ОПЕРАЦIЙНI СИСТЕМИ WINDOWS NT, NetWare, UNIX

***Оперцiйна система Windows NT.***

Windows NT – операцiйна система типу клiєнт-сервер, розроблена корпорацiєю Microsoft.

Функцiонально Windows NT дiлиться на двi частини: ***серверну*** - *Windows NT Server* та ***клiєнтську*** - *Windows NT Workstation*. Windows NT Server є ядром операцiйної системи та виконує основнi функцiї по управлiнню мережею. Windows NT Workstation – це набiр програм, якi надають користувачевi зручний доступ до мережi. Хоча ця система призначена для роботи з клiєнтами Windows NT Workstation, вона може працювати i з iншими системами: MS-DOS (з використанням Microsoft LAN Manager), OS/2, Windows for Workgroups та Windows 95/98.

***Windows NT Server.***

Windows NT Server – це повнiстю iнтегрована система, установка якої проводиться автоматично за допомогою спецiальної установочної програми. В процесi установки Windows NT створює спецiальну базу даних, що називається ***реєстр*** *(Registry)*, в якому мiститься iнформацiя про сервер та пiдключених клiєнтiв. За допомогою реєстра здiйснюється управлiння всiєю конфiгурацiєю мережi та її клiєнтами. Установка клiєнта Windows NT Workstation може бути здiйснена як з робочої станцiї, так i по мережi – з сервера чи iншої робочої станцiї. Це дуже зручно при установцi великої кiлькостi робочих станцiй, розмiщених далеко одна вiд одної.

В системi Windows NT данi клiєнтiв зберiгаються ценралiзовано. Кожний клiєнт представлений ***записом користувача*** *(user account)*. Адмiнiстратор мережi має централiзований контроль над всiма клiєнтськими записами та з метою безпеки може заборонити доступ до деяких служб. Записи користувача включають коротке та повне iм’я користувача, його пароль, список доступних груп i т.п.

Крiм записiв, у кожного користувача є ***профiль користувача*** *(user profile)*, який зберiгається на серверi*.* Профiль мiстить установки робочої станцiї користувача. Завдяки йому користувач при входi в систему з рiзних робочих станцiй бачить знайоме робоче оточення.

З метою забезпечення безпеки сервер Windows NT використовує паролi доступу до мережi та права користувача для доступу до мережевих служб. На рiвнi доступу до мережi адмiнiстратор мережi має звичайний контроль використання пароля: наприклад, мiнiмальна i максимальна довжина пароля, частота обновлення пароля i т.д.

Безпека на рiвнi користувачiв забезпечується подiлом користувачiв на категорiї, основанi на мережевих службах, до яких вони мають доступ, та привiлеях роботи з файлами даних. Адмiнiстратор мережi надiлений повноваженнями – керувати доступом до файлiв i директорiй, а також модифiкувати файли для кожної категорiї користувачiв. Нижче наведенi приклади стандартних категорiй користувачiв.

***Адмiнiстратор*** *(Administrator)* може керувати всiєю органiзацiєю мережi: клiєнтськими записами, доступом клiєнтiв до файлiв, процедурами резервного копiювання, установками безпеки i т.д.

***Оператор сервера*** *(Server Operator)* контролює функцiї сервера. Наприклад, виконує резервне копiювання файлiв, керує роздiлом файлiв, контролює служби друку.

***Оператор записiв*** *(Account Operator)* створює та модифiкує записи клiєнтiв (але не операторiв сервера чи записи адмiнiстраторiв) та профiлi користувачiв.

***Оператор друку*** *(Print Operator)* керує тiльки службою друку.

***Оператор резервного копiювання*** *(Backup Operator)* керує тiльки процедурами резервного копiювання.

***Повноважнi користувачi*** *(Power User)* входять як клiєнти, але мають наданi системним адмiнiстратором права зчитування, запису або модифiкацiї файлiв.

***Користувачi*** *(User)* входять в систему для доступу до мережевих служб та приложень i мають обмеженiший доступ до сервера, нiж повноважнi користувачi.

***Windows NT Workstation.***

Клiєнтська система Windows NT Workstation оптимiзована для пiдключення до Windows NT Server. Кожний клiєнт Windows NT може знаходитись або в доменi NT Server, або в окремiй робочiй групi. Пiдключення до мережi може здiйснюватись звичайним для Windows способом через виклик File Manager на робочiй станцiї або вiддалено, з iншої встановленої в мережi Windows NT Workstation.

При входi користувача Windows NT Workstation шукає ***вхiдний сценарiй*** *(logon script)*, який є пакетним файлом, що мiстить команди операцiйної системи. Якщо такий сценарiй iснує, то його команди виконуються автоматично.

Управлiння середовищем Windows NT Workstation здiйснюється за допомогою ***профiля користувача*** *(user profile)*; це спецiальний файл, в якому розмiщенi данi про конфiгурацiю клiєнта, наприклад назви зареєстрованих програм та груп, розмiри та мiсця розмiщення вiкон, кольори екрану та iнформацiя про пiдключенi принтери.

***Оперцiйна система UNIX.***

В даний час UNIX використовується на найрiзноманiтнiших апаратних платформах – вiд персональних робочих станцiй до потужних серверiв з тисячами користувачiв. Це пов’язано з тим, що UNIX – багатозадачна багатокористувацька система, що володiє широкими можливостями.

З точки зору користувача, в операцiйнiй системi UNIX iснує два типи об’єктiв: ***файли*** i ***процеси***. Всi данi зберiгаються у виглядi файлiв, доступ до периферiйних пристроїв здiйснюється як читання/запис в спецiальнi файли. Пiд час запуску програми ядро операцiйної системи завантажує вiдповiдний виконуваний файл, створює образ процесу i передає йому управлiння. Бiльше того, пiд час виконання процес може зчитувати або записувати данi в файл. З iншої сторони, вся функцiональнiсть операцiйної системи визначається виконанням вiдповiдних процесiв. Робота системи друку чи забезпечення вiддаленого доступу залежить вiд того, чи виконуються тi чи iншi процеси в системi.

Файли в UNIX вiдiграють ключову роль. Важко заперечувати значення файлiв для користувачiв, так як всi їх данi зберiгаються у виглядi файлiв. Однак помимо цього, файли в UNIX визначають привiлеї користувачiв, так як права користувача в бiльшостi випадкiв контролюються за допомогою прав доступу до файлiв. Файли забезпечують доступ до периферiйних пристроїв комп’ютера, включаючи диски, CD-ROM, принтери, термiнали, мережевi адаптери i навiть пам’ять. Для приложень UNIX доступ до дискового файла не вiдрiзняється вiд доступу, скажем, до принтера. Нарештi, всi програми, якi виконуються в системi, включно з прикладними задачами користувачiв, системнi процеси i навiть ядро UNIX, є виконуваними файлами.

Як i в багатьох сучасних операцiйних системах, в UNIX файли органiзованi у виглядi деревовидної структури (дерева), яка називається ***файловою системою***. Кожний файл має iм’я, яке визначає його розмiщення в деревi файлової системи. Коренем цього дерева є ***кореневий каталог*** *(root directory)*, який має iм’я “/ ”. Iмена решти файлiв мiстять ***шлях*** – список каталогiв (гiлок), якi необхiдно пройти, щоб досягнути файла. В UNIX весь доступний користувачевi файловий простiр об’єднаний в єдине дерево каталогiв, коренем якого є каталог “/ “. Таким чином, повне iм’я будь-якого файла починається з “/ “ i не мiстить iдентифiкатора пристрою (дискового накопичувача, CD-ROM чи вiддаленого комп’ютера в мережi), на якому вiн фактично зберiгається. Однак це не означає, що в системi присутня тiльки одна файлова система. В бiльшостi випадкiв єдине дерево, таке, яким його бачить користувач системи, складено з декiлькох окремих файлових систем, якi можуть мати рiзну внутрiшню структуру. В свою чергу, файли, що належать до цих файлових систем, можуть бути розмiщенi на рiзних пристроях.

***Безпека в UNIX.***

Бiльшiсть реалiзацiй ОС UNIX має добре продуману систему безпеки.

Першим рiвнем безпеки є вхiдне iм’я та пароль користувача. Системний адмiнiстратор може сконфiгурувати операцiйну систему так, щоб вона приймала тiльки конкретнi типи паролiв (наприклад, тiльки паролi вказаної мiнiмальної довжини). Процедура входу контролюється системою безпеки.

Пiсля входу в мережу користувач стає суб’єктом системи безпеки, а якщо виражатись точнiше, то на його роботу в мережi накладаються обмеження. Управлiння файлами та директорiями здiйснюється по праву доступа, тобто за допомогою установок, якi дозволяють виконання конкретних операцiй. В ОС UNIX iснує три базових класи доступу до файлiв, в кожному з яких встановленi вiдповiднi права доступу:

* **User (u)** – для користувача, який є власником файла;
* **Group (g)** – для членiв групи, яка є власником файла;
* **Other (o)** – для iнших користувачiв.

***Мережева файлова система NFS.***

Мережева файлова система NFS (продукт корпорацiї Sun) є набором протоколiв i програмних продуктiв, якi широко використовуються в мережах, що базуються на ТСР/IР. Особливо популярна NFS в мережах UNIX, крiм того, тепер вона доступна на багатьох iнших платформах i надiйно працює в локальних мережах. Iснує кiлька протоколiв, тiсно пов’язаних з NFS: ***протокол NIS*** (Network Information Service – мережева iнформацiйна служба) i ***протокол REX*** (Remote Execution Service – служба дистанцiйного виконання).

Sun створила NFS таким чином, щоб комп’ютери рiзних виробникiв працювали сумiсно навiть в тому випадку, коли вони використовують рiзнi операцiйнi системи. Sun опублiкувала специфiкацiї NFS, дозволяючи iншим виробникам адаптувати свої апаратнi та програмнi засоби для надiйної та зручної роботи в локальних та глобальних мережах. В результатi NFS фактично стала стандартом для систем пiд управлiнням UNIX та отримала широку пiдтримку в iнших операцiйних системах.

***Оперцiйна система NetWare.***

NetWare – це потужна система клiєнт/сервер, розроблена корпорацiєю Novell. В даний час приблизно в половинi систем файл-серверiв, побудованих на базi персональних комп’ютерiв, використовується NetWare. Використовується три рiзних версiї NetWare: версiї 2, 3 i 4. Версiя 2 вже знята з продажу, але вона ще використовується в деяких мережах. NetWare 3 дуже добре зарекомендувала себе i ще досить широко використовується.

Кожна нова версiя NetWare в порiвняннi з попереднiми версiями пропонує ряд переваг, додаткових можливостей та вдосконалень. NetWare версiї 4.11 (її також називають IntranetWare) включає спецiальнi можливостi для органiзацiї доступу мережi до Internet та iнтеграцiї мережi з Web-технологiями. NetWare версiї 4.х набагато бiльша, функцiональнiша та складнiша вiд попереднiх версiй. В нiй значно змiнена файлова система та представленi глобальнi служби директорiй.

NetWare завантажується поверх операцiйної системи DOS, але пiсля запуску вона бере контроль над всiєю мережею. DOS стає другорядною системою i продовжує працювати пiд NetWare, але в будь-який момент можна повернутись в DOS. З метою економiї пам’ятi DOS може бути видалена.

Файлова система NetWare оптимiзована для мережевого середовища. В нiй є ряд унiкальних можливостей, якi покращують характеристики мережi, пiдвищують швидкiсть роботи i надiйнiсть.

***Протоколи системи NetWare.***

Здiйснюючи пiдтримку стандартних мережевих протоколiв (крiм AppleTalk), NetWare використовує ряд додаткових протоколiв, якi частково дублюють функцiї стандартних протоколiв, але бiльш адаптованi до системи NetWare. Нижче перечисленi цi протоколи.

* **Мiжмережевий обмiн пакетами (IPX)** здiйснює перевiрку даних та адресацiї, тобто ТСР/IР. Цей протокол може обробляти мiжмережевi повiдомлення (мiж NetWare та iншими мережами).
* **Протокол ядра NetWare (NCP)** управляє потоком даних мiж робочими станцiями NetWare та файловими серверами для досягнення максимальної ефективностi цього процесу.
* **Послiдовний обмiн пакетами (SPX)** використовує функцiї NetWare для перевiрки точностi передачi даних.
* **Протокол рекламуючого Сервера (SAP)** контролює процес реєстрацiї в мережi та керує передачею повiдомлень мiж вузлами через всю мережу.

***Служби директорiй NetWare.***

В NetWare версiї 4.х Novell появилась служба директорiй Novell (**Novell Directory Services – NDS**), за допомогою якої можна створювати їєрархiю локальних мереж. Ця їєрархiчна структура має розгалужену органiзацiю, тому її часто називають ***деревом***.

В основi NDS лежить коренева ***директорiя*** *(root directory),* в якiй може мiститись будь-яка кiлькiсть ***об’єктiв*** *(object)*. Iснує два типи об’єктiв: об’єкт ***контейнер*** *(container)* та об’єкт ***лист*** *(leaf).* Об’єкт контейнер мiстить iншi об’єкти, наприклад країну, органiзацiю чи робочу групу в органiзацiї. Об’єкт лист означає окремий вузол мережi, наприклад робочу станцiю, файл-сервер, робочу групу чи iм’я користувача.

***Безпека в NetWare.***

Враховуючи, що NetWare розрахована на роботу в крупних комп’ютерних мережах з великою кiлькiстю користувачiв, передбачено декiлька рiвнiв захисту iнформацiї. Є можливiсть настройки рiвнiв безпеки, якi охоплюють всiх користувачiв мережi.

***Системний адмiнiстратор*** може сконфiгурувати систему так, щоб вона при входi вказаних користувачiв запитувала в них паролi, а також виконувала будь-якi з перечислених нижче операцiй:

* приймала паролi строго визначеної довжини;
* забороняла користувачам використовувати однаковi паролi;
* вимагала змiни паролю через вказаний промiжок часу;
* накладала обмеження на час дня, коли користувач може входити в мережу;
* задавала календарний перiод, на протязi якого даний користувач може входити в систему, або кiлькiсть часу, вiдведеного користувачевi для роботи в мережi.

**Користувач** навiть пiсля входу в мережу не може безкарно “бродити” по нiй. Кожному користувачу надається одне або декiлька перечислених нижче ***прав доступу до файлiв***.

* **Супервiзор (Supervisory).** Надає повний доступ до мережевих файлiв даних i право назначати права доступу до файлiв для iнших користувачiв.
* **Управлiння доступом (Access Control).** Дозволяє користувачу давати практично всi права, крiм прав супервiзора.
* **Сканування (Scan).** Дозволяє користувачевi переглядати вмiст файлiв та директорiй.
* **Тiльки читання (Read Only).** Дозволяє користувачевi переглядати вмiст файлiв, не вносячи в них змiн.
* **Створення (Create).** Дозволяє користувачевi створювати новi файли та директорiї.
* **Змiна (Modify).** Дозволяє користувачевi змiнювати назви файлiв чи директорiй, але не дає доступу до їх вмiсту.
* **Запис (Write).** Дозволяє користувачевi змiнювати вмiст файлiв i директорiй.
* **Видалення (Erase).** Дозволяє користувачевi видаляти файли.

***Файли та директорiї.***

В NetWare використовується дещо змiнена iєрархiчна структура DOS. На вершинi iєрархiї замiсть персонального комп’ютера знаходиться мережа. Пiд цим рiвнем знаходяться файловi сервери, а пiд кожним сервером – дисковi томи. Кожний сервер може мiстити до 64 томiв, i на кожному томi є власна iєрархiчна структура каталогiв. Ця iєрархiя утворює основу системи, що використовується в NetWare для визначення мiсцезнаходження файлiв, а саме: мiсцезнаходження файла визначається сервером, томом, каталогом, пiдкаталогом та iменем файла.

***Вiдслiдковування файлових транзакцiй.***

За допомогою ***системи вiдслiдковування транзакцiй*** *(Transaction Tracking System – TTS)* NetWare може захистити данi вiд системних збоїв пiд час операцiй запису. Ця система працює на рiвнi файл-сервера. Частина файлiв, що зберiгаються файл-сервером, можуть бути помiченi як ***транзакцiйнi*** *(transactional)* файли. Тепер, перш нiж змiнити вмiст такого файла, NetWare спочатку помiтить текучий файл як резервний i запише весь обновлений файл в iнше мiсце на диску. Пiсля успiшного завершення процесу копiювання NetWare видаляє резервний файл.

***Стiйкiсть при збоях системи.***

Як додатковий механiзм безпеки NetWare використовує спецiальнi способи збереження даних, якi призначенi для збереження iнформацiї при вiдмовi жорсткого диска. Всi цi способи об’єднують в ***Стiйкiсть при збоях системи*** *(System Fault Tolerance – SFT).*

NetWare надає два рiвнi стiйкостi при збоях системи (плюс третiй рiвень в NetWare 4). SFT першого рiвня виконує операцiю, що називається ***перевiрка читанням пiсля запису***. Це робиться для облiку можливостi появи збойного сектора, який в будь-який момент може появитись на жорсткому диску в результатi звичайного зносу.

SFT другого рiвня надає пiдтримку для ***створення дзеркальної копiї диска*** *(disk mirroring)* або ***дублювання диска*** *(disk duplexing)*. При створеннi дзеркальної копiї диска дублюючi жорсткi диски пiдключенi до одного контролера, i данi копiюються на два диски одночасно. Якщо один з дискiв повнiстю виходить з ладу, то другий диск може працювати як резервний i зразу бере на себе управлiння, завдяки чому пiд час замiни диска мережа може продовжувати працювати звичайним чином.

SFT третього рiвня надає пiдтримку вiдображення файл-серверiв (mirrored file servers). В цьому випадку данi зберiгаються на первинному серверi i зразу ж на великiй швидкостi переносяться на вторинний файл-сервер. Крiм того, NetWare може може використовувати вторинний сервер для доступу до даних та пiдвищення продуктивностi.