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 (root або 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 одноранговых 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 користува-

чів. 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, що 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 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.

Подібно до веб-сервера Apache, для опису властивостей каталогів сервера ProFTPD передбачено 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>
        DenyAl1
    </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
    AllowUser student
    Deny from all
</Limit>/
```

Для конфігурування публічного FTP-сервера можна використати директиви:

```
<Anonymous /var/ftp>
    UserAlias 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.

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.

Зміст