МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»

ОСНОВИ ТЕОРІЇ ТЕЛЕКОМУНІКАЦІЙ І РАДІОТЕХНІКИ. Частина 2

Лабораторний практикум

Навчальний посібник

Рекомендовано Методичною радою КПІ ім. Ігоря Сікорського
як навчальний посібник для здобувачів ступеня бакалавра за освітньою програмою
«Інформаційно–обчислювальні засоби радіоелектронних систем»
спеціальності 172 «Телекомунікації та радіотехніка»

Укладач: П. В. Кучернюк

Електронне мережне навчальне видання

Київ
КПІ ім. Ігоря Сікорського
2022

Рецензент: Ільяшенко А.М., директор центру телекомунікацій «КПІ–ТЕЛЕКОМ» КПІ ім. Ігоря Сікорського

Відповідальний редактор Корнєв В.П., канд. техн. наук, доц., КПІ ім. Ігоря Сікорського

Гриф надано Методичною радою КПІ ім. Ігоря Сікорського
(протокол № 6 від 24.06.2022 р.)
за поданням Вченої ради Факультету електроніки
(протокол № 5/22 від 31.05.2022 р.)

Навчальний посібник містить матеріали, які використовуються для підготовки до лабораторних робіт з освітнього компонента «Основи теорії телекомунікацій і радіотехніки. Частина 2», їх виконання та захисту. Лабораторний практикум включає шість лабораторних робіт: «ОСНОВНІ КОМАНДИ ДЛЯ РОБОТИ З МЕРЕЖНИМИ РЕСУРСАМИ В КОМАНДНОМУ РЯДКУ», «АНАЛІЗ СИСТЕМИ ЗА ДОПОМОГОЮ МОНІТОРУ ПРОДУКТИВНОСТІ», «ОСОБЛИВОСТІ АДМІНІСТРУВАННЯ КОНТРОЛЕРА ДОМЕНУ WINDOWS 20xx», «НАЛАШТУВАННЯ ТА ВИКОРИСТАННЯ СИСТЕМИ ДОМЕННИХ ІМЕН – DNS», «НАЛАШТУВАННЯ ТА ВИКОРИСТАННЯ МЕРЕЖНОГО СЕРВІСУ DHCP», «НАЛАШТУВАННЯ ТА АДМІНІСТРУВАННЯ IIS (Internet Information Services)». Навчальний посібник призначений для здобувачів першого (бакалаврського) рівня вищої освіти спеціальності 172 «Телекомунікації та радіотехніка», які навчаються за освітньо–професійною програмою «Інформаційно–обчислювальні засоби радіоелектронних систем».

Реєстр. № НП 21/22–847. Обсяг 5,2 авт. арк.

Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
проспект Перемоги, 37, м. Київ, 03056
https://kpi.ua
Свідоцтво про внесення до Державного реєстру видавців, виготовлювачів
і розповсюджувачів видавничої продукції ДК № 5354 від 25.05.2017 р.

ЗМІСТ

ВСТУП

Відповідно до положення про організацію навчального процесу в КПІ ім. Ігоря Сікорського, ***лабораторне заняття*** – вид навчального заняття, на якому студент під керівництвом науково–педагогічного працівника проводить натурні або імітаційні експерименти чи дослідження з метою практичного підтвердження окремих теоретичних положень, набуває практичного досвіду роботи з лабораторним обладнанням, оснащенням, обчислювальною технікою, вимірювальною апаратурою, оволодіває методикою експериментальних досліджень в конкретній предметній галузі та обробки отриманих результатів. Перелік тем лабораторних робіт визначається робочою програмою/силабусом освітнього компонента. Заміна лабораторних занять іншими видами навчальних занять не припустима.

Лабораторні заняття проводяться у спеціально оснащених навчальних лабораторіях з використанням обладнання, пристосованого до умов освітнього процесу (лабораторних макетів, установок та ін.). Лабораторні заняття можуть проводитися також в умовах реального професійного середовища (на підприємстві, в наукових лабораторіях тощо) або у комп'ютерних класах при виконанні віртуальних робіт. Кожна лабораторна робота має бути забезпечена методичною розробкою – методичними вказівками до виконання лабораторної роботи. До початка лабораторних занять викладач має провести інструктаж з техніки безпеки та отримати підписи студентів у відповідному журналі про ознайомлення із правилами техніки безпеки при проведенні лабораторних занять.

Для проведення лабораторних занять навчальна група поділяється на дві підгрупи. Поділ є можливим при чисельності підгрупи не менше ніж 12 студентів. З окремих навчальних дисциплін, з урахуванням особливостей вивчення цих дисциплін та безпеки життєдіяльності студентів, допускається поділ навчальної групи на підгрупи з меншою чисельністю. Перелік цих навчальних дисциплін за рекомендацією Методичної ради університету

затверджується наказом ректора. Такий поділ навчальних груп повинен бути зазначений у робочих навчальних планах.

Структура лабораторної роботи:

– вступна частина – тема роботи, її ціль, задачі, мотивація виконання; проведення контролю підготовленості студентів до виконання конкретної лабораторної роботи (колоквіум); інструктаж про виконання завдань та запобігання можливих типових помилок; інструктаж на робочому місці кожного студента; перевірка дотримання студентами вимог до послідовності та якості виконання завдань, санітарних, організаційних норм та техніки безпеки;
– основна частина – виконання студентами лабораторних досліджень; проведення проміжного контролю з метою коригування результатів роботи та своєчасного виявлення помилок; демонстрація викладачем оптимальних, раціональних окремих методів і прийомів виконання завдання;
– заключна частина – проведення контролю якості виконання завдань; визначення типових помилок в процесі проведення лабораторного завдання та засобів їх попередження; оцінка результатів діяльності кожного студента на основі встановлених критеріїв; видача домашнього завдання для самостійної підготовки до наступного лабораторного заняття.

Підсумкова оцінка, згідно з критеріями РСО, вноситься до рейтинг–листа та журналу обліку виконання лабораторних робіт і враховується в рейтингу результатів навчання студента з освітнього компонента. Наявність позитивних оцінок, одержаних студентом за всі лабораторні роботи, що передбачені робочою програмою, є необхідною умовою допуску студента до семестрового контролю з даного освітнього компонента.

При проведенні лабораторного заняття у викладача мають бути:

– робоча програма/силабус освітнього компонента;
– методичні вказівки до виконання лабораторних робіт;

– контрольні завдання (тести) для проведення контролю підготовленості студентів до виконання лабораторної роботи і критерії оцінювання;
– журнал обліку інструктажу з техніки безпеки при проведенні лабораторних робіт;
– журнал обліку виконання студентами лабораторних робіт;
– інструкції з техніки безпеки у місці, доступному широкому огляду;
– журнал обліку навчальної роботи навчальної групи, в якому викладач має зробити запис про проведення заняття.

Навчальна дисципліна «Основи теорії телекомунікацій і радіотехніки. Частина 2» належить до нормативних освітніх компонент циклу загальної підготовки першого (бакалаврського) рівня вищої освіти спеціальності 172 «Телекомунікації та радіотехніка» освітньо–професійної програми «Інформаційно–обчислювальні засоби радіоелектронних систем».

До забезпечуючих дисциплін відноситься дисципліна «Основи теорії телекомунікацій і радіотехніки. Частина 1», що дозволяє в даній дисципліні курсі перейти до вивчення специфічних питань сучасних мережних технологій і методів побудови телекомунікаційних мереж. У свою чергу програмні результати навчання даної дисципліни використовуються при проходженні переддипломної практики та для підготовки дипломного проєкту.

Предмет навчальної дисципліни: типи та характеристики фізичних середовищ передачі, архітектура мереж передачі даних, методи управління каналами передачі.

Метою навчальної дисципліни є формування у студентів здатностей:

– проводити аналіз та підбір необхідних технологій доставки даних в мережах;
– проводити оцінку характеристик фізичних середовищ передачі сигналів;

– вирішувати задачі по налаштуванню та адмініструванню мережного програмного забезпечення;
– використовувати програмні результати навчання для підготовки дипломного проєкту.

Основні завдання навчальної дисципліни.

Згідно з вимогами освітньо–професійної програми студенти після засвоєння навчальної дисципліни мають продемонструвати такі програмні результати навчання:

Загальні компетентності (ЗК)	
ЗК 1	Здатність до абстрактного мислення, аналізу та синтезу
ЗК 2	Здатність застосовувати знання у практичних ситуаціях
ЗК 4	Знання та розуміння предметної області та розуміння професійної діяльності
ЗК 7	Здатність вчитися і оволодівати сучасними знаннями
Фахові компетентності (ФК)	
ФК 1	Здатність розуміти сутність і значення інформації в розвитку сучасного інформаційного суспільства
ФК 3	Здатність використовувати базові методи, способи та засоби отримання, передавання, обробки та зберігання інформації
ФК 10	Здатність здійснювати монтаж, налагодження, налаштування, регулювання, дослідну перевірку працездатності, випробування та здачу в експлуатацію споруд, засобів і устаткування телекомунікацій та радіотехніки
ФК 12	Здатність проводити роботи з керування потоками навантаження інформаційно–телекомунікаційних мереж
Програмні результати навчання	
ПРН 6	грамотно застосовувати термінологію галузі телекомунікацій та радіотехніки;
ПРН 7	описувати принципи та процедури, що використовуються в телекомунікаційних системах, інформаційно–телекомунікаційних мережах та радіотехніці;
ПРН 8	аналізувати та виконувати оцінку ефективності методів проектування інформаційно–телекомунікаційних мереж, телекомунікаційних та радіотехнічних систем;
ПРН 12	застосування фундаментальних і прикладних наук для аналізу та розробки процесів, що відбуваються в телекомунікаційних та радіотехнічних системах;
ПРН 20	забезпечувати надійну та якісну роботу інформаційно–комунікаційних мереж, телекомунікаційних та радіотехнічних систем;
ПРН 21	контролювати технічний стан інформаційно–комунікаційних мереж, телекомунікаційних і радіотехнічних систем у процесі їх технічної експлуатації з метою виявлення погіршення якості функціонування чи відмов, та його систематична фіксація шляхом документування.

Лабораторний практикум з освітнього компонента «Основи теорії телекомунікацій і радіотехніки. Частина 2» включає 6 лабораторних робіт.

Основні завдання циклу лабораторних занять (комп'ютерного практикуму):

- придбання практичних знань та досвіду використання мережного програмного забезпеченням,
- отримання базового досвіду по обслуговуванню мережі та її адмініструванню.

В навчальному посібнику наведено матеріали до наступних лабораторних робіт.

№ з/п	Назва лабораторної роботи (комп'ютерного практикуму)	Кількість ауд. годин
1.	**ЛАБОРАТОРНА РОБОТА N 1** ОСНОВНІ КОМАНДИ ДЛЯ РОБОТИ З МЕРЕЖНИМИ РЕСУРСАМИ В КОМАНДНОМУ РЯДКУ	4
2.	**ЛАБОРАТОРНА РОБОТА N 2** АНАЛІЗ СИСТЕМИ ЗА ДОПОМОГОЮ МОНІТОРУ ПРОДУКТИВНОСТІ	4
3.	**ЛАБОРАТОРНА РОБОТА N 3** ОСОБЛИВОСТІ АДМІНІСТРУВАННЯ КОНТРОЛЕРА ДОМЕНУ WINDOWS 20xx	8
4.	**ЛАБОРАТОРНА РОБОТА N 4** НАЛАШТУВАННЯ ТА ВИКОРИСТАННЯ СИСТЕМИ ДОМЕННИХ ІМЕН – DNS	6
5.	**ЛАБОРАТОРНА РОБОТА N 5** НАЛАШТУВАННЯ ТА ВИКОРИСТАННЯ МЕРЕЖНОГО СЕРВІСУ DHCP	6
6.	**ЛАБОРАТОРНА РОБОТА N 6** НАЛАШТУВАННЯ ТА АДМІНІСТРУВАННЯ IIS (Internet Information Services)	6

1. ІНСТРУКЦІЇ ДО ЛАБОРАТОРНИХ РОБІТ

1.1. Лабораторна робота № 1. ОСНОВНІ КОМАНДИ ДЛЯ РОБОТИ З МЕРЕЖНИМИ РЕСУРСАМИ В КОМАНДНОМУ РЯДКУ

Мета та основні завдання:

- ознайомитись з форматами та синтаксисом базових команд командного рядку;
- навчитись використовувати базові команди командного рядку для роботи з мережними ресурсами.

Порядок виконання

1. Ознайомитись з методичними матеріалами.
2. З використанням команд командного рядку.

2.1. На диску C: виділити у загальне користування папку «Temp» (Net Share). Якщо потрібно, попередньо зробити вказану папку на диску.

2.2. Переглянути ресурси, виділені у загальне користування на Вашому ПК (Net Share).

2.3. Переглянути комп'ютери у мережному оточенні (Net View).

2.4. Переглянути доступні мережні ресурси по Netbios–імені або IP–адресі Вашого ПК (Net View).

2.5. Під'єднати мережний ресурс (загальну папку «Temp») на Вашому ПК, як мережний диск (Net Use).

2.6. Переглянути під'єднані мережні ресурси на Вашому ПК (Net Use).

2.7. Від'єднати мережний диск (Net Use) – після демонстрації викладачу.

2.8. Зняти виділення у загальний доступ з папки «Temp» (Net Share) – після демонстрації викладачу.

2.9. Завести групу користувачів на ПК (Net Localgroup). Дати відповідь, чим команда Net Localgroup відрізняється від команди Net group.

2.10. Завести користувача на ПК (Net User).

2.11. Включити користувача у створену групу (Net Localgroup).

2.12. Змінити пароль користувачу (Net User).

2.13. Видалити користувача (Net User) – після демонстрації викладачу.

2.14. Видалити групу (Net Localgroup) – після демонстрації викладачу.

2.15. Виконати синхронізацію часу на Вашому ПК з контролером домену (Net Time).

Основні теоретичні відомості

Базові утиліти для роботи з мережними ресурсами [1, 2]

Net Accounts

Використовується для оновлення бази облікових записів користувачів, зміни паролів і параметрів підключення для всіх користувачів [2] .

Синтаксис

net accounts [/ forcelogoff: *{хвилини* | **no}] [/ minpwlen:** *довжина]* **[/ maxpwage:** *{дні* | **unlimited}] [/ minpwage:** *дні]* **[/ uniquepw:** *число]* **[/ домен]**

Параметри

/Forcelogoff: ***{хвилини*** **| no} –** час очікування у хвилинах перед відключенням користувача від сервера у разі, якщо закінчився період дії облікового запису користувача або минув час, виділений для підключення. За замовчуванням використовується опція «**no**» **–** сеанси користувачів автоматично закриватися не будуть.

/Minpwlen: ***довжина*** **–** мінімальна довжина пароля користувача. Допустимі значення від 0 до 14 знаків, за замовчуванням використовується значення 0 знаків.

/Maxpwage: ***{дні*** **| unlimited} –** період часу в днях, протягом якого буде діяти пароль користувача. Значення **unlimited** знімає обмеження за часом. Значення параметра **/maxpwage** повинно бути більше, ніж значення параметра **/minpwage.** Допустимі значення від 0 до 999 днів (тобто значення **unlimited** дорівнює 999 днів), за умовчанням використовується значення 42 дні.

/Minpwage: ***дні*** **–** мінімальна кількість днів, які повинні пройти перед зміною пароля користувачем. За замовчуванням використовується нульове значення, тобто обмеження відсутнє. Допустимі значення від 0 до 999 днів.

/Uniquepw: ***число*** **–** заборона на повторне використання заданого числа останніх паролів. Можна заборонити використання до 24 останніх паролів, за замовчуванням це число дорівнює 0.

/Domain – виконання операції на основному контролері поточного домену. В іншому випадку операція здійснюється на локальному комп'ютері.

На комп'ютері, для якого будуть змінюватися облікові параметри, повинна бути запущена служба входу в мережу (Net Logon). При використанні команди net accounts без параметрів на екран виводяться поточні параметри пароля, параметри входу в систему і відомості про домен.

Перед використанням команди **net accounts** необхідно виконати наступні дії:

- створити облікові записи користувачів. Для цього слід скористатися диспетчером користувачів або командою **net user**;
- запустити службу Net Logon на усіх серверах, які перевіряють вхід в домен. Ця служба запускається автоматично при завантаженні комп'ютера.

При використанні параметра **/forcelogoff:** *хвилини* за вказану кількість хвилин перед примусовим відключенням користувачеві відправляється повідомлення. Користувачі також отримують повідомлення про відкриті файли. Якщо число *хвилин* менше двох, повідомлення користувачу буде відправлено негайно.

Приклад

Щоб задати довжину пароля не менше 7 знаків, введіть:

net accounts /minpwlen: 7

Щоб дозволити користувачеві змінювати пароль не частіше, ніж раз на 7 днів, примусово змінювати пароль раз на 30 днів, а також задати 5 –хвилинне очікування перед примусовим відключенням з відправкою повідомлення, введіть:

net accounts /minpwage: 7 /maxpwage: 30 /forcelogoff: 5

Net Config

Команда, яка служить для виведення відомостей про запущені служби, а також перегляду і зміни параметрів служби «Сервер» або «Робоча станція» [2].

Синтаксис

net config [{server | workstation}]

Параметри

Server – відображення і зміна параметрів служби «Сервер», якщо вона запущена.

Workstation – відображення і зміна параметрів служби «Робоча станція», якщо вона запущена.

Команда **net config server** служить для налаштування параметрів служби «Сервер». Зміни набувають чинності негайно і є постійними.

Команда **net config server** дозволяє змінювати не всі параметри служби «Сервер». Команда **net config server** виводить такі відомості, які не можна змінити:

- ім'я сервера,
- коментар для сервера,
- версія програми,
- активний сервер на (опис мережі),
- прихований сервер (параметр **/hidden)**,
- максимальне число користувачів (максимальна кількість користувачів, які можуть використовувати загальні ресурси цього сервера),
- максимальне число відкритих файлів в сеансі (максимальна кількість файлів сервера, яке користувач може відкрити протягом сеансу),
- час відсутності активності сеансу (хв).

Команда **net config workstation** служить для налаштування параметрів служби «Робоча станція».

Команда **Net config workstation** виводить такі відомості:

- ім'я комп'ютера (повне ім'я комп'ютера),

- ім'я користувача,
- активна робоча станція на (опис мережі),
- версія програми,
- домен робочої станції,
- DNS–ім'я домену робочої станції,
- домен входу,
- інтервал очікування відкриття COM–порту (с),
- лічильник передачі COM–порту (байт),
- таймаут передачі COM–порту (мс).

Net Start, Net Stop, Net Pause, Net Continue

Команди запуску, зупинки, паузи і продовження роботи служб [2].

Синтаксис

net start [служба] – запуск конкретної служби;

net stop [служба] – зупинка конкретної служби;

net pause [служба] – призупинення роботи конкретної служби;

net continue [служба] – продовження роботи конкретної служби.

Якщо ім'я служби містить пробіли, його слід брати в лапки (наприклад ***"ім'я служби").***

Net File

Виведення імен відкритих загальних файлів на сервері і кількості блокувань для кожного файлу, якщо вони встановлені. Також команда дозволяє закрити загальний файл і видалити блокування.

Синтаксис

net file *[номер* **[/close]]**

номер – ідентифікаційний номер файлу.

/close – закриття відкритого файлу і зняття блокування. Дана команда запускається на сервері, де знаходяться загальні файли.

Приклад

Щоб переглянути відомості про файли, що спільно використовуються, введіть:

net file

Щоб закрити файл під номером 1, введіть:

net file 1 /close

Net group, net localgroup

Відображення інформації та зміна глобальних груп в доменах або локальних груп на ПК [2].

Синтаксис

net group *[ім'я_групи* **[/comment:** ***"текст"]]*** **[/domain]**

net group *[ім'я_групи* **{/add [/comment:** ***"текст"]*** **| /delete} [/domain]]**

net group *[ім'я_групи ім'я_користувача* [...] **{/add** | **/delete} [/domain]]**

Параметри

Ім'я_групи **–** ім'я групи для додавання, видалення або виведення інформації. Для виведення списку користувачів в групі задається тільки ім'я групи.

/Comment: ***"текст"*** **–** додавання коментаря для нової або існуючої групи. Коментар може включати до 48 знаків. Текст слід брати в лапки.

/Domain – виконання операції на контролері поточного домену. В іншому випадку операція здійснюється на локальному комп'ютері.

/Add – додавання групи або імені користувача в групу. Для користувачів, що додаються в групу цією командою, необхідно завести обліковий запис.

/Delete – видалення групи або користувача з групи.

ім'я_користувача **[...] –** список з одного або декількох імен користувачів, яких потрібно додати або видалити з групи. Кілька імен повинні бути розділені пробілами.

Приклади

Щоб додати групу «Exec» в локальну базу облікових записів, введіть:

net localgroup exec /add

Щоб додати облікові записи існуючих користувачів «stevev», «ralphr» і «jennyt» у групу «exec» домену, введіть:

net group exec stevev ralphr jennyt /add /domain

Net Print

Використовується для друку файлу або файлів на мережному принтері [2].

Синтаксис

net print *ім'я_файлу* **[принтер]**

Параметри

ім'я_файлу	ім'я файлу або файлів, що виводяться на друк. В іменах можна використовувати трафаретні символи.
принтер	ім'я принтеру (не порту), на якому ви хочете роздрукувати файл. Якщо принтер не задається, файл посилається на перший з доступних мережних принтерів, підключених до ПК.

Net Send

Використовується для передачі повідомлень користувачам [2].

Параметри команди

Параметр	Опис
повідомлення	Повідомлення довжиною до 30 символів. Лапки обов'язкові. Лапки або керуючі символи ASCII всередині повідомлення не допускаються.
ALL або *	Повідомлення надсилається всім користувачам, у яких включений прийом повідомлення.
сервер	Ім'я сервера, користувачам якого ви хочете надіслати повідомлення.
ім'я_користувача	Користувач або користувачі, яким імя1 – імя3, ... ви хочете передати повідомлення.

Приклади

Щоб передати повідомлення користувачеві:

NET SEND "повідомлення" ім'я_користувача

Щоб надіслати повідомлення декільком користувачам в робочій групі використовуйте формат:

NET SEND "повідомлення" імя1 імя2 імя3

Щоб надіслати повідомлення всім:

NET SEND "повідомлення" ALL

Щоб послати повідомлення користувачеві, підключеному до конкретного сервера:

NET SEND "повідомлення" сервер /ім'я_користувача

Для передачі усім користувачам, підключеним до конкретного сервера:

NET SEND «повідомлення» сервер /ALL.

При передачі повідомлення ви побачите список користувачів, яким воно передано.

Net Share

Управління загальними ресурсами [2]**.**

Синтаксис

net share *[ім'я_ресурсу]*

net share *[ім'я_ресурсу* **= *диск:*** *шлях* **[{/users:** *число* | **/unlimited}] [/remark: *"текст"]* [/**cache: {manual** | **automatic** | **no}]]**

net share *[ім'я_ресурсу* [**{/users:** *число* | **unlimited}] [/remark: *"текст"]* [/**cache: {manual** | **automatic** | **no}]]**

net share *[{ім'я_ресурсу* | ***диск:*** *шлях}* **/delete]**

Параметри

ім'я_ресурсу – мережеве ім'я загального ресурсу.

Команда **net share** *ім'я_ресурсу* виводить відомості про окремий ресурс.

диск: *шлях* – абсолютний шлях до каталогу, який потрібно зробити загальним.

/Users: *число* – максимальна кількість користувачів, яким дозволений одночасний доступ до загального ресурсу.

/Unlimited – скасування обмеження на число користувачів, яким дозволений одночасний доступ до загального ресурсу.

/Remark: *"текст"* – додавання описового коментаря до ресурсу. Текст слід брати в лапки.

/Cache: automatic – включення автоматичного автономного кешування.

/Cache: manual – включення ручного автономного кешування.

/Cache: no – оповіщення клієнта про неможливість автономного кешування.

/Delete – скасування загального доступу до ресурсу.

Приклади

Щоб зробити каталог «C:\Дані» загальним ресурсом з ім'ям «Спільні дані» та додати куоментар до нього, введіть:

net share СпільніДані = c:\Дані /remark: "Для відділу 123"

Щоб скасувати спільний доступ до ресурсу СпільніДані, створеному в попередньому прикладі, введіть:

net share СпільніДані /delete

Щоб зробити папку «C:\Список малюнків» загальним ресурсом Список, введіть:

net share Список = "c:\Список малюнків"

Net Statistics

Висвітлення статистичної інформації**.**

Синтаксис

net statistics [{workstation | server}] – виведення на екран статистики роботи служби «Сервер» або «Робоча станція».

Net Time

Синхронізація годинника комп'ютера з іншим комп'ютером або сервером [2]**.**

Синтаксис

net time [{*ім'я_комп'ютера***|/domain[:***ім'я_домена]* |

/rtsdomain[: *ім'я_домена]}]* **[/set]**

net time [*ім'я_комп'ютера]* **[/querysntp] [/setsntp [:***список_серверов_NTP]]*

Параметри

\\ім'я_комп'ютера – вказує ім'я сервера, час на якому потрібно перевірити чи з яким потрібно синхронізувати таймер.

/Domain [:*ім'я_домена]* – задає ім'я домену, з основним контролером якого синхронізується годинник.

/Rtsdomain [:*ім'я_домена]*– вказує домен, з сервером надійного часу (RTS) якого буде синхронізуватися годинник.

/Set – синхронізує годинник з часом вказаного комп'ютера або домену.

/Querysntp – виводить ім'я сервера NTP (Network Time Protocol), призначеного для локального комп'ютера, або комп'ютера, вказаного в параметрі *ім'я_комп'ютера*.

/Setsntp [:*список_серверів_NTP]* – вказує список серверів часу NTP для використання на локальному комп'ютері.

Приклади

Щоб переглянути поточний час на комп'ютері CORPDC1, введіть:

net time \\CORPDC1

Щоб синхронізувати час комп'ютера з поточним часом в домені, введіть:

net time /domain /set

Net Use

Підключення до загальних мережних ресурсів або виведення інформації про підключення комп'ютера. Команда також управляє постійними мережними з'єднаннями [2]**.**

Синтаксис

net use *[{ім'я_пристрою* | ***}] [***ім'я_комп'ютера* *****ресурс* **[***том]] [{пароль* | ***}]] [/user:** *[ім'я_домена***\]] [/user:** *[ім'я_домена_з_крапкою***\]** *ім'я_користувача]* **[/user :** *[username @ ім'я_домена_з_крапкою]* **[/savecred] [/smartcard] [{/delete** | **/persistent: {yes** | **no}}]**

net use *[ім'я_пристрою* **[/home** *[{пароль* | ***}] [/delete: {yes** | **no}]]**

net use [/persistent: {yes | **no}]**

Параметри

Ім'я_пристрою – задає ім'я ресурсу при підключенні, або ім'я пристрою при відключенні. Існує два види імен пристроїв: імена для дискових пристроїв (тобто, диски з літерними позначеннями від D: до Z:) і для принтерів (відповідно, від LPT1: до LPT3:). Введення зірочки (*) замість імені певного

пристрою забезпечить привласнення такому пристрою найближчого доступного імені.

\\Ім'я_комп'ютера\ім'я_ресурсу – вказує ім'я сервера та загального ресурсу. Якщо параметр *ім'я_комп'ютера* містить пробіли, все ім'я комп'ютера від подвійної зворотної риски (\\) до кінця (наприклад, *"\\Computer Name\Share Name")* повинно бути наведено у прямих лапках ("). Ім'я комп'ютера може мати довжину від 1 до 15 знаків.

Пароль – задає пароль, необхідний для підключення до загального ресурсу. Введіть зірочку (*) для виведення запрошення на введення пароля. При введенні з клавіатури символи пароля не виводяться на екран.

/User – задає інше ім'я користувача для підключення до загального ресурсу.

Ім'я_домена – задає ім'я іншого домену, до ресурсу якого необхідно підключитися. Пропуск параметру і*м'я_домена* призводить до того, що команда **net use** використовує поточне ім'я домену, яке було використано при вході користувача в систему.

ім'я_користувача – вказує ім'я користувача для підключення.

им'я_домену _з_крапкою – вказує повне ім'я домену, в якому присутній обліковий запис користувача.

/Savecred – зберігає введені облікові дані для подальшого використання.

/Smartcard – вказує необхідність зчитування облікових даних зі смарт–карти для мережного підключення. За наявності декількох смарт–карт з'явиться запит на вибір однієї з них.

/Delete – скасовує зазначене мережне підключення. Якщо опція задана з символом зірочки (*), будуть скасовані всі мережні підключення.

/Persistent: {yes | no} – управляє постійними мережними підключеннями. За замовчуванням береться останнє використане значення. Підключення без пристрою не є постійними. Вибір значення **Yes** призводить до збереження всіх існуючих з'єднань і поновлення їх при наступному підключенні. При виборі значення **No** підключення не зберігаються. Існуючі підключення

відновлюються при наступному вході в систему. Для видалення постійних підключень використовується ключ **/delete.**

/Home – підключає користувача до його домашнього каталогу.

Якщо команду **net use** ввести без параметрів, на екран буде виведено список мережних підключень.

Приклади

Щоб підключити загальний каталог Letters на сервері \\Financial під ім'ям логічного диску E:, слід ввести:

net use e: \\financial\letters

Для відновлення поточних підключень при наступних входах в мережу, незалежно від майбутніх змін, необхідно використати команду:

net use /persistent: yes

Net User

Додавання, редагування або перегляд облікових записів користувача [2].

Синтаксис

net user *[ім'я_користувача [пароль* | ***]** *[параметри]]* **[/domain]**

net user *ім'я_користувача {пароль* | ***}** **/add** *[параметри]* **[/domain]**

net user *ім'я_користувача* **[/delete] [/domain]**

Параметри

ім'я_користувача – вказує ім'я облікового запису користувача, який можна додати, видалити, відредагувати або переглянути. Ім'я може мати довжину до 20 символів.

*Пароль – п*рисвоює або змінює пароль користувача. Введіть зірочку (*) для виведення запрошення на введення пароля. При введенні з клавіатури символи пароля не виводяться на екран.

/Domain – виконує операцію на основному контролері домена.

Параметри – задає параметр командного рядка.

Приклади

Для виведення інформації про користувача "jimmyh" необхідно скористатися командою:

net user jimmyh

Для додавання облікового запису користувача Jay Jamison з повним ім'ям користувача і правом на підключення з 8 до 17 години з понеділка по п'ятницю при обов'язковому введенні пароля (jayj) використовується наступна команда:

net user jayj /add /passwordreq: yes /times: Пн–Пт,08:00–17:00 /fullname:"Jay Jamison"

Для завдання часу підключення з 4 до 17 годин в понеділок, з 13 до 15 години у вівторок і з 8 до 17 години з середи по п'ятницю для користувача marysl використовується наступна команда:

net user marysl /time: Пн, 4:00–17:00; Вт,13:00–15:00; Ср–Пт,8:00–17:00

Net View

Виводить список доменів, комп'ютерів або загальних ресурсів на вказаному вузлі [2]**.**

Синтаксис

net view [*ім'я_комп'ютера]* **[/domain [:***ім'я_домену]]*

Параметри

ім'я_комп'ютера – задає ім'я комп'ютера для перегляду розташованих на ньому загальних ресурсів.

/Domain [:*ім'я_домена]* – задає домен, для якого виводиться список комп'ютерів. Якщо параметр *ім'я_домена* не заданий, команда виводить список всіх доменів мережі.

Приклади

Список загальних ресурсів комп'ютера \\Production може бути отриманий за допомогою команди:

net view \\production

1.2. Лабораторна робота № 2. АНАЛІЗ СИСТЕМИ ЗА ДОПОМОГОЮ МОНІТОРУ ПРОДУКТИВНОСТІ

Мета та основні завдання:

- ознайомитись з основними факторами, що впливають на продуктивність роботи робочої станції, інструментами додатку «Монітор продуктивності – Performance Monitor», видами звітності і сповіщеннями,
- навчитись вирішувати задачі по налаштуванню та адмініструванню монітору продуктивності.

Порядок виконання

1. Ознайомитися з документацією.
2. Використовуючи «засоби адміністрування Windows — Монітор продуктивності (Performance Monitor)» або «керування комп'ютером – Монітор продуктивності (Performance Monitor)» запустити монітор продуктивності.
3. Розібратися з базовими інструментами додатку: «Інструменти моніторингу – Monitoring tools», «Групи збирачів даних – Data collector Sets», «Звіти – Reports».
4. Створити, використовуючи інструмент «Групи збирачів даних – Data collector Sets» – «Особливі – User Defined» свою групу: створити вручну – лічильник продуктивності – додати лічильник (наприклад – процесор – завантаженість процесору). Змінити інтервал збору даних на 1 сек. Відкрити властивості журналу в створеній групі та задати ім'я файлу для збереження даних.
5. Запустити створену групу, зібрати статистику протягом декількох хвилин. Зупинити групу, візуалізувати статистику використовуючи інструмент «системний монітор» (в джерелі даних вибрати файл зі статистикою, додати лічильник, дані якого необхідно візуалізувати на

екрані). Переглянути засіб візуалізації статистики через «звіти – група збирачів даних».

6. Розібратися з налаштуванням оповіщень (Особливі – створити – групу збирачів даних – створити вручну – оповіщення лічильника продуктивності – додати лічильник (наприклад – процесор – завантаженість процесору). Задати поріг для оповіщень. Відкрити властивості журналу в створеній групі та задати ім’я файлу для збереження даних. Розібратися з налаштуваннями «дій оповіщення» – налаштувати запуск групи збирачів даних с попереднього завдання.

Основні теоретичні відомості

Монітор продуктивності

За допомогою монітора продуктивності (Performance Monitor) [3] користувач може не тільки аналізувати завантаженість апаратних ресурсів і програмних додатків робочої станції, а і поліпшувати продуктивність своєї системи, знаходити помилки в конфігурації, досліджувати, як впливають ті чи інші зміни в конфігурації на продуктивність, виявляти години пікових завантажень і багато іншого.

Монітор продуктивності використовує лічильники, кожен з яких пов'язаний з (і стежить за) конкретними об'єктами в системі. Наприклад, кількість процесів, що очікують роботи з дисками, відсоток завантаження процесора, кількість пакетів, що проходять через мережу за секунду. Монітор може збирати дані в файл, малювати діаграми або відправляти повідомлення в разі досягнення лічильником певного значення. У можливості монітора входить:

- перегляд даних одночасно від будь–якої кількості комп'ютерів,
- негайна реакція після внесення змін в систему,
- перегляд і динамічна зміна графіків, що відображають показники поточної активності системи,

• експорт даних з графіків, log–файлів і звітів в бази даних і електронні таблиці (наприклад: Excel, Access, SQL Server),

• створення порогових значень для будь–яких лічильників, у разі досягнення яких з'явиться запис в log–файлі і, за бажанням, буде відправлено повідомлення користувачеві,

• створення log–файлів для даних з різних комп'ютерів, включаючи різні (однакові) лічильники протягом різних (однакових) проміжків часу для подальшого спільного аналізу,

• дописування до існуючих log–файлів для організації довгострокової статистики,

• збереження конфігурації, графіка або звіту для подальшого використання.

Об’єкти монітору продуктивності

Операційна система Windows організована за об'єктним принципом. Запропонований користувачеві у моніторі продуктивності список об'єктів формується самою операційною системою. З кожним об'єктом асоційований якийсь набір лічильників, специфічних для даного типу об'єктів. Об'єктів даного типу в системі може бути кілька (наприклад: процесори, диски і т.д.). Деякі об'єкти в системі завжди зустрічаються в одному екземплярі (наприклад: пам'ять або служба «сервер»). У тому випадку, якщо об'єктів даного типу в системі декілька, користувач може збирати, аналізувати кожен з об'єктів окремо або всі разом. У ОС Windows можуть бути використані наступні об'єкти [1, 3].

- Cache (Кеш),
- Paging File (Файл сторінкової пам'яті),
- Logical Disk (Логічний диск),
- Physical Disk (Фізичний диск),
- Memory (Пам'ять, ОЗП),
- Process (Процес),
- Objects (Об'єкти),

- Processor (Процесор),
- Redirector (Редиректор),
- Server (Сервер),
- System (Система),
- Thread (Завдання).

Призначення більшої частини об'єктів інтуїтивно зрозуміле, але необхідно пояснити різницю між процесами і завданнями. Процес складається з виконуваної програми, пулу адрес, в якому виконується програмний код, і одного або кількох завдань,. Процесом може бути програма, сервіс або підсистема. Завдання породжуються процесами і ідентифікуються по імені процесу, що його породив, і порядковому номеру в процесі. Найменування процесу може бути тільки числовим (для системних процесів) або відповідним імені виконуваного файлу (для всіх інших). Шістнадцятирозрядні програми розглядаються як процеси, тільки коли вони виконуються в окремому просторі пам'яті (в ShortCut стоїть опція Run in Separate Memory Space).

Значення лічильників можуть бути усередненими по проміжку часу між двома послідовними опитуваннями об'єкта (всі лічильники, які мають суфікс / sec) або відповідати значенню, отриманому при останньому зверненні.

Оснастка «Монітор продуктивності».

За допомогою оснастки «Монітор продуктивності» можна вимірювати завантаженість ресурсів вашого комп'ютера або інших комп'ютерів в мережі, а саме [3]:

- збирати та переглядати дані поточної завантаженості системи на локальному комп'ютері або на декількох віддалених комп'ютерах,
- переглядати поточні дані або дані, зібрані раніше,
- представляти дані у вигляді графіка, гістограми або звіту, які можна вивести на друк,
- створювати HTML–сторінки для перегляду зібраної статистики,
- створювати конфігурації моніторингу, що допускають повторне використання, які можна інсталювати на інших комп'ютерах.

Об'єкти та лічильники продуктивності

Windows отримує інформацію про завантаженість від компонентів комп'ютера. Такі компоненти називаються об'єктами продуктивності.

В ОС є ряд об'єктів продуктивності, які, зазвичай, відповідають головним апаратним компонентам, таким як пам'ять, процесори і т.д. Додатки можуть також створювати свої об'єкти продуктивності [1].

Кожен об'єкт продуктивності надає лічильники, які збирають дані продуктивності. Наприклад, лічильник «Обмін сторінок/сек» об'єкта «Пам'ять» відслідковує ступінь кешування сторінок.

Об'єкти, які найбільш часто використовуються для відстеження роботи системних компонентів:

- кеш;
- логічний диск;
- фізичний диск;
- пам'ять;
- потік;
- процес;
- процесор;
- система;
- файл підкачки.

Деякі об'єкти (такі як «Пам'ять» і «Сервер») мають тільки один екземпляр, хоча інші об'єкти продуктивності можуть мати безліч екземплярів. Якщо об'єкт має безліч екземплярів, то ви можете додати лічильники для відстеження статистики по кожному примірнику або для всіх екземплярів одночасно.

Наприклад, якщо в системі встановлено декілька процесорів, то об'єкт «Процесор» буде мати декілька екземплярів. Більш того, якщо об'єкт підтримує декілька екземплярів, то при об'єднанні екземплярів в групу

з'являться батьківський екземпляр і дочірні екземпляри, які будуть належати даному батьківському екземпляру.

Налаштування лічильників

При виборі оснастки «Монітор продуктивності» за замовчуванням буде відкрито вікно для побудови графіків. Дії по додаванню лічильників [3]:

- у панелі результатів вікна натисніть праву кнопку миші і виберіть в контекстному меню команду «Додати лічильники». Альтернативний варіант – натиснути кнопку «Додати» на панелі інструментів;
- у вікні, виберіть перемикач «Використовувати локальні лічильники» для моніторингу комп'ютера, на якому запущена консоль моніторингу. Якщо ви збираєтеся проводити моніторинг певного комп'ютера, незалежно від того, де запущена консоль моніторингу, виберіть перемикач «Обрати лічильники з комп'ютера» і вкажіть ім'я комп'ютера (за замовчуванням встановлено ім'я локального комп'ютера);
- у списку «Елемент» виберіть об'єкт для моніторингу;
- у списку «Вибрати лічильники зі списку» вкажіть лічильник, який ви збираєтеся використовувати;
- для моніторингу всіх обраних екземплярів виберіть перемикач «Всі входження». Для моніторингу тільки певних екземплярів встановіть перемикач «Обрати входження зі списку» і виберіть екземпляри, які ви збираєтеся відслідковувати;
- натисніть кнопку «Додати» і потім кнопку «Закрити». Повторіть пункти для інших об'єктів.

Якщо у вас немає відповідних дозволів на моніторинг комп'ютера, то з'явиться повідомлення про помилку. Лічильник буде вказаний на гістограмі, але дані не будуть виводитися.

У разі відсутності на екрані лічильника, який ви збираєтеся відслідковувати, можливо, що сервіс або елемент, який є об'єктом лічильника, не інстальований або не активований на даному комп'ютері, і вам слід, перш за все, додати цей сервіс.

У таблиці 1.1 наведено мінімальний набір лічильників, які слід використовувати для моніторингу сервера [1, 3]. У процесі роботи ви зможете додати додаткові лічильники для інших об'єктів продуктивності.

Таблиця 1.1 – Мінімальний набір лічильників, які слід використовувати для моніторингу сервера

Компонент	**Досліджуваний параметр**	**Лічильники**
Пам'ять	Ступінь використання	Пам'ять; Доступно байт Пам'ять; Байт кеш–пам'яті
Пам'ять	Вузькі місця	Пам'ять; Обмін сторінок / сек Пам'ять; Читання сторінок / сек Пам'ять; Помилок транзиту / сек Пам'ять; Байт в що вивантажується сторінковому пулі Пам'ять; Байт в невивантажуваному сторінковому пулі Також корисні лічильники Файл підкачки;% використання Кеш;% влучень при відображенні даних
Процесор	Ступінь використання Вузькі місця	Процесор;% завантаженості процесора (всі входження) Процесор; Переривань / сек Система; Довжина черги процесора (всі входження) Система; контекстної перемикань / сек
Диск	Ступінь використання Вузькі місця	Фізичний диск; Звернень читання з диска / сек Фізичний диск; Звернень запису на диск / сек Фізичний диск; Середня довжина черги диска (всі входження)
Мережний інтерфейс	Ступінь використання Продуктивність	Сегмент мережі;% використання мережі Лічильники передачі по протоколах Мережний інтерфейс; Всього байт / сек Мережевий інтерфейс; Пакетів / сек Сервер; Всього байт / сек або Сервер; Послано байт / сек і Сервер; Отримано байт / сек)

Налаштування зовнішнього вигляду

В оснащенні «Монітор продуктивності» доступні три засоби перегляду інформації: два графічні («Графік» та «Гістограма») і одне текстове («Звіт») [3]. Для налаштування зовнішнього вигляду вікна моніторингу натисніть графік правою кнопкою миші і виберіть пункт «Властивості» контекстного меню. У вікні для графіка та гістограми можна задати ряд додаткових параметрів відображення:

- назва графіка або гістограми та осей координат;
- діапазон виведення значень;
- характеристики кривої на графіку або стовпців на гістограмі, такі як колір, товщина, стиль та інше.

На вкладці «**Загальні»** можна вказати необхідний вид засобу моніторингу. За умовчанням вибрана опція «**Графік»**. Можна також відображати дані про продуктивність у вигляді гістограми або звіту.

Робота з оснасткою «Монітор продуктивності»

Проводячи моніторинг системи, пам'ятайте кілька корисних правил, які дозволять вам найбільш ефективно використовувати ресурси системи [1].

- Визначте конфігурацію засобів моніторингу. Для відстеження роботи ви можете переглядати дані у вигляді графіка з допомогою «Монітора продуктивності», або збирати дані в журнали продуктивності для перегляду та аналізу в інших додатках. Налаштуйте оснастку «Оповіщення» і журнали продуктивності для збору даних з вибраних лічильників з певними інтервалами. Отримані журнали даних можна використовувати для створення звітів і аналізу загальної продуктивності системи, а також планування подальшої модернізації.
- Підтримуйте ресурси, необхідні для моніторингу на низькому рівні. Інструменти моніторингу сконфігуровані для споживання мінімальної кількості ресурсів. Однак у ряді випадків потрібно вжити додаткових заходів для його зниження. Представлення даних продуктивності у вікні «Монітору продуктивності» у вигляді графіка, часта вибірка даних, велика кількість

об'єктів і лічильників, що відслідковуються, – все це збільшує кількість ресурсів, що витрачаються на моніторинг продуктивності.

- Аналіз даних продуктивності та визначення базового рівня продуктивності. Як правило, корисно визначити базовий рівень продуктивності для типового навантаження. Це можна зробити шляхом виведення даних у графічному вигляді у вікні «Монітору продуктивності».
- Встановлення оповіщень. Встановіть генерацію оповіщень, коли значення лічильників будуть відхилятися від заданих порогових значення.
- Настроювання продуктивності. Використовуючи дані по продуктивності, виконайте налаштування системних установок для оптимального завантаження системи.
- Планування. Проводьте моніторинг тенденцій зміни завантаження сервера та необхідності проведення модернізації апаратної частини системи.

Аналіз даних продуктивності

Аналіз результатів моніторингу включає в себе перевірку показань лічильників, що фіксуються під час виконання системою різних операцій. У ході цього процесу слід визначити найбільш активні процеси, а також виявити програми або потоки, які монопольно використовують будь–які ресурси. У результаті ви повинні з'ясувати, як ваша система справляється з робочим навантаженням.

У ході такого аналізу ви повинні визначити рівень продуктивності системи, коли обробляється типове навантаження і запущені всі необхідні сервіси, який називається базовим рівнем. Базовий рівень визначається адміністратором, виходячи з робочого завантаження. Цей рівень визначається на основі показань ряду лічильників продуктивності і відповідає стану системи, коли вона задовільно обробляє всі запити користувачів.

Визначення прийнятних показань лічильників

У цілому, визначення прийнятного рівня продуктивності являє собою досить суб'єктивне рішення. В наведеній нижче таблиці 1.2 зазначені граничні

значення для ряду лічильників, які допоможуть вам визначити, чи свідчать показання лічильників про появу проблеми [1]. Якщо показання лічильників постійно знаходяться на граничному рівні, то є всі підстави говорити про наявність в системі вузького місця, і слід вжити заходів для налаштування або модернізації завантаженого ресурсу.

Таблиця 1.2 – Граничні значення лічильників

Об'єкт / лічильник	**Граничний рівень**	**Коментар**
1	**2**	**3**
Диск		
Фізичний диск;% активності диска	90	Перевірте значення лічильника Фізичний диск; Поточна довжина черги диска
Фізичний диск; Диск Читань / сек, Фізичний диск; Диск Записів / сек	Залежить від специфікацій виробника	Перевірте зазначену швидкість передачі для ваших дисків, щоб визначити, чи не перевищують показання лічильника зазначене виробником значення.
Фізичний диск; Поточна довжина черги диска	Число шпинделів, що утворюють фізичний диск (це значення перевищує одиницю для RAID–масивів) плюс 2	Даний лічильник є миттєвим. Перевірку показань лічильника слід проводити протягом декількох періодів часу. Для отримання середнього значення використовуйте показання лічильника фізичний диск; Середня довжина черги диска
Пам'ять		
Пам'ять; Доступно байт	Менш 4 Мбайт	Перевіряйте ступінь використання пам'яті. При необхідності збільшить об'єм пам'яті
Пам'ять; Сторінок / сек	20	Перевіряйте активність кешування
Мережа		
Сегмент мережі;% використання мережі	Залежить від типу мережі	Граничний рівень визначається на основі типу мережі. Для мереж Ethernet рекомендованим значенням є рівень в 30%
Файл підкачки		
Файл підкачки;% використання	99	Порівняйте показання цього лічильника в поєднанні з показаннями лічильників Доступно байт і Сторінок / сек для оцінки активності кешування на вашому комп'ютері

Продовження таблиці 1.2

1	2	3
Процесор		
Процесор;% завантаженості процесора	85	Визначте процес, який використовує велику частину процесорного часу. У разі необхідності встановіть додатковий процесор або модернізуйте наявний
Процесор; Переривань / сек	Залежить від процесора	Серйозне збільшення показань даного лічильника без відповідного збільшення системної активності вказує на апаратну проблему
Сервер		
Сервер; Всього байт / сек		Якщо сума показань всіх значень лічильників Всього байт / сек для всіх серверів приблизно дорівнює максимальної пропускної здатності вашої мережі, то вам, можливо, необхідно сегментувати мережу
Сервер; браків робочих елементів	3	Якщо показання лічильника досягають граничного значення, то спробуйте налаштувати значення InitWorkItems або MaxWorkItems в реєстрі (HKEY_LOCAL_MACHINE \ SYSTEM; CurrentControlSet; Services; LanmanServer)
Сервер; вивантажуваємий пул (пік)	Обсяг фізичної пам'яті (ОЗП)	Дане значення є індикатором максимального розміру файлу підкачки і об'єму фізичної пам'яті
Робочі черги сервера; Довжина черги	4	Якщо показання лічильника досягають максимального значення, то можливо перетворення процесора в вузьке місце. Даний лічильник є миттєвим, його показання слід відслідковувати протягом декількох інтервалів часу
Багатопроцесорні системи		
Система; Довжина черги процесора	2	Даний лічильник є миттєвим. Його свідчення слід відслідковувати протягом декількох інтервалів часу

Моніторинг мережної активності

Моніторинг мережної активності полягає в спостереженні за використанням ресурсів сервера і загального мережного трафіку. Однак оснастки «Монітор продуктивності» і «Монітор ресурсів» дозволяють виконувати і більш глибокий аналіз трафіку [3].

Почніть моніторинг комп'ютера з відстеження показників, що входять в мінімальний список рекомендованих показників. Ознайомтеся з використанням ресурсів вашого комп'ютера. Щоб сконцентруватися на відстеження ресурсів, пов'язаних з мережною активністю, застосовуйте показники, які відповідають різним рівням конфігурації мережі. Ненормальні значення мережних показників зазвичай вказують на проблеми з процесором або з пам'яттю чи з жорсткими дисками сервера.

Рекомендується стежити за мережними показниками в поєднанні з показниками Memory \ Pages / Sec, Processor \% Processor Time і Physical Disk \% Disk Time [1].

Наприклад, різке зростання Memory \ Pages / Sec, що супроводжується зменшенням показника Memory \ BytesTotal / Sec для сервера, найімовірніше пов'язане з тим, що обсяг фізичної пам'яті недостатній для виконання мережних операцій.

Мінімальний список рекомендованих показників

Мінімальний список показників, рекомендованих для моніторингу продуктивності мережі [1]:

- Server \ PoolPagedPeak. Показує обсяг фізичної пам'яті і максимальний розмір файлу підкачки сторінок пам'яті. В якості порогового значення можна використовувати обсяг фізичної оперативної пам'яті (RAM).

Щоб відстежувати можливі ситуації, пов'язані із завантаженістю, застосовуйте наступні показники:

- Server \ BytesTotal / Sec. Показує кількість байт, переданих в мережу або отриманих з мережі сервером. Цей показник корисний, коли потрібно зрозуміти, наскільки сильно завантажений сервер. Якщо сума BytesTotal / Sec для всіх серверів наближається до максимальної швидкості передачі даних вашої мережі, то, можливо, доведеться сегментувати мережу;

- Server \ WorkItemShortages. Показує, скільки разів не були доступні робочі елементи (work items) для обслуговування вхідних запитів. Якщо значення цього показника досягає порогового значення «3» або перевищує

його, то спробуйте налаштувати InitWorkItems і MaxWorkItems в ключі Реєстру HKEY_LOCAL_MACHINE \ SYSTEM \ CurrentControlSet \ Services \ LanmanServer.

Контрольні запитання

1. Для чого призначений монітор продуктивності?
2. Для яких вузлів мережі є необхідність налаштовувати засоби моніторингу та збирати статистику?
3. За допомогою яких елементів системного монітору можна зібрати статистику про роботу вузла в автономному режимі?
4. За допомогою яких елементів системного монітору можна налаштувати оповіщення про критичні події на вузлу?
5. Які основні об'єкти можна досліджувати за допомогою системного монітору?
6. Порогові значення найбільш важливих лічильників.

1.3. Лабораторна робота № 3. ОСОБЛИВОСТІ АДМІНІСТРУВАННЯ КОНТРОЛЕРА ДОМЕНУ WINDOWS 20xx

Мета та основні завдання: ознайомитись з

- поняттями Active Directory та структурних одиниць («ліс», «дерево», «сайт»),
- інструментами управління «лісом», «деревом», «сайтами» та зміною ролей серверів,
- навчитись вирішувати задачі по налаштуванню та адмініструванню контролерів домену.

Порядок виконання

1. Ознайомитися з документацією.
2. Ознайомитися з основними інструментами управління «лісом» (Програмна група «Адміністрування» – Active Directory – домени та довіра).
3. Ознайомитися з основними інструментами управління «деревом» (Програмна група «Адміністрування» – Active Directory–користувачі і комп'ютери).
4. Ознайомитися з основними інструментами управління «сайтами» (Програмна група «Адміністрування» – Active Directory – сайти і служби)
5. Ознайомитися з основними інструментами зміни функціональних ролей сервера (Програмна група «Адміністрування» – Управління даним сервером)

Основні теоретичні відомості

Базова концепція Active Directory

Для організації доменів на базі систем Windows Server 2000/2012 використовується служба каталогу Active Directory [1, 4]. Кожен контролер домену під керуванням цих систем є сервером каталогу Active Directory, і службу Active Directory неможливо розгорнути без створення доменної структури. Розглянемо спочатку можливості, організацію і використання служби Active Directory.

Поняття служби каталогу та Active Directory

Об'єднання комп'ютерів в єдину інформаційну мережу дозволяє користувачам спільно використовувати спільні ресурси. Сучасні операційні системи, орієнтовані на корпоративний ринок, використовують для організації ресурсів спеціальну мережеву службу, що дає користувачам можливість отримання доступу до ресурсів мережі без необхідності точного знання місця розташування цих ресурсів. Мова йде про службу каталогу (Directory Service) [1]. Каталог при цьому розглядається як глобальне уніфіковане сховище інформації про елементи мережної інфраструктури. Вся інформація про компоненти мережної інфраструктури, в якості яких можуть виступати користувачі, ресурси, мережеві служби і т. п., розміщується в каталозі. Усередині каталогу об'єкти організовуються або відповідно до фізичної, або логічної структури мережі. Нижче перераховані завдання, які служба каталогу дозволяє вирішити адміністратору.

- **Управління мережними ресурсами.** Оскільки задача надання ресурсів в загальне користування є основною, заради чого комп'ютери об'єднуються в мережу, необхідно, щоб користувачі отримували доступ до необхідних ресурсів найбільш ефективним способом. Служба каталогу полегшує користувачам пошук потрібних ресурсів, приховуючи від них подробиці реалізації механізму пошуку. Користувач формулює запит, а служба каталогу локалізує необхідний ресурс.

- **Управління користувачами.** Кожному користувачеві поставлений у відповідність певний набір характеристик, що дозволяє персоналізувати його

діяльність в мережі. Це дає можливість керувати доступом до мережних ресурсів на рівні користувачів. При цьому служба каталогу розглядає користувачів в якості звичайних об'єктів каталогу, що дає можливість організовувати їх у відповідності зі структурою мережі (логічною або фізичною).

•**Управління додатками.** В залежності від того, на рішення яких конкретно завдань орієнтуються користувачі, на їх комп'ютерах може бути розгорнуто різне програмне забезпечення. У невеликій локальній мережі здійснення контролю використовуваного програмного забезпечення не вимагає від адміністратора особливих зусиль. У разі великої корпорації на передній план виходить завдання по централізованому управлінню програмним забезпеченням, включаючи розгортання нових програм і виконання оновлення існуючих.

•**Управління службами.** При побудові мережі адміністратору доводиться також вирішувати питання, пов'язані з конкретним способом її організації. Наприклад, при побудові мережі на основі протоколів TCP/IP необхідно вирішити, яким чином буде здійснюватися виділення IP–адрес. Необхідно розробити угоду про мережеві імена і організувати процес їхнього співвідношення з відповідними IP–адресами. Більшість мережних служб може бути інтегровано зі службою каталогу, що дозволить більш ефективно організувати функціонування цих служб.

Практично всі виробники корпоративних операційних систем пропонують споживачам свої реалізації служби каталогу. Компанія Microsoft пропонує свою версію служби каталогу, названу Active Directory [4]. Вперше ця служба каталогу була реалізована в складі операційної системи Windows Server 2000. Оновлена версія Active Directory включена в Windows Server 2003. Концептуально ці версії практично не відрізняються, тому найчастіше можна говорити про домени Active Directory, маючи на увазі їх реалізацію на базі систем Windows Server 2000/2012.

Служба каталогу Active Directory базується на відкритих стандартах [1, 4]:

- протокол LDAP;
- система доменних імен (Domain Name System, DNS);
- протокол автентифікації Kerberos v5.

Ці стандарти (особливо LDAP) визначили термінологію, використовувану в архітектурі Active Directory, тому спочатку ми коротко розглянемо їх особливості та взаємодію зі службою Active Directory.

Протокол LDAP

Для кращого розуміння ролі протоколу LDAP розглянемо основні ідеї специфікації X.500. Дана специфікація була розроблена Міжнародним консультаційним комітетом з телефонії і телеграфії (Consultative Committee for International Telephone and Telegraph, CCITT) спільно з Міжнародною організацією зі стандартизації (International Standardization Organization, ISO). В рамках специфікації X.500 визначається ряд понять:

- системний агент каталогу (Directory System Agent, DSA) являє собою базу даних, в якій зберігається інформація каталогу. База даних має ієрархічну організацію і дозволяє швидко і ефективно здійснювати пошук необхідних даних;
- агент користувача каталогу (Directory User Agent, DUA) забезпечує функціональність доступу до каталогу, яка може бути реалізована в різних користувальницьких додатках;
- протокол доступу до каталогу (Directory Access Protocol, DAP) контролює процес взаємодії між системним і призначеним для користувача агентами каталогу.

Протокол DAP є досить громіздким і складним. Тому пізніше було запропоновано кілька його модифікацій, що забезпечують більш простий і швидкий спосіб доступу до каталогу. Однією з таких модифікацій є протокол Lightweight Directory Access Protocol (LDAP – Полегшений протокол доступу до каталогу), вперше описаний в рамках специфікації RFC 1487. На даний

момент є три версії цього протоколу. Версія 2 описана в рамках RFC 1777, а версія 3 в специфікації RFC 2251.

Протокол LDAP забезпечує доступ до каталогу, розробленому відповідно до рекомендацій стандарту X.500. Протокол являє собою стандартний засіб реалізації доступу та оновлення інформації в каталозі для програм. Протокол LDAP є частиною стеку протоколів TCP/IP, що й стало однією з причин його популярності.

Інша ключова особливість протоколу LDAP, що забезпечила йому широке поширення, полягає в тому, що протокол не вимагає від каталогу повної сумісності зі специфікацією X.500. Основна вимога – служба каталогу повинна підтримувати систему іменування X.500. Це дуже важливий факт, оскільки, всупереч широко поширеній помилці, служба каталогу Active Directory не є X.500 – каталогом. Розробники компанії Microsoft взяли за основу інформаційну модель X.500 і реалізували підтримку протоколу LDAP. Це дозволило забезпечити необхідний рівень сумісності з більшістю існуючого програмного забезпечення, що в умовах гетерогенних середовищ є одним з найважливіших факторів. Доступ до вмісту каталогу Active Directory по протоколу LDAP може здійснюватися за допомогою будь–якого LDAP–клієнта. При цьому використання протоколу LDAP не є єдино можливим способом доступу до каталогу Active Directory.

Специфікація протоколу LDAP базується на чотирьох моделях.

- Інформаційна модель (Information Model) описує структуру каталогу і інформації, що міститься в ньому.
- Модель іменування (Naming Model) описує схему організації інформації в каталозі та використовувані схеми іменування та ідентифікації об'єктів каталогу.
- Функціональна модель (Functional Model) визначає дії, які можуть бути здійснені над інформацією, розміщеною в каталозі.
- Модель безпеки (Security Model) описує механізми захисту інформації, розміщеної у каталозі.

Розуміння цих моделей необхідно як для ефективного використання служб Active Directory в цілому, так і для роботи з багатьма системними утилітами та програмами. Розуміння моделей, на яких базується протокол LDAP, необхідно також і для написання багатьох адміністративних сценаріїв.

Інформаційна модель Active Directory

Об'єкти і дерево каталогу

Основним структурним компонентом каталогу є елемент (entry), який в термінології Active Directory називається об'єктом (object). Об'єкти є фундаментальними одиницями, якими маніпулює служба каталогу. При цьому кожен об'єкт характеризує деяку окрему сутність (наприклад, принтер, комп'ютер, спільно використовувану теку або користувача) [4].

Виділяють об'єкти двох типів – контейнерного та неконтейнерного типу. Об'єкти контейнерного типу здатні виступати в якості батьківських об'єктів і можуть бути використані для розміщення інших об'єктів. Напрошується аналогія з каталогами файлової системи, в яких можуть бути розміщені файли та інші каталоги. Об'єкти контейнерного типу використовуються для організації об'єктів за якоюсь ознакою. Наприклад, всі об'єкти, асоційовані з користувачами, розміщуються всередині об'єкта контейнерного типу. Об'єкти, асоційовані з комп'ютерами, розміщуються в іншому об'єкті контейнерного типу. Такий підхід дозволяє впорядкувати об'єкти та полегшити управління ними.

Безліч об'єктів, що містяться в безлічі вкладених контейнерів, організовано в ієрархічну структуру, яка в термінології X.500 називається інформаційним деревом каталогу (Directory Information Tree, DIT). Листям цього дерева завжди виступають об'єкти неконтейнерного типу, в той час як у якості вузлів дерева (node) виступають об'єкти контейнерного типу.

Кожну гілку дерева, разом з усією сукупністю породжених нею гілок, можна розглядати окремо як самостійне дерево. Така сукупність називається прилеглим піддеревом (contiguous subtree). Можна уявити простір імен каталогу у вигляді безлічі прилеглих піддерев. Фрагменти, що представляють

собою закінчені і безперервні прилеглі піддерева, називаються контекстами імен (naming context). Самий верхній елемент в ієрархії об'єктів каталогу в термінології X.500 називають коренем дерева. Роль кореня інформаційного дерева каталогу в специфікації X.500 грає об'єкт rootDSE.

Атрибути

Кожен об'єкт каталогу складається з набору атрибутів (attributes), кожен з яких містить частинку інформації, що характеризує об'єкт [4]. Так, наприклад, в якості атрибутів екземпляра класу "користувач" можуть виступати ім'я і прізвище користувача, а також ім'я відповідного йому облікового запису. У документації Microsoft часто називає атрибутами властивості (properties) об'єкта. Атрибути можуть бути обов'язковими (mandatory) або необов'язковими (optional). Значення обов'язкових атрибутів повинні бути явно визначені в процесі створення об'єкта.

З кожним атрибутом в схемі пов'язане поняття синтаксису (syntax), який, за своєю суттю, є характеристикою атрибуту. Синтаксис визначає тип значення атрибуту (число, рядок), порядок проходження байтів і правила порівняння (matching rules), використовувані для порівняння атрибутів даного типу. Служба каталогу Active Directory допускає додавання описів нових атрибутів і зміну існуючих. Однак додавання нових синтаксисів, так само як і зміна існуючих, забороняється. Визначаючи новий атрибут, адміністратор може тільки вибрати необхідний синтаксис зі списку вже існуючих.

Схема каталогу

Визначення всіх класів об'єктів, а також сукупність правил, що дозволяють управляти структурою каталогу і його вмістом, зберігаються в спеціальній ієрархічній структурі, яка називається схемою каталогу (schema) [4]. Щоб створити в каталозі об'єкт нового типу, необхідно, перш за все, додати в схему визначення нового класу об'єктів. При цьому прийнято говорити про розширення (extending) схеми. Можливість розширення схеми фактично означає розширюваність каталогу шляхом його адаптації для зберігання нових типів об'єктів.

Інформація схеми також зберігається у вигляді об'єктів двох класів: схеми класів (Class schema) і схеми атрибутів (Attribute schema) [4]. Схема класів об'єднує класи, що визначають типи об'єктів. У схемі атрибутів описуються атрибути, які можуть бути визначені для об'єктів каталогу. Для кожного класу об'єктів в схемі визначаються:

- перелік атрибутів, які обов'язково повинні бути визначені для екземплярів зазначеного класу;
- перелік атрибутів, які можуть бути визначені для екземплярів даного класу;
- сукупність правил, що визначають можливих об'єктів–батьків і об'єктів–нащадків.

Модель іменування LDAP

Однією з умов успішного маніпулювання об'єктами каталогу є однозначна ідентифікація кожного об'єкта. Для іменування та ідентифікації об'єктів в каталозі протокол LDAP використовує механізм відмітних імен (Distinguished Name, DN) [4]. Відмітне ім'я однозначно визначає положення об'єкта в інформаційному дереві каталогу, представляючи інформацію про всі вузли дерева, які необхідно пройти, щоб прийти від даного об'єкта до кореня дерева. Можна провести аналогію з поняттям повного шляху, використовуваним для визначення місця розташування файлу у файловій системі. Нижче наводиться приклад відмітного імені, що ідентифікує об'єкт Tasha, що належить до підрозділу ND домену kpi.ua: DC = ua, DC = kpi, OU = ND, CN = Users, CN = Tasha

Для формування відмітного імені використовуються специфікатори (specifier), що визначають тип об'єкта:

- DC (Domain Component) – специфікатор "складова частина доменного імені";
- OU (Organizational Unit) – специфікатор "організаційна одиниця";
- CN (Common Name) – специфікатор "загальне ім'я".

Назва, яка ідентифікує сам об'єкт, відповідно до термінології LDAP виступає в якості відносного відмітного імені (Relative Distinguish Name, RDN). Відносне відмітне ім'я може повторюватися в рамках усього каталогу. Однак воно має бути унікально в межах батьківського контейнера. Нижче наводиться приклад відносного відмітної імені об'єкта Tasha: CN = Tasha

Механізм відмітних імен LDAP є кращою, але не єдиною схемою іменування об'єктів в Active Directory. Тому нижче ми розглянемо всі інші можливі схеми іменування.

Схеми іменування об'єктів в Active Directory

Протокол LDAP припускає єдиний спосіб ідентифікації об'єктів в каталозі за допомогою відмітних імен. Однак служба каталогу Active Directory дозволяє використовувати цілий ряд додаткових схем іменування, кожна з яких застосовується в певних ситуаціях [4].

Основні імена суб'єктів безпеки

Механізм основних імен (Security principal name, SPN) реалізує спосіб іменування об'єктів каталогу, які розглядаються підсистемою безпеки Windows Server 200x у якості своїх суб'єктів. Основне ім'я суб'єкта системи безпеки визначається в якості одного з атрибутів об'єкта каталогу і має наступний формат: <ім'я_суб'єкта> @ <суфікс_основного_імені> [4].

В якості суфікса основного імені може виступати DNS–ім'я поточного або кореневого домену. Можливо також застосування альтернативних суфіксів, наприклад, lex@ayan.ua або kaizer @kpi. Використовуваний для утворення основного імені суфікс повинен задовольняти правилам побудови доменних імен.

Стосовно об'єктів, асоційованих з користувачами, слід говорити про основне ім'я користувача (User Principal Name, UPN) [4]. Основне ім'я дозволяє спростити процес реєстрації користувачів в мережі на комп'ютерах, що належать до різних доменів. Основне ім'я унікально в межах лісу доменів, тому для реєстрації від користувача не потрібно вказувати домен, до якого він належить.

Інший плюс використання основних імен для ідентифікації об'єктів полягає в тому, що основне ім'я жодним чином не пов'язано з його відмітним ім'ям. Внаслідок цього основне ім'я не змінюється навіть у разі переміщення об'єкта в рамках каталогу.

Повні доменні імена

Повне доменне ім'я (Fully Qualified Domain Name, FQDN) використовується для однозначної ідентифікації об'єктів в просторі доменних імен [5]. Повне доменне ім'я утворюється відповідно до угод про доменні імена. В рамках служби каталогу механізм повних доменних імен використовується для ідентифікації доменів і належних їм комп'ютерів. Стосовно до комп'ютера повне доменне ім'я складається з імені комп'ютера та імені домену. Нижче наводиться приклад повного доменного імені для комп'ютера root, що є частиною домену kpi.ua: root.kpi.ua

Глобальні унікальні ідентифікатори

Відмітне ім'я однозначно визначає об'єкт в каталозі. Проте переміщення об'єкта або його перейменування (так само як і перейменування будь–якого з контейнерів, усередині яких даний об'єкт міститься) призводить до зміни його відмітного імені. Це може призвести до неправильної роботи програм, що використовують відмінні імена для унікальної ідентифікації об'єктів. Завдання унікальної і однозначної ідентифікації об'єкта може бути вирішене за допомогою введення спеціального атрибута, значення якого не змінювалося б при перейменуванні або переміщенні об'єкту. У службі каталогу Active Directory забезпечення унікальності об'єктів досягається за допомогою глобально унікального ідентифікатора (Global Unique Identifier, GLJID), що представляє собою 128–розрядне число [4].

Глобальний унікальний ідентифікатор генерується безпосередньо в момент створення об'єкту в каталозі і є одним з обов'язкових атрибутів, який не може бути змінений ні за яких обставин. У разі зміни відмітного імені глобально унікальний ідентифікатор залишається незмінним, визначаючи конкретний об'єкт каталогу. Цю властивість глобальних ідентифікаторів

можна використовувати при розробці програм, що працюють з об'єктами каталогу.

Імена NetBIOS

До появи служби каталогу Active Directory в якості основного способу іменування об'єктів в операційних системах Windows застосовувалися імена NetBIOS [5]. Більшість програм, розроблених для цього сімейства операційних систем, припускають використання тільки цієї схеми іменування. Дана схема іменування була реалізована в Active Directory з метою збереження зворотної сумісності зі старими операційними системами і розробленими для них додатками.

Ім'я NetBIOS повинна бути унікальною в межах домену та його довжина не повинна перевищувати 15 символів.

Уніфікований покажчик ресурсів LDAP

Протокол LDAP є одним із стандартних методів доступу до каталогу Active Directory. Будь яка LDAP–сумісна програма може звернутися до об'єктів каталогу за допомогою запиту, записаного у форматі уніфікованого покажчика ресурсів LDAP (LDAP Uniform Resource Locator, LDAP URL). Уніфікований покажчик ресурсів LDAP починається з ключового слова LDAP, потім слідує ім'я сервера, що містить копію каталогу, і відмітне ім'я ресурсу. Нижче наводиться приклад запису уніфікованого покажчика ресурсів: LDAP: / / root. kpi.ua / cn = tasha, cn = user, cu = r.d, clc = kpi, dc = ua [4].

Канонічні імена

Замість відмітного імені для визначення положення об'єкта в дереві каталогу можна використовувати так зване канонічне ім'я (canonical name) [4]. Принцип побудови канонічного імені аналогічний принципу формування відмітних імен, за винятком того, що при записі канонічного імені опускаються специфікатори, що позначають тип об'єкта або контейнера. Для вказівки домену в канонічному імені використовується угоду про доменні імена.

Служба DNS

Протокол LDAP являє собою механізм доступу користувачів до каталогу. Однак для того, щоб клієнт зміг підключитися до сервера LDAP і відправити свій запит, він повинен точно знати його розташування в мережі. До цих пір ми не торкалися питання про те, як саме клієнт дізнається про розташування серверу LDAP. Проблема ускладняється тим фактом, що в мережі може бути декілька LDAP–серверів, з якими клієнта з'єднують комунікаційні лінії з різною пропускною здатністю. Крім того інформація, що цікавить клієнта, може розташовуватися не на всіх LDAP–серверах.

Компанія Microsoft запропонувала задіяти Службу доменних імен (Domain Name Systems DNS) в якості засобу виявлення (визначення місцезнаходження) різних мережних служб, наприклад контролерів доменів та Центрів розподілу ключів Kerberos [4, 6]. Слід зауважити, що доменна служба імен традиційно використовується в TCP/IP – мережах для встановлення відповідності між символічними іменами та IP–адресами. Для виявлення мережних служб (сервісів) DNS використовує спеціальний тип ресурсних записів – SRV–записи [5].

Потрібно відразу відзначити два важливих моменти [4]:

- Active Directory вимагає обов'язкового використання служби DNS;
- Active Directory може працювати з будь–якою службою DNS, яка підтримує SRV–записи, дозволяє використання в іменах символу підкреслення ("_") і, бажано (але не строго обов'язково), забезпечує динамічне оновлення ресурсних записів.

Угода про доменні імена, що лежить в основі DNS, використовується як основний спосіб іменування доменів Active Directory. При цьому доменний простір імен Active Directory повністю відображається на простір імен DNS. Іншими словами, ієрархія доменів корпоративної служби DNS аналогічна ієрархії доменів Active Directory.

SRV–записи

Служба доменних імен використовує SRV–записи для визначення місцезнаходження серверів, що надають послуги певних служб. Кожний SRV–запис, що використовується для роботи з Active Directory, являє собою DNS–псевдонім служби, записаний у форматі: _Service._Protocol.DnsDomainName, де [4, 6]:

•Service – назва мережної служби, яка доступна на даному сервері (наприклад: ldap, kerberos, gc, kpasswd);

•Protocol – протокол, який клієнти можуть використовувати для підключення до зазначеної службі (tcp, udp);

•DnsDomainName – доменне ім'я домену, до якого належить зазначений сервер.

Наприклад, для LDAP–сервера, що належить до домену kpi.ua, DNS–ім'я служби буде виглядати наступним чином: _ldap._tcp. kpi.ua.

SRV–записи реєструються в базі даних DNS–сервера безпосередньо контролерами домену. За замовчуванням кожен контролер домену реєструє в базі даних DNS п'ятнадцять різних SRV–записів. Якщо контролер домену виконує також функції сервера глобального каталогу, в базі даних служби DNS реєструється двадцять SRV–записів.

Якщо на контролері домену розміщені репліки розділів програм, у базі даних служби DNS додатково реєструються три ресурсних записи – одна A–типу і дві SRV–типу для кожної репліки. Це записи _ldap._tcp. <Ім'я_розділу> І _ldap._tcp. <Ім'я_сайту>. _sites. <Ім'я_розділу>. У поточній версії Active Directory ці записи не використовуються службою каталогу. Однак вони дозволяють додаткам звертатися до служби доменних імен для пошуку сервера, що містить розділи додатка.

Протокол автентифікації Kerberos

Протокол автентифікації Kerberos є основним механізмом автентифікації, використовуваним в середовищі доменів Active Directory на базі Windows Server 2000/2012. У доменах Active Directory використовується

п'ята версія протоколу Kerberos [4], специфікація якого визначена в стандарті RFC 1510.

Проблема автентифікації користувача полягає в необхідності перевірки того факту, що він є тим, за кого себе видає. Відомо безліч різних способів перевірки автентичності особистості, які спрощено можна розділити на дві групи:

- перевірка особи за фактом відповідності деяким індивідуальним характеристикам людини (перевірка відбитків пальців, знімків райдужки ока, код ДНК і т. д.). Для застосування цієї групи методів автентифікації необхідно задіяти спеціальне обладнання;
- перевірка особи за фактом знання деякого секрету (паролі, цифрові комбінації і послідовності). В даному випадку під секретом розуміється якась символьна або цифрова послідовність, факт знання якої дозволяє судити про справжність користувача. Зазначені методи автентифікації найбільш прості в технологічному виконанні. Саме ці методи отримали широке поширення в сучасних операційних системах. Протокол автентифікації Kerberos також відноситься до цієї групи методів.

Компоненти служби Active Directory

Перейдемо від термінології до розгляду механізмів і підсистем, які складають архітектуру Active Directory. Для початку розглянемо структуру служби каталогу [4].

Active Directory являє собою сукупність служб, що обслуговують звернення користувачів до каталогу. Каталог розглядається як розподілена база даних, в якій зберігаються відомості про об'єкти мережі. Користувач не може працювати з каталогом безпосередньо, а взаємодіє з ним через цілий ряд підсистем і механізмів, які в сукупності називаються службою каталогу. З точки зору обслуговування звернень користувачів підсистеми служби каталогу утворюють деяку структуру, у якій компанія Microsoft виділяє п'ять рівнів.

1. Інтерфейси доступу до каталогу. Це самий верхній рівень служби каталогу, що відповідає за безпосередню взаємодію з програмами користувачів. На даному рівні описані всі можливі методи доступу до каталогу. Можна розглядати даний рівень як набір прикладних інтерфейсів програмування (Application Program Interfaces, API), за допомогою яких користувачі можуть взаємодіяти з системним агентом каталогу.

2. Системний агент каталогу (Directory System Agent, DSA). Будь–який клієнт, що підключається до каталогу, взаємодіє з DSA. Ми вже стикалися з системним агентом каталогу при розгляді специфікації X.500. Всі запити, що надходять від користувачів, обробляються агентом, він же повертає клієнтам результати запитів.

3. Рівень бази даних (Database Layer). Даний рівень служби каталогу здійснює перетворення запитів користувачів у формат, прийнятний для розширюваної оболонки сховища. Це перетворення необхідно, оскільки розширювана оболонка сховища маніпулює даними в уявленні реляційної бази даних. Однак вищестоящі рівні представляють вміст каталогу у вигляді деревовидної структури.

4. Розширювана оболонка сховища (Extensible Storage Engine, ESE). Розширювана оболонка сховища являє собою механізм управління реляційних сховищем даних, у формі якого реалізований каталог. Компанія Microsoft розглядає ESE в якості стандартного механізму управління реляційними сховищами і широко застосовує її в різних своїх продуктах. ESE бере на себе всі обов'язки з обслуговування запитів, що надходять від користувачів (і перетворених у відповідний формат на вищому рівні) на вилучення даних з каталогу і маніпуляції ними. Можна уявити ESE як систему управління базою даних (СУБД). При цьому в якості бази даних виступає безпосередньо сховище даних.

5. Файли сховища (Data Store files). Сховище даних реалізовано у вигляді набору файлів, які використовуються безпосередньо для організації зберігання даних каталогу. Оскільки інформація, що міститься в цих файлах, критично

важлива для функціонування Active Directory, доступ до них має тільки розширювана оболонка сховища. В даному випадку можна говорити про самий нижчий рівень операцій в рамках служби каталогу. Саме на цьому рівні відбувається маніпуляція з даними, що містяться в каталозі.

Доменна структура Active Directory

Поняття домену є ключовим для Active Directory [4]. Домени виступають в якості основного засобу формування простору імен каталогу. Інші рівні формування структури каталогу зосереджуються або на адміністративній ієрархії, або на фізичній структурі мережі.

Домени

Операційні системи Windows традиційно використовували поняття "домену" для логічного об'єднання комп'ютерів, які спільно використовують єдину політику безпеки. Домен традиційно виступає в якості основного способу створення областей адміністративної відповідальності. Як правило, кожним доменом управляє окрема група адміністраторів. У Active Directory поняття домену було розширено. Перерахуємо завдання, які можуть бути вирішені шляхом формування доменної структури.

- Створення областей адміністративної відповідальності. Використовуючи доменну структуру, адміністратор може поділити корпоративну мережу на області (домени), керовані окремо один від одного. Кожен домен управляється своєю групою адміністраторів (адміністратори домену). Однак хотілося б ще раз відзначити, що існують і інші способи формування адміністративної ієрархії (організація підрозділів), мова про які піде далі. З іншого боку, побудова доменної ієрархії є відмінним способом реалізації децентралізованої моделі управління мережею, коли кожен домен управляється незалежно від інших. Для цього кожну адміністративну одиницю необхідно виділити в окремий домен.

- Створення областей дії політики облікових записів. Політика облікових записів визначає правила застосування користувачами облікових записів і зіставлених їм паролів. Зокрема задається довжина пароля, кількість невдалих

спроб введення пароля до блокування облікового запису, а також тривалість подібної блокування. Оскільки ці питання вирішуються організаційно на рівні всього домену, даний комплекс заходів прийнято називати політикою облікових записів.

•Розмежування доступу до об'єктів. Кожен домен реалізує власні настройки безпеки (включаючи ідентифікатори безпеки і списки контролю доступу). Рознесення користувачів в різні домени дозволяє ефективно управляти доступом до важливих ресурсів. З іншого боку, застосування довірчих відносин (trust relationships) дозволяє забезпечити користувачам одного домену доступ до ресурсів інших доменів.

•Створення окремого контексту імен для національних філій. У випадку, якщо компанія має філії, розташовані в інших країнах, може знадобитися створити окремий контекст імен для кожної такої філії. Можна відобразити в імені домену географічне або національне місцеположення філії.

•Ізоляція трафіку реплікації. Для розміщення інформації про об'єкти корпоративної мережі використовуються доменні розділи каталогу. Кожному домену відповідає свій розділ каталогу, званий доменним. Всі об'єкти, що відносяться до деякого домену, поміщаються у відповідний розділ каталогу. Зміни, зроблені в доменному розділі, реплікуються виключно в межах домену. Відповідно, виділення віддалених філій в окремі домени може дозволити істотно скоротити трафік, викликаний реплікацією змін вмісту каталогу. Необхідно зазначити, однак, що домени є не єдиним (і навіть не основним) способом формування фізичної структури каталогу. Того ж самого результату адміністратор може добитися за рахунок використання механізму сайтів.

•Обмеження розміру копії каталогу. Кожен домен Active Directory може містити до мільйона різних об'єктів. Тим не менш, реально використовувати домени такого розміру непрактично. Наслідком великого розміру домену є великий розмір каталогу. Відповідно, величезним виявляється навантаження на сервери, що є носіями подібного каталогу. Адміністратор може використовувати домени як засіб регулювання розміру каталогу.

Ієрархія доменів

Для іменування доменів використовується угода про доменні імена. Ім'я домену записується у формі повного доменного імені (Fully Qualified Domain Name, FQDN), яке визначає положення домену щодо кореня простору імен. Повне доменне ім'я утворюється з імені домену, до якого додається ім'я батьківського домену. Так, наприклад, для домену fel, що є дочірнім по відношенню до домену kpi.ua, повне доменне ім'я буде записано в формі fel. kpi.ua.

Вибір подібної схеми іменування дозволив формувати доменний простір імен, аналогічне простору імен служби DNS. Відображення доменів Active Directory на домени DNS дозволило спростити процеси пошуку серверів служб та дозволу імен, здійснювані серверами DNS у відповідь на запити клієнтів служби каталогу [4].

Сукупність доменів, що використовують єдину схему каталогу, називається лісом доменів (forest) [4]. Строго кажучи, домени, що входять в ліс, можуть не утворювати "безперервного" простору суміжних імен. Тим не менш, так само як і у випадку простору імен DNS, домени Active Directory можуть утворювати безперервний простір імен. У цьому випадку вони зв'язуються між собою відносинами "батько–нащадок". При цьому ім'я дочірнього домену обов'язково включає в себе ім'я батьківського домену. Сукупність доменів, що утворюють безперервний простір суміжних імен, називають деревом доменів (domain tree). Ліс може складатися з довільної кількості дерев доменів.

Перше створене в лісі доменів дерево є кореневим деревом. Кореневе дерево використовується для посилання на ліс доменів. Перший створений в дереві домен називається кореневим доменом дерева (tree root domain), який використовується для посилання на дане дерево. Цілком очевидно, що кореневий домен є визначальним для всього дерева [4].

Відповідно, перший домен, створений в лісі доменів, називається кореневим доменом лісу (forest root domain) [4]. Кореневий домен лісу відіграє

дуже важливу роль, зв'язуючи дерева, що утворюють ліс доменів, воєдино і тому не може бути видалений. Зокрема, він зберігає інформацію про конфігурацію лісу і дерев доменів, що його утворюють.

Особливу увагу необхідно приділити питанню іменування доменів і, зокрема, кореневого домену. Для кореневого домену краще всього використовувати доменне ім'я другого рівня. Як буде показано нижче, саме домени другого рівня використовуються механізмом маршрутизації доменних суфіксів (у разі взаємодії двох лісів доменів).

Контролери домену

Сервери Windows Server 200x, на яких функціонує екземпляр служби каталогу Active Directory, називаються контролерами домену (domain controller, DC) [4]. Контролери домену є носіями повнофункціональних копій каталогу. Стосовно до Windows Server 200x контролери домену виконують завдання, перераховані нижче.

- Організація доступу до інформації, що міститься в каталозі, включаючи управління цією інформацією і її модифікацію. Контролер домену може розглядатися як LDAP–сервер, що здійснює доступ користувача до LDAP–каталогу.

- Синхронізація копій каталогу. Кожен контролер домену є суб'єктом підсистеми реплікації каталогу. Будь–які зміни, здійснювані в деякій копії каталогу, будуть синхронізовані з іншими копіями.

- Централізоване тиражування файлів. Служба реплікації файлів, що функціонує на кожному контролері домену, дозволяє організувати в корпоративній мережі централізоване тиражування необхідних системних і користувальницьких файлів (включаючи шаблони групової політики).

- Автентифікація користувачів. Контролер домену здійснює перевірку повноважень користувачів, що реєструються на клієнтських системах. Кожен контролер домену Windows Server 200x може розглядатися як Центр розподілу ключів (KDC) Kerberos.

Особливо слід зазначити той факт, що всі контролери домену володіють можливістю внесення змін у власну копію каталогу. Це дозволяє розглядати будь–який контролер домену як точку адміністративного впливу на корпоративну мережу. Практично всі адміністративні утиліти працюють в контексті якогось контролера домену. Це означає, що адміністратор може здійснювати конфігурування служби каталогу та мережі, підключившись до будь–якого контролеру домену Active Directory.

Спеціалізовані ролі контролерів домену

Служба каталогу Active Directory використовує модель реплікації з безліччю рівноправних учасників (multimaster replication) [4]. З точки зору підсистеми реплікації не має значення, який з носіїв здійснює зміни в каталозі. Зміни можуть бути зроблені в будь–якій з копій каталогу.

Однак існує певний клас операцій, які повинні виконуватися тільки одним контролером домену. Цей клас операцій називається операціями з одним виконавцем (Flexible Single–Master Operations, FSMO).

Якщо залучити до виконання подібних операцій більше одного контролера домену, не можна виключати можливість конфліктів. У певних випадках подібні конфлікти можуть призвести до порушення цілісності каталогу.

Є два типи операцій з одним виконавцем, які прийнято називати ролями контролерів домену [4]. Від першого типу ролей вимагається унікальність виконавця в межах усього лісу доменів. Роль даного типу може бути покладена тільки на один контролер в лісі доменів. До іншого типу ролей пред'являється вимога унікальності виконавця тільки в межах домену. У кожному домені може бути тільки один виконавець ролі. Таким чином, в рамках лісу доменів виконавців кожної з подібних ролей буде стільки ж, скільки і доменів, що утворюють ліс.

Розглянемо п'ять існуючих спеціалізованих ролей [4].

- **Власник схеми (Schema Master).** Контролер домену, який здійснює зміни в схемі каталогу. Існування тільки одного власника (хазяїна) схеми в

межах лісу доменів виключає можливість конфліктів, пов'язаних з її зміною. Відмова власника схеми призводить до того, що виконання операції розширення схеми стане неможливим.

- **Власник доменних імен (Domain Naming Master).** Контролер домену, що відстежує зміни в структурі лісу доменів. Будь–яка зміна простору імен доменів Active Directory (додавання, видалення, а також перейменування доменів) здійснюється виконавцем цієї ролі. Тим самим гарантується цілісність простору імен і унікальність його компонентів. Відмова виконавця цієї ролі призводить до того, що будь–яка зміна простору імен каталогу стане неможливим.

- **Власник ідентифікаторів (Relative ID Master).** Контролер домену, який здійснює генерацію ідентифікаторів (глобальні ідентифікатори, ідентифікатори безпеки і т. п.). Від ідентифікатора в першу чергу потрібно унікальність. Найпростіший спосіб гарантувати унікальність ідентифікаторів, що генеруються, – покласти обов'язок виконавця даної ролі на один контролер в домені. Відмова виконавця даної ролі призводить до того, що створення об'єктів в домені стане неможливим.

- **Емулятор основного контролера домену (PDC Emulator).** Якщо домен знаходиться на функціональному рівні Windows 2000 mixed, емулятор основного контролера домену (PDC) використовується для забезпечення реплікації змін між контролерами домену Windows NT і Windows Server 200x. Виконавець ролі фактично емулює домен Windows NT. Оскільки в домені Windows NT допустимо наявність тільки одного основного контролера, його емулятор в домені Active Directory також може бути тільки один. На інших функціональних рівнях емулятор основного домену використовується для зміни паролів облікових записів, а також відіграє провідну роль у процесі синхронізації системних годинників всіх контролерів домену. Емулятор PDC за замовчуванням вибирається оснащенням Group Policy Object Editor. Тому, якщо виконавець даної ролі недоступний, адміністратор може зіткнутися з серйозними проблемами при редагуванні об'єктів групової політики.

•**Власник інфраструктури (Infrastructure Master).** Контролер домену, який відповідає за структуру каталогу. У процесі видалення або переміщення об'єктів один з контролерів домену повинен взяти на себе обов'язки по зберіганню посилання на дані об'єкти до тих пір, поки ці зміни не будуть реплікуватись на всі інші контролери домену. Якщо в домені є декілька контролерів домену, бажано не поєднувати функції виконавця даної ролі і сервера глобального каталогу. Краще рознести ці функції на різні контролери домену, які обов'язково повинні бути з'єднані високошвидкісним каналом. Якщо в домені є тільки один контролер, цією вимогою можна знехтувати.

За замовчуванням усі спеціалізовані ролі покладаються на перший контролер домену, встановлений в новому лісі доменів. Аналогічним чином, в процесі створення нового домену перший встановлений контролер буде обраний в якості виконавця ролей, унікальних в межах домену. Пониження контролера домену, обраного в якості виконавця спеціалізованої ролі, до виділеного сервера призводить до того, що ролі передаються іншому контролеру домену.

При необхідності адміністратор може в будь–який момент передати обов'язки виконавця будь–якої ролі іншому контролеру домену. Це може знадобитися, наприклад, в ситуації, коли планується оновлення апаратного забезпечення сервера. У процесі нормальної передачі ролі поточний виконавець спеціалізованої ролі звільняється від виконання специфічних обов'язків і стає звичайним контролером домену. Одночасно з цим на інший контролер домену, обраний на роль нового виконавця, покладаються обов'язки виконавця спеціалізованою ролі.

Якщо адміністратор не може забезпечити доступність сервера, який є виконавцем спеціалізованої ролі, або відновлення його працездатності не представляється можливим, він повинен покласти обов'язки виконання даної ролі на інший контролер домену. Процес примусового передавання функцій виконавця спеціалізованою ролі іншому контролеру домену називається захопленням ролі (seize).

Довірчі відносини

Довірчі відносини (trusts) являють собою зв'язок, що встановлюється між доменами, що дозволяє користувачам одного домену автентифікуватися контролером іншого домену [4]. Наявність механізму довірчих відносин дозволяє організовувати сукупність доменів в деяку структуру. У цій структурі домени зв'язуються між собою певним чином відносинами довіри.

Довірчі відносини реалізуються в рамках механізму автентифікації. Суть довірчих відносин між двома доменами зводиться до того, що домен, що довіряє, (trusting domain) довіряє процес автентифікації довіреному домену (trusted domain). Користувач, автентифікований довіреним доменом, може отримати доступ до ресурсів в недовіреному домені.

Служба каталогу Active Directory допускає створення як односторонніх, так і двосторонніх довірчих відносин. Односторонні довірчі відносини реалізуються за допомогою механізму автентифікації NTLM. Двосторонні довірчі відносини будуються на основі протоколу автентифікації Kerberos v5 і мають властивість транзитивності [4].

Транзитивність довірчих відносин припускає наскрізну автентифікацію користувачів в ланцюжку доменів, пов'язаних між собою подібними відносинами. Наприклад, якщо домен А довіряє домену В, а домен В довіряє домену С, то між доменами А і С автоматично встановлюються довірчі відносини (ці відносини неявні). Односторонні довірчі відносини NTLM не володіють властивостями транзитивності. Для створення відносин повної довіри між п'ятьма доменами необхідно буде встановити двадцять односторонніх довірчих відносин. Аналогічного результату можна досягти за допомогою всього лише чотирьох двосторонніх транзитивних довірчих відносин.

Архітектура Windows Server 200x дозволяє використовувати довірчі транзитивні відносини як для з'єднання доменів в межах одного лісу, так і для з'єднання різних лісів доменів. Крім того, можуть бути встановлені довірчі відносини між різними областями (Kerberos realms).

Всі підтримувані типи довірчих відносин перераховані в табл. 1.3 [4].

Таблиця 1.3 – Довірчі відносини, підтримувані доменами на базі Windows Server 20xx

Довірчі відносини	**Характеристика**	**Опис**
Довірчі відносини всередині дерева	Двосторонні, транзитивні	Встановлюються автоматично при створенні в дереві нового домену. В рамках дерева доменів відносини описуються схемою "батько–нащадок"
Довірчі відносини всередині лісу	Двосторонні, транзитивні	Встановлюються автоматично при створенні в існуючому лісі нового дерева доменів. Фактично довірчі відносини встановлюються між кореневим доменом лісу і створюваним доменом, який буде кореневим для нового дерева
Довірчі відносини між лісами доменів	Двосторонні або односторонні, транзитивні	Встановлюються адміністраторами лісів доменів вручну. При цьому адміністратори самі вирішують, будуть відносини двосторонніми або однобічними
Перехресні (shortcut) довірчі відносини	Односторонні або двосторонні, транзитивні	Встановлюються між доменами різних дерев, що належать до одного лісі. Необхідність довірчих відносин даного типу не завжди очевидна, оскільки між доменами, що належать до одного лісу, через кореневі домени автоматично встановлюються неявні довірчі відносини. Перехресні відносини довіри дозволяють підвищити ефективність взаємодії між двома доменами, зменшуючи шлях довіри (trust path). Шлях довіри – послідовність переходів між доменами, довіряють один одному, необхідна для автентифікації запиту. У разі неявних довірчих відносин цей шлях може включати в себе кілька переходів, які перехресні стосунки довіри дозволяють уникнути
Довірчі відносини із зовнішніми доменами	Односторонні або двосторонні, нетранзитивні	Встановлюються між доменами, що належать до різних лісів, або між доменом Windows Server 200x і доменом Windows NT. Цей тип довірчих відносин може використовуватися для з'єднання лісів, коли неможливо встановити відносини довіри між лісами в цілому (внаслідок того, що один або обидва ліси не перебувають на функціональному рівні Windows Server 200x)
Довірчі відносини між областями Kerberos	Односторонні або двосторонні, транзитивні або нетранзитивні	Встановлюються між Windows Server 200x–доменом і областю Kerberos v5, реалізованої не на базі Windows. Даний тип довірчих відносин може використовуватися для забезпечення наскрізної автентифікації на Windows і UNIX–системах

Довірчі відносини всередині лісу і всередині дерева доменів встановлюються системою автоматично, в процесі створення домену або дерева доменів. Адміністратор не може якось відкликати їх або видалити. Всі інші типи довірчих відносин створюються адміністратором вручну.

Довірчі відносини між лісами доменів

Процес створення відносин між лісами доменів заслуговує особливої уваги. Організація взаємодії двох лісів доменів, з'єднаних між собою відносинами довіри, має свої специфічні моменти.

Розглянемо процес автентифікації користувачів. Коли користувач запитує доступ до ресурсів домену, розташованого в довіреному лісі доменів, активізується механізм, що отримав назву маршрутизації суфіксів (name suffix routing). Цей механізм працює тільки з доменними іменами другого рівня (такими, наприклад, як kpi.ua, ayan.ua). Домени третього рівня (наприклад, fel.kpi.ua) і нижче механізмом маршрутизації суфіксів не підтримуються. Механізм маршрутизації суфіксів гарантує, що всі запити автентифікації, адресовані домену другого рівня, будуть маршрутизуватися відповідному домену [1, 4].

Дочірні домени, що підключаються до доменів другого рівня, успадковують від них інформацію, необхідну для маршрутизації суфіксів. Тому вони також зможуть виконати маршрутизацію запиту на автентифікацію користувача.

Підрозділи (Організаційні одиниці)

Підрозділи, або організаційні одиниці (organizational unit) являють собою об'єкти каталогу контейнерного типу, за допомогою яких адміністратор може організувати об'єкти відповідно до деякої логічної структурою корпоративної мережі. Основне призначення підрозділів полягає в логічній організації мережних ресурсів з метою найбільш ефективного управління ними. Всі об'єкти, розміщення всередині підрозділу, розглядаються як деякий адміністративний блок [4].

Розглянемо завдання, для вирішення яких можуть бути застосовані організаційні одиниці [4].

•**Формування адміністративної ієрархії.** Механізм підрозділів поряд з доменами може бути використаний як засіб формування адміністративної ієрархії. Адміністратори рівня корпорації приймають глобальні рішення в рамках усього лісу доменів. Адміністратори доменів здійснюють управління доменами. При цьому вони передають (делегують) певним користувачам частину своїх повноважень на рівні підрозділів – це повноваження на управління об'єктами, розташованими всередині цих підрозділів. При цьому користувачі, яким делеговані виконавчі повноваження, можуть реалізувати їх виключно всередині свого підрозділу.

•**Відображення організаційної структури підприємства.** Механізм підрозділів може використовуватися для організації об'єктів каталогу відповідно до їх географічного розташування або приналежності до деякого структурному підрозділу підприємства. Наприклад, реалізувавши обчислювальну мережу університету у вигляді домену, можна створити для кожного факультету свій підрозділ. Для кафедр, наявних на кожному факультеті, можна також створити свої підрозділи.

•**Управління процесом застосування групових політик.** Групові політики можуть бути застосовані на трьох рівнях: на рівні домену, на рівні сайту та на рівні підрозділів. Якщо необхідно в рамках одного домену реалізувати кілька різних групових політик, можна використовувати ієрархію підрозділів.

•**Розподіл відповідальності.** Адміністратор може розмістити об'єкти одного класу в окремих підрозділах. Такий крок дозволяє розподілити обов'язки по управлінню домену між адміністраторами нижчої ланки. Наприклад, один з них відповідальний за керування користувачами, другий – за керування комп'ютерами.

•**Управління доступом до об'єктів.** Адміністратор може призначати права доступу по підрозділам. Відповідно, адміністратор може керувати

рівнем доступу до об'єктів каталогу, помістивши їх всередину підрозділу і надавши окремим категоріям користувачів відповідні дозволи на доступ до його вмісту.

Кожен домен реалізує власну ієрархію підрозділів. Підрозділи, що належать до різних доменів, ніяк не пов'язані між собою.

Застосування підрозділів дозволяє розмістити всі об'єкти в одному доменному контексті імен, незалежно від складності ієрархії підрозділів. Як наслідок, переміщення об'єктів (особливо таких, як користувачі) між підрозділами вимагає менших адміністративних зусиль, ніж переміщення між доменами. З іншого боку, поділ простору імен на доменні контексти дозволяє скоротити трафік, викликаний реплікацією.

Групи

Підрозділи є не єдиним механізмом, який адміністратор може використовувати для групування об'єктів за певною ознакою. Об'єкти, асоційовані з користувачами, комп'ютерами та контактною інформацією, можуть бути об'єднані в спеціальні групи (groups) [4]. Це дозволяє спростити процес управління, оскільки адміністратор може в процесі управління послатися на всю групу, а не вказувати окремі об'єкти. Найбільш часто групи згадуються в контексті об'єднання користувачів. Тим не менш, необхідно завжди пам'ятати, що група може включати в себе об'єкти наступних типів:

- користувачі (users);
- комп'ютери (computers);
- контакти (contacts).

Active Directory дозволяє об'єднувати об'єкти в групи двох типів: групи безпеки (security groups) і групи розсилки (distributed groups).

Групи безпеки розглядаються підсистемою безпеки в якості своїх суб'єктів. Іншими словами, вони можуть використовуватися для розмежування доступу до ресурсів мережі. Видаючи дозвіл на доступ до об'єкта певної групи, адміністратор автоматично дозволяє доступ до даного об'єкту всім членам даної групи.

Групи розсилки спочатку орієнтувалися на користування поштовою системою, як засіб одночасної передачі повідомлення деякого колективу користувачів. В даний час механізм груп розсилок Active Directory використовується в поштовій системі Microsoft 2000 Exchange.

З кожною групою об'єктів пов'язане поняття області дії (group scope). Область дії визначає, в якій частині лісу доменів на дану групу можна посилатися. Існує три області дії груп:

- доменна зона дії (domain local scope);
- глобальна область дії (global scope);
- універсальна область дії (universal scope).

Область дії групи може бути різною залежно від того, на якому функціональному рівні знаходиться домен. На функціональному рівні Windows 2000 mixed доступні лише дві області дії груп: доменна і глобальна.

На функціональному рівні Windows 2000 mixed також обмежена можливість використання механізму вкладених груп (nested groups). Дозволяється тільки включати групи з глобальної областю дії в групи з доменної областю дії. Подібні обмеження пояснюються вимогами збереження сумісності з контролерами домену Windows NT, які використовують описаний формат груп користувачів.

На функціональних рівнях домену Windows 2000 native і Windows Server 200x стає доступною універсальна область дії. Крім того, стає доступною можливість вкладеності груп. На цих функціональних рівнях адміністратор може конвертувати групи з одного типу в інший. Охарактеризуємо групи кожній області дії на цих функціональних рівнях.

- Групи з доменної областю дії. Ці групи доступні виключно в межах того домену, в якому вони визначені. Членами групи з доменної областю дії можуть бути об'єкти, а також інші групи з будь–якими областями дії. Об'єкти, а також групи з глобальною та універсальною областю дії можуть належати до будь–якого домену лісу. До складу групи можуть також входити групи з

доменною областю дії, що належать до того ж домену. Далі ми будемо називати групи цій області дії доменними групами.

•Групи з глобальною областю дії. Групи з даною областю дії доступні в рамках усього лісу доменів. Членами групи можуть бути об'єкти та групи з глобальною областю дії, що належать до того ж домену, що і сама група. Далі ми будемо називати групи цій області дії глобальними групами.

•Група з універсальною областю дії. Ці групи також доступні в рамках усього лісу доменів. До складу групи можуть входити об'єкти, а також групи з універсальною або глобальною областю дії, що належать до будь–якого домену лісу. Далі ми будемо називати групи цій області дії універсальними групами.

З кожною групою у момент створення асоціюється об'єкт каталогу, значення атрибутів якого визначають її характеристику. Один з атрибутів містить список всіх членів групи. У разі зміни складу групи будуть реплікуватись не всі значення атрибуту (у випадку, якщо група налічує тисячі об'єктів, подібна реплікація може викликати помітний трафік), а тільки зроблені зміни. У даному випадку мова йде про механізм реплікації пов'язаних значень (linked value replication). Цей механізм буде працювати тільки в разі, коли ліс доменів знаходиться на функціональному рівні Windows Server 200x.

Фізична структура каталогу

Обчислювальна мережа великих компаній являє собою сукупність підмереж, з'єднаних між собою комунікаційними каналами з різною пропускною здатністю. У цьому випадку на передній план виходить завдання оптимізації трафіку через ці комунікаційні канали. Недостатня пропускна здатність окремих комунікаційних каналів може стати причиною виникнення проблем з пошуком об'єктів, автентифікацією користувачів, а також реплікацією зміни каталогу.

Сайти

Фізична структура каталогу визначається фізичною структурою корпоративної мережі. В залежності від пропускної здатності комунікаційних

каналів адміністратор розділяє корпоративну мережу на області, що отримали назву сайтів. Сайт (site) являє собою сукупність підмереж, з'єднаних між собою високошвидкісними каналами зв'язку [4].

Передбачається, що сайти з'єднуються один з одним комунікаційними каналами з невеликою пропускною здатністю.

Фізична структура мережі, як правило, не є дзеркальним відображенням логічної (доменної) структури. Сайти являють собою самостійні одиниці, які напряму не залежать від доменної структури мережі. Хоча адміністратор може використовувати домени для регулювання трафіку реплікації, найчастіше структура сайтів не відображається на ієрархію доменів. Сайти не є частиною простору імен каталогу, вони лише характеризують його фізичну структуру. Це означає, що належність об'єкта до того чи іншого сайту не впливає на його положення в каталозі. Вибір того чи іншого сайту визначається, перш за все, тим, в якій підмережі фізично знаходиться даний об'єкт. Наприклад, в залежності від того, на якому комп'ютері користувач входить в мережу, він може розглядатися як такий, що знаходиться то в одному, то в іншому сайті.

Оскільки структура сайтів реалізується незалежно від структури доменів, один домен може бути розділений на кілька сайтів і, навпаки, один сайт може бути утворений фрагментами кількох доменів.

Структура сайтів є основним механізмом, за допомогою якого адміністратор може впливати на формування топології реплікації [4]. Оскільки вважається, що сайти з'єднуються один з одним повільними каналами зв'язку, реплікація змін усередині сайту і між сайтами має декілька відмінностей. Усередині сайту контролери домену з'єднані каналами з високою пропускною здатністю. Відповідно, зроблені зміни можуть відразу ж реплікуватись між контролерами домену. Для реплікації між сайтами зазвичай застосовується передача змін за визначеним розкладом. Крім того, в цьому випадку характерне використання маршрутів, заснованих на вартості доступних комунікаційних каналів. У разі реплікації між сайтами адміністратор може вдатися до стиснення переданих даних.

Процес автентифікації користувачів може викликати помітний трафік, особливо якщо мова йде про велику кількість користувачів (наприклад, коли всі співробітники компанії вранці приходять на роботу). Адміністратор повинен забезпечити можливість автентифікації користувачів сайту, навіть якщо комунікаційні канали, що зв'язують сайт із решті мережею, зайняті або недоступні.

При вході користувача в мережу, його автентифікація здійснюється найближчим контролером домену. У процесі локалізації найближчого контролера домену в першу чергу використовується інформація про сайт, до якого належить комп'ютер, що запитує автентифікацію. Найближчим вважається контролер домену, розташований в тому ж сайті, що і користувач, що автентифікується. У кожному сайті необхідно встановити як мінімум один контролер для кожного домену, охоплюваного сайтом.

Важливе місце в процесі автентифікації займає також сервер глобального каталогу. Тому рекомендується в кожному сайті розміщувати як мінімум один сервер глобального каталогу. Багато компонентів служби каталогу (а також користувачі) використовують сервери глобального каталогу для пошуку об'єктів. У разі, якщо доступ до сервера глобального каталогу здійснюється через канали зв'язку з низькою пропускною здатністю, багато операцій служби каталогу будуть виконуватися повільно.

У ході створення лісу доменів майстром установки автоматично створюється сайт за умовчанням з ім'ям Defauit–First–site–Name [4]. Формуючи фізичну структуру мережі, адміністратор повинен самостійно створити нові сайти і задати для них кордони, створивши об'єкти, асоційовані з наявними підмережами. У процесі створення нового контролера на підставі виділеної йому IP–адреси служба каталогу автоматично віднесе його до відповідного сайту. При цьому в розділі конфігурації каталогу в рамках даного сайту буде створений об'єкт класу Server, асоційований з контролером домену.

Транспорт реплікації

Поняття транспорту реплікації характеризує механізми та протоколи, використовувані для передачі змін. Active Directory може використовувати в якості транспорту RPC over IP ("RPC поверх IP") або протокол SMTP [4]. У табл. 1.4 перераховані правила використання різних транспортних протоколів для реплікації різних розділів.

Таблиця 1.4 – Транспортування реплікацій

Розділи каталогу	**Усередині сайту**	**Між сайтами**	
		Один домен	**Різні домени**
Доменний розділ каталогу	RPC over IP	RPC over IP	–
Розділи конфігурації та схеми	RPC over IP	RPC over IP	SMTP
	Трафік не стискається	Трафік стискається	

Протокол RPC over IP забезпечує низькошвидкісну двохточкову синхронну реплікацію всіх розділів каталогу. Цей транспорт найкраще підходить для ситуацій, коли вузли з'єднані надійними лініями зв'язку з низькою ймовірністю втрати пакетів. Протокол SMTP використовується для низькошвидкісної асинхронної реплікації між сайтами і підтримує реплікацію тільки для розділів конфігурації та схеми, а також для глобального каталогу.

Реплікація змін каталогу між контролерами домену, приналежними до одного вузла, завжди здійснюється за допомогою протоколу RPC over IP.

Якщо контролери домену розташовуються в різних сайтах, але належать до одного домену, то реплікація між ними здійснюється також за допомогою протоколу RPC over IP. Якщо контролери домену розташовані в різних сайтах і належать до різних доменів, то для реплікації змін між ними використовується протокол SMTP, що функціонує поверх IP.

З'єднання сайтів

Топологія реплікації формується за допомогою спеціального класу об'єктів – з'єднань (connections) [4]. З'єднання являє собою односпрямовану

угоду між двома контролерами домену про передачу змін. З кожним з'єднанням асоціюється об'єкт в розділі конфігурації каталогу. Атрибути об'єкта, асоційованого з з'єднанням, визначають передавального партнера по реплікації, а також розклад реплікації і використовуваний при цьому транспорт. Всі з'єднання автоматично генеруються системним сервісом Knowledge Consistency Checker (KCC), який перевіряє існуючу топологію і доступність наявних з'єднань і при необхідності вносить відповідні корективи.

Контролери домену, які розташовані в різних сайтах і взаємодіють між собою в процесі реплікації, називаються мостовими серверами (bridgehead server). У кожному сайті один з контролерів домену бере на себе обов'язки з управління вхідними з'єднаннями для всіх мостових серверів сайту. Цей контролер домену називається генератором топології між сайтами (Inter–Site Topology Generator, ISTG). Якщо контролер домену, що виконує функції ISTG, стає недоступний (наприклад, виходить з ладу), ця функція автоматично покладається на інший контролер домену.

У разі реплікації між сайтами використовується термін «зв'язок сайтів» (site link), який описує з'єднання двох і більш вузлів, здатних обмінюватися інформацією за допомогою єдиного транспорту. Зв'язок вузлів використовується для завдання вартості з'єднання (cost), розкладу реплікації і транспорту. Механізм вартостей дозволяє оцінити зв'язок сайтів з точки зору доступності комунікаційних ліній і їх пропускної спроможності. Якщо є декілька зв'язків сайтів, для реплікації буде обрана та, що володіє меншим значенням вартості.

Кілька зв'язків сайтів, що використовують єдиний транспорт, утворюють сполучний міст між вузлами (site link bridge). Використання зв'язуючих мостів між сайтами корисно у великих мережах, оскільки позбавляє від необхідності описувати всі можливі комбінації з'єднань між кожним з сайтів.

Розклад реплікації

Процес реплікації змін каталогу може бути ініційований одним із двох способів [4]:

•повідомлення про зміни (change notification) використовуються між контролерами домену усередині сайту. Якщо на деякому контролері модифікується атрибут якого–небудь об'єкта, даний контролер посилає повідомлення першому партнеру по реплікації, і це відбувається через певний час (за замовчуванням 5 хвилин). Після цього партнер запитує зміни у контролера–джерела змін (originating DC) і отримує їх;

•зміни реплікуються між сайтами згідно з розкладом (schedule). Ці розклади визначаються за допомогою оснащення Active Directory Sites and Services.

Сервери глобального каталога

Глобальний каталог (global catalog) являє собою базу даних, що містить фрагменти всіх доменних контекстів імен, що утворюють простір імен каталогу [4]. Глобальний каталог є важливою і невід'ємною частиною Active Directory. У глобальному каталозі містяться відомості про всі об'єкти, що належать до доменних контекстів імен. Однак у глобальному каталозі зберігаються не всі об'єкти цілком, а тільки підмножина їх атрибутів. Вибираються ті атрибути, які найчастіше присутні в запитах користувачів.

Атрибути, що розміщуються в глобальному каталозі, визначаються в рамках схеми каталогу. У кожного класу атрибутів є параметр isMemberof FartialAttributeSet. Якщо значення цього параметра дорівнює TRUE, атрибут буде розміщений в глобальному каталозі. Адміністратор може визначити для розміщення в глобальному каталозі додаткові атрибути. Однак необхідно пам'ятати, що розширення числа атрибутів, що заносяться в глобальний каталог, призводить до зростання його обсягу.

Процес додавання нового атрибуту для розміщення в глобальному каталозі тягне за собою синхронізацію всіх його реплік. Якщо ліс знаходиться на функціональному рівні Windows Server 200x, додавання нового атрибуту призведе до реплікації тільки цього атрибуту на всі носії глобального каталогу. Якщо ж ліс знаходиться на функціональному рівні Windows 2000,

додавання нового атрибуту призводить до повної синхронізації всіх реплік глобального каталогу.

Контролер домену, який виступає в якості носія глобального каталогу, прийнято називати сервером глобального каталогу (global catalog server). Необхідно звернути увагу на те, що функції сервера глобального каталогу можуть бути покладені тільки на контролер домену. При цьому на контролері домену створюється додатковий розділ, який використовується для розміщення бази даних глобального каталогу.

Сервер глобального каталогу виконує дві функції [4].

- **Пошук об'єктів.** Клієнти можуть звертатися до глобального каталогу із запитами на пошук об'єктів, грунтуючись на відомих значеннях атрибутів. Глобальний каталог зберігає в собі інформацію про всі доменні розділі лісу. Фактично використання сервера глобального каталогу є єдиним способом здійснювати пошук об'єктів по всьому лісу доменів.

- **Автентифікація користувачів.** Сервер глобального каталогу надає інформацію про членство користувача у різних групах з універсальною областю дії (universal group). Ця інформація потрібна в процесі автентифікації користувача. Саме на підставі членства користувача в тих чи інших групах відбувається призначення прав доступу. Більш того, сервер глобального каталогу необхідний у тому випадку, якщо для реєстрації в системі користувач використовує своє основне ім'я. Дозвіл основного імені здійснюється безпосередньо сервером глобального каталогу. Якщо сервер глобального каталогу виявляється недоступним, контролер домену, який здійснює автентифікацію, не буде мати даних, необхідними для авторизації користувача. У результаті користувачеві буде відмовлено в реєстрації. Виняток становлять члени групи Domain Admins (Адміністратори домену), автентифікація яких здійснюється навіть у тому випадку, коли сервер глобального каталогу недоступний.

У лісі доменів повинен бути як мінімум один сервер глобального каталогу. Тому за замовчуванням обов'язки сервера глобального каталогу

покладаються на перший контролер домену, встановлений в лісі доменів. Тим не менш, будь–який контролер домену може бути налаштований в якості сервера глобального каталогу. Це може бути зроблено в силу різних причин. Наприклад, щоб знизити навантаження на повільні лінії зв'язку, зазвичай прийнято встановлювати, як мінімум, по одному серверу глобального каталогу для кожного сайту.

Механізми реплікації каталогу

Каталог розглядається як база даних, розподілена між безліччю носіїв. Кожен контролер домену є носієм копії каталогу. При цьому кожна з копій є повнофункціональною. Це означає, що кожен контролер домену може вносити зміни у власну копію каталогу. Всі зроблені зміни повинні бути автоматично поширені на інші копії. Служба каталогу повинна користуватися механізмом, який би забезпечив підтримку окремих копій каталогу в узгодженому стані. У подібних випадках традиційно використовують механізм синхронізації, заснований на обміні між носіями копії каталогу інформацією про зміни. Оскільки на кожен носій каталогу передається репліка змін, цей процес одержав назву реплікації (replication) змін [4].

Розділи каталогу

З точки зору механізму реплікації Active Directory являє собою не цільну ієрархічну структуру, а окремі фрагменти [4]. Кожен фрагмент, будучи частиною каталогу, являє собою самостійне дерево. У термінології служби Active Directory подібна сукупність гілок називається прилеглим піддеревом (contiguous subtree) або контекстом імен (naming context).

Поділ простору імен каталогу на фрагменти дозволяє оптимізувати процес синхронізації копій каталогу між безліччю його носіїв. Це досягається за рахунок того, що в кожному контексті імен зберігається певного виду інформація. За замовчуванням каталог Active Directory поділений на три контексти імен, які називаються розділи каталогу (directory partition) [4]:

- **доменний розділ каталогу** (Domain partition) використовується для розміщення інформації про мережні ресурси, що належать до певного домену.

Репліки доменного розділу розташовуються на всіх контролерах домену. Відповідно зміни, що відбуваються в цьому розділі, реплікуються тільки на ці репліки;

•**розділ схеми (Schema partition).** Поняття схеми каталогу було дано вище. Для її зберігання використовується спеціальний розділ каталогу. Оскільки схема є загальною для всіх доменів лісу, зміни в ній поширюються на всі носії копії каталогу;

•**розділ конфігурації (Configuration partition)** містить інформацію, використовувану різними системними службами, в тому числі і самою службою каталогу. Зокрема, в розділі конфігурації зберігається інформація, що описує топологію реплікації між контролерами домену. Ця інформація необхідна для успішного функціонування служби каталогу в цілому, тому зміни в даному розділі реплікуються на всі носії каталогу в ліс доменів.

Репліки трьох зазначених розділів каталогу присутні в обов'язковому порядку на всіх контролерах домену. Доменний розділ каталогу індивідуальний для кожного домену. Репліки розділу схеми і розділу конфігурації однакові для всіх контролерів домену в лісі.

Будь–який контролер домену Active Directory може провадити зміни у власних репліках в будь–який момент часу. При цьому всі зроблені зміни будуть синхронізовані з іншими репліками. Подібна модель реплікації отримала назву реплікація з безліччю рівноправних учасників (multimaster replication).

Розділи програм

Додатково до перерахованих розділів, в каталозі Active Directory на базі систем Windows Server 200x можуть бути створені спеціалізовані розділи, які отримали назву розділів програм (application directory partitions) [4]. Розділи програм можуть бути створені при необхідності адміністратором або безпосередньо самими додатками. У розділі програм можуть бути розміщені будь–які об'єкти, визначення яких містяться в схемі, за винятком суб'єктів

підсистеми безпеки (таких, наприклад, як облікові записи користувачів або комп'ютерів).

Розділи програм були реалізовані в Windows Server 2003. Їх використання дозволяє скоротити накладні витрати, викликані реплікацією. На відміну від трьох основних розділів каталогу, що реплікуються на всі контролери домену, розділи програм можуть розташовуватися на суворо обумовлених контролерах. Адміністратор може перерахувати контролери домену, на які необхідно розмістити копії певного розділу каталогу. У даному питанні основним є потреба додатка в доступності даних. Додаткам часто не потрібно, щоб розміщена ними в каталозі інформація була доступна по всій мережі. Існують додатки, застосування яких обмежене окремим доменом або деревом доменів. Якщо додаток, для якого створюється розділ, використовується тільки в двох доменах лісу, то копії розділу додатка повинні бути розміщені тільки на контролерах домену двох зазначених доменів. Контролери інших доменів не будуть містити даний розділ.

Є два вбудованих розділи програм, які використовуються службою DNS для розміщення вмісту зон, інтегрованих з Active Directory. Це розділи ForestDnsZones.forestName і DomamDnsZones.forestName. При цьому замість суфікса forestName в імені розділу вказується DNS–ім'я кореневого домену лісу.

Існує три способи створення розділу програм [1, 4].

- **Використання утиліти NtdsUtil.exe.** Ця утиліта командного рядка являє собою основний інструмент адміністратора служби каталогу Active Directory, що використовується для діагностики і вирішення проблем. Цей спосіб передбачає створення розділу додатка адміністратором вручну.

- **Використання утиліти Ldp.exe.** Дана утиліта дозволяє адміністратору працювати з будь–яким LDAP–сумісним каталогом (яким, по суті, є Active Directory). Цей спосіб, так само як і попередній, передбачає створення розділу додатка адміністратором вручну.

•**Використання інтерфейсу прикладного програмування ADSI (Active Directory Service Interfaces).** Програми, що використовують даний інтерфейс для взаємодії зі службою каталогу Active Directory, можуть створювати розділи програм в каталозі самостійно (наприклад, в процесі розгортання).

Топологія реплікації

Процес реплікації передбачає обмін змінами в розділах каталогу між окремими учасниками. Для позначення односторонньої передачі даних від одного партнера по реплікації до іншого використовується термін з'єднання (connection). З'єднання являє собою односпрямовану угоду про реплікації, укладену між двома контролерами домену.

Одним з найбільш відповідальних моментів в процесі функціонування підсистеми реплікації служби каталогу є формування інфраструктури з'єднань між наявними контролерами домену. Подібна інфраструктура називається топологією реплікації (replication topology). Кожен розділ каталогу будує свою власну топологію реплікації.

За формування топології реплікації відповідає спеціальний системний процес Knowledge Consistency Checker, KCC. Цей процес виконується на всіх контролерах домену, автоматично генеруючи топологію реплікації. При цьому KCC ґрунтується на інформації про фізичну структуру каталогу. Періодично активізуючись, KCC перевіряє доступність існуючих з'єднань. Ґрунтуючись на отриманих даних, KCC може переформувати топологію реплікації для деякого розділу каталогу. Саме KCC відповідає за встановлення з'єднання з партнером по реплікації. З'єднання генеруються автоматично, хоча служба каталогу допускає визначення сполук безпосередньо адміністратором.

Служба реплікації файлів

Каталог розглядається як централізоване місце зберігання інформації про мережні ресурси. Однак в силу певних причин деяка частина інформації не може бути розміщена в каталозі. Наприклад, старі версії операційних систем (Windows 9x/NT) використовують спеціальний мережний ресурс NETLOGON для розміщення інформації, необхідної для реєстрації в мережі.

Цей каталог використовується для розміщення переміщуваних або обов'язкових профілів користувачів, сценаріїв реєстрації, системних політик і т. п. Ця інформація необхідна для коректного функціонування мережі. При цьому потрібно, щоб цей каталог був присутнім на всіх контролерах домену.

Служба реплікації файлів (File Replication Service, FRS) являє собою механізм реплікації з безліччю рівноправних учасників, що здійснює синхронізацію вмісту системного тому SYSVOL між контролерами домену [1, 4]. Том SYSVOL створюється на кожному сервері безпосередньо в ході підвищення його до контролера домену та використовується для розміщення системних файлів загального доступу. Зокрема, саме всередині нього розташовується вже згадуваний каталог NETLOGON. Крім цього, в томі SYSVOL розміщуються налаштування об'єктів групових політик, системні політики контролерів домену та сценарії реєстрації.

Служба реплікації файлів може також здійснювати синхронізацію вмісту набору реплік розподіленої файлової системи DFS.

Створення системного тому SYSVOL

Том SYSVOL створюється безпосередньо в ході підвищення сервера до контролера домену. Коли ви встановлюєте перший контролер домену в мережі, в цьому каталозі на базі наявних шаблонів створюються об'єкти політик за замовчуванням. Служба FRS сповіщає службу NETLOGON про те, що системний каталог доступний для загального доступу [4]. Тільки після цього сервер може використовуватися як контролер домену.

У разі встановлення наступних контролерів домену після створення тому SYSVOL служба реплікації файлів здійснює його наповнення. Зміст тому копіюється з вже існуючого контролера домену. Тільки по закінченні цього процесу наповнення сервер буде оголошений контролером домену.

Служба каталогу та служба FRS

Для своєї роботи служба FRS запитує інформацію про фізичну структуру служби каталогу, сервери каталогу і з'єднання між ними. Іншими словами, служба реплікації файлів не створює своєї інфраструктури, а

використовує топологію реплікації каталогу для власних цілей. Зокрема, служба реплікації файлів використовує об'єкти, асоційовані з з'єднанням (connection objects), для передачі файлів. При цьому враховується розклад реплікації, визначений в рамках цих об'єктів.

Такий підхід дозволяє спростити схему реплікації, виключивши дублювання схожих структур.

Групові політики

В даний час практично будь–який виробник системного програмного забезпечення встає перед проблемою зниження загальної вартості володіння системою (total cost ownership). Ця проблема полягає в тому, що розвиток і пов'язане з цим ускладнення технологій призводить до збільшення витрат на адміністрування. У таких умовах корпорації змушені або постійно збільшувати штат адміністраторів, або спрощувати процес управління за рахунок відмови від тих або інших сервісів і технологій.

Кожен розробник підходить до вирішення цієї проблеми по–своєму. Компанія Microsoft традиційно пропонує цілий набір рішень, що дозволяють спростити процес управління мережними ресурсами, а отже знизити загальну суму адміністративних витрат.

Однією з проблем, що постають перед системним адміністратором, є проблема формування індивідуального оточення користувачів. Починаючи з Windows 2000, для формування оточення користувачів використовується механізм групових політик (group policy) [4]. Під груповою політикою розуміється сукупність параметрів і налаштувань системи, що визначає конкретне оточення користувача. Адміністратор може використовувати механізм групових політик для централізованого управління середовищем користувачів.

- **Управління налаштуваннями операційної системи.** Всі параметри операційної системи, що визначають її функціональність, а також визначають режими роботи її служб і їх налаштування, зберігаються в системному реєстрі.

За допомогою механізму групової політики адміністратор може контролювати вміст окремих, найбільш важливих ключів реєстру.

•**Призначення сценаріїв.** За допомогою групової політики адміністратор може визначити сценарії, які будуть виконуватися при запуску і виключенні комп'ютера, а також при вході користувача в систему і вихід з неї.

•**Визначення параметрів системи безпеки.** З кожним користувачем або комп'ютером може бути асоційований певний набір налаштувань системи безпеки. У даному випадку прийнято говорити про політику безпеки (security policy), яка визначається в контексті групової політики. Політика безпеки дозволяє однотипно конфігурувати велику кількість суб'єктів безпеки. Наприклад, визначити рівень доступу до системного реєстру або задати порядок здійснення аудиту подій.

•**Управління додатками.** Використовуючи механізм групової політики, адміністратор може призначати і публікувати програми, виконувати їх централізоване оновлення та відновлення.

•**Перенаправлення користувальницьких папок.** Папка My Documents (Мої документи) традиційно розглядається як місце зберігання призначених для користувача документів. У корпоративній мережі, в якій працює безліч мобільних користувачів, актуальною стає проблема доступності цих документів. За допомогою механізму групової політики адміністратор може задати перенаправлення всіх звернень користувачів до цієї папки на деякий мережний ресурс.

Об'єкти групової політики

Параметри групової політики зберігаються у вигляді об'єктів групової політики (Group Policy Object, GPO) [4]. Ці об'єкти зберігаються в каталозі подібно іншим об'єктам. Для іменування об'єкта групової політики використовується глобальний унікальний ідентифікатор (GUID).

Розрізняють два види об'єктів групової політики – об'єкти групової політики, що створені в контексті служби каталогу, і локальні об'єкти групової політики [4]. Локальні об'єкти групової політики (Local Group Policy Object,

LGPO) створюються в процесі установки операційної системи Windows або Windows Server 2003. Локальний об'єкт GPO використовується в тому випадку, коли комп'ютер не включений до складу домену. Як тільки комп'ютер підключається до домену, комп'ютер і користувач, що працює на ньому, підпадають під дію об'єктів GPO, визначених у контексті даного домену, і параметри, задані локальним об'єктом GPO, можуть бути перевизначені на більш високому рівні (на рівні сайту, домену або підрозділу).

Об'єкти групової політики розміщуються в каталозі в спеціальних контейнерах групової політики (Group Policy Container, GTC). Крім того, для розміщення файлів, пов'язаних з об'єктами GPO, система використовує спеціальну папку SYSVOL \ sysvol \ <ім'я домену> \ policies. У цій папці розміщуються шаблони групової політики (Group Policy Template, GPT). Шаблон групової політики являє собою папку, в якості імені якої використовується глобальний унікальний ідентифікатор (GUID) відповідного об'єкта групової політики. У шаблоні групової політики розміщуються адміністративні шаблони, сценарії та параметри безпеки.

Користувальницькі облікові записи

Користувальницька обліковий запис містить ім'я і пароль для реєстрації на локальному комп'ютері або в домені. У Active Directory обліковий запис користувача може також містити додаткову інформацію, таку як повне ім'я користувача, адресу електронної пошти, номер телефону, відділ і фізичну адресу[4]. Крім того, обліковий запис користувача служить засобом для призначення дозволів, сценаріїв реєстрації, профілів і домашніх каталогів.

У Windows Server 200x визначені користувальницькі облікові записи двох типів: доменні облікові записи та локальні облікові записи.

Доменні облікові записи визначені в Active Directory. За допомогою системи одноразового введення пароля такі облікові записи можуть звертатися до ресурсів у всьому домені. Вони створюються в консолі «Active Directory – користувачі і комп'ютери» [4].

Локальні облікові записи визначені на локальному комп'ютері, мають доступ тільки до його ресурсів і повинні автентифікуватися, перш ніж отримають доступ до мережних ресурсів. Локальні облікові записи користувачів створюють в оснащенні «Локальні користувачі та групи».

Локальні облікові записи користувачів і груп зберігаються тільки на рядових серверах і робочих станціях. На першому контролері домену вони переміщаються в Active Directory і перетворюються в доменні облікові записи.

Усі облікові записи користувачів розпізнаються по імені для входу в систему. У Windows Server 200x воно складається з двох частин [4]:

- «Ім'я користувача» – текстове ім'я облікового запису;
- «Домен або робочу групу», в яких знаходиться обліковий запис.

Наприклад, для користувача mask, обліковий запис якого створена в домені is4.local, повне ім'я для входу в Windows Server 200x виглядає так: mask@is4.local. При роботі з Active Directory іноді потрібно повне ім'я домену користувача, що складається з DNS–імені домену в поєднанні з іменами контейнера і групи. У користувача is4.local \ Users \ mask, DNS–ім'я домену – is4.local, ім'я контейнера – Users, а ім'я користувача – mask.

З обліковим записом користувача можуть зіставлятися пароль і відкритий сертифікат. У відкритому сертифікаті поєднуються відкритий і закритий ключ для ідентифікації користувача. Вхід в систему по паролю проходить інтерактивно. При вході в систему з відкритим сертифікатом використовуються смарт–карта і зчитувальний пристрій.

Хоча для призначення привілеїв та дозволів у Windows Server 200x застосовуються імена користувачів, ключовим ідентифікатором облікового запису є унікальний ідентифікатор безпеки (SID), що генерується при створенні запису. Він складається з ідентифікатора безпеки домену та унікального відносного ідентифікатора, який був виділений господарем відносних ідентифікаторів.

За допомогою SID ОС Windows Server 200x здатна відстежувати облікові записи незалежно від імен користувачів [4]. Завдяки наявності SID ви

вправі змінювати імена користувачів і видаляти облікові записи, не турбуючись, що хтось отримає доступ до ресурсів, створивши обліковий запис з тим же ім'ям. Коли ви міняєте ім'я користувача, Windows Server 200x зіставляє колишній SID з новим ім'ям. Коли ви видаляєте обліковий запис, Windows Server 200x вважає, що конкретний SID більше недійсний. Якщо ви потім створите обліковий запис з тим же ім'ям, він не отримає привілеїв попереднього запису, так як у нього інший SID.

Крім облікових записів користувачів у Windows Server 200x використовуються групи [4]. Це дозволяє автоматично надавати дозволи схожим типам користувачів, що спрощує адміністрування облікових записів. Якщо користувач – член групи, яка має право звертатися до ресурсу, то він теж може до нього звернутися. Щоб надати користувачеві доступ до потрібних ресурсів, ви просто включаєте його в підходящу групу. Оскільки в різних доменах Active Directory можуть бути групи з однаковими іменами, на групи часто посилаються по повному імені – домен \ імя_групи.

Вище вже було зазначено, що у Windows Server 200x використовуються групи трьох типів:

- локальні групи визначаються і використовуються тільки на локальному комп'ютері, створюються в оснащенні «Локальні користувачі та групи»;
- групи безпеки визначаються в доменах за допомогою консолі «Active Directory – користувачі і комп'ютери». Це ті групи, для яких можна призначати права та дозволи.;
- групи поширення використовуються як списки розсилки електронної пошти, не мають дескрипторів безпеки і визначаються в доменах за допомогою консолі «Active Directory – користувачі і комп'ютери». Ці групи призначені тільки для розсилки користувачам повідомлень електронної пошти. Для них не визначаються права доступу до мережних об'єктів.

У Windows Server 2003 облікові записи груп, як і облікові записи користувачів, розрізняються за унікальним ідентифікатором безпеки. Це означає, що не можна видалити обліковий запис групи, а потім створити групу

з тим же ім'ям, щоб у неї з'явилися колишні дозволи та привілеї. У нової групи буде новий SID, і всі дозволи і привілеї старої групи будуть загублені. Для кожного сеансу користувача в системі Windows Server 200x створює маркер безпеки, що містить ідентифікатор облікового запису користувача і SID всіх груп безпеки, до яких відноситься користувач. Розмір маркера зростає по мірі того, як користувач додається в нові групи безпеки. Це призводить до наступних наслідків [4].

•Щоб користувач увійшов в систему, маркер безпеки повинен бути переданий процесу входу в систему. Тому по мірі збільшення членства користувача в групах безпеки процес входу вимагає все більше часу.

•Щоб з'ясувати дозвіл доступу, маркер безпеки пересилається на кожен комп'ютер, до якого звертається користувач. Тому чим більше маркер безпеки, тим вище мережний трафік.

Створення доменного облікового запису [4]

1. На сервері запустити консоль «Active Directory – користувачі і комп'ютери».

2. Перед створенням облікового запису користувача необхідно створити новий підрозділ. Для цього в лівому вікні консолі клацнути правою кнопкою миші по значку домену і з контекстного меню вибрати «Створити» – «Підрозділ».

3. У діалоговому вікні ввести ім'я підрозділи, наприклад «student».

4. Після створення підрозділу приступити до створення облікового запису користувача. Для цього потрібно клацнути правою кнопкою миші по створеному підрозділу «student» і з контекстного меню вибрати «Створити» – «Користувач».

5. У діалоговому вікні «Новий об'єкт – Користувач». Заповнити пункти «Ім'я» і «Прізвище».

6. У полі «Ім'я входу користувача» ввести «User1». Це ж реєстраційне ім'я буде автоматично введено і в полі «Ім'я входу в систему користувача. Дане значення можна змінити вручну, але це не рекомендується. Натисніть «Далі».

Рекомендується уникати використання в реєстраційному імені символів кирилиці.

7. Заповніть поля «Пароль» та «Підтвердження».

При цьому необхідно придумати і ввести складний пароль, що задовольняє наступним мінімальним вимогам:

- пароль не може містити ім'я облікового запису користувача або якусь його частину;
- пароль повинен складатися не менше ніж з семи символів;
- у паролі повинні бути присутніми символи трьох категорій з числа наступних чотирьох: прописні букви англійського алфавіту від A до Z, малі літери англійського алфавіту від a до z, десяткові цифри (від 0 до 9), неалфавітні символи (наприклад!, $, #, %).

8. При необхідності встановити прапорець «Вимагати зміну пароля при наступному вході в систему».

9. Після перевірки інформації про новий користувача завершити створення облікового запису нового користувача.

Вивчення властивостей створеного облікового запису [4]

1. Відкрити властивості створеного облікового запису користувача.
2. Вивчити всі вкладки.
3. Заповнити вкладки «Загальні», «Адреса», «Організація».
4. Зробити обліковий запис членом групи "Адміністратори домену". Для цього слід на вкладці «Член груп» виконати команду «Додати».
5. У діалоговому вікні, виконати команди «Додатково» – «Пошук».
6. З результатів пошуку вибрати групу "Адміністратори домену".
7. Задати основну групу – "Адміністратори домену"
8. Виключити обліковий запис з групи «Користувачі домену».

Включення облікового запису користувача в створені групи [4]

Для створення нової групи потрібно виконати наступне.

1. Клацнути правою кнопкою миші по підрозділу «student» і з контекстного меню вибрати «Створити» – «Група».

2. У діалоговому вікні заповнити поля «Ім'я групи» і «Ім'я групи» відповідно до правил, наприклад «security».

3. Визначити область дії «Глобальна» і «Тип групи» – «Група безпеки».

4. Створити групу «extending». Встановити «Область дії групи» – «Універсальна», «Тип групи» – «Група розповсюдження» .

5. Включити ваш обліковий запис в створені групи.

Створення шаблону [4]

Послідовність дій зі створення шаблону складається з наступних етапів.

1. Запустити консоль «Active Directory – користувачі й комп'ютери» та створити користувача з ім'ям «mask».
2. У вікні властивостей новоствореної запису заповнити всі необхідні поля на вкладках «Адреса» та «Організація».
3. Використовуючи вкладку «Обліковий запис», встановити час входу для користувача з понеділка по суботу з 8:00 до 18:00.
4. Далі потрібно натиснути на створеному обліковому запису правою кнопкою миші і з контекстного меню вибрати команду «Відключити обліковий запис» .

Створення облікового запису за шаблоном [4]

1. Натиснути на шаблон «mask» правою кнопкою миші і з контекстного меню вибрати команду «Копіювати».

2. У вікні ввести реєстраційне ім'я «mask1», в якості імені та прізвища теж «mask1».

3. Задати пароль для першого входу в систему і зняти прапорець "Вимкнути обліковий запис».

Контрольні запитання

1. Що розуміється під Active Directory?
2. Наведіть приклади об’єктів, які присутні в Active Directory
3. Що розуміється під «деревом» в Active Directory?

4. З якою структурною одиницею Windows – мережі асоціюється Active Directory?
5. Яка схема іменування об’єктів використовується в Active Directory?
6. Що розуміється під «лісом» в Active Directory?
7. Для чого встановлюються довірчі відносини між «деревами» в «лісі»?
8. Які існують типи довірчих відносин?
9. Наведіть приклад мережі, де може виникнути «ліс».
10. Що розуміється під сайтом в Active Directory?
11. У яких мережах і з якою метою створюються сайти Active Directory?
12. Які функції виконує контролер домену в Active Directory?
13. Що розуміється під «груповою політикою»?
14. Для вирішення яких задач може бути використана групова політика?
15. Що містить користувальницький обліковий запис?
16. Які типи облікових записів визначені в Windows Server 2003?
17. З яких частин складається ім'я для входу в систему Windows Server 2003?
18. Для чого створюються групи користувачів?
19. Які три типи груп використовуються в ОС Windows Server 2003?
20. Чи можна, видаливши обліковий запис групи, створити заново групу з таким же ім'ям з тим, щоб у неї з'явилися колишні дозволи та привілеї?

1.4. Лабораторна робота № 4. НАЛАШТУВАННЯ ТА ВИКОРИСТАННЯ СИСТЕМИ ДОМЕННИХ ІМЕН – DNS

Мета та основні завдання:

- ознайомитись з існуючими системами розпізнавання імен,
- навчитись вирішувати задачі по налаштуванню та адмініструванню DNS серверу

Порядок виконання роботи

1. Ознайомитися з документацією.
2. Ознайомитися з налаштуваннями і адмініструванням сервера DNS (програмна група «Адміністрування» – DNS).
3. Виконати практичні налаштування згідно завдання.
4. Розібратися з конфігуруванням клієнтів DNS сервера та перевірити роботу системи.
5. Розібратися з використанням утиліти nslookup.

Основні теоретичні відомості

Поняття адрес та імен вузлів

У мережі TCP/IP використовуються наступні типи адрес та імен вузлів [5].

Машинні адреси (фізичні, MAC–адреси). Це – унікальна адреса, яка «зашита» в мережеве апаратне забезпечення, наприклад, в карту мережного адаптера персонального комп'ютера. Машинна адреса складається з 12 шістнадцяткових цифр (наприклад, 00 04 AC 26 5E 8Б). При написанні для зручності сприйняття цю адресу групується в шість пар по дві цифри. MAC–адреса ідентифікує вузол в одному домені широкомовлення (на одному каналі).

IP–адреси. Логічна адреса, яка ідентифікує вузол в конкретній IP–мережі.

Ім'я NetBIOS (Windows ім'я) – ім'я комп'ютера в локальній Windows мережі. Розраховане на роботу мережі по стеку NetBIOS/NetBEUI. При використанні стеку TCP/IP у локальній Windows мережі для розпізнавання NetBIOS імен необхідно обов'язково включити опцію «NetBIOS over TCP/IP» в налаштуванні властивостей протоколу TCP/IP. NetBIOS ім'я може мати довжину до 15 символів.

Ім'я хоста. Це ім'я комп'ютера або пристрою в мережі TCP/IP (зазвичай, в Інтернеті). У комбінації з ім'ям Інтернет–домену визначає повністю специфіковане доменне ім'я – FQDN (Fully Qualified Domain Name).

Ім'я домену. Може використовуватись як у локальних Windows мережах, так і у глобальних мережах. У першому випадку воно визначає ім'я домену Active Directory і у комбінації з NetBIOS ім'ям вузла формує повне ім'я вузла у конкретному Windows домені (може розглядатись як аналог FQDN ім'я вузла у Windows домені). В Інтернеті – це ім'я інтернет–домену (наприклад, kpi.ua).

Механізми розпізнавання імен вузлів

Практично в кожній мережі потрібен механізм, що дозволяє перетворювати імена комп'ютерів в IP–адреси і навпаки. Ця вимога обумовлена тим, що користувачі і додатки зазвичай звертаються до комп'ютерів в мережі по іменах, і лише служби нижнього рівня звертаються до мережевих вузлів по IP–адресам.

Існують наступні служби і механізми, які можуть бути використані для вирішення задачі розпізнавання імен [5]:

- WINS (Windows Internet Name Service) – встановлює відповідність NetBIOS імен з IP адресами ;
- DNS (Domain Name System) – встановлює відповідність доменних імен (FQDN) з IP адресами;
- файл Hosts – спрощений аналог системи DNS;
- файл Lmhosts – – спрощений аналог системи WINS;
- відправлення широкомовних запитів.

Найбільш поширеним механізмом є DNS.

Побудова системи імен в Інтернеті

Система іменування DNS являє собою ієрархічну і логічну деревоподібну структуру, яку називають простір імен DNS (DNS namespace), де є один корінь, у якого може бути будь–яке число піддоменів [5]. У окремих піддоменів в свою чергу можуть бути дочірні піддомени. Наприклад, в просторі імен Інтернету корінь "" (порожній рядок) об'єднує безліч доменних імен верхнього рівня, одне з яких – .ua. У домені ua може бути піддомен НТУУ «КПІ»: kpi.ua, який в свою чергу є батьківським для дочірнього домену наступного рівня, наприклад домену факультету електроніки: fel.kpi.ua. Організації мають право створювати приватні мережі та використовувати власні, недоступні з Інтернету, простори DNS–імен.

Кожен вузол в дереві DNS–домену ідентифікується по його повному доменному імені (FQDN), яке однозначно визначає його розташування по відношенню до кореня дерева доменів [5]. Наприклад, FQDN поштового сервера в домені kpi.ua буде mail.kpi.ua. Воно являє собою об'єднання імені вузла (mail) основного суфікса DNS домена (kpi.ua) і замикаючої крапки (.). Замикаюча крапка є стандартним роздільником доменної мітки верхнього рівня і міткою порожнього рядка, відповідного кореню. При повсякденному використанні замикаючу крапку часто опускають, але її додає служба DNS–клієнта при виконанні запитів.

Корінь (самий верхній рівень) простору імен Інтернету управляється міжнародною організацією ICANN (Internet Corporation for Assigned Names and Numbers). Ця організація координує присвоєння ідентифікаторів, які повинні бути унікальними у всьому Інтернеті, в тому числі доменних імен, IP–адрес, параметрів протоколів і номерів портів. Нижче кореневого рівня розташовуються домени верхнього рівня, які також перебувають під управлінням ICANN. Існує два типи таких доменів [5].

Організаційні домени – в їх імені присутній трибуквений код, який вказує на основний рід діяльності організацій даного DNS–домену (наприклад, com – комерційні організації, edu – освітянські організації, gov – урядові організації і

т.і.). Деякі домени організацій мають глобальний характер, інші виділяються тільки організаціям всередині США.

Географічні домени – в їх імені присутній двобуквений код країни або регіону, як визначено Міжнародною організацією зі стандартизації (ISO 3166) (наприклад, ua – Україна, ru – Росія, uk – Великобританія і т.і.). Ці домени виділяються організаціями поза США, хоча ця вимога дотримується не занадто жорстко.

Нижче доменів верхнього рівня ICANN та інші уповноважені органи, які відповідають за присвоєння імен в Інтернеті, передають домени різним організаціям, наприклад Microsoft (microsoft.com) або КПІ ім. Ігоря Сікорського (kpi.ua). Ці організації підключаються до Інтернету і присвоюють імена вузлів в межах своїх доменів.

Крім того, організації надають піддомени своїм користувачам або клієнтам. Наприклад, інтернет–провайдери отримують домен від ICANN і можуть передавати піддомени в розпорядження своїх клієнтів. Для перетворення імен в IP–адреси в зоні дії простору імен організації використовуються DNS–сервери.

Організації вправі організовувати приватний простір імен (private namespace), тобто простір DNS–імен, в основі якого кілька кореневих серверів, повністю незалежних від простору доменних імен Інтернету. В рамках приватного простору імен можна призначати імена та створювати власний кореневий домен або домени і будь–які необхідні піддомени. Приватні імена недоступні і не дозволяються в Інтернеті. Приклад приватного доменного імені: mycompany.local.

Принципи функціонування системи DNS

Відповідність між доменними іменами (FQDN) і IP–адресами може встановлюватися як засобами локального вузла, так і засобами централізованої служби [5]. Найпростішим рішенням є створення вручну текстового файлу з ім'ям hosts. Цей файл складається з деякої кількості рядків, кожна з яких містить запис типу «IP–адреса – доменне ім'я», наприклад,

77.47.129.30 – www.kpi.ua. Файл необхідно розмістити у відповідному системному каталогу (наприклад, у випадку Windows–систем це каталог \WINDOWS\system32\drivers\etc).

У загальному випадку для вирішення задачі встановлення відповідності доменних імен і IP–адрес використовується спеціальна служба – *система доменних імен (Domain Name System, DNS)*. DNS – це централізована служба, заснована на розподіленій базі відображень «доменне ім'я – IP–адреса» [5]. Служба DNS використовує в своїй роботі схему взаємодії типу «клієнт–сервер». У рамках цієї взаємодії визначені DNS–сервери і DNS–клієнти. DNS–сервери підтримують розподілену базу записів, а DNS–клієнти звертаються до серверів із запитами на визначення IP–адреси по конкретному доменному імені вузла або ресурсу. Таким чином, DNS забезпечує механізми як для іменування вузлів, так і для пошуку IP– адрес вузлів по іменах.

Служба DNS використовує текстові файли майже такого ж формату, як і файл hosts, і ці файли адміністратор також може корегувати вручну. Проте, служба DNS спирається на ієрархію доменів, і кожен сервер служби DNS зберігає тільки частину імен мережі, а не всі імена, як це відбувається при використанні файлів hosts. При зростанні кількості вузлів в мережі проблема масштабування вирішується створенням нових доменів і піддоменів імен і додаванням в службу DNS нових серверів.

Для кожного домена імен створюється свій DNS–сервер. Цей сервер може зберігати записи «доменне ім'я – IP–адреса» для всього домена, включаючи всі його піддомени. Частіше сервер домена зберігає тільки імена, які закінчуються на наступному нижче рівні ієрархії в порівнянні з ім'ям домена. Саме при такій організації служби DNS навантаження розподіляється більш–менш рівномірно між всіма DNS–серверами мережі. Наприклад, в першому випадку DNS–сервер домена kpi.ua зберігатиме відображення для всіх імен, що закінчуються на kpi.ua. В другому випадку цей сервер зберігає відображення тільки імен типу fel.kpi.ua, fiot.kpi.ua, а решта всіх записів нижчих рівнів ієрархії повинна зберігатися на DNS–серверах піддоменів fel і fiot.

Кожен DNS–сервер окрім таблиці відображень імен містить посилання на DNS–сервери своїх піддоменів. Ці посилання зв'язують окремі DNS–сервери в єдину службу DNS. Посиланнями є IP–адреси відповідних серверів. Для обслуговування кореневого домена виділено декілька дублюючих один одного DNS–серверів, IP–адреси яких є широко відомими.

Схеми використання системи DNS

Існують дві основні схеми роботи системи DNS [5]. У першому варіанті роботу по пошуку IP–адрес координує DNS–клієнт:

– DNS–клієнт звертається до DNS–серверу, адреса якого явно вказана в налаштуваннях IP–протоколу конкретного вузла (надалі, локальний), із запитом. В запиті він передає повне доменне ім’я вузла, IP–адресу якого необхідно визначити;

– DNS–сервер відповідає, повертаючи клієнту адресу наступного DNS–сервера, обслуговуючого домен верхнього рівня, указаний в старшій частині доменного імені, яке надійшло у запиті;

– DNS–клієнт посилає запит на наступний DNS–сервер, який посилає його до DNS–серверу потрібного піддомена, і т. д., поки не буде знайдений DNS–сервер, в якому зберігається відповідність запитаного імені IP–адресі. Цей сервер дає остаточну відповідь клієнтові.

Така схема взаємодії називається нерекурсивною або ітеративною [5], коли клієнт сам виконує послідовність запитів до різних серверів імен. Оскільки ця схема завантажує клієнта достатньо складною роботою, то вона практично не застосовується.

У другому варіанті реалізується рекурсивна процедура [5]:

– DNS–клієнт посилає запит на локальний DNS–сервер, аналогічно попередній процедурі;

– якщо локальний DNS–сервер знає відповідь, то він відразу ж повертає його клієнтові; це може відповідати випадку, коли запитане ім'я входить в той же піддомен, що і ім'я клієнта, а також може відповідати випадку, коли сервер

вже дізнавався про дану відповідність для іншого клієнта і зберіг її в своєму кеші;

– якщо ж локальний сервер не знає відповідь, то він надсилає запити до кореневого сервера і так далі, як це робив клієнт в попередній процедурі. Отримавши відповідь, він передає його клієнтові, який весь цей час просто чекає її від свого локального DNS–сервера.

У цій схемі клієнт передоручає роботу своєму серверу, тому схема називається непрямою або рекурсивною. Практично всі DNS–клієнти використовують рекурсивну процедуру.

Для прискорення пошуку IP–адрес DNS–сервери широко застосовують процедуру кешування відповідей, що проходять через них. Щоб служба DNS могла оперативно відпрацьовувати зміни, що відбуваються в мережі, відповіді кешуються на певний час – зазвичай від декількох годин до декількох днів.

Порядок визначення імен за механізмом DNS має такий вигляд:

• пошук імені в кеші DNS–клієнта. Імена потрапляють в кеш при більш ранніх запитах;

• пошук імені в файлі Hosts (для Windows – систем розташований в папці Windows \ System32 \ Drivers \ Etc);

• запит DNS–сервера

Основні поняття і записи, які використовуються у системі DNS

Для нормальної роботи DNS необхідно правильно сконфігурувати DNS – сервери, зони і зробити необхідні записи [5].

DNS–сервер – це комп'ютер з відповідними програмними додатками, наприклад, служба DNS–сервера в Windows, або служба BIND в UNIX–системах. DNS–сервери підтримують базу даних DNS з інформацією про частини структури доменного дерева DNS і обробляють запити на дозвіл імен, що надходять від DNS–клієнтів. У відповідь на запит клієнта DNS–сервер надає запитувану інформацію, дає посилання на інший сервер, який може відповісти на запит, або повідомляє, що інформація недоступна або не існує. DNS–сервери поділяються на основні (повноважні) та резервні (додаткові).

Для кожної зони може існувати тільки один основний сервер (на якому можна вносити зміни в зонну інформацію) і будь–яка кількість резервних серверів (які отримують інформацію про зону з основного серверу). Встановлення резервних DNS серверів дозволяє вирішити дві задачі: збільшити надійність роботи системи DNS, розподілити запити клієнтів по різним серверам, збільшуючи таким чином продуктивність роботи системи DNS.

Зона DNS (DNS zone) – це єдина частина простору імен та IP – адрес, що обслуговується повноважним сервером [5]. Сервер може обслуговувати і кілька зон, а зона може містити один або декілька Інтернет – доменів. Наприклад, один сервер може бути повноважним для зон kpi.ua і kpi.edu, кожна з яких містить декілька доменів. Суміжні домени, наприклад, kpi.ua, fel.kpi.ua і keoa.fel.kpi.ua можна перетворити в окремі зони, застосувавши делегування, при якому відповідальність за піддомен всередині простору імен DNS присвоюється окремому об'єкту (відповідному DNS – серверу).

Файли зон (zone files) містять записи ресурсів зон, в яких сервер є повноважним. У багатьох реалізаціях DNS–сервера дані зон зберігаються в текстових файлах; DNS–сервери на контролерах доменів під керуванням Windows 2000 або Windows Server 2003 можуть також зберігати зонну інформацію в Active Directory.

Існують два види зон: прямого і зворотного перегляду [5]. У перших виконується зіставлення FQDN–імен з IP–адресами, у других навпаки, IP–адреси зіставляються з повними доменними іменами. Таким чином, зони прямого перегляду обслуговують запити по встановленню відповідності між FQDN–іменами і IP–адресами, а зони зворотного перегляду – між IP–адресами і FQDN–іменами.

Якщо ім’я прямої зони співпадає з іменем домену, то ім’я зворотної зони формується з мережної частини IP–адреси, записаної в зворотному порядку, до якої додається стандартний префікс – in–addr.arpa. Наприклад, кафедрі КЕОА виділено блок IP–адрес 10.12.80.0/24. Ім’я зворотної зони – 80.12.10. in–addr.arpa.

Існують поняття основної зони, додаткової зони і зони – заглушки [5].

Основна зона зберігає базові дані для всіх доменів в зоні. Резервна копія бази даних зони може створюватися в додатковій зоні.

Додаткова зона – повноважна резервна зона для основної зони або інших додаткових зон.

Зона–заглушка (розміщується на сервері) – копія зони, що містить тільки записи ресурсів повноважних DNS–серверів основної зони (master zone).

Записи ресурсів (resource records) – це інформація, що зберігається в базі даних DNS і використовувана для відповіді на запити DNS–клієнтів.

Кожен DNS–сервер містить записи ресурсів, необхідні йому для відповіді на запити, що відносяться до його частини простору імен DNS. Записи ресурсів розрізняються за типами: наприклад, адресний запис (A), канонічне ім'я (CNAME), сервер імен (NS), поштовий обмінник (MX).

Найбільш важливі типи DNS–записів [5].

Запис A (address record) або запис адреси – зв'язує ім'я вузла з IP – адресою. Наприклад, запит A–запису на ім'я www.kpi.ua поверне його IP– адресу – 10.7.10.22.

Запис AAAA (IPv6 address record) зв'язує ім'я вузла з адресою протоколу IPv6.

Запис CNAME (canonical name record) або канонічний запис імені (псевдонім) використовується для перенаправлення на інше ім'я. Дозволяє одній IP– адресі поставити у відповідність декілька імен.

Запис MX (mail exchange) або поштовий обмінник – вказує сервер (и) обміну поштою для даного домену.

Запис NS (name server) – вказує на DNS–сервер для даного домену.

Запис PTR (pointer) або запис вказівника – зв'язує IP – адресу вузла з його канонічним ім'ям. Використовується у зворотній зоні і є аналогом A–запису у прямій зоні. Запит PTR запису в зворотній зоні in–addr.arpa на IP – адресу вузла поверне ім'я (FQDN) даного вузла. З метою зменшення обсягу небажаної кореспонденції (спаму) багато серверів–одержувачів електронної пошти можуть перевіряти наявність PTR запису для вузла, з якого відбувається

відправлення. У цьому випадку PTR запис для IP – адреси повинен відповідати імені відправляючого поштового сервера, яким він представляється в процесі SMTP сесії.

Запис SOA (Start of Authority) або початковий запис зони – вказує на основний DNS – сервер зони, на якому зберігається еталонна інформація про зону, містить контактну інформацію особи, відповідальну за дану зону, задає параметри (серійний номер та часові параметри), необхідні для оновлення інформації про зону резервними DNS–серверами.

SRV–запис (server selection) вказує на сервери для деяких сервісів; використовується, зокрема, для Jabber і Active Directory.

Запис TXT (Text) – текстовий запис, який використовується для внесення коментарів, поміток і т.і.

Особливості налаштування системи DNS на Windows Server 2003

За замовчуванням на всіх комп'ютерах з ОС Windows встановлюється і запускається служба DNS–клієнта. Щоб встановити службу DNS–сервер в Windows Server 2003, потрібно спочатку додати роль DNS–сервера утилітою управління даним сервером (Manage Your Server) [6].

Після додавання цієї ролі в групі програм «Адміністрування» (Administrative Tools) з'являється значок консолі DNS – головного засобу налаштування і спостереження DNS–серверів, зон, доменів і записів ресурсів.

Налаштування параметрів DNS–сервера і створення нових зон значно спрощується, якщо скористатися майстром налаштування DNS–сервера [6]. Він автоматично запускається при додаванні ролі DNS–сервера. Якщо майстер вже закінчив роботу, перевірити і змінити параметри DNS–сервера можна в консолі DNS (її значок є в меню Пуск (Start) / Адміністрування (Administrative Tools)). DNS–сервер можна також налаштувати у вікні властивостей сервера в консолі DNS, зовсім не звертаючись до майстра налаштування DNS–сервера.

Зони прямого і зворотного перегляду створюються засобами майстра налаштування DNS–сервера або консолі DNS [6]. В останньому випадку потрібно натиснути правою кнопкою вкладку «Зони прямого перегляду»

(Forward Lookup Zones) або «Зони зворотного перегляду» (Reverse Lookup Zones) і в контекстному меню вибрати «Створити нову зону» (New Zone). Відкриється вікно «Майстер створення нової зони» (New Zone Wizard).

Нові зони містять тільки два записи ресурсів: початковий запис зони (SOA), якій відповідає даній зоні, і запис сервера імен (NS), у якому визначено DNS–сервер цієї зони. Після створення зони її треба заповнити додатковими записами ресурсів. Одні записи додаються автоматично, а інші (такі як записи MX і CNAME) потрібно зробити вручну.

Щоб вручну додати в зону запис ресурсу, натисніть значок зони в консолі DNS правою кнопкою і виберіть запис ресурсу, який плануєте створити.

Запис ресурсу в зоні створюється так [6].

1. У дереві консолі DNS натисніть потрібну зону правою кнопкою і виберіть «Інші нові записи» (Other New Records). Відкриється вікно «Тип запису ресурсу» (Resource Record Type).

2. У списку «Вибір типу запису ресурсу» (Select a Resource Record Type) виберіть тип запису створюваного ресурсу і натисніть кнопку «Створити запис» (Create Record).

3. У вікні «Новий запис ресурсу» (New Resource Record) введіть інформацію про запис ресурсу і натисніть «ОК».

4. Натисніть «Готово» (Done), щоб повернутися в консоль DNS.

Налаштування комп'ютерів – DNS–клієнтів в мережах ОС Windows передбачає виконання як мінімум наступних задач:

- **визначення на комп'ютері основного суфікса DNS домену.** Додаючи цей суфікс після імені вузла, отримуємо повне ім'я комп'ютера;
- **визначення списку DNS–серверів, використовуваних клієнтами для дозволу DNS–імен.** Цей список складається з основного DNS–сервера, а також (при необхідності) додаткових DNS–серверів, до яких клієнт звертається в разі недоступності основного сервера.

Крім того, в залежності від потреб, можуть бути налаштовані додаткові операції для DNS–клієнтів:

- **задання списку пошуку по DNS–суфіксам**, тобто порядок пошуку при запиті коротких (неповних) доменних імен;
- **встановлення для кожного конкретного адаптера на клієнтському комп'ютері DNS–суфіксів підключень.** Наприклад, вузол hostl.lucernepublishing.com, підключений до двох підмереж через різні мережеві адаптери в одній підмережі може мати ім'я hostl.subnetl.microsoft.com, а в іншій – hostl.subnet2.microsoft.com;
- **зміна порядку динамічного оновлення DNS.**

Коли у клієнта DNS виникає необхідність знайти зазначене додатком ім'я, він направляє на DNS–сервер запит на розпізнавання імені. Кожне таке повідомлення–запит містить таку інформацію:

• доменне ім'я DNS у вигляді FQDN;

• тип запиту. Запис ресурсу або тип операції запиту;

• визначення класу доменного імені DNS. Для служби DNS–клієнт цей клас завжди визначається як клас Інтернету (IN).

Для перевірки роботи системи розпізнавання імен використовують утиліту nslookup.

Nslookup – утиліта командного рядка (присутня у більшості ОС, у тому числі Windows), яка дозволяє направляти тестові запити на DNS–сервери і отримувати докладні відповіді у вікні командного рядка. Ця інформація використовується для діагностики та усунення несправностей зіставлення імен, перевірки коректності додавання або оновлення записів ресурсів в зони і т.і.

Nslookup можна виконувати як одноразову команду (неінтерактивний режим) або як програму, приймаючу послідовність команд і запитів (інтерактивний режим).

Контрольні запитання

1. Які типи адрес можуть бути у вузла?
2. Які типи імен можуть бути у вузла?
3. Які служби та механізми можуть бути використані для вирішення задачі перетворення імен в адреси?
4. Яку функцію виконує служба DNS?
5. Яку функцію виконує служба WINS?
6. Як побудовано простір імен DNS ?
7. За якими критеріями поділяють домени верхнього рівня?
8. Якими засобами може встановлюватись відповідність між доменними іменами (FQDN) і IP–адресами ?
9. Яку схему взаємодії покладено в основу функціонування системи DNS?
10. Що характерно для нерекурсивної або ітеративної процедури роботи системи DNS?
11. Що характерно для рекурсивної процедури роботи системи DNS?
12. Який порядок визначення імен за механізмом DNS застосовується на вузлу?
13. Що розуміють під DNS сервером?
14. На які типи поділяють DNS сервера?
15. Що розуміють під зоною DNS?
16. Які існують типи зон DNS?
17. Яку функцію виконує пряма зона DNS?
18. Яку функцію виконує зворотна зона DNS?
19. Призначення основних типів записів (A, NS, SOA, MX, CNAME, PTR, TXT).

1.5. Лабораторна робота № 5. НАЛАШТУВАННЯ ТА ВИКОРИСТАННЯ МЕРЕЖНОГО СЕРВІСУ DHCP

Мета та основні завдання: навчитись вирішувати задачі по налаштуванню та адмініструванню сервісу DHCP

Порядок виконання роботи

1. Ознайомитися з документацією.
2. Ознайомитися з налаштуваннями і адмініструванням сервера DHCP (програмна група «Адміністрування» – DHCP).
3. Виконати практичні налаштування згідно завдання.
4. Розібратися з конфігуруванням клієнтів DHCP сервера («панель керування – мережа–протокол TCP / IP») та перевірити роботу системи.

Основні теоретичні відомості

DHCP (Dynamic Host Configuration Protocol) – це протокол зі стеку TCP/IP, що автоматизує призначення IP–адрес вузлам мережі [5].

Для використання протоколу TCP/IP в мережі адміністратор повинен встановити для кожного з комп'ютерів щонайменше три параметри – IP–адресу, маску підмережі та адресу використовуваного за замовчуванням шлюзу. При цьому кожен комп'ютер повинен мати унікальну IP–адресу. Крім того, присвоєна адреса повинна знаходитися в діапазоні підмережі, до якої підключено пристрій. Якщо в мережі використовуються Windows Internet Naming Service (WINS) і Domain Name Service (DNS), то на кожному з клієнтських комп'ютерів адміністратору необхідно також вказати IP–адреси WINS і DNS–серверів.

Адміністратор може конфігурувати кожну з систем вручну або використати можливість автоматичного конфігурування за допомогою протоколу DHCP. Це потребує встановлення та налаштування одного або

кількох DHCP–серверів так, щоб вони автоматично присвоювали IP–адреси кожному комп'ютеру в мережі. Для цього достатньо сконфігурувати сервер, ввести діапазони адрес, налаштувати декілька додаткових параметрів і періодично здійснювати моніторинг.

За наявності в мережі DHCP–сервера клієнти, що підтримують протокол DHCP, автоматично отримують IP–адреси та пов'язані з ними параметри при кожному запуску і підключенні до мережі. DHCP–сервер надає конфігурацію клієнтам, що звернулися, у формі оренди адреси.

Одна з основних переваг протоколу DHCP полягає в тому, що DHCP–сервери значно скорочують час налаштування комп'ютерів в мережі. DHCP спрощує адміністрування не тільки за рахунок надання клієнтам IP–адрес, але і (при необхідності) адреси основного шлюзу, адрес DNS і WINS–серверів, а також інших необхідних клієнтам серверів. У DHCP є ще одна перевага: автоматичне призначення IP–адрес дозволяє уникнути помилок конфігурування, неминучих при ручному визначенні параметрів IP на кожному мережному вузлі. Зокрема, DHCP запобігає конфліктам адрес, що виникають через помилкове присвоєння однакових IP–адрес двом мережним вузлам.

Крім того, DHCP дозволяє здійснювати спільне використання IP–адрес. Припустимо, у вас є 50 вільних адрес і відділ зі штатом в 100 чоловік. Співробітники відділу проводять в офісі всього 1–2 дні на тиждень; таким чином, одночасно до мережі завжди підключені тільки 30–40 комп'ютерів. Кожного разу при підключенні до мережі співробітник отримує IP адресу. Після відключення система відновлює адресу, щоб видати її наступному користувачеві.

У невеликих локальних мережах для вирішення задачі автоматичного призначення IP – адрес може бути використана служба APIPA (Automatic Private IP Addressing) – служба для забезпечення роботи локальної мережі в разі, коли немає сервера DHCP та комп'ютери налаштовані на автоматичне отримання IP–адрес. При цьому комп'ютерам мережі автоматично

призначаються вільні адреси в діапазоні 169.254.XXX.XXX, маска 255.255.0.0. Служба APIPA кожні 5 хвилин перевіряє наявність DHCP–сервера і якщо такий з'явиться, управління отриманням IP–адрес буде передано йому. DHCP–сервер замінить адресу, отриману від APIPA на динамічну адресу, що призначається зі налаштованого на сервері діапазону.

Принцип роботи протоколу DHCP

Як було зазначено вище, для використання сервісу DHCP необхідно сконфігурувати, як мінімум, один DHCP–сервер. На сервері необхідно створити одну або декілька областей DHCP (DHCP scope) і задати додаткові параметри, які будуть автоматично передаватися клієнту [6].

Область DHCP (DHCP scope) являє собою сукупність IP–адрес (наприклад, адреси з діапазону 192.168.0.11–192.168.0.254) логічної підмережі, які DHCP–сервер присвоює клієнтам.

Крім IP–адрес в областях визначають і інші параметри для мережних клієнтів. Найчастіше використовуються наступні параметри: основний шлюз, маска підмережі, DNS сервер, ім'я домену. Протокол DHCP дозволяє передавати і велику кількість інших параметрів. Наприклад, можна передавати додаткові маршрути, щоб у різні мережі комп'ютер ходив через різні шлюзи. Або за допомогою DHCP можна організувати завантаження пристроїв по мережі. У цьому випадку клієнт отримує крім основних параметрів, адресу TFTP сервера та ім'я файлу на ньому (файл, який містить образ ОС для завантаження).

Процедура роботи протоколу DHCP наступна. Коли клієнт, наприклад, звичайний комп'ютер, запускається, ОС бачить, що з певної мережевої карти варто «Отримати параметри по DHCP». Такий комп'ютер, поки що, не має IP адреси.

1. Комп'ютер надсилає широкомовний запит. При цьому на другому рівні у кадрі стоїть мак адреса відправника – адреса комп'ютера, мак адреса одержувача – ffff.ffff.ffff, а на третьому рівні – у IP пакеті – адреса відправника

0.0.0.0, адреса одержувача 255.255.255.255. Таке DHCP повідомлення називається **DHCP discover**.

2. Далі всі пристрої в мережі отримують це широкомовне повідомлення. DHCP сервери (а їх теоретично може бути декілька) відповідають клієнту. Сервер резервує у своєму пулі адрес будь–яку адресу (якщо не було резервації до цього для даної mac–адреси клієнта) і виділяє цю IP–адресу клієнту на певний час (lease time). Призначена IP–адреса разом з іншими параметрами, які налаштовані на DHCP–сервері (маска, шлюз і т.і.) надсилається клієнту. При цьому, як адреса одержувача в IP пакеті, використовується широкомовна адреса 255.255.255.255 (мак адреса клієнта зазначена у відповідному полі цього повідомлення), а адреса відправника – IP–адреса DHCP сервера. Таке повідомлення носить назву **DHCP offer**. Для зменшення широкомовних повідомлень у мережі можлива реалізація, коли, як адреса одержувача, буде використана призначена клієнту IP–адреса (в адресному полі одержувача кадра – мас адреса клієнта).

3. При наявності відповідей від декількох DHCP серверів, клієнт, зазвичай, обирає сервер, який відповів першим. На повідомлення цього сервера клієнт надсилає повідомлення зі згодою на отримання IP–адреси – **DHCP request.** В IP пакеті, який містить це повідомлення, у якості адреси відправника буде вказана IP–адреса 0.0.0.0, а адресою одержувача буде широкомовна адреса 255.255.255.255, щоб це повідомлення змогли отримати усі DHCP сервери. IP–адреса DHCP сервера, якого обрав клієнт, буде вказана у відповідному полі цього повідомлення. Для зменшення широкомовних повідомлень у мережі можлива реалізація, коли у якості адреси відправника буде вказана отримана клієнтом IP–адреса, а адресою одержувача буде IP–адреса DHCP сервера, якого обрав клієнт.

4. Після отримання DHCP request від клієнта сервер резервує за клієнтом виділену адресу на певний час (Lease Time). Тепер IP–адреса буде остаточно закріплена за клієнтом протягом Lease Time. Сервер вносить також рядок у свою ARP таблицю і надсилає клієнту, повідомлення, що він успішно

зареєстрований – **DCHP Acknowledge**. В залежності від реалізації, повідомлення може надсилатися на широкомовну адресу 255.255.255.255 (мак адреса клієнта зазначена у відповідному полі цього повідомлення), або на призначену клієнту IP–адресу (в адресному полі одержувача кадра – мас адреса клієнта).

5. Клієнт починає працювати.

При призначенні адрес і клієнт і сервер можуть перевіряти їхню унікальність. Припустимо, на сервері налаштований пул адрес, який починається з адреси 192.168.13.2. Перша адреса пулу призначена комп'ютеру вручну одним із користувачів мережі. При призначенні такої адреси по DHCP відбудеться конфлікт. Для розв'язання конфліктів може бути використаний такий механізм.

1. Після отримання повідомлення DHCP discover сервер вибирає першу адресу з пулу (в даному випадку 192.168.13.2) і відправляє на неї ARP–запит. Оскільки комп'ютер з такою адресою існує в мережі, сервер отримує відповідь.

2. Щоб переконатися в наявності в мережі вузла з адресою 192.168.13.2, сервер відправляє на цю адресу Echo–Request ICMP протоколу і отримує відповідь.

3. У такому випадку сервер бере наступну вільну адресу з пулу (в даному випадку 192.168.13.3) і відправляє на неї ARP–запит.

4. Не дочекавшись відповіді протягом визначеного тайм–ауту (зазвичай – 15 сек.), сервер вважає адресу вільною і пропонує її клієнту в повідомленні DHCP request.

5. Клієнт, підтвердивши отримання адреси і дочекавшись підтвердження від сервера, також перевіряє, чи не зайнята видана адреса. Це робиться шляхом відправлення ARP–запитів клієнтом. Якщо відповідь на запит не надійшла, клієнт призначає собі на інтерфейс отриману адресу.

Встановлення та налаштування DHCP– серверу

Щоб встановити роль DHCP–сервера з вікна управління сервером в меню «Пуск» (Start) виберіть «Керування даним сервером» (Manage Your Server), натисніть «Додати або видалити роль» (Add or Remove a Role) [6]. Далі у вікні майстра виберіть роль «DHCP–сервер» (DHCP Server) і два рази натисніть «Далі» (Next).

При налаштуванні DHCP серверу, перш за все, необхідно створити область (scope) [6].

1. Задаємо ім'я області та її опис.
2. Вводимо діапазон адрес та маску підмережі. Після створення області адрес, маску змінити не можна. Вам або доведеться додавати ще одну область і настроювати маршрутизацію між підмережами, або видаляти існуючу і створювати заново.
3. Додаємо виключення на той випадок, коли деякий діапазон із загального, виділяється для резервування за обладнанням (сервери, маршрутизатори, точки доступу і т.і.).
4. Встановлюємо термін дії оренди виданої адреси. Кожна адреса виділяється сервером для певного комп'ютера. Коли комп'ютер запросив адресу, сервер створює запис для нього. Час життя запису – це термін дії оренди. За замовчуванням він дорівнює 8–и дням.
5. Наступним кроком є налаштування додаткових опцій (шлюз за замовчуванням, ім'я домену та адреси DNS серверів, інші додаткові опції – сервер WINS, сервери часу і т.і.).
6. По закінченні налаштувать необхідно активувати налаштувань область.

Розподіл IP–адрес

Протокол DHCP надає три способи розподілу IP–адрес [5].

Ручний розподіл. В цьому способі адміністратор мережі зіставляє апаратному адресу (для Ethernet мереж це MAC–адреса) кожного клієнтського комп'ютера певну IP–адресу. Фактично, даний спосіб розподілу адрес відрізняється від ручного налаштування кожного комп'ютера лише тим, що

відомості про адреси зберігаються централізовано (на сервері DHCP), і тому їх простіше змінювати за необхідності.

Автоматичний розподіл. В даному способі кожному комп'ютеру на постійне використання виділяється довільний вільний IP–адрес з заданого адміністратором діапазону.

Динамічний розподіл. Цей спосіб аналогічний автоматичному розподілу, за винятком того, що адреса видається комп'ютеру не на постійне користування, а на певний термін. Це називається орендою адреси. Після закінчення терміну оренди IP–адреса знову вважається вільною, і клієнт зобов'язаний запросити нову (вона може виявитися тією ж самою). Крім того, клієнт сам може відмовитися від отриманої адреси.

Деякі реалізації служби DHCP здатні автоматично оновлювати записи DNS, що відповідають клієнтським комп'ютерам, при виділенні їм нових адрес. Таке оновлення виконується за допомогою протоколу оновлення DNS, описаного в RFC 2136.

Діапазон IP–адрес

Діапазон IP–адрес, який виділяється для області, повинен складатися з послідовної сукупності адрес, що складають IP підмережу. Разом з тим з діапазону треба виключити адреси всіх комп'ютерів мережі, яким призначені статичні адреси. Можна обмежити діапазон області так, щоб статичні адреси в нього не входили. Є й інший спосіб: сконфігурувати область, що охоплює цілу підмережу, а потім визначити діапазони виключень (exclusion ranges), де вказати адреси, статично закріплені за вузлами.

Найпопулярніший метод одночасної підтримки в діапазоні статичних і динамічних адрес – зарезервувати декілька перших адрес підмережі для серверів зі статичними адресами, а DHCP–область почати з наступної адреси. Наприклад, в підмережі 192.168.1.0 зарезервувати адреси 192.168.1.1–192.168.1.10 для серверів з незмінними адресами (DHCP–сервер, DNS–сервер, WINS–сервер та ін), а діапазон 192.168.1.11–192.168.1.254 призначити DHCP–області підмережі.

Якщо серверам мережі вже призначені статичні адреси з діапазону підмережі, наприклад, 192.168.1.110 або 192.168.1.46, рекомендується використовувати діапазони виключень, щоб ці адреси не призначалися іншим комп'ютерам. Інакше доведеться сильно обмежити кількість адрес для оренди, так як для підмережі дозволяється тільки один діапазон області IP–адрес.

Діапазон виключення (exclusion range) – це сукупність одного або декількох IP–адрес з діапазону області, які неповинні надаватися в оренду DHCP–клієнтам. Якщо ці адреси включити в діапазон виключення, сервер ніколи не надасть їх DHCP–клієнтам в оренду.

Діапазони виключення можна використовувати і на краях діапазонів. Наприклад, визначити область 192.168.1.1–192.168.1.254 з діапазоном виключення 192.168.1.1–192.168.1.10 (сервери підмережі з налаштованими вручну статичними IP–адресами).

Створення резервування

Резервування (reservation) використовується для створення постійної оренди адреси, виділеної DHCP–сервером. Таким чином забезпечується призначення незмінних адрес певним пристроям в підмережі. Наприклад, у DHCP–області з діапазоном 192.168.1.11–192.168.1.254 можна зарезервувати IP–адресу 192.168.1.100 за мережним адаптером з апаратною адресою 00–bO–dO–01–18–86. При кожному перезавантаженні комп'ютера з цим адаптером сервер розпізнає апаратну MAC–адресу адаптера і надає йому в оренду одну й ту ж IP–адресу — 192.168.1.100.

Щоб створити резервування в консолі DHCP, відкрийте потрібну область, натисніть вкладку «Резервування» (Reservations) правою кнопкою і виберіть «Створити резервування» (New Reservations) [6]. Відкриється діалогове вікно «Створити резервування» (New Reservation). Налаштуйте резервування, вказавши потрібні значення в полях «Ім'я клієнта» (Reservation name), «IP–адреса» (IP address) і «MAC–адреса» (MAC address).

Присвоєння параметрів DHCP

DHCP дозволяє одночасно з виділенням адреси в оренду надавати клієнтам додаткові конфігураційні дані, наприклад адреси певних серверів. Зокрема, клієнтський комп'ютер, на якому у властивостях протоколу TCP / IP задано автоматичне отримання адреси DNS–сервера, отримає цю адресу (або набір таких адрес) з DHCP–сервера.

Конфігураційні параметри налаштовуються на рівні резервування, області або сервера. Параметри рівня резервування володіють найвищим пріоритетом, а параметри області переважають параметри сервера [6].

Щоб налаштувати конфігураційні параметри, виберіть значок потрібного резервування в дереві консолі DHCP, а потім у меню «Дія» (Action) або в контекстному меню виберіть команду «Настроїти параметри» (Configure Options) [6]. Щоб налаштувати параметри для області (по завершенні Майстра створення області (New Scope Wizard), виберіть у дереві консолі DHCP папку «Параметри області» (Scope Options), а потім в меню «Дія» або в контекстному меню виберіть команду «Настроїти параметри». Аналогічно настроюються параметри для сервера. Діалогове вікно, яке відкривається при кожній з цих процедур, практично однакове в усіх трьох випадках.

Доступно більше 60 стандартних параметрів DHCP [6]. Найбільш часто використовуються перераховані нижче.

- 003 Маршрутизатор (003 Router) – список IP–адрес маршрутизаторів в одній з DHCP–клієнтами підмережі. Клієнт відправляє цим маршрутизаторам IP–пакети, адресовані віддаленим вузлам мережі.
- 006 DNS–сервери (006 DNS Servers) – IP–адреси DNS–серверів, до яких можуть звертатися DHCP–клієнти із запитами на розпізнавання доменних імен вузлів.
- 015 DNS–ім'я домену (015 DNS Domain Name) – доменне ім'я, яке використовується DHCP–клієнтами в процесі розв'язання неповних DNS–імен.

Цей параметр так само дозволяє клієнтам здійснювати динамічне оновлення в DNS.

- 051 Оренда (051 Lease) – параметр, що визначає особливий термін оренди; застосовується тільки для віддалених клієнтів.

Налаштування клієнта

Щоб налаштувати клієнт на отримання IP–адреси від DHCP–сервера, відкрийте діалогове вікно «Властивості: Протокол Інтернету (TCP / IP)» (Internet Protocol (TCP/IP) Properties) для відповідного мережного підключення. При виборі варіанту «Отримати IP–адресу автоматично» (Obtain an IP address automatically) клієнт отримує від DHCP–сервера IP–адресу, маску підмережі і всі параметри DHCP, крім параметрів DNS. Щоб налаштувати клієнта на отримання параметрів DNS з DHCP–сервера, потрібно вибрати в тому ж вікні варіант «Отримати адресу DNS–сервера автоматично» (Obtain DNS Server address automatically). Якщо клієнт до цього мав статичний адресу, нова конфігурація набуває чинності відразу після закриття відкритих діалогових вікон.

Після налаштування та авторизації DHCP–сервера і активування області потрібно перевірити роботу служби на всіх клієнтських комп'ютерах. Відключіть/включіть відповідне мережне підключення на комп'ютері – DHCP–клієнті, (або скористайтеся командою ipconfig /renew) для оновлення налаштувань IP–адреси, а потім у командному рядку виконайте команду ipconfig /all. На екрані буде відображено усі параметри мережних підключень, включаючи і поточні параметри DHCP.

Контрольні запитання

1. Яку функцію виконує сервіс DHCP?
2. Для вирішення яких завдань використовується DHCP ?
3. Як повинна бути призначена IP–адреса серверу в мережі?
4. Як повинна бути призначена IP–адреса на інтерфейси маршрутизатора, на якому працює протокол динамічної маршрутизації?

5. Як може бути призначена IP–адреса звичайному ПК в мережі?
6. Яка IP–адреса джерела буде стояти в запиті від DHCP–клієнта, який від надсилає на DHCP–сервер для отримання IP–адреси?
7. Яка IP–адреса отримувача буде стояти в запиті від DHCP–клієнта, який від надсилає на DHCP–сервер для отримання IP–адреси?
8. Чи повинен DHCP–клієнт знати IP–адресу DHCP–сервера у мережі?
9. Що розуміють під областю DHCP (DHCP scope)?
10. Скільки областей з різними блоками IP–адрес можна створити на DHCP–сервері?
11. Чи можливо з діапазону IP–адрес «вирізати» частину, адреси з якої не будуть видаватися клієнтам?
12. Яким параметром визначається час, на який IP–адреса закріплюється за клієнтом?
13. Чи можливо видати IP–адреси усім клієнтам на необмежений термін?
14. Чи можливо закріпити конкретну IP–адресу за конкретним вузлом?
15. Що необхідно використати у якості ідентифікатору вузла для закріплення за ним IP–адреси на постійній основі в налаштуваннях DHCP–серверу?
16. Який мінімальний набір параметрів необхідно передати клієнту (крім IP–адреси) для його нормальної роботи в IP–мережі і виходу в Інтернет?
17. Які налаштування необхідно виконати на DHCP–клієнті?
18. Чи може виникнути якась проблеми при спільному використанні сервісів DNS і DHCP ? Якщо так, у чому вона полягає.
19. Які типи записів необхідно зробити для DHCP–клієнтів в DNS?
20. Яку IP–адресу отримає DHCP–клієнт, якщо в мережі відсутній DHCP–сервер?

1.6. Лабораторна робота № 6. НАЛАШТУВАННЯ ТА АДМІНІСТРУВАННЯ IIS (Internet Information Services)

Мета та основні завдання: вивчити можливості служби IIS, навчитись вирішувати задачі по налаштуванню та адмініструванню серверу IIS.

Порядок виконання роботи

1. Ознайомитися з методичними матеріалами.
2. Ознайомитися з налаштуваннями і адмініструванням сервера IIS (програмна група «Адміністрування» – Диспетчер служб IIS).
3. Виконати практичні налаштування WEB–вузла згідно завдання.
4. Перевірити доступ до стартової сторінки WEB–вузла.

Основні теоретичні відомості

Крім поняття Інтернет–мережі, під якою розуміють всесвітню глобальну інформаційну мережу, в сучасних корпоративних мережах існують поняття «Інтранет» та «Екстранет».

Intranet (Інтранет) – перенесення інформаційних технологій глобальної мережі Internet на рівень локальної мережі. Дана технологія передбачає організацію внутрішніх інформаційних ресурсів: web, ftp–сервера, внутрішньої електронної пошти, пошукових систем і ін.

Extranet (Екстранет) – перенесення інформаційних технологій глобальної мережі Internet на рівень корпоративних територіально–розподілених мереж.

Intranet включає 5 основних систем:

– інформаційна (web, ftp–вузли),

– система розпізнавання імен (DNS),

– система адресації вузлів і транспортна система (стек TCP/IP),

– система електронної пошти і телеконференцій,

– система безпеки і контролю доступу.

Служба IIS

IIS (Internet Information Services, до версії 5.1 — Internet Information Server) — це набір серверів для декількох служб Інтернету від компанії Майкрософт [7].

Основний компонент IIS — Web–сервер, який дозволяє створювати Web–вузли. IIS підтримує протоколи HTTP, HTTPS, FTP, POP3, SMTP, NNTP.

Створення Web–сайту

Ви можете використовувати Default Web Site для хостингу додатків ASP або ASP.NET, але зазвичай краще створювати для цих додатків нові Web–сайти.

Щоб створити новий Web–сайт за допомогою IIS Manager, виконайте такі кроки [7].

- Натисніть правою кнопкою на вузлі «Web Sites» і виберіть «New Web Site» (Створити /Web–сайт).
- Натисніть на кнопці «Next» у вікні, майстра створення Web–сайту «Web Site Creation Wizard».
- У полі «Description» (Опис) введіть опис сайту, наприклад, «Sample Web Site», і натисніть на кнопці «Next».
- Виберіть унікальну IP–адресу для цього сайту або вкажіть ім'я, яке буде передаватися в заголовку HTTP і натисніть на кнопці «Next».
- Виберіть каталог, який буде використовуватись у якості домашнього каталогу для цього сайту, або створіть новий каталог. Якщо ви не хочете, щоб анонімні користувачі мали доступ до вашого сайту, скиньте відповідний прапорець. Потім натисніть на кнопці «Next».
- Задайте права доступу користувачів до домашнього каталогу. За замовчуванням дозволені права «Read» (Читання) і «Run Scripts» (Запуск скриптів) і заборонені всі інші права. Налаштовані права доступу застосовуються в рівній мірі до всіх користувачів, які підключаються до

даного сайту (налаштуйте потім потрібні права на рівні NTFS для домашнього каталогу, щоб забезпечити більш високий рівень захисту сайту).

- Натисніть кнопку «Next» і потім кнопку «Finish».

Конфігурування Web–сайту

Після створення сайту ви можете сконфігурувати його, відкривши сторінку його властивостей. Натисніть правою кнопкою на вузлі для цього сайту та виберіть пункт «Properties» [7]. Потім використовуйте наступні вкладки цієї сторінки, щоб задати обліковий запис (identity) для цього сайту, ведення журналу, регулювання пропускної здатності, обмеження кількості одночасних з'єднань, домашню папку, права доступу, налаштування додатків, документи за замовчуванням, методи автентифікації, обмеження по IP–адресами, нестандартні повідомлення про помилки і т.і.

Створення додатку

Створимо простий ASP–додаток, що виконує дії, які ми можемо перевірити, наприклад, визначення поточного часу на сервері. Це робить наступний скрипт.

```
<html> <head> <title> Sample ASP Application </title>
</Head>
<body>
<%
Dim strMessage
strMessage = "Sample ASP Application"
Response.Write (strMessage)
Response.Write ("<hr>")
Response.Write ("The time is" & Time ())
%>
</Body>
</Html>
```

Введіть цей сценарій в Notepad і збережіть його під ім'ям default.asp в домашній папці, яку ви задали для свого нового Web–сайту. Для застосування додатку в IIS Manager натиснувши клавішу F5, натисніть правою кнопкою на вузлі «Sample Web» і потім виберіть пункт «Browse», щоб перевірити, чи працює це додаток [7].

За замовчуванням IIS конфігурує це новий додаток під тим же ім'ям – «Default Application», тому давайте змінимо його.

1. Натисніть правою кнопкою миші на вузлу «Sample Web Site» і виберіть пункт «Properties».
2. Перейдіть у вкладку «Home Directory» (Домашня папка).
3. Видаліть ім'я «Default Application» і замініть його на «Sample Application». Потім натисніть кнопку «Apply» (Застосувати).

Тепер у нас є ASP–додаток з ім'ям «Sample Application», точкою запуску якого є домашній каталог сайту Sample Web Site.

Віртуальний каталог

Віртуальний каталог – це окремий від домашнього каталог у структурі сайту, ім'я якого задається в IIS і вказує на фізичний каталог на локальному або віддаленому сервері [7]. Це ім'я каталогу стає частиною URL–адреси Web–сайту і користувачі зможуть використовувати дану URL–адресу в браузері з метою отримання доступу до вмісту фізичного каталогу, наприклад, Web–сторінки або списку додаткових каталогів і файлів. Web–сайт може містити не один, а кілька віртуальних каталогів. Наприклад, віртуальний каталог використовується в тому випадку, якщо до Web–сайту потрібно включити зображення з іншого місця файлової системи, але небажано переміщати файли зображень у фізичний каталог, який поставлений у відповідність домашньому каталогу Web–сайту. Аналогічно шляхом використання віртуальних каталогів можна підключити до сайту інформаційне наповнення інших сайтів без необхідності його копіювання у домашній каталог. Крім того віртуальні каталоги можуть бути використані для розміщення в них інформаційного наповнення з різними правами доступу (гіпертекст, скрипти, бази даних і т.і.).

Створення віртуального каталогу за допомогою диспетчера IIS [7]

1. В IIS Manager розгорніть локальний комп'ютер і Web–вузол, до якого потрібно додати віртуальний каталог.

2. Натисніть правою кнопкою миші на вузлу або каталогу, де потрібно створити віртуальний каталог, натисніть «Створити» та натисніть кнопку «Віртуальний каталог».

3. У «Майстрі створення віртуального каталогу» натисніть «Далі».

4. У полі «Псевдонім» введіть ім'я віртуального каталогу та натисніть «Далі». Виберіть коротку назву, яку просто вводити, оскільки користувачі вводять це ім'я для доступу до його вмісту.

5. У полі «Шлях» введіть або виберіть фізичний каталог, що буде відповідати віртуальному каталогу, і натисніть кнопку «Далі». Можна вибрати існуючий каталог або створити новий для розміщення вмісту віртуального каталогу.

6. Встановіть прапорці прав доступу, які потрібно призначати користувачам. За замовчуванням прапорці «Читання» і «Запуск скриптів» встановлені. Вони дозволяють запустити сторінки ASP.NET для багатьох поширених скриптів.

7. Натисніть кнопку «Далі», а потім «Готово».

Налаштування безпеки та перевірка справжності віртуального каталогу [7]

1. В IIS Manager натисніть правою кнопкою миші вузол віртуального каталогу, який потрібно настроїти, і натисніть кнопку «Властивості».

2. Натисніть вкладку «Безпека каталогу», виберіть «Управління перевіркою достовірності та доступом» та натисніть «Змінити».

3. Встановіть прапорець для методу перевірки автентичності або методів, які потрібно використовувати для віртуального каталогу, а потім натисніть «ОК». «Дозволити анонімний доступ» і «Вбудована перевірка достовірності Windows» вже встановлені. Два найбільш поширені сценарії перевірки автентичності: вбудована перевірка достовірності Windows для вузлів локальної інтранет–мережі; перевірка справжності форм для вузла Інтернету або екстранет–мережі, де користувачі отримують доступ до вузла через міжмережний екран.

4. Щоб налаштувати перевірку автентичності користувачів зніміть прапорець «Включити анонімний доступ» і переконайтеся, що встановлений прапорець «Вбудована перевірка справжності».

5. У провіднику Windows відкрийте домашній каталог, який буде містити сторінки вузла. Натисніть правою кнопкою миші каталог і натисніть «Загальний доступ і безпека». Буде відкрито діалогове вікно «Властивості».

6. Перейдіть на вкладку «Безпека».

7. У списку «Групи або імена користувачів» виберіть групу або ім'я користувача.

8. У списку «Дозволити» виберіть відповідні права для групи або імені користувача.

9. Натисніть кнопку «Застосувати».

10.Натисніть кнопку «ОК».

Застосування політики безпеки [7]

Права та обмеження, що привласнюються користувачам для роботи з ресурсами системи, дозволяють застосовувати політику безпеки до управління та доступу до інформації. У таблиці 1.5 наведено ключові параметри безпеки ресурсів Web–сервера.

Методи автентифікації в Microsoft IIS [7]

Анонімна автентифікація

Anonymous Authentication (Анонімна автентифікація) дозволяє користувачам входити на сайт без введення імені користувача або пароля. Коли користувач підключається до загального Web–сайту, Web–сервер присвоює йому обліковий запис Windows з ім'ям IUSR_ *<ім'я_комп'ютера>,* де *<ім'я_комп'ютера>* – ім'я сервера, на якому виконується IIS.

Користувач, який реєструється із записом IUSR, входить до групи Guests і, за замовчуванням, як член цієї групи, володіє правом доступу до різних даних на сервері. Анонімні Web–користувачі, як правило, в домені не реєструються. Замість цього вони звертаються до ресурсів сервера через програмне забезпечення IIS.

Таблиця 1.5 – Параметри політики безпеки Web–сервера

Параметр	Опис
Правила безпеки IP	Встановлення фільтрів IP–трафіку. Визначення причин і способів шифрування пакетів.
Присвоєння /створення/ передача повноважень адміністрування	Призначення адміністратора, відповідального за вміст і безпека сервера. Налаштування псевдо–адміністративних ролей.
Присвоєння /створення облікових записів користувачів	Налаштування анонімних і автентіфікованих облікових записів.
Правила безпеки облікових записів	Задання груп, до яких належать облікові записи. Використання блокування при введенні неправильного пароля. Задання числа спроб введення пароля перед блокуванням, а також тривалість блокування. Зазначення терміну дії користувацького сертифікату Kerberos.
Правила безпеки груп	Вказують групи, членів груп, а також правила, застосовані до груп.
Визначення правил безпеки паролів	Встановлення мінімальної довжини паролів, дозволу /заборони використання "порожніх" паролів. Встановлення відмови на повторне використання паролів. Визначення вимог для чисельно–буквених паролів.
Правила конфіденційності даних	Встановлення дозволів на каталоги та файли.

Якщо включена анонімна автентифікація, IIS в першу чергу буде автентифікувати користувачів за допомогою цього методу, навіть якщо включені інші методи автентифікації. У деяких випадках браузер запросить у користувача ім'я та пароль.

При використанні анонімної автентифікації можна включити опцію «Allow IIS To Control Password» (Дозволити IIS управління паролем) [7]. Коли дозволено керування паролем, користувач вже не виконує локальний вхід, а входить у систему з використанням мережного входу. При мережному вході існують декілька проблем. Наприклад, неможливість доступу до віддаленого ресурсу на іншому сервері. У цьому випадку слід відключити параметр «Allow IIS To Control Password» (Дозволити IIS управління паролем) в «Internet Services Manager» (Диспетчер служб інтернету). Слід обов'язково перевстановити пароль в «User Manager» (Диспетчер користувачів), щоб він відповідав облікового запису.

Базова автентифікація

Метод «Basic Authentication» (Базова автентифікація) широко використовується і є стандартним методом запиту імені користувача і пароля. За допомогою опції «Basic Authentication» Web–браузер на комп'ютері клієнта відображує діалогове вікно, в якому користувач вводить раніше призначені йому ім’я і пароль. Після підтвердження сервером IIS відповідності імені користувача і пароля дійсному обліковому запису Windows буде встановлено з'єднання.

Перевага базової автентифікації полягає в тому, що вона є частиною специфікації HTTP і підтримується більшістю браузерів. Недоліком є те, що Web–браузери, що використовують базову автентифікацію, передають паролі в незашифрованому вигляді. За допомогою моніторингу каналів зв'язку мережі зловмисник може легко перехопити і розшифрувати паролі з використанням загальнодоступних засобів. Не застосовуйте базову автентифікацію, якщо немає впевненості в тому, що канал зв'язку між користувачами і Web–сервером надійно захищений.

Інтегрована автентифікація Windows

Integrated Windows Authentication (Інтегрована автентифікація Windows) являє собою безпечну форму автентифікації, яка використовує криптографічний метод, званий хешуванням. В результаті здійснюється безпечний обмін даними між клієнтом і сервером.

На відміну від базової, інтегрована автентифікація спочатку не запитує у користувачів імена і паролі. Вона використовує інформацію про користувача з поточного сеансу на комп'ютері клієнта. Якщо автентифікація не змогла ідентифікувати користувача, браузер запросить у нього ім'я і пароль облікового запису для обробки інтегрованої автентифікацією.

Інтегрована автентифікація використовує як протокол автентифікації Kerberos v5, так і свій власний протокол типу "питання/відповідь". Якщо на сервері встановлений компонент «Directory Services» (Служби каталогів),

використовуються обидва ці протоколу, в іншому випадку використовується тільки протокол "питання/відповідь".

Асоціювання клієнтських сертифікатів

Можна асоціювати (або зв'язувати) клієнтські сертифікати з обліковими записами користувачів на Web–сервері [7]. Після створення і включення карти сертифікатів при кожному вході в систему користувача з сертифікатом клієнта Web–сервер буде автоматично зв'язувати цього користувача з відповідним обліковим записом Windows. Можна пов'язати один або декілька сертифікатів клієнта з обліковим записом Windows. Наприклад, якщо на сервері представлено декілька підрозділів компанії або кілька сайтів, використовується зв'язування "багато до одного" для асоціювання усіх сертифікатів клієнтів кожного підрозділу або компанії відповідному Web–сайту. Таким чином, доступ до кожного сайту буде дозволений тільки його безпосереднім клієнтам.

Організація декількох сайтів на одному сервері

Можливі три варіанті створення декількох сайтів на одному вузлу [7]:

- за кожним сайтом закріплюється окрема IP–адреса (в DNS робляться відповідні A–записи для кожного сайту);
- усі сайти закріплені за однією IP–адресою, але відрізняються номерами портів (в DNS робиться один A–запис для сервера і CNAME записи для кожного сайту. Схема допускає можливість використання одного імені для усіх сайтів. В такому випадку в DNS достатньо створити один A–запис. При введенні URL сайту в адресному рядку інтернет–браузера користувачам необхідно явно задавати номер порта для підключення, наприклад, kpi.ua:8000, kpi.ua:8001);
- усі сайти закріплені за однією IP–адресою і використовують один номер порта (зазвичай «80», який відповідає HTTP протоколу), але відрізняються іменами, які передаються у заголовках HTTP (в DNS робиться один A–запис для сервера і CNAME записи для кожного сайту).

Для організації (хостингу) декількох сайтів на одному Web–сервері необхідно зробити наступне. По–перше, потрібно розмістити HTML–файли різних сайтів в різних каталогах. По–друге, потрібно вказати Web–серверу метод, що дозволяє визначити, який саме сайт хоче відвідати клієнт. І, нарешті, слід налаштувати DNS так, щоб Web–браузери відвідувачів змогли відшукати Web–сервер.

Перший крок простий. Для кожного Web–сайту необхідно створити на жорсткому диску сервера свій каталог. Імена каталогів повинні відображати їх вміст (розмістити ці каталоги слід окремо від каталогу Inetpub і не на системному диску).

Доречно згадати і про систему безпеки. Щоб уникнути проблем при використанні анонімної автентифікації, необхідно встановити дозволи NTFS, які безпосередньо забороняють доступ IUSR в ті каталоги, куди звичайним відвідувачам сайту звертатися не можна.

Завершивши налаштування каталогів, слід повідомити сервер IIS про наявність двох сайтів. Необхідно запустити майстер «Web Site Creation Wizard», потім натиснути «Next» – з'явиться панель із запитом про найменування нового Web–сайту. Це ім'я відображається тільки в програмі адміністрування, тому воно може бути будь–яким. Ім’я необхідно набрати в полі «Description» і натиснути «Next» [7].

Наступним кроком необхідно задати, яким способом користувачі отримають доступ до сайту (по IP–адресі, номеру порту, заголовку). У списку «Enter the IP address to use for this Web site» знаходяться IP– адреси, призначені Web–серверу. Як правило, для Web–серверів використовується тільки одна IP – адреса, оскільки в системі є, ймовірно, лише один мережний адаптер, якому присвоєно тільки одну IP–адресу. Однак, тому ж самому мережному адаптеру можна призначити додаткові IP – адреси. В результаті адаптер стане відповідати на всі запити, що посилаються на будь–яку з призначених IP – адрес. Кількість IP–адрес, які можна призначити на мережний адаптер, обмежена і їх може не вистачити для кожного Web–сайту на сервері. Можна

підтримувати роботу декількох сайтів з однієї IP – адреси, але тоді потрібно налаштувати Web–сервер на використання різних портів TCP для кожного сайту. Поле «TCP port this web site should use» дозволяє змінити порт за замовчуванням для Web–сайту. Припустимо, потрібно запустити www.oranges.com, використовуючи стандартний порт 80, а www.apples.com, використовуючи порт 10000. Якщо адреса Web–сервера 1.1.1.1, то для цього створюються записи DNS, які вказують на IP–адресу 1.1.1.1, як для www.apples.com, так і для www.oranges.com. Однак для того, щоб відвідувачам підключитися до сайту www.apples.com, потрібно використовувати URL виду http://www.apples.com:10000.

Необхідність всякий раз при відвідуванні «нестандартного» сайту додавати суфікс з номером порту є досить незручною. Тому можна вибрати третій підхід: використовувати записи заголовків хоста (host header record). Поле «Host Header for this site» дає можливість Web–клієнтам – браузерам – повідомити Web–серверу, який саме сайт потрібен користувачу. За допомогою запису заголовка хоста можна розмістити на одному Web–сервері з 80–м портом будь–яку кількість Web–сайтів. Web–сервер може встановити, який сайт хоче відвідати клієнт, проаналізувавши запит Web–браузера. Замість того щоб просто запитати сторіночку default.htm, браузер просить показати default.htm з сайту www.oranges.com. Додаткова інформація, за допомогою якої ідентифікується конкретний сайт, називається записом заголовка хоста [7].

Види атак на WEB–сайти [7]

Підбір (Brute Force)

Підбір – автоматизований процес спроб і помилок, що використовується для того, щоб вгадати ім'я користувача, пароль, номер кредитної картки, ключ шифрування і т.д. Багато систем дозволяють використовувати слабкі паролі або ключі шифрування, і користувачі часто вибирають паролі, які легко вгадуються або містяться в словниках парольних фраз. Якщо пароль, що підбирається, дозволяє отримати доступ до системи, атака вважається

успішною і атакуючий може використовувати обліковий запис. Подібна техніка спроб і помилок може бути використана для підбору ключів шифрування. У разі використання ключів недостатньої довжини, зловмисник може отримати використовуваний ключ, протестувавши всі можливі комбінації.

Існує два види підбору: прямий і зворотний. При прямому підборі використовуються різні варіанти пароля для одного імені користувача. При зворотному перебираются різні імена користувачів, а пароль залишається незмінним. У системах з мільйонами облікових записів ймовірність використання різними користувачами одного пароля досить висока. Не дивлячись на популярність і високу ефективність, підбір може займати кілька годин, днів або років.

Виконання коду (Command Execution)

Передбачає розміщення власних, або модифікацію існуючих скриптів на сайті з метою доступу до конфіденційної інформації, або виводу сервера з ладу.

Переповнення буфера (Buffer Overflow)

Використання переповнення буфера дозволяє зловмисникові змінити порядок виконання програм шляхом перезапису даних у пам'яті системи. Переповнення буфера є найбільш поширеною причиною помилок в програмах. Коли буфер переповнюється, дані переписуються в інші області пам'яті, що призводить до виникнення помилок. Якщо зловмисник має можливість керувати процесом переповнення, це може викликати ряд серйозних проблем.

Переповнення буфера може викликати відмови в обслуговуванні, приводячи до пошкодження пам'яті і викликаючи помилки в роботі програмних засобів. Використовуючи переповнення буферу, можна перезаписувати службові області пам'яті, наприклад, адреси повернення функцій у стеці. Також, при переповненні можуть бути переписані значення

змінних в програмі. Переповнювання буфера є найбільш поширеною проблемою в безпеці і нерідко зачіпає Web–сервери.

Виконання команд ОС (OS Commanding)

Атаки цього класу спрямовані на виконання команд операційної системи на Web–сервері шляхом маніпуляції вхідними даними. Якщо інформація, отримана від клієнта, належним чином не верифікується, атакуючий отримує можливість виконати команди ОС. Вони будуть виконуватися з тим же рівнем привілеїв, з яким працює компонент додатку, що виконує запит (сервер СУБД, Web–сервер і т.д).

Зловживання функціональними можливостями (Abuse of Functionality)

Дані атаки спрямовані на використання функцій Web–додатків з метою обходу механізмів розмежування доступу. Деякі механізми Web–додатків, включаючи функції забезпечення безпеки, можуть бути використані для цих цілей. Рівень ризику і потенційні можливості зловмисника в разі проведення атаки дуже сильно залежать від конкретного додатка.

Зловживання функціональними можливостями дуже часто використовується спільно з іншими атаками, такими як зворотний шлях в директоріях і т.д. Наприклад, за наявності уразливості типу міжсайтового виконання сценаріїв в HTML–чаті, зловмисник може використовувати функції чату для розсилки URL, який використовує вразливість, всім поточним користувачам.

Відмова в обслуговуванні (Denial of Service or DoS)

Даний клас атак спрямований на порушення доступності Web–сервера. Зазвичай атаки, спрямовані на відмову в обслуговуванні реалізуються на мережному рівні, проте вони можуть бути спрямовані і на прикладний рівень. Використовуючи функції Web–додатку, зловмисник може вичерпати критичні ресурси системи, або скористатися уразливістю, що приводить до припинення функціонування системи.

Зазвичай DoS атаки спрямовані на вичерпання критичних системних ресурсів, таких як обчислювальні потужності, оперативна пам'ять, дисковий простір або пропускна спроможність каналів зв'язку. Якщо якийсь із ресурсів досягне максимального завантаження, додаток цілком буде недоступним.

Атаки можуть бути спрямовані на будь–який з компонентів Web–додатку, наприклад, такі як сервер СУБД, сервер автентифікації і т.д. У відмінності від атак на мережному рівні, що вимагають значних ресурсів зловмисника, атаки на прикладному рівні зазвичай легше реалізувати.

Контрольні запитання

1. Що розуміють під інтранет–мережею?
2. Що розуміють під екстранет–мережею?
3. Які системи необхідно налаштувати в корпоративній мережі, щоб її можна було віднести до інтранет–мережі?
4. Який протокол використовується для доступу до WEB–сайтів?
5. Який порт протоколу TCP відповідає цьому протоколу?
6. Що розуміють під віртуальним каталогом?
7. Де може бути розміщений каталог, визначений як віртуальний?
8. Для вирішення яких задач можуть бути використані віртуальні каталоги?
9. Чи доцільно, з точки зору безпеки, в одному каталозі тримати гіпертекст та скрипти? Чому?
10. Які права доступу користувачів необхідно поставити на каталог з гіпертекстом?
11. Які права доступу користувачів необхідно поставити на каталог зі скриптами?
12. Які схеми авторизації користувачів на сайті підтримує IIS?
13. Яка схема авторизації користувачів передає обліковий запис та пароль у нешифрованому вигляді?
14. Коли можна застосовувати схеми авторизації з інтегрованою автентифікацією (схемами шифрування) Windows?

15. Які існують основні типи атак на WEB–сайти?
16. Які механізми та засоби забезпечення інформаційної безпеки підтримуються IIS?
17. WEB–сервер має дві IP–адреси (10.12.80.253, 10.12.80.254) і на ньому необхідно розмістити два сайти: s1.fel.kpi.ua, s2.fel.kpi.ua. Наведіть тип записів, які необхідно зробити в ДНС для доступу до цих сайтів.
18. WEB–сервер має одну IP–адресу (10.12.80.254) і на ньому необхідно розмістити два сайти (s1.fel.kpi.ua, s2.fel.kpi.ua), для доступу до яких будуть використані порти 80 (s1.fel.kpi.ua) та 8000 (s2.fel.kpi.ua). Наведіть тип записів, які необхідно зробити в ДНС для доступу до цих сайтів та приклад URL, який користувач повинен ввести в браузері для доступу до кожного сайту.
19. Чи можливо на WEB–сервері, який має одну IP–адресу розмістити декілька сайтів, для доступу до яких буде використано тільки один порт (80)?
20. У разі позитивної відповіді на питання 19, вкажіть, що буде використано для направлення запиту користувача на необхідний сайт і який тип запису для кожного сайту необхідно зробити в ДНС.

2. КРИТЕРІЇ ОЦІНКИ ЛАБОРАТОРНИХ РОБІТ

Оцінка за кожну лабораторну роботу враховується у стартовому рейтингу студента.

Кількість балів r_k за кожну лабораторну роботу визначається у силабусі дисципліни.

Критерії оцінювання лабораторної роботи

Рівень засвоєння навчального матеріалу	Значення r_k	Опис критеріїв оцінювання
«відмінно»	(1,00 – 0,9) $\widehat{r_k}$	Виконані всі завдання лабораторної роботи, надані відповіді на усі запитання при захисті роботи.
«добре»	(0,89 – 0,75) $\widehat{r_k}$	Виконані всі завдання лабораторної роботи, надані відповіді на 75 % запитань при захисті роботи.
«задовільно»	(0,74 – 0,6) $\widehat{r_k}$	Виконані всі завдання лабораторної роботи, надані відповіді на 60 % запитань при захисті роботи.
«незадовільно»	0	Лабораторна робота не виконана, або надано відповіді менш ніж на 60 % запитань при захисті роботи – 0 балів.

Штрафні та заохочувальні бали:

- недопуск до лабораторних робіт у зв'язку з незадовільним вхідним контролем – 0,25 r_k ;
- недотримання терміну захисту лабораторної роботи – 0,25 r_k ;
- модернізації лабораторних робіт, виконання завдань із удосконалення дидактичних матеріалів з дисципліни – до 5 заохочувальних балів.

СПИСОК РЕКОМЕНДОВАНОЇ ЛІТЕРАТУРИ

1. Кучернюк П. В. Основи теорії телекомунікацій: текст лекцій з дисципліни «Основи теорії телекомунікацій і радіотехніки. Київ: КПІ ім. Ігоря Сікорського, 2020. 290 с. URL: https://ela.kpi.ua/bitstream/123456789/41495/1/Posibnyk_OTTR_2020.pdf (дата звернення: 21.04.2022).

2. Кучернюк П.В. Комп'ютерні мережі: навчальний посібник з дисципліни «Комп'ютерні мережі та засоби телекомунікацій» для студентів спеціальності 7.05090201, 8.05090201 «Радіоелектронні апарати та засоби». Київ: НТУУ «КПІ», 2015 р. 238 с. URL: https://ela.kpi.ua/handle/123456789/12042 (дата звернення: 21.04.2022).

3. Кучернюк П.В. Технології моніторингу та трафік–інжинірингу в телекомунікаційних мережах: підручник для студ. спеціальності 172 «Телекомунікації та радіотехніка». Київ : КПІ ім. Ігоря Сікорського, 2021. 257 с. URL: https://ela.kpi.ua/bitstream/123456789/41500/1/Pidruchkyk_TSU_2021.pdf (дата звернення: 21.04.2022).

ПЕРЕЛІК ПОСИЛАНЬ

1. Технічна документація Microsoft. URL: https://docs.microsoft.com/uk–ua/ (дата звернення: 21.04.2022).
2. Net Commands On Operating Systems. URL: https://docs.microsoft.com/en–us/troubleshoot/windows–server/networking/net–commands–on–operating–systems (дата звернення: 21.04.2022).
3. Windows Performance Monitor. URL: https://docs.microsoft.com/en–us/previous–versions/windows/it–pro/windows–server–2008–R2–and–2008/cc749249(v=ws.11) (дата звернення: 21.04.2022).
4. Active Directory Domain Services. URL: https://docs.microsoft.com/en–us/windows–server/identity/ad–ds/active–directory–domain–services (дата звернення: 21.04.2022).
5. Кучернюк П. В. Основи теорії телекомунікацій: текст лекцій з дисципліни «Основи теорії телекомунікацій і радіотехніки. Київ: КПІ ім. Ігоря Сікорського, 2020. 290 с. URL: https://ela.kpi.ua/bitstream/123456789/41495/1/Posibnyk_OTTR_2020.pdf (дата звернення: 21.04.2022).
6. Networking documentation. URL: https://docs.microsoft.com/en–us/windows–server/networking/ (дата звернення: 21.04.2022).
7. Internet Information Services (IIS) 6.0 SDK. URL: https://docs.microsoft.com/en–us/previous–versions/iis/6.0–sdk/ms525568(v=vs.90) (дата звернення: 21.04.2022).