Юрій Рамський,
Василь Олексюк,
Анатолій Балик

АДМІНІСТРУВАННЯ КОМП'ЮТЕРНИХ МЕРЕЖ І СИСТЕМ

Навчальний посібник

Рекомендовано Міністерством освіти і науки України

ТЕРНОПІЛЬ
НАВЧАЛЬНА КНИГА – БОГДАН

ББК 32.973.26-018.2
УДК 004.7
Р21

Рецензенти: *М.І. Жалдак* — академік АПН України, доктор педагогічних наук, професор, директор інституту інформатики Національного педагогічного університету імені М.П. Драгоманова
М.П. Малежик — доктор фізико-математичних наук, професор кафедри комп'ютерної інженерії інституту інформатики Національного педагогічного університету імені М.П. Драгоманова
В.І. Клочко — доктор педагогічних наук, професор кафедри вищої математики Вінницького національного технічного університету

Рекомендовано Міністерством освіти і науки України
(лист Міністерства освіти і науки України №1/11–4922 від 10.06.2010 р.)

Рамський Ю.С., Олексюк В.П., Балик А.В.

Р21 Адміністрування комп'ютерних мереж і систем: Навч. пос. — Тернопіль: Навчальна книга – Богдан, 2010.— 196 с.

ISBN 978-966-10-1561-5

У пропонованому посібнику розглянуто адміністрування як однорангових комп'ютерних мереж, так і мереж з виділеними серверами. Подано теоретичні відомості про основні сервіси локальних мереж та Інтернету. Описано конфігурування веб-сервера, поштового сервера, сервера передавання файлів на основі ОС Windows і ОС Linux.

Для студентів вищих навчальних закладів, учителів інформатики та широкого кола читачів.

ББК 32.973.26-018.2

ISBN 978-966-10-1561-5

Передмова

Сучасний етап розвитку інформаційного суспільства називають мережним, враховуючи поширення і роль комп'ютерних і мережних технологій. Вміння використовувати мережні технології необхідні кожному для здійснення професійної діяльності, навчання, організації дозвілля.

Формуванню згаданого вміння варто приділити належну увагу як у загальноосвітній школі, так і у вищих навчальних закладах. Вивчення мережних технологій передбачає оволодіння принципами мережного зв'язку, формування умінь щодо організації та управління (адміністрування) мережними структурами. Вищим рівнем застосування мережних технологій є вміння розробляти мережне програмне забезпечення.

Одним із завдань вивчення курсу є формування теоретичних знань щодо управління мережними системами в їх філософсько-логічному розумінні. Для цього передбачено вивчення основ адміністрування на базі двох операційних систем (ОС) (MicrosoftWindowsServer2003 і Linux).

Основні завдання щодо управління роботою мереж проаналізовані на прикладі однорангових мереж та мережних доменних структур. Завданням адміністрування однорангових мереж є організація роботи з кожним комп'ютером зокрема. Елементи централізованої моделі управління мережами застосовуються у процесі конфігурування доменних структур. Сервіси прикладного рівня розглядаються у межах одного модуля.

Лабораторні роботи з даного курсу доцільно виконувати так, щоб ті з них, які стосуються використання однієї й тієї самої технології в різних операційних системах, проводилися послідовно.

Зміст

1. Поняття про системне адміністрування

2. Адміністрування серверaоднорангової мережі з використанням MicrosoftWINDOWSSERVER2003

3. Адміністрування сервера однорангової мережі з використанням ОС Linux

4. Адміністрування домену Active directory

5. Організація доменів засобами мережиш інформаційної служби NIS

6. Організація домена засобами сервера Samba

7. Конфігурування клієнт-серверного програмного забезпечення

1. Поняття про системне адміністрування

У багатокористувацькій операційній системі (ОС) повинен бути зареєстрований принаймі один користувач, який виконує роль системного адміністратора. Він відповідає за функціонування системи, володіє навичками, потрібними для усунення помилок і збоїв, забезпечує користувачів необхідними програмними засобами.

Сучасні мережі будують на основі технології «клієнт-сервер». Серверні ОС вимагають початкового конфігурування й постійної уваги адміністратора для забезпечення коректного, безперебійного й ефективного функціонування системи та роботи користувачів. Системний адміністратор відповідає за виконання всіх вимог ОС і вирішує завдання, пов'язані з роботою системи.

Системний адміністратор — фахівець, відповідальний за проектування, встановлення, конфігурування, управління й обслуговування мереж і систем. Він повинен мати відповідні знання й уміння стосовно встановлення й налаштування системи для забезпечення її функціонування для багатьох користувачів. Таке конфігурування вимагає коректного виконання завдань з різними пріоритетами.

Кожна ОС має не менше одного облікового запису користувача, який виконує операції управління системою (його ще називають суперкористувачем (superuser)і має спеціальне реєстраційне ім'я — root, administrator).

У більших системах обов'язки системного адміністратора виконує, як правило, група людей; у малих — системний адміністратор — одна особа. Інколи, системного адміністратора серед працівників організації немає. Проте це не означає, що управління роботою систем і мереж не здійснюється взагалі. Зазначені компанії можуть запрошувати адміністраторів для виконання окремих завдань та моніторингу систем через віддалений доступ (такі послуги називають аутсорсингом (outsoursing)).

Для виконання завдань управління ОС системний адміністратор використовує відповідний обліковий запис (rootабо administrator). Для звичайної роботи адміністратор повинен використовувати звичайний обліковий запис. Кількість користувачів, що входять у систему з повноваженнями адміністратора, потрібно обмежити — не більше двох-трьох чоловік. У випадку реєстрації в ОС з використанням облікового запису адміністратора, користувач одержує над системою практично необмежений контроль, наприклад, може змінити атрибути будь-якого файла, припинити роботу системи, перезавантажити її або виконати інші операції, недоступні звичайному користувачеві системи.

Адміністратор повинен бути експертом з питань функціонування систем і мереж. Він повинен уміти знаходити компроміс між вимогами користувачів та можливостями їх реалізації у системі. Системний адміністратор розробляє правила роботи в корпоративній мережі та пояснює їх користувачам. Такі правила повинні базуватися на трьох основних положеннях:

- ✓ максимальний доступ користувачів до власних ресурсів;
- ✓ максимальне обмеження доступу до ресурсів інших користувачів;
- ✓ відповідальність користувачів за збереження власних ресурсів.

Перше положення передбачає створення розподілених ресурсів для кожного користувача мережі та надання йому повного доступу до них. Розподілені системи можуть бути побудованими на основі однорангових мереж або на основі мереж з виділеним сервером.Сервером є комп’ютер мережі, який надає свої ресурси (інформаційні, обчислювальні) іншим комп’ютерам, які називають клієнтами (робочими станціями). Бажано, щоб віддалений доступ до ресурсів мережі був організований різними засобами (VPN-сервер, FTP-сервер, RAS-сервер, сервер терміналів тощо).

У другому положенні зазначено, що користувачі повинні мати доступ лише до власних ресурсів й не мати доступу до ресурсів інших користувачів

або хоча б не мати доступу для внесення змін. Звичайно в деяких випадках, потрібно мати доступ до ресурсів інших користувачів. У такому разі потрібно додати «чужі» облікові записи до облікового запису групи (підрозділу) та надати відповідні дозволи для неї.

Третє положення передбачає формування у працівників розуміння, ідо за цілісність власних даних першочергово несе відповідальність користувач-власник. Користувачі корпоративної мережі повинні зберігати в таємниці власні реєстраційні дані. Кожен працівник персонально несе відповідальність за конфіденційність зберігання і паролів. Із метою підвищення безпеки збереження даних, особливо від атак добору паролів, користувачам доцільно час від часу змінювати власні паролі.

Наведемо типові завдання, які доводиться виконувати системним адміністраторам.

- ✓ Встановлення та конфігурування апаратного забезпечення.
- ✓ Встановлення та конфігурування мережних ОС.
- ✓ Керування обліковими записами користувачів. Додавання, видалення облікових записів користувачів і визначення їх привілеїв.
- ✓ Налаштування пристроїв, розподілених і локальних ресурсів.
- ✓ Створення резервних копій. Визначення правил створення резервних копій для зниження втрат і відновлення даних після можливих збоїв у роботі системи.
- ✓ Вимикання системи. Коректне вимикання системи дає змогу уникнути втрат даних і збоїв файлової системи.
- ✓ Навчання користувачів. Навчання користувачів особливостей роботи у системі для підвищення ефективності їхньої праці.
- ✓ Надання допомоги користувачам. Адміністратор виступає в ролі експерта, який допомагає користувачам вирішувати їхні проблеми, пов’язані з експлуатацією системи.
- ✓ Забезпечення безпеки системи. Системний адміністратор організовує взаємодію користувачів на основі їх привілеїв.

- ✓ Ведення системного журналу та реєстрація змін у системі. Переважна більшість сучасних мережних ОС дає змогу відслідковувати зміни у системі. Для цього використовують системні журнали різноманітних форматів (як текстових, так і кодованих).
- ✓ Документування власної діяльності щодо адміністрування мережі.

Контрольні запитання

1. Кого називають системним адміністратором?
2. Які завдання вирішує системний адміністратор?
3. Що називають сервером?
4. На основі яких ОС можна побудувати сервер?
5. Що називають системним журналом і яке його призначення?
6. Запропонуйте структуру журналу для документування діяльності системного адміністратора.

2. Адміністрування сервераоднорангової мережі з використанням MicrosoftWINDOWSSERVER2003

2.1. Загальна характеристика ОС WindowsServer2003

Досить поширеними є такі версії (редакції) ОСWindowsServer2003:

- ✓ Windows Server 2003 Standard Edition;
- ✓ Windows Server 2003 Web Edition;
- ✓ Windows Server 2003 Enterprise Edition;
- ✓ Windows Server 2003 Datacenter Edition.

Найбільш універсальною серед них є версія WindowsServer2003 EnterpriseEdition, яка маєтакі основні служби (сервіси):

- ✓ сервери розподілених ресурсів (файлів і принтерів);
- ✓ веб-сервер, FTP-серверу складі Internet Information Service (IIS);
- ✓ поштові служби (SMTP, POP);
- ✓ служба терміналів;
- ✓ служби маршрутизації та віддаленого доступу;
- ✓ контролер домену;
- ✓ сервер доменних імен (DNS-сервер);
- ✓ служба призначення мережних адрес (DHCP-сервер);
- ✓ мультимедіа-сервер.

WindowsServer2003 EnterpriseEditionможе забезпечити підтримку до восьми процесорів, роботу з оперативною пам’яттю обсягом до 32 Гб, кластеризацію на основі мереж зберігання даних, сумісну роботу з 64 розрядними процесорами.

Рекомендованими вимогами до апаратного забезпечення з боку ОС WindowsServer2003 EnterpriseEditionє:

- ✓ процесор із частотою від 500 МГц;
- ✓ 256 Мб оперативної пам’яті;
- ✓ 3 Гб на жорсткому диску.

Зазначимо, що практично всі відомості, наведені у цьому розділі, щодо адміністрування окремого сервера WindowsServer2003, стосуються й адміністрування ОС WindowsXP.

Контрольні запитання

1. Які версії ОС WindowsServer2003 Вам відомі?
2. Наведіть приклади, коли потрібно встановлювати ОС WindowsServer, а коли можна скористатися ОС WindowsXP, Windows7?

2.2 Консоль ММС як засіб адміністрування ОС WindowsServer2003

КонсольММС*(MicrosoftManagementConsole)*є засобом, що може містити один або кілька додатків, так званих оснащень (snapin), які застосовують для конфігурування складових ОС. ММС безпосередньо не виконує адміністративних завдань, проте в ній можна розмістити інструменти (оснащення), які дадуть можливість виконати ці завдання.

Завантаження консолі найпростіше здійснити за допомогою команди *mmc,* яку потрібно увести в пункті *Виконати (Run)*головного меню. Вікно консолі має два фрейми (підвікна): лівий, в якому розміщується оснащення, і правий, який містить зміни вибраного оснащення (рис. 2.1).

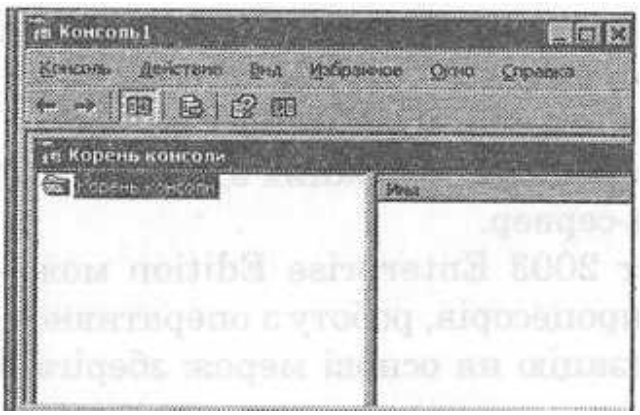


Рис. 2.1. Консоль ММС без оснащень

Існує два режими використання консолі ММС: користувальний та авторський. У першому режимі користувач використовує готові консолі ММС, а в другому — створює власні консолі, використовуючи оснащення. Прикладом користувального режиму є відома консоль *Управління комп'ютером (ComputerManagement).*

Для створення консолей в авторському режимі потрібно до порожньої

консолі додавати потрібні оснащення *(Консоль—Додати або видалити оснащення (Консоль — AddorremoveSnapIn)).*Зауважимо, що практично всі оснащення дають змогу виконувати задачі адміністрування як на локальному комп'ютері, так і на віддаленому. Наприклад, при додаванні оснащення «Локальні користувачі та групи», адміністратор може вибрати облікові записи комп'ютера, якого посуватиметься це оснащення (рис. 2.2).

Після внесення змін у консоль її можна зберегти як файл.

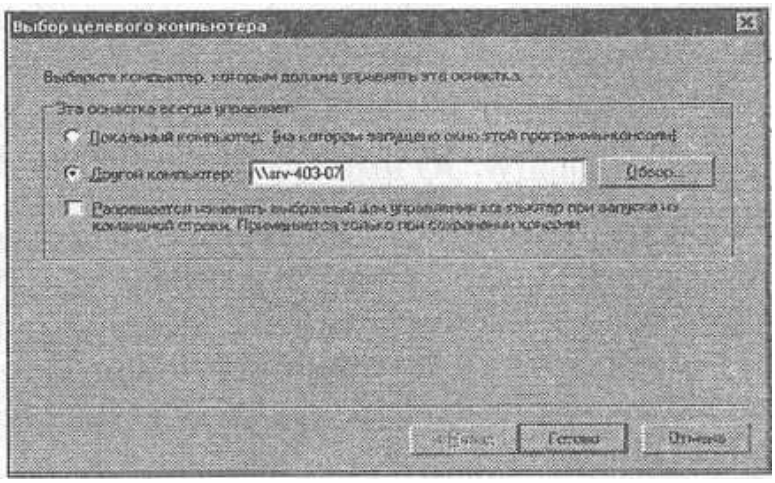


Рис. 2.2. Режим адміністрування віддаленого комп'ютера в консолі MMC

Контрольні запитання

1. Що називають оснащенням?
2. Які режими роботи з консоллю MMC Вам відомі?
3. Які стандартні консолі MMC Ви зустрічали на практиці?
4. Чи всі оснащення дають змогу адмініструвати віддалену ОС?
5. Для чого, на Вашу думку, розроблено консоль MMC, чи не досить панелі управління?

2.3.Управління обліковими записами користувачів і груп користувачів

Для управління роботою користувачів в ОС WindowsServer2003 реалізовано механізм облікових записів і груп. Перші дозволяють входити в мережу й отримувати доступ до мережних ресурсів окремим користувачам.

Другі застосовують для управління ресурсами кількох користувачів групи. Правила роботи для окремих користувачів і груп визначають дії, які можуть виконувати відповідні користувачі, а також комп'ютерні системи і ресурси, до яких у них е доступ.

Процес підтвердження відповідності ідентифікаційних даних, уведених користувачем, його обліковому запису, який зареєстрований в ОС, називають автентифікацією. Зазвичай у процесі автентифікації користувач надає системі відомості, які ідентифікують його — ім'я власного облікового запису (л о г і н) і певне кодове слово (пароль). Крім логіна і пароля автентифікація може здійснюватися за допомогою сертифікатів, голосу, відбитків пальців особи тощо.

Автентифікація в WindowsServer2003 здійснюється в два етапи: інтерактивний вхід у систему і мережна автентифікація.

WindowsServer2003 підтримує кілька протоколів автентифікації.

- ✓ NTLANManager (NTLM) — основний протокол в ОС WindowsNT, використовується для автентифікації в домені WindowsNT.
- ✓ Kerberos— стандартний Інтернет—протокол автентифікації користувачів і систем (основний механізм автентифікації в доменах ActiveDirectory).
- ✓ SSL/TLS (SecureSocketLayer/TransportLayerSecurity) — основний механізм автентифікації на захищених Web-серверах;
- ✓ .NETPassportAuthentication— механізм автентифікації в Інтернет-сервісах Microsoft (InternetInformationServices (IIS)), що дає змогу використовувати відомості домену ActiveDirectoryудля автентифікації користувачів з мережі Інтернет, внутрішніх і зовнішніх мереж.

Робота з ОС або мережею вимагає не лише здійснення автентифікаці'ї користувачів, а й надання їм доступу до певних ресурсів. Такий процес називають авторизацією.

У WindowsServer2003 визначені облікові записи двох типів.

- ✓ Локальні облікові записи—де зареєстровані записи в базі даних

локального комп'ютера (ОС). Після автентифікації користувач отримує доступ тільки до ресурсів цього комп'ютера. Для доступу до інших мережних ресурсів користувач повинен знову проходити процедуру автентифікації.

- ✓ Доменні облікові записи — зареєстровані записи в базі даних домену (у WindowsServer2003 — це ActiveDirectory). Після одноразової автентифікації користувачі з такими обліковими записами можуть звертатися до ресурсів усього домену.

Як уже зазначалося, у WindowsServer2003 є можливість використовувати облікові записи не тільки окремих користувачів, а й облікові записи груп, що дозволяє автоматично надавати права доступу до ресурсів подібним типам користувачів і спростити адміністрування Опікових записів. Кожний користувач — член групи (обліковий зате якого включено у відповідну групу) може звертатися до ресурсів, право доступу до яких надано групі.

Основними локальними групами ОС WindowsServer2003 є:

- ✓ адміністратори, що мають необмежені повноваження для управління ОС;
- ✓ досвідчені користувачі, що мають більшість повноважень адміністраторів;
- ✓ користувачі, які не мають повноважень для зміни параметрів ОС;
- ✓ гості, які мають повноваження, аналогічні до групи «користувачі», проте часто не мають повноважень для зберігання власних профілів;
- ✓ користувачі віддаленого робочого столу—група для віддаленого входу в ОС за допомогою служби терміналів;
- ✓ debuggerusers— користувачі, які можуть впливати на процеси ОС;
- ✓ оператори архіву, які мають повноваження для резервного копіювання та відновлення файлів ОС.

Локальні облікові записи користувачів створюють в оснащенні *Локальні користувачі і групи (LocalUsersandGroups)*(рис. 2.3).

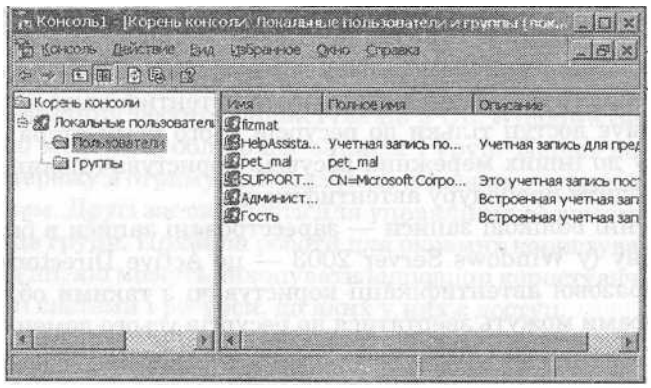


Рис. 2.3. Консоль для роботи з обліковими записами користувачів і груп

Для створення облікового запису користувача потрібно з меню виконати команду *Дія — Новий користувач (Action— NewUser).* Параметрами створюваного запису є (рис. 2.4):

- ✓ логін (ім’я облікового запису користувача);
- ✓ повне ім’я користувача (можна вводити прізвище, ім’я та по батькові);
- ✓ опис облікового запису;
- ✓ пароль;
- ✓ вимога зміни пароля користувачем при наступному вході;
- ✓ заборона зміни пароля користувачем;
- ✓ необмежений термін дії пароля;
- ✓ відключення облікового запису.

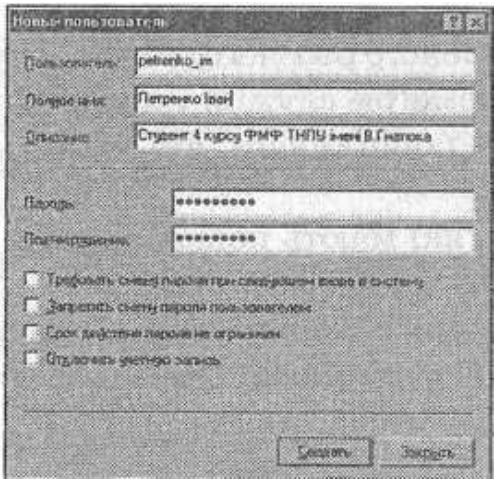


Рис. 2.4. Вікно створення нового облікового запису користувача

За допомогою контекстного меню облікового запису користувача адміністратор може змінити його пароль. Вікно властивостей облікового

запису дає змогу додати або видалити його з певної групи.

Контрольні запитання

1. Який зміст понять: користувач, обліковий запис користувача, обліковий запис групи користувачів?
2. Який зміст понять: автентифікація, авторизація?
3. Які протоколи автентифікації Вам відомі?
4. Перелічіть стандартні облікові записи груп користувачів ОС WindowsServer2003.
5. Як створити обліковий запис користувача?
6. Для чого потрібні облікові записи груп користувачів?

2.4. Правила доступу до об'єктів файлової системи MTFS

Файлова система NTFSзабезпечує управління доступом до файлів і папок. Правила доступу зберігаються як записи управління поступом таблиці ACL (ACL— AccessControlList), що е частиною дескриптора безпеки кожного ресурсу. Кожен запис містить так звані ідентифікатори захисту (SID— SecurityIdentifier) облікового запису користувача або групи, яким дозволено або заборонено певний вид поступу. Причому правила, які забороняють доступ, мають пріоритет і під правилами, що його надають. При звертанні до ресурсу кожен ідентифікатор захисту порівнюється з ідентифікаторами SIDy записах і таблиці ACL.

Провідник Windowsє стандартним засобом управління дозволами доступу до ресурсів як на локальному диску, так і на віддаленому сервері Для зміни правил доступу засобами файлової системи NTFSпотрібно в контекстному меню папки або файла вибрати пункт *Властивості* (*Properties)* та перейти на вкладку *Безпека (Security)*(рис. 2.5).

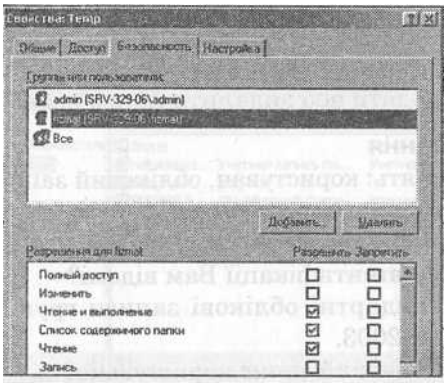


Рис. 2.5. Вікно для налаштування правил доступу до файлової системи NTFS

Кілька правил групують у шаблони. Вікно, зображене на рисунку 2.5, містить загальну картину правил безпеки для папки або файла. Використовуючи його, можна переглянути або замінити шаблони правил доступу для вибраного облікового запису. Кожний шаблон у цьому вікні містить сукупність правил, які разом забезпечують певний типовий рівень доступу. Наприклад, щоб користувач міг зчитати файл, потрібно надати кілька дозволів низького рівня. Для того, щоб приховати цю складність, можна застосувати шаблон *Читання й виконання (Read&Execute),*а ОС сама встановить потрібні дозволи доступу до файла або папки.

Найбільш поширеними є такі шаблони:

- ✓ *Читання й виконання (Read&Execute).*Призначення цього шаблону дозволів дає можливість користувачам відкривати й читати файли і папки. Він також дозволяє користувачеві скопіювати об’єкт, якщо той має дозвіл на запис для цільової папки або носія.
- ✓ *Запис (Write)*і *Зміна (Modify).*Шаблон *Запис (Write)*дозволяє створювати файли й папки (коли він стосується папки) і змінювати вміст й атрибути файлів. Шаблон *Зміна (Modify)*також дозволяє видалити об’єкт.
- ✓ *Зміна дозволів (ChangePermissions).*За замовчуванням змінювати правила доступу може тільки власник папки. Крім нього, це може зробити й будь-який користувач з діючим дозволом *Зміна дозволів (ChangePermissions),*що задають за допомогою розширеного режиму

зміни таблиці ACL. Цей дозвіл також входить у шаблон *Повний доступ (FullControl).*

Для детального ознайомлення з правилами доступу до файлової системи NTFSварто перейти в розширений режим (за допомогою кнопки *Додатково (Advanced)).*Як результат отримаємо друге вікно редактора ACL, в якому перелічені конкретні записи управління доступом, призначені для даного файла або папки. Відомості в цьому переліку максимально наближені до даних таблиці ACL. Друге допоміжне вікно дає змогу також налаштовувати аудит, змінювати власника файла чи папки, а також визначати діючі дозволи (рис. 2.6).

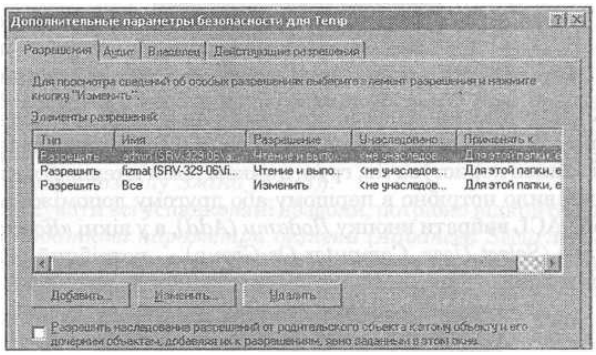


Рис. 2.6. Вікно додаткових параметрів доступу до файлової системи NTFS

Якщо вибрати запис списку *Елемент дозволів (PermissionEntries)* і послугу *Змінити (Edit),*то відкриється третє допоміжне вікно редактора ACL. У вікні *Елемент дозволів* для ресурсу *(PermissionEntryForDocs)*виводиться перелік можливих дозволів/заборон, які можуть бути надані певному користувачу (рис. 2.7).

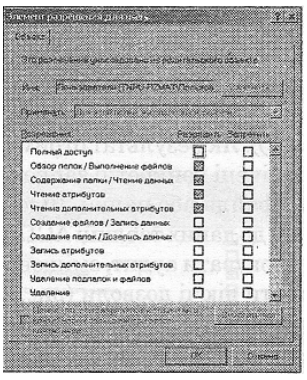


Рис. 2.7. Вікно для внесення змін правил безпеки

Будь-якому учасникові безпеки можна надати або заборонити доступ до певного ресурсу. У WindowsServer2003 учасниками безпеки е облікові записи користувачів, груп, а також комп'ютерів. Для того щоб додати правило потрібно в першому або другому допоміжному вікні редактора ACLвибрати кнопку *Додати (Add),*а у вікні*«Користувачі або Групи» (SelectUser, ComputerOrGroup)* — потрібний обліковий запис (рис. 2.8).

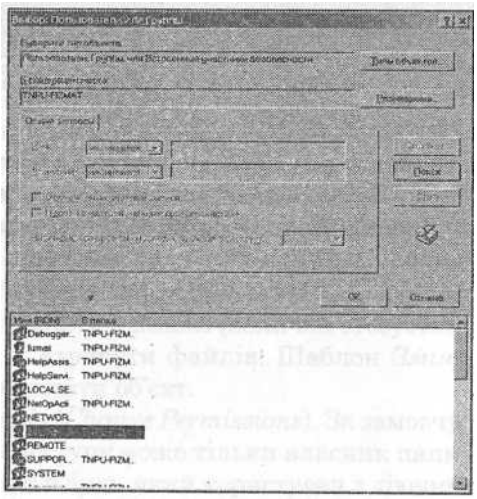


Рис. 2.8. Вікно вибору користувачів для встановлення правила доступу

Windows Server 2003 підтримує успадкування дозволів — за замовчуванням правила на доступ до папки поширюються на всі її файли та підпапки. Будь-які зміни батьківської таблиці ACL будуть відображені й на всьому вмісті папки.

Успадковані дозволи відображаються у вигляді «сірих» прапорців, що дає змогу відрізнити їх від явних дозволів. Друге допоміжне вікно — *Додаткові параметри безпеки (Advanced Security Settings)*— містить папки, з яких успадковується кожний елемент дозволу.

Проте іноді потрібно змінити дозволи підпапки або файла, щоб розширити або обмежити доступ користувача або групи. Успадковані дозволи не можна видалити з ACL. їх можна перекрити (замінити), призначивши явні дозволи. Можна також скасувати успадкування й створити записи в таблиці ACL, які міститимуть тільки явні правила.

Наприклад, якщо папка успадковує дозвіл на читання і зміну, наданий

групі st5, а необхідно, щоб певний користувач, що належить до цієї групи, не мав змоги записувати в папку, потрібно створити для його облікового запису відповідне правило (прапорець *Заборонити (Deny)*напроти дозволу *Зміни (Read)).*

Щоб скасувати всі успадковані дозволи, потрібно відкрити допоміжне вікно *Додаткові параметри безпеки (Advanced Security Settings)* ресурсу й зняти прапорець, що дозволяє успадкування дозволів від батьківського об'єкта *(Allow Inheritable Permissions From The Parent To Propagate To This Object...)*(рис. 2.9).

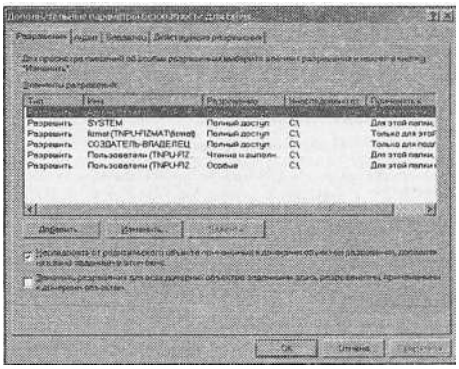


Рис. 2.9. Видалення успадкування правил

Видаляючи успадкування правил, адміністратор може обрати один з варіантів (рис. 2.10):

- ✓ видалити успадкування, зберігши діючі правила як явні (будуть створені явні дозволи, ідентичні до успадкованих);
- ✓ видалити успадкування і правила;
- ✓ відмовитися від видалення успадкувань

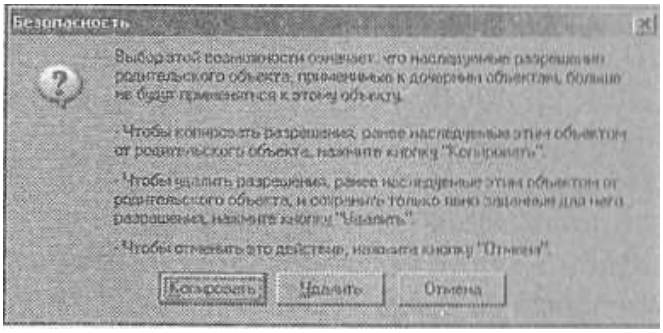


Рис. 2.10. Дії при видаленні успадкування правил

Успадкування можна відновити двома способами; з дочірнього ресурсу або з батьківської папки.

Windows Server 2003 підтримує спеціального учасника безпеки — користувача, який створив об’єкт файлової системи, власника *('CreatorOwner).*У дескрипторі безпеки ресурсу с лапне, шані визначає власника об’єкта.

Якщо користувач створює файл або папку, то пін< гас власником цього ресурсу. Якщо з деяких причин змінюються правила таблиці ACLстосовно власника так, що для нього діють правила заборони, то власник може змінити правила таблиці ACI, п тримати потрібний рівень доступу.

Для того щоб стати власником ресурсу, потрібно перейти на вкладку *Власник (Owner)*у вікні додаткових параметрів доступу до файлової системи NTFS(рис. 2.11).

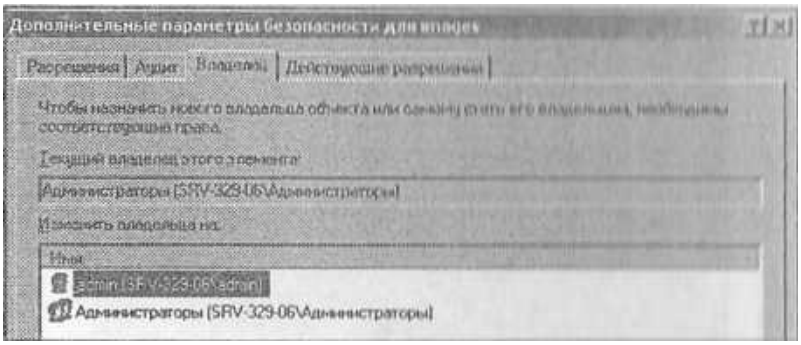


Рис. 2.11. Зміна власника об’єкта файлової системи

Змінюючи власника, варто враховувати таке:

- ✓ власниками файлів і папок можуть бути користувачі з групи *Адміністратори (Administrators).*Адміністратори можуть передавати права на володіння;
- ✓ права на володіння можуть набувати користувачі з дозволом *Зміна власника (Таке Ownership).*Такий дозвіл може бути надано користувачеві або групі, що дозволить їм володіти ресурсом, а отже, і змінити правила таблиці ACL та одержати достатні потрібні дозволи.

Зазвичай облікові записи користувачів належать до кількох груп з різними рівнями доступу до ресурсів. У цьому випадку говорять про діючі правила (effective permissions). Такі правила можна переглянути на

вкладці *Діючі дозволи (Effective permissions)*у вікні додаткових параметрів доступу до файлової системи NTFS.

Перелічимо основні принципи, за якими визначають діючі дозволи:

- ✓ правила, які стосуються файлів, мають пріоритет над правилами доступу до каталогів;
- ✓ дозволи, які задають рівень доступу, додаються;
- ✓ правила, що забороняють доступ, мають пріоритет над правилами, які надають його.

Контрольні запитання

1. Де зберігаються правила доступу до файлової системи NTFS?
2. Як переглянути правила безпеки диска, папки, файла?
3. Які протоколи автентифікації Вам відомі?
4. Які Вам відомі шаблони правил доступу до файлової системи NTFS?
5. Які дії можна виконувати із файловою системою при встановленні шаблонів правил *Запис, Зміна, Повний доступі*
6. Що таке успадкування правил доступу до файлової системи, для чого воно потрібне?
7. Як можна встановити успадкування правил та як видалити його?
8. Кого називають власником об’єкта файлової системи?
9. Хто може бути власником об’єктів файлової системи NTFS?

2.4. Створення розподілених мережних ресурсів засобами ОС Windows Server 2003

Розподіленим мережним ресурсом є папка, до якої організовано доступ через мережу і яка має унікальне мережне ім’я. Створення загального доступу до папки вказує *Службі доступу* до *файлів і принтерів Microsoft (File And Printer Sharing For Microsoft Networks)*на можливість підключення до цієї папки та її підпайок клієнтам, на комп’ютерах яких виконується служба *Клієнт для мереж Microsoft (Client For Microsoft Networks).*

Розподілені ресурси можна створювати з контекстного меню папки або за допомогою консолі MMC. Відкривши оснащення *Загальні папки (Shared Folders)*у консолі MMC або в консолі *Керування комп'ютером (Computer Management),*спостерігаємо, що у Windows Server 2003 вже налаштовано декілька стандартних адміністративних загальних ресурсів: системний каталог (зазвичай C:\Windows) і корінь кожного жорсткого диска. Ім'я ресурсу для таких загальних папок закінчується знаком долара ($) (рис. 2.12). Знак «долар» наприкінці мережного імені позначає приховані загальні папки системного призначення. їх не можна побачити у програмі переглядачі (провіднику), але до них можна звернутися, вказавши їх ім'я на зразок:

\\ім'я_сервера\ім'я_загального_ресурсу$

До адміністративних загальних ресурсів (наприклад, логічних дисків c$, d$ тощо) можна звернутися тільки з використанням облікового запису адміністратора.

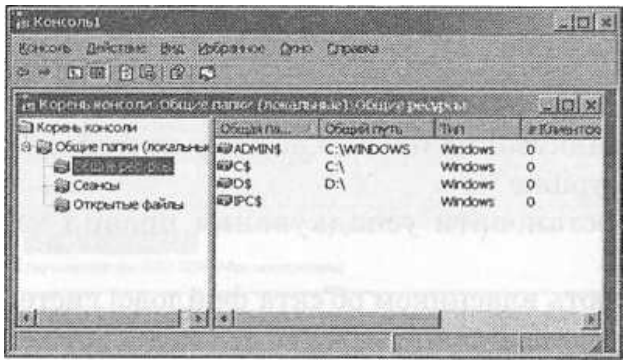


Рис. 2.12. Системні мережні ресурси в консолі MMC

Для відкриття загального доступу до папки потрібно додати оснащення *Загальні папки* до консолі MMC. У контекстному меню пункту*Загальні папки* або в меню *Дія (Action)*необхідно вибрати *Новий загальний ресурс (New Share).*Майстер створення загальних ресурсів містить такі сторінки:

- ✓ *Шлях до папки (Folder Path)*— вказує шлях до загальної папки на локальному диску;
- ✓ *Ім'я, опис і параметри (Name, Description and Settings)* — задає ім'я загального ресурсу. Ім'я ресурсу разом з іменем сервера утворюють мережний шлях до спільної папки — *\\ім'я_сервера*

ім'я_загальногоjресурсу;

- ✓ *Дозволи (Permissions)*— дає змогу вибрати користувачів, які матимуть доступ до ресурсу, та задати правила доступу (читання, запис). Правила доступу до мережних ресурсів не такі детальні, як дозволи файлової системи NTFS, проте вони дають змогу налаштувати основні типи доступу до спільної папки (таблиця 2.1).

Таблиця 2.1.*Правила доступу до розподілених ресурсів*

Правило	Опис
Читання (Read)	Користувачі можуть переглядати назви папок, а також імена, вміст та атрибути файлів, запускати програми й звертатися до інших підпапок у середині папки із загальним доступом.
Зміна (Change)	Користувачі можуть створювати папки, додавати файли й редагувати їхній вміст, змінювати атрибути файлів, видаляти файли і папки та виконувати дії, визначені дозволом *Читання (Read).*
Повний доступ(Full Control)	Користувачі можуть змінювати локальні правила доступу, отримувати права власності на файли і виконувати всі дії, допустимі дозволом *Зміна (Change).*

Іншим способом створення спільних ресурсів є використання вікна властивостей папки. Після виклику цього вікна потрібно перейти на вкладку *Доступ (Sharring),*у якій можна вказати (рис 2.13):

- ✓ максимальну кількість одночасних з'єднань користувачів. Важливим аспектом використання ОС WindowsProfessionalє те, що вона не підтримує більше ніж 10 одночасних з'єднань. На операційну систему WindowsServer2003 зазначені обмеження не поширюються;
- ✓ правила доступу для окремих користувачів.

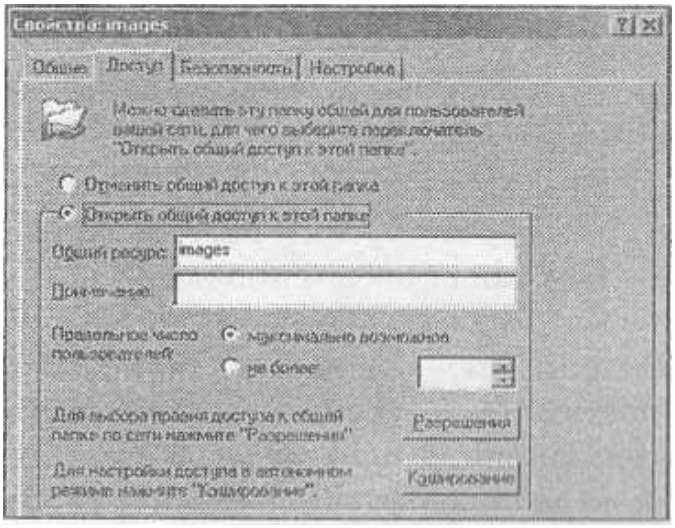


Рис. 2.13. Налаштування параметрів доступу до спільної папки

Параметри доступу до спільного ресурсу визначають максимальні діючі дозволи для всіх файлів і папок усередині нагальної папки. Призначаючи дозволи на рівні файлової системиNTFSдля окремих файлів і папок, на рівні роботи через мережу, доступ можна посилити, але не розширити. Інакше кажучи, доступ користувача до файла або папки визначається найбільш жорстким набором до. і поліп загального ресурсу й правил таблиці ACL. Це одна з причин, з якої, зазвичай, групі *Всі (Everyone)*надається дозвіл*Повнийдоступ, (FullControl),*для захисту папок і файлів використовують тільки дозволифайлової системи NTFS.

Після створення ресурсу піктограма папки набуде вигляду «папки з рукою». Для доступу до створеного ресурсу можна скористатись різними способами.

1. За допомогою об’єкта *Мережне оточення (Mynetworkplaces)*перейти до потрібного комп’ютера (рис. 2.14). Проте можливі випадки, коливикористання цього способу не дає потрібних результатів, оскільки вробочій групі відображаються не всі комп'ютери.

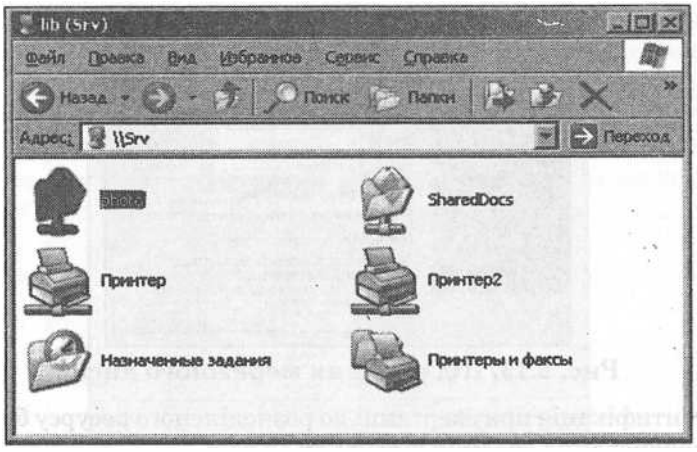


Рис. 2.14. Мережні ресурси

2. Використовуючи пункт *Виконати (Run)*головного меню, в рядку потрібно ввести: *srv**share*,де srv— ім'я комп'ютера, share— назва розподіленого ресурсу. Доволі часто трапляється ситуація, коли виконання такої команди призводить до виведення вікна з повідомленням *Не знайдено мережний шлях (Networkpathnotfound).*Причиною зазначеної ситуації може бути невстановлення відповідності між іменем комп'ютера та його IP-адресою. У цьому разі потрібно в команді *srv**share*замість імені комп'ютера ввести його IP-адресу, наприклад, \\192.168.0.3\share.
3. Використання мережного диска. Мережним диском є названий за правилами присвоєння імен локальним дискам спільний ресурс мережі. Для його під'єднання необхідно:

у вікні переглядача *Мій комп'ютер (Mycomputer)*виконати команди меню *Сервіс — Підключити мережний диск (Tool— Mapnetworkdrive);*

- ✓ задати ім'я диска;
- ✓ вказати розташування мережного ресурсу;
- ✓ вказати необхідність автоматичного під'єднання диска при кожній реєстрації користувача в системі: *Відновлювати при вході в систему (Reconnectatlogon);*
- ✓ за потреби вказати ім'я користувача та пароль доступу до ресурсу: *Під'єднання під іншим іменем (Connectusingadifferentusername)*(рис. 2.15).

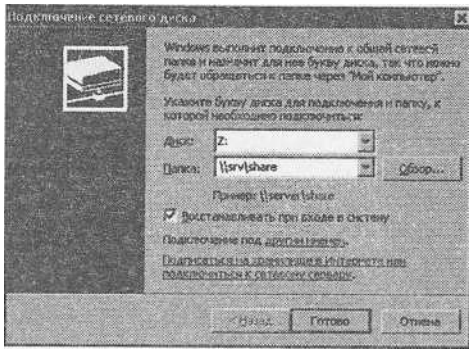


Рис. 2.15. Під'єднання мережного диска

Автентифікація при звертанні до розподіленого ресурсу будь-яким із запропонованих способів відбувається так:

- ✓ клієнт надсилає дані, які були введені користувачем у процесі реєстрації в системі;
- ✓ якщо логін і пароль збігаються із записом бази користувачів сервера, то сервер авторизує клієнта;
- ✓ якщо логін і пароль не збігаються з жодним записом бази користувачів сервера, то сервер надсилає запит клієнту на введення імені користувача та пароля.

Ще одним завданням, яке постає перед системним адміністратором, є конфігурування принтера для друку документів з віддаленого комп'ютера. Для цього потрібно встановити загальний доступ до принтера (за умови, що драйвер принтера вже встановлено на одному з комп'ютерів).

Для цього можна використати *Панель управління — Принтери й факси (ControlPanel— Printerandfaxes).*На вкладці *Доступ* властивостей принтера потрібно вказати режим загального доступу (рис. 2.16). На вкладці *Безпека (Security)*можна вказати правила доступу до принтера окремих користувачів та їх груп.

Тоді можна встановити принтер на інших комп'ютерах мережі, дотримуючись вказівок майстра встановлення принтера.

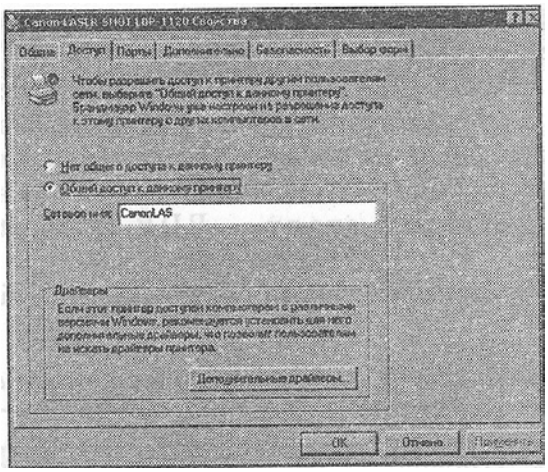


Рис. 2.16. Конфігурація мережного принтера

Після цього можна друкувати документи з будь-якого комп'ютера локальної мережі.

Контрольні запитання

1. Що таке розподілений ресурс?
2. Як створити розподілений ресурс?
3. Які способи створення розподілених ресурсів Вам відомі?
4. Перелічіть параметри, які потрібно вказати при створенні спільної папки.
5. Які правила доступу до спільної папки Вам відомі?
6. Які способи звертання до спільних папок Ви знаєте?
7. Як співвідносяться правила доступу через мережу та правила доступу до файлової системи NTFS?

2.5. Віддалене адміністрування сервера за допомогою служби терміналів

Під терміналом в інформаційних технологіях розуміють робоче місце багатокористувацьких систем. Відповідно сервером терміналів називатимемо сервер, який надає інтерфейс користувача (графічний, командний) програмі-клієнту. В ОС Windows Server 2003 служби терміналів дають змогу спільно використовувати програми за допомогою таких інструментів, як *Дистанційне управління робочим столом(RemoteDesktop), Віддалений*

помічник(RemoteAssistance) і *Сервер терміналів(TerminalServer).*

За замовчуванням служба терміналів встановлюється разом з WindowsServer2003 у режимі віддаленого адміністрування — дозволяє тільки два паралельних віддалених підключення. Для функціонування сервера терміналів у ОС типу Windowspeалізовано протокол віддаленого робочого столу — RDP (RemoteDesktopProtocol).

Основні засоби адміністрування служби терміналів наведені в таблиці 2.2.

Таблиця 2.2.*Засоби адміністрування служби терміналів*

Засіб	**Опис**
Служба терміналів (Terminal Service)	Налаштування властивостей сервера терміналів, *(Terminal Services Configuration)*зокрема параметрів сеансу, мережі, робочого столу клієнта та
Диспетчер служб терміналів (Terminal Services Manager)	Надсилання повідомлень клієнтам, відключення або завершення сеансів, а також ініціювання віддаленого управління.
Підключення до віддаленого робочого столу	Програма-клієнт *Дистанційне управління робочим столом (Remote Desktop),*яка входить до складу Windows Server 2003
Ліцензуванняслужбтерміналів	Налаштування форм ліцензій для клієнтських підключень.

Розглянемо докладніше кожен із цих засобів.

Конфігурування служб терміналів проводять за допомогою утиліти *Конфігурація служб терміналів (TerminalServicesConfiguration)* з розділу *Адміністрування (AdministrativeTools)*панелі управління (рис. 2.17).

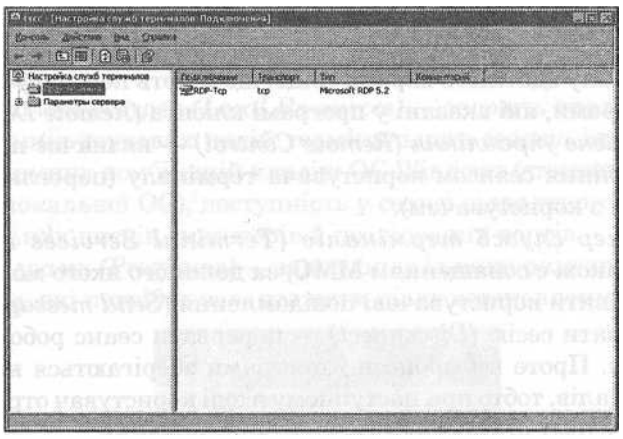


Рис. 2.17. Утиліта конфігурування служб терміналів

Ця утиліта є оснащенням MMC, у розділі *З'єднання (Connection)* якої можна встановлювати параметри сервера терміналів. Розглянемо деякі з них.

- ✓ *Загальні (General)*— надає можливість вказати рівень шифрування й механізм перевірки вірогідності підключень до цього сервера.
- ✓ *Мережний адаптер (NetworkAdapters)*—можна вказати мережні плати на сервері, які будуть приймати віддалені підключення за протоколом RDP.
- ✓ *Параметри входу (LogonSettings)* — адміністратор може задати певні реквізити для підключення замість логіна та пароля, які передає клієнт.
- ✓ *Дозволи (Permissions)*— дає змогу вказати облікові записи користувачів і груп, яким буде дозволено реєструватися в системі через службу терміналів (подібно до правил файлової системи NTFS).
- ✓ *Середовище (Environment)*— надає можливість встановити розміщення профілю користувача та визначити програму, яка завантажуватиметься при вході на сервер терміналів, і яка буде єдиним програмним засобом у сеансі. Після закриття вказаної програми сеанс буде завершено. Зазначені параметри перекривають відповідні налаштування програми клієнта *(RemoteDesktop).*
- ✓ *Параметри клієнта (ClientSettings)*— надає можливість змінити параметри інтерфейсу клієнта, зокрема глибину кольорів, роздільну здатність екрана тощо, що мають перевагу перед параметрами, які вказані у програмі клієнта *(RemoteDesktop).*

- ✓ *Віддалене управління (RemoteControl)*— визначає параметри управління сеансом користувача терміналу (перегляд чи взаємодія з користувачем).

Диспетчер служб терміналів (TerminalServicesManager) (рис. 2.18) також є оснащенням ММС, за допомого якого можна:

- ✓ відправити користувачеві повідомлення *(Sendmessage)]*
- ✓ від'єднати сесію *(Disconnect)*— перервати сеанс роботи користувача. Проте всі процеси і програми зберігаються на сервері терміналів, тобто при наступному вході користувач отримає свій сеанс у тому стані, в якому він був перерваний;
- ✓ завершити сеанс роботи користувача *(LogOff)*— сеанс роботи користувача буде перервано, при цьому всі програми будуть завершені коректно;
- ✓ перервати сеанс *(Reset)*— сеанс роботи користувача буде перервано, всі процеси будуть завершені в аварійному режимі, документи користувача збережені не будуть;
- ✓ отримати статистику сеансу *(Status).*

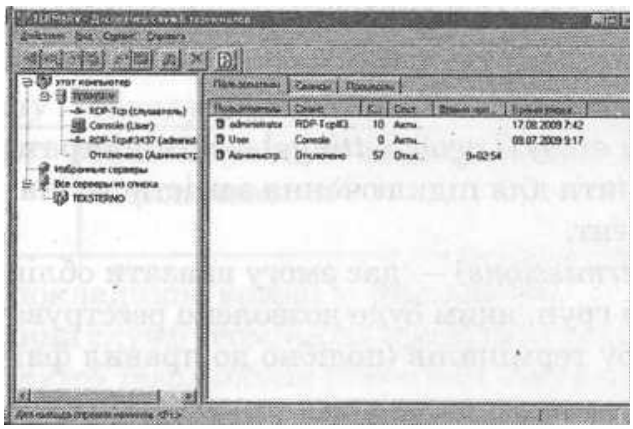


Рис. 2.18. Диспетчер служб терміналів

До параметрів клієнта віддаленого робочого столу (рис. 2.19) належать:

- ✓ *Загальні (General)*— параметри вибору комп'ютера для під'єднання, налаштування імені облікового запису користувача та пароля для входу в систему;*Екран (Display)*— задає розмір вікна клієнта, глибину кольорів і доступність панелі підключень при роботі в режимі на

повний екран;

- ✓ *Локальні ресурси (LocalResources)*— задають параметри передавання звукових подій термінального сеансу, інтерпретацію системних комбінацій клавіш ОС Windows(стосовно термінала чи локальної ОС), доступність у сеансі віддаленого доступу локальних дисків, принтерів й послідовних портів.
- ✓ *Програми (Programs)*— задає шлях і папки розташування програм, які потрібно завантажити після встановлення з'єднання.

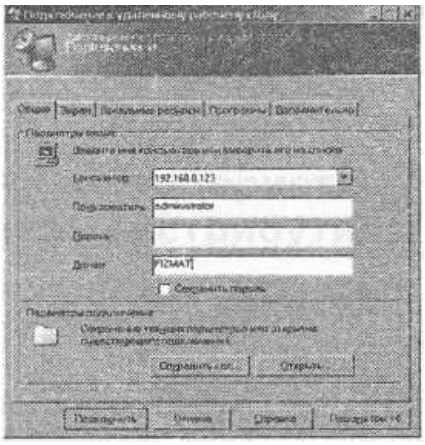


Рис. 2.19. Програма-кліент служби терміналів

Ліцензування сервера терміналів використовують тоді, коли сервер потрібен не лише для віддаленого адміністрування (дві одночасних сесії), а й для віддаленої роботи багатьох користувачів.

Сервер терміналів може працювати в одному із двох режимів:

- ✓ ліцензія на з'єднання (*Per-sessionlicensing)*— у цьому випадку сервер повинен мати окрему ліцензію для кожної з одночасних сесій;
- ✓ ліцензія на пристрій (комп'ютер клієнта) *(Per-devicelicensing)*— кожен клієнт повинен мати власну ліцензію.

Отримати ліцензії можна з віддаленого сервера ліцензування або шляхом встановлення відповідної служби на сервері терміналів.

Докладний розгляд цього питання можна знайти в літературі [24, с. 1103-1107].

Контрольні запитання

1. Яке тлумачення термінів: термінал, сервер терміналів?
2. Які є засоби адміністрування служби терміналів ОС WindowsServer2003?
3. Які є режими функціонування сервера терміналів?
4. Які є параметри служби терміналів?
5. Як встановити дозвіл входу на сервер терміналів для користувача?
6. Які є види ліцензування термінальних сесій?
7. Які відмінності між відключенням, завершенням і перериванням сеансу користувача сервера терміналів?

3. Адміністрування сервера одноранговой мережі з використанням ОС Linux

3.1. Загальна характеристика ОС Linux (на прикладі дистрибутиву Fedora)

ОС Linux — один з видів UNIX-подібних операційних систем, побудований на основі однойменного ядра. Linux — це ОС з відкритими вихідними кодами.

На відміну від більшості інших ОС Linux не має єдиної «офіційної» комплектації. Linux поставляють у вигляді так званих дистрибутивів, в яких інтегровані ядро, програмне забезпечення, що вільно поширюється, та комерційні програми. Найбільш відомими дистрибутивами Linux є Slackware, Debian Linux, Red Hat, Fedora, Mandriva, SUSE, Gentoo, Ubuntu.

Тут розглядатимемо один з дистрибутивів ОС Linux — Fedora, який розробляє компанія Red Hat. Fedora може бути платформою для побудови сервера, оскільки містить необхідні сервіси:

- ✓ службу терміналів (сервер SSHD);
- ✓ сервери розподілених ресурсів (NFS, Samba);
- ✓ сервер доменних імен (DNS-сервер BIND);
- ✓ службу призначення мережних адрес (DHCP-сервер);
- ✓ веб-сервер Apache;
- ✓ FTP-сервери (VSFTPD, ProFTPD тощо);
- ✓ поштові служби (Senmail, Postfix, Dovecot, Cyrrus).

Рекомендованими вимогами до апаратного забезпечення з боку Fedora є:

- ✓ процесор із частотою від 400 МГц;
- ✓ 256 Мб оперативної пам яті;
- ✓ 100 Мб - 9 Гб на жорсткому диску (залежно від обраного програмного забезпечення).

Стосовно адміністрування сервера на основі Fedora, то практично всі відомості наведені у цьому розділі стосуються й адміністрування серверів під управлінням й інших дистрибутивів ОС Linux.

Контрольні запитання

1. Що розуміють під дистрибутивом стосовно ОС Linux?

2. Які дистрибутиви ОС Linux Вам відомі?
3. Порівняйте програмне забезпечення ОС Windows Server 2003 і Fedora, яке потрібне для організації сервера.
4. Порівняйте рекомендовані вимоги до апаратного забезпечення від ОС Windows Server 2003 і Fedora.

3.2. Командний рядок як засіб адміністрування ОС Linux

Незважаючи на те, що до складу дистрибутивів ОС Linux належать й потужні графічні середовища (наприклад, KDE, Gnome), основним засобом її адміністрування залишаються команди ОС та параметри сервісів, записані в текстових файлах. Команда ОС Linux має формат:

команда [-опції] [параметри].

Опціями є літери, які дещо змінюють результат виконання команди. Перед ними вводять знак «мінус». Параметрами, зазвичай, є назви файлів або каталогів, до яких застосовують команду. Складові команди, які містяться у квадратних дужках є необов'язковими. Основні команди ОС Linux наведено у таблиці 3.1.

Таблиця 3.1. Структура файлової системи ОС Linux

Команда	**Дія команди**
ls	виведення списку файлів поточного каталогу
cd [каталог]	зміна поточного каталогу
cp [що копіювати] [куди копіювати]	копіювання файлів
mv[щоперемістити] [куди перемістити]	переміщення або перейменування файлів
rm [файл(и)]	вилучення файлів
mkdir [каталог]	створення каталогу
rmdir [каталог]	вилучення каталогу
touch [назва файла]	створення файла
cat [назва файла]	перегляд вмісту файла

grep [рядок]	знаходить рядки, що містять вказаний рядок
less [назва файла]	перегляд вмісту файла з можливістю повернутися до попередніх сторінок
find <назва файла>	пошук файлів
pico [назва файла]	редагувати текстовий файл
lynx [URL]	перегляд WWW сторінок
tc	файловий менеджер "Midnight Commander"
telnet [IP:порт]	з'єднання із сервером на вказаний порт
ftp [сервер]	з'єднання із сервером за протоколом FTP
startx	запуск графічного інтерфейсу X-Window
назва_програми	запуск файла з стандартних каталогів
./назва_програми	запуск файла з поточного каталогу

Наприклад, для того щоб скопіювати файл*resolv.conf* з каталогу */etc* у каталог */home/student* потрібно викопати команду:

cp /etc/resolv.conf/home/student

Відомості про формат команд Linux можна отримати за допомогою довідкової команди*man:*

man <імя команди>

ОС Linux використовує деревоподібну файлову систему Ext3, в якій всі файли зберігаються в каталогах, що логічно об'єднані в загальне дерево зі спільним коренем, який позначають символом «/». Файлова система ОС Linux, на відміну від ОС Windows, не має логічних дисків. Логічні або фізичні пристрої приєднують (монтують) до певних каталогів. Структура каталогів ОС Linux наведена у таблиці 3.2.

Таблиця 3.2. Структура файлової системи ОС Linux

Назва каталогу	Опис
/	кореневий каталог файлової системи
/bin	каталог стандартних виконуваних файлів
/boot	каталог завантаження, містить ядро ОС
/etc	каталог конфігураційних файлів
/dev	каталог файлів пристроїв
/sbin	каталог програм для адміністрування системи
/lib	каталог файлів бібліотек і модулів ядра системи
/mnt	каталог для монтування інших файлових систем
/proc	каталог файлів, які відображають процеси системи
/root	домашній каталог адміністратора системи
/home	каталог для розміщення домашніх каталогів і файлів користувачів
/usr	каталог для прикладних програм, документації, вихідних кодів
/var	каталог файлів ОС, які постійно змінюються
/tmp	каталог зберігання тимчасових файлів ОС

Основною складовою ОС Linux, що постійно знаходиться в оперативній пам'яті, є ядро (Kernel). Ядро ОС опрацьовує переривання від пристроїв, виконує запити системних процесів і програмного забезпечення користувача, розподіляє віртуальну пам'ять, створює й завершує процеси, забезпечує багатозадачність за допомогою перемикання між ними, містить драйвери пристроїв, обслуговує файлову систему.

Дані про кожен процес містять:

- ✓ PID — ідентифікатор процесу;
- ✓ PPID — ідентифікатор батьківського процесу;
- ✓ TTY — назву термінала, з якого був завантажений процес;
- ✓ WD — робочий каталог процесу;
- ✓ RID, RGID — ідентифікатори облікового запису користувача та групи, що завантажив процес;
- ✓ NICE — пріоритет процесу.

У ОС Linux процеси поділяють на:

- ✓ *системні*, які породжує ядро при завантаженні ОС;
- ✓ *користувальні,* які завантажують під час сеансу роботи користувачі;
- ✓ *демони (daemon),* що завантажуються під час старту ОС після ініціалізації ядра; демони є потрібними для виконання операційною системою своїх функцій (наприклад, служби NFS або DNS).

Розглянемо команди для роботи з процесами в ОС Linux.

Команда*top* подібна до диспетчера задач ОС Windows. Вона виводить таблицю процесів, які відсортовані за обсягом пам'яті, яку займають.

Команда*ps* виводить список процесів. Важливими опціями команди*ps* є:

- ✓ -p <PID> — процеси з певними ідентифікаторами ID;
- ✓ -u <UID> — процеси, завантажені обліковим записом користувача з ідентифікатором UID;
- ✓ -e — усі процеси в системі;
- ✓ -H — виведення списку процесів у вигляді дерева.

Конвеєр — технологія передачі результатів виконання однієї команди на вхід іншої. Символом конвеєра є знак «|», який розміщують між командами.

Наприклад, для пошуку запису про процес postfix у результаті виконання команди*ps* можна використати конвеєр:

ps -e | grep postfix.

Команда*kill* дає змогу припинити виконання процесу. Синтаксис команди такий:

kill [-s <сигнал>] <PID>

Процеси ОС Linux можуть опрацьовувати понад 10 сигналів завершення. Наприклад, при завершенні сеансу роботи ОС надсилає процесам користувача сигнал з номером 1. Для коректного завершення процесу в команді*kill* використовують сигнал з номером 15. Безумовне завершення процесу викликає сигнал з номером 9. Звичайно, застосовувати всі сигнали команди*kill* може лише системний адміністратор. Інші користувачі можуть завершувати лише власні процеси.

Для завантаження команд з певним пріоритетом використовують команду*nice*. Синтаксис команди:

nice -<номер><команда>

Рівень процесу визначає номер, значення якого є обернено пропорційним пріоритету і лежить у діапазоні -20 до 19. Для зміни пріоритету процесу використовують подібну до*nice* команду:

renice -<номер><PID>,

де PID — ідентифікатор процесу. Збільшувати пріоритет процесу (вводити від'ємні номери в командах*nice* і*renice)* може лише адміністратор (root).

Ще одним завданням, яке доводиться виконувати адміністратору ОС Linux, є монтування файлових систем. Для виконання цього завдання використовують файл */etc/fstab.* Кожен рядок цього файла є записом, що відповідає одній файловій системі та містить поля, що розділені пробілами. Формат файла такий:

<пристрій><точкамонтування><тип><опції><дамп><номер_fsck>

Розглянемо поля файла.

- ✓ Пристрій — це файл, наприклад,*/dev/sda1*.
- ✓ Точка_монтування — це каталог, у який здійснюється приєднання файлової системи.
- ✓ Тип — тип файлової системи. Якщо в цьому полі вказати параметр*auto,* то ОС намагатиметься визначити тип файлової системи автоматично.

- ✓ Дамп — ознака потреби в резервному копіюванні системи за допомогою утиліти*dump.* Значення 1 задіює резервне копіювання, значення 0 — відміняє.
- ✓ «номер_fsck» — визначає порядок тестування файлової системи утилітою*fsck.* Якщо в цьому полі вказати значення «0», то тестування проводитись не буде.

Опції монтування за допомогою файла*/etc/fstab* наведені у таблиці 3.3.

Таблиця 3.3. Основні опції монтування

Опція	Значення
auto	Автоматичне монтування (без команди mount)
ro	Монтування файлової системи в режимі тільки читання
rw	Монтування файлової системи в режимі читання і запису
exec	Файли у файловій системі можуть бути виконуваними
suid	Використання режиму запуску від імені адміністратора
user	Дозволити монтування від імені користувача
defaults	Застосувати опції за замовчуванням (*rw,suid, exec, auto)*
codepage = = <значення>	Кодова сторінка в іменах файлів
iocharset = = <значення>	Виводити символи в іменах файлів згідно певного набору

Якщо файлова система не описана у файлі*/etc/fstab*, то монтування можна здійснити за допомогою команди*mount.* Формат команди такий:

mount опції <пристрій><точка_монтування>

Опції команди*mount* аналогічні файлу */etc/fstab.* Наприклад, для монтування*usb* флеш-диска потрібно виконати:

mount -t vfat /dev/sda1/mnt/usb

Конфігурування сервісів у ОС Linux (веб-, FTP-, поштові сервери тощо) передбачає виконання адміністратором таких завдань:

- ✓ вивчення теоретичних основ функціонування служби;

- ✓ ознайомлення з документацією розробника, наприклад, за допомогою команди*man;*
- ✓ конфігурування сервісу — редагування файлів у каталогах*/etc* та*/usr/local/etc;*
- ✓ запуск (перезавантаження) служби — виконання команд */etc/init.d/<назва_сервісу>start (restart)* або*service<назва_сервісу>start (restart);*
- ✓ аналіз журналів (файлів) повідомлень ОС, які містяться в каталозі */var/log.*

Контрольні запитання

1. Порівняйте логіку виконання задач системного адміністрування в ОС Linux та ОС Windows.
2. Яка структура файлової системи Ext3? Порівняйте її зі структурою системного диска ОС Windows.
3. Перелічіть основні команди для роботи з процесами ОС Linux. Чи можна їх реалізувати в диспетчері задач ОС Windows?
4. Як приєднати додатковий вінчестер у ОС Linux?
5. Опишіть процес конфігурування сервісів у ОС Linux.

3.3. Управління обліковими записами користувачів і груп

Для управління роботою користувачів у ОС Linux реалізовано механізм облікових записів і груп. Система опрацьовує дані про облікові записи користувачів і груп, використовуючи такі конфігураційні файли:

- ✓ */etc/passwd* — дані про облікові записи користувачів (окрім паролей);
- ✓ */etc/shadow* — шифровані паролі облікових записів користувачів;
- ✓ */etc/group* — дані про облікові записи груп користувачів;
- ✓ */etc/default/useradd* — властивості, які присвоюють новим обліковим записам;
- ✓ */etc/login.defs* — параметри безпеки паролів (мінімальна довжина, термін дії тощо);

- ✓ */etc/skel* — файли налаштувань, які у процесі створення нового облікового запису користувача копіюються в домашній каталог останнього.

У файлі*/etc/passwd* дані про облікові записи користувачів записані у такому вигляді:

username:password:UID:GID:full_name:home_dir:login_shell, *де*

- ✓ username — реєстраційне ім'я (логін користувача);
- ✓ password — у файлі*/etc/passwd* у цьому полі записано знак «*», а криптований пароль міститься у файлі /*etc/shadow;*
- ✓ UID — унікальний числовий ідентифікатор облікового запису користувача;
- ✓ GID — унікальний числовий ідентифікатор облікового запису первинної групи користувачів; окрім первинної групи обліковий запис може належати й до інших груп;
- ✓ full_name — повне ім'я користувача;
- ✓ home_dir — домашній каталог користувача; за замовчуванням він міститься у каталозі */home;*
- ✓ login_shell — командний інтерпретатор — програма для виконання команд, уведених користувачем.

Наприклад, запис про користувача student у файлі*/etc/passwd* має вигляд:

student:x:501:501:Student TNPU:/home/student :/bin/bash

Якщо в розглянутому записі замість *«x»* ввести «!!», то пароль вважається не введеним і користувач не зможе зареєструватися в системі.

Використання двох файлів з обліковими записами користувачів *(/etc/passwd та /etc/shadow)* є виправданим з точки зору безпеки системи. Зазвичай, до файла*/etc/passwd* доступ для читання мають усі користувачі. До файла*/etc/shadow* такий доступ має лише користувач root.

Дані про облікові записи груп користувачів містяться у файлі */etc/group* у такому форматі:

group name:password:GIB: membe r_gr up*, де*

- ✓ groupname — ім'я групи;
- ✓ password — пароль групи (практично не використовують);

- ✓ GID — унікальний числовий ідентифікатор облікового записугрупи користувачів;
- ✓ member_group — облікові записи користувачів, які є членами групи.

Наведемо приклад запису з файла/etc/group:

webmasters:*:250: victor,alex.

Звичайно, додавати облікові записи користувачів і груп можна редагуванням файлів */etc/passwd* та */etc/group.* Проте ОС Linux надає й стандарні утиліти для виконання цих завдань. Розглянемо деякі з них.

Команда*useradd* додає новий обліковий запис користувача. Синтаксис команди такий:

useradd [-опції] <ім'я користувача>

Важливими опціями команди*useradd* є:

- ✓ -d <каталог> — домашній каталог користувача;
- ✓ -g <група> — основна група, до якої буде додано обліковий запис користувача; за замовчуванням в ОС Fedora для кожного нового облікового запису користувача створюється аналогічний запис і про групу;
- ✓ -G <групи> — список інших груп, до складу яких буде доданообліковий запис користувача;
- ✓ -s <файл> — командний інтерпретатор.

Команда*groupadd* додає новий обліковий запис групи користувачів. Синтаксис команди такий:

groupadd <ім'я групи>

Для встановлення пароля облікового запису користувача використовують команду*passwd.* Як і у випадку ОС Windows, адміністратор може змінити пароль будь-якого користувача системи. Для цього йому досить виконати команду:

passwd <логін>

Якщо команду*passwd* виконає звичайний користувач, то він зможе змінити лише власний пароль, але для цього йому доведеться ввести старий пароль.

Для зміни параметрів облікового запису користувача, використовують команду*usermod.* Синтаксис команди аналогічний до команди *useradd.* Важливими

опціями команди*usermod* є:

- ✓ -d <каталог> — домашній каталог користувача;
- ✓ -s<файл> — командний інтерпретатор;
- ✓ -u <UID> — числовий ідентифікатор облікового запису користувача;
- ✓ -g <група> — основна група;
- ✓ -e <12/31/2009> — дата закінчення терміну дії облікового запису.

Наприклад, якщо для облікового запису student потрібно встановити домашнім каталогом папку*/home/student*1, то потрібно виконати команду:

usermod -d /hote/student1 student

Для зміни параметрів облікового запису групи користувачів використовують команду*groupmod.*

Команда*userdel* видаляє обліковий запис користувача. Синтаксис команди такий:

userdel [-опції] <ім'я користувача>

Якщо вказати опцію -r ,то буде видалено не лише обліковий запис із файлів */etc/passwd, /etc/shadow,* а й відповідний домашній каталог.

Контрольні запитання

1. Як Ви розумієте зміст понять: користувач, обліковий запис користувача, обліковий запис групи користувачів?
2. Де зберігаються дані про облікові записи користувачів і груп ОС Linux?
3. Для чого в ОС Linux використовують файли /*etclpasswd* та */etc/shadow?*
4. Перелічіть команди для роботи з обліковими записами користувачів і груп.
5. Чи може обліковий запис користувача ОС Linux одночасно належати до декількох груп?
6. Пригадайте поля, які Ви заповнювали у процесі створення облікового запису користувача ОС Windows Server 2003. Чи можливо реалізувати їх в ОС Linux?

3.4. Правила доступу до об'єктів файлової*системи***Ext3**

Оскільки Linux є багатокористувацькою ОС, то її файлова система підтримує

механізм захисту файлів користувача від інших користувачів. Такий механізм відомий як система правил доступу до об'єктів файлової системи.

Кожен обліковий запис користувача може входити в одну із трьох категорій: власник, член групи власника, інші користувачі. Першим власником файла є користувач, що його створив. У подальшому можна змінити користувача та групу, які є власниками. Для цього застосовують команду:

chown [-опції] <користувач> [:<група>] файл *або*

chgrp [-опції] <група> файл

У деяких дистрибутивах Linux змінити власника може лише адміністратор, в інших — адміністратор і власник файла.

Правила доступу бувають трьох типів: *читання (read), запис (write) і виконання (execute).* У символьному вигляді правила записують як *rwx,* де r — читання,*w* — запис, *x* — виконання, знак «—» (мінус) позначає відсутність правила. Очевидно, що такі правила можна подати як двійкову тріаду. Наприклад, правило r—x, можна записати як $101_{(2)}$або як цифру $5_{(8)}$ у вісімковій системі числення.

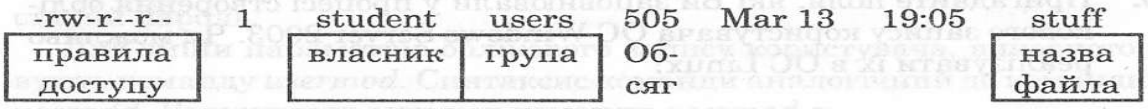
Оскільки правила доступу стосуються трьох типів користувачів (власник, група, інші), то абсолютні правила доступу повинні мати вигляд:

<правила_власника><правила_групи><правила_інших>

У вісімковому поданні абсолютні правила мають вигляд трицифрового числа, в якому старший розряд позначає правила власника, другий — групи, третій — інших користувачів.

Використовуючи команду*ls*з опцією -1, можна одержати на екрані перелік файлів у форматі, що містить відомості про права доступу.

Наприклад:



Якщо в колонці правил доступу замість першого знака «мінус» виведено літеру то це означає, що такий запис стосується каталогу.

Для зміни правил доступу використовують команду *chmod.* Синтаксис команди такий:

chtod [-опції] <правила доступу><файл (каталог)>

Важливою опцією команди ***chmod*** є -R. Вона дає змогу застосувати правила доступу до каталогу рекурсивно — правила будуть застосовані до всіх його дочірніх каталогів і файлів.

У команді *chmod*, окрім вісімкового подання, можна застосовувати й символьні позначення правил доступу (табл. 3.4).

Таблиця 3.4. Правила доступу в символьному вигляді

Аргумент		**Значення**
Категорія користувачів	u	Власник
	g	Група власника
	o	Інші
	a	Усі користувачі
Дія	+	Додати набір правил
	—	Видалити набір правил
	=	Встановити набір правил
Правило	r	Право на читання
	w	Право на запис
	x	Право на виконання
	s	Право зміни ідентифікатора користувача або групи
	t	Біт «прилипання» (sticky-bit)

Наприклад, для того щоб додати право на виконання файла *run.sh* групі-власнику й іншим користувачам потрібно виконати команду:

chmod go+x run.sh

Назва біта «прилипання» походить з тих часів, коли обсяг оперативної пам’яті був незначним, а процес підкачування повільним. Тоді наявність цього біта давала змогу залишати в пам'яті невеликі файли, які часто використовувались. На сьогодні визначення цього біта застосовують до каталогів. Це означає, що видаляти файли з каталогу матимуть право лише власники каталогу або файла. Зазвичай такий біт використовують до каталогів, відкритих для запису, наприклад, до каталогу */tmp.*

Правило зміни ідентифікатора користувача (s) означає, що під час виконання файл буде завантажено від імені користувача root. Таке правило є потенційною небезпекою в системі. Для надання користувачам прав інших користувачів можна скористатися командою:

su <користувач>.

Контрольні запитання

1. Які Вам відомі правила доступу до файлової системи Ext3?
2. Яких категорій користувачів стосуються правила доступу до файлової системи Ext3?
3. Як переглянути правила доступу до папки, файла?
4. Як позначають правила доступу із застосуванням вісімкової системи числення?
5. Для чого застосовують біт «прилипання» та правило зміни ідентифікатора користувача?

3.5. Створення розподілених мережних ресурсів засобами мережної файлової система

Мережка файлова система NFS (Network Filesystem) с засобом створення розподілених ресурсів у ОС типу Unix.

Ресурси, доступ до яких здійснюється за допомогою NFS, з точки зору користувача опрацьовуються так, як і локальні ресурси. Після монтування віддалений ресурс стає частиною локальної файлової системи користувача. NFS — система, що абстрагована від типів файлових систем як сервера, так і клієнта. Існує значна кількість реалізацій NFS-серверів та клієнтів для різних операційних систем.

Основою NFS є однойменний протокол (NFS), який має ту особливість, що кожен запит між клієнтом і сервером містить всі потрібні дані, а тому не потребує попередніх трансакцій. Це дає можливість зупиняти сервери NFS й знову завантажувати без перезавантаження клієнтів.

Для конфігурування сервера NFS використовують файл*etc/exports.* У цьому

файлі варто створити набір послідовних записів, кожен з яких визначатиме експортований каталог. Кожен такий запис повинен займати один рядок і мати такий формат:

каталог [клієнт1(опції)] [клієнт2(опції) [...]]

Першою складовою запису є повний маршрут до каталогу, який варто зробити доступним через мережу. Наприклад, таким маршрутом може бути */tmp/share.*

Існує кілька способів опису клієнтів у файлі */etc/export.*

- ✓ Один комп'ютер можна визначити, вказавши його IP-адресу або DNS-ім’я.Наприклад, один комп'ютер може бути визначений так: *172.25.3.5* або*ws-403-03.fizmat.tnpu.edu.ua.*
- ✓ Групу комп'ютерів можна визначити, вказавши їх маску під-мережі, наприклад *172.25.3.0/24.*
- ✓ Групу комп'ютерів можна визначити, вказавши їх DNS-імена в поєднанні з відомими символами * (зірочка) та ? (знак питання). Проте потрібно врахувати, що зазначені символи не позначають крапку, яка традиційно присутня в DNS-іменах.

Наприклад, запис **.fizmat.tnpu.edu.ua* не передбачатиме отримання доступу комп'ютера з DNS-іменем*ws-403-05.lab403.fizmat.tnpu.edu.ua.*

З точки зору безпеки системи доцільно використовувати для ідентифікації комп'ютерів IP-адреси, а не DNS-імена.

Для кожного клієнта або їх групи можна задати окремий набір опцій. Ці опції містяться в дужках і вказуються після ідентифікатора клієнта. Опції відділяють одна від одної комами. Наведемо найбільш важливі з них:

- ✓ *sync* або*async*—задають відповідно синхронний і асинхронний режими виконання операцій. У процесі запису в асинхронному режимі сервер може повідомити клієнта про те, що операція завершена, у той час як запис на диск ще триває. Це прискорює процес обміну даними, але створює загрозу їхній цілісності. За замовчуванням у сучасних серверах NFS передбачено асинхронний режим;

- ✓ *wdelay* та *no_wdelay* — відтермінування сервером процедури запису. В багатьох випадках такий підхід дозволяє збільшити продуктивність сервера;
- ✓ *secure* — вимагає, щоб запити до сервера надходили з портів привілейованого діапазону (1-1023). Протилежною за значенням є опція *insecure.*

Інші опції дають змогу управляти доступом до розподілених ресурсів. NFS-сервер не може перевірити ім'я користувача й пароль, як це відбувається, наприклад, у системі Microsoft Windows. NFS-клієнт працює, як правило, від імені*nobody* або*nfsnobody.* Тому для такого клієнта, що заслуговує довіри, рішення про надання доступу приймається на підставі відомостей про належність файла власникові й відповідних його прав.

Опціями, які управляють доступом у файлі /*etc/exports,* є:

- ✓ *ro* та*rw.* Опція*ro* визначає доступ тільки для читання вмісту експортованого каталогу, а опція*rw* надає також можливість записувати дані в цей каталог;
- ✓ *hide* та*nohide*. Наприклад, нехай у файловій системі сервера NFS каталог*usr* розміщений на одному розділі, а каталог*/usr/local* — в іншому. Опція*nohide* визначає необхідність надання доступу й до дочірнього каталогу, що міститься на іншому розділі диска (у прикладі таким каталогом є */usr/local);*
- ✓ *noaccess.* Опція забороняє доступ до каталогу, навіть якщо він є підкаталогом експортованого каталогу. Наприклад, потрібно надати доступ до піддерева каталогів */home,* за винятком каталогу */home/webmaster.* Для цього потрібно створити у файлі */etc/exports*типовий запис для каталогу /*home* й окремий запис для каталогу */home/webmaster,* вказавши в ньому опцію*noaccess;*
- ✓ *root_squash* і *no_root_squash.* За замовчуванням сервер NFS відкидає запити, які надходять від імені облікового запису користувача root, зареєстрованого в системі клієнта NFS. Такі запити, з точки зору безпеки, інтерпретуються як спроби доступу локального анонімного користувача (*nobody* або*nfsnobody).* Якщо потрібно виконувати адміністрування сервера з віддаленого вузла, то для того, щоб мати можливість працювати із правами локального користувача root, потрібно задати опцію *no_root__squash.* Подібна ситуація може трапитися, наприклад, при створенні резервних копій файлової системи;

- ✓ *anonuid* і*anongid.* Опції дають змогу перевизначити ідентифікатори користувача (UXD) та групи (GID), від імені яких будуть виконуватися операції на сервері NFS. За замовчуванням такими ідентифікаторами є ідентифікатори облікового запису *nobody (nfsnobody).*

Після кожної зміни файла */etc/exports* потрібно виконувати перезапуск сервера NFS за допомогою команди */etc/init.d/nfsrestart* або *servicenfsrestart.*

Для монтування розподілених каталогів використовують команду *mount*, яка має такий формат:

mount -t nfs<сервер:маршрут_до_каталогу><каталог_кліента>

Опція -t визначає тип файлової системи — NFS. Маршрут до спільного каталогу повинен бути повним (починатися із символу «/»).

Для того щоб експортований каталог був постійно доступний, потрібно створити запис у файлі*/etc/fstab.*

Контрольні запитання

1. Як Ви розумієте термін розподілений ресурс?
2. Як створити розподілений ресурс за допомогою сервера NFS?
3. Який формат має запис файла */etc/exports?*
4. Перелічіть параметри, які потрібно вказати при створенні спільного каталогу.
5. Які Вам відомі правила доступу до спільної папки?
6. Як співвідносяться правила доступу сервера NFS і правила доступу до файлової системи Ext3?

3.6. Віддалене адміністрування сервера за допомогою сервера терміналів OpenSSH

Для функціонування сервера терміналів у ОС типу UNIX реалізовано протокол SSH (Secure Shell — захищена оболонка). SSH використовує криптографію з'єднання між двома машинами, а також для автентифікації користувачів. Протокол SSH можна використовувати для безпечної реєстрації в системі віддаленого сервера, а також для копіювання даних між двома

комп'ютерами.

Сервером SSH у системах типу Unix є демон*sshd,* а клієнтом — програма*ssh,* яка поширюється як для ОС Linux, так і для ОС Windows.

- ✓ Файл конфігурації сервера*sshd* називають */etc/ssh/sshd_config.* Рядки файла*sshd_config*, які починаються з символа «#», є коментарями. Основними параметрами сервера *sshd* є:
- ✓ allowedadress <IP-адреса_1 > [<IP-адреса_2>] [<IP-adpeca_N>]— перелік IP-адрес, з яких дозволено з'єднання з сервером;
- ✓ KeyRegenerationlnterval lh — час (у годинах), протягом якогозмінюються ключі шифрування;
- ✓ *PermitRootLoginno*— заборона користувачеві реєструватися з використанням облікового запису root; для адміністрування системи потрібно після реєстрації в системі виконати команду su root;
- ✓ LogLevel INFO — режим ведення системного журналу;
- ✓ PasswordAuthenticacion yes — обов'язкова автентифікація з використанням паролів;
- ✓ PermicEmptyPasswords по — заборона застосування порожніх паролів;
- ✓ *LoginGraceTime 2m* — час (у хвилинах) для введення пароля;
- ✓ *RSAAuthenticationyes* — використання методу шифрування звідкритим ключем;
- ✓ *X11Forwardingyes* — дозвіл на роботу з графічним інтерфейсом ОС Linux.

Після кожної зміни файла */etc/ssh/sshd_config* потрібно виконувати перезапуск сервера*sshd* за допомогою команди */etc/init.d/sshdrestart*або*servicesshdrestart.*

Для приєднання до сервера терміналів*sshd* використовують команду*ssh,* формат якої такий:*ssh [-опції] <логін>@<сервер>*

Контрольні запитання

1. Які параметри сервера терміналів Ви знаєте?
2. З якою метою забороняють вхід на сервер терміналів для користувача root?
3. Де можна переглянути системний журнал сервера*sshd?*

4. Адміністрування домену Active directory

4.1. Робоча група і домен

У другому розділі розглянуто адміністрування сервера однорангової мережі, який входить до складу робочої групи. Робоча група — логічне об'єднання комп'ютерів, основними характеристиками якого є:

- ✓ кожен комп'ютер має свою, незалежну від інших, базу даних облікових записів користувачів (SAM — Security Account Manager);
- ✓ кожен користувач повинен мати локальний обліковийзапис на кожному комп'ютері, за яким він працює;
- ✓ щоб працювати з ресурсами віддаленого комп'ютера, користувачповинен мати обліковий запис;
- ✓ якщо користувач змінює пароль, то він повинен змінити пароль і на всіх комп'ютерах, до яких йому доведеться звертатися, інакше йому доведеться вводити старі реєстраційні дані;
- ✓ у робочій групі неможливе централізоване адмініструваннякомп'ютерів, які належать до неї;
- ✓ усі параметри безпеки стосуються тільки того комп'ютера, наякому вони були застосовані.

Враховуючи ці характеристики, можна вважати, що робоча група є ефективною формою об'єднання лише невеликої кількості комп'ютерів.

Доменом є логічне об'єднання комп'ютерів, основними характеристиками якого є:

- ✓ ієрархічна схема розташування комп'ютерів, коренем якої є контролер домену;
- ✓ контролер домену містить спільну базу облікових записів користувачів;
- ✓ користувач має єдиний доменний обліковий запис;
- ✓ користувач має обліковий запис, щоб працювати з ресурсамивіддаленого комп'ютера;
- ✓ користувач отримує доступ до комп'ютерів домену з використанням єдиних реєстраційних даних;

- ✓ зміна пароля користувача не призводить до зміни його авторизації при доступі до розподілених ресурсів;
- ✓ параметри безпеки можуть стосуватися різних комп'ютерів домену.

Отже, домен є мережною структурою, якою можна ефективно управляти, незважаючи на зміну кількості комп'ютерів, користувачів і зміну умов роботи.

4.2. Основні принципи функціонування домену Active Directory

Доменом є мережна структура, що має єдину базу даних із відомостями про об'єкти: облікові записи користувачів, груп, комп'ютерів тощо.

Із фізичної точки зору, домен — локальна мережа, яка містить контролер — комп'ютер, який містить базу даних об'єктів. Оскільки база даних домену може бути розміщена не на одному сервері, наприклад, містити копії на інших серверах, то в домені може бути кілька контролерів. Процес синхронізації всіх копій бази даних домену називають реплікацією.

Із логічної точки зору, домен Active Directory організовано у вигляді дерева об'єктів. Причому об'єктами такого дерева є не лише облікові записи, а й сам домен.

База даних Active Directory містить такі структурні об'єкти:

- ✓ розділи;
- ✓ домени;
- ✓ дерева доменів;
- ✓ ліси;
- ✓ сайти;
- ✓ організаційні одиниці.

Розглянемо детальніше кожен з наведених об'єктів. Розділів Active Directory є кілька.

- ✓ Розділ домену каталогу містить дані про користувачів, групи, комп'ютери і контакти домену.
- ✓ Розділ конфігурації каталогу містить дані про конфігурацію лісу, наприклад, про сайти, зв'язки сайту і підключення реплікації.

- ✓ Розділ схеми каталогу містить схему для всього лісу. Схема є набором правил про типи об'єктів Active Directory та допустимі операції з ними, розділ схеми реплікується на всі контролери домену в лісі.
- ✓ Розділ програмних засобів каталогу містить дані прикладних програм і сервісів, які інтегруються з Active Directory (наприклад, дані сервера DNS).

Домен є основним блоком у моделі служби Active Directory. Встановлюючи Active Directory, системний адміністратор створює домен. Домен є адміністративною межею, оскільки визначає межу правил безпеки. Домени Active Directory організовані ієрархічно. Перший домен стає кореневим доменом лісу, зазвичай, його називають кореневим доменом або доменом лісу. Наприклад, перший домен в установі fizmat.

Решта доменів в установі існують або як рівноправні, або як дочірні домени. Рівноправні за положенням домени знаходяться на тому ж ієрархічному рівні, що й кореневий домен. На рис. 4.1 зображена модель рівноправних доменів.

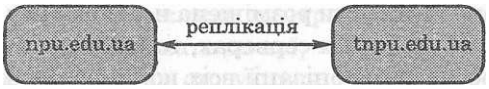


Рис. 4.1. Рівноправні домени

Домени, що встановлюються вслід за кореневим доменом, стають дочірніми доменами.

Дочірні домени використовують той самий простір імен Active Directory, що й батьківський домен. Наприклад, якщо перший домен — *tnpu.edu.ua*, то дочірній можна назвати *fizmat.tnpu.edu.ua.* На рис. 4.2 зображено батьківський (кореневий) та дочірні домени, які утворюють дерево доменів. Стрілками зображено процеси реплікації.

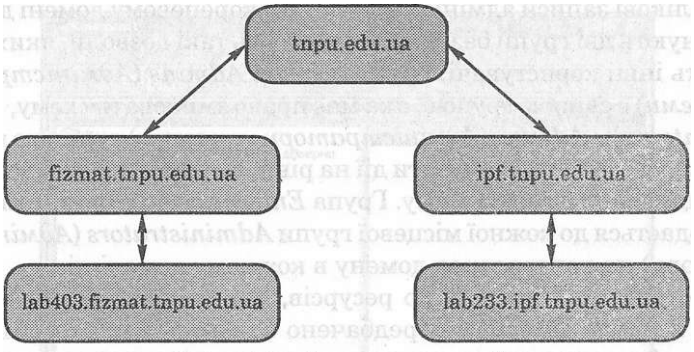


Рис. 4.2. Дерево доменів

Ліс доменів (рис. 4.3) є найдальшою межею реплікації в доменах установи. Всі домени і доменні дерева існують у межах одного або декількох лісів Active Directory. Ліс є загальним для всіх контролерів домену в лісі.

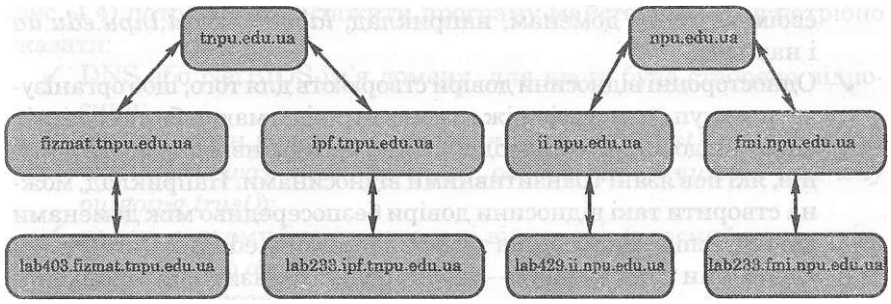


Рис. 4.3. Ліс доменів

Загальними компонентами лісу можуть бути:

- ✓ загальна схема;
- ✓ загальний розділ конфігурації каталогу — всі контролери домену в лісі мають той самий конфігураційний контейнер, який використовують для реплікації в межах лісу;
- ✓ загальний глобальний каталог, який містить дані про всі об'єкти лісу, що забезпечує ефективний пошук і дає можливість користувачам входити на будь-який домен лісу;
- ✓ загальна конфігурація відносин довіри — усі домени в лісі автоматично сконфігуровані так, що довіряють іншим доменам лісу;
- ✓ облікові записи адміністраторів — у кореневому домені для лісу існують дві групи безпеки. їм надають такі дозволи, яких не мають інші користувачі. Група*SchemaAdmins (Адміністратори схеми*) є єдиною групою, яка має право змінювати схему, а група *EnterpriseAdmins (Адміністратори у станови)* є єдиною групою, яка має право виконувати дії на рівні лісу, такі як додавання або видалення доменів з лісу. Група*EnterpriseAdmins* автоматично додається до кожної місцевої групи*Administrators (Адміністратори)* на контролерах домену в кожному домені лісу.

Для отримання доступу до ресурсів, які знаходяться за межами домену, в Active Directory передбачено відносини довіри, які є зв'язком між двома

доменами, за допомогою якого учасники безпеки можуть отримувати повноваження на доступ до ресурсів, розташованих в іншому домені. Існує кілька типів відносин довіри.

- ✓ Транзитивні — дерева доменів підтримують транзитивні двосторонні відносини довіри з іншими доменами в цьому дереві. Якщо повернутися до рис. 4.3, то домен*tnpu.edu.ua* довіряє своїм дочірнім доменам, наприклад,*lab403.fizmat.tnpu.edu.ua*і навпаки.
- ✓ Односторонні відносини довіри створюють для того, щоб організувати доступ до ресурсів між доменами, які не мають безпосередніх відносин довіри, або для підвищення продуктивності роботи доменів, які пов'язані транзитивними відносинами. Наприклад, можна створити такі відносини довіри безпосередньо між доменами lab403.fizmat.tnpu.edu.ua та lab233.ipf.tnpu.edu.ua.
- ✓ Відносини довіри лісу — двосторонні транзитивні відносини довіри між окремими лісами. Якщо встановлено такі відносини, то дочірній домен може отримати доступ ресурсів іншого лісу транзитивно через свій кореневий домен.

Для створення або перегляду відносин довіри між доменами використовують оснащення*ActiveDirectory — Домени і довіра (ActiveDirectory — DomainsandTrusts)* консолі MMC (рис. 4.4).

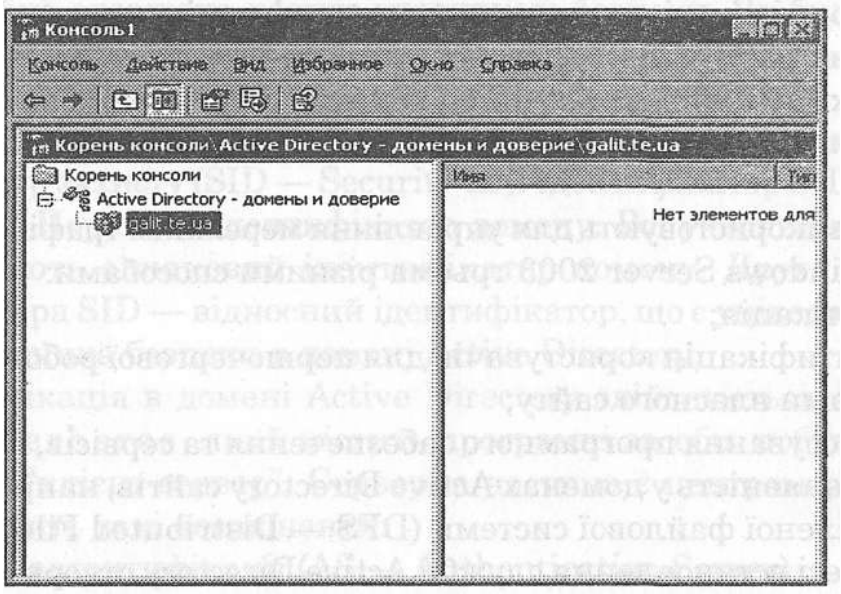


Рис. 4.4.Оснащення для роботи з відносинами довіри

Для створення відносин довіри в контекстному меню домену (рис. 4.4) потрібно завантажити програму-майстер, в якому потрібно вказати:

- ✓ DNS або NetBIOS-ім'ядомену, для якого буде створено відносини;
- ✓ *тип відносин довіри (*двосторонні (two-way trust), *односторонні* вхідні (one-way incoming trust), односторонні вихідні (one-way outgoing trust));
- ✓ домен, в якому будуть створені відносини (власний домен, віддалений або обидва домени);
- ✓ пароль відносин довіри;
- ✓ *рівень автентифікаїцї* — автентифікація в межах усього домену (Domain-wide authentication*), яка стосуватиметься всіх користувачів або* вибіркова автентифікація (Selective Authentication).

Для перегляду відносин довіри у вікні консолі потрібно відкрити властивості домену.

Логічні компоненти Active Directory, які розглянуті вище, практично не залежать від фізичної інфраструктури мережі. Наприклад, при проектуванні структури корпоративного домену питання про розташування користувачів не є суттєвим. Усі користувачі в домені можуть знаходитися як в одному офісному будинку, так і в офісах, розташованих по всьому світу.

Сайти забезпечують з'єднання між логічними компонентами Active Directory і фізичною мережною інфраструктурою. Сайт є частиною мережі, де всі контролери домену зв'язані швидким і надійним мережним підключенням. Переважно сайт містить підмережі локальної мережі або швидкодіючої глобальної мережі. З'єднання такого сайту з рештою мережі домену може здійснюватися через повільніші мережі.

Сайти використовують для управління мережним трафіком у межах мережі Windows Server 2003 трьома різними способами:

- ✓ реплікація;
- ✓ ідентифікація користувачів для першочергової роботи з контролерами власного сайту;

- ✓ застосування програмного забезпечення та сервісів, що передбачає наявність у доменах Active Directory сайтів, наприклад, розподіленої файлової системи (DFS — Distributed File System).

У процесі встановлення служби Active Directory створюється за замовчуванням сайт (Default First Site Name). Усі комп'ютери лісу належать цьому сайту. Створення нових сайтів пов'язане підмережами IP. Якщо сервер стає контролером існуючого домену, то його буде додано до сайту, який пов'язаний з IP-адресою підмережі цього сервера. За потреби контролери домену можна переміщувати між сайтами за допомогою оснащення*ActiveDirectory: Сайти і служби (ActiveDirectorySitesAndServices).*

Клієнтські комп'ютери визначають свої сайти вперше у процесі реєстрації в домені. Оскільки комп'ютеру клієнта не відомо, до якого сайту він належить, то він з'єднується з будь-яким контролером домену в домені. У процесі входу в систему контролер домену повідомляє клієнта, якому сайту він належить.

Ще однією структурною одиницею бази даних Active Directory є організаційні одиниці або підрозділи (OU — Organization Unit). Вони є контейнерами, в яких можуть зберігатися інші об'єкти Active Directory. Наприклад, до підрозділів можуть належати облікові записи користувачів, комп'ютерів, інші підрозділи тощо. Саме організаційні одиниці дають змогу реалізувати ієрархію об'єктів поточного каталогу. Крім того їх застосування спрощує адміністрування домену, завдяки механізмам встановлення правил доступу ACL (подібно до файлової системи NTFS), групових політик і делегування адміністративних повноважень.

Система безпеки Active Directory побудована з використанням двох типів об'єктів. Перший — учасник безпеки (обліковий запис користувача, групи, служби, комп'ютера). Другим об'єктом є сам ресурс, до якого потрібно одержати доступ учасникові безпеки. Як було зазначено вище до кожного об'єкта Active Directory застосовують правила доступу ACL.

При створенні об'єкта кожному учасникові безпеки призначають ідентифікатор захисту (SID — Security ID). Ідентифікатор SID містить дві складові.

Перша — ідентифікатор домену. Всі учасники безпеки в домені мають однаковий ідентифікатор домену. Друга частина ідентифікатора SID — відносний ідентифікатор, що є унікальним для кожного учасника безпеки в домені Active Directory.

Автентифікація в домені Active Directory здійснюється засобами протоколу Kerberos, який містить програмні засоби, побудовані за технологією "клієнт-сервер". Серверна частина є центром розподілу ключів і містить такі компоненти:

- ✓ сервер автентифікації (AS — Authentication Server);
- ✓ сервер видачі дозволів (TGS — Ticket Granting Server).

Кожному об'єкту сервер Kerberos видає ключ симетричного шифрування. Нехай, наприклад, клієнту Wsl потрібно отримати доступ до ресурсів сервера Srvl. Розглянемо етапи автентифікації клієнта за протоколом Kerberos.

- ✓ Клієнт Wsl надсилає серверу автентифікації AS власний ідентифікатор.
- ✓ Сервер автентифікації AS перевіривши, що клієнт Wsl є в його базі, повертає йому квиток$\mathbf{T}_{TGT}$ для доступу до сервера видачі дозволів і ключ $К_{C\_TGS}$ для взаємодії з сервером видачі дозволів TGS. Ці дані шифруються за допомогою ключа клієнта Wsl. Якщо на першому кроці взаємодії ідентифікатор відправив не клієнт Wsl, а зловмисник X, то отримані дані він розшифрувати не зможе. Проте і клієнт Wsl не зможе скористатися квитком T_{TGT}, оскільки він зашифрований ключем, який розподілили між собою сервер автентифікації та сервер видачі дозволів.
- ✓ Клієнт Wsl надсилає квиток, отриманий від сервера автентифікації AS, серверу видачі дозволів TGS, а також автентифікаційний блок, що містить ідентифікатор і час, коли було сформовано запит. Сервер видачі дозволів TGS розшифровує квиток T_{TGT} й отримує з нього дані про те, кому видано квиток, коли, на який термін, а також ключ шифрування, згенерований сервером AS для взаємодії між клієнтом Wsl і сервером TGS. За допомогою цього ключа розшифровується автентифікаційний блок. Якщо мітка в блоці збігається з міткою квитка $К_{C\_TGS}$, це свідчить, що посилку згенерував насправді клієнт

Wsl. Сервером TGS проводиться також перевірка часу дії квитка і часу відправлення запиту.

- ✓ Сервер TGS надсилає клієнту Wsl ключ шифрування K_{Ws1_Srv1}і квиток T_{Srv1}, що необхідні для доступу до Srvl.
- ✓ Клієнт Wsl надсилає квиток K_{Ws1_Srv1} і свій автентифікаційний блок серверу Srvl, який до цього часу зареєструвався в домені й отримав свій ключ шифрування $K_{TGT\ Srv1}$. Маючи цей ключ, сервер Srvl може розшифрувати квиток T_{Srv1} й отримати ключK_{Ws1_Srv1}.
- ✓ На останньому етапі сервер Srvl повинен підтвердити свою достовірність перед клієнтом Wsl.

Особливості реалізації протоколу Kerberos у Windows Server 2003:

- ✓ ключ клієнта генерується на основі його пароля. Тому в доменах Active Directory за замовчуванням діють правила безпеки, які забороняють використовувати занадто короткі та прості паролі;
- ✓ роль Kerberos -серверів виконують контролери домену;
- ✓ використання Kerberos вимагає синхронізації годинників на всіх робочих станціях домену.

Контрольні запитання

1. Як Ви розумієте терміни: домен, дерево доменів?
2. У чому відмінність функціонування комп'ютерів у домені та робочій групі?
3. Що називають реплікацією?
4. Які структурні об'єкти містить база даних Active Directory?
5. Для чого, на Вашу думку, реалізовано відносини довіри?
6. Наведіть приклад, коли необхідно створити односторонні нетран- зитивні відносини довіри.
7. У чому полягає основна ідея поточного каталогу?
8. У чому відмінність між підрозділами та групами користувачів Active Directory?

9. Чи правомірно називати автентифікацією процес розподілу ключів за протоколом Kerberos?
10. Порівняйте процес автентифікації користувачів робочої групи за протоколом NTLM і домену Active Directory за протоколом Kerberos.

4.3. Основи адміністрування домену Active Directory

Основним інструментом адміністрування домену Active Directory є оснащення консолі MMC*ActiveDirectory — користувачі та комп'ютери (ActiveDirectory — usersandcomputers).* Як видно з рис. 4.5 згадане оснащення має подібний вигляд до програми *Провідник (Explorer)* ОС Windows. У лівому вікні оснащення розташоване дерево організаційних одиниць домену, коренем якого є домен.

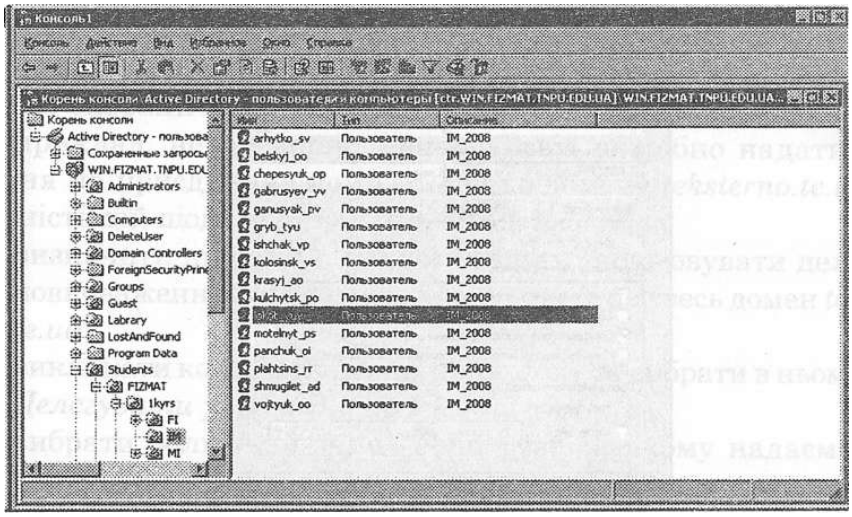


Рис. 4.5. Оснащення Active Directory — користувачі такомп'ютери

Основними операціями з об'єктами домену є їх створення, зміна і видалення. Створюючи підрозділ, обліковий запис користувача або групи користувачів, потрібно викликати контекстне меню того об'єкта, в якому створюємо новий об'єкт і з якого вибираємо відповідний пункт. Вводячи пароль для облікового запису користувача, потрібно враховувати вимоги правил безпеки домену щодо паролів користувачів (за замовчуванням: довжина пароля — не менше шести символів, пароль повинен містити великі та малі літери, цифри й інші символи).

Параметри облікового запису користувача можна змінити на відповідних вкладках у вікнах властивостей цього об'єкта.

Найбільш важливими серед них є:

- ✓ ім'я, прізвище, опис, адреса електронної пошти, які можна змінити на вкладці *Загальні (General);*
- ✓ логін користувача, заборона зміни пароля, режим вимкнення облікового запису, часові обмеження входу, реєстрація користувача лише в системі певних комп'ютерів, які можна змінити на вкладці *Обліковий запис (Account)* (рис. 4.6);
- ✓ розміщення профілю та мережних дисків користувача (вкладка*Профіль (Profile));*
- ✓ належність облікового запису користувача до груп (вкладка *Член груп (Memberof)).*

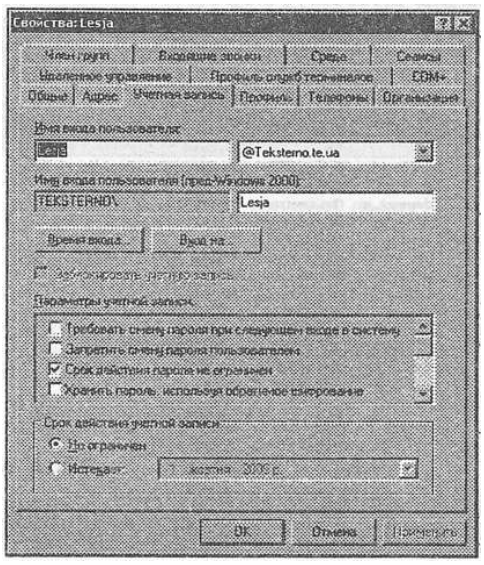


Рис. 4.6. Параметри облікового запису користувача

Профіль користувача — це сукупність налаштувань, які визначають робоче середовище користувача. Профілем користувача ОС Windows є вміст папки*DocumentsandSettings\Username,* де *Username* — логін користувача. До профілю належать такі папки як *Робочий стіл (Desktop), Мої документи (MyDocuments), Головне меню (StartMenu)* тощо. Якщо користувач працює за комп'ютером робочої групи, то налаштування його облікового запису зберігаються в локальному профілі. Оскільки в домені дані про облікові записи користувачів зберігаються централізовано, то існує можливість централізовано зберігати й профілі користувачів. На практиці профілі зберігають на одному з контролерів домену або на виділеному файл-сервері. Такий профіль можна копіювати із сервера

на локальний комп'ютер при реєстрації користувача в домені, а також копіювати на сервер при завершенні сеансу роботи. За способом зберігання профілю його називають переміщуваним.

Належність облікових записів користувачів до груп також можна змінити у властивостях відповідних груп.

Існують випадки, коли адміністратору необхідно дозволити виконання певних адміністративних завдань іншому користувачеві, який не належить до групи адміністраторів. У такому разі йдеться про делегування адміністративних повноважень. Для делегування повноважень адміністратору домену потрібно визначити:

- ✓ підрозділ, в якому будуть застосовувати делеговані адміністративні повноваження;
- ✓ якому користувачеві передаватимуться права на адміністрування;
- ✓ які операції щодо управління підрозділом делегуються.

Наприклад, нехай користувачеві Lesja потрібно надати повноваження на приєднання комп'ютерів до домену*teksterrio.te.ua.* Прослідовність дій щодо делегування буде такою:

- ✓ визначити підрозділ, в якому будуть застосовувати делеговані повноваження. У даному випадку ним буде увесь домен*teksterno.te.ua;*
- ✓ викликати контекстне меню підрозділу та вибрати в ньому пункт*Делегувати управління (Delegatecontrol);*
- ✓ вибрати обліковий запис користувача, якому надаємо права (рис. 4.7);
- ✓ *вказати делеговані повноваження (*Приєднання комп'ютера до домену (Connect computer to domain)) *(рис. 4.7),*

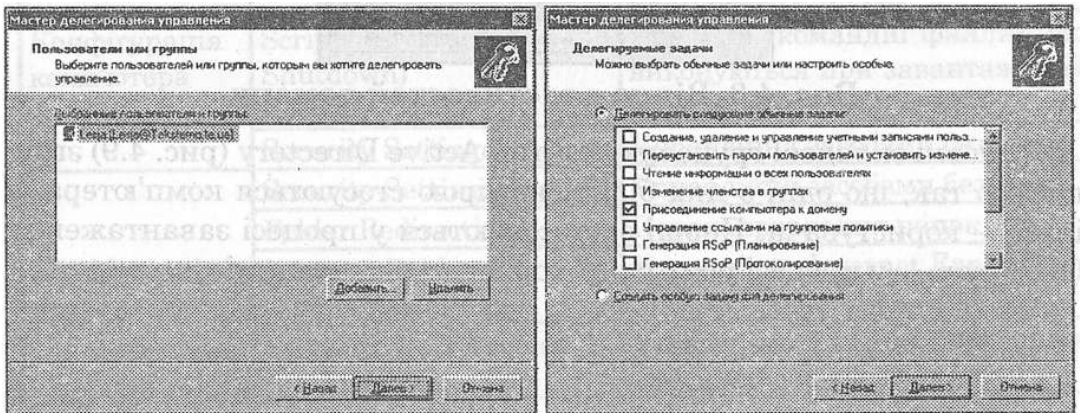


Рис. 4.7. Майстер делегування адміністративних повноважень

Ще одним засобом централізованого управління доменом Active Directory є групові правила (політика). Цей засіб можна застосовувати для визначення параметрів облікових записів користувачів, груп, комп'ютерів, опції віддаленого встановлення програмного забезпечення, сценарію реєстрації користувачів у домені, правила перенаправления папок. Групові політики можуть бути задіяні лише стосовно контейнерів (підрозділів, сайтів і самого домену).

Групові політики можна створити або редагувати з вікна властивостей контейнера на вкладці *Групова політика (GroupPolicy)* (рис. 4.8). Як видно з рисунка, до одного й того самого підрозділу можуть бути застосовані кілька окремих політик безпеки. Крім того у Windows Server 2003 редактор об'єктів групової політики реалізовано у вигляді оснащення консолі MMC.

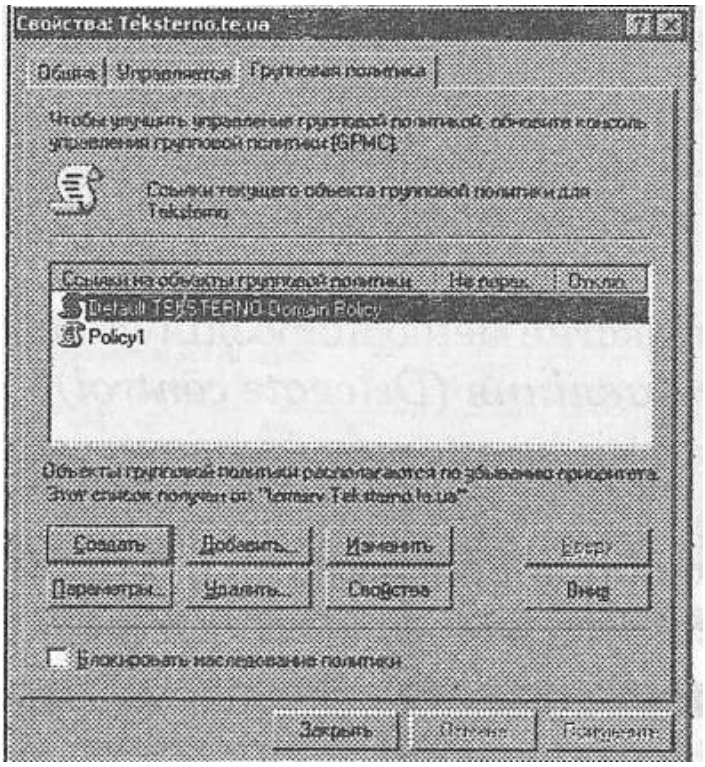


Рис. 4.8. Вікно властивостей домену

Основні складові групових політик Active Directory (рис. 4.9) згруповано так, що одні з них більшою мірою стосуються комп'ютера, а інші — користувача. Перші застосовуються у процесі завантаження ОС, другі — у процесі реєстрації користувача в системі.

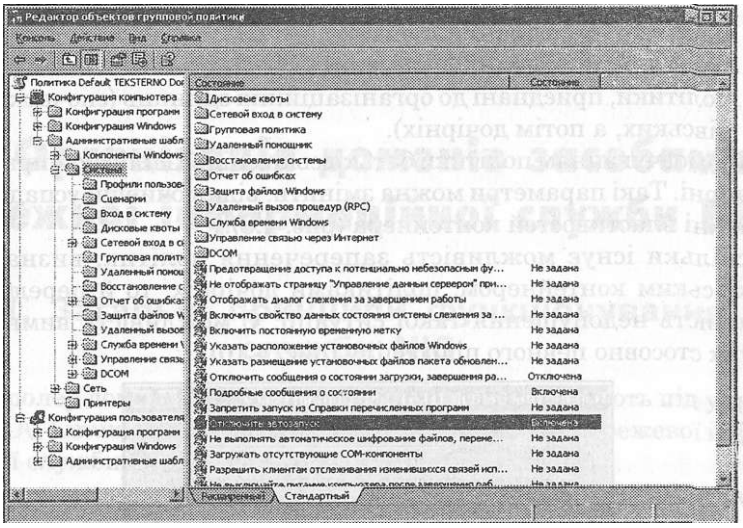


Рис. 4.9. Редактор об'єктів групової політики

У таблиці 4.1 наведено деякі складові групових політик та їх короткий опис.

Таблиця 4.1. Деякі складові групових політик Active Directory

Розділ	Складова	Опис
Конфігурація комп'ютера	Software Installation	Централізоване встановлення програмного забезпечення
	Scripts(Startup/Shutdown)	Сценарії (командні файли), що виконуються при завантаженні/ вивантаженні ОС
	Security Settings	Управління засобами безпеки
Конфігурація користувача	Security Settings	Управління засобами безпеки
	Folder Redirection	Перенаправлення папок
	Internet Explorer Maintenance	Управління Internet Explorer
	Roaming User Profiles	Управління переміщуваними профілями користувачів

Оскільки об'єкти домену Active Directory утворюють деревовидну структуру, то групові політики можуть діяти рекурсивно вздовж усього дерева об'єктів. На клієнтських комп'ютерах групові політики опрацьовуються у такій послідовності:

- ✓ локальні політики;

- ✓ політики, приєднані до сайтів;
- ✓ політики, приєднані до доменів;
- ✓ політики, приєднані до організаційних одиниць (спочатку батьківських, а потім дочірніх).

За замовчуванням політики батьківських підрозділів поширюються на дочірні. Такі параметри можна змінити, відключивши успадкування у вікні властивостей контейнера (рис. 4.8).

Оскільки існує можливість заперечення політик, визначених батьківським контейнером, політиками дочірніх, то й передбачено можливість недопущення такої ситуації. Є можливість вимкнення політик стосовно певного підрозділу (рис. 4.10).

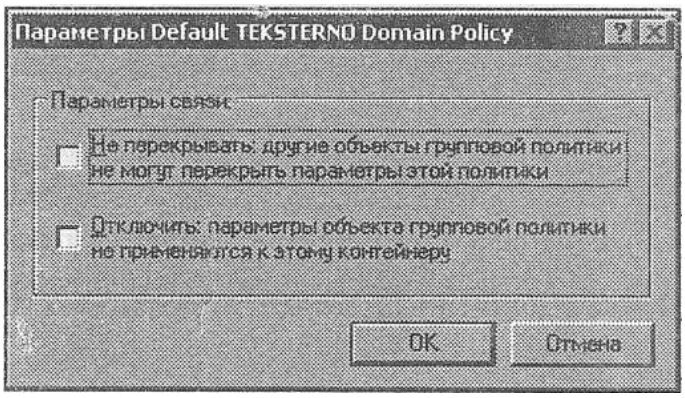


Рис. 4.10. Параметри політик безпеки

Контрольні запитання

1. У чому відмінність між обліковим записом користувача локального комп'ютера і домену?
2. Чи існують у системі контролера домену локальні облікові записи?
3. Як додати обліковий запис користувача до групи?
4. Що називають профілем користувача?
5. Яким повинен бути маршрут до переміщуваного профілю користувача?
6. Який зміст терміну делегування адміністративних повноважень? Яка послідовність дій щодо делегування повноважень?
7. Для чого, на Вашу думку, реалізовано механізм групової політики?
8. Чи можна застосовувати політики безпеки до окремого користувача домену?

9. Чи можуть окремі правила двох політик безпеки стосуватися одного підрозділу й суперечити одна одній?

5. Організація доменів засобами мережиш інформаційної служби NIS

5.1. Загальні принципи функціонування служба NIS

Контролер домену в мережі, комп'ютери якої працюють під управлінням ОС Linux, можна організувати за допомогою мережевої інформаційної служби (NIS — Network Information Service).

Загалом мережна інформаційна служба е універсальною клієнт-серверною базою даних. Проте в ОС Linux її зазвичай використовують для спільного доступу до файлів паролів і груп (*/etc/passwd* та */etc/group).* Найменшим елементом, який використовує NIS, є запис, що е рядком конфігураційного файла. Сервер зберігає копії системних файлів і забезпечує доступ до них через мережу.

З метою підвищення ефективності пошуку текстові файли кодують у двійкові файли. У процесі створення двійкових файлів обирають унікальні поля, за якими здійснюватиметься пошук. Оскільки у файлі */etc/passwd* унікальними є ім'я облікового запису користувача та його числовий ідентифікатор, то у процесі кодування створюються два файли — *passwd.byname* і*passwd.byuid.* Після кожної зміни файлів */etc/passwd* та */etc/group* необхідно наново створити двійкові файли бази даних.

Механізм взаємодії клієнтів і сервера NIS забезпечується роботою двох демонів*ypserv* та*ypbind*. Перший з них працює лише на серверах; він приймає запити від клієнтів і відповідає на них, здійснюючи пошук даних у двійкових файлах. Демон*ypbind* формує запити до серверів NIS. Сучасні версії демона*ypbind* у ОС Linux також перевіряють доступність інших контролерів у домені NIS. Така можливість має перевагу перед явним визначенням сервера як єдиного контролера домену NIS.

Існує два типи NIS-серверів:

- ✓ первинні (Primary) сервери NISзберігають текстові файли, які використовуються для створення двійкових файлів;
- ✓ вторинні (Secondary) NIS-сервери приймають на себе частину запитів

клієнтів. Після кожної зміни двійкових файлів на первинному сервері відбувається їх розсилання на вторинні сервери NIS.

Для виявлення серверів клієнти надсилають широкомовні запити, які не перенаправляються в інші мережі маршрутизаторами й шлюзами. Для конфігурування клієнтів для роботи окремим сервером NISвикористовують команду *ypset.*Проте при перших ознаках відсутності зв'язку з сервером клієнт пробує виявити новий сервер, перейшовши в широкомовний режим.

У ОС Linuxреалізовано значну кількість команд для роботи з двійковими файлами серверів NIS. Деякі з них наведено у таблиці 5.1.

Таблиця 5.1.*Деякі команди служби NIS*

Команда	**Опис**
ypserv	демон сервера NIS
ypbind	демон клієнта NIS
domainname	визначення домену NIS
yppush	оновлення двійкових файлів на вторинних серверах
makedbm	створення двійкового файла із текстового
ypmake	оновлення двійкових файлів на сервері
ypinit	ініціалізація сервера
ypset	з'єднання з певним сервером
ypuihich	виявлення поточного сервера
ypcat	виведення вмісту двійкового файла
yppasswd	зміна пароля на первинному сервері

Контрольні запитання

1. У чому відмінність між обліковим записом користувача локального комп'ютера і домену NIS?
2. Чи містять копії двійкових файлів паролів і груп домену робочі станції (вторинні сервери NIS)?
3. Чи досить команд *useradd* і *passwd* для створення облікового запису користувача в домені NIS?

5.2. Конфігурування сервера NIS

У дистрибутиві Fedoraсервер NISміститься в окремому пакеті *ypserv.*У дистрибутивах Debianта Ubuntuпакет *nis*містить як сервер, гак і клієнт.

Послідовність налаштування сервера NISнаведено у таблиці 5.2.

Таблиця 5.2.*Етапи конфігурування сервера NIS*

Опис	Команда
Перехід у каталог сервера NIS	***cd luarlyp***
Визначення імені домену	***donainname <домен>***
Ініціалізація первинного сервера	***ypinit*** *-m*
Ініціалізація вторинних серверів	***ypinit -s***
Завантаження сервісу NIS	***/etc/init.d/ypserv start***

На кожному з вторинних серверів потрібно за допомогою утиліти *cron*створити порядок оновлення двійкових файлів. Для зміни паролів користувачі домену можуть скористатися командою *yppasswd. У* цьому випадку на сервера NISповинен бути завантажений сервіс *yppasswdd.*

Для налаштування параметрів доступу до сервера NISвикористовують файл */etc/ypserv.conf.*Кожен рядок цього файлу має формат:

<комп'ютер>:<домен NIS>:<двійковий файл>:<дія>

У полі «комп'ютер» можна вказати як IP-адресу одного комп'ютера, так і IP-адресу та маску всієї підмережі. Поле «двійковий файл» може містити значення «*passwd.byuid*» і «*passwd.byname*». Поле «дія» може набувати значень:

- ✓ deny— відхилення запиту;
- ✓ port— опрацювання запиту, якщо він надійшов із привілейованого порту (<1024);
- ✓ none — опрацювання запиту в будь-якому випадку.

У перших трьох полях файла можна вказувати символ зірочку (*) для співставлення їм довільних значень.

Наведемо приклад файла */etc/ypserv.conf*:

172.25.3.0/255.255.252.0:fizmat::none*

**:* :passwd.byuid:deny*

*10.41.1.100.:fizmat: * :port*

**:* :*:deny*

У першому рядку визначено дозвіл на опрацювання запитів з підмережі *172.25.3.0,* які стосуються домену *fizmat.*Другий рядок забороняє доступ усім клієнтам до файла *passwd.byuid.*У наступному рядку дозволено доступ з комп'ютера, який має IP-адресу *10.41.1.100.* Нарешті, останній рядок забороняє доступ усім клієнтам, які не потрапили під дію попередніх правил.

Контрольні запитання

1. Опишіть етапи конфігурування сервера NIS?
2. У чому відмінність між командами *passwd*і *yppasswd?*
3. За якими критеріями можна обмежити доступ до сервера NIS?

5.3. Конфігурування клієнта NIS

Для приєднання клієнта до домену NIS потрібно внести зміни до файлів:

/etc/yp.conf, /etc/nsswitch.

Файл */etc/yp.conf*потрібен для початкового зв'язку NIS-клієнта з сервером. Формат файла такий:

domain<домен>server<IP або DNS-адреса сервера NIS>

Замість IP-адреси сервера може бути вказано параметр *broadcast,* що означатиме необхідність широкомовного пошуку сервера NIS. Такий режим не є безпечним, оскільки не має гарантій, що знайдений сервер справді відповідає за вказаний домен NIS.

Файл */etclnsswitch*визначає метод пошуку даних, потрібних для автентифікації. Розглянемо його фрагмент:

passwd: filesnis

shadow: *filesnis*

group: *filesnis*

Перший стовпець вказує на файл (тип даних — облікові записи користувачів, груп, паролі тощо). У першому рядку прикладу ним є файл *passwd.*Другий стовпець вказує на шляхи пошуку даних з файла *passwd.*Він може набувати одне зі значень:

- ✓ nis— пошук здійснюється у базі даних сервера NIS;
- ✓ dns — пошук здійснюється у базі даних сервера DNS;
- ✓ files— пошук здійснюється у локальному файлі.

Для визначення імені домену, до складу якого буде додано комп'ютер-клієнт, потрібно відредагувати файл */etc/sysconfig/network,* в який записати рядок:

NISDOMAIN-"<назва домену NIS>"

Завантаження демона NIS-клієнта можна здійснити за допомогою команди:

/etc/init.d/ypbindstart.

Після завершення конфігурування сервера і клієнтів NISможна перевірити коректність їх роботи за допомогою команди *ypcat passwd.*

Якщо конфігурування здійснене без помилок, то результатом команди буде виведення вмісту файла */etc/passwd.yp*сервера NIS.

Контрольні запитання

1. Які існують методи пошуку сервера NIS?
2. У чому полягає небезпека широкомовного пошуку сервера NIS?
3. Яка роль файла */etc/nsswitch*для організації автентифікації?

6. Організація домена засобами сервера Samba

6.1. Особливості конфігурування сервера Samba

Для інтеграції в мережі серверів і клієнтів, які працюють під управлінням ОС Linuxта ОС Windows, розроблено пакет Samba. Сервер Sambaзабезпечує:

- ✓ створення розподілених ресурсів;
- ✓ виконання функцій контролера домену;
- ✓ отримання доступу до розподілених ресурсів ОС Windows;
- ✓ створення мережевих принтерів і надання доступу до них.

Складовими пакета сервера Sambaє демони *smbd*і *nmbd*.Перший з них забезпечує функціонування протоколу SMB (SimpleMessageBlock— протокол простих повідомлень), другий — підтримку мережних імен за протоколом NetBIOS.

Основним конфігураційним файлом сервера Sambaє файл */etc/smb.conf (/etc/samba/smb.conf)*.Цей файл містить кілька секцій, назви яких містяться у квадратних дужках («[» «]»). Параметри кожної секції записують у форматі: *Параметр — значення.* Рядки файла, які починаються із символу «#» або «,» є коментарями.

Основною секцією файла *smb.conf є*[global]. Найбільш важливі параметри зазначеної секції наведено у таблиці 6.1.

Таблиця 6.1.*Параметри секції [global]*

Параметр	**Можливі**	**Опис**
workgroup	*lab 403*	назва робочої групи або домену, до яких належатиме сервер Samba
netbiosname	*srv-403*	назва сервера Samba
encryptpasswords	*yes(no)*	обов’язковекриптування паролів
security	*user*	для автентифікації потрібен логін і пароль
	domain	автентифікація відбувається в домені WindowsNT

	ads	автентифікація здійснюється в домені ActiveDirectory
	share	автентифікації на рівні ресурсів (як в ОС Windows98)
log file	*/var/log/smb.log*	розміщення файлів повідомлень сервера
interfaces	*10.0.0.018*	адреси мереж, з якими працюватиме сервер Samba
wins	*yes (no)*	виконання сервером Sambaфункцій сервера WINS
local master	*yes (no)*	виконання сервером Sambaфункцій основного переглядача робочої групи

Якщо у файлі smb.confвизначено параметр *security= user*, то автентифікація користувачів відбуватиметься за записами локальної бази облікових записів сервера Samba. Такою базою є файл *smbpasswd*, який будується на основі записів файла */etc/passwd*ОС Linux.

Для створення облікового запису користувача сервера Sambaвикористовують команду *smbpasswd*,яка має такий формат:

smbpasswd -a <назва облікового запису користувача>

Якщо обліковий запис користувача використовують лише для роботи із сервером Samba, то для підвищення безпеки ОС Linuxадміністратор може заборонити використання командного інтерпретатора зазначеним обліковим записом.

Якщо в команді *smbpasswd*не вказати опцію -a, то результатом виконання буде зміна пароля для зазначеного облікового запису.

Сервер Sambaможе виконувати функції основного локального браузера (localmasterbrowser). Вказана функція передбачає визначення й оновлення списку комп'ютерів робочої групи, а також повідомлення його клієнтам. Для отримання адреси основного браузера комп'ютер під управлінням ОС Windowsнадсилає широкомовні повідомлення. Виявивши сервер, який виконує функції основного браузера, клієнт повідомляє йому дані про себе. Таким чином основний браузер завжди містить найновіші дані про членів

робочої групи.

Сервер Sambaнадає, можливості для створення розподілених мережних ресурсів. Синтаксис опису кожного з таких ресурсів має вигляд:

[docs]	#назва мережного ресурсу
path-/share	#маршрут до ресурсу у файловій системі OCLinux
comment	#опис ресурсу
browseable=yes	#чи є ресурс доступним для перегляду
writeable=yes	#чи є ресурс доступним для запису
validusers= st, st4	#список користувачів, яким дозволено доступ до ресурсу.

У наведеному прикладі створено мережний ресурс *docs,*який у файловій системі ОС Linuxрозміщений в каталозі */share.*До ресурсу встановлено режим читання та запису даних для облікових записів користувачів *st*і *st4.*

Створюючи розподілені ресурси у такий спосіб, адміністратор повинен враховувати й правила доступу до об’єктів файлової системи Ext3.

Для встановлення відповідності між правилами файлових систем NTFSта Ext3 у файлі *smb.conf*визначають параметр *security mask.* Тобто користувач ОС Windowsматиме змогу змінювати правила доступу до файлів і папок так, як в ОС Windows(див. п. 2.4). Значенням параметра є чотирицифрове число у вісімковій системі числення, яке визначає, які з правил доступу можна змінити. Наприклад, параметр *securitymask= 0600* дає можливість змінити правила читання та запису стосовно власника файла. Аналогічний параметр (*directory security mask*) існує стосовно каталогів.

Параметр *force security mode*дає можливість встановити правила доступу, що мають перевагу перед правилами користувача. Наприклад, якщо у секції *[docs]*вказано параметр *forcesecuritymode- 0440,* то змінюючи правила доступу до файлів ресурсу *docs,*користувач не зможе видалити правила для читання стосовно власника та групи.

Аналогічний параметр *{force directory security mode)*існує стосовно

каталогів.

Для автоматизації створення розподілених ресурсів для кожного користувача, зокрема у файлі *smb.conf,*передбачено секцію *[homes].* У цьому випадку користувач, що пройшов автентифікацію, отримує доступ до власної домашньої папки.

Після кожної зміни файла *smb.conf*потрібно виконувати перезапуск демонів *smb*і *nmb*за допомогою команди *letc/init.dlsmb restart*і *letc/init.dlnmb restart.*

Контрольні запитання

1. Які функції може виконувати сервер Samba?
2. Які демони входять до складу сервера Samba?
3. Який формат файла конфігурації сервера Samba?
4. Які існують механізми автентифікації користувачів сервера Samba?
5. Як створити обліковий запис користувача сервера Samba?
6. Як створити розподілений ресурс за допомогою сервера Samba?
7. Порівняйте правила доступу до мережних ресурсів ОС WindowsServer2003 і сервера Samba.
8. Як можна узгодити правила доступу файлів і папок ОС Linuxта ОС Windows, використовуючи сервер Samba?

6.2. Конфігурування сервера Samba для виконання функцій контролера домену

Наразі сервер Sambane може виконувати функції контролера домену на зразок служби ActiveDirectory. Проте в ньому реалізовано функціональність на рівні ОС WindowsNTServer. Де означає, що Sambane має деревовидної структури об’єктів, до якої можуть бути застосовані переваги поточного каталогу (застосування політик безпеки, делегувань тощо).

Для виконання сервером Sambafункції контролера домену до секції *[global]*файла *smb.conf*потрібно додати параметри з такими значеннями:

- ✓ *security= user*— для автентифікації потрібен логін і пароль;
- ✓ *domainmaster= yes*— сервер повинен бути головним переглядачем домену (відповідати за відображення комп'ютерів домену в мережному оточенні);
- ✓ *preferredmaster= yes* — сервер повинен брати участь у виборах головного браузера домену (робочої групи), поки він не переможе;
- ✓ *domain logons* =yes— дозвіл користувачам реєструватися в домені;
- ✓ *logonpath= <мережний маршрут>* — шлях до мережного каталогу, що містить профіль користувача.

Використовуючи параметр *logonpath,*можна сконфігурувати сервер Sambадля роботи з переміщуваними профілями. Оскільки зазначений параметр використовується один раз, а профіль для кожного користувача повинен бути окремим, то у файлі *smb.conf*передбачено використання змінних:

- ✓ %U— назва облікового запису користувача;
- ✓ %L— NetBIOSім'я сервера Samba;
- ✓ %m— NetBIOSкомп'ютера, з якого здійснено автентифікацію в домені.

Наприклад, значенням параметра *logon path*може бути: \\Srv*Profiles**%U*.Оскільки у процесі автентифікації користувача (наприклад, st) змінній %Uбуде надано значення (логін користувача (*st*)), то профіль буде скопійовано з його особистої папки *(\\Sru\Profiles\st*). Враховуючи формат мережного маршруту, приходимо до висновку, що для використання переміщуваних профілів у файлі *smb.conf*потрібна секція *[Profiles],*наприклад:

[Profiles]

path=/home/profiles

browseable = no

writeable= yes

Стосовно правил безпеки каталогу, який містить профілі користувачів варто зазначити, що до нього повинні мати право на запис усі користувачі

домену. Підкаталоги з профілями користувачів матимуть правила доступу лише для їхніх власників.

Для приєднання комп'ютера до домену, роль контролера в якому виконує сервер Samba, необхідно створити його обліковий запис. Оскільки база облікових записів сервера Sambaпобудована на основі файла */etc/passwd,*то необхідним є створення облікового запису комп'ютера в ОС Linux. Сервер Sambaвідрізняє облікові записи комп'ютерів від інших облікових записів завдяки символу «$». Наприклад, для створення облікових записів комп'ютерів *ws-403-01*та *ws-403-02*можна використати команди:

groupadd computers

useradd ws-403-01$ -g computers -s /bin/false -d /dev/null

useradd ws-403-02$ -g computers -s /bin/false -d /dev/null

Звертаємо увагу на те, що для підвищення безпеки системи для облікових записів комп'ютерів змінено командний інтерпретатор і домашній каталог.

Для того щоб додати створені облікові записи до бази даних Samba, необхідно виконати команду *smbpasswd,*наприклад:

smbpasswd -m ws-403-01

Опція *-m* у команді *smbpasswd*вказує на додавання комп'ютера, а отже, (на відміну від додавання облікового запису користувача) запит на введення та підтвердження пароля видано не буде.

Приєднання комп'ютерів, які працюють під управлінням ОС Windows, здійснюється аналогічно до приєднання їх у домен ActiveDirectory. Важливим є те, що зазначену операцію може виконати лише адміністратор домену, яким за замовчуванням є root. Додавання його облікового запису здійснюється за допомогою команди *smbpasswd.*

Контрольні запитання

1. Які параметри конфігураційного файла потрібно змінити для того, щоб сервер Sambaпочав виконувати функції контролера домену?

2. Який механізм автентифікації повинен бути задіяний, щоб Sambaпочав виконувати функції контролера домену?
3. Як створити обліковий запис користувача домену Samba?
4. Як створити обліковий запис комп'ютера домену Samba?
5. Як налаштувати сервер Sambaдля роботи з переміщуваними профілями користувачів?
6. Порівняйте можливості адміністрування доменів, контролерами яких є ОС WindowsServer2003 і сервер Samba.
7. Як можна узгодити правила доступу до файлів і папок ОС Linuxта ОС Windows, використовуючи сервер Samba?

7. Конфігурування клієнт-серверного програмного забезпечення

7.1. **Організація веб-сервера засобами MicrosoftInternet InformationService**(IIS)

Термін «веб-сервер»вживають у двох значеннях. У вузькому значенні веб-сервер — це набір програм, які забезпечують обмін даними засобами протоколу передавання гіпертексту (HTTP— HyperTextTransferProtocol).HTTP — протокол прикладного рівня моделі OSI, який є основою функціонування WordWideWeb (WWW). Основою WWWє гіпертекстові документи (веб-сторінки). Практично всі складові веб-сторінок (текст, графічні та мультимедійні об'єкти) можуть бути хіперпосиланнями, тобто вказувати на інші веб-сторінки. Кожне гіперпосилання містить універсальний вказівник ресурсу (URL— UniformResourceLocator). Синтаксис URLмає вигляд:

<протокол>://<сервер>:<порт>/<шлях>,

де

- ✓ протокол — протокол прикладного рівня; крім HTTP, в URLможуть бути вказані й інші протоколи (HTTPS, FTP, IRC, NNTP, NFSтощо);
- ✓ сервер — IPабо доменна адреса сервера, який надаватиме ресурс;
- ✓ порт — порт, з яким працює програма (сервер); шлях — маршрут розміщення файла.

Якщо сервер працює із стандартним (зарезервованим) номером порту, то його не вказують. Наприклад, стандартним номером порту для веб-серверів є номер 80.

Найбільш відомими серед програм-кліентів сервісу WWWe браузери. Після введення користувачем URLбраузер формує запит до веб-сервера. Наприклад, типовий запит браузера має вигляд:

GET./.HTTP/1.1

Accept:, image/gif,. image/xxbitmap,. image/jpeg,. image/pjpeg,. application/vnd.mspowerpoint,.

*application/vnd.ms-excel, .application/msword,. * /*

Accept -language: .en-us. .Accept-Encoding: .gzip,.deflate..

User-agent: .Mozilla!4.0.(compatible; .MSIE.7.0;. Windows. NT.5.2)

Host: www.mywebsite.com

Перший рядок вказує версію протоколу HTTP. Наступних три рядки описують типи графічних форматів і програмного забезпечення, роботу .і якими підтримує браузер. П'ятий рядок містить тип кодування даних, які будуть передані від сервера. Шостий рядок вказує тип, версію та сумісність програми-клієнта (браузера). Останній рядок містить назву веб-вузла, до якого надсилають запит.

У широкому розумінні під веб-сервером розуміють набір апаратних і програмних засобів, що забезпечують функціонування одного або кількох веб-вузлів (веб-сайтів) — сукупності взаємопов'язаних веб-сторінок, URLяких має спільне доменне ім'я (DNS-ім'я). Серед веб-серверів найбільш поширеними є Apachета MicrosoftInternetInformationServer.

InternetInformationServer (IIS) містить такі програмні складові:

- ✓ веб-сервер;
- ✓ сервер передавання електронної пошти (SMTP);
- ✓ FTP-сервер;
- ✓ сервер передавання груп новин (NNTP);
- ✓ диспетчер управління IIS— оснащення консолі MMC для конфігурування IIS;
- ✓ бібліотеки мови динамічного формування веб-сторінок (ASP— ActiveServerPages);
- ✓ серверні розширення Fronpage — компонент для публікування веб-сторінок за допомогою редактора Microsoft Fronpage;
- ✓ SSI (Server-SideIncludes) — зовнішні програмні модулі, які можуть бути використані при розробці веб-сторінок.

У процесі встановлення служб IISна системному диску створюється каталог Inetpub, у якому містяться підкаталоги з файлами відповідних складових IIS— *ftproot, mailroot, nntpfile, wwwroot.*

Конфігурування служб IIS проводять за допомогою відповідного оснащення MMC (рис. 7.1).

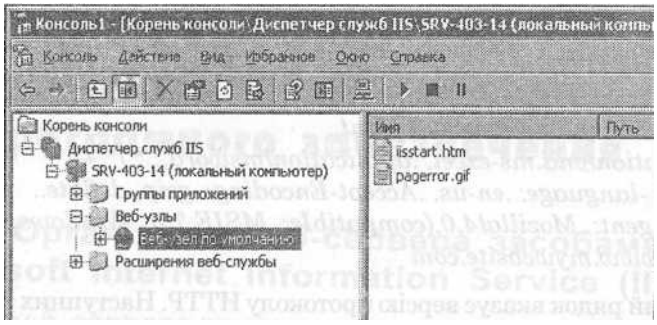


Рис. 7.1. Оснащення для адміністрування служб IIS

Після встановлення IISсеред його компонентів можна побачити веб-сайт за замовчуванням (DefaultWebSite). Використовуючи пункт меню *Дія (Action),*можна створити інший веб-сайт. Для того щоб користувачі могли звертатися до кожного веб-сайту, його ім'я повинно бути зареєстроване в доменній системі імен (DNS). За допомогою кнопок панелі інструментів консолі MMC можна зупиняти, запускати й призупиняти роботу окремих веб-сайтів. Вони подібні на кнопки відтворення, зупинки й паузи мультимедійного програвача. Стовпець *Стан (State)*у правій частині консолі MMC відображає один зі станів веб-сайту:

- ✓ працює (running);
- ✓ зупинений (stopped) — веб-сайт не обслуговує клієнтів і не відповідає на їхні запити;
- ✓ призупинений (paused) — веб-сайт не відповідає на нові запити. Процеси, завантажені до призупинення веб-сайту, виконуються, поки не завершать обслуговування поточних запитів. Зазначений стан використовують, якщо потрібно зупинити веб-сайт без несподіваного відключення клієнтів.

Загальні параметри кожного веб-сайту можна переглянути та змінити у вікні його властивостей на вкладці *Веб-вузол (WebSite)* (рис. 7.2).

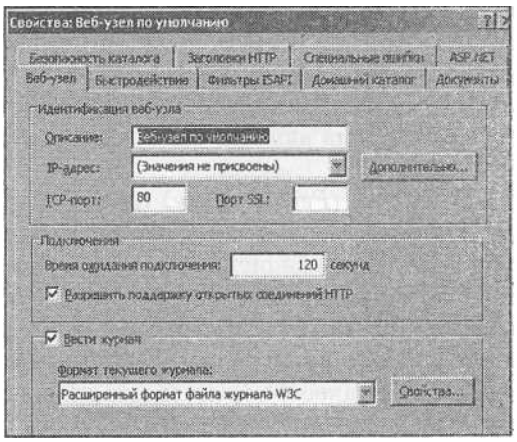


Рис. 7.2. Загальні параметри веб-вузла за замовчуванням

Рядок, що введено в поле *Опис (Description),*буде відображено лише в консолі MMC, а користувачі сайту побачити його не зможуть.

Окрім веб-сайту за замовчуванням IISнадає можливості для створення інших веб-сайтів, які ще називають віртуальними. Кожен з них повинен мати унікальний спосіб ідентифікації власного трафіку. Виділити веб-сайт з поміж інших можна, створивши унікальну комбінацію з трьох складових: IP-адреси вузла, номера порту або його заголовка. Саме останній рядок заголовка *(Host: www.mywebsite.com*) дає можливість створити віртуальні веб-вузли, які працюють з однією і тією ж IP-адресою та номером порту.

*Я*кщо в полі *IP-адреса (IP-address)*вказано *Значення не присвоєні (AllUnassigned),*то веб-сайт обслуговуватиме запити за будь-якою IP-адресою, яка не закріплена за іншим веб-вузлом.

Поле *TCP-port (TCP-port)*визначає номер порту, за яким веб-сайт обслуговуватиме запити. В цьому полі обов'язково потрібно вказувати незайнятий іншими сервісами номер порту.

Для передавання даних за криптованим протоколом SSL (SecureSocketsLayer) потрібно вказати номер порту SSL.

Параметр *Час очікування з'єднання (Connection Timeout) з* вкладки *Веб-вузол (Web Site)*задає час, протягом якого сервер підтримує відкрите з'єднання. Браузери використовують відкриті з'єднання для кількох запитів. Зазначена технологія забезпечує підвищення швидкості

передавання даних, оскільки ні серверу, ні клієнту не потрібно повторно встановлювати з'єднання для кожного запиту.

Кожен веб-сайт, що входить до складу IIS, надає можливості для ведення статистики (журналу), зокрема й реєстрації звертань клієнтів. Параметри функціонування журналу можна вказати в розділі *Вести журнал(Enablelogging)*(рис. 7.2). За допомогою кнопки властивостей із зазначеного розділу можна вказати розміщення журналу, а також деталізацію його ведення.

На вкладці *Швидкодія (Performance)*(рис. 7.3) можна вказати максимальну швидкість передавання *(Maximum Bandwidth)*даних веб-вузлом до клієнтів. Для конфігурування обмеження смуги пропускання потрібно встановити програму WindowsPacketScheduler. Крім цього, обмежуючи швидкість, системному адміністратору варто врахувати можливість доступу до сервера як з мережі Інтернет, так і з локальної мережі, швидкості передавання даних в яких можуть суттєво відрізнятися.

Вкладка *Швидкодія (Performance)*також надає змогу обмежити максимальну кількість одночасних з'єднань до веб-вузла.

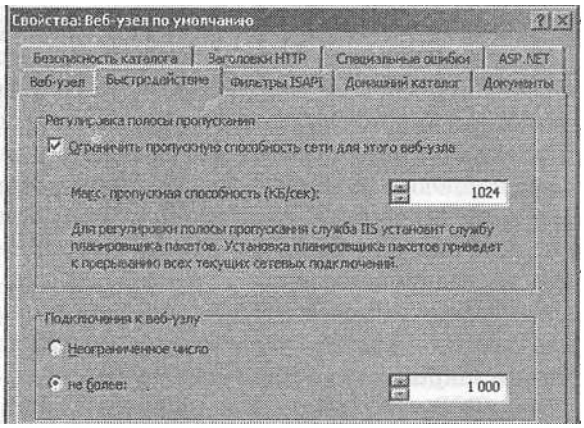


Рис. 7.3. Параметри швидкодії веб-вузла

На вкладці *Фільтри ISAPI (ISAPIFilters)*можна вказати програмні модулі, які сервер буде викликати для опрацювання певних типів файлів. Таким модулем, наприклад, є інтерпретатор мови PHP.

На вкладці *Домашній каталог (Home Directory)*вікна властивостей веб-сайту можна вказати папку розміщення його документів (рис. 7.4).

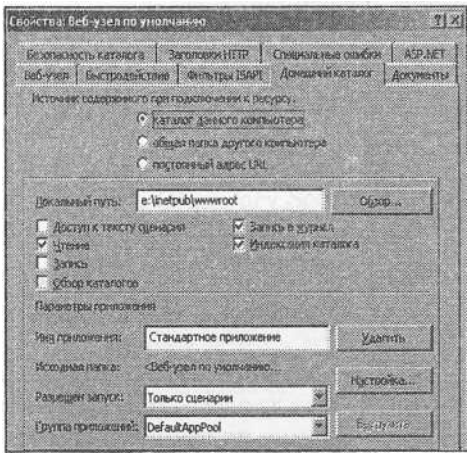


Рис. 7.4. Параметри домашнього каталогу веб-вузла

Місцем розміщення документів веб-сайту можуть бути:

- ✓ каталог на локальному диску веб-сервера;
- ✓ мережний каталог віддаленого комп’ютера;
- ✓ URL, тобто каталог або документ іншого веб-сервера.

У випадку використання мережного каталогу потрібно ввести мережний маршрут до нього, а також вказати обліковий запис користувача та пароль для авторизації.

IISнадає можливості обмеження доступу до домашнього каталогу веб-сайту. На вкладці *Домашній каталог (HomeDirectory)*можна встановити такі режими доступу (рис. 7.4):

- ✓ *Доступ до тексту сценарію (ScriptSourceAccess)*— клієнти отримують доступ до вихідних кодів сценаріїв, написаних мовою ASP. Оскільки такі сценарії виконуються на сервері, то така можливість є потенційною небезпекою для системи;
- ✓ *Читання (Read)*— оскільки передавання даних за протоколом HTTPпередбачає їх зчитування з домашнього каталогу, то даний режим доступу є обов’язковим;
- ✓ *Запис (Write)*забезпечує можливість запису даних на сервер. Такий режим також є потенційною небезпекою для системи. Особливо небезпечним є його ввімкнення у поєднанні з режимом читання, оскільки зловмисник матиме змогу не лише завантажити власний скрипт на сервер, а й виконати його;

- ✓ *Перегляд каталогів (Directory Browsing)*— користувач, при звертанні до каталогу, матиме змогу переглянути його вміст. Проте якщо в каталозі існуватиме документ за замовчуванням (так званий індексний документ), то його буде передано клієнтові, а вміст каталогу відображено не буде;
- ✓ *Запис у журнал (LogVisits)*— якщо в IISувімкнено режим ведення статистики, то всі звертання до каталогу будуть записані в журнал;
- ✓ *Індексація каталогу (IndexThisResource)*— каталог буде проіндексовано за допомогою сервісу індексування*(MicrosoftIndexingService).*

У секції *Параметри програм (Application Settings)*конфігурують параметри програмних засобів для визначення меж їх функціонування, що забезпечує відокремлення програмних засобів один від одного. Детальніше про налаштування параметрів програм можна прочитати у [11, с. 57-65].

На вкладці *Документи (Documents)*(рис. 7.5) визначають файли, які завантажують при звертанні до каталогу (тобто якщо в рядку URLне вказано файл). Пошук документів у каталозі здійснюватиметься у тому порядку, в якому вони вказані.

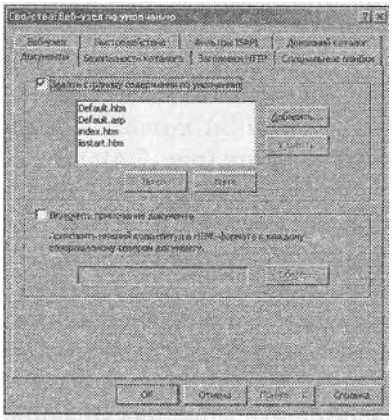


Рис. 7.5. Параметри документів веб-вузла

Наприклад, якщо серед таких документів вказано *index.htm,*то при звертанні за URL*http://srv.com/docs/*веб-сервер *srv.com*передасть файл *index.htm з* каталогу *docs.*Якщо ж такого файлу в папці *docs*виявлено не буде, то залежно від налаштувань сервера буде передано вміст каталогу або

повідомлення про помилку.

Крім документів за замовчуванням на вкладці *Документи (Documents)*можна вказати нижній колонтитул, який буде додано до кожної веб-сторінки сайту.

Для конфігурування параметрів безпеки веб-сайту використовують вкладку *Безпека каталогу(Directory Security*) (рис. 7.6).

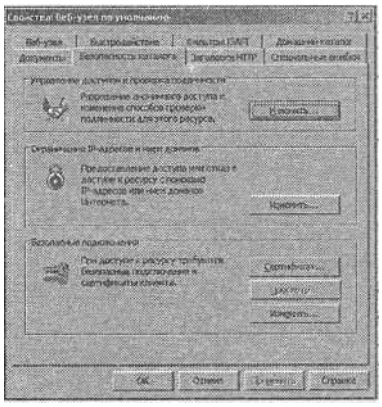


Рис. 7.6. Параметри безпеки веб-вузла

Оскільки функціонування компонентів веб-сервера в складі IISрозглядають з точки зору безпеки, то потрібен обліковий запис, з повноваженнями якого працюватиме веб-вузол. IISдодає два записи користувачів до бази даних облікових записів ОС WindowsServer2003. Обліковий запис *IUSR_<назвасервера>* забезпечує анонімний доступ до веб-сайту. Такий користувач за замовчуванням є членом групи *Гості (Guests).*

Обліковий запис *IWAM_<назва сервера>* використовують для запуску процесів веб-сервером. Цей обліковий запис має права мережної служби. Процеси, що завантажені з привілеями мережної служби, здійснюють доступ до веб-сервера так, немов вони перебувають поза сервером, а тому не мають безпосереднього доступу до операційної системи.

Для зміни параметрів автентифікації та контролю доступу до сайту потрібно використовувати кнопку *Редагувати (Edit).*У вікні, яке відкриється, можна змінити методи автентифікації (рис. 7.7).

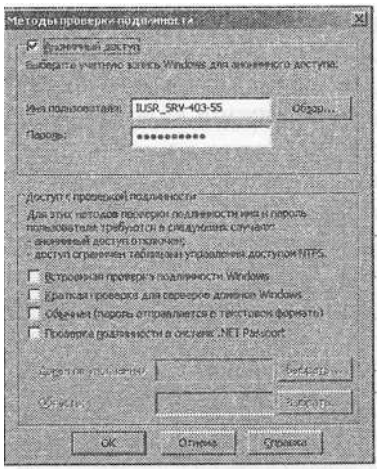


Рис. 7.7. Параметри автентифікації веб-вузла

Якщо ввімкнено режим анонімного доступу, то користувачі отримуватимуть доступ до веб-вузла без введення реєстраційних даних. Доступ до файлової системи веб-сервера здійснюватиметься від імені користувача *IUSR_<Назва сервера>*. У зв'язку з цим потрібно надати його обліковому запису відповідні права доступу до файлової системи NTFS.

- ✓ Секція*Доступ з перевіркою достовірності (AuthenticatedAccess)* відображає доступні типи автентифікації:
- ✓ інтегрована автентифікація Windows, при якій використовують дані облікового запису користувача, а для їх передавання використовують відомі протоколи Kerberosабо NTLM;
- ✓ спрощена автентифікація для серверів доменів Windowsдоступна при використанні облікових записів ActiveDirectory, а перевірка здійснюється за протоколом HTTP;
- ✓ звичайна автентифікація — логін і пароль сервер та клієнт передають у відкритому вигляді (без криптування);
- ✓ автентифікація на основі паспорта .NETPassportдає можливість використовувати одноразовий вхід на декілька сайтів, що підтримують технологію паспортів .NET.

До параметрів безпеки також належить обмеження доступу до веб-сайту на основі IP-адрес клієнтів. При цьому необхідно визначити (рис. 7.8):

- ✓ режим доступу (дозвіл або заборона);
- ✓ IP-адреси комп’ютерів, підмереж або доменні імена, які є винятками стосовно обраного режиму доступу.

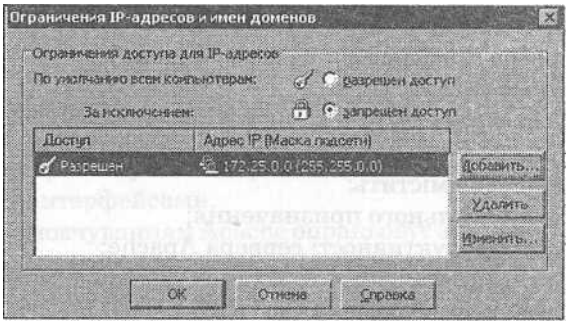


Рис. 7.8. Обмеження доступу до веб-вузла на основі адрес клієнтів

Варто зазначити, що надання доступу на основі доменного імені здійснюється у зонах зворотного пошуку служби DNS. Оскільки такий пошук вимагає певного часу, то швидкість опрацювання запитів веб-сервером зменшується.

Контрольні запитання

- ✓ Як Ви розумієте терміни: веб-сервер, веб-браузер, веб-вузол, URL?
- ✓ Опишіть процес передавання даних за протоколом HTTP.
- ✓ Чи можна вважати IISвеб-сервером?
- ✓ Як переглянути журнал статистики веб-вузла?
- ✓ Які режими доступу до каталогів веб-вузла передбачено в IIS?
- ✓ Як Ви розумієте термін документ за замовчуванням (індексний документ)?
- ✓ У який спосіб в IISрозв’язують проблеми безпеки веб-сервера?
- ✓ Як організувати авторизацію користувача до окремого каталогу засобами IIS?

7.2. Конфігурування веб-сервера Apache

Сучасні дистрибутиви ОС Linuxдля організації веб-сервера пропонують Apache. Проте існують версії Apacheй для інших ОС, зокрема й для ОС Windows. Налаштування сервера здійснюється шляхом редагування файлів конфігурації, основним з яких є *httpd.conf (apache.conf).*У ОС Linuxзазначені файли розміщені в каталозі /*etc/httpd (/etc/apache).*Після кожної зміни файла *httpd.conf*потрібно виконувати перезапуск сервера Apacheза допомогою команди */etc/init.d/httpdrestart*або */etc/init.d/apacherestart.*

Рядки файла *httpd.conf,*що починаються із символу #, містять коментарі. Подібно до вікна властивостей веб-вузла IISконфігураційний файл сервера Apacheмістить:

- ✓ директиви загального призначення;
- ✓ параметри продуктивності сервера Apache;
- ✓ директиви відображення та доступу до папок сервера;
- ✓ параметри ведення журналів;
- ✓ директиви опрацювання помилок;
- ✓ директиви створення віртуальних веб-вузлів.

Розглянемо найважливіші опції загального призначення.

ServerName— задає ім’я сервера.

Наприклад,*ServerNamesrv-403-01.fizmat.tnpu.edu.ua.*

Зазначимо, що ім’я сервера, до якого потрібно звернутися із за$_т$питом, заздалегідь повинно бути зареєстроване в службі доменних імен (DNS).

*ServerAdmin*визначає поштову адресу адміністратора сервера, яку буде виведено в повідомленнях про помилку.

*Port*вказує серверу Apacheпорт, який повинен використовуватися для взаємодії з клієнтами. За замовчуванням використовується порт 80.

*User*і *Group*визначають ідентифікатори облікових записів користувача та групи, від імені яких працюватиме веб-сервер. Зазвичай сервер завантажують із застосуванням окремо створеного облікового запису

apache.

ServerRoot— директива, що задає каталог, який використовується для зберігання конфігураційних файлів Apache. Оскільки програма встановлення коректно задає цей параметр, то змінювати його не варто.

DocumentRoot—директива, що визначає папку збереження документів веб-сервера. Значення директиви *DocumentRoot*не варто завершувати косою рискою, оскільки це може призвести до виникнення помилки.

Наприклад, якщо директива визначає *DocumentRoot/var/www/ wwwroot,*то при звертанні клієнта за URL*http://srv-403-01.fizmat.tnpu.edu.ua/doc.html*веб-сервер передасть файл*doc.html*з каталогу/*var/www/wwwroot.*

*BindAddress.*Якщо сервер, на якому встановлено сервер Apache, містить кілька мережних інтерфейсів, то за допомогою цієї директиви можна організувати роботу сервера лише з одним із них. За замовчуванням використовується директива *BindAddress* *, що відповідає роботі з усіма інтерфейсами.

*Listen*за замовчуванням Apacheопрацьовує звернення до мережних інтерфейсів з використанням порту 80. Зазначена директива дає змогу обмежити звертання до сервера за мережними інтерфейсами та портами. Наприклад, директива *Listen172.25.3.1:8080* визначає, що сервер працюватиме з інтерфейсом з адресою 172.25.3.1 і портом 8080.

Розглянемо параметри продуктивності веб-сервера Apache.

*MinSpareServers MaxSpareServers.*Для більш ефективного опрацювання запитів клієнтів ОС Linuxзавантажує кілька копій демона Apache. Кожен екземпляр опрацьовує окремий запит. Якщо кількість дочірніх процесів є менша за *MinSpareServers*і вони не виконують опрацювання запитів, то у випадку надходження нових запитів ОС завантажуватиме нові процеси. Аналогічно, якщо число копій Apacheбільше за *MaxSpareServers,*то нові копії демона не буде завантажено. За замовчуванням значення *MinSpareServers*і *MaxSpareServers*дорівнюють 5 і

10 відповідно. У випадку незначного навантаження на сервер ці значення можна зменшити.

*StartServers*визначає кількість копій демона Apache, які буде створено при завантаженні сервера.

*MaxClients*задає максимальну кількість одночасних з'єднань із сервером. Значення *MaxClients*не дорівнює максимальній кількості браузерів клієнтів, оскільки в межах однієї веб-сторінки може бути створено кілька з'єднань із сервером.

Timeout— проміжок часу в секундах, протягом якого сервер продовжує спроби відновлення призупиненої передачі даних.

*Keep Alive*дозволяє або забороняє постійні з'єднання, в межах яких клієнт може надсилати серверу кілька запитів.

KeepAliveTimeOut— час в секундах, протягом якого сервер очікує наступний запит у межах постійного з'єднання.

Директиви налаштувань доступу до папок веб-сервера Apache:

для переадресації запитів на інші файли або папки використовують директиву *Redirect,*формат якої такий:

Redirect<папка чи файл><шлях переадресації>.

Наприклад,*Redirect limages http://srv2.org.uaHm*

Alias— директива, що надає доступ до папок, які містяться за межами кореневого, каталогу документів (директива *DocumentRoot*) та його підкаталогів.

*Directoryindex.*Деякі посилання (URL) не містять назви файла; в них зазначене лише ім'я папки. Коли сервер Apache одержує подібний URL, він спочатку намагається знайти файл індексу, який задається даною директивою. За замовчуванням приймається назва файлу *index.html.* Якщо задано кілька файлів індексу, Apache по черзі здійснює їх пошук відповідно до вказаної послідовності. Якщо файл індексу не заданий, то сервер повертає залежно від налаштувань вміст папки або повідомлення про помилку.

Для налаштування параметрів окремих папок застосовують багато-рядкові директиви, синтаксис опису яких такий:

<Directory <назва каталогу» параметри

</Directory>

У директиві*<Directory>...</Directory>*використовують параметри*Options, AllowOverride.*

Параметр *Options*може набувати таких значень:

- ✓ *None*— у каталозі заборонено використовувати додаткові функції сервера;
- ✓ *ExecCGI*— дозволено виконання сценаріїв CGI;
- ✓ *FollowSy mLinks*— дозволено перехід за символьними посиланнями;
- ✓ *Includes*— дозволено включення вставок програмного коду з боку сервера;
- ✓ *Indexes*— дозволено виведення вмісту каталогу, за умови, що в ньому не виявлено файла індексу;
- ✓ *SymLinksIfOwnerMatch*— дозволено перехід за символьними посиланнями у випадку, якщо папка призначення належить тому самому користувачеві, що й саме посилання;
- ✓ *All*— у папці дозволено всі наведені вище функції.

Наприклад, для виведення вмісту папки */var/www/docs*у директиві *<Directory>*потрібно вказати параметр індексування *Indexes.*

<Directory "/var/www/docs">

Options Indexes

</Directory>

Для визначення параметрів доступу в кожній папці може бути використано файл *.htaccess,*який може містити всі ті самі опції, що й директива *<Directory>*.З метою уникнення конфліктів між параметрами, вказаними в конфігураційному файлі та у файлі *.htaccess,* у кожній секції *Directory*файла *httpd.conf*можна вказати параметр *AllowOverride,*який визначає клас інших параметрів, що можуть використовуватися у файлах

.htaccess.

Значеннями параметра *AllowOverride*можуть бути:

- ✓ *All*— у файлах *.htaccess*можуть використовуватись усі директиви;
- ✓ *AuthConfig*— дозволяється використання директив, які управляють автентифікацією;
- ✓ *Fileinfo*— дозволяється використання директив типів файлів;
- ✓ *Indexes*— дозволяється використання директив, пов'язаних з індексуванням;*Limit*— дозволяється використання директив, пов'язаних із захистом папок;
- ✓ *Options*— дозволяється використання директив *Option;*
- ✓ *None*— не дозволяється використання файлів *.htaccess.*

У файлі *.htaccess*може бути проведена авторизація на рівні IP-адрес чи доменних імен.

Наприклад, якщо необхідно надати доступ до каталогу */var/www/docs*лише комп'ютерам з підмережі 172.25.0.0/255.255.0.0, то до конфігураційного файла *http.conf*потрібно додати директиву:

<Directory /var/www/docs >

AllowOverride AuthConfig

</Directory>

Файл *.htaccess,*який міститься у папці */uar/www/docs,*повинен мати вигляд:

allow from172.25.0.0/255.255.0.0 deny from all order deny,allow

Останній рядок файла *.htaccess*визначає порядок застосування директив дозволу *(allow)*та заборони *(deny).*

У файлі *.htaccess*може бути проведена авторизація на рівні користувачів чи їх груп.

Приклад файла *.htaccess:*

AuthType Basic

Auth User File l/tc/httpd/users.passwd AuthName "Введіть ім'я і пароль " require valid-user

У першому рядку вказано тип авторизації — стандартний для ОС, другий рядок задає файл користувачів і паролів, третій рядок — підказку. Останній рядок задає правила доступу: доступ до папки матимуть усі користувачі, вказані у файлі *htusers.*Правила доступу можуть бути задані й іншими директивами:

- ✓ *requireuserкористувач1 користувач2...* —надає доступ перерахованим користувачам;
- ✓ *requiregroupгрупа1 група2 ...* — надає доступ перерахованим групам користувачів.

Файл *users.passwd*можна створити за допомогою утиліти *htpasswd.* Для створення файла паролів потрібно виконати команду з такими параметрами:

htpasswdusers.passwdwebmaster,

де

users.passwd— файл з паролями, *webmaster*— ім'я користувача. Крім цього, у файлі *.htaccess*або у файлі *httpd.conf*у межах секції <*Directory*>вказують директиви:

- ✓ *Order*— зазначення послідовності застосування правил доступу до папки *(Orderallow, deny)*-,
- ✓ *Allow* — визначення правил дозволу; після директиви потрібно вказати слово *from,*за яким можна вказати IP-адресу комп'ютера чи мережі або DNS-ім'я; слово *all*визначає усі комп'ютери;
- ✓ *Deny*— визначення правил заборони; синтаксис директиви аналогічний директиві *Allow.*

Подібними до директив <*Directory*>е директиви <*Files*>,які застосовують для управління доступом до файлів.

Приклад. Заборонити доступ засобами веб-сервера до файлів *Jitaccess*можна за допомогою директиви:

<*Files «.htaccess»*>

Order allow,deny Deny from all

</Files>

Параметри ведення журналів визначають дані, які потрібно записувати в журнали статистики.

*HostnameLookups.*Якщо значення параметра дорівнює *on,*то до журналу буде записано доменне ім'я комп'ютера клієнта. Якщо ж значення дорівнює *off*, то в журналі реєструватимуться IP-адреси клієнтів.

*ErrorLog*і *TransferLog*— директиви, які визначають файли журналів сервера Apache. Журнал *ErrorLog*містить діагностичні записи, а також повідомлення про помилки. До журналу *TransferLog*вносять запити клієнтів.

ErrorDocument— директива на співставлення кодів помилок Apachei URL-адрес цього сервера.

Наприклад,

ErrorDocument404 /missing.html

Наведена директива визначає, що при звертанні до неіснуючого ресурсу, сервер передасть клієнту веб-документ *missing.html.*

Для налаштування віртуальних вузлів засобами сервера Apacheвикористовують методи:

- ✓ для кожного вузла виділяють окрему IP-адресу;
- ✓ використовують одну IP-адресу для всіх вузлів.

Підтримка віртуальних веб-вузлів забезпечується використанням директив <*VirtualHost*>і <*NameVirtualHost*>.

Якщо ОС сервера мас лише одну IP-адресу, то її потрібно вказати в директиві <*NameVirtualHost*>,наприклад, <*NameVirtualHost 172.25.3.1*>.

У випадку наявності двох IP-адрес, одну з них можна присвоїти основному серверу (директива *Bindaddress),*а іншу — віртуальному.

Директива <*VirtualHost*>визначає параметри віртуального веб-вузла. Синтаксис директиви такий:

<VirtualHost IP-адреса сервера [:порт]>... </VirtualHost>

Основними параметрами директиви є:

- ✓ *DocumentRoot*— коренева папка документів;
- ✓ *ServerName*— ім’я вузла;
- ✓ *ServerAdmin*— адреса електронної пошти адміністратора вузла;
- ✓ *ErrorLog*— файл журналу помилок—звертань до вузла;
- ✓ *CustomLog*— файл журналу звертань до вузла.

У директиві <*VirtualHost*>замість IP-адреси можна використовувати символ «*», який визначає використання значень основного сервера.

Крім цього в директиві можуть бути визначені й інші параметри: / обробка сценаріїв;

- ✓ визначення параметрів індексування папок;
- ✓ управління доступом та авторизація.

У випадку використання однієї IP-адреси для всіх вузлів ім’я вузла має бути зареєстровано за допомогою сервера доменних імен DNS.

Приклад. Опишемо віртуальний веб-вузол *site.org.ua,*який опрацьовуватиме запити за номером порту 8080.

*<VirtualHost *:8080>*

ServerAdmin webmaster@site.org.ua

DocumentRoot /var/www/vhosts/site

ServerName site.org.ua

ErrorLog logs/site.org.ua-error_log

</VirtualHost>

Залежно від дистрибутиву OCLinux або версії сервера Apache конфігурація віртуальних веб-вузлів може бути описана або у файлі *httpd.conf,*або в окремому файлі, наприклад, *vhosts.conf.*

Контрольні запитання

1. У який спосіб здійснюють конфігурування сервера Apache?
2. Які групи директив можна виділити у файлі *httpd.conf*?
3. Що відбудеться, якщо в каталозі, до якого звертається користувач, не виявлено файла індексу?

4. Як переглянути журнал статистики веб-сервера (веб-вузла)?
5. Які існують способи встановлення параметрів папок веб-сервера?
6. Як організувати авторизацію користувача до окремого каталогу засобами Apache?
7. Порівняйте основні параметри конфігурації сервера Apacheта веб-вузлів у складі MicrosoftInternetInformationService.

7.3. Організація сервера передавання файлів засобами MicrosoftInternetInformationService(ISS)

Сервер передавання файлів (FTP-сервер)— це набір програм, які забезпечують обмін даними засобами протоколу передавання файлів (FTP— FileTransferProtocol).FTP — один із найстаріших протоколів прикладного рівня моделі OSLПротокол FTPдає можливість клієнту обмінюватися двійковими і текстовими файлами з сервером, що підтримує протокол FTP. Установивши зв'язок із сервером, клієнт може скопіювати файл із віддаленого комп'ютера на свій або скопіювати файл зі свого комп'ютера на віддалений. Сучасні браузери є не лише програмами-клієнтами сервісу WWW, а й сервісу FTP.

При розгляді FTPяк сервісу Інтернет мають на увазі не просто протокол, а саме сервіс, який забезпечує доступ до файлів. Подібно до протоколу передавання гіпертексту для кожного файла, який розміщено на FTP-сервері, можна вказати універсальний вказівник ресурсу (URL). Наведемо приклад такого URL:

ftp://ftp.somehost.ua/pub/images.zip,

де

- ✓ *ftp*— протокол передавання файлів;
- ✓ *ftp.somehost.ua*— доменна адреса сервера (також можна вказувати IP-адресу);
- ✓ *pub*— каталог розміщення файла;
- ✓ *images.zip***— *файл.***

У наведеному прикладі після доменної адреси сервера не вказано номер порту, оскільки він є стандартним. Взагалі кажучи, FTP-сервер працює з двома портами.

Розглянемо схему передавання даних за протоколом FTP.

- ✓ Клієнт створює з'єднання із сервером.
- ✓ Сервер проводить автентифікацію клієнта.
- ✓ Сервер виконує команди клієнта (наприклад, рухається деревом каталогів веб-сервера, переглядає папки).
- ✓ Клієнт копіює файли із сервера або завантажує власні файли на сервер.
- ✓ Клієнт завершує сеанс роботи.

Для створення і завершення з'єднання, автентифікації, отримання команд клієнта сервер використовує порт (зазвичай 21). Для завантаження файлів передбачено окремий порт (зазвичай 20). Передаючи дані через порт з номером 20, сервер встановлює з'єднання на певний порт клієнта. Такий режим роботи FTP-сервера називають активним. Як відомо в мережі Інтернет зазвичай між клієнтом і сервером працюють NAT-перетворювачі абопроксі-сервери, які змінюють IP-адресу клієнта. Враховуючи це, порт, відкритий клієнтом, не буде доступним для FfP-сервера. Для розв'язання цієї проблеми FTP-сервери крім активного режиму використовують також і пасивний. Передаючи файли в пасивному режимі, FTP-сервер відкриває власний додатковий порт (як правило непривілейований). Саме через цей додатковий порт клієнт копіює дані з сервера та завантажує їх на сервер.

Доволі часто FTP-сервер конфігурують так, щоб з'єднатися з ним можна було не тільки за допомогою логіну та пароля облікового запису користувача ОС, але й за допомогою загальнодоступного імені *anonymous*(анонім). У цьому випадку для користувача стає доступною не вся файлова система сервера, а лише деяка її частина, яка складає вміст публічного каталогу. Отже, для надання у вільне користування файлів у

локальній мережі та мережі Інтернет, потрібно налаштувати FTP-сервер для роботи в анонімному режимі.

Після встановлення IISсеред його компонентів можна побачити FTP-вузол за замовчуванням (DefaultFTPSite). Використовуючи пункт меню *Дія (Action),*можна створити інший FTP-вузол. Для того щоб користувачі могли звертатися до FTP-вузла, його ім'я повинно бути зареєстроване в доменній системі імен (DNS). За допомогою кнопок панелі інструментів консолі MMC можна зупиняти, запускати й призупиняти роботу окремих FTP-вузлів. Завантаження, зупинення та призупинення функціонування FTP-вузлів здійснюється так само, як і веб-сайтів.

Загальні параметри кожного веб-сайту можна переглянути та змінити у вікні його властивостей на вкладці *FTP-вузол (FTPSite)* (рис. 7.9).

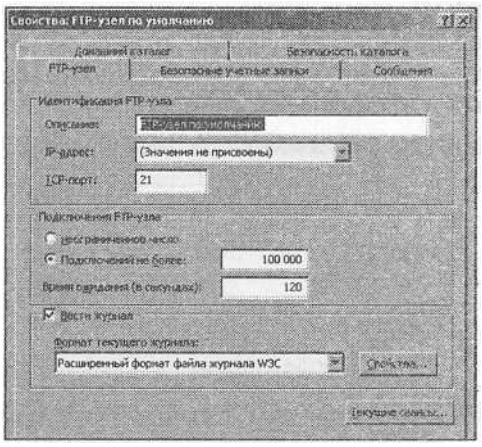


Рис. 7.9. Загальні параметри FTP-вузла за замовчуванням

Рядок, що введено в поле *Опис (Description),* буде відображено лише в консолі MMC, а користувачі сайту побачити його не зможуть. Для створення інших FTP-вузлів кожен з них повинен мати унікальний спосіб ідентифікації власного трафіку. Виділити FTP-сайт з-поміж інших можна за допомогою унікальної комбінації з IP-адрєси вузла і номера порту. Отже, на відміну від протоколу HTTP, створити кілька FTP-вузлів, які використовуватимуть ту саму IP-адресу та номер порту, неможливо.

Поле *IP-адреса (IP-address)*призначено для введення IP-адреси, за якою FTP-вузол буде очікувати з'єднання. Якщо вказано *Значення не присвоєні (All Unassigned),*то FTP-сайт обслуговуватиме запити за будь-

якою IP-адресою, яка не закріплена за іншим вузлом.

Поле *TCP-port (TCP-port)*визначає номер порту, за яким FTP-вузол обслуговуватиме запити (створення і завершення з'єднання, автентифікація, отримання команд клієнта). Якщо замість стандартного номера 21 введено інший номер, то його потрібно додати і в URL.

Наприклад, *ftp:llftp.someserver.ua:2121l*

У секції *З'єднання FTP-вузла (FTPsite connection)*можна вказати максимальну кількість одночасних з'єднань, а також час очікування, після завершення якого сервер завершить сеанс неактивного клієнта.

Параметри функціонування журналу FTP-вузла можна вказати в розділі *Вести журнал (Enablelogging).*За допомогою кнопки *Властивості (Properties)*можна вказати розміщення журналу, а також особливості його ведення.

Використовуючи кнопку *Поточні сеанси (Current sessions)*(рис. 7.10) можна переглянути відкриті сесії користувачів.

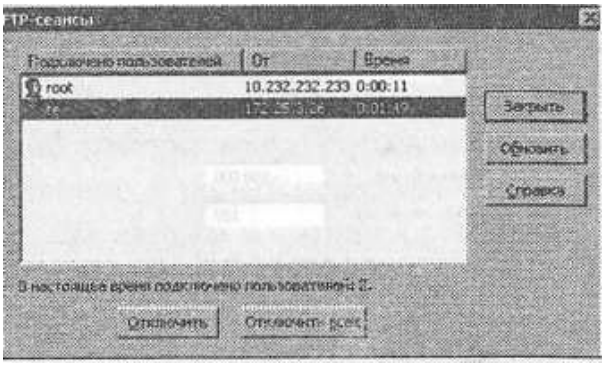


Рис. 7.10. Відкриті сесії користувачів FTP-вузла

Використовуючи вкладку *Безпечні облікові записи (Security Accounts)*(рис. 7.11), можна вказати ім'я облікового запису, за допомогою якого здійснюватиметься анонімний доступ до об'єктів файлової системи. Подібно до веб-сервера в складі IIStаким обліковим записом є **IUSR_<назва***сервера*>.

Якщо режим анонімного доступу вимкнути, то із сервером зможуть працювати тільки зареєстровані в системі користувачі. Оскільки протокол FTPне передбачає криптування даних, то автентифікація користувачів є

потенційно небезпечною. У зв'язку з цим на вкладці *Безпечні облікові записи (Security Accounts)*передбачено можливість використання лише публічного доступу.

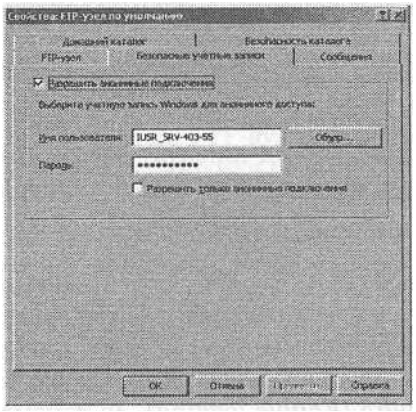


Рис. 7.11. Параметри облікових записів користувачів FTP-вузла

На вкладці *Повідомлення (Messages)* вказують повідомлення, які будуть виведені у процесі реєстрації користувача, при завершенні сеансу, у випадку перевищення максимальної кількості одночасних сесій.

На вкладці *Домашній каталог (Home Directory)*вікна властивостей FTP-вузла можна вказати папку розміщення його документів (рис. 7.12).

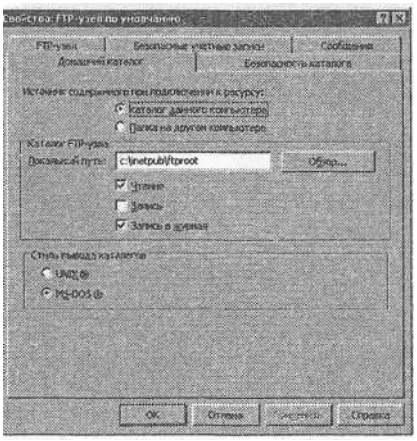


Рис. 7.12. Параметри домашнього каталогу FTP-вузла

Місцем розміщення документів веб-сайту можуть бути:

- ✓ каталог на локальному диску веб-сервера;
- ✓ мережний каталог від даленого комп'ютера.

IISнадає можливості обмеження доступу до домашнього каталогу веб-сайту. На вкладці *Домашній каталог (HomeDirectory)*можна встановити такі режими доступу (рис. 7.12):

- ✓ *Читання (Read)*— передбачає перегляд вмісту каталогів і файлів, а також їх копіювання із сервера;
- ✓ *Запис (Write)*— забезпечує можливість запису даних на сервер;
- ✓ *Запис у журнал (LogVisits)*— якщо в IISувімкнено режим ведення статистики, то всі звертання до каталогу будуть записані в журнал.

Як і у випадку використання веб-сервера, IISнадає можливість обмежити доступ до FTP-вузла на основі IP-адрес клієнтів. При цьому потрібно визначити (рис. 7.13):

- ✓ режим доступу (дозвіл або заборона);
- ✓ XP-адреси комп'ютерів або підмереж, які є винятками стосовно обраного режиму доступу.

Наприклад, встановивши параметри, зображені на рис. 7.13, ми надаємо доступ до БТР-сервера клієнту з IP-адресою 172.25.3.254. Усім іншим комп'ютерам доступ буде заборонено.

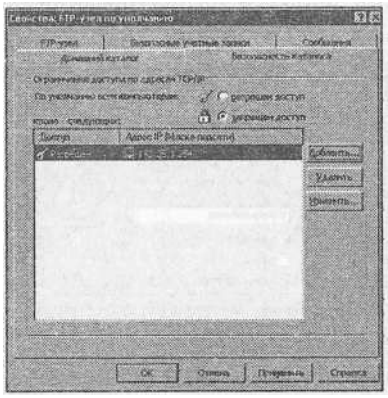


Рис. 7.13. Обмеження доступу до веб-вузла на основі IP-адрес клієнтів

Контрольні запитання

1. Як Ви розумієте терміни: FTP-сервер, FTP-вузол?
2. Опишіть процес передавання даних за протоколом FTP.
3. Які режими роботи FTP-сервера Вам відомі? У чому полягає відмінність між ними?
4. Як переглянути журнал статистики FTP-вузла?
5. Які режими доступу до каталогів FTP-вузла передбачено в IIS?

6. Як налаштувати публічний FTP-вузол засобами IIS?

7.3. Конфігурування FTP-сервера ProFTPD

Сучасні дистрибутиви ОС Linuxдля організації FTP-сервера пропонують різні програмні засоби. З-поміж них нами обрано сервер ProFTPD. Налаштування сервера здійснюється шляхом редагування файла конфігурації */etc/proftpd/proftpd.conf*.Після кожної зміни цього файла потрібно виконувати перезапуск сервера за допомогою команди */etc/init.d/proftpd restart.*

Рядки файла *proftpd.conf*, що починаються із символу #, містять коментарі. У таблиці 7.1 наведено основні директиви файла конфігурації сервера ProFTPD.

Таблиця 7.1. Директиви файла proftpd.conf

Директива	**Можливі**	**Опис**
ServerName	*FTP-server*	Назва сервера, яка буде відображена у процесі встановлення з'єднання
ServerType	*standalone* *inetd*	Спосіб завантаження сервера, *standalone*— окремий демон, інший спосіб завантаження за допомогою сервера *inet.d*
Port	*21*	Номер порту для виконання команд
Timeout Session	*86400*	Максимальна тривалість сесії в секундах
Timeoutldle	*1800*	Максимальний час не активності клієнта в секундах
TimeoutLogin	*1200*	Максимальна тривалість авторизації
TimeoutNoTransfer	*3600*	Максимальна тривалість сесії без передавання даних
MaxInstances	*30*	Максимальна кількість процесів сервера, що одночасно працюють в режимі *standalone*
AccessGrantMsg	*Access granted*	Повідомлення, яке буде виведено при успішній автентифікації
AccessDenyMsg	*Access denied*	Повідомлення, яке буде виведено при невдалій автентифікації
ServerAdmin	*ftp@sru.com*	Адреса email адміністратора сервера

AllowForeignAddress	*on| off*	Дозвіл на передавання даних з одного FTP-сервера на інший
AllowOverride	*on |off*	Дозвіл для зміни параметрів у файлах *.ftaccess*
AllowOverwrite	*on |off*	Можливість перезапису файлів
DefauitRoot	*/* *~*	Каталог, який буде кореневим для клієнта (значення ~ означає домашній каталог клієнта)
User	*nobody*	Обліковий запис користувача та групи для завантаження сервера
Group	*nobody*	
RequireValidShell	*on* *off*	У процесі авторизації обов'язкова наявність командного інтерпретатора
AnonRequirePassword	*on* *off*	Дозвіл на авторизацію публічного користувача без пароля
User Alias anonymous	*ftp*	Псевдонім анонімного користувача
MaxClients	*10*	Максимальна кількість одночасних авторизацій публічних користувачів
SystemLog	*/var/log/ proftpd.log*	Шлях до системного журналу
TransferLog	*/var/log/ ftpdtransfer.log*	Шлях до журналу передавання даних
SyslogLeuel	*notice | error | debug | warn*	Рівень деталізації записів до журналу сервера
Umask	*022*	Права доступу для створених файлів
AuthOrder	*mod_auth_ unix.c*	Модулі, які будуть застосовані для автентифікації користувачів

Подібно до веб-сервера Apache, для опису властивостей каталогів сервера ProFTPDпередбачено багаторядкові (блокові) директиви *<Directory>... <!Directory>*.Якщо необхідно змінити правила доступу до каталогу, то використовують директиви *<Limit>... <!Limit>*.

Наприклад,

```
<Directory incoming>
    <Limit WRITE>
    AllowAll
    </Limit>
    <Limit READ>
        Deny All
    </Limit>
</Directory>
```

У наведеному прикладі директива *Directory*визначає властивості каталогу *inconming,*а директива *Limit*задає правила доступу до нього. Параметр *WRITE*разом з директивою *AllowAll*встановлюють режим запису для усіх користувачів. Параметр *READ*разом із директивою *DenyAll*забороняють режим читання для усіх користувачів.

Поряд з *WRITE* і *READ* у директиві *<Limit>* передбачено використання параметра *LOGIN,* який обмежує реєстрацію користувачів. Додатковими директивами в блоці *<Limit>... </Limit>*можуть бути:

- ✓ *Allow*— дозвіл на виконання дії;
- ✓ *AllowAll* — дозвіл усім користувачам;
- ✓ *AllowGroup* — дозвіл групі користувачів;
- ✓ *AllowUser* — дозвіл окремому користувачеві;
- ✓ *Deny*— заборона на виконання дії;
- ✓ *DenyAll*— заборона всім користувачам;
- ✓ *DenyUser*— заборона окремому користувачеві.

Наприклад, наведемо директиву, яка дозволяє доступ до сервера лише обліковому запису користувача *student*з IP-адреси 11.50.1.215:

<Limit LOGIN>

Order allow,deny

Allow from 11.50.1.215

Allow User student

Deny from, all

</Limit>/

Для конфігурування публічного FTP-сервера можна використати директиви:

<Anonymous /var/ftp>

User Alias anonymous ftp

<Limit WRITE>

DenyAll

</Limit>

</Anonymous>

Перший рядок є початком багаторядкової директиви, яка стосується публічного доступу до каталогу */var/ftp.*Директива *UserAlias*визначає псевдонім анонімного облікового запису (ftp). Наступні три рядки забороняють запис у каталог */var/ftp*для усіх клієнтів.

Зазвичай у процесі автентифікації користувача *anonymous*як пароль використовують адресу електронної пошти користувача. Проте можна вимагати введення пароля й анонімним користувачем. Для цього потрібно додати директиву *AnonRequirePassword*.

Сервер ProFTPD надає можливості для авторизації користувачів не лише на основі облікових записів ОС Linux, а й із застосуванням файлів авторизації. Для цього за допомого команди *ftpasswd*потрібно створити файли з обліковими записами користувачів і груп.

Наприклад,

ftpasswd --passwd --name user1 --home /ftp/user1/ --shell /bin/ sh --uid 801

ftpasswd --group --name group1--member user1--member user2 --gid 801

Розглянемо параметри команди:

- ✓ *--passwd* — визначає формат файла (на зразок файла */etc/passwd*);
- ✓ *--group* — визначає формат файла (на зразок файла */etc/group*);
- ✓ *--name* — ім'я облікового запису користувача або групи;
- ✓ *--home*— домашній каталог для облікового запису користувача;
- ✓ *--member*— облікові записи користувачів, які входять до групи;
- ✓ *--shell*— командний інтерпретатор;
- ✓ *--uid*— числовий ідентифікатор облікового запису користувача;
- ✓ *--gid*— числовий ідентифікатор облікового запису групи.

Оскільки, ми змінюємо спосіб автентифікації, то у файлі */etc/proftpd/proftpd.conf* варто використовувати відповідний програмний модуль:

AuthOrdermod_auth_file.c

Крім цього в конфігурації сервера ProFTPD потрібно вказати розміщення файлів, які містять облікові записи:

AuthUserFile /etc/ftpd.passwd

AuthGroupFile /etc/ftpd.group

Визначаємо правила доступу до каталогів користувачів:

```
<Directory /var/user1>
        <Limit ALL>
                Allow Group group1
        </Limit>
</Directory>
```

Контрольні запитання:

1. Як Ви розумієте термін FTP-сервер?
2. Опишіть процес передавання даних за протоколом FTP.
3. Які директиви сервера ProFTPDВам відомі?
4. Перелічіть директиви для визначення властивостей каталогів сервера ProFTPD. Який їх синтаксис?

5. Як налаштувати публічний доступ до сервера ProFTPD?
6. Опишіть процес конфігурування сервера ProFTPDдля автенти-фікаціїкористувачів на основі окремих файлів.

7.5. Організація сервера електронної пошти засобами MicrosoftWindowsServer 2003

Однією з найпоширеніших служб мережі Інтернет є автоматизована система передавання повідомлень — електронна пошта (e-mail).

Складовими кожної поштової системи є:

- ✓ сервер пересилання, призначений для отримання повідомлень відправника та їх подальшого передавання в мережі (MTA — MailTransferAgent);
- ✓ сервер передавання отриманих сервером повідомлень клієнту (MDA— MailDeliveryAgent);
- ✓ програма для роботи з повідомленнями на комп'ютері користувача (MUA— MailUserAgent).

Серед цих складових перша та друга належать до серверної частини комплексу, а третя — до клієнтської.

Організацію обміну електронною поштою між робочими станціями здійснює поштовий сервер. Основними його функціями є прийом листів від клієнтів і доставка їх адресатам. Клієнтами можуть бути як користувачі, так й інші поштові сервери.

Користувачі за допомогою програми-пошти клієнта (OutlookExpress, TheBat!, Mozilla, Thunderbird тощо) можуть створювати листи, відправляти їх на сервер і забирати пошту зі своїх поштових скриньок на сервері.

Обмін даними між сервером і клієнтом відбувається згідно з поштовими протоколами: Simple Mail Transfer Protocol (SMTP) — використовується для передавання листів на сервер. Для одержання листів з поштової скриньки використовують протоколи Post Office Protocolv.3 (POP3) та Internet Message Access Protocol (IMAP).

Підключення клієнтів до сервера відбувається через певні порти. Для SMTPстандартним є порт 25, для POP3 — порт 110. Сервер, що працює із протоколом IMAP зазвичай використовує порт 143.

В адресі електронної пошти можна виділити ім'я облікового запису користувача та доменне ім'я сервера, які розділені символом «@». Наприклад, адреса user@server.edu.uaозначає що на сервері *server.edu.ua*зареєстровано обліковий запис користувача *user*.Ім'я DNS, яке вказано за символом «@», також називають поштовим доменом. Крім локальних облікових записів сучасні поштові сервери для автентифікації користувачів можуть використовувати:

- ✓ локальні облікові записи користувачів;
- ✓ записи домену ActiveDirectory;
- ✓ файли, що містять облікові записи користувачів разом з криптованими паролями;
- ✓ бази даних (MySQL, PostgreSQL, MicrosoftSQL).

Роботу поштової системи проілюстровано на рис. 7.14.

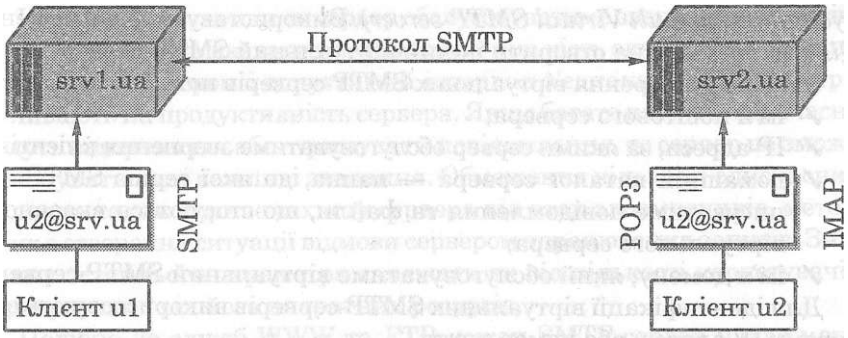


Рис. 7.14. Схема функціонування поштової системи

У процесі надсилання листа SMTP-сервер відправника (на рис. 7.14 це сервер *srv1.ua*) за допомогою служби DNSвизначає адресу SMTP-сервера, який обслуговує одержувача (на рис. 7.14 це сервер *srv2.ua*). Згодом сервери встановлюють з'єднання за протоколом SMTPі передають повідомлення.

Для ОС Windows існують різні поштові сервери. Найвідоміші з них — поштовий сервер, вбудований в ОС WindowsServer 2003 та ExchangeServer.

Для виконання функцій сервера передавання пошти у складі InternetInformationService реалізовано SMTP-сервер. Для його конфігурування використовують консоль MMC (рис. 7.15).

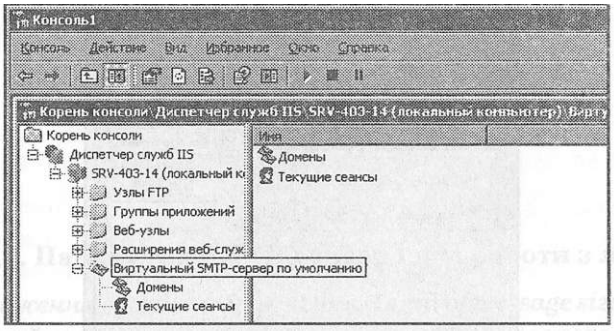


Рис. 7.15. Консоль MMC для адміністрування сервера SMTP

Подібно до веб-сервера, що забезпечує роботу кількох веб-вузлів, один SMTP-сервер може обслуговувати декілька поштових доменів, які називають віртуальними. Після встановлення компонентів InternetInformationService створюється *віртуальний SMTP-сервер за замовчуванням (DefaultVirtualSMTP-server).* Використовуючи пункт меню *Дія (Action),*можна створити інший віртуальний SMTP-сервер.

У процесі створення віртуальних SMTP-серверів потрібно вказати:

- ✓ ім'я поштового сервера;
- ✓ IP-адреси, за якими сервер обслуговуватиме звернення клієнтів;
- ✓ домашній каталог сервера — папка, до якої сервіс SMTPзаписуватиме повідомлення та файли, що стосуються вказаного віртуального сервера;
- ✓ ім'я домену, який обслуговуватиме віртуальний SMTP-сервер.

Для ідентифікації віртуальних SMTP-серверів використовують або окрему IP-адресу, або номер порту.

Складовими домашнього каталогу кожного SMTP-сервера є папки:

- ✓ BadMail— каталог для запису повідомлень, які неможливо надіслати;
- ✓ Drop— каталог для запису вхідних повідомлень даного домену;
- ✓ Pickup— каталог для запису повідомлень, які використовує служба SMTP;
- ✓ Queue— каталог, у якому повідомлення електронної пошти надходять

у чергу для надсилання зовнішнім адресатам.

Загальні параметри кожного SMTP-сервера можна переглянути та змінити у вікні його властивостей на вкладці *Загальні (General)*(рис. 7.16).

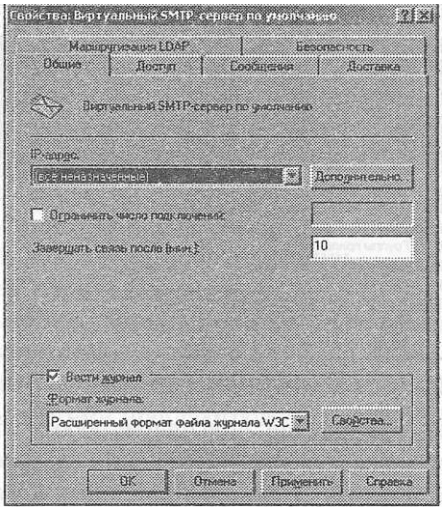


Рис. 7.16. Загальні параметри SMTP-сервера за замовчуванням

Крім IP-адрес, за якими сервер обслуговуватиме звернення клієнтів, на вкладці можна вказати максимальну кількість одночасних вхідних з’єднань із сервером і допустимий інтервал з'єднання. Ці параметри впливають на продуктивність сервера. Якщо багато клієнтів одночасно будуть відправляти або отримувати повідомлення, то сервер не зможе виконувати інші важливі завдання. Обмеження кількості одночасних з'єднань також сприяє захисту сервера від атак зловмисників, метою яких є створення ситуації відмови сервером опрацювання запитів. Значення останнього параметра залежать як від кількості користувачів сервера, так і від його апаратних ресурсів.

Подібно до служб WWW та FTP кожен SMTP-сервер надає можливості ведення журналу подій, налаштування якого здійснюють на вкладці *Загальні (General).*

На вкладці *Повідомлення (Messages)*можна вказати такі параметри (рис. 7.17):

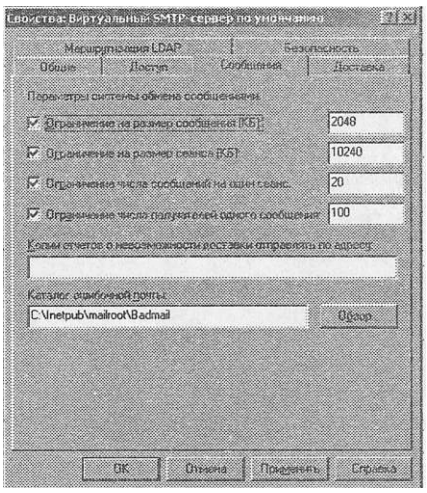


Рис. 7.17. Параметри SMTP-сервера для роботи з листами

- ✓ *Обмеження обсягу повідомлення (Limitofmessagesize)* — сервер не прийматиме листи обсягом більшим від вказаного, а відправник отримуватиме повідомлення про помилку;
- ✓ *Обмеження обсягу сеансу (Limitonsessionsize)* — визначає максимальний обсяг даних, які можуть бути передані протягом одного сеансу роботи із сервером;
- ✓*Обмеження кількості повідомлень для з єднання (Limit on the number of messages for a given connection);*
- ✓ */Обмеження кількості одержувачів кожного повідомлення (Limit on the number of recipients per message);*
- ✓ *Адресу для надсилання копій звітів про неможливість доставки (Addressforsendinganondeliveryreportmo);*
- ✓ *Каталог для збереження звітів про неможливість доставки (Directory for storing non delivery reports).*

Як відомо, крім приймання поштових повідомлень SMTP-сервер також здійснює їх доставку. Для цього він встановлює з’єднання з іншими SMTP-серверами. Розглянемо параметри, які впливають на процес надсилання повідомлень, що розміщені на вкладці *Доставка (Delivery)* (рис. 7.18).

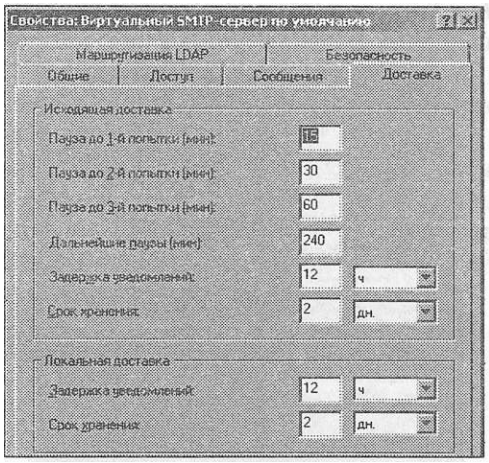


Рис. 7.18. Параметри доставки листів SMTP-сервером

- ✓ *Інтервал перед першим повтором (Firstretryinterval)* — проміжок часу в хвилинах, протягом якого сервер очікує повторну доставку листа, якщо його не було надіслано з першої спроби;
- ✓ *Інтервал перед другим повтором (Secondretryinterval)*— проміжок часу в хвилинах, протягом якого сервер очікує наступну спробу доставки листа, якщо його не було надіслано з першої та другої спроб;
- ✓ *Інтервал перед третім повтором (Thirdretryinterval)* — проміжок часу в хвилинах, протягом якого сервер очікує наступну спробу довставки листа, якщо його не було надіслано з першої, другої та третьої спроб;
- ✓ *Інтервал наступних повторів (Subsequentretryinterval)* — проміжок часу в хвилинах, протягом якого сервер очікує кожну наступну спробу надсилання, за умови, що здійснено більше ніж три повтори надсилання;
- ✓ *Строк повтору (Expiretiontimeout)*— проміжок часу, після завершення якого сервер не здійснюватиме спроб надіслати листа;
- ✓ *Затримка повідомлення (Delaynotification)*— проміжок часу, протягом якого сервер не надсилатиме повідомлення про невдалі доставки листів.

Клієнти, які надсилають листи за допомогою SMTP-сервера, можуть проходити автентифікацію. її параметри можна встановити, використ-

товуючи вкладку *Доступ (Access)*вікна властивостей віртуального SMTP-сервера (рис. 7.19).

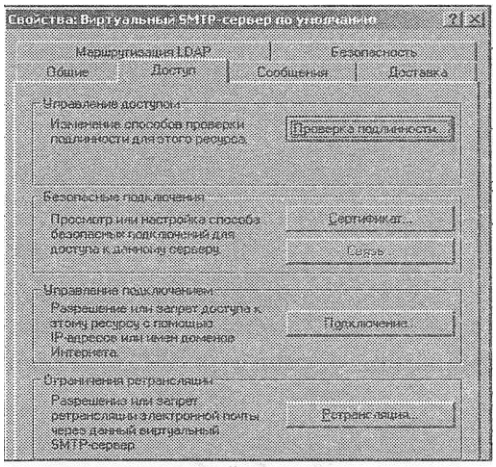


Рис. 7.19. Параметри доступу до SMTP-сервера

Секція *Управління доступом (AccessControl)* дає можливість обрати один з типів автентифікації клієнтів SMTP-сервера:

- ✓ анонімний доступ — для автентифікації реєстраційні дані не потрібні;
- ✓ базова автентифікація — логін і пароль сервер та клієнт передають у відкритому вигляді (без криптування);
- ✓ автектифікація з обов'язковим криптуванням згідно протоколу TLS(Transport Layer Security);
- ✓ доменне ім’я — автентифікація відбувається на основі доменного імені з адреси відправника;
- ✓ інтегрована автентифікація Windows — для автентифікації використовують дані облікового запису користувача, а для їх передачі — відомі протоколи Kerberos або NTLM.

Секція *Безпечні з'єднання (SecureConnection)* надає засоби для створення ключів криптування за протоколом TLS.

До параметрів безпеки також належить обмеження доступу до сервера на основі адрес клієнтів. їх можна встановити в секції *Управління з'єднанням {ConnectionControl)* вкладки *Доступ* (*Access*) вікна властивостей SMTP-сервера. При цьому потрібно визначити (рис. 7.20):

- ✓ режим доступу (дозвіл або заборона);
- ✓ IP-адреси комп'ютерів, підмереж або доменні імена, які є винятками стосовно обраного режиму доступу.

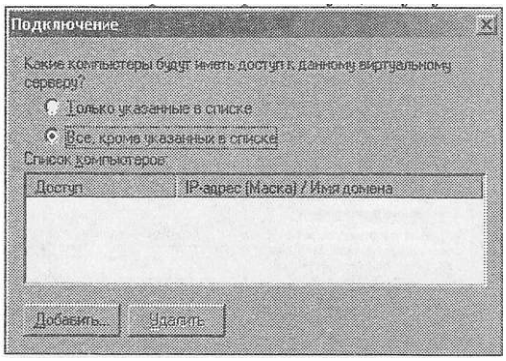


Рис. 7.20. Обмеження доступу до SMTP-сервера на основі адрес клієнтів

До важливих параметрів кожного сервера передачі пошти належить режим ретрансляції, тобто обмеження передавання листів, що надсилаються різними клієнтами. Зрозуміло, що сервер, який без обмежень ретранслює повідомлення, може бути використаний для розсилання спаму. Параметри ретрансляції можна вказати в секції *Обмеження ретрансляції {RelayRestriction*), що розміщена на вкладці *Доступ {Access)* вікна властивостей SMTP-сервера. Параметри обмеження ретрансляції аналогічні до параметрів доступу до сервера (рис. 7.21).

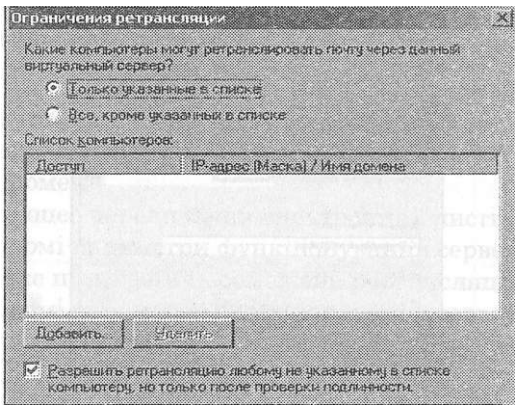


Рис. 7.21. Обмеження ретрансляції листів SMTP-сервером

Як бачимо з рис. 7.21, додатково можна встановити режим ретрансляції листів для довільного користувача, який пройшов автентифікацію.

Функції сервера передавання повідомлень клієнту в ОС WindowsServer 2003 виконує служба POP3. її конфігурування традиційно

здійснюють за допомогою оснащення MMC (рис. 7.22).

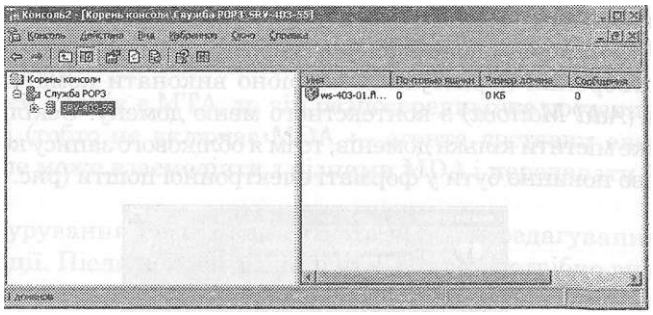


Рис. 7.22. Консоль MMC для адміністрування сервера POP3

Подібно до розглянутих раніше серверів існує можливість створити віртуальні поштові домени служби POP3. Варто зауважити, що домени серверів SMTPі POP3 не є взаємооднозначими. Проте для коректного функціонування поштових скриньок для кожного поштового домену варто створювати відповідні домени служб SMTPі POP3.

Параметри сервера POP3 можна переглянути та встановити у вікні його властивостей (рис. 7.23).

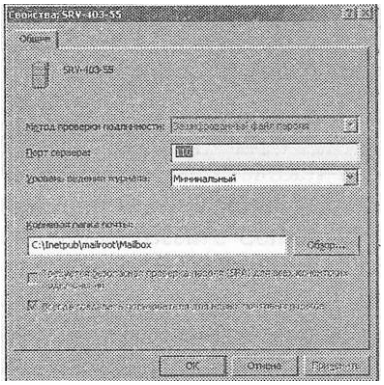


Рис. 7.23. Параметри сервера POP3

Розглянемо основні з них:

- ✓ метод перевірки достовірності на основі записів ActiveDirectory або файла, що містить облікові записи користувачів разом із криптованими паролями;
- ✓ номер порту, за яким сервер очікуватиме з’єднання;
- ✓ рівень деталізації ведення журналу;
- ✓ каталог для зберігання повідомлень.

Слід зазначити, що метод перевірки достовірності визначають у процесі встановлення поштового сервера, й потім він змінений бути не

може.

Для створення користувача потрібно виконати команду *Додати скриньку (AddMailbox)*з контекстного меню домену. Оскільки сервер POP3 може містити кілька доменів, то ім’я облікового запису користувача обов'язково повинно бути у форматі електронної пошти (рис. 7.24).

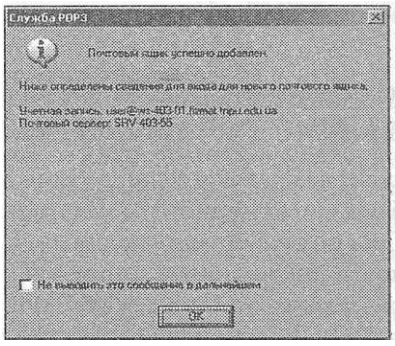


Рис. 7.24. Відомості про створений обліковий запис сервера POP3

Налаштування в різних поштових клієнтах можуть мати різні назви, але обов’язковими є такі: SMTP-сервер, POP3-сервер, Користувач (Обліковий запис), Пароль.

Контрольні запитання

1. Як Ви розумієте терміни: електронна пошта, поштовий сервер, поштовий домен?
2. Опишіть процес передавання електронних листів.
3. Які Вам відомі параметри функціонування сервера SMTP?
4. До чого може призвести необмежена ретрансляція листів?
5. Які Вам відомі параметри функціонування сервера POP3?
6. У чому полягає відмінність автектифікації користувачів серверами SMTP і POP3?

7.6. Організація сервера електронної пошти засобами ОС Linux

Сучасні дистрибутиви ОС Linux для організації поштового сервера пропонують програмні пакети Sendmail і Postfix. З-поміж них було обрано сервер Postfix.

Postfix— агент передавання пошти (MTA). Postfix створювався як альтернатива Sendmail. Вважається, що Postfix швидше працює, зручніший в адмініструванні, більш захищений і, що важливо, сумісний з Sendmail.

Оскільки Postfix є MTA, то він безпосередньо не доставляє пошти адресатові (тобто не включає MDA — агента доставки електронної пошти), але може взаємодіяти з різними MDA і передавати їм вхідну пошту.

Конфігурування Postfix здійснюють шляхом редагування файлів конфігурації. Після кожної зміни в цих файлах потрібно виконувати перезапуск сервера за допомогою команди */etc/init.d/postfixrestart.* Основним конфігураційним файлом Postfixє */etc/postfix/main .cf.*

Повідомлення про функціонування сервер Postfixзаписує у файлі журналу, який за замовчуванням знаходиться в */var/log/maillog.*

Рядки файла *main.cf*що починаються із символу #, містять коментарі. У таблиці наведено основні параметри файла конфігурації поштового сервера Postfix.

Таблиця 7.2.Основні директиви файла main.cf

Параметр	**Значення**	**Опис**
relayhost =	*smtp.isp.ua*	Листи відправлятимуться через проміжний поштовий сервер (*smtp.isp.ua).* Якщо параметр порожній, то листи будуть надіслані безпосередньо серверу отримувача
myhostname =	*mail.example.ua*	Назва сервера. Найбільш доцільно встановити її значенням DNS-ім’я сервера
mydomain =	*example.ua*	Назва домену. Якщо змінна не буде встановлена, то Postfix буде використовувати значення *myhostname* за винятком першого компонента

inet_interfaces =	*all* *$localhost* *$my hostname*	Адреси встановлених інтерфейсів, з яких можна приймати *smtp* з'єднання. Значення *all* встановлює режим роботи з усіма інтерфейсами. Змінні *$localhost* або *$myhostname* визначають IP-адресу 127.0.0.1 та IP-адресу інтерфейсу, яка відповідає назві, визначеній в змінній *$myhostname*
mydestination =	*$myhostname* *$mydomain*	Список назв доменів, які обслуговує сервер
mynetworks =	*192.168.0. 0/24, 127.0. 0.0/8*	Визначає список довірених мереж. Клієнти з адресами, що належать до вказаних мереж, можуть виконувати
myorigin =	*example.ua*	Значення цього параметра встановлює доменну частину поштової адреси відправника
local_recipient_ maps=		Параметр вказує необхідність перевірки існування користувача, якому адресована пошта. Якщо значення параметра порожнє, перевірка не відбувається, в іншому випадку значення параметра вказує на знаходження таблиці облікових записів користувачів. Якщо обліковий запис користувача не знайдено, то повідомлення, що було йому адресовано, буде відкинуто сервером
mail_spool_ directory =	*/var/spool/mail*	Встановлює шлях до поштових скриньок користувачів поштового сервера

home_mailbox =	*Mailbox*	Встановлює спосіб зберігання пошти у файловій системі сервера. Якщо вказано значення *Mailbox*, то пошта користувача буде збережена в одному файлі, якщо ж значення параметра *Maildir*/, то пошта користувача зберігатиметься в папці, а кожне повідомлення буде зберігатися у вигляді окремого файла. За замовчуванням пошта потраплятиме у файли виду */var/spool/ mail/імя*
mailbox_size_ limit =	*52428800*	Обмежує обсяг поштової скриньки в байтах
message_size_ limit =	*1012000*	Обмежує обсяг повідомлення в байтах

Сервер Postfix надає можливості обслуговування поштових скриньок не лише для облікових записів користувачів ОС Linux, а й для окремо створених файлів.

Наприклад, якщо в конфігурації сервера Postfix була директива *$mydestination= mydomain.ua,* то у процесі одержання листа для адресата user@mydomain.ua сервер здійснював пошук облікового запису користувача user у файлі */etc/passwd* ОС Linux. Оскільки поштовий сервер може обслуговувати значну кількість користувачів, то створювати кожному з них окремий обліковий запис нераціонально з точки зору розподілу ресурсів і неправильно з точки зору безпеки ОС. Тому облікові записи користувачів поштового сервера розміщують в окремому файлі. Такі облікові записи інколи називають «віртуальними користувачами».

Для того щоб налаштувати Postfix для роботи з файлами, які містять облікові записи, необхідно зробити відповідні зміни в конфігураційному файлі */etc/postfix/ main.cf* (див. табл. 7.3).

Таблиця 7.3.Директиви файла таіп.cfдля роботи з файлами, що містять облікові записи користувачів

Параметр	Значення	Опис
virtual_mailbox_ domains	*example1.ua*	Імена віртуальних поштових доменів, які обслуговуватиме Posfix. Параметру не слід надавати значення, яке вказане в директиві *mydestination*
virtual_mailbox_maps =	*hash:/etc/ postfix/virtual_ mailbox*	Визначає розміщення таблиці локальних користувачів. Запис *hash* задає формат файла — *BerkeleyDB*
virtual_mailbox_base =	*/var/spool/mail*	Вказує шлях розташування поштових скриньок
virtual_uid_maps =	*static:1100*	Визначає власника поштових скриньок віртуальних користувачів. Дане значення означає, що власником усіх поштових скриньок віртуальних користувачів буде користувач з ідентифікатором 1100
virtual_gid_maps =	*static:1101*	Вказує групу поштових скриньок віртуальних користувачів. Дане значення означає, що групою всіх поштових скриньок віртуальних користувачів буде група з ідентифікатором 1101

Після внесення вищезазначених змін необхідно створити текстовий файл*/etc/postfix/virtual_mailbox.* Записи в файлі*virtual_mailbox* повинні мати такий формат:

ім'я користувача шлях до поштової скриньки.

Наприклад:

user@example1.com user/inbox

user1@example1.com user1/inbox

Шлях до поштової скриньки вказуємо відносно значення параметра *virtual_mailbox_base.*Після останнього рядка файла *virtual_mailbox*необхідно залишити порожній рядок.

Створивши файл *virtual_mailbox,* потрібно згенерувати двійковий файл *virtual_mailbox.db* у форматі BerkeleyDB за допомогою команди:

postconfvirtual_mailbox

Оскільки Postfix не може виконувати функції MDA, то для виконання функцій передавання електронних листів до клієнта потрібно налаштувати сервер, що працює за протоколами POP3 або IMAP. Таким сервером є Dovecot.

Для того щоб Dovecot міг коректно працювати, його налаштування необхідно проводити у відповідності з налаштуваннями сервера Postfix. Налаштування Dovecot здійснюється шляхом редагування файлів конфігурації. Після кожної зміни в цих файлах потрібно виконувати перезапуск сервера за допомогою команди */etc/init.d/dovecotrestart.* Основним конфігураційним файлом Dovecot є */etc/dovecot.conf.* Рядки файла *dovecot.conf*, що починаються із символу #, містять коментарі.

У таблиці 7.4 наведено основні директиви файла конфігурації сервера Dovecot.

Таблиця 7.4.Основні директиви файла dovecot.conf

Параметр	Значення	Опис
protocols=	*imapimapspop-3*	Протоколи, з якими працює сервер.
imap_listen=	* *10.1.1.101:143*	Вказує на яких інтерфейсах очікувати з'єднання за протоколом IMAP. Значення «*» означає, що будуть задіяні всі інтерфейси сервера, значення параметра можуть мати вигляд IP-адреси:port
Pop3_listen=	* *10.1.1.101:110*	Вказує на яких інтерфейсах очікувати з'єднання за протоколом
disable _plaintext_ auth =	*no* *yes*	Вказує на заборону некриптованої автентифікації
mail_location =	*mbox:~/mail/:INBOX =/var/mail/%u*	Вказує маршрут до поштових скриньок, %и — змінна, ім'я користувача: значення параметра необхідно встановлювати в каталозі, у якому зберігає листи сервер Postfix
auth_mechanisms=	plain cram-md5 ntlm	Визначає механізм автентифікації, *plain* — відкритий текст; *cram-md5* — за допомогою алгоритмів MD5
userdb	passwd { args }	Вказує місце розташування бази даних облікових записів користувачів, а також додаткові параметри (аргументи) роботи з нею
auth_passdb =	pam	Вказує метод доступу до бази паролів. PAM (PluggableAuthenticationModules) — системна бібліотека для
log_path =	/var/log/dovecot.log	Визначає шлях до журналу сервера

Якщо ж Postfix налаштовано на роботу з віртуальними користувачами відповідно до директив таблиці 7.3, то в конфігурації сервера Dovecot необхідно зробити відповідні зміни (табл. 7.5).

Таблиця 7.5.Директиви файладevecot.confдляроботи з файлами, що містять облікові записи користувачів

Параметр	Значення	Опис
userdbpasswd-file	*{ args = username_ format— %n/etc/dovecot_ pass }*	Вказує, що база даних облікових записів користувачів знаходиться у файлі */etc/dovecot_pass*
passdb passwd-file	*{ args = username_ format-%n /etc/dovecot_ pass }*	Вказує, що база даних паролів знаходиться в файлі /*etc/dovecot_ pass*
mail_location=	*mbox: / var/spool / mail / %n:INDEX= /var / spool/mail/%n*	Значення цього параметра було змінено відповідно до шляху до поштових скриньок віртуальних користувачів Postfix

Після внесення змін у файл *dovecot.conf* потрібно створити файл */etc/dovecot_pass,* який повинен мати такий формат:

ім’я Kopucmувача:naроль:uid:gid::шляхдо поштової скриньки

Наприклад:

user:{plain}pass: 1100:1101::/var/mail/user

user1:{plain}pass2:1100:1101::/var/mail/user1

Контрольні запитання

1. Перелічіть основні директиви Postfix. Який їх синтаксис?
2. Опишіть процес конфігурування сервера Postfixдля роботи з

віртуальними користувачами.

3. Перелічіть основні директиви Dovecot. Який їх синтаксис?
4. Опишіть процес конфігурування сервера Dovecotдля автентифікації користувачів на основі окремих файлів.
5. Які з директив сервера Postfixпотрібно враховувати у процесі конфігурування сервера Dovecot?

7.6. Конфігурування проксі-сервера

Для організації доступу до Інтернету в локальних мережах використовують шлюз (маршрутизатор) — це проміжний вузол, що забезпечує зв'язок комп'ютерів з різних мереж (рис. 7.25).

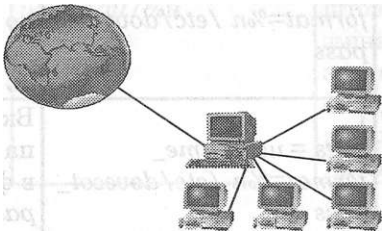


Рис. 7.25. Підключення локальної мережі до Інтернету через шлюз

Оскільки, на відміну від комп'ютерів локальної мережі, маршрутизатор має реальну IP-адресу, то, зазвичай, він виконує перенаправления їх запитів, замінюючи в усіх пакетах адресу відправника на свою адресу. Такий механізм передавання даних відомий як NAT-маршрутизація.

Іншим засобом організації доступу комп'ютерів локальної мережі до Інтернету є проксі-сервер. Проксі є програмою, що надає доступ до мережі Інтернет для всієї локальної мережі, перенаправляє запити до зовнішніх веб-серверів, зберігає (кешує) відвідані веб-сторінки на диску (з можливістю перегляду в режимі offline), організовує систему заборон. Переважно проксі-сервер працює із запитами, надісланими за протоколами HTTPі FTP.

Подібно до NAT-маршрутизатора застосування проксі-сервера дає можливість використовувати фіктивні IP-адреси у внутрішній мережі. Крім

цього завдяки механізму кешування проксі-сервер значно швидше виконує повторні запити, а також забезпечує додаткову безпеку.

Серед служб проксі своєрідним стандартом є сервер Squid. Програма є досить поширеною та має версії для багатьох ОС, в тому числі і для ОС Linuxта Windows.

Налаштування сервера здійснюється шляхом редагування файла конфігурації */etc/squid/squid.conf.* Після кожної зміни цього файла в ОС Linux потрібно перезапускав сервер за допомогою команди */etc/init.d/squidrestart*. В ОС Windows потрібно перезавантажувати виконуваний файл *squid.exe* або відповідну системну службу.

Конфігураційний файл сервера Squidмістить:

- ✓ мережні параметри сервера;
- ✓ директиви, що визначають продуктивність сервера;
- ✓ параметри ведення журналів;
- ✓ директиви обмеження доступу клієнтів до Інтернету;
- ✓ параметри зовнішніх програм, до яких звертається проксі-сервер.

До мережних параметрів проксі-сервера Squidналежать:

- ✓ *http_port*— порт для запитів клієнтів. Із цього порту проксі-сервер очікуватиме й опрацьовуватиме запити клієнтів. Значення параметра за замовчуванням дорівнює 3128;
- ✓ *icp_port*—порт для обміну даними з «сусідніми» проксі-серверами засобами протоколу обміну даними кешування (ICP — InternetCacheProtocol). Якщо таких проксі-серверів немає, то потрібно встановити значення, що дорівнює нулеві. Значення параметра за замовчуванням дорівнює 3130;
- ✓ *passive_ftp*— використання пасивного або активного режиму надсилання запитів за протоколом FTP. Якщо проксі-сервер працює через NAT-маршрутизатор, то значення параметра потрібно встановити рівне *on;*
- ✓ *cachejpeer*— проміжний проксі-сервер, через який необхідно

надсилати запити. Синтаксис директиви *cache_peer* такий:

cache_peer hostname type proxy-port icp-port options,

де

- ✓ *hostname* — DNS-ім’я або IP-адресапроміжного проксі;
- ✓ *type* — тип проміжного проксі: *parent* — старший, *sibling* — рівний;
- ✓ *proxy-port*— порт, за яким проміжний проксі-сервер опрацьовує запити;
- ✓ *icp-port*— порт протоколу ICP проміжного проксі;
- ✓ *options*— додаткові параметри.

Продуктивність проксі-сервера залежить від обсягів оперативної пам’яті та дискового простору для збереження кешу. Розглянемо параметри продуктивності сервера:

- ✓ *cache_mem<число>* — визначає обсяг оперативної пам’яті, що відводиться під кеш. Обсяг можна вказати в байтах, кілобайтах, мегабайтах (Mb) або гігабайтах (Gb);
- ✓ *cache_swap_high<число>* — відсоток заповнення кешу, після досягнення якого сервер видаляє старі об’єкти;
- ✓ *cache_swap_low<число>* — відсоток заповнення кешу, при досягненні якого припиняється видалення старих об’єктів;
- ✓ *maximum_object_size<число>* — максимальний обсяг об’єкта в кілобайтах для кешування;
- ✓ *У minimum_object_size* — мінімальний обсяг об’єкта в кілобайтах для кешування; файли меншого обсягу не кешуються. Значення за замовчуванням дорівнює 0 кілобайт;
- ✓ *cache_dir*— визначає шлях до каталогу з кешем і його параметри. Синтаксис директиви *cache_dir*такий:

cache_dir<тип><каталог><обсяг><каталог_1><каталог_2>,

де

- ✓ *<тип>* — тип кешу. Переважно використовують значення *ufs;*
- ✓ *<каталог>* — маршрут до каталогу, в якому міститиметься кеш;

- ✓ *<обсяг>* — обсяг кешу в мегабайтах;
- ✓ *<каталог_1 >* — максимальна кількість підкаталогів першого рівня, які міститимуться в каталозі кешу;
- ✓ *<каталог_2>* — максимальна кількість підкаталогів другого рівня, які міститиме кожен каталог першого рівня.

Наприклад, директиву *cache_dir* можна визначити так:

cache_dirufs/var/squid/cache 4096 64 256

Ведення журналів функціонування сервера визначають параметри:

- ✓ *cache_access_log /var/squid/access.log* — файл, який містить протокол запитів до сервера Squid;
- ✓ *cache_log /var/squid/cache.log* — файл, який містить протокол завантаження процесів;
- ✓ *cache_store_log /usr/loca/lsquid/logs/store.log* — файл, що містить протокол запису файлів у кеш.

Варто звернути увагу на те, що власником вищезазначених файлів, а також каталогів кешу повинен бути обліковий запис користувача *squid.*

У файлі конфігурації *squid.conf* важливими є такі параметри зовнішніх програм і сервісів:

- ✓ *ftp_user<email-адреса>*—поштова адреса, яку буде використано замість паролю при анонімному доступі до ftp-серверів;
- ✓ *dns_nameservers<список IP-адрес>* — адреси DNS-серверів, до яких буде звертатися *squid*;
- ✓ *authenticate_program<шлях>*— маршрут до програми, яка здійснює автентифікацію клієнтів. При цьому потрібно визначити правило ACL*proxy_auth.*

Із метою розмежування доступу користувачів до мережі Інтернет у файлі *squid.conf* передбачено списки управління доступом (ACL — Access Control Lists).

Синтаксис списків ACLмає формат:

acl<ім'я><тип>

Тип є критерієм належності клієнта до того чи іншого списку. Основні типи, які можна використовувати у списках ACL, наведено у таблиці 7.6.

Таблиця 7.6.Основні типи, які застосовують у списках ACL

Тип	Опис
src<IP-адреса>/<маска>	IP-адреса комп'ютера або підмережі клієнта
dst<IP-адреса>/<маска>	IP-адреса комп'ютера або підмережі призначення (до яких надсилають запит)
dstdomain <URL>	Доменне ім'я сервера або його частина, до якого надсилають запит
Time[день] [Г1:Х1 - Г2:Х2]	Час, де день — один із днів тижня (від неділі до суботи), які позначають літерами SMTWHFA
Port	Список портів
Port portl-port2	Діапазон портів
Proto	Протокол запиту. Зазвичай цей тип має значення HTTP або FTP
proxyjauth	Необхідність автентифікації клієнта

Наприклад, опишемо правило, яке визначатиме комп'ютери- клієнти мережі 172.25.0.0 з маскою підмережі 255.255.0.0:

aci somenetsrc172.25. 0.0/255.255.0.0

Правило, яке визначає час з 8:00 до 17:00 у робочі дні має вигляд:

aci worktimetimeMTWHF8:00-17:00

Правило, яке визначає всі комп'ютери-клієнти, має вигляд:

aci allsrc0.0.0.0/0.0.0.0.

Після опису списків доступу потрібно вказати параметри доступу до проксі-сервера:

http_access<дія><правило ACL>,

де під дією розуміють дозвіл *{allow)*або заборону *{deny).*

Наприклад, визначимо параметри доступу, які надають доступ для

комп’ютерів з описаного правила *somenet*, а також забороняють доступ усім іншим комп’ютерам:

http_access allow somenet

http_access deny all

Зауважимо, що параметри доступу діють у порядку їх опису. Тобто, якщо у попередньому прикладі їх поміняти місцями, то доступ буде заборонено всім комп'ютерам. Якщо потрібно в межах одного параметра задіяти кілька правил за логікою кон’юнкції, то ці правила потрібно вказати послідовно.

Наприклад, для того щоб надати доступ до проксі-сервера в час, що визначений правилом *worktime*, для комп'ютерів з описаного правила *somenet*, потрібно додати параметри:

http_access allow somenet worktime

http_access deny all

Якщо необхідно, щоб автентифікація користувачів відбувалася через введення логіна та паролю, то потрібно вказати такі директиви:

auth_param basic program /usr/libexec/ncsa_auth /etc/squid_passwd,

де

- ✓ *basic* — базовий для ОС спосіб автентифікації;
- ✓ *program /usr/libexec/ncsa_auth* — маршрут до програми, яка здійснює автентифікацію;
- ✓ */etc/squid/passwd* — файл, що містить облікові записи користувачів та їх паролі. Його можна створити за допомогою програми *htpasswd.*

Крім налаштування програми автентифікації потрібно описати відповідні правила ACLта параметри доступу:

aci good_user proxy_auth REQUIRED

http_access allow good_user

Проксі-сервер Squidнадає засоби для розподілу трафіку, який проходить через нього. Це необхідно тоді, коли одна група комп'ютерів або користувачів повинна мати доступ до Інтернету з більшою швидкістю, ніж

інша.

Для цього необхідно визначити кількість таких груп (пулів):

delay_pools2

Визначити належність кожного пулу до одного із трьох класів:

- ✓ *delay_class 1* — надає одне обмеження пропускної здатності каналу на всіх клієнтів;
- ✓ *delay_class 2* — надає одне загальне обмеження і 255 окремих для кожного вузла підмережі класу С;
- ✓ *delay_class3* —- для кожної підмережі класу В буде використано власне обмеження й окреме обмеження для кожного вузла.

Наприклад, визначимо перший пул класу 1 і другий пул класу 2:

delay_class 1 1

delay_class 2 2

Визначимо правила ACL та їх відповідність пулам:

acl servers src 10.41.1.100/255.255.255.255,

10.41.1.200/255.255.255.255

aci workstations src 172.25.0.01255.255.0.0

delay_access 1 allow servers

delay_access 1 deny all

delay_access 2 allow workstation

delay_access 2 deny all

Опишемо обмеження щодо швидкості для кожного з пулів:

delayparameters 1 262144/262144

delayparameters 2 524288/524288 84000/168000

Оскільки перша група (пул) належить до класу 1, то використовується одне обмеження для всіх комп’ютерів, що входять у пул — 262144 байт. Перше число визначає швидкість наповнення трафіком усього пулу (байт/с). Друге — максимальне значення швидкості користувача. Для пулу класу 2 використовують обмеження на всю підмережу й окремо на кожного користувача.

Наведемо приклад обмеження для пулу класу 3:

delay_parameters3 128000/128000 64000/128000 12800/64000

Перші два числа визначають швидкість наповнення і максимальну швидкість доступу до всієї мережі. Наступна пара чисел вказує на швидкість наповнення та доступ для кожної підмережі, а третя — стосується окремого комп'ютера.

Контрольні запитання

1. Яке тлумачення термінів: проксі-сервер, кеш, пул?
2. Опишіть процес функціонування проксі-сервера.
3. Які мережні параметри та директиви продуктивності проксі-сервера Squid?
4. На основі яких критеріїв проксі-сервер Squidнадає клієнтам доступ до мережі Інтернет?
5. Як налаштувати автентифікацію користувачів проксі-сервера Squid?
6. Перелічіть директиви обмеження швидкості передавання даних через сервер Squid.

8. Лабораторний практикум

Традиційною формою формування практичних умінь і навичок у студентів на курсах інформатики е лабораторні роботи. Для виконання кожної лабораторної роботи з курсу «Адміністрування комп'ютерних мереж і систем» потрібно передбачити дві, чотири або шість академічних годин залежно від складності та кількості завдань.

Оскільки переважна більшість завдань лабораторних робіт вимагають проведення налаштувань мережних сервісів, основою яких є технології «клієнт-сервер», то доцільно сформувати мікрогрупи в складі двох осіб. Робота у складі таких мікрогруп дає змогу студентам оволодіти досвідом різних видів діяльності, в тому числі виконавської, управлінської, організаційної, консультаційної, аналітичної та синтетичної.

Вивчення мережних технологій часто відбувається в умовах, які можуть призвести до зриву навчального процесу. Це зумовлено тим, що для виконання лабораторних робіт необхідними є повноваження адміністратора. Це може призвести до зниження рівня безпеки як ОС окремого комп'ютера, так і всієї мережі навчального закладу. В зв'язку з цим студенти не повинні мати можливості пошкодити свою мережну ОС або систему товариша. Для розв'язання зазначеної проблеми можна запропонувати два способи:

1. Виділення окремої лабораторії для проведення відповідних занять. Реалізація такого підходу практично є неможливою через значні матеріальні затрати.
2. Встановлення окремих ОС (MicrosoftWindowsServer 2003 і Linux) на студентських комп'ютерах поряд із основною ОС.

У процесі виконання лабораторних робіт студентам пропонують оформити результати виконання кожного завдання у вигляді таблиці, що містить:

- ✓ детальний опис кожного кроку адміністрування сервера;
- ✓ підтвердження виконаної дії у вигляді копії вікон (переважно для ОС Windows) або команд (переважно для ОС Linux);

- ✓ результати тестування коректності встановлених значень параметрів серверів.

Завдання лабораторної роботи разом із сформованими таблицями рекомендуємо надсилати викладачеві як електронний звіт виконання лабораторної роботи.

Лабораторна робота №1

Тема. ***Робота з обліковими записами користувачів і груп ОС WindowsServer 2003***

Мета роботи: формування вмінь створення й редагування облікових записів користувачів ОС WindowsServer 2003.

1. Створити обліковий запис користувача *root.*Заповнити поля опису облікового запису, ввівши до них відомості про себе, і встановити пароль для зазначеного облікового запису. Заповнити таблицю.

№з/п	Дія	Команда

2. Задати такі значення параметрів створеного облікового запису:

- ✓ вимагати змінити пароль при наступному вході користувача всистему;
- ✓ необмежений термін дії пароля.

Заповнити таблицю.

№з/п	Дія	Команда

3. Визначити групу, до якої належить створений обліковий запис користувача. Заповнити таблицю.

№з/п	Дія	Команда

4. Зареєструватися в системі, використовуючи створений обліковий запис. Перевірити, чи відповідають повноваження облікового запису повноваженням групи, до якої він належить. Вказівка: можна спробувати встановити драйвер пристрою або програмне забезпечення. Заповнити таблицю.

№з/п	Дія	Команда

5. Змінити пароль створеного облікового запису, використовуючи оснащення консолі MMC, а також комбінацію клавіш C^1+A1i+Be1eie. Чим відрізняються ці способи між собою?

6. Зареєструватися в системі, ввівши дані адміністратора. Додати створений обліковий запис до групи адміністраторів. Заповнити таблицю.

№з/п	Дія	Команда

7. Зареєструватися в системі, використовуючи створений обліковий запис. Перевірити, якій групі відповідають повноваження облікового запису.

№з/п	Дія	Команда

8. Створити обліковий запис користувача *student1*. Встановити для нього пароль. Заповнити таблицю.

№з/п	Дія	Команда

9. Створити обліковий запис користувача *student2* на віддаленому комп'ютері (за вказівкою викладача). Встановити для нього пароль. Заповнити таблицю.

№з/п	Дія	Команда

10. Змінити пароль створеного облікового запису на віддаленому комп'ютері.

11. Створити обліковий запис групи користувачів *students*.Додати до його складу облікові записи користувачів *student1*і *student2*. Заповнити таблицю.

№з/п	Дія	Команда

Контрольні запитання

1. До якої групи повинен належати обліковий запис користувача, щоб у нього були повноваження створювати інші облікові записи?
2. Чи може обліковий запис належати до двох груп? Які повноваження він отримає в цьому разі?
3. Яких правил потрібно дотримуватися, аби створити обліковий запис користувача віддаленого комп'ютера?

Лабораторна робота №2

Тема. ***Встановлення правил доступу до об'єктів файлової системи NTFS***

Мета роботи: навчитися змінювати власників і правила доступу до об'єктів файлової системи NTFS.

1. На системному диску створити каталог *Folder1*. Переглянути правила доступу до створеного каталогу. Заповнити таблицю.

№з/п	Дія	Команда

2. Вилучити всі правила доступу до каталогу Folder 1. Встановити правила повного доступу користувача root до каталогу Folder 1. Заповнити таблицю.

№з/п	Дія	Команда

3. Перевірити дію встановлених правил, послідовно зареєструвавшись під обліковими записами *root*і *student1*. Заповнити таблицю.

№з/п	Дія	Команда

4. Для каталогу *Folder1* додати правила читання та завантаження файлів, а також перегляду вмісту, які стосуються користувача *student!*.Заповнити таблицю.

№з/п	Дія	Команда

5. Перевірити дію встановлених правил, послідовно зареєструвавшись під обліковими записами *student1* і *student2*. Заповнити таблицю.

№з/п	Дія	Команда

6. Для каталогу *Folder1* додати правила читання та завантаження файлів, а також перегляду вмісту, які стосуються групи *students*.Правила, що стосуються облікового запису *student 1*, вилучити. Заповнити таблицю.

№з/п	Дія	Команда

7. Перевірити дію встановлених правил, послідовно зареєструвавшись під обліковими записами student1 і student2. Заповнити таблицю.

№з/п	Дія	Команда

8. Для каталогу *Folder1* додати правила запису і зміни об’єктів, які стосуються облікового запису користувача *student2*.Заповнити таблицю.

№з/п	Дія	Команда

9. Перевірити дію встановлених правил, зареєструвавшись під обліковою запис *student2*. Заповнити таблицю.

№з/п	Дія	Команда

10. Для каталогу *Folder1* додати правила заборони запису, які стосуються облікового запису групи *students*.Заповнити таблицю.

№з/п	Дія	Команда

11. Перевірити дію встановлених правил, послідовно зареєструвавшись під обліковими записами *student1* і *student2*. Заповнити таблицю.

№з/п	Дія	Команда

12. Для каталогу *Folder 1* вилучити правила заборони, які стосуються облікового запису групи *students*. Заповнити таблицю.

№з/п	Дія	Команда

13. Для каталогу *Folder1* додати правило повного доступу, яке стосується облікового запису користувача *student1*. Заповнити таблицю.

№з/п	Дія	Команда

14. Перевірити дію встановлених правил, послідовно зареєструвавшись під обліковими записами *student1* і *student2*. Заповнити таблицю.

№з/п	Дія	Команда

15. Для каталогу *Folder1* додати правило дозволу для зміни власника, яке стосується облікового запису користувача *student1*. Заповнити таблицю.

№з/п	Дія	Команда

16. Перевірити дію встановлених правил, послідовно зареєструвавшись під обліковими записами *student1* і *student2*. Заповнити таблицю.

№з/п	Дія	Команда

17. Встановити власником каталогу *Folder1* користувача *student2*. Для каталогу Folder 1 додати правило заборони повного доступу, яке стосується всіх облікових записів. Заповнити таблицю.

№з/п	Дія	Команда

18. Для каталогу Folder 1 встановити правила повного доступу для групи Адлініструватори і правила доступу для читання і виконання для групиКористувачі. Заповнити таблицю.

№з/п	Дія	Команда

19. На системному диску створити каталог *Folder2*. Встановити такі правила доступу до *Folder2*, щоб користувачі *student1* і *student2* могли переглядати його вміст та створювати каталоги. До підкаталогів папки *Folder2* власникам надати повний доступ. Окрім власників до підкаталогів повний доступ надати користувачеві root. Заповнити таблицю.

№з/п	Дія	Команда

Контрольні запитання

1. Як змінити або видалити правила, які помічені блідими прапорцями?
2. Чи гарантовано користувач, для облікового запису якого встановлено режим повного доступу до файла, зможе скопіювати (знищити) файл?
3. Чи можна користувачеві з групи Адміністратори гарантовано заборонити доступдо об'єкта файлової системи NTFS?

Лабораторна робота №3

Тема. ***Створення розподілених ресурсів засобами ОС Microsoft Windows Server 2003***

Мета роботи:навчитися створювати спільні ресурси локальної мережі й обмежувати доступ до них.

1. За допомогою консолі MMC переглянути спільні ресурси. Знайти системні ресурси *c$, d$* та визначити правила доступу до них. Заповнити таблицю.

№з/п	Дія	Команда

2. Для каталогу *Folder1* встановити правила файлової системи NTF3, які передбачають повний доступ для групи Адміністратори та читання і виконання файлів для групи Користувачі. Заповнити таблицю.

№з/п	Дія	Команда

3.Створити спільний мережний ресурс з назвою *Share1*, вказавши маршрутом шлях до папки *Folder1*. Задати такі правила доступу до ресурсу: повний доступ для всіх облікових записів.

№з/п	Дія	Команда

4.Перевірити дію заданих правил, послідовно звернувшись до ресурсу *Share1* із застосуванням облікових записів *root* і *student1*. Виконати копіювання та запис даних з (до) ресурсу *Share1*. Заповнити таблицю.

№з/п	Дія	Команда

5. Змінити правила доступу до мережного ресурсу *Share1*:

- ✓ група адміністратори — доступ відсутній;
- ✓ користувач *student1*— повний доступ.

№з/п	Дія	Команда

6. Перевірити дію заданих правил, послідовно звернувшись до ресурсу *Share1* із застосуванням облікових записів *root* і *student1*. Виконати копіювання та запис даних з (до) ресурсу *Share1*. Заповнити таблицю.

№з/п	Дія	Команда

7. Додати правило доступу для читання мережного ресурсу*Share1*, яке стосується облікового запису користувача *root.*

№з/п	Дія	Команда

8.Перевірити дію заданих правил, звернувшись до ресурсу *Share1* із застосуванням облікового запису *root*. Заповнити таблицю.

№з/п	Дія	Команда

9. Для каталогу *Folder1* задати правила файлової системи NTFS, які передбачають доступ для читання і виконання стосовно групи *Користувачі*. Заповнити таблицю.

№з/п	Дія	Команда

10. Перевірити дію заданих правил, звернувшись до ресурсу *Share1* із застосуванням облікового запису *student1*. Заповнити таблицю.

№з/п	Дія	Команда

11. Створити розподілений ресурс *Share2* на віддаленому комп’ютері (за вказівкою викладача). Задати правила повного доступу до нього для групи *Адміністратори* і доступу для читання для облікового запису користувача *student2*. Заповнити таблицю.

№з/п	Дія	Команда

12. Перевірити дію заданих правил, звернувшись до ресурсу Share2 із застосуванням облікових записів *root* і *student1*. Заповнити таблицю.

№з/п	Дія	Команда

Висновок:

В ході лабораторної роботи мною було засвоєно навички на практиці по створеню спільних локальниї мережевих ресурсів й обмежувати доступ до них.

Лабораторна робота №4

Тема.*Конфігурування. сервера терміналів у ОС Microsoft Windows Server 2003*

Мета роботи: оволодіти практичними навичками управління сервером терміналів у ОС Windows Server 2003.

1. Додати до консолі ММС оснащення *Служба терміналів* і *Диспетчер служб терміналів.* Заповнити таблицю.

№з/п	Дія	Команда

2. Задати максимальну кількість з'єднань із сервером терміналів, що дорівнює двом. Заповнити таблицю.

№з/п	Дія	Команда

3. Встановити три одночасних з'єднання із сервером. Для реєстрації в системі використати облікові записи *root, student1, student2*. Заповнити таблицю.

№з/п	Дія	Команда

4. Послідовно встановити з'єднання із сервером та зареєструватися в системі під обліковими записами *root,student1, student2*. Заповнити таблицю.

№з/п	Дія	Команда

5. Для облікового запису *student2* встановити дозвіл реєстрації в системі через службу терміналів. Заповнити таблицю.

№з/п	Дія	Команда

6. Перевірити дію заданого параметра. Заповнити таблицю.

№з/п	Дія	Команда

7. Замість логіка і пароля, які передає клієнт, вказати реквізити облікового запису *student2*. Заповнити таблицю.

№з/п	Дія	Команда

8. Перевірити дію встановленого параметра. Заповнити таблицю.

№з/п	Дія	Команда

9.Отримати список поточних сесій. Надіслати користувачеві*student2*повідомлення про завершення сеансу через 2 хвилини. Завершити сеанс роботи користувача з обліковим записом *student2*.

10.Визначити такі часові параметри сервера терміналів:

- ✓ завершення вимкненого сеансу через 3 хвилини;
- ✓ обмеження тривалості сеансу — 5 хвилин;
- ✓ завершення сеансу у випадку перевищення кількості одночасних з'єднань або при розриві підключення.

Заповнити таблицю.

№з/п	Дія	Команда

11. Перевірити дію заданих параметрів. Заповнити таблицю.

№з/п	Дія	Команда

12. Задати такі параметри клієнта сервера терміналів:

- ✓ глибина кольору —16 біт;
- ✓ роздільна здатність екрана — 1024x768 пікселів.

Заповнити таблицю.

№з/п	Дія	Команда

13. Перевірити дію заданих параметрів. Заповнити таблицю.

№з/п	Дія	Команда

14. Задати програму *Блокнот (Notepad)* як середовищесеансівсервера терміналів. Заповнити таблицю.

№з/п	Дія	Команда

15. Перевірити дію заданого параметра. Заповнити таблицю.

№з/п	Дія	Команда

16. Налаштувати сервер терміналів для віддаленого управління сеансами.

Заповнити таблицю.

№з/п	Дія	Команда

Висновок:

В ході практичної роботи мною було засвоєнно практичні навички управління сервером терміналів у ОС Windows Server 2003.

Лабораторна робота №5

Тема.*Робота з обліковими записами користувачів ОС Linux*

Мета роботи: оволодіти практичними навичками управління обліковими записами користувачів у ОС Linux.

1.Отримати системну допомогу для вказаних команд. Заповнити таблицю.

	Команда	Призначення
	adduser	
	passwd	
	userdel	
	groupadd	
	usermod	

2. Додати нові облікові записи користувачів *student1*і*student2*, створити для них пароль. Заповнити таблицю.

№з/п	Дія	Команда

4. У файлах */etc/passwd*та */etc/group* знайти записи, які стосуються користувачів *student1* і *student2*. Заповнити таблицю.

№з/п	Команда	Результат

5. Зареєструватися в системі з використанням реєстраційних даних облікового запису *student1*. Змінити пароль користувача *student1*. Змінити паролі користувачів *student1* і*student2*. Заповнити таблицю.

№з/п	Дія	Команда

6.Додати новий обліковий запис користувача *st_no_ home*, задавши для нього файл */dev/null* як домашній каталог. Створити пароль для облікового запису *st_no_ home*. Заповнити таблицю.

№з/п	Дія	Команда

7.Зареєструватися в системі з використанням реєстраційних даних створеного облікового запису. Пояснити результат.

8.Додати новий обліковий запис користувача *st_no_ shell*, задавши для нього файл */bin/false* як командний інтерпретатор. Створити пароль для облікового запису *st_no_ shell*. Заповнити таблицю.

№з/п	Дія	Команда

9.Зареєструватися в системі з використанням реєстраційних даних створеного облікового запису. Пояснити результат.

10.Призупинити дію облікового запису*student2*. Заповнити таблицю.

№з/п	Дія	Команда

11.Зареєструватися в системі з використанням реєстраційних даних облікового запису *student2*. Пояснити результат.

12.Відновити дію облікового запису *student2*. Заповнити таблицю.

№з/п	Дія	Команда

13. Створити обліковий запис групи користувачів *students*. Додати облікові записи користувачів *student1* і *student2* в групу *students*. Заповнити таблицю.

№з/п	Дія	Команда

14. Визначити ідентифікаційні номери облікових записів користувачів *student1* і *student2* та групи *students*. Заповнити таблицю.

№з/п	Обліковий запис	Ідентифікаційний номер

15. Створити каталог */home/st_no_home*. Встановити власником створеного каталогу користувача з обліковим записом *st_no_home*.

Встановити каталог */home/st_no_home*для облікового запису користувача *st_no_home*. Заповнити таблицю.

№з/п	Дія	Команда

16.Перевірити дію встановлених параметрів, зареєструвавшись під обліковим записом користувача *st_no_home*.

17.Встановити файл*/bin/bash*, командним інтерпретатором для облікового запису користувача*st_no_home*. Заповнити таблицю.

№з/п	Дія	Команда

18.Перевірити дію встановленого параметра.

19.Перейменувати облікові записи користувачів *st_no_bash* і *st_no_ home* в *stl*

і *st2* відповідно. Заповнити таблицю.

№з/п	Дія	Команда

20. Видалити обліковий запис користувача*st2* разом з його домашнім каталогом. Заповнити таблицю.

№з/п	Дія	Команда

Контрольні запитання

1.Які проблеми виникають із реєстрацією користувачів, якщо при створенні їх облікових записів були застосовані параметри *-s, -h*?

2.Як змінюється вміст файлів */etc/passwd* та */etc/shadow* при застосуванні команд *useradd, passwd, usermod, userdel*.

3.Як визначається обліковий запис групи за замовчуванням у команді *useradd* та у файлі */etc/passwd*?

4.За яких умов неможливо призупинити використання облікового запису?

Лабораторна робота №6

Тема. ***Налаштування правил доступу до об'єктів файлової системи ОС Linux***

Мета роботи: оволодіти практичними навичками інтерпретації прав доступу і використання команд ОС Linux для зміни прав доступу, власника файлів і каталогів.

1. Визначити власника, групу і правила доступу для файлів каталогів, наведених у таблиці. З'ясувати причини обмеження доступу до вказаних папок. Заповнити таблицю.

Каталог	Власник	Група	Правила доступу
/bin			
/etc			
/home			
/etc/passwd			
/etc /shadow			
/root			

2. У домашньому каталозі створити каталог *test*. У каталозі *test* створити файл *file.tst*. Визначити правила доступу і власника створених об'єктів файлової системи. Заповнити таблицю.

№з/п	Дія	Команда

3.Зареєструватися в системі з використанням реєстраційних даних облікового запису*student1*. У каталозі */tmp*створити каталог *test1*. У каталозі*test1* створити файл *filel.tst*. Визначити правила доступу і власника створених об'єктів файлової системи. Заповнити таблицю.

№з/п	Команда	Результат

4. Задати правила доступу 444 до каталогу */tmp/test1*. Перейти в каталог *testl*. Пояснити результат. Заповнити таблицю.

№з/п	Дія	Команда

5. Зареєструватися в системі з використанням реєстраційних даних облікового запису *student1*. Задати правила доступу 700 до каталогу */tmp/test*. Перейти в каталог*test1*. Пояснити результат. Заповнити таблицю.

№з/п	Дія	Команда

6. Зареєструватися в системі з використанням реєстраційних даних облікового запису *student2*. Перейти в каталог */tmp/testl*. Пояснити результат.

7.Зареєструватися в системі з використанням реєстраційних даних облікового запису *root*. Встановити власником каталогу */tmp/test1* обліковий запис *student2*. Заповнити таблицю.

№з/п	Дія	Команда

8.Зареєструватися в системі з використанням реєстраційних даних облікового запису *student2*. Перейти в каталог */tmp/test1*. Створити в каталозі */tmp/test1* каталог *test2*. Перейменувати файл *filel.tst* і файл *file2.tst*. Пояснити результат.

9. Зареєструватися в системі з використанням реєстраційних даних облікового запису *root*. Встановити власником каталогу */tmp/test1*, його підкаталогів і файлів обліковий запис *student1*. Перевірити коректність налаштувань. Заповнити таблицю.

№з/п	Дія	Команда

10. Для каталогу */tmp/test1/test2* встановити режим запису лише для облікових записів *student1* і *student2*. Заповнити таблицю.

№з/п	Дія	Команда

11. Перевірити дію заданих правил, послідовно зареєструвавшись під обліковими записами *st1, student1 і student2*.

Контрольні запитання

1. Чи завжди власник має право доступу до об’єктів файлової системи?

2. Як забезпечити одночасний доступ до файла (папки) кільком обліковим записам?

3.Що відбудеться, якщо до файла */bin/bash* встановити права 4755?

Лабораторна робота №7

Тема. ***Створення розподілених ресурсів засобами сервера NFS***

Мета роботи: оволодіти практичними навичками експортування і

монтування каталогів за допомогою мережної файлової системи.

1. У каталозі */tmp* створити каталог *export_dir*. Задати права доступу для читання та перегляду каталогу *export _dir* власником, групою й іншими обліковими записами. Заповнити таблицю.

№з/п	Дія	Команда або параметр конфігурації

2.У файлі конфігурації сервера NFS визначити каталог*/tmp/export_dir*, як загальнодоступний з такими параметрами:

- ✓ доступ лише для комп'ютера з певного IP-адресою (вказує викладач);
- ✓ синхронний режим виконання операцій читання (запису);
- ✓ доступ для читання і запису;
- ✓ не інтерпретувати запити від облікового запису *root* як адміністратора.

Завантажити сервер NFS. Заповнити таблицю.

№з/п	Дія	Команда або параметр конфігурації

3. Зареєструватися як адміністратор в системі комп'ютера, визначеного в попередньому завданні. Створити каталог */mnt/nfs*. Провести монтування спільного ресурсу *export_dir* у каталог */mnt/nfs*. Заповнити таблицю.

№з/п	Дія	Команда або параметр конфігурації

4.Спробувати створити файл у каталозі */mnt/nfs*. Пояснити результат.

5.У системі NFS-сервера змінити правила доступу до каталогу */tmp/export_dir* так, щоб забезпечити запис даних із віддаленого комп'ютера. Заповнити таблицю.

№з/п	Дія	Команда або параметр конфігурації

6.Перевірити коректність налаштувань, створивши файл у каталозі */mnt/nfs*із комп'ютера-кліента.

7.Провести монтування експортованого каталогу в каталог */mnt/nfs* комп'ютера, IP-адреса якого не вказана в конфігурації сервера NFS.

8.У системі NFS-сервера змінити правила доступу до каталогу і */tmp/export_dir*так, щоб забезпечити доступ з усіх комп'ютерів підмережі.

Заповнити таблицю.

№з/п	Дія	Команда або параметр конфігурації

9. Зареєструватися як адміністратор в системі будь-якого комп'ютера підмережі. Створити каталог */mnt/nfs*. Провести монтування спільного ресурсу *export_dir*у каталог */mnt/nfs*. Перевірити доступність ресурсу для читання та запису. Заповнити таблицю.

№з/п	Дія	Команда або параметр конфігурації

10.У каталозі */tmp/export_dir* сервера NFS створити каталог *subdir*. Задати такі правила доступу до каталогу *tmp/export_dir/subdir*:

- ✓ власник — читання, запис і виконання;
- ✓ група — читання;
- ✓ інші облікові записи — читання, запис і виконання.

Заповнити таблицю.

№з/п	Дія	Команда або параметр конфігурації

11. У файлі конфігурації сервера визначити каталог */tmp/export_dir/subdir*, як загальнодоступний з наступними параметрами:

- ✓ доступ лише для комп'ютерів з підмережі;
- ✓ синхронний режим виконання операцій читання (запису);
- ✓ доступ лише для читання.

Заповнити таблицю.

№з/п	Дія	Команда або параметр конфігурації

12.Зареєструватися як адміністратор в системі будь-якого комп'ютера підмережі. Створити каталог */mnt/nfs*. Провести монтування спільного ресурсу *subdir* у каталог */mnt/nfs*. Перевірити доступність ресурсу для читання і запису.

№з/п	Дія	Команда або параметр конфігурації

13.Змінити параметри сервера так, щоб можна було проводити запис у каталог *subdir*. Перевірити доступність ресурсу для читання і запису.

14.Відмотувати всі експортовані каталоги.

15.Змінити параметри експортування каталогу */tmp/export_dir_N*так, щоб заборонити доступ до каталогу *subdir*. Заповнити таблицю.

№з/п	Дія	Команда або параметр конфігурації

16.Зареєструватися як адміністратор в системі будь-якого комп'ютера підмережі. Провести монтування спільного ресурсу *subdir* у каталог */mnt/nfs*. Пояснити результати.

Контрольні запитання

1.Чому для забезпечення запису засобами сервера NFS потрібно у правилах доступу файлової системи Ext3 вказувати режим запису для усіх облікових записів?

2.Чи можна налаштувати доступ до експортованого каталогу так, щоб через мережу існував доступ для запису, а локально — ні?

3.Які відомості повинен повідомити адміністратор NFS-сервера клієнтам після створення спільного ресурсу?

Лабораторна робота №8

Тема. ***Створення та адміністрування домену Active Directory.***

Мета роботи: оволодіти практичними навичками встановлення служби Active Directory й управління її об'єктами.

1.Налаштувати сервер, з яким Ви працюєте, для виконання функцій контролера домену (N — номер комп'ютера, за яким Ви працюєте). Утворити новий простір імен, створивши кореневий домен з іменем *domainN.ua* (NetBIOS-ім'я домену—domainN). Заповнити таблицю.

№з/п	Дія	Екранна копія

2. Додати два сусідніх комп'ютери до складу створеного домену. Заповнити таблицю.

№з/п	Дія	Екранна копія

3. У домені *domainN.ua* створити організаційні одиниці *Співробітники* і *Студенти*. Заповнити таблицю.

№з/п	Дія	Екранна копія

4.В організаційній одиниці *Співробітники* створити обліковий запис *teacher1* користувача Романа Петренка, а в організаційній одиниці *Студенти* — обліковий запис *student1* користувача Олени Тимочко. Паролі вибрати самостійно. Заборонити користувачу Олені Тимочко змінювати пароль, а Роману Петренку передбачити необхідність зміни пароля під час наступної реєстрації в домені. Заповнити таблицю.

№з/п	Дія	Екранна копія

5. Змінити пароль облікового запису *student1* і призначити термін дії пароля до 31 грудня цього року, дозволити вхід в систему з 08 до 18 години. Заповнити таблицю.

№з/п	Дія	Екранна копія

6. Створити облікові записи груп користувачів *teachers* і *students*. Додати до складу групи користувачів *Співробітники* обліковий запис користувача *teacher1*, а в групу *Студенти* — обліковий запис користувача *student1*.

Заповнити таблицю.

№з/п	Дія	Екранна копія

7.На системному диску створити папки *Profiles і Disks*. Папки *Profiles і Disks* зробити загальнодоступними мережними ресурсами і надати для них правила автоматичного створення папок групою *teachers* (див. завдання 19 лабораторної роботи №2), а також правила повного доступу для групи *Адміністратори*. Для облікового запису *teacher1* вказати для зберігання переміщуваного профілю мережний маршрут до папки *Staff\teacher1*, а мережний диск *Z* приєднати до мережного маршруту *Disks\teacher1*. Заповнити таблицю.

№з/п	Дія	Екранна копія

8.Перевірити правильність виконаних дій, послідовно зареєструвавшись із застосуванням облікових даних користувачів Олена Тимочко та Роман Петренко.

9.У підрозділі *Співробітники* для користувача Володимира Коршака створити обліковий запис *teacher2*, скопіювавши його з облікового запису *teacher1*. Встановити пароль для створеного облікового користувача. Додати обліковий запис до групи *teachers*. Заповнити таблицю.

№з/п	Дія	Екранна копія

10.Перевірити правильність функціонування переміщуваних профілів користувачів з групи *teachers*, послідовно зареєструвавшись в системі приєднаних до домену комп'ютерів.

11.Обліковому запису групи *teachers* делегувати повноваження на рівні домену *domainN.ua* для виконання операцій приєднання комп'ютерів до цього домену. Заповнити таблицю.

№з/п	Дія	Екранна копія

12.Перевірити правильність виконаних дій, приєднавши ще один комп'ютер до домену, використовуючи обліковий запис користувача з групи *teachers*.

13.Для контейнера домену змінити правила групової політики безпеки так,

щоб мінімальна довжина пароля дорівнювала трьом символам. Для цього ж контейнера вимкнути вимогу складності стосовно паролів користувачів. Заповнити таблицю.

№з/п	Дія	Екранна копія

14.Перевірити правильність виконаних дій, змінивши пароль для облікового запису *teacher*2.

15.Для контейнера *Контролери домену* задати правила політики безпеки, які б дозволяли реєстрацію в системі контролера домену групі*teachers*. Заповнити таблицю.

№з/п	Дія	Екранна копія

16. Обліковому запису групи користувачів *teachers* делегувати повноваження, необхідні для створення, зміни облікових записів користувачів і груп та зміни паролів підрозділу *Студенти*. Заповнити таблицю.

№з/п	Дія	Екранна копія

17. Використовуючи обліковий запис *teacher2*, зареєструватися в системі контролера домену і змінити пароль для облікового запису *student1*. Заповнити таблицю.

№з/п	Дія	Екранна копія

18. Для контейнера домену змінити правила групової політики безпеки стосовно браузера Internet Explorer. У правилі політики безпеки визначити адресу проксі-сервера — 10.1.1.100 та порт — 3128. Заповнити таблицю.

№з/п	Дія	Екранна копія

19. Для контейнера *Співробітники* змінити правила групової політики безпеки стосовно браузера Internet Explorer. У правилі політики безпеки визначити адресу проксі-сервера —10.41.1.100 і порт — 3128. Заповнити таблицю.

№з/п	Дія	Екранна копія

20. Перевірити, як перекриваються задані правила політики безпеки. Змінити параметри політики, щоб правила контейнера переозначували (не переозначували) відповідні правила домену. Заповнити таблицю.

№з/п	Дія	Екранна копія

21.Змінити значення параметрів об’єктів групової політики підрозділу *Співробітники* так, щоб перенаправити розміщення папок *Робочий Стіл* і *Мої документи* в каталоги *Desktop* та *MyDOCs* мережного диска *Z*.

22.Перевірити правильність виконаних дій, зареєструвавшись із застосуванням облікових записів користувачів підрозділу *Співробітники*. Заповнити таблицю.

№з/п	Дія	Екранна копія

Контрольні запитання

1.Чи можлива ситуація, за якої той самий об’єкт Active Directory буде належати різним підрозділам?

2.У чому відмінність між копіюванням облікового запису користувача і створенням нового?

3.Як можна дозволити реєстрацію користувача з певним обліковим записом у системі лише деяких комп’ютерів домену?

4.Як можна делегувати повноваження на приєднання комп’ютера до домену стосовно певної групи комп’ютерів?

5.У чому перевага перенаправлення папок перемішуваного профілю безпосередньо в каталог мережного ресурсу?

Лабораторна робота №9

Тема. ***Створення домену засобами сервера NIS***

Мета роботи: оволодіти практичними навичками створення й адміністрування централізованої бази облікових записів користувачів за допомогою служби NIS.

1.Встановити сервер мережної інформаційної служби — пакет*ypserv*.

2. Створити обліковий запис групи*domainusers*. Змінити ідентифікаційний номер групи на число 600. Заповнити таблицю.

№з/п	Дія	Команда або параметр конфігурації

3. Створити облікові записи користувачів: *student1, student2, student3.* Додати їх до групи *domainusers.* Встановити паролі для облікових записів *student1, student2, student3*. Заповнити таблицю.

№з/п	Дія	Команда або параметр конфігурації

4. Змінити числові ідентифікатори облікових записів *student1, student2, student3* на 701, 702, 703 відповідно. Заповнити таблицю.

№з/п	Дія	Команда або параметр конфігурації

5. Задати назву нового NIS-домену *domainN.ua* (N— номер комп'ютера, за яким Ви працюєте). Заповнити таблицю.

№з/п	Дія	Команда або параметр конфігурації

6. У файлі конфігурації сервера NIS створити запис, за яким довільний комп'ютер Вашої підмережі можна приєднати до домену domainN.ua. Заповнити таблицю.

№з/п	Дія	Команда або параметр конфігурації

7. Провести ініціалізацію бази даних первинного сервера NIS. Завантажити сервер на виконання. Заповнити таблицю.

№з/п	Дія	Команда або параметр конфігурації

8. Приєднати два сусідніх комп'ютери до домену. Заповнити таблицю.

№з/п	Дія	Команда або параметр конфігурації

9.Зареєструватися в системі приєднаного до домену комп’ютера.

10.У системі NIS-сервера за допомогою сервера мережної файлової системи зробити загальнодоступним каталог */home* з такими параметрами:

- ✓ доступ лише для власної підмережі;
- ✓ синхронний режим виконання операцій читання (запису);
- ✓ доступ для читання і запису;
- ✓ не інтерпретувати обліковий запис *root* як суперкористувача. Завантажити сервер NFS.

Заповнити таблицю.

№з/п	Дія	Команда або параметр конфігурації

11. Приєднати спільний ресурс */home* до каталогу */home*. Заповнити таблицю.

№з/п	Дія	Команда або параметр конфігурації

12. Послідовно зареєструватися в системі комп’ютерів домену. Перевірити можливість запису даних у домашній каталог і функціонування профілю. Заповнити таблицю.

№з/п	Дія	Команда або параметр конфігурації

Контрольні запитання

1.Які проблеми виникають при реєстрації користувачів у домені NIS? Чому так відбувається?

2.Опишіть послідовність дій щодо створення нового облікового запису користувача домену NIS.

3.У який спосіб можна забезпечити приєднання лише певних комп’ютерів до домену NIS?

4.Чому після приєднання каталогу /home не доводиться змінювати правила доступу до об’єктів файлової системи Ext-3?

5.Чи можна назвати профілі облікових записів домену NIS переміщуваними?

6.У чому відмінність профілів, створених у домені NIS, від профілів домену Active Directory?

Лабораторна робота №10

Тема. ***Створення дожену засобами сервера Samba***

Мета роботи: оволодіти практичними навичками адміністрування домену, функції контролера якого виконує сервер Samba.

1.Встановити сервер Samba.

2.Створити облікові записи, що відповідають іменам комп'ютерів, які будуть додані в домен. Провести редагування файла /etc/passwd, додавши до імен комп'ютерів символ долара «$». Заповнити таблицю.

№з/п	Дія	Команда або параметр конфігурації

3. Додати до бази даних сервера Samba облікові записи комп'ютерів і облікові записи користувачів *student1, student2, root* (адміністратора домену). Заповнити таблицю.

№з/п	Дія	Команда або параметр конфігурації

4.Встановити такі параметри сервера Samba:

- ✓ назва домену — domainN.ua;
- ✓ використання бази облікових записів користувачів ОС Linux;
- ✓ виконання сервером функції переглядача домену;
- ✓ виконання сервером функції контролера домену;
- ✓ можливість користувачів входити в домен.

Заповнити таблицю.

№з/п	Дія	Команда або параметр конфігурації

5.У конфігурації сервера Samba описати такі ресурси:

- ✓ домашній каталог кожного користувача;
- ✓ каталог *pub* для сумісного читання і запису користувачів домену;
- ✓ каталог із профілями користувачів розмістити в */home/profiles*;
- ✓ для комп'ютерів з ОС Windows каталог *Profiles* повинен бути доступний за мережною адресою *\\server\Profiles*;
- ✓ спільний ресурс *Profiles* має бути недоступним для читання, але доступним для запису профілів відповідних користувачів.

Заповнити таблицю.

№з/п	Дія	Команда або параметр конфігурації

6.Розглядаючи каталог */home/profiles* як об’єкт файлової системи Ext3, задати такі правила доступу до нього, які б забезпечували запис профілів.

7.Завантажити сервер Samba. Заповнити таблицю.

№з/п	Дія	Команда або параметр конфігурації

8. Додати два сусідніх комп’ютери до складу створеного домену. Заповнити таблицю.

№з/п	Дія	Екранна копія

9. Перевірити коректність реєстрації облікових записів користувачів *student1 і student2* у домені. Перевірити доступність їхніх мережних дисків. Заповнити таблицю.

№з/п	Дія	Екранна копія

10. Перевірити правильність функціонування спільного ресурсу *pub*. Заповнити таблицю.

№з/п	Дія	Екранна копія

Контрольні запитання

1.У чому відмінність приєднання комп’ютера до доменів Active Directory, NIS, Samba?

2.Як безпечно організувати доступ до каталогу із профілями облікових записів користувачів */home/profiles*?

3.Як у файлі описують параметри, що містять назви різних облікових записів?

4.Чи можна засобами сервера Samba забезпечити доступ до ресурсу для запису, заборонивши при цьому його зчитування?

5.Чи повинно збігатися ім’я сервера Samba з іменем в ОС Linux?

Лабораторна робота №11

Тема. ***Створення веб-сервера засобами служби IIS***

Мета роботи: оволодіти практичними навичками адміністрування веб-сервера і віртуальних веб-вузлів за допомогою служби IIS.

1.Перевірити наявність веб-сервера серед складових сервера IIS. Якщо компонент не встановлений, то його інсталювати.

2.Задати такі параметри веб-вузла за замовчуванням:

- ✓ DNS-ім'я вузла вказує викладач;
- ✓ використання всіх ЕР-адрес, які вказані в мережних з'єднаннях ОС;
- ✓ опрацювання запитів за портом номер 80 протоколу TCP;
- ✓ запис запитів клієнтів у журнал.

Заповнити таблицю.

№з/п	Дія	Команда або екранна копія

3. Перевірити наявність з'єднання із сервером, використовуючи утиліту *telnet* та браузер. Заповнити таблицю.

№з/п	Дія	Команда або екранна копія

4. Переглянути журнал веб-вузла. Заповнити таблицю.

Дата	Запис журналу	Опис

5.Задати такі параметри швидкодії веб-вузла за замовчуванням:

- ✓ максимальна швидкість передавання даних веб-вузлом — 1024 біт/с;
- ✓ максимальна кількість одночасних з'єднань — 3.

Перевірити значення заданих параметрів, розмістивши в домашньому каталозі веб-вузла файл обсягом більшим за 50 Мб. Заповнити таблицю.

№з/п	Дія	Екранна копія

6.Визначити індексними документами веб-вузла такі файли: *index.html, index.htm, default.htm, iisstart.htm* та *default.asp.*

7.Вказати параметри домашнього каталогу веб-вузла за замовчуванням:

- ✓ розміщення домашнього каталогу в папці *%systemdrive%:\ interpub\wwwroot*, де *%systemdrive%* — системний диск;

- ✓ режими доступу до домашнього каталогу — читання, перегляд каталогів.

Перевірити встановлені параметри за допомогою звертання до каталогу без індексного файла. Заповнити таблицю.

№з/п	Дія	Екранна копія

8. Налаштувати веб-вузол на опрацювання запитів клієнтів з Вашої підмережі, за винятком одного комп'ютера (за вказівкою викладача). Перевірити встановлені параметри і заповнити таблицю.

№з/п	Дія	Екранна копія

9.Налаштувати веб-вузол за замовчуванням для інтегрованої автентифікації Windows. У домашньому каталозі веб-вузла створити каталоги *pub* та *auth*. До каталогу *pub* надати доступ через веб-сервер для довільного облікового запису. До каталогу *auth* надати доступ через веб-сервер облікового запису користувача *student1*і групи *Адміністратори*. Перевірити встановлені параметри і заповнити таблицю.

№з/п	Дія	Екранна копія

10. Створити віртуальний веб-вузол з DNS-іменем, яке вкаже викладач. Вузол повинен обслуговувати запити за всіма IP-адресами сервера і номером порту 81. Перевірити параметри та заповнити таблицю.

№з/п	Дія	Екранна копія

11. Створити віртуальний веб-вузол з DNS-іменем, яке вкаже викладач. Вузол повинен обслуговувати запити за всіма IP-адресами сервера та номером порту 80. Перевірити параметри та заповнити таблицю.

№з/п	Дія	Екранна копія

Контрольні запитання

1.Як потрібно вибирати DNS-ім'я веб-вузла?

2.Які параметри впливають на продуктивність веб-сервера?

3.Як створити веб-сайт, який використовує ту саму IP-адресу і порт, що й

інший веб-сайт?

Лабораторна робота №12

Тема. ***Робота з веб-сервером Apache***

Мета роботи: оволодіти практичними навичками адміністрування веб-сервера Apache.

1.Перевірити, чи встановлений веб-сервер Apache в ОС Linux. За потреби інсталювати його.

2.Встановити такі параметри веб-сервера:

- ✓ ім’я сервера — за вказівкою викладача;
- ✓ поштова адреса адміністратора сервера — адреса Вашої елек-тронної скриньки;
- ✓ опрацювання запитів, які надходять на всі IP-адреси сервера, на порт з номером 80;

У кореневий каталог документів — папка /var/www/wwwroot. Заповнити таблицю.

№з/п	Дія	Команда або параметр конфігурації

3. Перевірити коректність заданих параметрів. Заповнити таблицю.

№з/п	Дія	Команда або параметр конфігурації

4.Задати такі параметри продуктивності сервера Apache:

- ✓ максимальна та мінімальна кількість копій сервера, які завантажуються до оперативної пам’яті — 5 і 2 відповідно;
- ✓ час очікування з’єднання — 450 секунд;
- ✓ максимальна кількість одночасних з’єднань із сервером — 15.

Заповнити таблицю.

№з/п	Дія	Команда або параметр конфігурації

5. Перевірити коректність заданих параметрів. Заповнити таблицю.

№з/п	Дія	Команда або параметр конфігурації

6.Задати такі параметри доступу до папок веб-сервера:

- ✓ індексні файли — *index.html, index.php, index.htm, main.html*;
- ✓ заборона виведення вмісту кореневого каталогу документів;

- ✓ опрацювання файлів з каталогів користувачів; у домашньому каталозі користувача каталог з документами повинен мати назву public_html;
- ✓ заборона доступу до файлів *.htaccess*і *.htpasswd* для всіх клієнтів.

Заповнити таблицю.

№з/п	Дія	Команда або параметр конфігурації

7. Перевірити коректність заданих параметрів. Заповнити таблицю.

№з/п	Дія	Команда або екранна копія

8.У кореневому каталозі документів створити папки *access1 і access2.*

9.Задати такі параметри доступу до папок веб-сервера:

- ✓ можливість переозначення параметрів доступу в файлах *.htaccess* для кореневого каталогу;
- ✓ дозвіл на доступ до каталогу *access1* лише для клієнта з визначеною IP-адресою; усі інші комп'ютери до каталогу *access1* не мають доступу;
- ✓ доступ до каталогу access2 засобами автентифікації сервера; дані про облікові записи користувачів і їх паролі потрібно зберігати в каталозі *access2*, у файлі *.htpasswd.*

Заповнити таблицю.

№з/п	Дія	Команда або параметр конфігурації

10. Перевірити коректність заданих параметрів. Заповнити таблицю.

№з/п	Дія	Команда або екранна копія

11.Задати такі параметри ведення журналу веб-сервера:

- ✓ шлях до журналу, який містить діагностичні записи та повідомлення про помилки, — */var/log/httpd-error.log*;
- ✓ шлях до журналу, який містить дані про запити клієнтів, — */var/log/httpd-transfer.log*;
- ✓ реєстрація у журналі IP-адрес клієнтів, а не їх доменних імен.

Заповнити таблицю.

№з/п	Дія	Команда або параметр конфігурації

12. Переглянути журнал веб-вузла. Заповнити таблицю.

13. Створити віртуальний веб-вузол з DNS-іменем, яке вкаже викладач. Параметри веб-вузла задати такі:

- ✓ опрацювання запитів за всіма IP-адресами сервера та номером порту 80;
- ✓ каталог документів — */var/www/vhosts/<DNS- ім'я веб-вузла>;*
- ✓ шлях до журналів віртуального веб вузла — */var/log/<DNS-імя веб-вузла>*.

Заповнити таблицю.

№з/п	Дія	Команда або параметр конфігурації

14. Перевірити коректність встановлених параметрів. Заповнити таблицю.

№з/п	Дія	Команда або екранна копія

Контрольні запитання

1.Чи дорівнює значення директиви *MaxClients* максимальній кількості браузерів клієнтів?

2.Яка директива дає можливість серверу *Apache* виділяти запити до різних віртуальних веб-вузлів, якщо вони надходять на ту саму IP-адресу і порт?

3.У чому відмінність між параметрами *MaxClients* і *MaxSpareServers*?

4.Якщо директиви, які зазначені у файлі *.htaccess* суперечать одна одній, то яке правило буде виконуватися?

Лабораторна робота 13

Тема. ***Створення FTP-сервера засобами служби IIS***

Мета роботи: оволодіти практичними навичками створення й адміністрування FTP-сервера та віртуальних FTP-вузлів за допомогою служби IIS.

1.Перевірити наявність FTP-сервера серед складових сервера IIS. Якщо компонент не встановлений, то інсталювати його.

2.Задати такі параметри FTP-вузла за замовчуванням:

- ✓ використання всіх IP-адрес, які вказані в мережних з'єднаннях ОС;
- ✓ опрацювання запитів за портом з номером 21 протоколу TCP;
- ✓ максимальна кількість одночасних з'єднань — 3;
- ✓ запис запитів клієнтів у журнал.

Заповнити таблицю.

№з/п	Дія	Команда або екранна копія

3. Перевірити наявність з'єднання із сервером, використовуючи утиліту *telnet* та FTP-клієнт у активному і пасивному режимі. Переглянути поточні сеанси клієнтів сервера. Заповнити таблицю.

№з/п	Дія	Команда або екранна копія

4. Переглянути журнал FTP-вузла. Заповнити таблицю.

№з/п	Запис журналу	Опис

5.Вказати параметри домашнього каталогу FTP-вузла за замовчуванням:

- ✓ розміщення домашнього каталогу в папці *%systemdrive%:\ interpub\ftproot*, де *%systemdrive%* — системний диск;
- ✓ режими доступу до домашнього каталогу — читання, запис.

Перевірити задані параметри. Заповнити таблицю.

№з/п	Дія	Екранна копія

6. Налаштувати FTP-вузол на опрацювання запитів одного комп'ютера (за вказівкою викладача). Перевірити задані параметри і заповнити таблицю.

№з/п	Дія	Екранна копія

7. У домашньому каталозі FTP-вузла створити каталоги *pub* та *auth*. До каталогу *pub* надати доступ через FTP-сервер для анонімного облікового запису. До каталогу *auth* надати доступ через веб-сервер облікового запису користувача *student1* і групи *Адміністратори*. Перевірити встановлені параметри та заповнити таблицю.

№з/п	Дія	Екранна копія

8.Створити віртуальний FTP-вузол з DNS-іменем, яке вкаже викладач. Вузол повинен обслуговувати запити за всіма IP-адресами сервера і номером порту 2121.

9.Домашній каталог FTP-вузла розмістити у папці *%systemdrive%:\ temp*, до якого надати доступ лише для читання обліковому запису *student2*. Перевірити задані параметри та заповнити таблицю.

№з/п	Дія	Команда або параметр конфігурації

Контрольні запитання

1.Чому не можна створити FTP-вузол, який використовує ту саму IP-адресу і порт, що й інший FTP-вузол?

2.Чому в службі IIS немає налаштувань стосовно пасивного режиму FTP-сервера?

3. Як заборонити доступ до FTP-вузла для певного облікового запису користувача або групи?

Лабораторна робота №13

Тема. ***Створення FTP – сервера засобами служби***

Мета роботи: оволодіти практичними навичками створення й адміністрування FTP - сервера та віртуальних вузлів за допомогою службиIIS.

1.Перевірити наявністьFTP– сервера серед складових сервераIIS. Якщо компонент не встановлений, то інсталювати його.

2. Здати такі параметри FTP - вузла за замовчуванням:

- ✓ Використання всіх IP–адрес, які вказані в мережних з'єднаннях ОС;
- ✓ Опрацювання запитів за портом з номером 21 протоколуTCP;
- ✓ Максимальна кількість одночасних з'єднань -3;
- ✓ Запис запитів клієнтів у журнал.

Заповнити таблицю

№ з\п	Дія	Команда або екранна копія

3.Перевірити наявність з'єднання із сервером, використовуючи утилітуtelnet та FTPклієнт у активному і пасивному режимі. Переглянути поточні сеанси клієнтів сервера. Заповнити Таблицю.

№ з\п	Дія	Команда або екранна копія

4. Переглянути журнал вузла. Заповнити таблицю.

Дата	Запис журналу	Опис

5.Вказати параметри домашнього каталогу FTP-вузла за замовчуванням:

- ✓ Розміщення домашнього каталогу в папці – *%systemdrive%:\interpub\ftroot,* де *%systemdrive%* - системний диск;
- ✓ Режими доступу до домашнього каталогу – читання, запис.

Перевірити задані параметри. Заповнити таблицю

№ з\п	Дія	Екранна копія

6.Налаштувати FTP– вузол на опрацювання запитів одного комп'ютера(за

вказівкою викладача). Перевірити задані параметри і заповнити таблицю.

№ з\п	Дія	Екранна копія

7. У домашньому каталозі FTP– вузла створити каталоги *pub*taauth . До каталогу *pub*надати доступу через FTP– сервер для анонімного облікового запису. До каталогу*auth* надати доступ через веб - сервер облікового запису користувача*student1* і групи *Адміністратори*. Перевірити встановлені параметри та заповнити таблицю.

№ з\п	Дія	Екранна копія

8. Створити віртуальний FTP–вузол з DNS-іменем, яке вкаже викладач. Вузол повинен обслуговувати запит за всіма IP - адресами сервера і номером порту 2121,

9.Домашній каталог FTP–вузла розмістити у папці*%systemdrive%*:\temp, до якого надати доступ лише для читання облікового запису*student2*. Перевірити задані параметри та заповнити таблицю.

№ з\п	Дія	Команда або параметр конфігурації

Контрольні запитання

1. Чому не можна створити FTP–вузол, який використовує ту саму IP-адресу і порт, що й інший FTP–вузол?
2. Чому в службі IISнемає налаштувань стосовно пасивного режимуFTP–сервера?
3. Як заборонити доступ до FTP–вузла для певного облікового запису користувача або групи?

Лабораторна робота № 14

Тема. ***Конфігурування сервера ProFTPD***

Мета роботи: Оволодіти практичними навичками адміністрування серверaProFTPD .

1.Перевірити наявність серверaProFTPD серед сервісів OCLinux.

Якщо компонент не встановлений, то інсталювати його. Заповнити таблицю.

№ з\п	Дія	Команда

2. Визначити такі параметри конфігурації сервера:

- ✓ Назва – за вказівкою викладача;
- ✓ Режим роботи – окремий демон;
- ✓ Максимальна кількість копій сервера, що завантажується до оперативної пам’яті, - 10;
- ✓ Авторизація лише облікових записів користувачів OCLinux.
- ✓ Для авторизації необов’язкова наявність командного інтерпретатора;
- ✓ Максимальна кількість одночасних авторизацій публічних користувачів – 5;
- ✓ Кореневий каталог кожного клієнта – його домашній каталог;
- ✓ Шлях до журналу сервера *–/var/log/proftpd/log;*
- ✓ Шлях до журналу передавання даних - */var/log/ftpd-transfer.log;*
- ✓ Передавання даних на інші FTP - сервера вимкнути;

Заповнити таблицю.

№ з\п	Дія	Команда або параметр конфігурації

3.Перевірити задані параметри, встановивши з’єднання із сервером з реєстраційними даними облікового записуstudent1. Заповнити Таблицю.

№ з\п	Дія	Команда або екранна копія

4.Задати параметри доступу анонімних користувачів:

- ✓ Дозвіл авторизації без пароля;
- ✓ Псевдонім анонімного користувача *–ftp;*

- ✓ Домашній каталог - */var/ftp;*
- ✓ Заборона запису даних на сервер

Заповнити таблицю.

№ з\п	Дія	Команда або параметр конфігурації

5.Перевірити задані параметри, зокрема передавання файлів у пасивному режимі. Заповнити таблицю.

№ з\п	Дія	Команда або екранна копія

6.Переглянути записи про авторизацію у журналі сервера. Заповнити таблицю.

Дата	Запис журналу	Опис

7.З журналу сервера отримати відомості про авторизацію користувачі. Заповнити Таблицю.

Дата	Запис журналу	Опис

8.Визначити спосіб авторизації користувачів на основі створених адміністратором файлів. Заповнити таблицю.

№ з\п	Дія	Команда або параметр конфігурації

9.За допомогою утиліти *ftpasswd*створити обліковий запис користувача з такими параметрами:

- ✓ Назва облікового запису – *ftpuser*;
- ✓ Числовий ідентифікатор -*1200*;
- ✓ Домашній каталог - */home/ftpuser1;*
- ✓ Командний інтерпретатор - */bin/true/*

Заповнити таблицю.

№ з\п	Дія	Команда

10. За допомогою утиліти *ftpasswd*створити обліковий запис групи

користувачів з такими параметрами:

- ✓ Назва облікового запису – *ftpgroup;*
- ✓ Числовий ідентифікатор – 1200;
- ✓ Члени групи – обліковий запис *ftpuser1*.

Заповнити таблицю.

№ з\п	Дія	Команда

11.Перевірити задані параметри, встановивши з'єднання із сервером з реєстраційними даними облікового запису*student1*. Заповнити таблицю.

№ з\п	Дія	Команда або екранна копія

12.Задати обмеження доступу до FTR - сервера лише з сусіднього комп'ютера і лише з використанням логіну *user*.

13.перевірити задані параметри. Заповнити таблицю.

№ з\п	Дія	Команда або екранна копія

Контрольні запитання

1. У чому відмінність між параметрами *MaxInstances і MaxClients*?
2. Чи є у файлі конфігурації сервера ProFTPDпараметри пасивного режиму?
3. У яких випадках потрібно застосовувати директиву *AuthOrder*?
4. Яке потрібно задати значення параметра*DefaultRoot* , щоб кореневим каталогом для користувачів був їхній домашній каталог?

Лабораторна робота №15

Тема. ***Конфігурування поштового сервера в ОС WindowsServer 2003***

Мета роботи: оволодіти практичними навичками адміністрування серверів електронної пошти в ОСWindowsServer 2003.

1.Перевірити наявність служб SMTPiPOP3 серед складових сервера. Якщо компоненти не встановлені, то інсталювати їх. Для сервера POP3 визначити метод перевірки, достовірності на основі файлу, що містить облікові записи користувачів разом із криптованими паролями. Заповнити таблицю.

№ з\п	Дія	Екранна копія

2.Створити віртуальнийSMTP- сервер, для якого за вказівкою викладача вказати:

- ✓ Ім’я поштового сервера;
- ✓ Ім’я домену, який обслуговуватиме віртуальний SMTP-сервер;
- ✓ Адреси, за якими сервер обслуговуватиме звернення клієнтів;
- ✓ Домашній каталог сервера – папка, до якої сервіс SMTPзаписуватиме повідомлення, що стосуються вказаного віртуального сервера.

Заповнити таблицю.

№ з\п	Дія	Екранна копія

3.Використовуючи утилітуtelnet ,перевірити зв’язок із сервером.

4.Налаштувати поштовий клієнт, у якому вказати:

- ✓ Власне прізвище та ім’я;
- ✓ Електронну пошту postmaster@<>;
- ✓ Адреси серверів SMTPi POP3;
- ✓ Логін і пароль доступу до сервера POP3.

Заповнити таблицю.

№ з\п	Дія	Екранна копія

5.Для створення віртуального SMTP- сервера визначити такі параметри роботи з листами:

- ✓ Обмеження обсягу повідомлення - 1мб;
- ✓ Обмеження кількості повідомлень для з'єднання - 3;
- ✓ Обмеження кількості одержувачів кожного повідомлення - 2;
- ✓ Надсилання копій звітів про неможливість доставки за адресою

Перевірити правильність налаштувань і заповнити таблицю.

№ з\п	Дія	Команда або екранна копія

6.Встановити обмеження доступу до сервера, яке стосується окремого комп'ютера. Перевірити дію налаштування і заповнити таблицю.

№ з\п	Дія	Екранна копія

7.Надати дозвіл для ретрансляції листів, які надходять від окремого комп'ютера мережі або самого сервераSMTP. Перевірити дію налаштування і заповнити таблицю.

№ з\п	Дія	Екранна копія

8.Створити віртуальний POP3 – сервер, для якого за вказівкою викладача вказати:

- ✓ Ім'я домену, який обслуговуватиме віртуальний SMTP- сервер;
- ✓ Каталог, в якому сервер зберігатимелист,- <systemdrive>\interpub\mailroot\<domainname>,де<systemdrive> - системний диск ,а <domainname> - DNS – ім'я домену;
- ✓ Максимальний рівень деталізації журналу.

№ з\п	Дія	Екранна копія

9.Створити такі облікові записи користувачів сервера POP3:postmaster, student1, student2.

Заповнити таблицю.

№ з\п	Дія	Команда або екранна копія

10.Змінити налаштування поштового клієнта, в якому вказати параметри

з’єднання до POP3 – сервера. Заповнити таблицю.

№ з\п	Дія	Команда або екранна копія

11.Надіслати листа за адресоюpostmaster@<domainname>.

12.Перевірити журнал сервераSMTP. Заповнити таблицю.

Дата	Запис журналу	Опис

13.Отримати надісланий лист. Заповнити таблицю

Дата	Запис журналу	Опис

14.Перевірити журнал сервераSMTP . Заповнити таблицю.

№ з\п	Дія	Екранна копія

15.Перевірити журнал сервера POP3. Заповнити таблицю.

Дата	Запис журналу	Опис

16.Надіслати листа за адресою student1@<domainname>. Перевірити вміст журналів серверівSMTP і POP3.

Заповнити таблицю.

Дата	Запис журналу	Опис

17.Надіслати листа за адресоnoexistent@<domainname>. Перевірити вміст журналів серверів SMTPі POP3. Заповнити таблицю.

Дата	Запис журналу	Опис

18.Відправити листа облікового запису користувача postmaster@<domainname1>, dedomainname – доменне ім’я сервера сусіда. Отримати листи. Заповнити таблицю.

№ з\п	Дія	Екранна копія

19. Перевірити журнали серверівSMTP і POP3. Заповнити таблицю.

Дата	Запис журналу	Опис

Контрольні питання:

1. У чому відмінність між обмеженням з’єднання з SMTP- сервером та обмеження ретрансляції?
2. Для чого обмежують ретрансляцію листів поштовим сервером?
3. Як налаштувати автентифікацію користувачі SMTP- сервера?
4. Коли листи потрапляють у каталог SMTP- сервера, а коли в POP3?

Лабораторна робота № 16

Тема. ***Конфігурування поштового сервера ОС Linux***

Мета роботи: оволодіти практичними навичками адміністрування сервісі PostfixiDovecot у OCLinux

1.Перевірити, чи наявні службиPostfix таDovecot серед складових сервера. Якщо компоненти не встановлені, Інсталювати їх. Заповнити таблицю.

№ з\п	Дія	Команда

Задати мережні параметри сервераPostfix:

- ✓ DNS - Ім’я поштового сервера – за вказівкою викладача;
- ✓ DNS - Ім’я поштового домену – за вказівкою викладача;
- ✓ Опрацювання запитів. Які надходять на всі мережні інтерфейси;
- ✓ Отримання сервером листів. Адреси яких містять його DNS– ім’я або DNSім’я поштового домену;
- ✓ Режим пересилання листів для комп’ютерів з під мережі, до якої належить сервер;
- ✓ Доменна частина поштової адреси відправника –DNS ім’я поштового домену, який обслуговує сервер.

Заповнити таблицю.

№ з\п	Дія	Команда або параметр конфігурації

3.Задати параметр поштових скриньок сервераPostfix.

- ✓ Шлях до поштових скриньок - /var/spool/mail;
- ✓ Формат скринька – один файл;
- ✓ Обмеження обсягу поштової скриньки користувача – 500мб;
- ✓ Обмеження обсягу листа – 10мб;

Заповнити таблицю.

№ з\п	Дія	Команда або параметр конфігурації

4.Використовуючи утиліту telnet,перевірити зв’язок із сервером.

5.В ОС Linuxстворити обліковий запис користувачаpostmaster.

6.Налаштувати поштовий клієнт, у якому вказати:

- ✓ Власне прізвище та ім’я;
- ✓ Електронну поштуpostmaster@<DNS - Ім’я домену>;
- ✓ Адреси серверів SMTPiPOP3;
- ✓ Логін і пароль доступу до сервера POP3;

Заповнити таблицю.

№ з\п	Дія	Екранна копія

7.Надіслати листа за адресоюpostmaster@<domainname>, де domainname– DNS ім’я сервера. Заповнити таблицю.

№ з\п	Дія	Екранна копія

8.Перевірити журнал сервераPostfix. Заповнити таблицю.

Дата	Запис журналу	Опис

9.Задати такі параметри сервераDovecot:

- ✓ Обробка запитів клієнтів за протоколами IMAPi POP3.
- ✓ Опрацювання запитів, які находять на всі мережні інтерфейси;
- ✓ Дозвіл автентифікації без шифтування даних;
- ✓ Зчитування листів із файлів/var/spool/mail/<>;
- ✓ Автентифікація користувачів на основі файла /etc/passwd;
- ✓ Шлях до журналу сервера - /var/log/dovecot.log.

Заповнити таблицю.

№ з\п	Дія	Команда або параметр конфігурації

10.Отримати листи, адресовані обліковому записуpostmaster. Заповнити таблицю.

№ з\п	Дія	Екранна копія

11. Надіслати листа за адресою student1@<damainname> . Перевірити вміст журналів серверів SMTP і POP3.

Заповнити таблицю.

№ з\п	Дія	Екранна копія

12. Відправити листа обліковому запису користувачаhostmaster@<domainname1> , де domainname1 – доменне ім’я сервера сусіда. Отримати листи. Заповнити таблицю.

№ з\п	Дія	Екранна копія

13. Перевірити журнали серверів PostfixiDovecot . Заповнити таблицю.

Дата	Запис журналу	Опис

14. Налаштувати сервер Postfixдля роботи із файлами, що містить облікові записи користувачів:

- ✓ Файл з обліковими записами - /ect/postfix/virtual_mailbox;
- ✓ Шлях розташування поштових скриньок - /var/spool/mail;
- ✓ Ідентифікаційні номери власника та групи файлів(поштових скриньок) – 1100 та 1101 відповідно.

Заповнити таблицю.

№ з\п	Дія	Команда або параметр конфігурації

15. У файлі /ect/postfix/virtual_mailbox додати облікові записи користувачівuser1 user2 , листи яких серверPostfix повинен зберігати у файлах/var/spool/mail. Заповнити таблицю.

№ з\п	Дія	Команда або параметр конфігурації

16. Налаштувати сервер Devecotдля роботи з файлами, що містять облікові записів користувачів:

- ✓ Файл з обліковими записами - /ect/dovecot_pass;
- ✓ Шлях розташування поштових скриньок – відповідно до налаштувань сервера Postfix.

Заповнити таблицю.

№ з\п	Дія	Команда або параметр конфігурації

17.У файлі dovecot_passдодати облікові записи користувачів user1 tauser 2 . Заповнити таблицю.

№ з\п	Дія	Команда або параметр конфігурації

18.Надіслати та отримати листа за адресою user1<domainname>, де <domainname>, –DNS ім’я сервера. Заповнити таблицю.

№ з\п	Дія	Екранна копія

19.Перевірити журнали серверів PostfixiDevecot . Заповнити таблицю.

Дата	Запис журналу	Опис

20. Надіслати листа за адресами noixistent@<domainname>tause@noexistent.edu.ua . Перевірити вміст журналів серверів Postfix і Devecot . Заповнити таблицю.

Дата	Запис журналу	Опис

21.Надіслати та отримати листа за адресоюuser2<domainname1>, де<domainname1> – доменне ім’я сервера сусіда.

Заповнити таблицю.

№ з\п	Дія	Екранна копія

22.Перевірити журнали серверівPostfixDevecot . Заповнити таблицю.

Дата	Запис журналу	Опис

Контрольні запитання

1. Для чого в конфігурації сервера Postfixвикористовують директивуlocal_recipient_maps? Яких значень вона може набувати?

2. Яких значень може набувати директива home_mailboxсервера Postfix? У чому відмінність між цими значеннями?
3. Які директиви сервера Postfixне сприяють розсиланню спаму? Який їх вміст?
4. Який зміст директив default_mail_enu? Які фактори потрібно враховувати при встановленні її значень?

Лабораторна робота №17

Тема. ***Конфігурування проксі – сервера Squid***

Мета роботи: оволодіти практичними навичками розподілу Інтернет каналу засобами проксі – сервера Squid.

1.Перевірити, чи встановлено серверSquid . За Необхідності інсталювати його. Заповнити таблицю.

№ з\п	Дія	Команда або екранна копія

2.Задати мережні параметри проксі – сервера:

- ✓ Порт для опрацювання запитів клієнтів – 3128;
- ✓ Використання пасивного режиму надсилання запитів за протоколом передавання файлів;
- ✓ Використання проміжного проксі – сервера – за вказівкою викладача.

Заповнити таблицю.

№ з\п	Дія	Команда або параметр конфігурації

3.Задати параметри продуктивності сервера Squid:

- ✓ Обсяг оперативної пам’яті для кешування даних – 32 мб;
- ✓ Відсоток заповнення кешу, після досягнення якого сервер видаляє старі об’єкти, - 90;
- ✓ Максимальний обсяг об’єкта кешування – 5 мб;
- ✓ Шлях до папки кешування – /var/ Squid/cache;
- ✓ Максимальний обсяг папки кешування 100мб;
- ✓ Максимальна кількість підкаталогів першого та другого рівня, які містяться у каталозі кешу, - 64 і 128 відповідно.

Заповнити таблицю.

№ з\п	Дія	Команда або параметр конфігурації

4.Створити папку з кешем проксі – сервера. Згенерувати каталоги кешу. Перевірити кількість підкаталогів. Заповнити таблицю.

№ з\п	Дія	Команда або параметр конфігурації

5.Задати параметри ведення журналів сервером Squid:

- ✓ Шлях до журналу, який містить протокол запитів, -/var/ Squid/access.log
- ✓ Шлях до журналу, який містить протокол завантаження процесів сервера, -/var/ Squid/cache.log;
- ✓ Шлях до журналу, який містить протокол запису файлів у кеш, - /var/ Squid/store.log.

Заповнити таблицю.

№ з\п	Дія	Команда або параметр конфігурації

6.Перевірити встановлені параметри.

7.Задати такі параметри зовнішніх програм, які використовує сервер:

- ✓ Адреси – DNS - серверів, до яких буде звертатися проксі – сервер, - DNS- сервери, які використовує ОС;
- ✓ Маршрути до програми, яка здійснює автентифікацію клієнтів, - шлях до файлansca_auth.

Заповнити таблицю.

№ з\п	Дія	Команда або параметр конфігурації

8.Визначити такі правила доступу клієнтів до інтернету:

- ✓ Дозвіл доступу для Вашого сервера без авторизації;
- ✓ Заборонити доступ усім клієнтам до сайтів vkontakte.rutavk.com
- ✓ Дозві доступу без автентифікації для комп’ютера вашого сусіда протягом робочих днів з 9-ої до 14-ої години;
- ✓ Заборонити доступу усім іншим клієнтам.

Заповнити таблицю.

№ з\п	Дія	Команда або параметр конфігурації

9.Перевірити дію заданих параметрів. Заповнити таблицю.

№ з\п	Дія	Екранна копія

10. Додати такі правила доступу клієнтів до Інтернету:

- ✓ Базовий автентифікації на основі файла /ect/ Squid_passwd;
- ✓ Програма, яка здійснює автентифікацію, -nsca_auth;
- ✓ Дозвіл доступу з автентифікацією для комп'ютерів Вашої під мережі.

Заповнити таблицю.

№ з\п	Дія	Команда або параметр конфігурації

11.У файл /var/ Squid_passwdдодати облікові записи користувачі та.

Заповнити таблицю.

№ з\п	Дія	Екранна копія

12.Перевірити правила доступу, які вимагають автентифікації. Заповнити таблицю.

№ з\п	Дія	Екранна копія

13.Додати такі правила обмеження швидкості передавання даних з Інтернету:

- ✓ Швидкість завантаження даних для свого комп'ютера – без обмежень;
- ✓ Швидкість завантаження даних для комп'ютера сусіда – 128 кбіт\с;
- ✓ Загальна швидкість завантаження даних клієнтами з Вашої під мережі 256 Кбіт\с; швидкість кожного клієнта – 64Кбіт\с;
- ✓ Швидкість завантаження для вашої під мережі – 256Кбіт\с.

Заповнити таблицю.

№ з\п	Дія	Команда або параметр конфігурації

14.Перевірити правила доступу, які обмежують швидкість передавання даних. Заповнити таблицю.

№ з\п	Дія	Екранна копія

Словник термінів

ACL(**AccessControlList**)Список або таблиця правил доступу до файлової системи(сервера).

ActiveDirectory - Служба каталогів для організації доменів OCWindows. Домен ActiveDirectoryорганізовано у вигляді дерева об'єктів.

DNS(DomainNameSystem) - Служба перетворення рядкових адрес серверів Інтернет у числові IP - адреси, що організовує групи комп'ютерів у мережі Інтернет за допомогою ієрархії доменів.

Ethernet - Пакетна технологія комп'ютерних мереж. Визначає провідні з'єднання й електричні сигнали на фізичному рівні, формат пакетів даних і протоколи керування доступом до середовища.

FTP - Програмний засіб, який надає доступ файлів за протоколом передавання файлів.

GID-Унікальний числовий ідентифікатор облікового запису первинної групи користувачі ОС ; окрім первинної групи обліковий запис може належати й до інших груп.

Internet - Глобальна комп'ютерна мережа, яку утворюють з'єднані мережі провайдерів, організацій, осіб тощо.

IP (Internetprotocol) - Мережний протокол, що відповідає за передавання і маршрутизацію повідомлень між вузлами Інтернет.

IP - Це послідовність чотирьох байт, які записують у вигляді десяткових чисел, розділених крапками; є унікальною адресою комп'ютера в мережі.

HTTP (HypertextTranferProtocolПротокол передавання гіпертексту) – один з найпоширеніших мережних протоколів Інтернету, основа.

Kerberos -Протокол автентифікації користувачів у доменах , який передбачає взаємне підтвердження достовірності сервера та клієнта. Функціонування протоколу вимагає наявності довіреного сервера автентифікації.

Karnel,Див. **Ядро.**

Localmasterbrowser - Див.

Linux - Один із видів UNIX– подібних операційних систем, побудованих на основі однойменного ядра. LinuxЄ вільно поширюваною ОС з відкритими

Контрольні запитання

1.Які відомості потрібно знати про проксі–сервер, щоб налаштувати браузер чи іншу програму на роботу через нього?

2.Як налаштувати проксі–сервер так, щоб він завжди проводив автентифікацію?

3.Чи можливе збільшення швидкості передавання даних клієнтами з пулу другого класу, якщо інші клієнти з пулу відсутні?

вихідними кодами.

MAC (MediaAccessControl) -Керування доступом до носія) – це унікальний ідентифікатор, що зіставляється з різними типами устаткування для комп'ютерних мереж.

MMC (MicrosoftManagementConsole)Програмний засіб, який містить один або кілька додатків, так званих оснащень, які застосовують для конфігурування складових ОС.

NAT (NetworkAddressTranslation)Процес передавання даних між під мережами, внаслідок якого змінюються адреси відправника або отримувача.

NFS, Див. **Мережева файлова система.**

NIS (NetworkInformationService)-Сервіс, який реалізує спільну базу даних облікових записів у мережі, комп'ютера якої працюють під управлінням OCLinux.

OrganizationUnit, Див. **Підрозділ.**

POP3 (PostOfficeProtocolVersion 3 Протокол поштового відділення, версія 3) – це мережний протокол, що використовується для доставки повідомлень електронної пошти адресатам у мережах TCP/IP. Зазвичай використовується в парі з протоколом SMTP; при цьому SMTPзабезпечує передачу повідомлення від відправника до кінцевого поштового сервера, а POP3 дає змогу адресату одержати це повідомлення із сервера.

RDP (RemoteDesktopProtocol)Протокол віддаленого робочого столу – протокол OCWindows , який описує правила передачі даних між клієнтом і сервером терміналів.

RouterДив.

Samba - Сервер, який надає можливість інтеграції в мережі серверів і клієнтів, які працюють під управлінням ОС Linuxта OCWindows. Може виконувати функції контролера домену.

SMTP (SimpleMailTransferProtocol)- Простий протокол передавання пошти) – це мережний протокол, призначений для передавання електронної пошти.

SSH (SecureShell - Захищена оболонка) – протокол функціонування сервера

терміналів у ОС типуUNIX. Використовує криптографію з'єднання між двома машинами, а також для автентифікації користувачів.

Switch,Див. **Маршрутизатор.**

Telnet - Мережний протокол для віддаленого доступу до комп'ютера за допомогою командного інтерпретатора. Не використовує шифтування і тому вразливий для атак хакерів при застосуванні в локальній мережі чи мережі Інтернет. Подібну функціональність з більшим захистом забезпечує мережний протокол SSH.

TCP (TransmissionControlProtocol)Протокол керування передачею – мережний протокол, призначений для керування передачею і передавання даних у мережах стеку протоколів TCP/IP.

TCP/IP - Стек мережних протоколів, на яких базується Інтернет. Назва утворена з абревіатури двох базових протоколів –TCP таIP .

UID- Унікальний числовий ідентифікатор облікового запису користувача OCLinux.

URL (UniformResourceLocator)Це стандартизований спосіб запису адреси ресурсу в мережі Інтернет.

Автентифікація – процес перевірки достовірності користувачем даних, введених у систему, який полягає у порівнянні його імені та пароля даними, що зберігаються в базі даних операційної системи.

Авторизація – процес надання доступу до мережних ресурсів. Зазвичай відбувається після автентифікації.

Активний режим – режим передавання даних від FTP– сервера до клієнта, при цьому сервер встановлює з'єднання на певний порт клієнта.

Анонімний режим – режим функціонування FTP– сервера, при якому з'єднання з ним можна не тільки за допомогою логіну та пароля облікового запису користувача ОС, але й за допомогою загальнодоступного імені anonymous(анонім).

Браузер – програма для перегляду веб сторінок. Існує чимало програм – браузері: InternetExplorer, Mozilla, Operatощо.

Веб - вузол, див. **Веб – сайт.**

Веб – сайт – це сукупність веб – сторінок, об'єднаних за змістом, URLяких має спільне доменне ім'я(DNS - ім'я).

Веб – сервер – це набір програм, які забезпечуються обмін даними засобами протоколу передавання гіпертекстуHTTP.

Віртуальний веб – хостинг – ситуація, в якій на одному сервері функціонує кілька веб – вузлів.

Власник – обліковий запис користувача, який створив об'єкт файлової системи.

Групова політики – сукупність правил, які можна застосовувати до підрозділів для визначення параметрів їх облікових записі користувачів і комп'ютерів.

Делегування адміністративних повноважень – надання дозволу для використання певних адміністративних задач користувачеві, який не належить до групи Адміністратори.

Демон – процес OCLinux, який завантажується під час старту ОС після ініціалізації ядра. Демони є необхідними для виконання операційною системою своїх функцій.

Домен – логічне об'єднання комп'ютерів, контролер яких містить спільну базу облікових записів користувачів.

Доменний обліковий запис – зареєстрований запис об'єкта в базі даних домену.

Інтернет – провайдер (InternetServiceProvider, ISP)– організація, що надає послуги доступу до Інтернету.

Інтернет, див. **Internet.**

Інтранет – локальна або регіональна мережа, що, як правило, не має з'єднання з мережею Інтернет, але в якій працюють Інтернет – служби мережі.

Клієнт – сервер – мережна архітектура, в якій усі пристрої є або клієнтами, або серверами. Клієнтом є машина (зазвичай ПК), що відправляє запит, сервером – машина, що відповідає на запит. Обидна терміни (клієнт і сервер) можуть бути застосовані як до фізичних пристроїв, так і до програмного

забезпечення.

Комутатор – пристрій, що визначає адресу кожного повідомлення і з'єднує комп'ютер – відправник з комп'ютером – адресатом.

Консоль, див **MMC.**

Контролер домену – комп'ютер, який містить базу даних об'єктів домену.

Концентратор (hub)– пристрій, що забезпечує фізичне з'єднання різних ланок кабелю між собою і повторення сигналу, що надійшов з однієї ланки на інші.

Логін – ім'я користувача, яке використовують у процесі втентифікації.

Локальна комп'ютерна мережа – сукупність певного числа комп'ютерів, розміщених на відносно незначній території.

Локальний обліковий запис – це зареєстрований запис користувача або його групи в базі даних локального комп'ютера (ОС).

Маршрутизатор(router) – пристрій, що з'єднує в одну мережу окремі мережі, що можу працювати за різними протоколами. Роль маршрутизатора може виконувати комп'ютер. Основними завданнями маршрутизатора є визначення раціонального маршруту передачі пакетів даних від основного вузла мережі до іншого та саме передавання.

Мережа з виділеним сервером – це комп'ютерна мережа, в якій мережні пристрої централізовані й керуються одним чи кількома серверами. Індивідуальні робочі станції чи клієнти(такі як ПК) повинні звертатися до ресурсів мережі через сервери.

Мережна плата(мережний адаптер)- це апаратний пристрій, що забезпечує фізичне підключення комп'ютера до мережі. Це або спеціальна плата розширення, що містить гніздо для підключення мережних кабелів, або окремий пристрій, який підключають через портUSB. У сучасних комп'ютерах мережна плата часто інтегрується в материнську плату. Для використання мережної плати необхідно встановити її драйвер.

Мережна служба (мережний сервіс) – це мережна підсистема, призначена для виконання конкретної задачі. Наприклад, в одноранговій мережі Windowsспільний доступ до файлів і принтерів забезпечується спеціальною

службою. В Інтернеті робота електронної пошти, передача файлів та інші можливості також забезпечуються особливими службами.

Мережний адаптер, див. **Мережна плата.**

Мережний протокол – набір правил, за якими відбувається обмін даними між комп'ютерами в мережі.

Мережна файлова система (NFS – NetworkFilesystem) – засіб для створення розподілених ресурсів у ОС типу UNIX. Основою функціонування NFSє однойменний протокол(NFS).

Монтування – процес приєднання файлових систем в OCLinux.

Обліковий запис – дані про користувача, що зберігає ОС або програмне забезпечення, використовуються для одержання і передавання повідомлень. Наприклад, поштовий клієнт OutlookExpressвикористовує обліковий запис для перевірки наявність й одержання повідомлень електронної пошти чи телеконференцій, а також при відправленні повідомлень.

Однорангові мережі – такі комп'ютерні мережі, в яких відсутні сервери, а кожен користувач є як клієнтом, так і сервером одночасно.

Організаційна одиниця, див. **Підрозділ.**

Оснащення, див.**MMC**.

Основний(локальний) браузер (localmasterbrowser) – сервер, який виконує визначення й оновлення списку комп'ютерів робочої групи, а також повідомляє його клієнтам.

Пароль – код доступу для одержання закритих даних(наприклад, для входу в домен).

Пасивний режим – режим передавання даних від FTP-сервера до клієнта, при якому сервер відкриває власний додатковий порт(як правило непривілейований). Через цей додатковий порт клієнт копіює дані сервера та завантажує їх на сервер.

Патч - корд (patchingcord- сполучний шнур) – електричний кабель для підключення одного електричного пристрою до іншого. На кінцях кабелю обов'язково є конектори або наконечники, які відповідають пристроям, що з'єднуються.

Підмережа – окрема мережа об’єднаної мережі.

Підрозділи – контейнер, в якому можуть зберігатися інші об’єктиActiveDirectory .

Пінг (PingPacketInternetGroper) – інструментальний засіб, що посилає інформаційні пакети заданому комп’ютеру в мережі, наприклад, мережі Інтернет. Може визначити, чи перебуває на зв’язку в даний момент вузол за зазначеною адресою.

Порт – інтерфейс на мережному пристрої.

Поштовий клієнт – програма передавання клієнтові отриманих поштовим сервером повідомлень.

Поштовий сервер – програма пересилання, основним призначення якої є отримання повідомлення відправника та їхнє подальше передавання в мережі, а також передавання отриманих поштовим сервером повідомлень клієнтові.

Правила доступу до файлової системи – допустимі для певного облікового запису операції з об’єктами файлової системи. У файловій системі NTFSзаписами є таблиці ACL.

Проксі – сервер (proxy) – служба в комп’ютерних мережах, що надає можливість клієнтам виконувати непрямі запити до інших мережних служб. Спочатку клієнт підключається до проксі – сервера і запитує потрібний ресурс (наприклад, файл), розташований на іншому сервері. Потім проксі – сервер або підключається до зазначеного сервера й одержує ресурс у нього, або повертає ресурс із власного кеша. В деяких випадках запит клієнт чи відповідь сервера може бути змінена проксі – сервером з певною метою.

Профіль користувача — це сукупність налаштувань, які визначають робоче середовище користувача.

Пул — група комп’ютерів або користувачів, яка має доступ до Інтернету з певною швидкістю.

Реплікація — процес синхронізації всіх копій бази даних домену.

Ретрансляція — функція SMTP-сервера, який передбачає обмеження передачі листів, що надсилаються різними клієнтами.

Робоча група — логічне об'єднання комп'ютерів локальної мережі, кожен комп'ютер якого має свою, незалежну від інших, базу даних облікових записів користувачів.

Розподілений мережний ресурс — каталог або пристрій, до якого організовано доступ через мережу і який має унікальне мережне ім'я.

Сайт — частина мережі в доменах Active Directory, де всі контролери домену зв'язані швидким, недорогим і надійним мережним підключенням.

Сервер — комп'ютер або програма, що надає свої ресурси іншим комп'ютерам у мережі.

Системний адміністратор — особа, яка виконує функції управління операційною системою. Використовує відповідний обліковий запис операційної системи, наприклад, root або administrator.

Складена мережа — сукупність кількох мереж. Мережі, які належать до складеної мережі, називають підмережами.

Термінал — робоче місце багатокористувацьких систем. Сервер, який надає інтерфейс (графічний, командний) користувача програмі-клієнту називають сервером терміналів.

Топологія — спосіб організації фізичних з'єднань, опис конфігурації мережі, схема розташування і з'єднання мережних пристроїв.

Мережна топологія може бути: фізичною — опис реального розташування і зв'язків між вузлами мережі; логічною — опис переміщення сигналу в рамках фізичної топології.

Трафік — 1) потік даних у локальній або глобальній мережі; 2) обсяг даних, що надходить на комп'ютер з мережі й відправляється з нього в мережу.

Файл індексу — файл, який передає веб-сервер клієнтові у випадку, якщо його запит містить звертання до каталогу.

Хост — будь-яка одиниця комп'ютерної техніки, підключена до комп'ютерної мережі, наприклад, комп'ютер, сервер, маршрутизатор

тощо. Як правило, для позначення імені хоста, використовують його мережне ім’я (для локальної мережі), IP-адресу чи доменне ім’я (для Інтернету).

Шлюз — проміжний вузол у комп’ютерних мережах, що забезпечує зв’язок комп’ютерів з різних сегментів мережі.

Ядро — основна складова ОС, яка постійно знаходиться в оперативній пам’яті. Ядро ОС опрацьовує переривання від пристроїв, виконує запити системних процесів і програмного забезпечення користувача, розподіляє віртуальну пам’ять, створює й завершує процеси, забезпечує багатозадачність за допомогою перемикання між ними, містить драйвери пристроїв, обслуговує файлову систему.