових засобів від сторонніх виробників, для адміністрування мережі і об'єктів що знаходяться в ній.

І що у нас вийшло з впровадженням такого поняття як **Active Directory** або як ще його називають – **Служби каталогів**. Дивимося рис. 3.

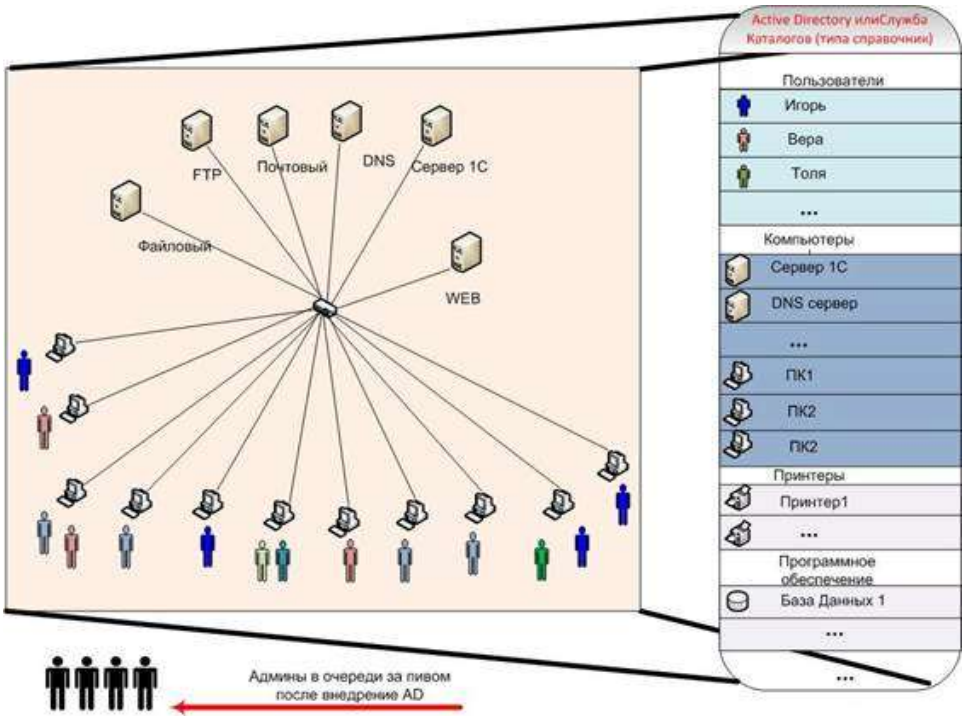


Рис. 3

Основні терміни і поняття Active Directory.

Каталог (directory) – сукупність інформації про об'єкти, які тим або іншим способом пов'язані один з одним.

Тобто це певний інформаційний ресурс, використовуваний для зберігання інформації про який-небудь об'єкт. Приміром найпростіший історичний каталог, це такий зошит в який деякий громадянин записує своїх боржників. Чи сучасніший приклад – телефонний довідник що містить інформацію про абонентів телефонної мережі. У файловій системі каталоги (директорії, теки) зберігають інформацію про файли, пов'язані між собою тим або іншим способом, приміром, усі файли з теки такої-то – це деякі оповідання.

У нашій мережі в каталозі може зберігатися інформація про об'єкти нашої мережі. Це можуть бути принтери, комп'ютери, користувачі, програмні продукти і різні бази даних які є у нас. Головна «фішка» або завдання тут в тому, що б надати користувачам можливість виявити (знайти) ці об'єкти і використовувати їх, але під гострозорим оком адміністратора, а не так як хочуть користувачі.

Давайте розберемося із поняттям об'єкт. І розглянемо це поняття саме в контексті мережі.

Об'єкт – самостійна одиниця, яка представляє деякий ресурс, існуючий в мережі (ПК, користувачі, ПО, ...) з усіма його атрибутами. Що таке атрибут? Уявіть, що у нас є автомобіль, так от автомобіль це об'єкт, а його колір, потужність і інше це атрибути або властивості і характеристики. Але ми не будемо використовувати, коли говоритимемо про об'єкти у більшості випадків словосполучення «властивості і характеристики» а говоритимемо – його атрибути. Приміром у такого об'єкту нашої мережі як «користувач» є такі атрибути як – прізвище, ім'я, логін, пароль, адреса електронної пошти і інші. Дивіться рис 4.

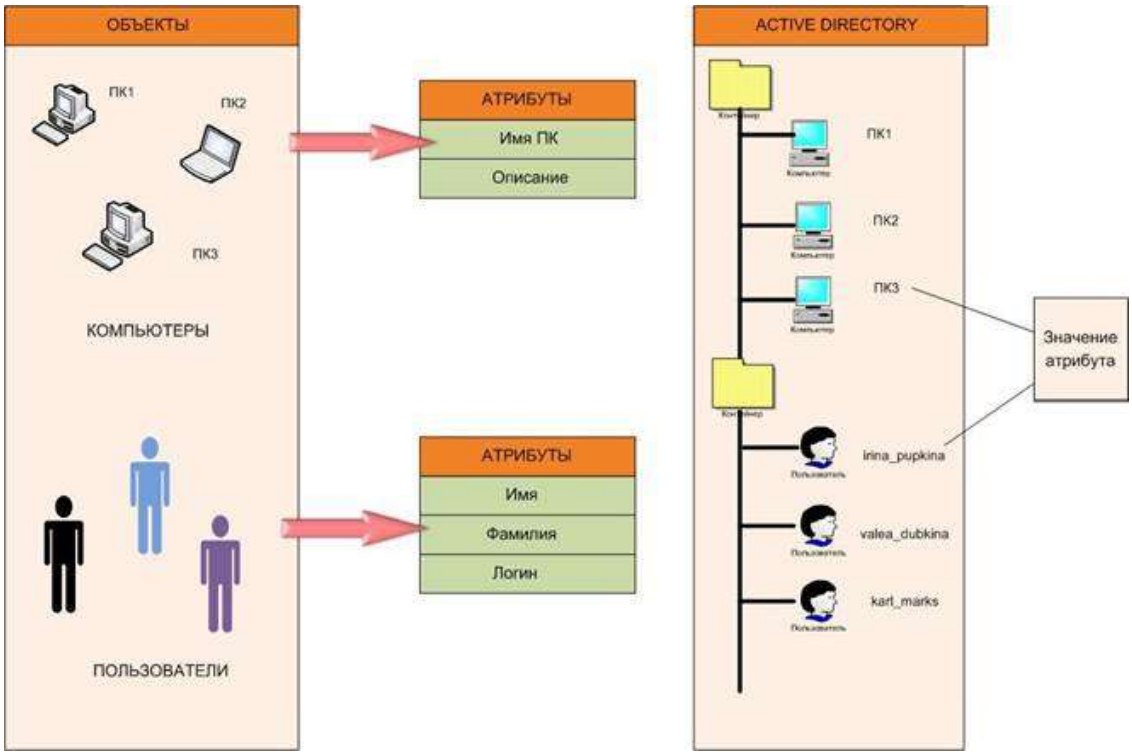


Рис. 4

Служба каталогів (directory service) – за допомогою допоміжних служб забезпечує зберігання усієї необхідною для застосування об'єктів і управління ними інформації, в одному місці (централізовано), і завдяки цьому процес виявлення і адміністрування ресурсів мережі спрощується. На відміну від каталогу, служба каталогів має одночасно дві ролі:

- джерела інформації;
- механізму, за допомогою якого ця інформація готується для доступу з боку користувачів.

Служба каталогів – щось на зразок основної панелі керування мережевої операційної системи (центрального пульта). Чи що б було зовсім зрозуміло.

Служба каталогів – це таке програмне забезпечення (така програма) у складі мережевої операційної системи, яка **зберігає усю інформацію про об'єкти мережі, і яка дозволяє виявляти ці об'єкти** (різні комп'ютери, принтери, користувачів і інше, що є у нас в мережі, а усе, що є у нас в мережі, ми розглядаємо як об'єкти), **надавати їх в розпорядження користувачам, і управляти ними (адмініструвати)**.

Тобто на питання – що таке служба каталогів? Ви жваво відповідайте – це таке ПЗ (програмне забезпечення) яке «зберігає», «виявляє», «робить доступним користувачам» і «управляє ними», тобто об'єктами.

Контролер домена – це комп'ютер на якому встановлено таке ПЗ як Active Directory.

Так от, вже слово «фішка», яким ми користувалися на початку нашого важкого оповідання набуло деякого сенсу, і тепер воно з'явилося перед нами як «Служба Каталогів». Що б не плутатися що таке «Служба каталогів» і «Active Directory», то напишемо так.

Служба каталогів Active Directory – це програмне забезпечення написане (розроблене) Microsoft. Тобто Microsoft назвав «службу каталогів» ім'ям «Active Directory». Макінтош назвав свою службу каталогів – Open Directory, а Novell – NDS.

І виходить двома словами, що **Active Directory містить каталог, в якому зберігається інформація про наші мережеві ресурси і служби що надають доступ до цієї інформації**. Ну щось на кшталт бази даних з інформацією про мережеві ресурси.

Так от «**Служба каталогів»** – це з одного боку інструмент адміністрування, а з іншого засіб взаємодії кінцевого користувача з системою.

Чим більше розростається наша мережа, тим більше в ній об'єктів, якими необхідно управляти, і тут без впровадження Служби Каталогів – Active Directory не обійтися.

Обліковий запис користувача (акаунт) – складається з імені користувача (логін) і пароля (наприклад pupkin і пароль «d345rtHfa»). Не маючи цих даних не можна увійти до мережі або працювати на комп'ютері. Перший раз при вході в мережу пароль вам повідомить адміністратор і залежно від того як він налаштував роботу з паролем в Active Directory ви можете відразу його змінити на ваш пароль, який окрім вас ніхто не знає. Системний адміністратор дуже МОГУТНЯ ЛЮДИНА і він може змінити будь-які налаштування вашого облікового запису, тому з ним потрібно дружити і шанувати його...

Контейнер – контейнер аналогічний об'єкту в тому сенсі, що він також має атрибути і належить простору імен. Проте, на відміну від об'єкту, контейнер не означає нічого конкретного: він може містити групу об'єктів або інші контейнери.

Ще в Active Directory передбачено ряд компонентів, що допомагають збудувати структуру каталогу відповідно до наших потреб і діляться ці компоненти на логічні і фізичні компоненти. Рис. 5.

Логічне ділення робиться на такі компоненти як **домени, підрозділи** (OU, organizational unit), **дерева і ліси**. Фізичне на **контролери домена і сайти**. Логічні і фізичні компоненти розділені.

Рис. 5

Підрозділи або організаційні одиниці OU використовуються для групування об'єктів в адміністративних цілях (ну що б нам було зрозуміліше, а головне зручніше працювати). Вони можуть делегувати (передавати) адміністративні права і управляти групою об'єктів як окремим підрозділом.

Active Directory – LDAP-сумісна реалізація інтелектуальної служби каталогів корпорації Microsoft для операційних систем родини Windows NT. Active Directory дозволяє адміністраторам використовувати групові політики (GPO) для забезпечення детального налаштування користувацького робочого середовища, розгортати ПЗ на великій кількості комп'ютерів (через групові політики або за допомогою Microsoft Systems Management Server 2003 (або System Center Configuration Manager)), встановлювати оновлення ОС, прикладного та серверного ПЗ на всіх комп'ютерах в мережі (із використанням Windows Server Update Services (WSUS); Software Update Services (SUS) раніше). Active Directory зберігає дані і налаштування середовища в централізованій базі данних. Мережі Active Directory можуть бути різного розміру: від кількох сотень до кількох мільйонів об'єктів.

Презентація Active Directory відбулась в 1999 році, продукт був вперше випущений із Windows 2000 Server, а потім був модифікований і покращений при випуску спочатку Windows Server 2003, а потім Windows Server 2003 R2.

На відміну від версій Windows до Windows 2000, котрі використовували в основному протокол NetBIOS для мережевої взаємодії, служба Active Directory інтегрована з DNS та TCP/IP.

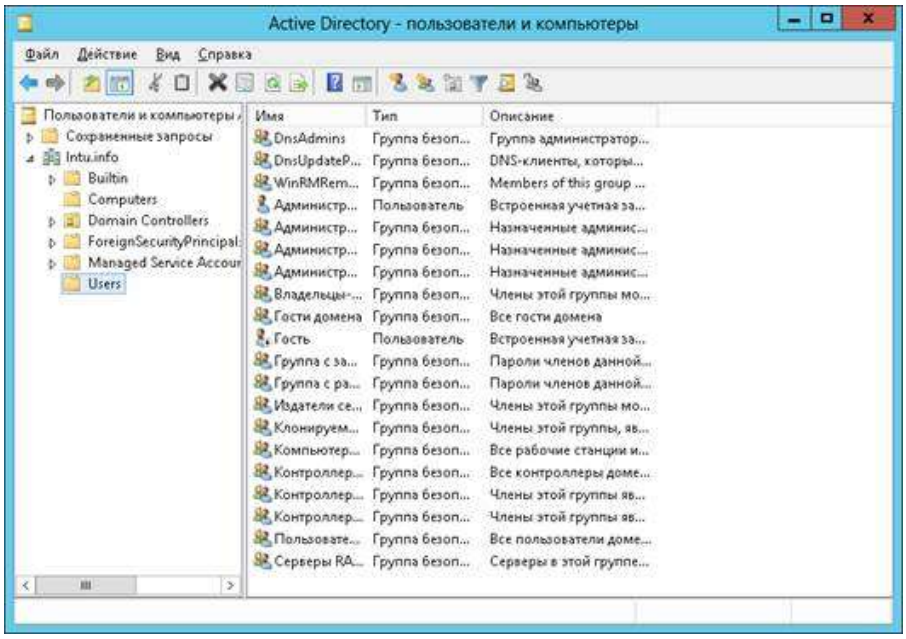


Рис. 16

Інтеграція з UNIX

Різні рівні взаємодії з *Active Directory* можуть бути реалізовані у більшості *UNIX* – подібних операційних систем за допомогою відповідних стандарту *LDAP* клієнтів, але такі системи, як правило, не сприймають велику частину атрибутів, що асоціюються з компонентами *Windows*, наприклад групові політики і підтримку односторонніх доручень.

Сторонні постачальники пропонують інтеграцію *Active Directory* на платформах UNIX, включаючи UNIX, Linux, Mac OS X і ряд додатків на базі Java, з пакетом продуктів :

- *Centrify DirectControl* (Centrify Corporation) – *сумісні* з Active Directory централізовану аутентифікацію і контроль доступу.
- *Centrify Express* (Centrify Corporation) – набір *вільних сумісних* з Active Directory сервісів для централізованої аутентифікації, моніторингу, доступу до файлів, що розділяється, і віддаленого доступу.
- *UNAB* (Computer Associates).
- *TrustBroker* (*CyberSafe Limited*) – реалізація Kerberos.
- *PowerBroker Identity Services*, раніше *Likewise* (BeyondTrust) – дозволяє клієнтові увійти *до домена Active* Directory.
- *Authentication Services* (Quest Software).
- *ADmitMac* (*Thursby Software Systems*).
- *Samba* – може виконувати роль контроллера домена.

Альтернативним варіантом є використання іншої служби каталогів, наприклад *389 Directory Server (раніше Fedora Directory Server*, FDS), *eB2Bcom ViewDS v7.1XML Enabled Directory* або *Sun Java System Directory Server* від Sun Microsystems, що виконує двосторонню синхронізацію з Active *Directory,* реалізовуючи таким чином «відбиту» інтеграцію, коли клієнти UNIX і Linux аутентифікуються FDS, а клієнти Windows аутентифікуються Active Directory. Іншим варіантом є використання OpenLDAP з можливістю напівпрозорого перекриття, що розширює елементи віддаленого сервера LDAP додатковими атрибутами, що зберігаються в локальній базі даних.

Active Directory автоматизуються за допомогою Powershell.

3. Консоль керування MMC та інтерфейс Windows Management Instrumentation (WMI).

Консоль керування MMC

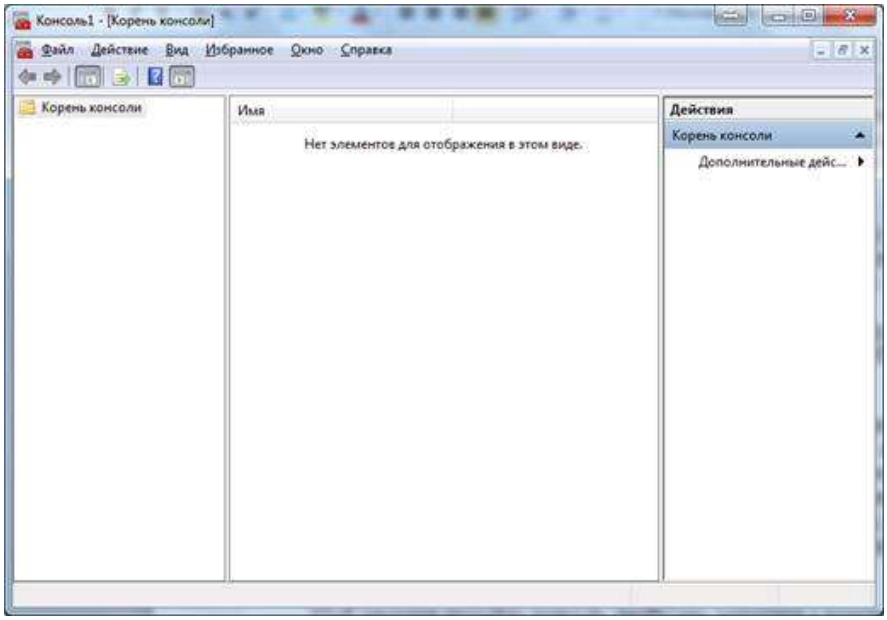
Консоль (consol) – пристрій, який забезпечує взаємодію оператора комп'ютера з операційною системою. Як правило, як консоль використовується дисплей і клавіатура. Також під словом консоль часто мають на увазі інтерфейс командного рядка (термінал).

Консоль керування Microsoft Management Console (MMC) – інструмент, призначений для створення, збереження і відновлення засобів адміністрування (консолей MMC), які здатні керувати різноманітними пристроями, програмними і мережевими елементами операційної системи Windows. MMC здатна працювати з різними версіями операційної системи Windows.

MMC уніфікує і спрощує повсякденні завдання керування системою. Інструменти, що містяться в ній, відображаються у вигляді консолей. Консолі, що складаються з одного або декількох додатків, побудовані з модулів, які називаються оснащеннями – невеликими програмами, що дозволяють налаштувати різні аспекти операційної системи. Також з консолі керування можна отримати розширені функції керування користувачами і групами, в ній можна налаштувати безліч параметрів (наприклад, заголовок вікон Internet Explorer). Більш широким вбудованим інструментом керування Windows є «Редактор реєстру».

Існує два способи використання можливостей консолі MMC: у призначеному для користувача режимі (використовуючи готові консолі: *gpedit.msc, lusrmgr.msc і т.д.*) або в авторському режимі (створюючи нові або редагувати вже створені).

Щоб дати користувачеві право на виконання певних адміністративних завдань, необхідно створити нову консоль MMC, додати в неї всі потрібні інструменти, налаштувати її конфігурацію, відрегулювати права даного користувача і лише після цього необхідно записати створену консоль на змінний носій і передати її тому, кому вона призначалася. Після запуску консолі користувач отримає всі необхідні інструменти для виконання конкретного завдання, що дозволить йому відразу перейти до її виконання.



Щоб створити потрібну консоль, необхідно запустити з командного рядка файл *mmc.exe*. Після цього MMC почне роботу, а на екрані відобразиться нова консоль, За допомогою командного рядка також можна запустити вже створену консоль.

Збережена консоль представлена файлом з розширенням *.msc*.

Одна і та ж консоль може поєднувати в собі безліч різноманітних інструментів, які вбудовуються в неї у вигляді окремих модулів. Windows XP,7 містить безліч таких модулів MMC, проте якщо яке-небудь завдання не може бути виконано з їх допомогою, то можна спробувати додати оснащення інших розробників.

У консолі MMC можна створити вікно, яке міститиме значки, що відповідають за виконання певних завдань або дій. Такі спеціальні вікна називаються «Панелями завдань».

Windows Management Instrumentation (WMI) в дослівному перекладі – це інструментарій керування Windows. Якщо говорити більш широко, то WMI – це одна з

базових технологій для централізованого керування і стеження за роботою різних частин комп'ютерної інфраструктури під керуванням платформи Windows.

Технологія WMI – це розширена і адаптована під Windows реалізація стандарту *WBEM* (на англ.), Прийнятого багатьма компаніями, в основі якого лежить ідея створення універсального інтерфейсу моніторингу та керування різними системами і компонентами розподіленої інформаційної середовища підприємства з використанням об'єктно-орієнтованих ідеологій і протоколів HTML і XML.

В основі структури даних в WBEM лежить Common Information Model (CIM), що реалізує об'єктно-орієнтований підхід до подання компонентів системи. CIM є розширюваною моделлю, яка дозволяє програмам, системам і драйверам додавати в неї свої класи, об'єкти, методи і властивості.

WMI, заснований на CIM, також є відкритою уніфікованою системою інтерфейсів доступу до будь-яких параметрів операційної системи, пристроїв і додатків, що функціонують в ній.

Важливою особливістю WMI є те, що об'єкти, які зберігаються в ній відповідають динамічним ресурсам, тобто параметри цих ресурсів постійно змінюються, тому параметри таких об'єктів не зберігаються постійно, а створюються за запитом споживача даних. Сховище властивостей об'єктів WMI називається репозиторієм і розташоване в системній папці операційної системи Windows:

%SystemRoot%\System32\WBEM\Repository

Використання WMI у програмах

Ресурси WMI доступні не тільки через скрипти, до них можна звертатися з інших мов програмування і навіть з програм.

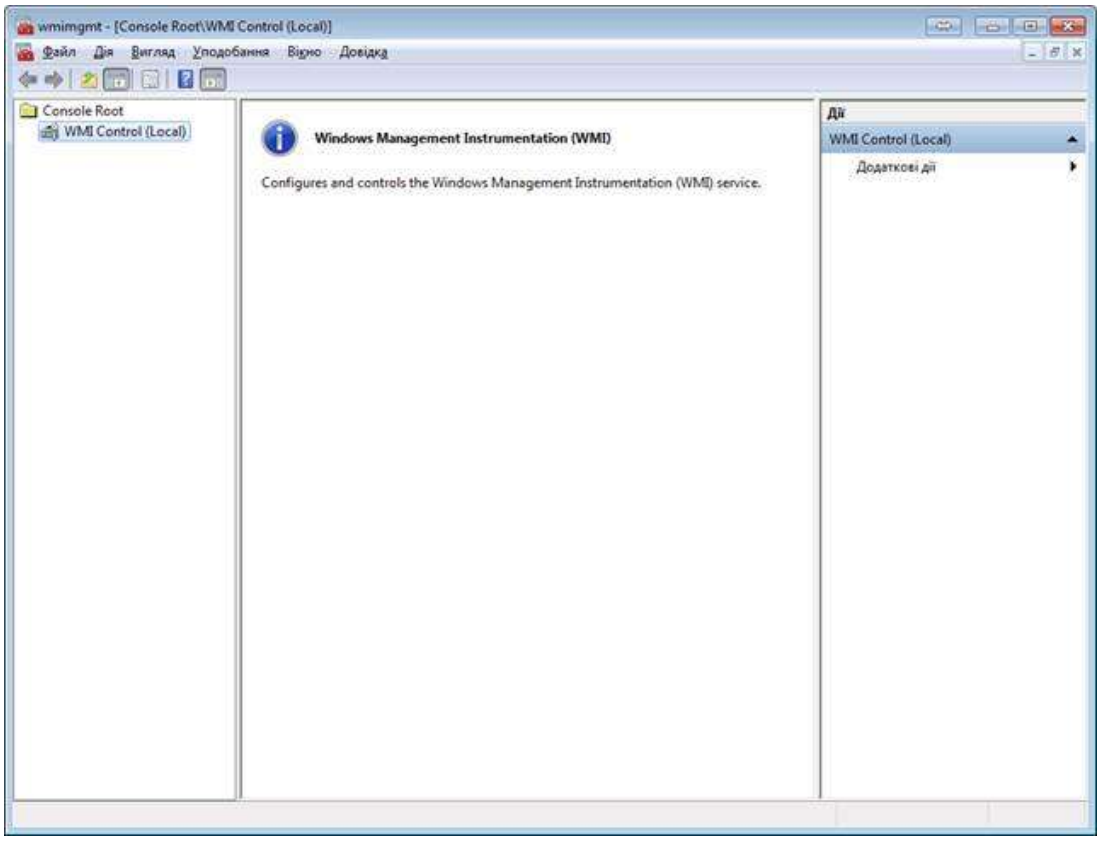
Як приклад програми використання WMI в Visual Basic.Net можна представити консольний додаток керування сервісом друку комп'ютера. Додаток запитує модель комп'ютера і виводить результат у консоль. Після чого запрошувати стан сервісу друку і, якщо він зупинений, пропонує запустити його.

Для запуску засобу, що дозволяє налаштовувати параметри wmi на віддаленому та локальному комп'ютерах потрібно ввести у вікні виконати:

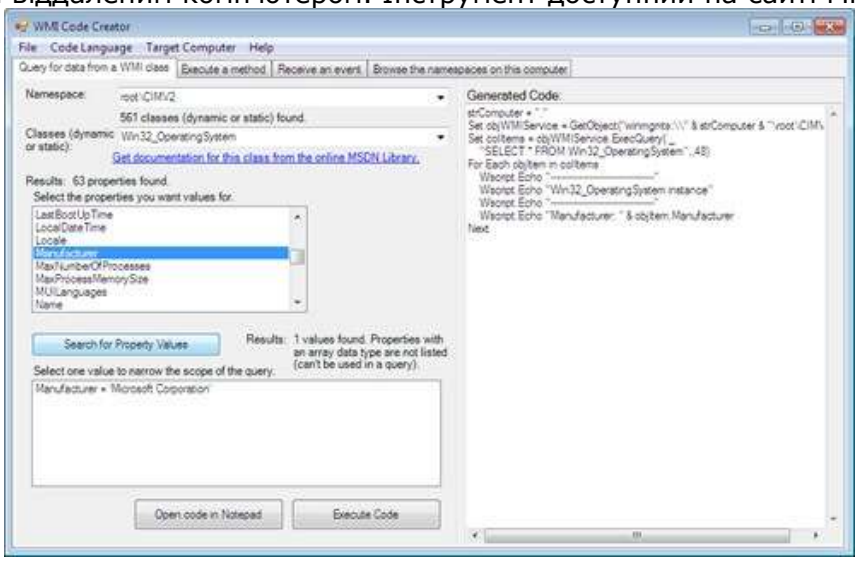
wmimgmt.msc

Використання спеціальних засобів для написання запитів

Для того, щоб полегшити написання скриптів і програм, існують спеціальні утиліти, які допомагають переглянути структуру простору WMI і показують приклади використання усіх класів. Найбільш поширені утиліти – це Scriptomatic і WMI Code Creator.



Програма WMI Code Creator являє собою генератор коду, який використовує WMI для отримання інформації та для здійснення завдань керування комп'ютерами. Програма може допомогти навчитися використовувати WMI – скрипти і WMI – додатки для керування як локальним, так і віддаленим комп'ютером. Інструмент доступний на сайті Microsoft.



WMI Code Creator – Query

Використовуючи WMI Code Creator можна знайти будь-яку інформацію про комп'ютер: ім'я і версія операційної системи, вільне місце на диску, стан сервісів і так далі. Можна виконати метод з WMI класу для здійснення керування комп'ютером: створити або видалити сервіс, запустити або закрити програми, призначити дозволи на папки або файли і багато іншого. Цей інструмент так само дозволяє переглядати доступний WMI-простір і WMI-класи, щоб знайти потрібну для програмування інстанцію з її описом, властивостями, методами і прикладом використання.

Отже, Windows Management Instrumentation – це потужний інструмент для адміністрування операційних систем сімейства Windows за допомогою скриптів. За

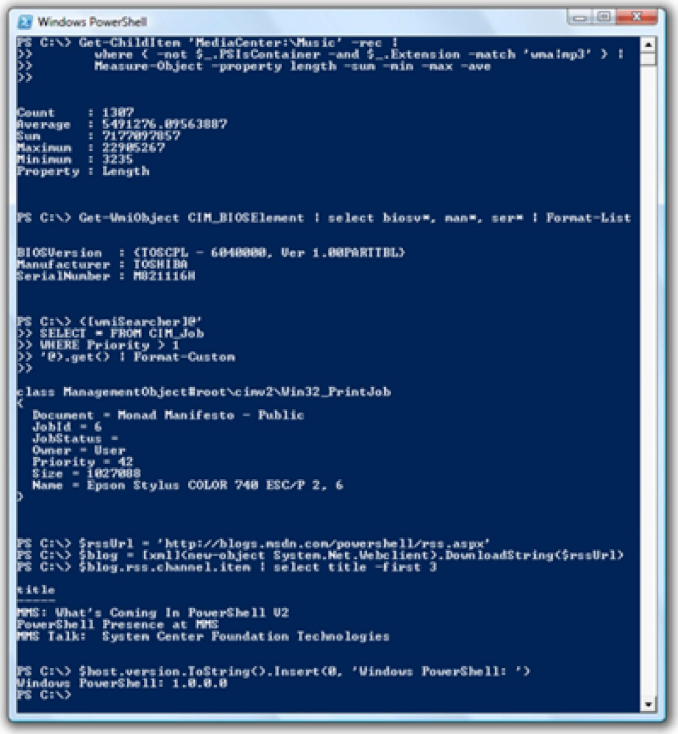
допомогою WMI можна керувати пристроями, обліковими записами, сервісами, процесами, мережевими інтерфейсами і іншими програмам, які розширюють базову структуру WMI своїми класами.

Крім скриптів WMI може застосовуватися і в повноцінних програмах, тобто програмісти можуть писати запити до WMI у виконавчий код, зав'язуючи свою програму з роботою WMI, завдяки чому програма стає простішою і легшою, але залежною від правильності роботи Windows Management Instrumentation.

4. Windows Power Shell та редактор реєстру

Windows PowerShell – розширювана оболонка з інтерфейсом командного рядка і супутньою мовою сценаріїв, розроблена Microsoft. Версія 1.0 випущена в 2006 році і зараз доступна для Windows XP SP2, Windows Server 2003, Windows Vista, і вбудована в Windows Server 2008 як опціональний компонент.

Windows PowerShell 2.0 був випущений в складі Windows 7, Windows 8 і Windows Server 2008 R2, Windows Server 2012 як невід'ємний компонент системи. Крім того, друга версія доступна і для інших систем, таких як Windows XP SP3, Windows Server 2003 SP2, Windows Vista SP1, Windows Vista SP2 і Windows Server 2008.



Сесія в Windows PowerShell

Windows PowerShell побудований на базі Microsoft. NET Framework і інтегрований з ним. Додатково PowerShell надає зручний доступ до COM, WMI і ADSI, так само як і дозволяє виконувати звичайні команди командного рядка, щоб створити єдине оточення, в якому адміністратори змогли б виконувати різні завдання на локальних і віддалених системах.

Ці адміністративні завдання зазвичай виконуються за допомогою командлетів [⇨] (в оригіналі cmdlets), які є спеціалізованими класами. NET. Користувач може комбінувати їх у скриптах (сценаріях), використовуючи різні конструкції, утиліти командного рядка і звернення до звичайних класах. NET, об'єктам WMI або COM.

Командлети (англ. cmdlets) – це спеціалізовані команди PowerShell, які реалізують різну функціональність. Це вбудовані в PowerShell команди. Командлети іменуються за правилом *Дієслово-Іменник*, наприклад Get-ChildItem, завдяки чому їх призначення зрозуміло з назви. Командлети виводять результати у вигляді об'єктів або їхніх колекцій.

PowerShell включає мову сценаріїв з динамічними типами, на якій можна реалізовувати складні операції з використанням командлетів. Мова сценаріїв підтримує змінні, функції, конструкції розгалуження (if-then-else) цикли (while, do, for і foreach), структуровану обробку помилок і безліч інших можливостей, включаючи інтеграцію з. NET. Змінні в PowerShell позначаються префіксом $ перед ім'ям; їм може бути присвоєно будь-яке значення, включаючи висновок командлетів.

Реєстр Windows (англ. Windows Registry), або системний реєстр –ієрархічно побудована база даних параметрів і налаштувань в більшості операційних систем сімейства Microsoft Windows.

Реєстр містить інформацію і налаштування для апаратного забезпечення, програмного забезпечення, профілів користувачів і т.д. Більшість змін в Панелі керування, асоціації файлів, системні політики, список встановленого ПО фіксуються в реєстрі.

Реєстр Windows був введений для впорядкування інформації, що зберігалася до цього в безлічі INI-файлів, забезпечення єдиного механізму (API) запису-читання налаштувань і позбавлення від проблем коротких імен, відсутності розмежування прав доступу і повільного доступу до ini-файлів, що зберігаються на файловій системі FAT16, що мала серйозні проблеми швидкодії при пошуку файлів в директоріях з великою їх кількістю. З часом (остаточно – з появою файлової системи NTFS) проблеми, які вирішувались реєстром, зникли, але реєстр залишився через зворотню сумісність, і присутній у всіх версіях Windows, включаючи останню. Оскільки зараз не існує реальних передумов для використання подібного механізму, Microsoft Windows – єдина (не рахуючи ReactOS) операційна система з використовуваних сьогодні, в якій використовується механізм реєстру операційної системи.

Сам реєстр як деревоподібна ієрархічна база даних (registration database - реєстраційна база) вперше з'явився в Windows 3.1 (квітень 1992). Це був всього один двійковий файл, який називався REG.DAT і зберігався в каталозі C: \ Windows \. Реєстр Windows 3.1 та мав тільки одну гілку HKEY_CLASSES_ROOT. Він служив для зв'язку DDE, а пізніше і OLE-об'єктів.

Далі технологія і ідеологія (призначення) реєстру вже не змінювалися. Усі наступні версії Windows (NT 3.5, 95, NT 4.0, 98, 2000, XP, Vista, 7,8) використовували реєстр як основну БД, що містить всі основні дані по конфігурації як самої ОС, так і прикладних програм. Далі мінялися назви файлів реєстру та їх розташування, а також назва і призначення ключів.

5. Керування операційною системо Windows за допомогою групових політик

Одним з найефективніших способів керування комп'ютерною мережею є використання групових політик. Групова політика дозволяє централізовано встановлювати єдині параметри для налаштування як операційної системи, так і прикладного програмного забезпечення.

Політика являє собою набір налаштувань і правил, які можуть бути застосовані до групи комп'ютерів (склад групи може регулюватися адміністратором).

За допомогою політики можна:

- автоматично встановити на комп'ютер програмне забезпечення;
- налаштувати права доступу до файлів і папок на дисках з файловою системою NTFS;
- лімітувати членство користувачів в групах безпеки (наприклад, жорстко фіксувати складу групи адміністраторів);
- змінити параметри реєстру, внести налаштування в режими запуску служб комп'ютера;
- встановити параметри використання прикладних програм і т. д.

Доменні групові політики, основні характеристики та застосування

Доменна групова політика являє собою найпростіший спосіб налаштування комп'ютера і параметрів користувачів в мережах на основі доменних служб Active Directory. Якщо ваша компанія не використовує групову політику, ви втрачаєте відмінну можливість

для зниження витрат, керування конфігураціями, підтримки продуктивності і зручності для користувачів, а також підвищення рівня безпеки. Групова політика дає можливість налаштувати численні параметри одночасно.

Вимоги, яких потрібно дотримуватися для використання доменної групової політики:

- Мережа повинна працювати на основі доменних служб Active Directory (тобто хоча б на одному сервері повинна бути встановлена роль доменних служб Active Directory).
- Комп'ютери, якими потрібно керувати, повинні бути приєднані до домену, а користувачі, якими потрібно керувати, повинні використовувати на своїх комп'ютерах для входу в систему облікові дані домену.
- Необхідно дозвіл для зміни групової політики в домені.

Параметри групової політики можна також налаштувати локально на кожному комп'ютері. Ця можливість добре підходить для одноразових сценаріїв або комп'ютерів робочої групи, але локальну групову політику не рекомендується використовувати в комерційних мережах на основі доменних служб Active Directory. Причина проста. Групова політика на основі домену централізує управління, що дозволяє працювати з безліччю комп'ютерів з одного місця. Локальна групова політика вимагає роботи з кожним комп'ютером окремо, що не є ідеальним сценарієм для великих середовищ.

Основні концепції групової політики

Всіма аспектами групової політики можна керувати за допомогою консолі керування груповими політиками. На рис. 1 показана консоль керування груповими політиками.

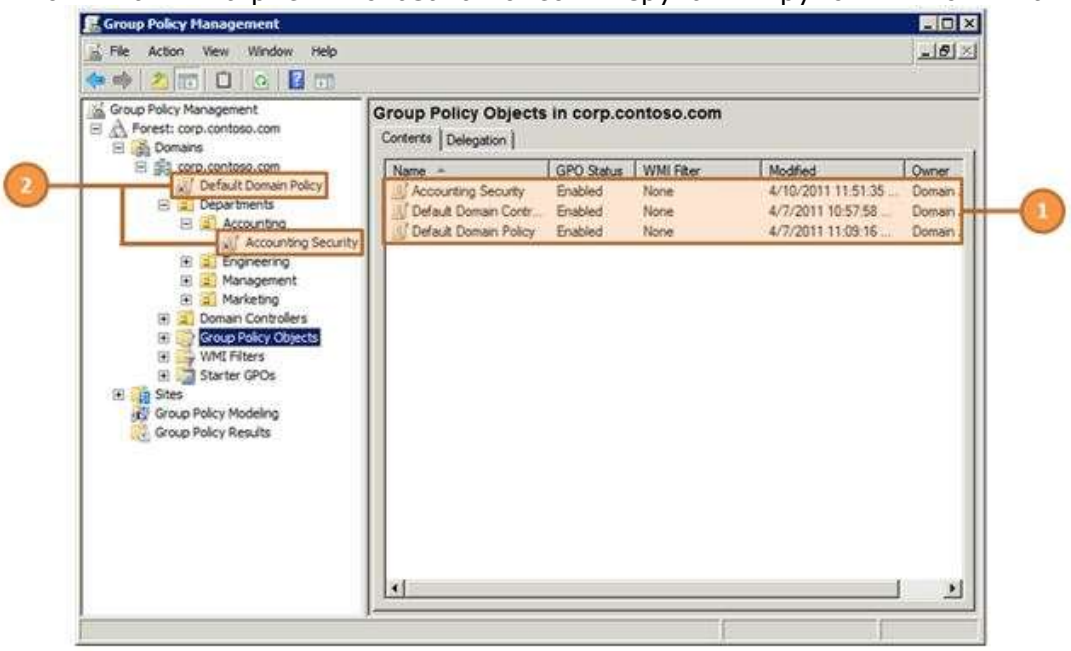


Рис.1. Консоль керування груповими політиками

Консоль управління груповими політиками запускається з меню «Пуск». Кліки: *Пуск, Усі програми, Адміністрування, Керування груповими політиками.*

Зв'язки групової політики

На верхньому рівні доменних служб Active Directory знаходяться сайти і домени. У простих випадках є один сайт і один домен. У домені можна створити підрозділи. Підрозділи схожі на папки в провіднику. Однак замість файлів і підпапок вони можуть містити комп'ютери, користувачів і інші об'єкти.

Спадковість групової політики

Як було зазначено в попередньому розділі, при зв'язуванні об'єкта групової політики з доменом цей об'єкт групової політики застосовується до всіх комп'ютерів і користувачам усіх підрозділів і дочірніх підрозділів домена. Подібним же чином при зв'язуванні об'єкта групової політики з підрозділом цей об'єкт групової політики застосовується до всіх комп'ютерів і користувачам всіх дочірніх підрозділів. Ця концепція називається спадковістю.

Оновлення групової політики

Як було сказано вище, об'єкти групової політики містять параметри комп'ютерів і користувачів. Групова політика застосовує їх таким чином:

- *параметри комп'ютера при запуску Windows.*
- *параметри користувача після входу користувача в систему.*

Групова політика також регулярно оновлює об'єкти групової політики, щоб забезпечити застосування нових і змінених об'єктів групової політики, не чекаючи перезавантаження комп'ютера або виходу користувача з системи. Проміжок часу між такими оновленнями називається **інтервалом оновлення групової політики**. За замовчуванням використовується значення **90 хвилин з невеликим фактором випадковості**, що дозволяє запобігти одночасному оновленню всіх комп'ютерів. Якщо змінити об'єкт групової політики в середині робочого дня, групова політика застосує ці зміни протягом приблизно 90 хвилин. Не треба чекати кінця робочого дня, коли користувачі вийдуть з системи або перезавантажать комп'ютери. У складніших сценаріях інтервал оновлення за замовчуванням можна змінити.

У будь-який момент можна оновити групову політику вручну за допомогою команди gpupdate.exe. Наприклад, після оновлення об'єкта групової політики може знадобитися оновити групову політику на комп'ютері, щоб протестувати зміни, не чекаючи інтервалу оновлення групової політики.

Об'єктами групової політики можна **керувати** за допомогою **консолі керування груповими політиками**, і їх можна правити за допомогою **редактора «Керування груповими політиками»**.

Контрольні запитання:

1. Дайте загальну характеристику групових політик сімейства Microsoft Windows.
2. Об'єкти та зв'язки групової політики.
3. Спадковість та оновлення групової політики.
4. Дайте характеристику служби DNS.
5. Формування простору імен DNS.
6. Служба Active Directory винекнення та загальна характеристика.
7. Дайте визначення основним термінам і поняттям Active Directory.
8. Active Directory логічна організація.
9. Active Directory фізична організація.
10. Active Directory – сучасний етап використання.
11. Характеристика протоколу DHCP.
12. Що таке інтерфейс Windows Management Instrumentation (WMI), дайте вичерпну характеристику.
13. Дайте характеристику консолі управління MMC.
14. ОболонкаWindows PowerShell, характеристики та параметри.
15. Що ви знаєте про редактор реєстру Windows?
16. Дайте характеристику способам та засобам адміністрування операційних систем сімейства Windows.

Лекція 6. Віртуалізація та віддалена робота в комп’ютерних системах

1. Віддалене керування комп’ютерною системою.

1.1. Види віддаленого керування.

Віддалене керування комп'ютером через Інтернет – це можливість використовувати комп'ютер з будь-якої точки світу так, як працювати безпосередньо за ним. Скрізь, де є Інтернет, з'являється можливість підключатися до офісного або домашнього комп'ютера і використовувати всі його можливості для вирішення різних завдань.

Застосування віддаленого керування

- **Для отримання доступу до офісного комп'ютера** або файл-серверу з дому, або з іншого офісу. Ви зможете користуватися повним набором програм на своєму робочому комп'ютері з будь-якого місця, мати доступ до своїх документів і вести офісну роботу навіть з кафе. Подібний тип віддаленого керування комп'ютером через Інтернет активно використовується бізнесменами, що часто мають відрядження. Просто не вимикайте офісний комп'ютер – і він буде «з вами» скрізь, де є вихід в Інтернет.
- **Для керування критичними комп'ютерами,** що працюють в складних мережах, наприклад, серверами. Віддалене керування комп'ютером через Інтернет дозволяє системному адміністратору постійно мати доступ до ресурсу, на збої в роботі якого повинна слідувати негайна реакція.
- **Для роботи з віддаленими комп'ютерами і мережами через віддалений робочий стіл.** Завдяки можливості керування через Інтернет, технічні фахівці мають можливість обслуговувати будь-які системи, що знаходяться в різних точках світу. Один системний адміністратор, наприклад, може налаштувати комп'ютери відразу в кількох містах: це дуже зручно для компаній, що мають велику мережу філій або складну інформаційну інфраструктуру.
- **Для проведення веб-семінарів або дистанційного навчання.** Можливість безпосередньо працювати на комп'ютері викладача або ж можливість викладача бачити всі дії учня і допомагати йому.
- За допомогою мобільного комп'ютера (ноутбука, нетбука, планшета IPad) з виходом в Інтернет можна **здійснювати віддалене керування домашнім комп'ютером,** перевіряти пошту, планувати завдання і користуватися документами та програмами.

Організація віддаленого керування

Практично всі сучасні операційні системи мають вбудовані функції керування віддаленим робочим столом. Проте, скористатися ними вдається далеко не завжди. Адже для того, щоб ці функції запрацювали, необхідно заздалегідь налаштувати комп'ютер. Не кожен користувач зможе це зробити самостійно. Крім того, в багатьох користувачів на це елементарно немає прав, а з системним адміністратором домовитися вдається не завжди.

Для організації віддаленого доступу та керування слід:

1. Встановити спеціальну програму на комп'ютер, який буде керованим. Ця програма дозволяє захистити дані, забезпечити

конфіденційність обміну інформацією, а також правильність і надійність авторизації. Керувати своїм комп'ютером може лише власник, а інформація буде надійно захищена.

2. Залишити керований комп'ютер включеним і під'єднаним до мережі для віддаленого керування комп'ютером. Це цілком нормальний стан для сервера, але психологічно незвичний для домашнього комп'ютера. Згодом, його можна вимкнути в любий час, використовуючи віддалене керування *(remote dekstop).*

3. Використати програму або мережний сервіс на комп'ютері, з якого буде здійснено доступ. Технічно можливим є під'єднання з Інтернет-клубу, з нетбука або з мобільного телефону.

Дистанційне керування

Режим «дистанційного керування» дозволяє віддаленим клієнтам керувати роботою сервера або робочої станції, включеної в локальну мережу. Робота в режимі «дистанційного керування» відповідає клієнт-серверній моделі «сервер терміналів».

Віддалений комп'ютер (віддалений хост) – сервер, фізично розміщений на деякій відстані від клієнта і доступ до якого (для клієнтів) можливий тільки через мережу.

Термінальний режим

З середини 1970-х до середини 1980-х років вся робота за комп'ютером виконувалася через спеціальні пристрої введення-виведення – термінали. З поширенням персональних ЕОМ термінальний доступ став використовуватися в основному для вирішення завдань віддаленого адміністрування.

Термінальний режим роботи – організація мережевої роботи інформаційної системи шляхом розміщення усіх користувацьких програм і даних на центральному сервері (серверах), доступ до яких відбувається з машин-терміналів виготовлених в спрощеному виконанні і, як наслідок, більш дешевих, які займають мінімум місця, безшумні і практично не вимагають обслуговування.

Термінал – кінцевий мережевий пристрій, підключений до обчислювальної системи і призначений для введення і виведення даних. Команди, які приймає з пристрою вводу терміналу (клавіатури), передаються на головний комп'ютер (сервер, віддалений хост), де і виконуються. Результати опрацювання повертаються і виводяться на дисплеї терміналу.

Фізичний або *реальний термінал* – як правило мається на увазі пристрій, обчислювальні можливості якого обмежені можливістю відображати те, що йому передано з мережі (як максимум – повноекранну графіку).

Віртуальний термінал – це програма, що виконує функції реального терміналу. З боку віддаленого хоста така програма, емулятор терміналу, нічим не відрізняється від реального терміналу.

Типи терміналів

Текстові термінали

Текстовий термінал – це пристрій (або програма) введення/ виведення, які працюють в дуплексному режимі і використовують символьно-орієнтовані протоколи передачі даних, такі як telnet (рис. 6.1).

Потоки даних між терміналом і сервером представляють ASCII-символи. Спеціальні символи (або послідовність символів) представляють команди керування сервером і відповіді сервера. Існують і службові команди, які керують виводом (переведення рядка, напівжирний/похилий текст, звуковий сигнал тощо) і сеансом зв'язку (узгодження версій протоколу тощо).

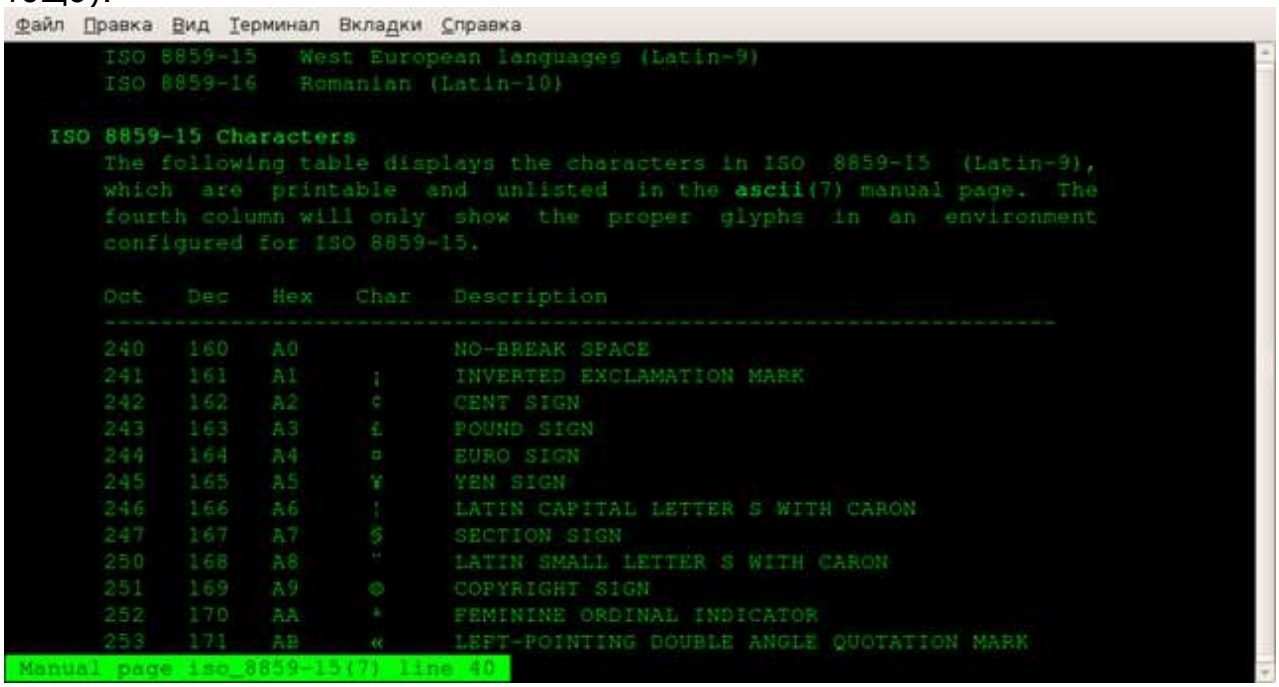


Рис. 6.1 – Вигляд текстового терміналу

Текстові термінали UNIX-подібних систем зазвичай підключаються до мейнфрейму або серверу через послідовний порт (RS-232C). Це дозволяє керувати фізично віддаленими серверами (наприклад, в Інтернеті), використовуючи повільні комутовані з'єднання.

Графічні можливості текстових терміналів обмежені спеціальними символами ASCII, які можуть бути використані для малювання рамок таблиць, стрілок, горизонтальних і вертикальних ліній, заливок різної щільності тощо. Використання VGA палітри дозволяє задавати колір фону і тексту. Але все це зводиться до псевдографіки, оскільки текстові термінали не керують виводом на рівні окремих пікселів.

Графічні термінали

Графічні термінали, на відміну від текстових, надають можливості роботи з повноколірною растровою і векторною графікою як при вводі даних, так і при їх відображенні. Графічні термінали застосовуються в системах, які підтримують графічний користувацький інтерфейс (GUI, Graphic User Interface).

Вимоги до пропускної здатності лінії зв'язку при використанні графічних терміналів, в загальному, значно більше в порівнянні з текстовими, оскільки передавати приходиться не коди символів, а, фактично, скріншоти. Для зиження навантаження на мережу використовуються різні способи: компресія, обмеження на глибину кольору і роздільної здатності екрану, передача лише областей, які змінилися тощо.

Текстовий режим роботи також підтримуються графічними терміналами, але реалізований інакше – всередині основного протоколу.

Рис. 6.2 – Вигляд графічного терміналу

Інтелектуальний термінал

Інтелектуальний термінал – під цим терміном вважають апаратно-програмний комплекс, комп'ютер, ресурсів якого достатньо не лише для виводу повноекранної графіки, але і для виконання деяких обчислень. Принциповою відмінністю інтелектуального терміналу від звичайного ПК є те, що виконуючі програми повинні завантажуватися з сервера (наприклад - *бездискова робоча станція).*

1.2. Протоколи віддаленого керування

Сервіс telnet

Служба віддаленого керування telnet (Teletype Network) – одна з найстаріших мережевих технологій Internet. Протокол telnet з початку розроблявся для використання в гетерогенних мережах. В його основі — концепція мережевого віртуального терміналу (Network Virtual Terminal, NVT) – механізму абстрагування від специфіки введення/виведення різних апаратних і програмних платформ. Так, в UNIX в якості символу переходу на інший рядок використовується LF (код 13), в той же час як в MS-DOS і Windows – пара символів CR-LF (коди 10 і 13). Мережевий віртуальний термінал NVT пропонує використання уніфікованого набору символів: telnet-клієнт відповідає за перетворення власних кодів в коди NVT, а сервер робить зворотне перетворення.

Протокол rlogin

Протокол rlogin (англ. *remote login* – віддалений вхід в систему, RFC 1282, порт сервера – 513) дозволяє користувачам робочих станцій UNIX підключатися до віддалених серверів UNIX через Internet і працювати так же, як при прямому підключенні терміналу до машини. Попри rlogin існує ще декілька подібних протоколів: rsh (remote shell), rcp

(remote copy). Утиліти rlogin, rsh и rcp часто об'єднують під загальною назвою r-команд.

SSH (Secure Shell)

SSH (англ. Secure SHell – безпечна оболонка) – безпечний протокол віддаленого керування комп'ютером і передачі файлів. Схожий за призначенням з протоколом telnet і rlogin, але використовує алгоритми шифрування передаваючої інформації. Основна специфікація – RFC 4251. The Secure Shell (SSH) Protocol Architecture

SSH представляє істотно більші можливості, ніж telnet, і дозволяє не лише використовувати захищену оболонку на віддаленому хості, але і тунелювати графічний інтерфейс – X11 forwarding (для ОС і програм, які використовують X-Window System). SSH також може (при вдалому налаштуванні) передавати через безпечний канал будь-який інший мережевий протокол – port forwarding. Криптографічний захист протоколу SSH не фіксований, можливий вибір різних алгоритмів шифрування.

Remote Desktop Protocol

RDP (англ. *Remote Desktop Protocol,* протокол віддаленого робочого столу) – відкритий протокол прикладного рівня, розроблений Microsoft і з самого початку призначений для підключення графічних терміналів до Windows Terminal Server. Клієнти існують практично для всіх версій Windows (включаючи Windows CE і Mobile), Linux, Free BSD, Mac OS X. Типово використовується порт TCP 3389. Офіційна назва Майкрософт для клієнтського ПЗ - Remote Desktop Connection або Terminal Services Client (TSC), зокрема, клієнт в Windows XP/2003/vista називається mstsc.exe.

RDP-клієнт, – Remote Desktop – дозволяє вам, перебуваючи на одному комп'ютері, віддалено керувати іншим.

Remote Desktop підтримує роботу в двох режимах:

- Remote Desktop (Віддалений робочий стіл) – підходить для використання в локальній мережі і вимагає встановлення програмного забезпечення на комп'ютері-клієнті.
- Remote Desktop Web Connection (Інтернет-підключення до віддаленого робочого столу) – потребує на клієнтській машині лише наявність браузера, але на сервері для неї необхідно встановити і налаштувати велику кількість програм.

Remote Desktop підтримує 24-бітні кольори – це дозволяє варіювати кількість картинки в широких межах.

Remote Desktop-сервер і Remote Desktop-клієнт користуються загальним буфером. Це дозволяє їм вільно обмінюватися інформацією.

1.3. Веб-технології віддаленого керування

VNC-системи (Virtual Network Computing)

VNC система – це система віддаленого доступу до іншого комп'ютера, що використовує протокол RFB (*Remote FrameBuffer).* Керування здійснюється шляхом ретрансляції вмісту екрану через комп'ютерну мережу.

Системи VNC є платформо незалежними: VNC-клієнт (VNC viewer), що запущений на одній операційній системі, може підключатися до VNC-сервера, що діє на іншій операційній системі. Реалізація клієнтської і серверної частини існує майже для всіх операційних систем.

До одного VNC-сервера синхронно можуть під'єднуватися кілька клієнтів. Найчастіше VNC системи використовують для технічної підтримки

і доступу з дому до комп'ютера на роботі.

Популярними VNC системами є TeamViewer, TightVNC, Logmein, CrossLoop, AMMYY Admin, ShowMyPC, Radmin та інші.

VPN (**Віртуальна приватна мережа**, англ. *Virtual Private Network*) – це логічна мережа, створена поверх інших мереж, на базі загальнодоступних або віртуальних каналів інших мереж (Інтернет). Безпека передавання пакетів через загальнодоступні мережі може реалізуватися за допомогою шифрування, внаслідок чого створюється закритий для сторонніх канал обміну інформацією. VPN дозволяє об'єднати, наприклад, декілька географічно віддалених мереж організації в єдину мережу з використанням для зв'язку між ними непідконтрольних каналів.

LogMeIn Hamachi – це хост-служба VPN, що дозволяє безпечно організовувати віртуальні ЛОМ для розподілених команд, мобільних співробітників і друзів з відеоігор - в лічені хвилини.

2. Системи віртуалізації

Термін віртуалізація останнім часом став дуже популярним. Віртуальні рішення в тій чи іншій мірі застосовуються в переважній більшості інформаційних систем. Фахівці використовують їх з метою тестування, для виконання додаткових завдань на існуючому обладнанні, для навчання і т. д. Віртуалізують сервери, робочі станції, системи зберігання, мережеву інфраструктуру.

Наприкінці 80-х майже всі думали, що IT-інфраструктура буде виглядати як досить малопотужні, легко замінні термінали і суперкомп'ютери, до яких ідуть підключення. Все повільно йшло до цього (і це було логічно), але в кінцевому підсумку перемогла парадигма зберігання даних на локальних вузлах. У чому чимала заслуга Microsoft, до речі. У довіртуальній інфраструктурі у кожного є системний блок і жорсткий диск всередині. Там обробляються дані, і тільки результати відправляються на сервер.

Економічні аспекти віртуалізації

Перш ніж приступати до впровадження віртуальних систем, слід ретельно продумати, що ми хочемо отримати в результаті і скільки це буде коштувати. Незважаючи на те, що практично в кожній презентації ми чуємо про економічну ефективність технології, на практиці впровадження віртуалізації супроводжується витратами, причому досить значними.

По-перше, віртуалізація вимагає наявності інфраструктури, наприклад, системи зберігання даних, підключеної до декількох серверів. По-друге, програмне забезпечення, що дозволяє використовувати переваги віртуальних середовищ: мігрувати віртуальні машини з одного фізичного сервера на інший в реальному режимі часу, балансувати навантаження на фізичних серверах, вимикаючи обладнання, яке не використовується і т. д., – є комерційним і порівняно недешевим продуктом.

У результаті економічний ефект переходу у віртуальні середовища досягається, починаючи з деякого числа серверів. Якщо вам і не потрібно відразу встановити 10 нових серверів, то купувати нове обладнання доведеться відразу і в розрахунку на розміщення всіх майбутніх систем.

Ефективність керування комплексом віртуальних машин в наших умовах рідко можна оцінити в цифрах, оскільки штатних змін серед IT-спеціалістів підприємства (наприклад, скорочення числа системних адміністраторів) після впроваджень рішень з віртуалізації не відбувається,

а витрати на електропостачання серверних кімнат підприємства зазвичай не враховуються окремим рядком.

У підсумку впровадження віртуалізації часто призводить тільки до додаткових витрат на утримання IT-інфраструктури.

Основні терміни

Гіпервізором (hypervisor) називають програмне забезпечення, що забезпечує віртуалізацію ресурсів і дозволяє декільком операційним системам працювати одночасно на одному фізичному пристрої, який прийнято називати *хост-системою* або просто хостом. Назва гіпервізор збереглася історично, більш зрозумілим міг би бути термін «менеджер віртуальних машин».

Операційну систему, що працює під керуванням гіпервізора, прийнято називати *гостьовою операційною системою*.

Жорсткі диски гостьових операційних систем є файлами на рівні гіпервізора. Їх прийнято називати віртуальними жорсткими дисками. Відповідно мережеві адаптери, пам'ять в гостьових системах називають віртуальними адаптерами, віртуальною пам'яттю і т. д.

На рівні гіпервізора можна створити різні віртуальні мережі: з підключенням до реального мережного адаптера в режимі моста, в режимі трансляції мережевих адрес, сегмент мережі без доступу до реального адаптера (внутрішня мережа) і т. д.

Комерційні рішення віртуалізації включають в себе віртуальні комутатори, які ви можете налаштувати на необхідні правила пересилання і фільтрації пакетів з однієї мережі в іншу.

Як правило, розробники гіпервізорів підготовлюють спеціальні пакети оновлень, що оптимізують роботу гостьових операційних систем. Наприклад, в гостьові ОС додаються мережеві адаптери, що працюють на швидкості внутрішньої шини гіпервізора. При цьому з'являється можливість обмінюватися даними між гостьовими ОС через буфер пам'яті, підключати папки хоста як мережевих папок в гостьові ОС і т. д. Таке ПЗ прийнято називати *розширеннями віртуальних машин* (virtual machine additions). Якщо немає спеціальних вимог, то для підвищення продуктивності систем розширення повинні бути встановлені в гостьовій ОС (зазвичай команди встановлення розширень присутні в меню вікна віртуальної машини).

VDI (Virtual Desktop Infrastructure, інфраструктура віртуальних робочих столів) – так називають ПЗ, що дозволяє керувати великою кількістю віртуальних робочих станцій (рис. 3.3).

Рис. 3.3 – Представлення інфраструктури VDI

Розробники віртуальних рішень

Існує декілька технологій віртуалізації, розроблених різними вендорами. Ми наведемо лише короткий список систем, які найбільш активно, використовуються на практиці.

Лідером ринку віртуалізації сьогодні є продукти компанії *VMware* (www.vmware.com). Рішення від VMware забезпечують віртуалізацію практично всієї лінійки операційних систем (Windows, Linux, Apple Macintosh і т. д.), ПЗ компанії тісно інтегровано з апаратними можливостями багатьох платформ, реалізовані технології відмовостійких рішень і т. д. Лінійка ПЗ представлена як вільно поширюваними, так і комерційними продуктами гіпервізор ESXi (рис. 3.4).

Рис. 3.4 – Логотип компанії VMware

XEN (www.xensource.com, www.virtualiron.com, http://www.xen.org/) багатоплатформовий гіпервізор, розроблений в комп'ютерній лабораторії Кембриджського університету і поширюваний на умовах ліцензії GPL (рис. 3.5).

Рис. 3.4 – Логотип гіпервізора Xen

На базі цього гіпервізора компанією Citrix створені сервери XenServer, які також є безкоштовними рішеннями. Правда, ПЗ централізованого керування серверами XenServer є комерційним продуктом.

Компанією Sun (нині Oracle) випущена віртуальна машина *VirtualBox*. Це рішення безкоштовне і може бути завантажене з сайту Oracle. У компанії Oracle є і рішення VDI – Oracle Virtual Desktop Infrastructure (VDI), причому у варіанті до 10 віртуальних робочих столів воно може безкоштовно тестуватися напротязі необмеженого часу.

У складі серверних операційних систем починаючи з Windows 2008 присутній гіпервізор – *HyperV*, який може бути завантажений з сайту Microsoft і в якості окремого продукту і може бути використаний повністю безкоштовно.

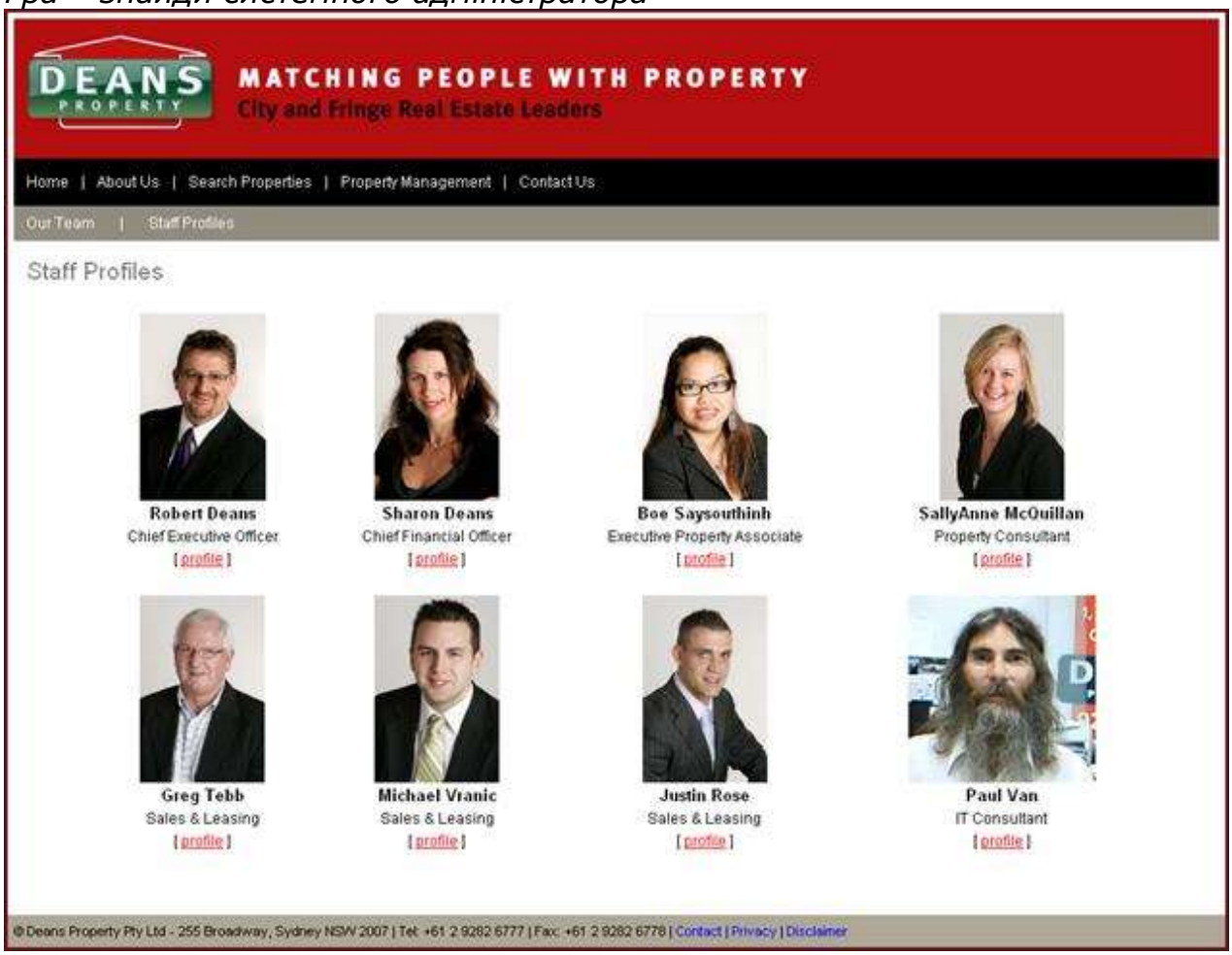
Рис. 3.4 – Логотип гіпервізора Microsooft Hyper-V

Продукти відкритого коду останнім часом активно починають використовувати рішення з віртуалізації з назвою *KVM* (Kernel-based Virtual Machine) (наприклад, цей гіпервізор включений до складу Ubuntu, RedHat і т. д.). Гіпервізор KVM реалізує віртуалізацію на Linux-системах і доступний як у складі відповідних дистрибутивів, так і через пакети установки.

Довідкова інформація

Енікейщік – від «Press any key to continue». Як правило – людина, яка знає трохи більше, ніж вище середнього. Але може бути і фахівець, який робить просту (на його погляд) роботу з підтримки комп'ютерного парку в порядку. Може вживатися з іронією та самоіронією (вважається помічником сисадміна).

Гра – знайди системного адміністратора



Шаманський бубен – ударний музичний інструмент. Вважається, поряд із заячою лапкою, необхідним атрибутом адміна. Через те, що дії, виконувані адміном при налаштуванні софта і заліза, досить неочевидні

(часто навіть для нього самого), адмінських робота багато в чому схожа з шаманством. Отже, корисно мати і шаманські пристосування – для повернення сервера з царства смерті, вигнання злого духа з бази і т. д.

Були згадки про те, що в день сисадміна продавців дуже дивував вибух попиту на різні бубни.

Бубен в роботі

Контрольні запитання:

1. Назвіть основні причини застосування віддаленого керування комп'ютерною системою.
2. Які кроки необхідно виконати для організації віддаленого доступу та керування?
3. Охарактеризуйте основні типи терміналів, що використовуються для віддаленого керування комп'ютерною системою.
4. Протоколи, системи та технології віддаленого керування.
5. Основні терміни систем віртуалізації.
6. Призначення та характеристика систем віртуалізації.
7. Яких Ви знаєте розробників рішень для систем віртуалізації?

Лекція 7. Моніторинг та визначення несправностей комп'ютерної системи

1. Моніторинг комп'ютерної системи

Щоб працювати не тільки за фактами інцидентів, а попереджати можливі відмови системний адміністратор істотну частину свого робочого часу повинен витрачати на оцінку стану обладнання та програмних забезпечення, переглядання протоколів роботи різних служб і т. д.

Аналіз одержаної інформації зазвичай потребує високої кваліфікації, будучи при цьому вельми рутинною операцією. Навіть якщо адміністратор і не нехтує цією частиною своїх повсякденних обов'язків, тим не менше, всі ці зусилля не можуть гарантувати контроль функціонування компонентів в реальному часі.

Тому наявність тієї чи іншої системи моніторингу системи є вимогою до сучасної інформаційної системи.

Основні способи контролю комп'ютерної системи

Для моніторингу системи традиційно використовують:

- аналіз повідомлень в журналах системи;
- SNMP-протокол (для контролю активного обладнання);
- імітація запитів до системи (наприклад, тестовий запит до бази даних);
- спеціальні агенти, які додатково встановлені в систему (для розширеного моніторингу).

Nagios

Nagios є програмою моніторингу інформаційних систем на основі відкритого коду (рис. 7.1). Продукт є практично стандартом для систем моніторингу.

Вона дозволяє:

- контролювати хости (завантаження процесора, використання диска, журнали і т. д.) з різноманітними операційними системами – Windows, Linux, AIX, Solaris і т. д.;
- контролювати мережеві служби (SMTP, POP3, HTTP, SSH і т. д.);
- підключати додаткові модулі розширення (плагіни) написані різними мовами програмування (Shell, C++, Perl, Python, PHP, C# та ін. – архітектура модулів повинна бути відкрита), використовувати власні способи перевірки служб;
- здійснювати паралельних перевірку систем (для підвищення продуктивності);
- відправляти оповіщення у разі виникнення проблем за допомогою електронної пошти, повідомлень SMS і т. д.;
- автоматично реагувати на події служби або хоста.

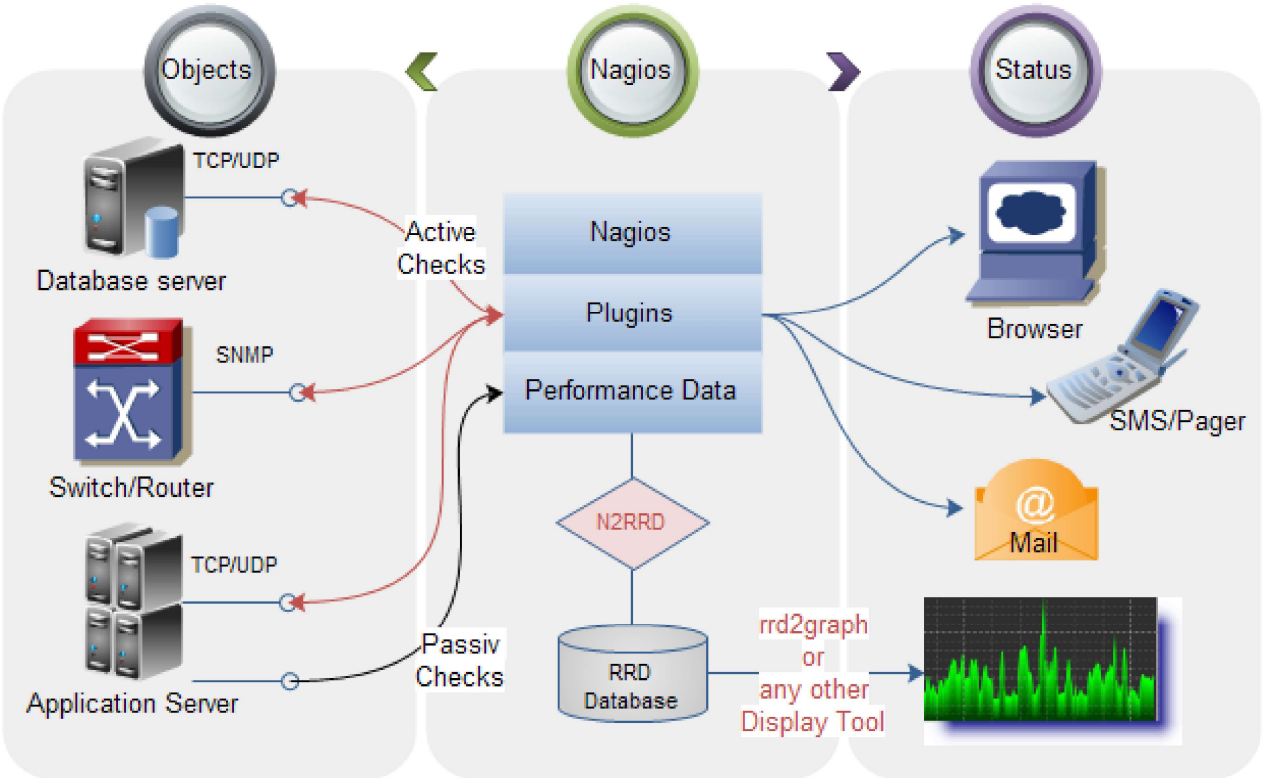


Рис. 7.1 – представлення інтерфейсу Nagios

ZABBIX

ZABBIX – вільна система моніторингу та відстеження статусів різноманітних сервісів комп'ютерної мережі, серверів та мережевого обладнання, написана Олексієм Владишевим (Литва). Для зберігання даних використовується MySQL, PostgreSQL, SQLite або Oracle (рис. 7.2).

Веб-інтерфейс написаний на PHP. ZABBIX підтримує кілька видів моніторингу:

Simple checks – може перевіряти доступність і реакцію стандартних сервісів, таких як SMTP або HTTP без установки будь-якого програмного забезпечення на хості за яким спостерігають.

ZABBIX agent – може бути встановлений на UNIX-подібних або Windows хостах для отримання даних про навантаження процесора, використання мережі, дискового простору і т. д.

External check – виконання зовнішніх програм. ZABBIX також підтримує моніторинг через SNMP.

Рис. 7.2 – представлення інтерфейсу Zabbix

Ganglia

Ganglia – масштабована розприділена система моніторингу кластерів паралельних і розподілених обчислень та хмарних систем з ієрархічною структурою (рис. 7.3). Дозволяє відстежувати статистику та історію (завантаженість процесорів, мережі) обчислень в реальному часі для кожного з спостережуваних вузлів.

Проект створений в 1998 році в Каліфорнійському університеті в Берклі як продовження проекту Millennium, який був ініційований Національним науковим фондом США.

Рис. 7.3 – представлення інтерфейсу Ganglia

2. Визначення несправностей та порядок налаштування комп'ютерної системи

Відмови інформаційної системи все більшою мірою впливають на ефективність бізнес-процесів підприємства, тому одне з головних завдань адміністратора працюючої системи полягає в попередженні відмов і максимальному скороченні часу простою обслуговування.

Перш ніж почати ...

Якщо відмова все ж сталася, не поспішайте відразу ж починати щось робити.

Спробуйте заспокоїтися, можна випити кави і тільки після цього приступати до активної діяльності.

Насамперед, спробуйте отримати про несправність максимум інформації як від користувачів, так і за даними об'єктивного контролю.

Спробуйте конкретизувати проблему. Після цього слід скласти попередній перелік можливих причин відмови з оцінкою часу усунення по кожній позиції. Намагайтеся не починати ремонт з найбільш витратних позицій, якщо тільки ви абсолютно не впевнені, що саме вони стали причиною несправності.

Виконайте операції, які ви запланували для ліквідації відмови. Перевірте результат. Якщо Ви не досягли успіху, то доведеться повторити кроки: висловити нові припущення про причини, скласти новий план дій і т. д.

Не намагайтеся вносити відразу багато змін в налаштування. Протоколюється всі свої кроки. Часто, якщо систему не вдається відновити за короткий час, без таких записів дуже складно не заплутатися і повернутися до вихідної точки.

Якщо ви довго не можете впоратися з відмовою, спробуйте розповісти про несправності кому-небудь ще. По-перше, намагаючись пояснити проблему, ви розкладете її для себе «по поличках». По-друге, *поради неспеціалістів* часто можуть направити вас на несподіваний шлях вирішення.

Обов'язково складіть який-небудь документ за результатами інциденту, щоб фахівцю, який прийде на ваше місце, було легше орієнтуватися в стані системи.

П'ять дев'яток?

Мета, яку ставлять виробники устаткування і розробники програмного забезпечення, – досягти доступності інформаційної системи на «п'ять дев'яток» – 99,999%. При цілодобовій роботі цей показник відповідає приблизно п'яти хвилинам простою за рік.

Звичайно, досягнення такого показника вимагає дуже істотних витрат як на відповідне обладнання, так і на обслуговування, нереальних для малих і середніх організацій. У той же час в силах системного адміністратора як налагодити роботу з попередження відмов, так і створити умови для оперативного відновлення інформації. *Адміністратор повинен бути готовий до виникнення будь-якої нештатної ситуації і мати певний план дій* – план забезпечення неперервності функціонування інформаційної системи.

Подібний план являє собою перелік заходів, які необхідно здійснити в разі відмови обладнання або в іншій нештатній ситуації. У ньому має бути визначено, наприклад, на яке обладнання перенести сервери в разі його відмови? Де повинні зберігатися дистрибутиви, щоб відновлення могло бути проведено черговим оператором? Яка повинна бути процедура відновлення даних? Описавши всі передбачувані аварійні ситуації та шляхи їх усунення, ви зможете розрахувати очікуваний час відновлення системи у кожному випадку відмови.

Саме при складанні плану забезпечення безперервної роботи можна оцінити вартість відновлення системи при різних відмовах і для деяких випадків *спочатку відмовитися від можливості оперативного відновлення*. *Досить співвіднести витрати на підтримку відмовостійкості з потенційними втратами від відмови в обслуговуванні і прийняти зважене рішення.*

Якщо такий план буде затверджений керівництвом, то, з одного боку, ви отримаєте захист від невиправданих вимог негайного відновлення роботи, оскільки для кожної ситуації досяжні тимчасові рамки будуть чітко обумовлені. З іншого боку, цей план стане інструкцією, що потрібно робити в аварійній ситуації.

Будьте готові до гіршого

Продумуючи заходи щодо забезпечення безперервної роботи інформаційної системи, слід враховувати всі можливості: *в реальному житті відбуваються найнесподіваніші відмови і необхідно зустрічати їх підготовленими*.

Будьте готові, що незалежно від прийнятих заходів захисту ваша система або може бути зламана, або виникне інша ситуація з повною втратою даних.

І практично єдине, що може допомогти, – це *підготовленість до відновлення даних «з нуля»*, наявність і регулярне створення резервних копій інформації.

Отримати копію даних, достатню для повного відновлення сервера, можна різними способами. Починаючи від звичайних операцій копіювання на змінний носій і закінчуючи комерційними системами підтримки актуальної копії даних в реальному режимі часу. Все залежить від вимог, що пред'являються до інформаційної системи. Скільки даних може бути втрачено, за який період часу система повинна бути відновлена «з нуля» і т. д.

Головне, що потрібно запам'ятати, – *резервна копія, резервна копія і ще раз резервна копія*!

Запасні деталі

Будь-яка інформаційна система потребує ЗІП – запасних інструментів і приладів. В ідеалі склад ЗІП повинен розраховуватися при створенні системи, але зазвичай для цього не вистачає показників надійності і *ЗІП складається у відсотках від обсягу (наприклад, 10% – цифра залежить від практики, прийнятої на конкретному підприємстві), але не менше одного елемента кожного типу*.

Слід врахувати, що запасні деталі до обладнання, що знаходиться на експлуатації більше 3-х років, придбати стає вельми складно. Часто для цього необхідна наявність сервісних контрактів, вартість яких за 3-5 років вже починає перевищувати вартість вихідного обладнання.

Тому при придбанні обладнання потрібно одночасно купувати запасні жорсткі диски, блоки живлення, сполучні кабелі і т. д. Не кажучи вже про те, що у системного адміністратора повинен бути запас таких компонентів, що найчастіше виходять із ладу, як клавіатури, миші, пасивне обладнання.

Збір інформації про відмову

Для успіху відновлення велике значення має якість зібраної інформації про відмову. Спочатку перевірте здається очевидні факти: чи включено обладнання, чи горять індикатори стану, чи не з'явилися додаткові шуми і т. д.

Потім систематизуйте інформацію про систему:

- публічні журнали (журнал подій Windows, syslog для unix-систем, журнали додатків);
- уточніть час виникнення проблеми, які операції виконувалися в цей момент;
- з'ясуйте, чи проводилися зміни в налаштуваннях системи перед виникненням проблеми, чи змінювалося обладнання і т. д.;
- проаналізуйте ситуацію: чи зустрічалися спостережувані симптоми раніше, чи були подібні відмови, які могли призвести до поточної проблеми і т.д.;
- якщо помилка спостерігається у користувача, переговоріть з ним, уточніть ситуацію, спробуйте відтворити проблему.

Контрольні запитання:

1. Назвіть завдання моніторингу комп’ютерної системи.
2. Які Ви знаєте способи моніторингу та контролю комп’ютерної системи.
3. Програмні засоби моніторингу інформаційних систем.
4. Які основні кроки потрібно здійснити для виявлення несправностей комп’ютерної системи.
5. Порядок налаштування комп’ютерної системи.

Лекція 8. Планові операції обслуговування комп'ютерної системи

1. Планові операції обслуговування

Обов'язок контролю функціонування інформаційної системи тягне за собою виконання ряду рутинних операцій. Їх склад специфічний для кожного підприємства. Однак я спробую навести зразковий шаблон, на основі якого може бути складений конкретний план періодичних заходів. Зручно, якщо цей план буде виконаний у вигляді відповідного переліку, виконання кожного пункту якого відзначатиметься в цьому ж документі.

Звичайно, обсяг операцій повинен бути скоректований з урахуванням розміру організації, наявності та обсягу моніторингу і т. д.

Щоденні операції

Щоденні операції спрямовані, в першу чергу, на контроль поточного стану інформаційної системи. Кожна позиція даного шаблону повинна бути доповнена конкретними операціями перевірки. Можна назвати наступні операції перевірки.

- *Оцінка зовнішнього стану серверів і навколишнього середовища*. Адміністратору необхідно оцінити температуру навколо серверів, перевірити відсутність зовнішніх ознак пошкодження корпусів, стан кабельної системи і т. д.
- *Перевірка функціонування основних служб інформаційної системи*. Адміністратор зобов'язаний перевірити стан всіх основних служб системи: працездатність каналу Інтернету, можливість прийому і відправки повідомлень електронної пошти, відгуки від інформаційного серверу підприємства і т. д. Обсяг подібних операцій залежить від складу інформаційної системи.
- *Оцінка показань датчиків апаратного контролю*. Серверні платформи оснащені датчиками, що дозволяють контролювати температурний режим всередині корпусу, параметри електроживлення, частоту обертання вентиляторів, стан RAID-контролерів. Адміністратору необхідно переконатися, що відповідні свідчення знаходяться в допустимих діапазонах.
- *Перевірка результатів виконання операцій резервного копіювання*. Слід переконатися, що всі операції резервного копіювання завершилися успішно і без будь-яких повідомлень про помилки. Особливо хочеться звернути увагу, що контролю підлягають усі операції резервного копіювання: виконувані як системними засобами, так і внутрішніми операціями прикладного програмного забезпечення.
- *Перевірка результатів оновлення антивірусних баз.* Необхідно переконатися, що всі працюючі комп'ютери (сервери і робочі станції) мають останню версію вірусних баз локального сервера, а цей сервер, у свою чергу, успішно оновлений з мережі.
- *Перевірка результатів інших планових операцій в системі*. В інформаційній системі можуть існувати інші операції, що виконуються за спеціальними графіками. Наприклад, заходи щодо оптимізації баз даних SQL-сервера, формування звітів статистики використання інтернету і т. д. Адміністратору слід перевірити підсумки виконання таких операцій.
- *Перевірка вмісту протоколів роботи серверів*. Адміністратор повинен переглянути та проаналізувати протоколи роботи всіх серверів інформаційної системи, в першу чергу звертаючи увагу на протоколи системи безпеки і на повідомлення про помилки або попередження. Слід

зазначити, що і чисто інформаційні повідомлення можуть допомогти досвідченому адміністратору у попередженні аварії.

- *Перевірка доступного обсягу жорстких дисків*. Необхідно перевірити наявність на основних виробничих серверах достатнього вільного об'єму дискового простору, який дозволить продовжити нормальне виконання бізнес-операцій. Ця вимога відноситься до тих серверів, обсяг інформації на яких може змінюватися. Наприклад, поштовий сервер (прийом великої кількості повідомлень), файловий сервер (користувачі перенесли на нього істотний обсяг даних), сервер баз даних (розробники змінили структуру інформації, внаслідок чого розмір баз істотно виріс) і т. д. Природно, що для серверів, які виконують такі функції, як маршрутизація мереж і т. д., даний контроль не актуальний.
- *Перевірка роботи служб систем*. Адміністратор повинен перевірити, що все автоматично запускаються служби всіх серверів інформаційної системи перебувають у стані «працює».

Звичайно, існують служби, які автоматично запускаються і згодом зупиняються. Але я на цьому не будемо загострювати увагу.

Щотижневі операції

У наступній групі щотижневих операцій представлені завдання, які адміністратор повинен виконувати кілька разів на місяць. Конкретна періодичність – раз на тиждень або раз на два тижні – повинна бути визначена в залежності від специфіки інформаційної системи.

- *Формування звіту*. Хоча це чисто організаційне пропозиція, наявність періодичного звіту системного адміністратора, з одного боку, стимулює самого адміністратора, з іншого – дозволяє тримати керівника в курсі стану інформаційної системи.
- *Очищення фільтрів вентиляторів охолодження*. Практика показує, що в умовах звичайної установи повітряні фільтри «забиваються» вже через один-два тижні. У зв'язку з цим слід щотижня очищати фільтруючі елементи як всього приміщення, так і на корпусах обладнання (звичайно, якщо відповідні фільтри передбачені).
- *Перевірка продуктивності серверів*. Адміністратору необхідно перевірити параметри продуктивності серверів системи і проаналізувати їх зміни в порівнянні з минулими періодами. У разі зниження параметрів – вжити заходів з підтримки необхідного рівня обслуговування користувачів.

Планові операції другої періодичності

Адміністратору не слід забувати і про ті роботи, виконувати які йому доводиться досить рідко. Наступні роботи можна запланувати, наприклад, в квартальному або піврічному планах.

- *Встановлення оновлень.* Адміністратор повинен періодично перевірити наявність оновлень для всього програмного забезпечення, яке використовується в організації. Навіть якщо в організації реалізована система поточного оновлення безпеки, необхідно переконатися у відсутності оновлень, які не охоплюються нею.
- *Видалення застарілих об'єктів служби каталогів.* Часто створення і видалення облікових записів користувачів відстає від фактичного кадрового складу підприємства, склад комп'ютерів, перелічених у службі каталогів, не відповідає реальності. Має сенс періодично видаляти застарілі об'єкти зі служби каталогів, хоча б на основі часу, що пройшов з моменту останнього входу відповідного облікового запису в домен.

- *Очищення обладнання від пилу.* Зазвичай дану операцію поєднують з проведенням на обладнанні тих чи інших робіт, оскільки при цьому зазвичай передбачається відключення електроживлення. Періодичність робіт визначається якістю навколишнього середовища, і при відсутності спеціальних заходів щодо фільтрації повітря дана операція повинна виконуватися не рідше одного разу в три-п'ять місяців.
- *Тренування повного відновлення системи.* Вкрай важливо, щоб фахівець міг оперативно виконати комплекс робіт з повного відновлення інформаційної системи після аварійної ситуації. Тому в організації повинні бути заплановані роботи з відновлення тестової системи на основі тих резервних копій, які створюються в плановому порядку.
- *Коригування керівної документації*. Доцільно раз на рік упорядковувати документацію: актуалізувати схеми мереж, відображати виконані ремонти і т. д. Слід переглянути керівні документи організації, що стосуються IT-технологій, внести в них необхідні зміни, які враховують стан справ, затвердити і опублікувати на внутрішніх ресурсах для ознайомлення користувачів.
- *Планування розвитку.* За підсумками завантаженості інформаційної системи за деякий період адміністратор може припустити про додаткові ресурси, які можуть знадобитися для подальшого нормального функціонування системи (наприклад, придбання додаткового жорсткого диска). Відповідні пропозиції повинні бути передані керівнику.

План-звіт операцій

На основі наведеного в попередньому пункті плану заходів слід скласти список конкретних, поточних операцій адміністратора. При цьому кожна позиція має бути пооперaційно розгорнута у відповідності зі специфікою інформаційної системи.

Заповнений адміністратором звіт буде документом, за яким можна оцінити як роботу фахівця, так і об'єктивно проаналізувати стан системи.

Облік комп'ютерів і програм

Автоматична інвентаризація програмного забезпечення і устаткування для функціонуючих систем не представляє великої складності. Сучасні операційні системи дозволяють зібрати такі дані різними способами (через об'єкти операційної системи, через командний інтерпретатор спеціального призначення WMIC (Windows Management Instrumentation Command-line).

Дані про параметри обладнання та програмного забезпечення легко зібрати централізовано при наявності прав доступу до відповідного комп'ютера. В домені з цією метою зазвичай використовуються облікові записи, включені в групу адміністраторів домену. У робочій групі доведеться вказувати параметри облікових записів кожної системи.

Сніффери

Хоча адміністраторові і не потрібно розбиратися в тонкощах мережевих протоколів, але він повинен вміти на базовому рівні використовувати той чи інший варіант програми мережного аналізатора (сніффер). Сніффер (sniffer) може бути використаний для оцінки основних параметрів функціонування мережі: відсотка використання смуги пропускання, оцінки використовуваних протоколів, кількості пакетів з помилками і т. д. Крім того, сніффер дозволяє виявити відхилення в роботі пристроїв: надмірна кількість пакетів того чи іншого

типу, що може бути ознакою зараження якої-небудь системи вірусом або підготовки атаки.

2. Автоматизація встановлення програмного забезпечення

Системному адміністраторові постійно доводиться вводити в експлуатацію нові робочі місця, а так само модернізувати існуючі. Адміністратору зазвичай необхідно або повністю підготувати комп'ютер (починаючи від установки операційної системи і закінчуючи прикладними програмами і всіма оновленнями), або тільки встановити прикладні програми (якщо комп'ютер поставлений з OEM-версією Windows).

У першому випадку потрібно використовувати або варіанти розгортання операційних систем, або операції з дублювання. У разі тільки установки прикладного програмного забезпечення на нову систему можна скористатися засобами групового керування (сценаріями входу в систему або груповими політиками) для розповсюдження програмного забезпечення. Але при цьому інсталяційні пакети повинні бути спеціально підготовлені: в них повинні бути включені налаштування, прийняті для даної організації, і виключені запити до користувача (для повної автоматизації процесу).

Клонування систем

Найшвидший спосіб підготувати нову систему до експлуатації – зробити її копією вже існуючої, тобто клонувати. Клонування являє собою процес відтворення даної системи на іншому робочому місці. Клонована станція матиме аналогічну версію операційної системи, ті ж встановлені (і відповідним чином налаштовані) прикладні програми користувачів і т. д.

До клонування вдаються при оновленні апаратної частини робочого місця (новий системний блок), при створенні нових робочих місць і т. д.

Існують різні способи клонування. Новий образ можна скопіювати на жорсткий диск, завантажившись зі змінного носія і перенісши дані зі змінного пристрою або по мережі з сервера, якщо забезпечити віддалене завантаження нової робочої станції. Перший варіант більш простий в налаштуванні і використанні, другий – більш гнучкий, оскільки на сервері можна зберігати образи для різних варіантів установки.

Адміністратор вибирає той варіант, який оптимальним чином підходить для його системи.

Підводні камені процесу клонування

При уявній простоті операції дублювання системного адміністратора чекає багато проблем.

Перша група труднощів пов'язана з можливим розходженням обладнання на старій і новій системі. Для нової платформи можуть знадобитися нові драйвери і система не зможе працювати з програмним забезпеченням тих пристроїв, на які була налаштована вихідна система.

Підготовка програм для тихого встановлення

При установці прикладних програм часто доводиться вводити багато відповідей, вказуючи шлях установки, склад обраних функцій і т. д. Необхідність таких операцій, з одного боку, знижує швидкість встановлення програмного забезпечення, з іншого – ускладнює виконання операцій встановлення в автоматичному режимі.

Контрольні запитання:

1. Які Ви знаєте планові операції обслуговування комп’ютерної системи?
2. Щоденні операції обслуговування комп’ютерної системи.
3. Щотижневі операції обслуговування комп’ютерної системи.
4. Планові операції обслуговування комп’ютерної системи другої періодичності.
5. Розкажіть про автоматизацію встановлення програмного забезпечення.