Хорунжий О.В.

VirtualBox

vmware

Microsoft Azure

АДМІНІСТРУВАННЯ ПРОГРАМНИХ СИСТЕМ І КОМПЛЕКСІВ

122 Комп'ютерні науки

конспект лекцій

Windows Server

MikroTik

CISCO

ВСП «КПЕФК ЛНТУ»

Міністерство освіти і науки України
ВСП «Ковельський промислово-економічний фаховий коледж ЛНТУ»

АДМІНІСТРУВАННЯ
ПРОГРАМНИХ СИСТЕМ І КОМПЛЕКСІВ

КОНСПЕКТ ЛЕКЦІЙ

для здобувачів освітньо-професійного ступеня

фаховий молодший бакалавр спеціальності

122 Комп'ютерні науки

денної форми здобуття освіти

Ковель
2025

УДК 004.5 (07)
А 28

Затверджено до видання методичною радою ВСП «КПЕФК ЛНТУ», протокол № 5 від «28» січня 2025 року.

Голова методичної ради ВСП «КПЕФК ЛНТУ» _____ Ігор ІЛЮШИК
(підпис)

Розглянуто та схвалено на засіданні циклової комісії з комп'ютерних наук ВСП «КПЕФК ЛНТУ», протокол № 4 від 20 січня 2025 року.

Голова циклової комісії _____ Олександр ПРИСАДА
(підпис)

Електронна копія друкованого видання передана до книжкового фонду бібліотеки ВСП «КПЕФК ЛНТУ»

Завідувачка бібліотеки_____ Неля ТЕЛЮЧИК
(підпис)

Укладач: _____ Олександр ХОРУНЖИЙ, викладач ВСП «КПЕФК ЛНТУ».
(підпис)

Рецензент: _____ Тетяна СЕЛІВОНЧИК, к.т.н., доцент ЛНТУ.
(підпис)

Відповідальний
за випуск: _____ Леся ПРОКОПЧУК, методист ВСП «КПЕФК ЛНТУ».
(підпис)

Адміністрування програмних систем і комплексів [конспект лекцій]: для здобувачів освітньо-професійного ступеня фаховий молодший бакалавр спеціальності 122 Комп'ютерні науки денної форми здобуття освіти / уклад. Олександр ХОРУНЖИЙ – Ковель: ВСП «КПЕФК ЛНТУ», 2025. – 124 с.

Відповідно до нормативної програми освітнього компонента «Адміністрування програмних систем і комплексів» викладено конспект лекцій, метою яких є формування у здобувачів освіти системного підходу до адміністрування сучасних інформаційних систем, розвиток професійних знань і навичок, необхідних для роботи системним адміністратором, включаючи управління сучасними операційними системами Windows, серверними платформами Windows Server, а також мережевими пристроями на базі Mikrotik.

Зміст

Передмова

Сучасний світ інформаційних технологій стрімко розвивається, і професія системного адміністратора залишається однією з ключових у підтримці стабільного функціонування IT-інфраструктури. Системний адміністратор забезпечує налаштування, оптимізацію, захист та безперебійну роботу програмного й апаратного забезпечення. У межах освітнього компонента «Адміністрування програмних систем і комплексів» розглядаються базові та поглиблені аспекти адміністрування програмних систем, включаючи локальні середовища та хмарні технології.

Перший розділ присвячений вступу до професії системного адміністратора, а також технологіям віртуалізації, які є фундаментальними для побудови сучасних IT-рішень. Детально вивчаються такі популярні платформи, як VMware, VirtualBox, Hyper-V, а також хмарні сервіси Microsoft Azure. Цей блок забезпечить необхідну базу для подальшого опанування практичних навичок у реальному середовищі.

У другому розділі увагу зосереджено на адмініструванні операційних систем Windows 10 та 11. Здобувачі освіти отримають знання про встановлення ОС, початкові налаштування, роботу з користувачами та групами, оптимізацію системи, налаштування брандмауера та застосування групових політик безпеки. Також розглядатимуться інструменти діагностики, резервного копіювання та відновлення, що є критично важливими для підтримки безпеки та стабільності систем.

Третій розділ знайомить із адмініструванням серверних операційних систем Windows Server 2016, 2019 та 2022. У ньому розглядаються мінімальні вимоги, вибір обладнання, встановлення та налаштування серверів, управління ролями та компонентами, а також роботу з критичними службами, серед яких: VPN, DHCP та веб-сервери. Цей матеріал допоможе підготуватися до роботи в складних корпоративних середовищах.

Завершальний четвертий розділ зосереджений на адмініструванні мережевих систем Mikrotik. Огляд інтерфейсу, базові налаштування, налаштування Firewall, сегментація мереж, а також використання VPN та IPsec – це ключові теми, які забезпечать здобувачів освіти практичними знаннями для управління сучасними мережами. У підсумку, вивчення всіх розділів сформує цілісне

розуміння системного адміністрування в умовах сучасної IT-інфраструктури.

Освітній компонент «Адміністрування програмних систем і комплексів» також акцентує увагу на важливості безпеки в адмініструванні як операційних систем, так і мережевих інфраструктур. Зокрема, в рамках лекцій будуть детально розглянуті питання захисту даних, використання шифрування, налаштування брандмауерів, а також методи забезпечення безпеки при роботі з хмарними технологіями та віртуальними машинами. Системний адміністратор повинен не лише ефективно управляти ресурсами, але й гарантувати високий рівень безпеки, що є основою для забезпечення довіри до корпоративних IT-систем і даних.

Розділ 1. Вступ. Віртуалізація

Тема: Професія «Системний адміністратор»

План

1. Сертифікації та вміння.
2. Посадові обов’язки і спеціалізація.
3. Плюси і мінуси професії. Перспективи.

Системний адміністратор (System Administrator, або sysadmin) — це IT-фахівець, відповідальний за налаштування, підтримку, управління та безперебійну роботу апаратного й програмного забезпечення в організації. Його основна мета — забезпечити стабільне функціонування інформаційної інфраструктури, досягнення високої продуктивності систем і мінімізація збоїв у роботі.

Системний адміністратор займається обслуговуванням серверів, комп'ютерів, мереж, баз даних, засобів зберігання інформації, а також мережевих пристроїв. Він гарантує, що користувачі мають доступ до необхідних ресурсів, які працюють без перебоїв, а дані залишаються захищеними від втрати або несанкціонованого доступу.

Крім цього, системні адміністратори часто відповідають за створення і впровадження політик безпеки, моніторинг мережевої активності для запобігання можливим загрозам, а також проводять навчання користувачів з питань безпеки та ефективного використання інформаційних систем. Вони також займаються відновленням систем після збоїв, виконують резервне копіювання та відновлення даних, а також розробляють та впроваджують стратегії аварійного відновлення.

Системні адміністратори постійно вдосконалюють свої знання та навички, слідкуючи за новітніми розробками та тенденціями в галузі інформаційних технологій. Вони працюють з різними операційними системами, мережевими протоколами та програмним забезпеченням, забезпечуючи безперебійну та ефективну роботу всіх компонентів інформаційної інфраструктури організації.

Основні сертифікації

- ✓ Сертифікований фахівець Майкрософт (MCP), Сертифікований Системний Інженер Майкрософт (MCSE), сертифікований системний адміністратор «Майкрософт» англ. *Microsoft Certified Systems Administrator* – MCSA) та інші для роботи в Windows-середовищах;
- ✓ для роботи в Unix-подібних середовищах:
    - *сертифікат Linux Professional Institute для роботи в Linux-середовищах;*
    - *сертифікати Програми видачі свідоцтв Red Hat для роботи в Red Hat Enterprise Linux-середовищах;*
    - *сертифікат для роботи в Solaris-середовищах;*
- ✓ сертифікати Мережевої академії Cisco для роботи з обладнанням Cisco;
- ✓ сертифікати для роботи з базами даних Oracle.

Вміння

Суть системного адміністрування включає знання комп'ютерних систем і ефективні способи їх використання працівниками організації. Це потребує знань операційних систем і застосунків, вирішення проблем з апаратним та програмним забезпеченням, але також і мети, з якою співробітники організації застосовують комп'ютери.

Чи не найважливішим вмінням системного адміністратора є здатність до вирішення проблем, часто під тиском ряду обмежень. Сисадмін необхідний і незамінний у випадку неполадок в комп'ютерній системі, мусить швидко і правильно діагностувати і найкращим чином усувати їх.

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

Під час роботи Інтернет-орієнтованих або бізнес-критичних систем системний адміністратор повинен особливо надійно контролювати безпеку мережі. Це включає не тільки своєчасне

оновлення програмного забезпечення, але й попереджувальні заходи проти зламу системи захисту і вторгнення в комп'ютерну систему. В деяких організаціях за безпеку комп'ютерної мережі і підтримку брандмауера (фаєрволу) відповідає адміністратор захисту мережі, але кожен сисадмін в значній мірі здатен підтримувати безпеку системи.

Системні адміністратори – працівники, які протистоять атакам зломщиків і сприяють безпечному спілкуванню всередині інфраструктури організації, а також за її межами. Системний адміністратор – в певному сенсі також комп'ютерний зломщик, так як він повинен знати всі ті способи зламу і обходу захисту (наприклад, брандмауера), які застосовують зломщики. Однак в більшості організацій обов'язками системного адміністратора є не тільки спостереження за безпекою мережі організації, а також й інші супутні проблеми: боротьба з комп'ютерними вірусами, налаштування програмного забезпечення користувачів та ін.

Через швидкий розвиток Інтернет і мережевих технологій, системному адміністратору-одинаку щоразу складніше протистояти всім проблемам, тому є і з'являються нові спеціалізовані Інтернет-форуми і друковані видання, спрямовані на поглиблення знань сисадмінів-початківців і надання допомоги у вирішенні

Основні обов'язки системного адміністратора

1. Встановлення та налаштування програмного забезпечення та операційних систем
    - *Сюди входить встановлення та оновлення операційних систем (Windows, Linux, macOS), програм, серверів та мережевих рішень.*
2. Управління мережами
    - *Адміністратор відповідає за проектування, налаштування та обслуговування локальних мереж (LAN), бездротових мереж (Wi-Fi) і корпоративних мереж (WAN).*
3. Забезпечення інформаційної безпеки
    - *Включає моніторинг вразливостей, налаштування брандмауерів, групових політик безпеки, управління VPN, шифрування даних (BitLocker, EFS) та резервне копіювання інформації.*
4. Моніторинг та діагностика систем
    - *Використовуються інструменти для аналізу продуктивності систем, журналів подій, діагностики обладнання та програмного забезпечення.*

5. Резервне копіювання та відновлення даних
    - *Системний адміністратор створює стратегії резервного копіювання, управляє архівами та забезпечує швидке відновлення даних у разі аварій.*
6. Підтримка користувачів
    - *Це налаштування робочих станцій, допомога з вирішенням технічних проблем, управління правами доступу користувачів до ресурсів.*
7. Управління хмарними та віртуалізованими системами
    - *Робота з платформами віртуалізації (VMware, Hyper-V) і хмарними сервісами (Microsoft Azure, AWS).*
8. Автоматизація рутинних процесів
    - *Використання скриптів (PowerShell, Bash, Python) для автоматизації щоденних завдань.*

Спеціалізація

Системне адміністрування охоплює широкий спектр спеціалізацій, які дозволяють адміністраторам фокусуватися на конкретних аспектах IT-інфраструктури. Ось список основних сучасних спеціалізацій системних адміністраторів:

1. Адміністратор операційних систем
    - *Фокус на підтримці, налаштуванні та оптимізації ОС, таких як Windows, Linux або macOS.*
2. Адміністратор серверів
    - *Встановлення, налаштування та управління серверними операційними системами (Windows Server, Ubuntu Server тощо) та ролями, такими як DHCP, DNS, RDP, VPN.*
3. Адміністратор баз даних (DBA)
    - *Управління базами даних (SQL Server, Oracle, PostgreSQL, MySQL), моніторинг продуктивності, резервне копіювання та безпека даних.*
4. Хмарний адміністратор (Cloud Administrator)
    - *Підтримка хмарних сервісів і платформ (Microsoft Azure, AWS, Google Cloud), управління віртуальними машинами, контейнерами та обчислювальними ресурсами.*
5. Мережевий адміністратор
    - *Проектування, налаштування та підтримка мереж (Cisco, Mikrotik, Ubiquiti), включаючи маршрутизацію, комутацію, брандмауери та VPN.*

6. Віртуалізація та адміністрування контейнерів
    - *Робота з платформами віртуалізації (VMware, Hyper-V, VirtualBox) і контейнерами (Docker, Kubernetes).*
7. Адміністратор безпеки
    - *Забезпечення інформаційної безпеки, робота з шифруванням, груповими політиками безпеки, налаштуванням SIEM-систем (наприклад, Splunk, QRadar).*
8. DevOps-адміністратор
    - *Зосередження на автоматизації, CI/CD-процесах, хмарній інфраструктурі, роботі з інструментами, такими як Jenkins, Ansible, Terraform.*
9. Адміністратор систем резервного копіювання та відновлення
    - *Розробка та підтримка стратегій резервного копіювання (Veeam, Acronis, Commvault), управління відновленням даних у разі збоїв.*
10. Адміністратор апаратного забезпечення
    - *Управління фізичними серверами, системами зберігання даних (NAS, SAN) та серверними шафами.*
11. Адміністратор IT-інфраструктури (Infrastructure Administrator)
    - *Відповідальний за весь спектр інфраструктурних рішень, включаючи хмарні, локальні та гібридні середовища.*
12. Адміністратор поштових систем та спільної роботи
    - *Налаштування та підтримка корпоративних поштових систем (Exchange, Google Workspace, Microsoft 365), систем спільної роботи (Microsoft Teams, Slack).*

Кожна спеціалізація може вимагати сертифікацій (наприклад, CompTIA, Microsoft, Cisco, AWS), що підтверджують компетентність у вибраній галузі.

Плюси та мінуси

До плюсів професії можна віднести високу необхідність в таких фахівцях. Сфера інформаційних технологій в нашій країні розвивається швидкими темпами, які значно обганяють аналогічні показники в Європі і США. Попит на таких кандидатів постійно перевищує пропозицію, тому працевлаштування для системного адміністратора не складає великої проблеми.

До позитивних моментів відноситься і те, що сисадмін може вільно розпоряджатися своїм робочим часом, оскільки багато

компаній приймають на роботу так званих «прихідних адміністраторів», котрі мають від одного до трьох службових днів в тиждень і з'являються в офісі під час виникнення якої-небудь серйозної проблеми чи необхідності.

В той же час в роботі системного адміністратора є і певні складнощі. Наприклад, якщо трапляється збій в системі, або відбуваються серйозні зміни в мережевій інфраструктурі компанії, робочий день такого фахівця збільшується рівно настільки, скільки потрібно часу для усунення неполадок. Також дуже часто адміністратори стикаються з недостатньою увагою до проблем інформаційних технологій в компанії з боку керівництва, яке вважає, що такі фахівці повинні самі про все піклуватися і підтримувати комп'ютерну техніку в робочому стані, налагоджувати і забезпечувати роботу локальної мережі.

Особисті якості системного адміністратора

1. Технічна грамотність — здатність швидко розбиратися в нових технологіях та їх особливостях.
2. Стресостійкість — адже робота часто передбачає усунення критичних збоїв у стислі терміни.
3. Вміння аналізувати та вирішувати проблеми — логічне мислення та навички пошуку причин несправностей є обов'язковими.
4. Готовність до навчання — IT-сфера швидко змінюється, тому системний адміністратор повинен постійно оновлювати свої знання.

Перспективи

Горизонтальну кар'єру можна збудувати, перейшовши на позицію системного архітектора, адміністратора баз даних, наприклад Oracle. Як вертикальна перспектива зростання – обійняти посаду старшого системного адміністратора в крупній компанії, в підпорядкуванні якого знаходиться декілька системних адміністраторів з вузькою спеціалізацією, а в майбутньому претендувати на крісло керівника управління інфраструктури або відділу інформаційних технологій.

Чому роль системного адміністратора важлива?

Системний адміністратор — це своєрідний "опорний стовп" IT-інфраструктури. Без його роботи компанії ризикують зіштовхнутися з простоєм серверів, втратою даних, низькою продуктивністю систем та ризиками порушення кібербезпеки. Його завдання забезпечити не лише стабільну роботу інфраструктури, але й адаптацію до нових технологій, що забезпечує конкурентоспроможність організації.

Контрольні питання

1. Хто такий системний адміністратор?
2. Основні сертифікації професії.
3. Суть системного адміністрування.
4. Типові обов’язки системного адміністратора.
5. Плюси та мінуси професії.

Тема: Віртуалізація

План

1. Основні поняття віртуалізації.
2. Віртуальна машина.
3. Технології.

Віртуалізація — це технологія, яка дозволяє створювати віртуальні версії фізичних ресурсів, таких як сервери, сховища, мережеві ресурси та операційні системи. Для системного адміністратора віртуалізація є потужним інструментом для оптимізації використання апаратних ресурсів і підвищення ефективності роботи інформаційної інфраструктури.

В контексті системного адміністратора, віртуалізація має кілька ключових переваг:

1. **Консолідація ресурсів**. *Віртуалізація дозволяє зменшити кількість фізичних серверів, об'єднуючи кілька віртуальних машин (VM) на одному фізичному сервері.*
2. **Гнучкість і масштабованість**. *Віртуальні середовища можуть бути швидко створені, змінені або видалені, що дозволяє системним адміністраторам легко адаптувати інфраструктуру до змін у потребах бізнесу.*
3. **Відновлення після збоїв**. *Віртуалізація спрощує процес резервного копіювання та відновлення, оскільки віртуальні машини можуть бути легко копійовані та перенесені на інші фізичні сервери в разі збоїв.*
4. **Оптимізація ресурсів**. *Віртуалізація дозволяє максимально ефективно використовувати апаратні ресурси, розподіляючи їх між кількома віртуальними машинами на основі поточних потреб.*

Отже, системні адміністратори використовують віртуалізацію для підвищення ефективності та надійності своєї інформаційної інфраструктури, а також для зменшення витрат на апаратне забезпечення та обслуговування.

Віртуальна машина (VM) — це програмна емуляція фізичного комп'ютера, яка працює як окрема незалежна система на фізичному сервері. Вона забезпечує функціонування операційних систем і додатків у віртуальному середовищі, використовуючи ресурси хостової машини (фізичного сервера).

У контексті системного адміністрування, віртуальна машина має кілька важливих характеристик:

1. **Ізоляція.** *Кожна віртуальна машина працює незалежно від інших VM та хостової системи, що забезпечує безпеку та стабільність.*
2. **Гнучкість.** *Віртуальні машини можуть бути легко створені, змінені або видалені, що дозволяє швидко налаштовувати і тестувати нові середовища.*
3. **Ефективність використання ресурсів.** *Віртуальні машини дозволяють оптимально використовувати апаратні ресурси фізичного сервера, розподіляючи їх між кількома VM.*
4. **Відновлюваність.** *Віртуальні машини можуть бути легко резервовані, клоновані та перенесені на інші фізичні сервери у разі збоїв, що забезпечує надійне відновлення після аварій.*

Віртуальні машини значно спрощують управління IT-інфраструктурою, дозволяючи системним адміністраторам ефективніше керувати ресурсами, тестувати нові рішення та забезпечувати стабільну роботу систем.

Визначення

Раніше віртуальну машину визначали як «ефективну ізольовану копію реальної машини». Проте сучасні віртуальні машини можуть не мати прямого апаратного аналогу. Наприклад, в залежності від способу моделювання набору інструкцій віртуального центрального процесора, віртуальна машина може моделювати реальну або абстрактну обчислювальні машини. Під час моделювання реальної обчислювальної машини набір інструкцій процесора віртуальної машини збігається з набором інструкцій обраного для моделювання центрального процесора.

Віртуальні машини поділяються на 2 головні категорії, в залежності від їх використання та відповідності до реальної апаратури:

- ✓ **системні** (апаратні) віртуальні машини, що забезпечують повноцінну емуляцію всієї апаратної платформи і відповідно підтримують виконання операційної системи;
- ✓ **прикладні** віртуальні машини, які розроблені для виконання лише застосунків (прикладних програм), наприклад, Віртуальна машина Java.

Системні віртуальні машини

Системні віртуальні машини дозволяють розподіл апаратних ресурсів фізичної машини між різними копіями віртуальних машин, на кожній з яких може бути встановлена своя операційна система. Пласт програмного забезпечення, що виконує віртуалізацію, називається гіпервізором. Гіпервізори поділяються на 2 типи: ті, що можуть виконуватися на "голій" апаратурі (**1-й тип** або **рідні** (англ. **native**)), та ті, що виконуються в певній операційній системі (**2-й тип** або **хостові**).

Основні переваги системних ВМ:

- ✓ різні операційні системи можуть співіснувати на одному комп'ютері, і при цьому знаходитися в строгій ізоляції одна від одної;
- ✓ ВМ можуть забезпечувати розширений набір машинних інструкцій, адже при моделюванні абстрактної обчислювальної машини набір інструкцій процесора віртуальної машини може бути довільним;
- ✓ широкі можливості контролю за програмами;
- ✓ легкість модифікацій та відновлення.

Основний недолік:

- ✓ віртуальна машина не така ефективна як реальна, тому що доступ до апаратури в ній відбувається опосередковано.

Різні ВМ, на кожній з яких може бути встановлена своя власна ОС (які також називаються **гостьовими ОС**), часто використовуються для **серверного об'єднання**: різні сервіси (що повинні виконуватися на окремих машинах, щоб запобігти взаємовтручанню) запускаються в різних ВМ, проте на одній фізичній машині, що дозволяє економити апаратні ресурси.

Прикладні віртуальні машини

Прикладні віртуальні машини виконують звичайні програми всередині ОС. Вони зазвичай створюються коли програма запускається та знищуються після її завершення. Їхня ціль – забезпечити платформно-незалежне програмне середовище, яке

дозволяє абстрагуватися від конкретної апаратури та операційної системи, на якій виконується програма.

Прикладна ВМ забезпечує високорівневу абстракцію (наприклад, інтерпретатори високорівневих мов програмування – Lisp, Java, Python, Perl), в той час як системні ВМ зазвичай обмежуються низькорівневою абстракцією (машинним набором кодів). Сучасні прикладні ВМ, що реалізуються за допомогою інтерпретаторів, для підвищення швидкості виконання використовують компіляцію "на льоту" (англ. JIT – just-in-time).

Технології

Рідна емуляція – цей підхід полягає в простому розподіленні тих апаратних ресурсів, на яких запущена ВМ. Кожна копія ВМ обмежена реальною апаратурою. Відповідно, ми зможемо використовувати лише ті ОС, які підтримують нашу апаратуру.

Нерідна емуляція – в цьому випадку ВМ емулює апаратуру, яка може відрізнятися від тієї, на якій вона запущена. Це розширює круг ОС, які ми можемо на неї встановити.

Віртуалізація рівня ОС

Ядро ОС дозволяє створювати багато ізольованих один від одного просторів користувачів. В цьому випадку крах програми в одному просторі ніяк не вплине на програми в інших просторах.

Приклади та підтримка

Першою і до сьогодні однією з найкращих операційних систем, які підтримували концепцію віртуальної машини є операційна система VM (в межах колишнього СРСР також відома як СВМ – Система Віртуальних Машин) фірми IBM.

На окремих апаратних платформах можлива апаратна підтримка віртуальних машин. Вперше технологія апаратної підтримки віртуальних машин була реалізована в машині IBM-370 (початок 1970 рр.) як можливість завантаження мікропрограмного коду, який забезпечував додаткову функціональність центрального процесора IBM-370 для обслуговування віртуальних машин.

Розглянемо популярні платформи для створення та управління віртуальними машинами (віртуалізації).

Десктопні рішення:

1. **VMware Workstation Player/Pro**
   - *Продукти від VMware для створення, запуску й управління віртуальними машинами на робочих станціях.*
   - *Підтримує більшість операційних систем (Windows, Linux, macOS).*
2. **Oracle VirtualBox**
   - *Безкоштовне рішення для віртуалізації з відкритим кодом.*
   - *Підтримує широкий набір платформ і зручне для користувачів, які хочуть експериментувати з різними ОС.*
3. **Parallels Desktop**
   - *Програмне забезпечення для віртуалізації, створене спеціально для macOS.*
   - *Дозволяє запускати Windows, Linux або інші ОС паралельно з macOS.*
4. **Microsoft Hyper-V**
   - *Інтегроване рішення для віртуалізації в операційних системах Windows 10 Pro, Enterprise та Windows Server.*
   - *Підходить як для домашнього використання, так і для корпоративних середовищ.*
5. **QEMU**
   - *Відкрите програмне забезпечення для віртуалізації.*
   - *Часто використовується разом із KVM (Kernel-based Virtual Machine) на Linux.*

Серверні платформи:

1. **VMware vSphere/ESXi**
   - *Платформа для корпоративної віртуалізації, яка дозволяє керувати великими кластерними середовищами.*
   - *Забезпечує високу продуктивність і функції надійності для великих підприємств.*
2. **Proxmox Virtual Environment (Proxmox VE)**
   - *Відкрита платформа для управління віртуальними машинами й контейнерами.*
   - *Підтримує KVM і контейнерну віртуалізацію (LXC).*
3. **Citrix Hypervisor (раніше XenServer)**
   - *Корпоративна платформа для віртуалізації серверів, що підтримує високу масштабованість і стабільність.*

4. **Red Hat Virtualization (RHV)**
    - *Рішення на основі KVM для підприємств, інтегроване з Red Hat Enterprise Linux.*
5. **Microsoft Azure Virtual Machines**
    - *Хмарна платформа для створення та запуску віртуальних машин.*
    - *Пропонує широкий вибір конфігурацій для Windows і Linux-серверів.*
6. **AWS EC2 (Elastic Compute Cloud)**
    - *Віртуальні машини в хмарному середовищі Amazon Web Services.*
    - *Використовуються для створення масштабованих серверів для різних задач.*
7. **Google Compute Engine (GCE)**
    - *Частина Google Cloud Platform для створення віртуальних машин.*
    - *Підтримує індивідуальні налаштування та хмарні сервіси.*
8. **OpenStack**
    - *Відкрита платформа для управління хмарними обчисленнями та віртуалізації.*
    - *Широко використовується у великих корпоративних середовищах.*

Контейнерна віртуалізація:

1. **Docker**
    - *Технологія для запуску контейнерів, яка відрізняється легкістю й швидкістю.*
    - *Використовується для ізоляції додатків.*
2. **Kubernetes**
    - *Платформа для оркестрації контейнерів, яка дозволяє масштабувати й автоматизувати розгортання додатків.*

Інші платформи:

1. **Xen Project**
    - *Відкрите рішення для віртуалізації з високою продуктивністю.*
    - *Використовується в корпоративних і дослідницьких середовищах.*
2. **Nutanix AHV**
    - *Гіперконвергентна платформа для віртуалізації, яка інтегрує серверні ресурси, мережі та зберігання даних.*

3. **KVM (Kernel-based Virtual Machine)**
    - *Віртуалізація на рівні ядра Linux, що дозволяє запускати кілька ОС одночасно.*

Ці платформи використовуються залежно від потреб: домашнє тестування, розробка програм, корпоративна віртуалізація чи хмарна інфраструктура.

Контрольні питання

1. В яких випадках використовується віртуалізація?
2. Визначення віртуальної машини.
3. Технології віртуалізації (емуляції).
4. Наведіть приклади віртуальних машин.

Тема: VM Ware

План

1. Загальна інформація.
2. Огляд інтерфейсу VMware Workstation.
3. Основні можливості.

VMware, Inc. (NYSE: VMW) — компанія-розробник програмного забезпечення, найбільш відома продуктами для віртуалізації x86-сумісних комп'ютерів, тобто програмних середовищ, що дозволяють на одному фізичному комп'ютері імітувати роботу кількох віртуальних машин, запускаючи на кожній з них різні операційні системи і застосунки. Популярні продукти компанії VMware vSphere, VMware Workstation, VMware Server, VMware ESX Server, VMware VirtualCenter, VMware ACE, VMware Player та кілька інших. Компанія перебуває у власності EMC Corporation (як незалежний підрозділ), основний підрозділ компанії розташований в Пало-Альто, Каліфорнія.

Настільне програмне забезпечення

VMware випустив свій перший продукт, VMware Workstation, в 1999 році. Цей набір програмного забезпечення дозволяє користувачам запускати кілька екземплярів x86 або x86-64-сумісних операційних систем на одному фізичному комп'ютері. VMware Fusion забезпечує подібну функціональність для споживачів платформи MacIntel, разом з повною сумісністю з віртуальними машинами, створеними іншою продукцією VMware.

Для споживачів без ліцензії на використання VMware Workstation або VMware Fusion, VMware пропонує безкоштовний продукт VMware Player, у якому можна запускати вже сконфігуровані віртуальні машини, а також створювати нові (починаючи з версії 3.0).

Серверне програмне забезпечення

VMware пропонує два продукта віртуалізації для серверів: VMware ESX Server (колишня назва «ESX Server») та VMware Server (колишня назва «GSX Server»).

VMware ESX, продукт рівня підприємства, забезпечує більшу продуктивність, ніж вільний VMware Server. Крім того, VMware ESX

інтегрується у VMware Virtual Infrastructure, що надає додаткові послуги для збільшення надійності і керованості серверного застосування. Продукт VMware Server пропонує інтерфейс користувача, подібний до VMware Workstation у вигляді і функціональності.

VMware Server також поширюється вільно, подібно до VMware Player, але водночас здатний створити віртуальні машини.

Починаючи з версії ESXi 3.5 update 2, гіпервізор VMware розповсюджується безоплатно. Гіпервізор дозволяє розділити комп'ютер на кілька віртуальних машин. Аналогічний інструмент Microsoft — Hyper-V — коштує $28.

Приєднання до Linux Foundation

У серпні 2008 VMware приєдналася до некомерційної організації Linux Foundation. Після вступу в Linux Foundation компанія VMware планує передати розробникам співтовариства відкритий код низки своїх технологій. Зокрема, йдеться про інтерфейс Virtual Machine Interface (VMI) і інтерфейси паравіртуалізації. Крім того, VMware надаватиме допомогу в поліпшенні засобів віртуалізації програмних платформ Linux.

Конкуренти

За даними звіту аналітичної компанії IDC «Долі ринку світових постачальників ПЗ віртуалізації в 2007 р.», лідером ринку є VMware з часткою 76% загальної виручки ($1,283 млрд). Найбільшими постачальниками продуктів віртуалізації на світовий ринок, крім VMware, є IBM, HP, Parallels та Microsoft.

У цілому оборот світового ринку віртуалізації в 2007 р., згідно з оцінками IDC, зріс на 68,5% і досяг відмітки в $1,681 млрд проти $997,6 млн в 2006 р. Для порівняння, темпи приросту в 2006 р. склали 58,7%. За прогнозами IDC, зростання ринку ПЗ віртуалізації продовжиться і впродовж найближчих років. Дослідники називають технологію віртуалізації основою для побудови динамічної і швидко реагуючої на потребі бізнесу IT-інфраструктури.

VMware Workstation — гіпервізор компанії VMware для платформ x86 і x86-64, що дозволяє запустити на комп'ютері декілька операційних систем одночасно. Кожна віртуальна машина може виконувати свою власну операційну систему, включаючи Microsoft

Windows, Linux, BSD і MS-DOS. VMware Workstation розроблений компанією VMware Inc., підрозділом корпорації EMC.

VMware Workstation підтримує з'єднання дійсних мережевих хостів та обміну фізичних дисків і USB пристрої з віртуальною машиною. Крім того, за допомогою VMware Workstation можна імітувати образи дисків. Можна змонтувати файл ISO у віртуальний привід оптичних дисків, так що віртуальна машина побачить його як реальний диск.

У VMware Workstation є можливість призначати кільком віртуальним машинам команди, які потім можуть бути запущені, закриті, перервані або відновлені як єдиний об'єкт, що робить її особливо корисною для тестування клієнт-серверних середовищ.

VMware Player на відміну від Workstation з аналогічною, але обмеженою функціональністю, був безкоштовним. У 2015 році ці два пакети були об'єднані в VMware Workstation 12, з безкоштовною версією VMware Workstation Player для некомерційного використання. VMware Workstation 12 по кількості проданих ліцензійних екземплярів обігнала навіть саму VMware Workstation Pro.Зараз, через створення VMware Workstation безкоштовною, версію, менш довершену, за інформацією блогу VMware Workstation Pro закрито.

Програмне забезпечення VMware Workstation Pro 12 пропонує новітні можливості для професіоналів віртуальних машин. VMware Workstation Pro 12 призначений для розробки, тестування, демонстрації та розгортання програмного забезпечення шляхом одночасного запуску декількох операційних систем x86 на одному ПК. Завдяки підтримці останніх версій Windows і Linux, новітніх процесорів і обладнання, а також підключенню до VMware vCloud Air і VMware vSphere, VMware Workstation 12 ідеально підходить для підвищення операційної ефективності, економії часу і освоєння хмари.

Підтримка Windows 10 і інших систем

Робоча станція 12 Pro ідеально підходить для розробки та тестування в середовищах Windows 10 або Linux. Робоча станція 12 Pro дозволяє скористатися новими можливостями Windows 10 (голосовий помічник Cortana, новий браузер Edge і т.д.).

Для організацій та користувачів, які працюють з найновішими дистрибутивами Linux, Workstation 12 Pro підтримує Ubuntu 15.04, Red Hat Enterprise Linux 7.1, Fedora 22 та інші. Ви можете створити вкладені гіпервізори для роботи з Hyper-V або VMware ESXI і vSphere, щоб створити універсальну платформу для навчання, демонстрації та

тестування. Робоча станція 12 Pro також додала підтримку VMware Photon.

Потужна 3D графіка

Робоча станція 12 Pro підтримує DirectX 10 і OpenGL 3.3, що дає вам гнучкість для запуску 3D-додатків і забезпечує кращу візуалізацію даних. Він також надає розширені опції для запуску додатків AutoCAD або SOLIDWORKS.

Підтримка екранів з високою роздільною здатністю

Робоча станція 12 Pro була оптимізована для дисплеїв планшетів 4K UHD (3840 x 2160), QHD+ (3200x1800) і x86.

Що нового у створенні віртуальних машин

Створюйте потужні віртуальні машини з до 16 vCPUs, віртуальними дисками на 8 Тб і до 64 Гб пам'яті для запуску найвимогливіших додатків.

Підтримка сучасних апаратних рішень

Рішення дозволяє працювати на планшетах з движком Intel через віртуальні датчики. Ви також можете використовувати найновіші планшети Microsoft Surface з віртуальним акселометром, гіроскопом, компасом та датчиками освітленості, щоб дозволити програмам, що працюють у віртуальних машинах, реагувати, коли користувач рухається, обертається та виконує інші дії на планшеті. Підтримуються 64-розрядні процесори Intel x86, включаючи мікроархітектури Broadwell і Haswell.

Покращене підключення

Робоча станція 12 Pro використовує переваги новітнього аудіообладнання HD з об'ємним звуком 7.1 каналу, пристроями USB 3.0 і технологією Bluetooth для підключення веб-камери, гарнітури або принтера до віртуальної машини. Крім того, Workstation 12 Pro покращує продуктивність Skype або Lync всередині гостьових віртуальних машин.

Створення віртуальних мереж

Покращена підтримка IPv6, включаючи мережеві адреси IPv6-to-IPv4, що дозволяє створювати більш складні мережеві топології, ніж будь-коли раніше. За допомогою Workstation 12 Pro ви можете додавати та видаляти віртуальні мережі IPv4 або IPv6, а також створювати власні конфігурації віртуальної мережі, які ідеально підходять для тестування та демонстрації вашої інфраструктури.

Переваги хмари

Підключення до VMware vCloud Air, а також поліпшена інтеграція з серверами Sphere і ESXi, що дозволяє легко розширювати і масштабувати віртуальні машини в хмарі.

Інтерфейс користувача

Інтерфейс Workstation 12 включає спрощені меню, динамічні значки, вкладки, екрани параметрів і бібліотеку віртуальних машин з можливістю пошуку.

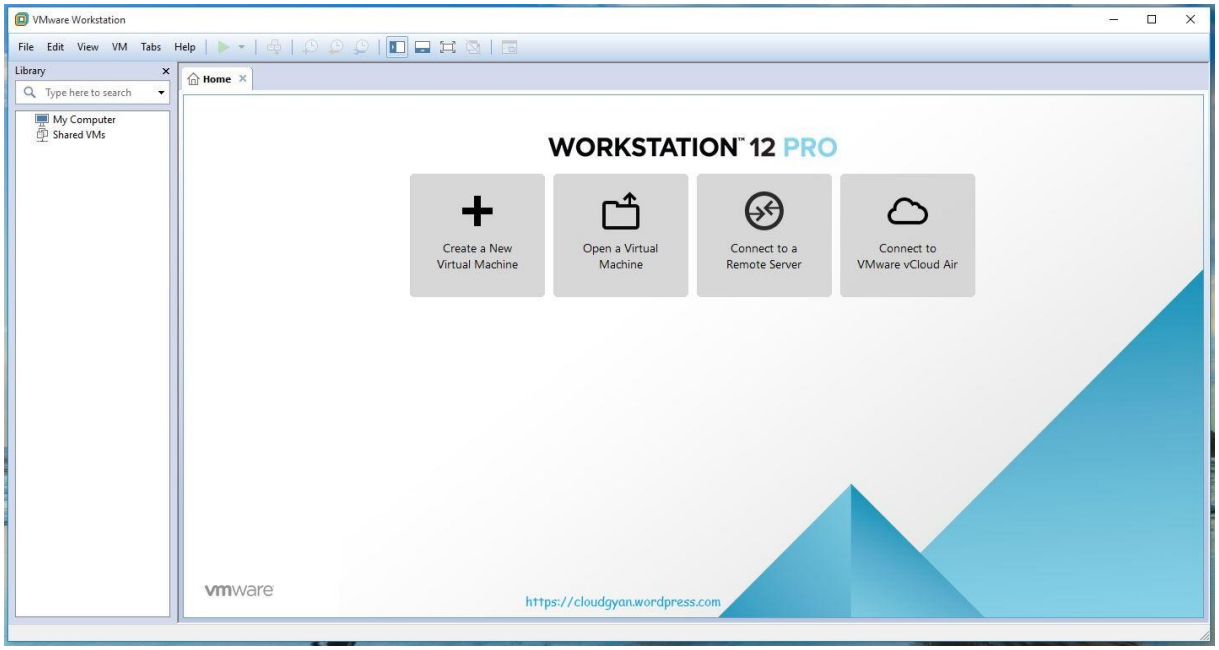


Рис. 1.1. Інтерфейс програмного продукту VMware Workstation 12 Pro

Обмежені віртуальні машини

За допомогою Workstation 12 IT-адміністратори можуть створювати політики для віртуальних машин і керувати ними, а також надавати додатки кінцевим користувачам як контейнери віртуальних

машин з обмеженим доступом. Рішення підтримує захист корпоративного контенту, обмежуючи доступ до налаштувань віртуальної машини Workstation, таким як операції перетягування, копіювання та вставки, а також підключення usb-пристроїв. Крім того, віртуальні машини в Workstation 12 можна захистити за допомогою шифрування і підказок пароля, щоб запобігти несанкціонованим змінам налаштувань корпоративної віртуальної машини.

Віртуальні машини з обмеженим терміном служби

Для короткострокових проектів, адаптації тимчасових співробітників або просто для оцінки програмного забезпечення, Workstation надає можливість створювати обмежені віртуальні машини, які перестануть працювати в даний момент часу. Включена віртуальна машина відправляє запити на сервер через рівні проміжки часу, зберігаючи поточний системний час в обмеженому файлі політики віртуальної машини як останню надійну позначку часу. Після закінчення терміну дії віртуальної машини її робота автоматично призупиняється і перезапустити її може тільки IT-адміністратор.

Перехресна сумісність віртуальних машин

Робоча станція забезпечує сумісність з багатьма іншими продуктами та платформами VMware. За допомогою Workstation 12 ви можете створювати віртуальні машини, які можуть запускати багато інших продуктів VMware, а також обмежені віртуальні машини для використання з VMware Fusion Pro і VMware Player Pro.

Контрольні питання

1. Які основні функції виконує гіпервізор VMware Workstation, і як він дозволяє використовувати кілька операційних систем на одному комп'ютері?
2. Чим відрізняються серверні продукти VMware ESX Server і VMware Server, і для яких сценаріїв використання вони оптимально підходять?
3. Які переваги надає інтеграція VMware Workstation з хмарними сервісами, такими як VMware vCloud Air, VMware vSphere і ESXi?
4. Які технології та функції віртуалізації зробили VMware лідером ринку з часткою 76% у 2007 році за звітом IDC, і як це вплинуло на розвиток IT-інфраструктури?

Тема: VirtualBox

План

1. Загальна інформація.
2. Огляд інтерфейсу VirtualBox.
3. Основні можливості.

VirtualBox — це програма віртуалізації для операційних систем, розроблена німецькою фірмою Innotek, зараз вона належить Oracle Corporation. Вона встановлюється на наявну операційну систему, яка називається хостовою, усередину цієї програми встановлюється інша операційна система, яку називають гостьовою операційною системою.

Підтримується основними операційними системами Linux, FreeBSD, Mac OS X, OS/2 Warp, Microsoft Windows, які підтримують роботу гостьових операційних систем FreeBSD, Linux, OpenBSD, OS/2 Warp, Windows і Solaris.

Починаючи з 2007 року, за спостереженнями DesktopLinux.com, VirtualBox займає третє місце за популярністю серед програмних засобів, які дозволяють запуск Windows-програм на стільниці Linux.

Історія

Програма була створена компанією Innotek з використанням початкового коду Qemu. Перша публічно доступна версія VirtualBox з'явилась 15 січня 2007 року. В лютому 2008 року Innotek був викуплений компанією Sun Microsystems, модель поширення VirtualBox при цьому не змінилася. В січні 2010 року Sun Microsystems була поглинена Oracle Corporation, модель поширення залишилась попередньою.

Ключові можливості:

- *Крос-платформовість*
- *Модульність*
- *Жива міграція*
- *Підтримка USB 2.0, коли пристрої хост-машини стають доступними для гостьових ОС (лише в пропрієтарній версії)*
- *Підтримка 64-бітних гостьових систем (починаючи з версії 2.0), навіть на 32-бітних хост-системах (починаючи з версії 2.1, для цього потрібна підтримка технології віртуалізації процесором)*

- *Підтримка SMP на стороні гостьової системи (починаючи з версії 3.0, для цього потрібна підтримка технології віртуалізації процесором)*
- *Вбудований RDP-сервер, а також підтримка клієнтських USB-пристроїв поверх протоколу RDP (лише в пропрієтарній версії)*
- *Експериментальна підтримка апаратного 3D-прискорення (OpenGL, DirectX 8/9 (з використанням коду wine) (лише в 32-бітних Windows XP і Vista)), для гостьових DOS / Windows 3.x / 95 / 98 / ME підтримка апаратного 3D-прискорення не передбачена*
- *Підтримка образів твердих дисків VMDK (VMware) і VHD (Microsoft Virtual PC), включаючи снапшоти (починаючи з версії 2.1)*
- *Підтримка iSCSI (лише в пропрієтарній версії)*
- *Підтримка віртуалізації аудіопристроїв (емуляція AC97 або SoundBlaster 16 на вибір)*
- *Підтримка різноманітних видів мережевої взаємодії (NAT, Host Networking via Bridged, Internal)*
- *Підтримка ланцюжка збережених станів віртуальної машини (snapshots), до яких можна повернутися з будь-якого стану гостьової системи*
- *Підтримка Shared Folders для простого обміну файлами між хостовою та гостьовою системами (для гостьових систем Windows 2000 і новіше, Linux та Solaris).*
- *Підтримка інтеграції робочих столів (seamless mode) хостової та гостьової ОС*
- *Є можливість вибору мови інтерфейсу (підтримується і україномовний інтерфейс).*
- *Підтримка Extensible Firmware Interface (EFI) (починаючи з версії 3.1)*
- *Починаючи з версії 5:*
- *Підтримка USB 3.0 (лише в пропрієтарній версії) (вимагає встановлення VirtualBox Extension Pack)*
- *Шифрування дисків віртуальних машин в реальному часі за алгоритмом AES з довжиною ключа 256 біт (вимагає встановлення VirtualBox Extension Pack)*
- *Підтримка "гарячого" підключення SATA дисків*
- *Робота в окремих процесах, які не зв'язані з інтерфейсом*
- *Підтримка NDIS6 для Windows (починаючи з Windows Vista)*
- *Підтримка HiDPI*
- *Підтримка Drag-and-drop для гостьових систем Windows, Linux та Solaris*

Відмінності між відкритою та закритою версіями

Існує дві версії, які відрізняються за ліцензією та функціональністю:

- *Відкрита версія (OSE, англ. Open Source Edition) — початкові коди доступні під ліцензією GNU GPL, відповідно немає обмежень у використанні. Функціональність аналогічна повній версії, за винятком деяких особливостей, доступних для корпоративних клієнтів:*
- *RDP сервер — дозволяє підключатися до віртуальної системи віддалено з допомогою будь-якого RDP сумісного клієнта;*

- *Підтримка USB — дозволяє передавати віртуальній машині USB пристрої;*
- *USB поверх RDP — дозволяє надати віддалений доступ до USB пристроїв.*
- *Повна версія поширюється лише в бінарному вигляді під власницькою ліцензією (PUEL), безкоштовна — лише для особистого використання.*

Інтерфейс користувача

Рис. 1.2. Інтерфейс програмного продукту VirtualBox

Чим відрізняється VMware Workstation Player та VirtualBox ?

Віртуальні машини стають ключовим інструментом для тих, хто прагне до максимальної безпеки в онлайн-просторі. Вони створюють ізольоване середовище, яке ефективно відсікає потенційні загрози та шкідливе ПЗ. Користування віртуальною машиною зменшує ризик компрометації основної системи та забезпечує додатковий шар захисту від вторгнень. Таким чином, для тих, хто прагне зберігати свої дані в безпеці, віртуальні машини стають незамінним інструментом в сучасному цифровому світі.

VMware Player та VirtualBox представляють собою дві відомі віртуалізаційні платформи для створення віртуальної машини. Їхня ключова різниця полягає у тому, що VMware Player безкоштовний лише для особистого користування, тоді як VirtualBox є повністю безкоштовним програмним забезпеченням з відкритим кодом, доступним для особистого та комерційного використання. VMware Player розробляється компанією VMware, лідером у сфері віртуалізації, тоді як VirtualBox належить Oracle. "Oracle" – це американська корпорація, яка спеціалізується на виробництві програмного забезпечення, обладнання для обчислювальної техніки та інших продуктів і послуг у сфері інформаційних технологій.

VirtualBox завдяки її прозорій роботі має більший набір особливостей та налаштувань, отже тому ми, вважаємо, цю віртуальну машину найкращою, Також, VirtualBox надає гнучкіші опції і це все завдяки своєму відкритому коду. Ще й до всього сумісность у VirtualBox, завдяки своєму відкритому характеру, підтримує ширший діапазон операційних систем порівняно з VMware Player.

Обидва інструменти, VMWare Player та VirtualBox, мають свої переваги, і кожен із них може бути кращим в залежності від конкретного сценарію використання. Найкращий спосіб визначити, яка програма найкраще підходить для ваших потреб – це встановити обидві та експериментувати з ними. Тільки практика допоможе вам розібратися, яка віртуальна машина найкраще відповідає вашим вимогам.

Контрольні питання

1. Що таке хостова і гостьова операційна система в контексті VirtualBox?
2. Які операційні системи підтримуються як гостьові у VirtualBox?
3. Які ключові можливості пропонує VirtualBox для створення та управління віртуальними машинами?
4. Чим відрізняється відкрита версія VirtualBox від пропрієтарної?

Тема: Microsoft Azure

План

1. Загальна інформація.
2. Огляд інтерфейсу Microsoft Azure.
3. Основні можливості.

Microsoft Azure («Майкрософт Ежур»), часто згадується просто як Azure — хмарна платформа та інфраструктура корпорації Microsoft, призначена для розробників застосунків хмарних обчислень (англ. cloud computing) і покликана спростити процес створення онлайнових додатків.

Історія

Корпорація Microsoft представила платформу Windows Azure 27 жовтня 2008 року.

Microsoft Azure дозволяє розгортати додатки як за допомогою Microsoft .NET і Visual Studio, так і за допомогою інших інструментів. Платформа працює на серверах Microsoft, доступ до неї можна отримати за протоколами HTTP, Representational State Transfer (REST), WS-* і Atom Publishing Protocol (AtomPub).

Платформа Azure Services Platform включає п'ять основних компонентів. Це сама операційна система Windows Azure, що керує дисковим простором, додатками і мережами, і Microsoft SQL Services для роботи з базами даних. Також в платформу входять Microsoft .NET Services, Live Services, і бізнес-компонент, що включає Microsoft SharePoint Services і Microsoft Dynamics CRM Services.

Концепція хмарних обчислень — це використання обчислювальних потужностей, дискового простору і каналів зв'язку «обчислювальної хмари» для виконання трудомістких завдань. Навантаження між комп'ютерами, що входять в цю хмару, розподіляється автоматично. Більшість хмарних застосунків працюють у браузері.

На момент оголошення, розробка Windows Azure, за словами представників Microsoft, все ще перебуває на ранній стадії. Очікується, що можливості системи будуть значно розширені. Крім того, всі сервіси для Windows Azure повинні бути побудовані на базі наперед

заданих шаблонів, хоча Microsoft планує незабаром значно збільшити їхню кількість, а також дозволити створювати застосунки, які не вписуються в шаблони.

За оцінками аналітиків, анонс Azure є «захисним маневром», щоб нинішні клієнти Microsoft, які користуються її серверами й іншими продуктами, не переходили на хмарні рішення від таких компаній, як Amazon чи IBM, що вже надають низку сервісів для зберігання даних і обчислювальні потужності «в хмарі».

У грудні 2009 Microsoft об'єднав існуючі підрозділи, що займалися Windows Server та Azure, в один Server & Cloud Division (SCD).

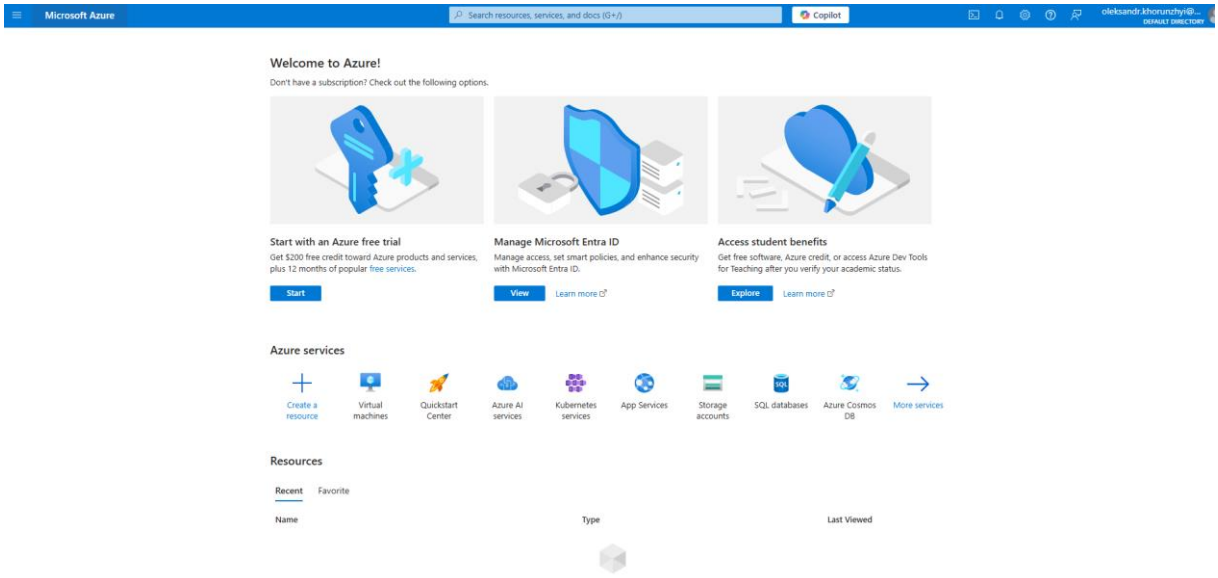


Рис. 1.3. Інтерфейс програмного продукту Microsoft Azure

Побудова

Платформа виготовлена з групи із трьох технологій, що забезпечують спеціалізований набір можливостей для розробників. Більше того, платформу Windows Azure можна використовувати в додатках, що працюють локально на комп'ютерах користувачів і додатків, які працюють в хмарі.

Платформа Windows Azure складається з таких компонентів:

Windows Azure — надає середовище виконання для додатків, заснованих на операційних системах, та на Windows Server, а також місця для зберігання даних. Система працює на віртуальних машинах за допомогою, аналогічної технології Hyper-V.

Обчислення — відповідає за обчислення розміщення додатків.

Зберігання — відповідає за зберігання даних в хмарі.

SQL Azure — надає можливість використовувати реляційну базу даних для запуску в хмарі.

Платформа Windows Azure AppFabric — компонент, який забезпечує додаткову функціональність у вигляді послуг.

Створення програм

На додаток до технології .NET при створенні програм для Azure можуть використовуватися такі технології, як Java, PHP, C / C++ або Python.

Важливим компонентом є SDK емулятор хмари. Застосунок працює на емуляторі, він має доступ до бібліотек, зареєстрованих у місцевому глобальному кеші збірок (GAC), для реєстрації та конфігурації комп'ютера. Ці послуги доступні не на фактичній платформі. Емулятор дозволяє запам'ятовувати діагностичну інформацію на консолі або використовувати Windows Azure Diagnositcs . Уся інформація зберігається в спеціальній таблиці в Windows Azure Storage. Всі екземпляри, що працюють на емуляторі, мають привілеї адміністратора і ті, які працюють на платформі є силою стандартного користувача Windows. Емулятор неповною мірою відображає поведінку балансування навантаження, використовувану на Windows Azure Platform.

Список сервісів Azure налічує більш ніж 600 різних, деякі з них перераховані нижче.

Зберігання даних

Служби зберігання даних надають **REST** та **SDK API** для зберігання та доступу до даних у хмарі.

Table Service надає можливість програмам зберігати структурований текст у розподілених колекціях, доступ надається за ключем розділу та первинним ключем. Є NoSQL (не-реляційною) базою даних.

Blob Service дозволяє зберігати неструктурований текст та бінарні дані як blob'и, які доступні за HTTP(S) адресою. Blob service також надає способи контролю доступу до даних.

Queue Service забезпечує асинхронну комунікацію для програм за допомогою повідомлень-запитів.

File Service надає доступ до даних у хмарі через REST API або SMB протокол.

Безконтактні сенсорні контролери

В 2019 році компанія Microsoft випустила безконтактний сенсорний ігровий контролер Azure Kinect Developer Kit, який мав покращену камеру, мікрофони та інші сенсори. Цей комплект був призначений для розробників, які прагнули використовувати технологію Kinect у своїх проєктах з використанням хмарної платформи Microsoft Azure. Виробництво Azure Kinect Developer Kit тривало до серпня 2023 року, тобто до часу, коли компанія Microsoft оголосила про припинення його виробництва через зміну потреб клієнтів та партнерів.

Машинне навчання

Сервіс Microsoft Azure Machine Learning (Azure ML) є частиною Cortana Intelligence Suite, що дозволяє взаємодію з даними з використанням природної мови і усно за допомогою Cortana.

Конкуренти

- ✓ *Amazon Web Services*
- ✓ *Engine Yard*
- ✓ *Google App Engine*
- ✓ *Heroku*
- ✓ *Force.com*
- ✓ *Skytap*
- ✓ *VMware*
- ✓ *Rackspace Cloud*
- ✓ *GoGrid*

Контрольні питання

1. Що таке Microsoft Azure і які основні можливості вона надає для розробників хмарних додатків?
2. Які основні компоненти входять до складу платформи Microsoft Azure?
3. Які мови програмування та технології, окрім .NET, можна використовувати для створення додатків у Microsoft Azure?
4. Які сервіси Microsoft Azure забезпечують зберігання даних, і як вони працюють (наприклад, Table Service, Blob Service, Queue Service)?

Розділ 2. Адміністрування Windows 10/11

Тема: Специфікація ОС. Мінімальні вимоги

План

1. Короткий огляд.
2. Системні вимоги.
3. Особливості Windows 10.
4. Поради для встановлення та налаштування.
5. Заключення.

Windows 10 — основний випуск ОС Windows NT компанії Microsoft. Вона є прямим наступником Windows 8.1, яка була оприлюднена майже двома роками раніше. Вона була випущена у виробництво 15 липня 2015 року, а згодом — у роздрібну торгівлю 29 липня 2015 року. Windows 10 була доступна для завантаження через MSDN та TechNet, як безоплатне оновлення для користувачів роздрібних копій Windows 8 та Windows 8.1 через Windows Store, а також для користувачів Windows 7 через Windows Update. Windows 10 отримує нові збірки на постійній основі, які доступні без додаткових витрат для користувачів, на додаток до додаткових тестових збірок Windows 10, які доступні для Windows Insiders. Пристрої в корпоративному середовищі можуть отримувати ці оновлення повільніше або використовувати довгострокові етапи підтримки, які отримують лише критичні оновлення, такі як виправлення безпеки, упродовж десятирічного терміну розширеної підтримки. У червні 2021 року корпорація Microsoft оголосила, що основна підтримка версій Windows 10, які не входять у канал довгострокового обслуговування (LTSB/LTSC) 2016 року або пізніше, завершилася 13 жовтня 2020 року і розширена підтримка завершиться 14 жовтня 2025 року. Відповідно, звичайні користувачі перестануть отримувати патчі безпеки та будуть змушені перейти на нову ОС. Більше пощастило корпоративним клієнтам – вони зможуть продовжити користуватися Windows 10 навіть після припинення підтримки, аж до 2028 року, однак за додаткову плату.

Windows 10 набула загалом ствердні відгуки після свого першого випуску. Критики високо оцінили рішення Microsoft надати інтерфейс, орієнтований на настільні комп’ютери, як і в попередніх версіях Windows, на відміну від орієнтованого на планшети підходу Windows

8, хоча режим сенсорного інтерфейсу Windows 10 критикували за те, що він містить регресивні елементи сенсорного інтерфейсу її попередниці. Критики також високо оцінили поліпшення комплектного програмного забезпечення Windows 10 у порівнянні з Windows 8.1, інтеграцію Xbox Live, а також функціональність і можливості персонального асистента Cortana і заміну Internet Explorer на Microsoft Edge. Водночас ЗМІ критично оцінили зміни в поведінці ОС, зокрема, обов'язкове встановлення оновлень, занепокоєння щодо конфіденційності під час збору даних, що здійснюється ОС для Microsoft та її партнерів, а також тактику просування операційної системи, що нагадує рекламне ПЗ, після її релізу.

Корпорація Microsoft спочатку мала на меті інсталювати Windows 10 на понад мільярд пристроїв протягом трьох років із моменту її випуску, ця мета була досягнута майже через п'ять років після випуску 16 березня 2020 року і на сьогодні Windows 10 є найбільш використовуваною версією практично в усіх країнах світу. До січня 2018 року Windows 10 перевершила Windows 7 як найпопулярніша версія Windows у всьому світі. Станом на серпень 2022 року, Windows 10, за оцінками аналітиків, має 72 % частку ПК з Windows, що все ще в 6,2 раза перевищує частку її наступниці Windows 11 (і в 6,0 разів — Windows 7). Ця частка знижується з пікового значення 82 % у січні 2022 року, , оскільки Windows 11, яка зараз є другою за популярністю версією Windows у багатьох країнах, є другою найпопулярнішою версією Windows. Частка Windows 10 серед усіх ПК становить 58 % (решта — інші версії Windows та інші ОС, такі як macOS та Linux), а 22 % всіх пристроїв (зокрема мобільні, планшетні та консольні) працюють під управлінням Windows 10. 24 червня 2021 року компанія Microsoft анонсувала наступницю Windows 10 — Windows 11, яка вийшла 5 жовтня 2021 року.

Windows 10 — фінальна версія Windows, яка підтримує 32-розрядні процесори (на базі IA-32 та ARMv7) та пристрої з прошивкою BIOS. Для її наступниці, Windows 11, потрібен пристрій, який використовує прошивку UEFI і 64-розрядний процесор у будь-якій підтримуваній архітектурі (x86–64 для x86 і ARMv8 для ARM).

Користувацький інтерфейс

Оформлення Windows 10 засновано на принципах дизайну під назвою Metro, для якого притаманні прямокутні одноколірні форми, великі шрифти, схематичні іконки та плавні ефекти переходів.

У Windows 10 повернуто меню «Пуск», за структурою подібне до меню «Пуск» з версій до Windows 8, але з представленням застосунків та інформації в плитках. Сповіщення від системи та застосунків (поради, помилки, події календаря тощо) збираються в Центрі сповіщень, що являє собою панель з правого боку екрана, яка розгортається значком на панелі завдань. Додатково в Центрі сповіщень представлені елементи управління режимами роботи комп'ютера, підключеннями до бездротових пристроїв та іншими параметрами системи.

Windows 10 має вдосконалену функцію мультивіконності Snap Assist, яка допомагає розподіляти простір екрана між вікнами. Вона дозволяє розташувати на робочому столі до чотирьох вікон одночасно. При цьому Windows 10 підказує, які ще додатки запущені в системі і як їх можна розмістити. В цій ОС додано функцію створення кількох робочих столів (подібну функцію можна побачити в Apple OS X та Ubuntu).

Служба для входу до системи за допомогою біометричних даних Windows Hello дозволяє входити в систему за допомогою свого обличчя або в тих застосунках і сайтах, котрі її підтримують. Паралельно із Windows Hello. Microsoft запускає систему, котра називається Microsoft Passport, що призначається для заміни пароля за допомогою особистих пристроїв, таких як смартфони, щоб можна було пройти аутентифікацію в корпоративних системах і онлайн-контенті.

Додатки й функції

Cortana — особистий помічник. Secure Boot — можливість використовувати апаратну віртуалізацію для запобігання виконання шкідливих програм в момент старту ОС. Virtual Smart Cards — можливість використання двофакторної авторизації. Miracast — дозволяє транслювати зображення екрана через проєктор або телевізор. Зокрема, з використання технології WiDi. Hyper-V — система віртуалізації на основі гіпервізора (запуск кількох ОС на одному пристрої). Enterprise Data Protection — технологія для захисту корпоративних даних, де дозволено використовувати особисті пристрої співробітника. Device Guard — технологія для запуску тільки дозволених застосунків. Microsoft Passport — використання альтернативних типів автентифікації в ОС, зокрема біометрії. Microsoft Edge — браузер для Інтернету. Azure Active Directory — хмарна активна директорія. Microsoft Store — магазин застосунків, де можна

розміщувати власні розробки. MDM — управління мобільними пристроями для доступу до віртуальної приватної мережі.

Вимоги до системи

Основні вимоги для установки Windows 10 такі ж, як і для Windows 8.1. Пристрої, що працюють на Windows 8.1 RTM не підтримуються. Windows 10 працює на всіх типах сучасних гаджетів (смартфон, планшет, комп'ютер, ноутбук, телевізор та приставка). Windows Phone не супроводжує цю ОС, замість неї введено Windows 10 зі спрощеним для мобільних пристроїв інтерфейсом (Windows Mobile). Якщо користувач підключає до мобільного пристрою клавіатуру і монітор, ОС пропонує перейти на повноцінну модель використання ОС (функція Continium). Якщо пристрій під'єднаний до Інтернету і користувач під'єднав до комп'ютера пристрій, незнайомий для комп'ютера або ОС, Windows сама шукає відповідний драйвер

Апаратні вимоги для Windows 10 Windows 10 Specifications & Systems Requirements. ***Windows Help***. **Microsoft.** Архів оригіналу за 1 травня 2018.[31].

Компонент	Мінімальні	Рекомендовані
Процесор	Тактова частота 1 ГГц Архітектура IA-32 або x64 з підтримкою PAE, NX та SSE2[32][33]. Процесори x64 також мають підтримувати CMPXCHG16B, PrefetchW та LAHF/SAHF інструкції.	
Оперативна пам'ять (RAM)	**IA-32:** 1 ГБ **x64:** 2 ГБ	4 ГБ
Відеокарта	Графічний пристрій з підтримкою DirectX 9 WDDM 1.0 або новіший	Графічний пристрій з підтримкою DirectX 10 WDDM 1.3 або новіший
Екран пристрою	800×600 пікселів	Н/Д
Пристрій введення	Клавіатура та миша	Мультитач дисплей
Пам'ять на жорсткому диску	До 1903: **IA-32:** 16 ГБ; **x64:** 20 ГБ Після 1903: обидва 32 ГБ[34].	Н/Д
Інше	Н/Д	UEFI v2.3.1 Errata B з Microsoft Windows Certification Authority Trusted Platform Module (TPM) 2.0 Інтернет з'єднання

Рис. 2.1. Інтерфейс програмного продукту Microsoft Azure

Поради для встановлення та налаштування

Перевірка сумісності комп'ютера

Перевірка системних вимог	Переконайтеся, що ваш комп'ютер відповідає мінімальним системним вимогам для Windows 10. Це включає процесор, оперативну пам'ять, місце на диску, графічний адаптер та інші апаратні характеристики.
Інструмент "PC Health Check"	Скачайте та використовуйте інструмент "PC Health Check" від Microsoft. Цей інструмент дозволяє швидко перевірити сумісність вашого комп'ютера з Windows 10 та виявити потенційні проблеми.
Перевірка драйверів та оновлень	Переконайтеся, що всі драйвери та прошивки вашого обладнання оновлені до останніх версій. Це допоможе уникнути проблем під час встановлення та роботи нової ОС.
Перевірка програмного забезпечення	Перевірте, чи всі важливі програми та додатки, які ви використовуєте, сумісні з Windows 10. Це особливо важливо для спеціалізованих або застарілих програм.

Кроки підготовки до встановлення ОС

Резервне копіювання даних	Перед початком встановлення створіть резервну копію всіх важливих файлів і даних. Ви можете скористатися зовнішніми накопичувачами або хмарними сервісами для зберігання копій.
Створення інсталяційного носія	Скачайте засіб для створення інсталяційного носія Windows 10 з офіційного сайту Microsoft. Ви можете створити завантажувальну флешку або DVD-диск.
Перевірка налаштувань BIOS/UEFI	Переконайтеся, що налаштування BIOS або UEFI вашого комп'ютера правильні для встановлення Windows 10. Це може включати увімкнення завантаження з USB, відключення Secure Boot та інші необхідні зміни.
Від'єднання непотрібних пристроїв	Відключіть усі непотрібні зовнішні пристрої (принтери, зовнішні жорсткі диски, тощо) перед початком встановлення. Це допоможе уникнути конфліктів під час інсталяції.
Початок встановлення	Вставте інсталяційний носій та перезавантажте комп'ютер. Дотримуйтесь інструкцій на екрані для завершення процесу встановлення.

Оптимізація налаштувань для кращої роботи системи

Оновлення Windows	Після встановлення ОС обов'язково виконайте всі доступні оновлення Windows через Центр оновлень. Це забезпечить останні виправлення безпеки та оптимізації.
Видалення непотрібних програм	Видаліть або відключіть непотрібні стандартні програми, які можуть сповільнювати роботу вашої системи. Це можна зробити через меню "Панель керування" або "Параметри".
Оптимізація запуску системи	Вимкніть непотрібні програми, які запускаються автоматично під час завантаження системи. Це можна зробити через "Диспетчер завдань" у вкладці "Автозавантаження".
Налаштування параметрів продуктивності	Налаштуйте параметри продуктивності, наприклад, візуальні ефекти та план електроживлення, щоб покращити загальну продуктивність системи.
Антивірус та безпека	Переконайтеся, що на вашому комп'ютері встановлений надійний антивірус та інші засоби безпеки для захисту від шкідливого ПЗ та вірусів.
Регулярне обслуговування	Виконуйте регулярне обслуговування, таке як дефрагментація диска, очищення тимчасових файлів та перевірка диска на наявність помилок.

З урахуванням цих рекомендацій, ваш комп'ютер зможе працювати стабільно та ефективно на Windows 10.

Важливість дотримання мінімальних вимог

Дотримання мінімальних системних вимог для Windows 10 має велике значення для стабільної та ефективної роботи системи та є критичним для забезпечення стабільної, безпечної та ефективної роботи операційної системи. Це не тільки допомагає уникнути технічних проблем, але й забезпечує зручність та продуктивність під час щоденного використання комп'ютера. Врахування та дотримання цих вимог є важливим кроком для отримання найкращого досвіду користування Windows 10.

Ключові причини, чому це важливо

Забезпечення стабільності роботи	Системні вимоги розроблені для забезпечення мінімальної стабільності роботи Windows 10. Невідповідність вимогам може призвести до частих зависань, збоїв та інших проблем.
Плавна робота додатків	Мінімальні вимоги гарантують, що операційна система може запускати базові програми та виконувати основні завдання без значних затримок. Це особливо важливо для офісних програм, браузерів та інших основних додатків.
Оновлення та безпека	Дотримання мінімальних вимог дозволяє системі отримувати та встановлювати останні оновлення безпеки та функцій, що забезпечує захист від шкідливого ПЗ та покращення продуктивності.
Сумісність обладнання	Відповідність вимогам забезпечує сумісність з більшістю сучасного обладнання та периферійних пристроїв, що дозволяє користувачам без проблем використовувати принтери, сканери, зовнішні накопичувачі та інші пристрої.
Запобігання втраті даних	Використання комп'ютера, що не відповідає мінімальним вимогам, може призвести до несподіваних збоїв і втрати даних. Відповідність вимогам допомагає уникнути цих ризиків і забезпечує безпеку даних.
Оптимальна продуктивність	Виконання вимог дозволяє системі працювати з оптимальною продуктивністю, забезпечуючи комфортне користування та швидке виконання завдань.

Контрольні питання

1. Які мінімальні вимоги до процесора для встановлення Windows 10?
2. Скільки оперативної пам'яті потрібно для 32-бітної версії Windows 10?
3. Що таке функція Continuum в Windows 10?
4. Яке мінімальне розширення екрану потрібне для встановлення Windows 10?
5. Який інструмент від Microsoft дозволяє перевірити сумісність комп'ютера з Windows 10?

Тема: Налаштування, оптимізація та захист ОС Windows

План

1. Встановлення ОС
2. Початкові налаштування та оптимізація
3. Користувачі та групи
4. Журнал подій
5. Служби
6. Розклад завдань
7. Керування дисками
8. Системні утиліти для дисків
9. Диспетчер завдань
10. Відомості про систему
11. Резервне копіювання та відновлення
12. Контрольні точки
13. Засіб діагностики DirectX
14. Діагностика RAM
15. Реєстр Windows
16. Брандмауер
17. Локальна політика безпеки
18. Групові політики безпеки
19. BitLocker
20. EFS

Процес встановлення ОС Windows 10 складається з кількох кроків:

1. **Підготовка:**
   - *Створіть резервні копії важливих даних, щоб запобігти їх втраті.*
   - *Переконайтеся, що ваш комп'ютер відповідає мінімальним системним вимогам для Windows 10.*
   - *Завантажте інсталяційний носій Windows 10 з офіційного веб-сайту Microsoft або використовуйте USB-накопичувач/DVD з інсталяційними файлами.*

2. **Запуск установника:**
   - *Вставте інсталяційний носій (USB-накопичувач або DVD) у ваш комп'ютер і перезавантажте його.*
   - *Під час завантаження увійдіть у меню BIOS/UEFI вашого комп'ютера (зазвичай потрібно натиснути клавішу F2, F12, Delete або Esc під час*

запуску) і налаштуйте порядок завантаження так, щоб ваш комп'ютер завантажувався з інсталяційного носія.

3. **Процес встановлення:**
   - *Після завантаження з інсталяційного носія з'явиться екран "Windows Setup". Виберіть мову, формат часу та розкладку клавіатури, а потім натисніть "Next".*
   - *Натисніть "Install now".*
   - *Введіть ліцензійний ключ продукту, якщо запитується, або виберіть "I don't have a product key", щоб активувати Windows пізніше.*
   - *Прийміть умови ліцензії та натисніть "Next".*
   - *Виберіть тип інсталяції: "Upgrade" (оновлення з попередньої версії Windows) або "Custom" (чиста установка). Зазвичай рекомендується вибирати "Custom" для чистої установки.*
   - *Виберіть розділ диска для встановлення Windows 10. Якщо потрібно, створіть нові розділи або видаліть існуючі, а потім натисніть "Next". Встановлення розпочнеться, і комп'ютер декілька разів перезавантажиться.*

4. **Початкові налаштування:**
   - *Після завершення встановлення з'явиться екран початкових налаштувань (Out-of-Box Experience, OOBE). Виберіть регіон, розкладку клавіатури та підключення до мережі.*
   - *Увійдіть до свого облікового запису Microsoft або створіть новий.*
   - *Налаштуйте параметри конфіденційності та налаштування облікового запису згідно з вашими уподобаннями.*
   - *Після завершення початкових налаштувань ви будете готові до використання Windows 10.*

Користувачі та групи у Windows 10 є важливими компонентами управління системою, які дозволяють адміністраторам і користувачам ефективно працювати з правами доступу та безпекою.

Користувачі

У Windows 10, користувачі — це окремі облікові записи, які надають доступ до системи. Кожен користувач має свій профіль, який містить особисті налаштування, файли, налаштування програм тощо.

Важливі аспекти роботи з користувачами включають:

1. **Створення облікових записів користувачів**. *Адміністратори можуть створювати облікові записи для нових користувачів, вибираючи локальні облікові записи або облікові записи Microsoft.*
2. **Рівні доступу**. *Користувачі можуть мати різні рівні доступу, зокрема стандартні користувачі та адміністратори. Адміністратори мають вищий рівень доступу і можуть здійснювати зміни в системі.*
3. **Налаштування паролів**. *Кожен користувач може мати свій пароль для захисту доступу до свого облікового запису.*
4. **Управління профілями**. *Кожен користувач має свій профіль, який містить дані про налаштування, файли та програмні налаштування.*

Групи

Групи у Windows 10 дозволяють об'єднувати користувачів для спрощення управління правами доступу та безпеки. Основні аспекти роботи з групами включають:

1. **Створення груп**. *Адміністратори можуть створювати групи для організації користувачів за функціями або відділами.*
2. **Призначення прав доступу**. *Групи можуть мати певні права доступу до ресурсів системи, таких як файли, папки, мережеві ресурси тощо. Це дозволяє спрощувати управління правами, оскільки адміністратору достатньо змінити права доступу для групи замість кожного окремого користувача.*
3. **Вбудовані групи**. *Windows 10 має декілька вбудованих груп, таких як Administrators, Users, Guests тощо, які мають встановлені права доступу.*

Переваги використання користувачів та груп:

1. **Підвищення безпеки**: *Згрупування користувачів дозволяє адміністратору легко керувати правами доступу та забезпечити захист конфіденційної інформації.*
2. **Спрощення управління**: *Використання груп дозволяє зменшити кількість ручної роботи та спрощує управління правами доступу.*
3. **Ефективне використання ресурсів**: *Групи дозволяють об'єднувати користувачів зі схожими потребами, що сприяє ефективнішому використанню ресурсів системи.*

Журнал подій у Windows 10 — це інструмент для моніторингу та реєстрації різних подій, що відбуваються в системі. Це важливий інструмент для системних адміністраторів та користувачів, які хочуть відслідковувати стан системи, діагностувати проблеми та забезпечувати безпеку.

Основні категорії журналів подій:

1. **Системні події (System).** *Включає події, що стосуються роботи операційної системи та драйверів, такі як помилки, попередження та інформаційні повідомлення.*
2. **Події програм (Application).** *Реєструє події, пов'язані з роботою встановлених програм та додатків.*
3. **Безпека (Security).** *Зберігає інформацію про події безпеки, такі як успішні та неуспішні спроби входу в систему, зміни у правах доступу та інші події, які впливають на безпеку системи.*
4. **Інші журнали подій.** *Містять події, пов'язані з іншими службами та компонентами системи, такими як журнали для встановлених додатків, робочих станцій, DNS-сервера тощо.*

Використання журналу подій:

1. **Відкриття переглядача подій:**
   - *Натисніть комбінацію клавіш **Win + X** і виберіть "Перегляд подій" (Event Viewer) з меню.*
   - *У вікні переглядача подій зліва відкрийте категорії "Windows Logs" (журнали Windows), де можна знайти системні журнали, журнали програм та безпеки.*
2. **Аналіз подій:**
   - *Кожен запис у журналі подій містить детальну інформацію про подію, включаючи час, джерело, код події та опис.*
   - *Системні адміністратори можуть фільтрувати, сортувати та шукати записи для виявлення проблем та аналізу збоїв.*
3. **Створення журналів та попереджень:**
   - *Ви можете налаштувати правила для автоматичного створення попереджень та повідомлень на основі певних типів подій або порогових значень.*

- *Це допомагає проактивно відслідковувати критичні події та реагувати на них у разі необхідності.*

Переваги журналу подій:

1. **Моніторинг стану системи.** *Дає можливість відслідковувати роботу системи та додатків у реальному часі.*
2. **Діагностика та усунення несправностей.** *Допомагає виявити причини збоїв та проблем у системі.*
3. **Забезпечення безпеки.** *Журнал безпеки дозволяє відслідковувати спроби несанкціонованого доступу та інші події, що впливають на безпеку.*

Журнал подій є ключовим інструментом для підтримки стабільності та безпеки системи Windows 10.

Служби (Services) у Windows 10 — це програми, які працюють у фоновому режимі і надають важливі функції для операційної системи та додатків. Вони можуть бути автоматично запущені під час завантаження системи або запущені вручну за потреби. Служби забезпечують широкий спектр функцій, таких як підключення до мережі, управління апаратним забезпеченням, забезпечення безпеки та інші критичні завдання.

Основні аспекти роботи зі службами у Windows 10:

1. Перегляд і управління службами:

- *Щоб відкрити інструмент управління службами, натисніть комбінацію клавіш **Win + R**, введіть "services.msc" і натисніть Enter.*
- *У вікні "Служби" відображаються всі доступні служби, їхній статус (запущено або зупинено), тип запуску (автоматичний, вручну або відключений) та інша інформація.*
- *Користувачі можуть запустити, зупинити, призупинити або перезапустити службу, натиснувши правою кнопкою миші на відповідну службу та вибравши потрібну дію.*

2. Типи запуску служб:

- **Автоматичний (Automatic).** Служба автоматично запускається під час завантаження системи.
- **Вручну (Manual).** Служба може бути запущена користувачем або додатком за потреби.
- **Відключено (Disabled).** Служба не може бути запущена, поки не буде змінено її тип запуску.

3. Важливі системні служби:

- **Windows Update:** Відповідає за завантаження та встановлення оновлень для операційної системи та програмного забезпечення.
- **Windows Defender:** Забезпечує захист від шкідливого програмного забезпечення та вірусів.
- **Print Spooler:** Управляє чергою друку та контролює друкарські завдання.
- **Event Log:** Реєструє події системи, які можуть бути використані для моніторингу та діагностики.
- **Networking Services:** Включає служби для підключення до мережі, такі як DHCP Client, DNS Client та інші.

4. Резервування ресурсів та безпека:

- *Деякі служби можуть споживати значні ресурси системи, тому важливо регулярно перевіряти їхню роботу та налаштовувати тип запуску для оптимальної продуктивності.*
- *Вимкнення критичних служб може призвести до нестабільної роботи системи або втрати функціональності, тому зміни повинні вносити лише досвідчені користувачі або системні адміністратори.*

Служби є важливою частиною операційної системи Windows 10, забезпечуючи її стабільну роботу та надаючи критично важливі функції для користувачів та додатків.

Розклад завдань (Task Scheduler) у Windows 10 — це інструмент, що дозволяє автоматизувати виконання різних завдань та процесів на комп'ютері. З його допомогою можна планувати запуск програм, скриптів або інших дій в певний час або у відповідь на певні події.

Основні функції розкладу завдань:

1. **Автоматизація завдань.** *Розклад завдань дозволяє налаштовувати автоматичний запуск програм та скриптів в певний час, що знижує потребу в ручному виконанні рутинних завдань.*
2. **Запуск у відповідь на події.** *Ви можете налаштувати завдання на запуск у відповідь на певні події, такі як вхід у систему, створення файлу, зміна стану системи тощо.*
3. **Повторення завдань.** *Завдання можна налаштувати на повторення з певною періодичністю, наприклад, щоденно, щотижня або щомісяця.*

Як створити завдання у Розкладі завдань:

1. **Відкриття Розкладу завдань:**
   - *Натисніть комбінацію клавіш Win + R, введіть "taskschd.msc" і натисніть Enter, щоб відкрити Розклад завдань.*
2. **Створення нового завдання:**
   - *У вікні Розкладу завдань виберіть "Створити базове завдання" (Create Basic Task) або "Створити завдання" (Create Task).*
   - *Введіть ім'я та опис завдання, потім натисніть "Next".*
3. **Налаштування тригера:**
   - *Виберіть умову, яка буде запускати завдання (наприклад, за розкладом, під час входу користувача, при події тощо).*
   - *Налаштуйте деталі тригера, такі як дата, час, частота повторення.*

4. **Вибір дії:**
    - *Виберіть дію, яку потрібно виконати (наприклад, запуск програми, відправка електронного листа, показ повідомлення).*
    - *Введіть шлях до програми або скрипту, якщо потрібно, та налаштуйте додаткові параметри.*

5. **Налаштування додаткових параметрів:**
    - *Можна налаштувати додаткові параметри, такі як умови запуску, додаткові тригери та дії.*

6. **Збереження та запуск завдання:**
    - *Після налаштування всіх параметрів натисніть "Finish", щоб зберегти та активувати завдання.*

Переваги використання Розкладу завдань:

1. **Ефективність.** *Автоматизація рутинних завдань дозволяє зекономити час та підвищити продуктивність.*
2. **Гнучкість.** *Розклад завдань дозволяє налаштовувати різноманітні сценарії запуску програм та дій.*
3. **Контроль.** *Адміністратори та користувачі можуть контролювати, коли і як виконуються завдання, забезпечуючи стабільну роботу системи.*

Розклад завдань є потужним інструментом для автоматизації та управління завданнями у Windows 10, що допомагає забезпечити стабільну та ефективну роботу системи.

Керування дисками (Disk Management) у Windows 10 — це вбудований інструмент, який дозволяє адміністраторам та користувачам створювати, налаштовувати та керувати розділами та дисками на їхньому комп'ютері.

Основні функції керування дисками:

1. **Створення та видалення розділів:**
   - *За допомогою інструменту "Керування дисками" можна створювати нові розділи на диску, видаляти існуючі розділи та змінювати їхній розмір.*
   - *Для цього, відкрийте "Керування дисками" (натисніть комбінацію клавіш Win + X та виберіть "Керування дисками"), потім натисніть правою кнопкою миші на диск і виберіть необхідну дію.*

2. **Форматування розділів:**
   - *Ви можете форматувати розділи з використанням різних файлових систем, таких як NTFS, FAT32 або exFAT.*
   - *Форматування видаляє всі дані на розділі, тому переконайтеся, що ви створили резервні копії важливих даних перед форматуванням.*

3. **Зміна розміру та об'єднання розділів:**
   - *Інструмент дозволяє змінювати розмір існуючих розділів, збільшувати або зменшувати їхній обсяг без втрати даних.*
   - *Ви також можете об'єднувати або розділяти розділи для оптимального використання дискового простору.*

4. **Створення логічних та первинних розділів:**
   - *Користувачі можуть створювати як первинні (primary), так і логічні (logical) розділи на дисках, що дозволяє розділити дисковий простір на декілька окремих частин для різних цілей.*

5. **Додавання та видалення томів:**
   - *Крім створення та форматування розділів, ви можете додавати або видаляти томи, що дозволяє ефективно організовувати дані на дисках.*

Переваги використання керування дисками:

1. **Оптимальне використання дискового простору.** *Керування дисками дозволяє ефективно розподілити дисковий простір, створюючи нові розділи або змінюючи розмір існуючих.*
2. **Гнучкість та контроль.** *Користувачі можуть легко налаштовувати розділи та томи відповідно до своїх потреб, забезпечуючи оптимальне використання ресурсів.*

3. **Зручність.** *Інструмент має простий та інтуїтивний інтерфейс, що дозволяє швидко виконувати необхідні дії з керування дисками.*

Керування дисками є потужним інструментом для налаштування та оптимізації використання дискового простору в Windows 10.

Системні утиліти для дисків у Windows 10 надають користувачам можливість ефективно керувати дисковим простором, діагностувати проблеми та підтримувати стабільну роботу жорстких дисків і твердотільних накопичувачів (SSD).

Основні системні утиліти для дисків:

1. **Дефрагментація та оптимізація дисків (Defragment and Optimize Drives):**
   - *Ця утиліта дозволяє дефрагментувати файлову систему на традиційних жорстких дисках (HDD), що може підвищити їхню продуктивність. Для SSD утиліта проводить оптимізацію, яка підтримує належну роботу накопичувачів.*
   - *Щоб відкрити утиліту, натисніть Win + S, введіть "Defragment and Optimize Drives" та оберіть відповідний результат.*

2. **Перевірка диска (Check Disk):**
   - *Утиліта "Check Disk" (chkdsk) перевіряє жорсткі диски на наявність помилок файлової системи та фізичних дефектів. Вона також може виправляти знайдені проблеми.*
   - *Щоб запустити перевірку диска, відкрийте командний рядок (Command Prompt) з правами адміністратора і введіть команду chkdsk C: /f (де "C:" — літера диска, який потрібно перевірити).*

3. **Диск для очищення (Disk Cleanup):**
   - *Утиліта "Disk Cleanup" дозволяє звільнити місце на диску, видаляючи тимчасові файли, кешовані файли, кошик та інші непотрібні дані.*
   - *Щоб запустити утиліту, натисніть Win + S, введіть "Disk Cleanup" і оберіть відповідний результат. Виберіть диск, який хочете очистити, та натисніть "OK".*

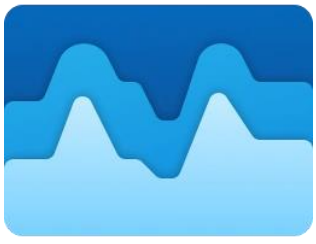
4. **Керування дисками (Disk Management):**
    - *Цей інструмент дозволяє створювати, видаляти, форматувати та змінювати розмір розділів на жорстких дисках та SSD.*
    - *Щоб відкрити утиліту, натисніть Win + X і виберіть "Керування дисками" (Disk Management).*

5. **Стан накопичувача (Storage Spaces):**
    - *Ця утиліта дозволяє створювати віртуальні накопичувачі з об'єднанням кількох фізичних дисків для підвищення надійності та продуктивності.*
    - *Щоб налаштувати Storage Spaces, натисніть Win + S, введіть "Storage Spaces" та оберіть відповідний результат.*

Переваги використання системних утиліт для дисків:

1. **Підтримка продуктивності.** *Дефрагментація та очищення дисків допомагають підтримувати високу швидкість роботи системи.*
2. **Діагностика та виправлення проблем.** *Перевірка диска дозволяє виявляти та виправляти проблеми, що можуть призвести до втрати даних або нестабільної роботи системи.*
3. **Ефективне використання дискового простору.** *Утиліти для керування дисками допомагають оптимально розподілити дисковий простір та забезпечити ефективну роботу накопичувачів.*

Системні утиліти для дисків у Windows 10 надають користувачам потужні інструменти для підтримки стабільної та ефективної роботи їхніх комп'ютерів.



Диспетчер завдань (Task Manager) у Windows 10 — це потужний інструмент, який дозволяє користувачам переглядати і керувати виконуваними процесами, програмами, службами та ресурсами системи. Він допомагає діагностувати проблеми продуктивності, закривати не відповідаючі програми та контролювати використання ресурсів.

Відкриття Диспетчера завдань:

- ✓ *Натисніть комбінацію клавіш **Ctrl + Shift + Esc**.*
- ✓ *Натисніть **Ctrl + Alt + Delete** та виберіть "Диспетчер завдань".*
- ✓ *Натисніть правою кнопкою миші на панелі завдань і виберіть "Диспетчер завдань" з контекстного меню.*

Основні вкладки Диспетчера завдань:

1. Процеси (Processes):

- *Відображає всі активні процеси, додатки та фонові служби.*
- *Користувачі можуть переглядати інформацію про використання процесора (CPU), оперативної пам'яті (RAM), диска та мережі кожним процесом.*
- *Можливість завершення процесів, які не відповідають або споживають багато ресурсів.*

2. Продуктивність (Performance):

- *Відображає графічні показники продуктивності системи, такі як використання процесора, пам'яті, диска, мережі та графічного процесора (GPU).*
- *Інформація про основні характеристики апаратного забезпечення, такі як модель процесора, кількість ядер та поточна швидкість роботи.*

3. Історія програм (App history):

- *Показує історію використання ресурсів додатками з Універсальної платформи Windows (UWP).*
- *Інформація про споживання процесора та мережі кожним додатком за певний період.*

4. Запуск (Startup):

- *Відображає список програм, які запускаються автоматично під час завантаження системи.*
- *Можливість вимкнення або ввімкнення програм для покращення часу завантаження системи.*

5. Користувачі (Users):

- *Показує інформацію про активних користувачів системи та їхні процеси.*

- *Можливість завершення процесів користувачів або відключення користувачів для звільнення ресурсів.*

6. **Подробиці (Details):**
   - *Відображає детальну інформацію про всі активні процеси, включаючи ідентифікатор процесу (PID), статус, використання ресурсів тощо.*
   - *Можливість налаштування пріоритетів процесів та завершення процесів.*

7. **Служби (Services):**
   - *Показує список всіх служб у системі та їхній статус.*
   - *Можливість запуску, зупинки, призупинення або перезапуску служб.*

Переваги використання Диспетчера завдань:

1. **Моніторинг продуктивності.** *Диспетчер завдань надає актуальну інформацію про використання ресурсів системи, що допомагає виявляти проблеми з продуктивністю.*
2. **Контроль над процесами.** *Користувачі можуть завершувати не відповідаючі програми та фонові процеси, що покращує стабільність роботи системи.*
3. **Оптимізація запуску.** *Можливість керувати програмами автозапуску для швидшого завантаження системи.*

Диспетчер завдань є важливим інструментом для підтримки стабільної роботи та продуктивності системи Windows 10.

Відомості про систему (System Information) у Windows 10 — це інструмент, який надає детальну інформацію про апаратне та програмне забезпечення вашого комп'ютера. Він корисний для діагностики проблем, управління конфігурацією системи та отримання докладних технічних характеристик.

Відкриття Відомостей про систему:

- ✓ *Натисніть **Win + R**, введіть "msinfo32" та натисніть Enter.*
- ✓ *Вікно "Відомості про систему" відкриється, відображаючи загальний огляд вашої системи.*

Основні розділи Відомостей про систему:

1. **Системний підсумок (System Summary):**
    - *Відображає загальну інформацію про систему, включаючи версію операційної системи, модель комп'ютера, тип процесора, кількість оперативної пам'яті, версію BIOS та інші основні характеристики.*
    - *Це корисний розділ для швидкого перегляду основних параметрів системи.*

2. **Апаратні ресурси (Hardware Resources):**
    - *Включає підрозділи для перегляду конфліктів ресурсів, стану вхідних/вихідних портів, використання пам'яті, переривань (IRQ) та інших апаратних ресурсів.*
    - *Корисно для діагностики апаратних проблем та конфліктів ресурсів.*

3. **Компоненти (Components):**
    - *Містить інформацію про різні компоненти системи, такі як диски, дисплей, мережеві адаптери, порти, принтери, звукові пристрої та інші периферійні пристрої.*
    - *Корисно для перегляду докладної інформації про кожен компонент та його стан.*

4. **Програмне середовище (Software Environment):**
    - *Включає підрозділи для перегляду драйверів, запущених завдань, налаштувань системи, змінних середовища та інших аспектів програмного забезпечення.*
    - *Допомагає визначити встановлене програмне забезпечення та активні процеси в системі.*

Переваги використання Відомостей про систему:

1. **Діагностика та усунення несправностей.** *Надає детальну інформацію про систему, яка допомагає виявляти та вирішувати проблеми.*

2. **Управління конфігурацією.** *Допомагає відстежувати встановлене апаратне та програмне забезпечення, що дозволяє оптимізувати конфігурацію системи.*
3. **Докладні технічні характеристики.** *Надає точну інформацію про всі компоненти системи, що може бути корисно під час оновлення або заміни апаратного забезпечення.*

Відомості про систему є важливим інструментом для отримання повної картини про стан вашого комп'ютера та його конфігурацію у Windows 10.

Резервне копіювання та відновлення у Windows 10 є важливими процесами для захисту даних та забезпечення відновлення системи у разі збоїв або втрати даних.

Резервне копіювання та відновлення даних у Windows 10 є ключовими процесами для забезпечення безпеки та стабільності вашої системи. Використання цих інструментів допоможе зберегти важливі дані та швидко відновити роботу системи у разі збоїв.

Резервне копіювання даних

1. **Інструмент "Історія файлів" (File History):**
   - *"Історія файлів" дозволяє автоматично створювати резервні копії ваших файлів, таких як документи, фотографії, відео та інші важливі дані.*
   - *Щоб налаштувати "Історію файлів", відкрийте "Параметри" (Settings), перейдіть до розділу "Оновлення та безпека" (Update & Security), оберіть "Резервне копіювання" (Backup) та активуйте "Історію файлів". Виберіть диск для зберігання резервних копій та налаштуйте параметри.*

2. **Резервне копіювання системного образу:**
   - *Системний образ — це повна копія вашої операційної системи, включаючи всі встановлені програми та налаштування. Він дозволяє відновити систему до певного стану у разі серйозних збоїв.*

- *Щоб створити системний образ, відкрийте "Панель управління" (Control Panel), перейдіть до розділу "Система та безпека" (System and Security) та виберіть "Резервне копіювання та відновлення (Windows 7)" (Backup and Restore (Windows 7)). Оберіть "Створити образ системи" (Create a system image) та слідуйте інструкціям.*

3. **Резервне копіювання з використанням сторонніх програм:**
   - *Крім вбудованих інструментів Windows, існують сторонні програми для резервного копіювання, такі як Acronis True Image, Macrium Reflect, EaseUS Todo Backup та інші. Ці програми можуть надавати додаткові функції та можливості для резервного копіювання.*

Відновлення даних та системи

2. **Відновлення файлів з "Історії файлів":**
   - *Якщо ви втратили або пошкодили файли, ви можете відновити їх з резервних копій, створених за допомогою "Історії файлів". Для цього відкрийте "Параметри" (Settings), перейдіть до розділу "Оновлення та безпека" (Update & Security), оберіть "Резервне копіювання" (Backup) та натисніть "Відновити файли з поточної резервної копії" (Restore files from a current backup).*

3. **Відновлення системного образу:**
   - *Для відновлення системи з системного образу відкрийте "Параметри" (Settings), перейдіть до розділу "Оновлення та безпека" (Update & Security), оберіть "Відновлення" (Recovery) та натисніть "Перезавантажити зараз" (Restart now) під розділом "Особливі завантаження" (Advanced startup). Після перезавантаження оберіть "Усунення несправностей" (Troubleshoot), потім "Додаткові параметри" (Advanced options) та "Відновлення системного образу" (System Image Recovery).*

4. **Відновлення з точки відновлення (System Restore):**
   - *Точки відновлення дозволяють відновити систему до попереднього стану без втрати особистих файлів. Це корисно, якщо система працює нестабільно після встановлення програм або оновлень.*
   - *Щоб створити або відновити з точки відновлення, відкрийте "Панель управління" (Control Panel), перейдіть до розділу "Система та безпека" (System and Security) та виберіть "Система" (System). Оберіть "Захист системи" (System Protection) з лівого меню та натисніть "Відновлення системи" (System Restore).*

Контрольні точки (System Restore Points) у Windows 10 — це функція, яка дозволяє створювати знімки стану системи в певний момент часу. Ці знімки можуть бути використані для відновлення системи до попереднього стану у разі виникнення проблем, таких як збої програмного забезпечення, помилки налаштувань або інші проблеми, що впливають на стабільність роботи системи.

Основні аспекти роботи з контрольними точками:

1. **Створення контрольних точок:**
   - *Контрольні точки можуть бути створені автоматично (наприклад, перед встановленням нових програм або оновлень) або вручну користувачем.*
   - *Щоб створити контрольну точку вручну, відкрийте "Панель управління" (Control Panel), перейдіть до розділу "Система та безпека" (System and Security), оберіть "Система" (System) і з лівого меню натисніть "Захист системи" (System Protection). У вікні, що відкрилось, натисніть "Створити" (Create), введіть опис контрольної точки і натисніть "Створити".*

2. **Використання контрольних точок для відновлення системи:**
   - *Якщо ваша система працює нестабільно або виникли інші проблеми, ви можете відновити її до попереднього стану за допомогою контрольної точки.*
   - *Щоб виконати відновлення системи, відкрийте "Панель управління" (Control Panel), перейдіть до розділу "Система та безпека" (System and Security), оберіть "Система" (System) і з лівого меню натисніть "Захист системи" (System Protection). Натисніть "Відновлення системи" (System Restore) і дотримуйтесь інструкцій майстра для вибору потрібної контрольної точки та виконання відновлення.*

3. **Налаштування захисту системи:**
   - *Ви можете налаштувати параметри захисту системи для кожного диска окремо, включаючи максимальний розмір місця на диску, виділений для зберігання контрольних точок.*
   - *Щоб налаштувати захист системи, відкрийте "Панель управління" (Control Panel), перейдіть до розділу "Система та безпека" (System and Security), оберіть "Система" (System) і з лівого меню натисніть*

"Захист системи" (System Protection). У вікні, що відкрилось, виберіть диск і натисніть "Налаштувати" (Configure), щоб налаштувати параметри захисту.

Переваги використання контрольних точок:

1. **Безпечне відновлення системи.** *Контрольні точки дозволяють відновити систему до попереднього стабільного стану без втрати особистих файлів.*
2. **Простота використання.** *Процес створення та відновлення контрольних точок є інтуїтивно зрозумілим і не потребує глибоких технічних знань.*
3. **Захист від збоїв.** *Контрольні точки забезпечують додатковий рівень захисту у випадку збоїв програмного забезпечення, конфліктів драйверів або інших проблем, що можуть вплинути на стабільність системи.*

Контрольні точки у Windows 10 є важливим інструментом для підтримки стабільної роботи системи та забезпечення безпеки ваших даних.

Засіб діагностики DirectX (DirectX Diagnostic Tool, DxDiag) — це утиліта, яка дозволяє перевірити стан вашого обладнання та драйверів, пов'язаних із DirectX. Це дуже корисно для виявлення і усунення проблем, пов'язаних із графікою та звуком.

Як використовувати засіб діагностики DirectX:

1. **Запуск утиліти:**
   - *Натисніть клавішу **Win + R**, щоб відкрити діалогове вікно "Виконати" (Run).*
   - *Введіть команду **dxdiag** і натисніть Enter.*

Перегляд інформації:

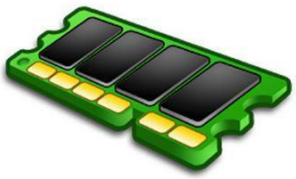
- *У вікні DxDiag ви зможете переглянути інформацію про вашу систему, включаючи версію DirectX, драйвери відеокарт, звукові пристрої та інше.*

- *На вкладці "Система" (System) ви зможете перевірити версію DirectX та інші важливі деталі.*

2. **Збереження інформації:**
   - *Якщо вам потрібно надіслати інформацію службі підтримки, ви можете натиснути кнопку "Зберегти всю інформацію" (Save all information), щоб зберегти деталі у файл.*

Переваги використання DxDiag:

- **Виявлення проблем.** *Допомагає швидко виявити проблеми з драйверами або обладнанням.*
- **Перевірка версій.** *Дозволяє перевірити, чи інстальовані останні версії DirectX та драйверів.*
- **Підтримка під час вирішення проблем.** *Інформація, зібрана DxDiag, може бути корисною для служб підтримки або форумів.*



Діагностика оперативної пам'яті (RAM) у Windows 10 — це процес перевірки стану вашої оперативної пам'яті на наявність помилок або проблем. Це важливо для підтримки стабільної роботи системи та виявлення можливих проблем, які можуть впливати на продуктивність комп'ютера.

Як використовувати діагностику RAM у Windows 10:

1. **Запуск діагностики:**
   - *Натисніть клавішу Win + R, щоб відкрити діалогове вікно "Виконати" (Run).*
   - *Введіть команду mdsched.exe і натисніть Enter.*
   - *Виберіть один з варіантів: "Виконати тест під час наступного запуску" або "Виконати тест зараз і перезавантажитися".*

2. **Проведення тесту:**
   - *Комп'ютер перезавантажиться і запустить діагностику RAM.*

- *Тест може зайняти декілька хвилин, залежно від обсягу оперативної пам'яті.*

3. **Перегляд результатів:**
   - *Після завершення тесту комп'ютер автоматично перезавантажиться.*
   - *Якщо проблеми були виявлені, вони будуть відображені на екрані після перезавантаження.*
   - *Якщо немає проблем, буде відображено повідомлення про успішне завершення тесту.*

Переваги використання діагностики RAM:

- **Виявлення помилок.** *Допомагає швидко виявити проблеми з оперативною пам'яттю.*
- **Профілактика.** *Регулярне тестування допомагає уникнути серйозних проблем*.
- **Підтримка продуктивності.** *Забезпечує стабільну роботу системи.*

Реєстр Windows (Windows Registry) — це централізована база даних, яка зберігає налаштування та параметри операційної системи, програмного забезпечення, апаратного забезпечення і користувачів. Він є критично важливою частиною операційної системи Windows і впливає на її роботу та функціональність.

Основні аспекти Реєстру Windows:

1. **Структура реєстру:**

Вулик (Hive). Реєстр складається з різних частин, відомих як вулики (hives), які містять ключі та значення. Основні вулики включають:

- ***HKEY_LOCAL_MACHINE*** *(HKLM): Зберігає* конфігурацію *апаратного забезпечення та налаштування програмного забезпечення для всіх користувачів.*

- ***HKEY_CURRENT_USER*** *(HKCU): Містить налаштування поточного користувача.*
- ***HKEY_CLASSES_ROOT*** *(HKCR): Зберігає інформацію про типи файлів та їх асоціації.*
- ***HKEY_USERS*** *(HKU): Містить налаштування всіх користувачів.*
- ***HKEY_CURRENT_CONFIG*** *(HKCC): Зберігає поточну конфігурацію апаратного забезпечення.*

2. **Ключі та значення:**
   - ***Ключі.*** *Реєстр організований у вигляді ієрархії папок, які називаються ключами (keys). Ключі можуть містити підключі (subkeys) та значення (values).*
   - ***Значення.*** *Значення — це конкретні параметри, що зберігаються у ключах. Існують різні типи значень, включаючи строки (string), двійкові дані (binary) та числові дані (DWORD).*

3. **Редагування реєстру:**
   - *Редагування реєстру може бути виконане за допомогою вбудованого інструменту "Редактор реєстру" (Registry Editor). Щоб відкрити його, натисніть* ***Win + R****, введіть "regedit" і натисніть Enter.*
   - *Важливо бути обережним при редагуванні реєстру, оскільки неправильні зміни можуть призвести до нестабільної роботи системи або її виходу з ладу.*

4. **Резервне копіювання та відновлення реєстру:**
   - *Перед внесенням змін до реєстру рекомендується створити резервну копію для відновлення у випадку проблем. Ви можете експортувати гілку реєстру або створити точку відновлення системи.*
   - *Щоб створити резервну копію реєстру, відкрийте "Редактор реєстру", виберіть гілку, яку хочете зберегти, натисніть "Файл" -> "Експортувати" (File -> Export) і збережіть файл.*

Переваги та важливість реєстру:

1. **Централізоване управління.** *Реєстр забезпечує централізоване місце для зберігання налаштувань, що полегшує управління системою та програмним забезпеченням.*

2. **Конфігурація програмного забезпечення.** *Реєстр зберігає налаштування додатків, дозволяючи їм працювати коректно та відповідно до вимог користувача.*
3. **Підтримка стабільності.** *Правильне налаштування реєстру допомагає забезпечити стабільну роботу операційної системи та програмного забезпечення.*

Реєстр Windows є важливою частиною операційної системи, і його правильне налаштування та управління можуть суттєво вплинути на продуктивність та стабільність вашого комп'ютера.

Брандмауер Windows (Windows Defender Firewall) — це вбудований інструмент безпеки, який забезпечує захист вашого комп'ютера від несанкціонованого доступу та шкідливих програм, контролюючи вхідний та вихідний мережевий трафік. Він грає важливу роль у захисті системи від мережевих загроз.

Основні функції Брандмауера Windows:

1. **Контроль мережевого трафіку:**
   - *Брандмауер фільтрує вхідний та вихідний трафік на основі правил, що визначають, який трафік дозволяється чи блокується. Це забезпечує захист від несанкціонованого доступу та атак.*

2. **Налаштування профілів:**
   - *Брандмауер підтримує три профілі: приватний, громадський та доменний. Кожен профіль має свої налаштування безпеки, що дозволяє гнучко налаштовувати захист залежно від мережі, до якої підключений комп'ютер.*

3. **Створення та редагування правил:**
   - *Користувачі та адміністратори можуть створювати власні правила для контролю мережевого трафіку. Це включає дозволення або блокування програм, портів або IP-адрес. Ви можете налаштувати як вхідні, так і вихідні правила.*

4. **Моніторинг та ведення журналу:**
    - *Брандмауер може вести журнал подій для моніторингу мережевої активності. Це допомагає виявляти підозрілий трафік та аналізувати мережеві події.*

Використання Брандмауера Windows:

1. **Відкриття Брандмауера:**
    - *Відкрийте "Панель управління" (Control Panel), перейдіть до розділу "Система та безпека" (System and Security) та виберіть "Брандмауер Windows Defender" (Windows Defender Firewall).*

2. **Управління правилами:**
    - *Щоб створити або редагувати правила, натисніть "Додаткові параметри" (Advanced settings) в лівій частині вікна. У вікні, що відкрилось, ви зможете створювати нові правила для вхідного та вихідного трафіку, а також редагувати існуючі правила.*

3. **Налаштування профілів:**
    - *Відкрийте "Параметри" (Settings), перейдіть до розділу "Оновлення та безпека" (Update & Security), оберіть "Безпека Windows" (Windows Security) та натисніть "Брандмауер та мережевий захист" (Firewall & network protection). Тут ви зможете налаштувати різні профілі брандмауера для приватної, громадської та доменної мереж.*

Переваги використання Брандмауера Windows:

1. **Захист від загроз.** *Брандмауер забезпечує базовий захист від мережевих атак та шкідливих програм, що намагаються отримати доступ до вашої системи.*
2. **Гнучкі налаштування.** *Ви можете налаштувати правила та профілі відповідно до своїх потреб, забезпечуючи оптимальний рівень захисту.*
3. **Інтеграція з системою.** *Брандмауер Windows є частиною операційної системи, що забезпечує його високу сумісність та стабільність роботи.*

Брандмауер Windows 10 є важливим компонентом безпеки, який допомагає захистити ваш комп'ютер від мережевих загроз.

Разом із брандмауером Windows варто використовувати різні засоби захисту, щоб забезпечити багаторівневу безпеку системи. Ось деякі з них:

1. **Антивірусне програмне забезпечення:**
    - *Антивірусна програма допомагає виявляти та видаляти шкідливі програми, такі як віруси, трояни, шпигунські програми та інші види шкідливих програм.*
    - *Популярні антивірусні програми включають Microsoft Defender, ESET Internet Security, Bitdefender та інші.*

2. **Антишпигунське програмне забезпечення:**
    - *Антишпигунське програмне забезпечення спеціалізується на виявленні та видаленні шпигунських програм, які можуть збирати конфіденційну інформацію з вашого комп'ютера.*
    - *Деякі антивірусні програми мають вбудовані функції антишпигунського захисту, але окремі програми, такі як Malwarebytes, можуть надати додатковий рівень безпеки.*

3. **Фільтрація веб-контенту:**
    - *Засоби фільтрації веб-контенту допомагають блокувати доступ до небезпечних або шкідливих веб-сайтів. Вони можуть запобігти завантаженню шкідливих програм та фішингових атак.*
    - *Деякі антивірусні програми включають функції фільтрації веб-контенту, а також можна використовувати розширення для браузерів, такі як uBlock Origin або AdGuard.*

4. **Оновлення програмного забезпечення:**
    - *Регулярне оновлення операційної системи та програмного забезпечення забезпечує захист від відомих вразливостей. Microsoft регулярно випускає оновлення безпеки для Windows, які варто встановлювати своєчасно.*
    - *Встановлюйте оновлення для всіх програм, включаючи браузери, антивірусні програми та інші додатки.*

5. **Шифрування даних:**
    - *Шифрування даних захищає вашу інформацію від несанкціонованого доступу. Windows 10 має вбудовану функцію BitLocker для шифрування дисків.*
    - *Використовуйте шифрування для захисту конфіденційних файлів і даних.*

6. **Двофакторна аутентифікація (2FA):**
    - *Двофакторна аутентифікація додає додатковий рівень захисту до ваших облікових записів, вимагаючи введення додаткового коду, що надсилається на ваш телефон або інший пристрій.*
    - *Налаштуйте 2FA для своїх облікових записів у соціальних мережах, електронної пошти, онлайн-банкінгу та інших сервісів.*

7. **Навчання безпеці:**
    - *Вивчення основних принципів кібербезпеки допомагає уникати поширених загроз, таких як фішинг, шкідливі посилання та соціальна інженерія.*
    - *Регулярно оновлюйте свої знання про нові загрози та методи захисту.*

Використання комбінації цих засобів захисту допоможе забезпечити багаторівневу безпеку системи та захистити від різноманітних кіберзагроз.

Локальна політика безпеки (Local Security Policy) у Windows 10 — це набір параметрів та правил, що визначають безпеку системи на локальному рівні. Ці політики можуть бути налаштовані адміністратором для забезпечення захисту від несанкціонованого доступу, контролю дій користувачів і захисту конфіденційної інформації.

Основні аспекти Локальної політики безпеки:

1. **Налаштування облікових записів:**
    - *Локальна політика безпеки дозволяє налаштувати правила управління обліковими записами, такі як вимоги до паролів (довжина, складність, термін дії), обмеження на кількість спроб входу в систему та інші параметри.*
    - *Наприклад, можна налаштувати політику, що вимагає від користувачів змінювати паролі кожні 90 днів та використовувати складні паролі.*

2. **Аудит подій:**

- *Адміністратори можуть налаштувати аудит подій для відстеження дій користувачів та системних подій, таких як входи в систему, зміни у правах доступу, встановлення програмного забезпечення та інші дії.*
- *Аудит подій допомагає виявляти підозрілу активність та забезпечувати відповідність політикам безпеки.*

3. **Політики безпеки локального комп'ютера:**
   - *Ці політики визначають налаштування безпеки, які застосовуються до локального комп'ютера, включаючи правила брандмауера, налаштування шифрування даних, обмеження на використання USB-пристроїв та інші параметри.*
   - *Наприклад, можна налаштувати брандмауер для блокування певних портів або заборонити підключення незнайомих USB-пристроїв для захисту від вірусів.*

4. **Управління груповими політиками:**
   - *Локальна політика безпеки дозволяє налаштовувати групові політики, які можуть застосовуватися до певних груп користувачів або комп'ютерів. Це забезпечує централізоване управління політиками безпеки у великій організації.*
   - *Наприклад, можна налаштувати політику, що забороняє користувачам встановлювати програми без дозволу адміністратора.*

Використання Локальної політики безпеки:

1. **Відкриття інструменту Локальна політика безпеки:**
   - *Натисніть комбінацію клавіш Win + R, введіть "secpol.msc" і натисніть Enter. Відкриється вікно "Локальна політика безпеки" (Local Security Policy).*

2. **Налаштування політик:**
   - *У вікні "Локальна політика безпеки" ви зможете налаштувати різні політики безпеки, такі як політики облікових записів, локальні політики, політики аудиту та інші параметри.*
   - *Виберіть потрібну політику з меню зліва, двічі натисніть на неї та налаштуйте відповідні параметри.*

Переваги використання Локальної політики безпеки:

1. **Захист від загроз.** *Локальна політика безпеки допомагає захистити вашу систему від несанкціонованого доступу, вірусів та інших загроз.*
2. **Контроль дій користувачів.** *Адміністратори можуть налаштовувати політики для обмеження дій користувачів та забезпечення відповідності політикам безпеки.*
3. **Централізоване управління.** *Використання локальної політики безпеки дозволяє централізовано управляти налаштуваннями безпеки на всіх комп'ютерах у мережі.*

Локальна політика безпеки є важливим інструментом для забезпечення безпеки та стабільності роботи операційної системи Windows 10.

Групові політики безпеки (Group Policy) у Windows — це потужний інструмент, який дозволяє адміністраторам централізовано керувати налаштуваннями безпеки та іншими параметрами на комп'ютерах у доменній мережі. Вони використовуються для забезпечення відповідності політикам безпеки, управління доступом та автоматизації адміністрування.

Основні аспекти Групових політик безпеки:

1. **Структура групових політик:**
   - *Групові політики поділяються на два основних типи: політики комп'ютера та політики користувача.*
   - *Політики комп'ютера застосовуються до всіх комп'ютерів у домені, незалежно від того, який користувач увійшов у систему.*
   - *Політики користувача застосовуються до облікових записів користувачів, незалежно від того, на якому комп'ютері вони увійшли в систему.*

2. **Області налаштувань групових політик:**
   - *Групові політики охоплюють широкий спектр налаштувань, включаючи налаштування безпеки, програмне забезпечення,*

мережеві параметри, облікові записи користувачів, робочий стіл та інші параметри.

- *Політики можуть налаштовувати, наприклад, вимоги до паролів, налаштування брандмауера, обмеження доступу до певних програм та ресурсів, автоматичне встановлення оновлень та багато іншого.*

3. **Групові політики об'єктів (GPO):**
   - *Групові політики застосовуються через Групові політики об'єктів (Group Policy Objects, GPO), які можуть бути створені, змінені та застосовані до організаційних одиниць (OU) у Active Directory.*
   - *Адміністратори можуть створювати нові GPO та призначати їх до певних OU, комп'ютерів або користувачів.*

4. **Інструменти для управління груповими політиками:**
   - ***Group Policy Management Console (GPMC).*** *Інструмент, який дозволяє адміністраторам створювати, редагувати та керувати GPO. Відкривається з Панелі управління або за допомогою команди* ***gpmc.msc****.*
   - ***Local Group Policy Editor (gpedit.msc).*** *Інструмент для налаштування локальних групових політик на окремих комп'ютерах. Відкривається за допомогою команди* ***gpedit.msc****.*

Переваги використання групових політик безпеки:

1. **Централізоване управління.** *Групові політики дозволяють адміністраторам централізовано керувати налаштуваннями безпеки та іншими параметрами на всіх комп'ютерах у домені.*
2. **Автоматизація.** *Адміністратори можуть автоматизувати налаштування та оновлення політик, що знижує ручну роботу та зменшує можливість помилок.*
3. **Безпека.** *Групові політики забезпечують високий рівень безпеки, контролюючи доступ до ресурсів та забезпечуючи відповідність політикам безпеки.*
4. **Гнучкість.** *Групові політики можуть бути налаштовані на різних рівнях, включаючи окремих користувачів, комп'ютери або організаційні одиниці.*

Приклади налаштувань групових політик:

1. **Вимоги до паролів.** *Встановлення складних паролів, тривалості дії паролів та вимог до зміни паролів.*

2. **Обмеження доступу.** *Заборона доступу до певних програм або мережевих ресурсів для певних користувачів або груп.*
3. **Налаштування брандмауера.** *Створення правил брандмауера для захисту від зовнішніх загроз.*
4. **Автоматичне оновлення.** *Налаштування автоматичного встановлення оновлень для операційної системи та програмного забезпечення.*

Групові політики безпеки є ключовим інструментом для забезпечення безпеки та стабільності систем у великих мережах.

BitLocker — це функція шифрування дисків, вбудована в операційну систему Windows 10 (і інші версії Windows), яка допомагає захистити дані на вашому комп'ютері від несанкціонованого доступу. BitLocker використовує алгоритми шифрування для захисту вмісту жорстких дисків або знімних накопичувачів, що забезпечує високий рівень безпеки.

Основні функції BitLocker:

1. **Шифрування диска:**
   - *BitLocker може шифрувати як системний диск (де встановлена операційна система), так і додаткові диски або знімні накопичувачі, такі як USB-флешки.*
   - *Шифрування запобігає несанкціонованому доступу до даних, навіть якщо диск вийнятий з комп'ютера і підключений до іншого пристрою.*

2. **Захист за допомогою TPM:**
   - *BitLocker використовує модуль захисту TPM (Trusted Platform Module), який забезпечує збереження ключів шифрування на апаратному рівні, що підвищує безпеку.*
   - *Якщо ваш комп'ютер не має TPM, можна налаштувати BitLocker для використання ключів на флеш-накопичувачі або паролів.*

3. **Опції відновлення:**
   - *BitLocker пропонує кілька варіантів відновлення, включаючи збереження ключа відновлення (recovery key) в обліковому записі*

Microsoft, друк ключа або збереження його на знімному носії. Це дозволяє відновити доступ до зашифрованого диска у разі проблем із завантаженням або втрати доступу.

4. **Динамічне шифрування:**
    - *BitLocker підтримує динамічне шифрування, що дозволяє використовувати шифрування "на льоту" — шифрувати лише зайнятий простір диска, що зменшує час і ресурси, необхідні для завершення процесу шифрування.*

Як увімкнути BitLocker:

1. *Відкрийте "Панель управління" (Control Panel).*
2. *Перейдіть до розділу "Система та безпека" (System and Security).*
3. *Оберіть "Шифрування диска BitLocker" (BitLocker Drive Encryption).*
4. *Натисніть "Увімкнути BitLocker" (Turn on BitLocker) для відповідного диска.*
5. *Слідуйте інструкціям майстра налаштування BitLocker для вибору методу шифрування та способу зберігання ключа відновлення.*

Переваги використання BitLocker:

1. **Високий рівень безпеки.** *BitLocker забезпечує надійне шифрування даних, що захищає ваші файли від несанкціонованого доступу навіть у разі втрати або крадіжки комп'ютера.*
2. **Інтеграція з Windows.** *BitLocker є частиною операційної системи Windows і забезпечує високу сумісність та зручність використання.*
3. **Гнучкі налаштування.** *BitLocker пропонує різні варіанти шифрування та відновлення, що дозволяє налаштувати захист відповідно до ваших потреб.*

BitLocker є важливим інструментом для забезпечення безпеки ваших даних і допомагає захистити конфіденційну інформацію від несанкціонованого доступу.

EFS (Encrypting File System) — це технологія шифрування файлів, вбудована в операційну систему Windows, яка дозволяє користувачам шифрувати файли та папки для захисту від несанкціонованого доступу. EFS використовує шифрування на рівні файлової системи, що забезпечує захист даних навіть у разі їхнього копіювання на інший комп'ютер або зовнішній носій.

Основні аспекти EFS:

1. **Шифрування файлів і папок:**
   - *EFS дозволяє шифрувати окремі файли або цілі папки. Користувачі можуть вибрати файли або папки для шифрування через властивості файлів/папок.*
   - *Шифровані файли залишаються доступними для користувача, який їх зашифрував, але вони недоступні для інших користувачів без відповідних ключів шифрування.*

2. **Інтеграція з файловою системою NTFS:**
   - *EFS працює з файловою системою NTFS і використовує асиметричні ключі шифрування для захисту даних. Це забезпечує високий рівень безпеки і захист від несанкціонованого доступу.*

3. **Управління сертифікатами і ключами:**
   - *Для шифрування файлів EFS використовує сертифікати і ключі, які автоматично генеруються для кожного користувача. Сертифікати можуть бути збережені на комп'ютері або у зовнішньому сховищі.*
   - *Користувачі можуть експортувати сертифікати та ключі для створення резервних копій або перенесення їх на інший комп'ютер.*

4. **Відновлення доступу:**
   - *EFS підтримує механізми відновлення доступу, які дозволяють адміністраторам створювати агентів відновлення даних (Data Recovery Agents, DRA). Ці агенти мають можливість розшифровувати файли у разі втрати ключа користувачем.*

Як використовувати EFS:

1. **Шифрування файлів і папок:**
    - *Відкрийте Провідник файлів (File Explorer) і знайдіть файл або папку, яку хочете зашифрувати.*
    - *Натисніть правою кнопкою миші на файл або папку і виберіть "Властивості" (Properties).*
    - *Перейдіть до вкладки "Загальні" (General) і натисніть кнопку "Додатково" (Advanced).*
    - *У вікні "Додаткові атрибути" (Advanced Attributes) відзначте опцію "Шифрувати вміст для захисту даних" (Encrypt contents to secure data) і натисніть "OK".*

2. **Експорт сертифікатів і ключів:**
    - *Відкрийте "Панель управління" (Control Panel) і перейдіть до розділу "Центр сертифікатів" (Certificate Manager).*
    - *Знайдіть сертифікат, який використовується для шифрування, і експортуйте його для створення резервної копії.*

Переваги використання EFS:

1. **Високий рівень безпеки.** *EFS забезпечує надійне шифрування файлів та папок, що захищає дані від несанкціонованого доступу.*
2. **Простота використання.** *EFS легко налаштовується і використовує інтуїтивний інтерфейс для шифрування файлів і папок.*
3. **Інтеграція з Windows.** *EFS є частиною операційної системи Windows і забезпечує високу сумісність з іншими функціями безпеки.*

EFS є важливим інструментом для захисту конфіденційних даних у Windows, що допомагає забезпечити безпеку ваших файлів і папок.

Контрольні питання

1. З яких основних кроків складається процес встановлення ОС Windows 10?
2. Опишіть поняття «Користувачі» у Windows 10?
3. Опишіть поняття «Групи» у Windows 10?
4. Для чого потрібен інструмент «Журнал подій»?
5. Що забезпечують «Служби» у Windows 10?
6. Призначення інструменту «Розклад завдань»?
7. Основні функції інструменту «Керування дисками»?
8. Назвіть основні системні утиліти для дисків?
9. Назвіть основні вкладки Диспетчера завдань?
10. Як відобразити Відомості про систему?
11. Призначення резервного копіювання та відновлення?
12. Опишіть роботу функції «Контрольні точки»?
13. Як відобразити Засіб діагностики DirectX?
14. Як використовувати діагностику RAM у Windows 10?
15. Основні аспекти Реєстру Windows?
16. Основні функції Брандмауера Windows?
17. Основні аспекти Локальної політики безпеки?
18. Основні аспекти Групових політик безпеки?
19. Основні функції BitLocker?
20. Основні аспекти EFS?

Розділ 3. Адміністрування Windows Server 2016/2019/2022

Тема: Специфікація ОС. Мінімальні вимоги

План

1. Короткий огляд.
2. Системні вимоги.
3. Особливості Windows Server.
4. Типові ролі сервера.

Windows Server - це лінійка серверних операційних систем від Microsoft, яка надає інфраструктуру для побудови мереж, хостингу веб-сайтів, управління базами даних та інших задач підприємств та організацій. Ось декілька ключових аспектів:

1. **Різновиди**. *Windows Server має кілька версій, наприклад, Windows Server 2012, 2016, 2019 та остання - Windows Server 2022. Кожна нова версія додає нові функції та поліпшення.*
2. **Функції**. *Операційна система підтримує віртуалізацію через Hyper-V, дозволяючи створювати і керувати віртуальними машинами. Вона також забезпечує функції Active Directory для централізованого управління користувачами та ресурсами мережі.*
3. **Безпека**. *Windows Server має вбудовані засоби безпеки, такі як Windows Defender, контролі доступу до мережевих ресурсів та різні інструменти для захисту від кібератак.*
4. **Сумісність**. *Підтримує широкий спектр додатків і служб, що дозволяє легко інтегруватися в існуючі інфраструктури.*
5. **Управління**. *Містить потужні інструменти для адміністрування, як-от PowerShell, Server Manager, та Remote Desktop Services, що спрощують управління серверами і ресурсами.*

Windows Server - це надійна і масштабована платформа, що дозволяє підприємствам ефективно керувати своїми IT-ресурсами та забезпечувати стабільну роботу своїх додатків і сервісів.

Мінімальні вимоги до Windows Server 2022:

1. **Процесор**: *1.4 ГГц 64-бітний процесор, сумісний з архітектурою x64.*
2. **Оперативна пам'ять (RAM)**: *512 МБ для Server Core, 2 ГБ для Server з Desktop Experience.*
3. **Диск**: *32 ГБ або більше.*
4. **Мережевий адаптер**: *Ethernet адаптер, який може досягати пропускної здатності не менше 1 Гбіт/сек.*
5. **UEFI**: *Firmware UEFI версії 2.3.1c з підтримкою Secure Boot.*
6. **TPM**: *TPM версії 2.0.*

Ці вимоги можуть змінюватися в залежності від конфігурації вашого системи та встановлених додатків.

Для Windows Server 2022 рекомендується використовувати обладнання, яке забезпечує високу продуктивність та стабільність. Ось деякі рекомендації:

1. **Процесор**. *Використовуйте 64-бітний процесор з частотою не менше 2.0 ГГц та кількома ядрами (рекомендується 4 ядра або більше). Підтримка SLAT (Second Level Address Translation) для віртуалізації через Hyper-V.*
2. **Оперативна пам'ять (RAM)**. *Мінімально 8 ГБ RAM, але для кращої продуктивності рекомендується 16 ГБ або більше.*
3. **Диск**. *SSD з обсягом не менше 128 ГБ для операційної системи та додаткових даних. Використовуйте RAID для забезпечення високої надійності1.*
4. **Мережевий адаптер**. *Gigabit Ethernet адаптер, який підтримує PCI Express.*
5. **UEFI**. *Firmware UEFI версії 2.3.1c з підтримкою Secure Boot.*
6. **TPM**. *TPM версії 2.0 для підтримки функцій безпеки, таких як BitLocker Drive Encryption.*
7. **Графіка**. *Відеокарта, яка підтримує Super VGA (1024 x 768) або вищу роздільну здатність.*
8. **Клавіатура та мишка**. *Комп'ютер повинен мати клавіатуру та мишку (або інше сумісне пристрій вводу).*

Windows Server 2022 доступний у кількох основних версіях. Ось основні з них:

1. **Windows Server 2022 Datacenter**. *Основна версія для великих підприємств, яка підтримує високу ступінь віртуалізації та масштабованість.*
2. **Windows Server 2022 Standard**. *Ідеальна для середніх підприємств, які потребують деяких функцій віртуалізації.*
3. **Windows Server 2022 Essentials**. *Рекомендована для малих підприємств та індивідуальних користувачів з базовими потребами.*
4. **Windows Server 2022 Hyper-V Server**. *Версія, яка спеціалізується на використанні Hyper-V для віртуалізації. Вона не має графічного інтерфейсу.*

Кожна з цих версій має свої особливості та підходить для різних сценаріїв використання.

Windows Server 2022 може виконувати різні **Ролі** - набір специфічних функцій та сервісів, які можна додати і налаштувати на сервері для виконання певних задач. Кожна роль надає серверу можливість виконувати певні функції та забезпечувати певні сервіси для користувачів та інших пристроїв у мережі.

Ролі дозволяють адміністраторам серверів встановлювати лише ті функції, які необхідні для виконання конкретних завдань, що підвищує ефективність і безпеку роботи серверу.

Windows Server 2022 містить різноманітні ролі, які можна налаштувати в залежності від потреб вашої організації. Ось деякі з основних ролей:

1. **Active Directory Domain Services (AD-Domain-Services)**. *Забезпечує управління користувачами та комп'ютерами в мережі.*
2. **Active Directory Federation Services (ADFS-Federation)**. *Дозволяє користувачам входити до різних доменів за допомогою єдиного входу.*
3. **DHCP Server (DHCP)**. *Надає IP-адреси пристроям в мережі.*
4. **DNS Server (DNS)**. *Обслуговує запити на доменні імена.*
5. **File and Storage Services (FileAndStorage-Services)**. *Забезпечує управління файлами та пам'яткою.*
6. **Hyper-V (Hyper-V)**. *Віртуалізація для створення та управління віртуальними машинами.*
7. **Print and Document Services (Print-Services)**. *Управління принтерами та документами.*

8. **Remote Access (RemoteAccess)**. *Забезпечує віддалений доступ до мережі.*
9. **Remote Desktop Services (Remote-Desktop-Services)**. *Дозволяє віддалене керування комп'ютерами.*
10. **Web Server (IIS) (Web-Server)**. *Забезпечує веб-сервіси та управління веб-сайтами.*

Ці ролі можуть бути налаштовані та доповнені різними функціями та службами для задоволення специфічних потреб вашої IT-інфраструктури.

Контрольні питання

1. Ключові аспекти Windows Server 2022?
2. Мінімальні вимоги до Windows Server 2022?
3. Рекомендації до обладнання для встановлення Windows Server 2022?
4. Основні версії Windows Server 2022?
5. Основні ролі Windows Server 2022?

Тема: Розгортання, налаштування та адміністрування Windows Server

План

1. Встановлення ОС Windows Server.
2. Користувачі та групи.
3. Додавання ролей та компонентів.
4. Служба архівування Windows Server.
5. RDP.
6. Ліцензування служби терміналів.
7. VPN.
8. DHCP.
9. WEB-сервер.
10. Підведення підсумків.

Процес встановлення Windows Server схожий на аналогічний процес у Windows 10 чи 11 та складається з кількох основних кроків.

Підготовка до встановлення

1. **Оберіть версію Windows Server**. *Визначте, яку версію ви будете встановлювати (Standard, Datacenter, Essentials).*
2. **Завантажте інсталяційний носій**. *Завантажте ISO-образ з офіційного сайту Microsoft або підготуйте інсталяційний носій (DVD, USB-накопичувач).*
3. **Перевірте системні вимоги**. *Переконайтесь, що ваш сервер відповідає мінімальним системним вимогам.*

Встановлення операційної системи

1. **Завантаження з інсталяційного носія**:
   - *Вставте інсталяційний носій (DVD, USB) у сервер.*
   - *Перезавантажте сервер і зайдіть у BIOS/UEFI.*
   - *Оберіть завантаження з інсталяційного носія.*

2. **Інсталяція Windows Server**:
   - *Після завантаження з інсталяційного носія оберіть мову, формат часу та клавіатури, та натисніть "Далі".*
   - *Натисніть "Встановити зараз".*

- *Введіть ключ продукту або пропустіть цей крок, якщо у вас є ключ на наступному етапі.*
- *Оберіть версію Windows Server, яку ви хочете встановити, і натисніть "Далі".*
- *Прийміть умови ліцензії та натисніть "Далі".*

3. **Вибір типу встановлення**:
   - *Оберіть "Вибіркове встановлення: лише Windows (додатково)".*
   - *Оберіть розділ для встановлення (створіть новий розділ, якщо необхідно), і натисніть "Далі".*

4. **Завершення встановлення**:
   - *Після завершення копіювання файлів і налаштування системи сервер автоматично перезавантажиться.*
   - *Встановіть обліковий запис адміністратора та введіть пароль.*
   - *Налаштуйте початкові параметри серверу (настройки мережі, оновлення тощо).*

Після встановлення

1. **Оновлення системи**:
   - *Встановіть усі доступні оновлення через Windows Update.*

2. **Налаштування ролей і функцій**:
   - *Відкрийте "Server Manager" і додайте необхідні ролі та функції (DNS, DHCP, Active Directory тощо).*

3. **Безпека і резервне копіювання**:
   - *Налаштуйте заходи безпеки (брандмауер, антивірус, політики груп).*
   - *Налаштуйте резервне копіювання даних і системи.*

У Windows Server 2022 користувачі та групи є основними елементами управління доступом до ресурсів та забезпечення безпеки системи.

Користувачі

Користувач - це індивідуальний обліковий запис, який дає змогу конкретній особі чи сервісу доступ до ресурсів на сервері.

1. **Облікові записи користувачів**:
    - ***Локальні користувачі***. *Користувачі, які створюються та існують лише на конкретному сервері. Вони мають доступ лише до ресурсів цього серверу.*
    - ***Доменні користувачі***. *Користувачі, які створюються у Active Directory і можуть мати доступ до ресурсів на всіх серверах в домені.*

2. **Керування користувачами**. *Для управління обліковими записами користувачів використовується інструмент "Active Directory Users and Computers" або "Local Users and Groups" для локальних користувачів.*

Групи

Групи - це колекції користувачів, які об'єднані для спрощення управління правами доступу.

1. **Типи груп**:
    - ***Локальні групи***: *Діють лише на конкретному сервері. Містять облікові записи користувачів та інших локальних груп цього серверу.*
    - ***Глобальні групи***: *Використовуються в домені Active Directory. Містять облікові записи користувачів та інших глобальних груп з того ж домену.*
    - ***Універсальні групи***: *Діють на всіх серверах у лісу Active Directory. Містять облікові записи користувачів, глобальні та інші універсальні групи з будь-якого домену.*

2. **Права та дозволи**. *Призначення прав групам дозволяє ефективно керувати доступом до ресурсів. Наприклад, замість налаштування прав для кожного користувача окремо, можна призначити права всій групі.*

Створення та управління

- **Створення користувачів та груп**. *Використовуйте "Server Manager", "Active Directory Users and Computers" або PowerShell для створення та управління обліковими записами користувачів та груп.*

- **Призначення прав**. *Використовуйте політики груп та ACL (Access Control Lists) для призначення прав доступу до ресурсів.*

Локальні та Доменні Користувачі та Групи

Локальні користувачі та групи обмежені одним сервером і використовуються, коли сервер не входить до домену Active Directory.

Доменні користувачі та групи дозволяють централізовано управляти доступом на всіх серверах в домені через Active Directory, що полегшує адміністрування в великих організаціях.

Коректне налаштування користувачів та груп є основою для безпеки та ефективного управління ресурсами в Windows Server 2022.

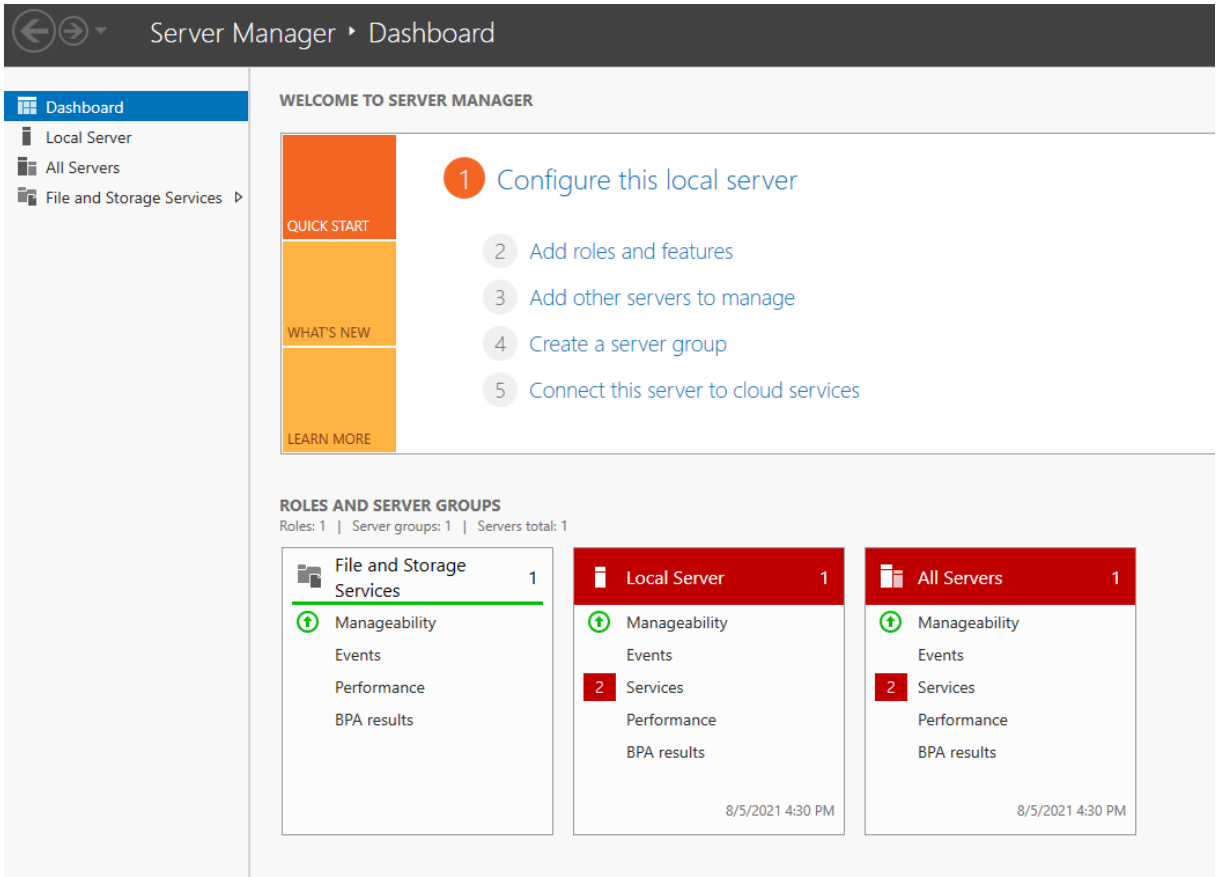


Рис. 3.1. Диспетчер сервера

Додавання ролей та компонентів у Windows Server є важливим процесом, який дозволяє налаштовувати сервер для виконання конкретних задач та надання певних сервісів. Ось покроковий посібник з додавання ролей та компонентів:

Додавання ролей та компонентів за допомогою Server Manager

1. **Відкриття Server Manager**:
    - *Натисніть кнопку "Пуск" та виберіть "Server Manager" або натисніть комбінацію клавіш Win+R, введіть "ServerManager" та натисніть Enter.*

2. **Додавання ролей і компонентів**:
    - *У вікні Server Manager виберіть "Manage" у верхньому правому кутку та натисніть "Add Roles and Features".*

3. **Майстер додавання ролей і компонентів**:
    - *З'явиться "Add Roles and Features Wizard". Натисніть "Next", щоб продовжити.*
    - *Оберіть тип інсталяції "Role-based or feature-based installation" та натисніть "Next".*
    - *Виберіть сервер, на якому будуть встановлені ролі та компоненти, та натисніть "Next".*

4. **Вибір ролей**:
    - *На сторінці "Select server roles" позначте ролі, які ви хочете додати (наприклад, Active Directory Domain Services, DNS Server, File and Storage Services тощо).*
    - *Після вибору ролей натисніть "Next". Майстер може запропонувати додати додаткові функції, необхідні для вибраної ролі.*

5. **Вибір компонентів**:
    - *На сторінці "Select features" позначте додаткові функції, які ви хочете додати (наприклад, .NET Framework, Windows Server Backup тощо).*
    - *Натисніть "Next", щоб продовжити.*

6. **Підтвердження вибору**:
    - *Перевірте обрані ролі та компоненти на сторінці "Confirm installation selections".*
    - *Якщо хочете, щоб сервер автоматично перезавантажився після інсталяції (у разі потреби), позначте опцію "Restart the destination server automatically if required".*

- *Натисніть "Install", щоб розпочати процес інсталяції.*

7. **Завершення інсталяції**:
   - *Дочекайтеся завершення інсталяції ролей та компонентів.*
   - *Після завершення інсталяції натисніть "Close".*

Використання PowerShell для додавання ролей і компонентів

Якщо ви віддаєте перевагу використанню командного рядка, ви можете додати ролі та компоненти за допомогою PowerShell:

1. **Відкрийте PowerShell від імені адміністратора**:
   - *Натисніть кнопку "Пуск", введіть "PowerShell", клацніть правою кнопкою миші на "Windows PowerShell" та виберіть "Run as administrator".*

2. **Додавання ролей і компонентів**:
   - *Використовуйте команду Install-WindowsFeature для додавання ролей і компонентів. Наприклад:*

     powershell

     Install-WindowsFeature -Name AD-Domain-Services, DNS -IncludeManagementTools
   - *Параметр -IncludeManagementTools додає інструменти управління для вибраних ролей.*

3. **Перегляд доступних ролей і компонентів**:
   - *Ви можете переглянути список доступних ролей і компонентів за допомогою команди:*

     powershell

     Get-WindowsFeature

Після додавання ролей і компонентів важливо налаштувати їх для правильного функціонування. Наприклад:

- **Active Directory Domain Services (AD DS)**. *Налаштуйте доменний контролер, створіть домен або приєднайтеся до існуючого.*
- **DNS Server**. *Налаштуйте зони та записи DNS.*
- **File and Storage Services**. *Налаштуйте загальний доступ до файлів і управління дисковими просторами.*

Цей процес дозволяє адаптувати сервер під конкретні потреби вашої організації, забезпечуючи надійну та ефективну роботу.

Служба архівування Windows Server (Windows Server Backup) допомагає створювати резервні копії файлів, директорій та системи. Ось основні кроки для налаштування та використання цієї служби:

Налаштування служби архівування

1. **Встановлення компонента Windows Server Backup**:
    - *Відкрийте "Диспетчер серверів" (Server Manager).*
    - *Натисніть "Додавання ролей і функцій" (Add Roles and Features).*
    - *Виберіть тип інсталяції (Role-based or Feature-based).*
    - *Оберіть сервер для інсталяції.*
    - *На етапі вибору компонентів позначте "Windows Server Backup" і натисніть "Далі" (Next).*
    - *Підтвердіть вибір і натисніть "Встановити" (Install).*

2. **Налаштування розкладу архівації**:
    - *Відкрийте "Диспетчер серверів" і натисніть "Резервне копіювання Windows Server" (Windows Server Backup).*
    - *Оберіть "Розклад резервного копіювання" (Backup Schedule).*
    - *Встановіть час і частоту архівації.*
    - *Оберіть цільовий диск або мережеве сховище для збереження резервних копій.*

3. **Виконання резервного копіювання**:
    - *Відкрийте "Диспетчер серверів" і натисніть "Резервне копіювання Windows Server" (Windows Server Backup).*
    - *Оберіть "Резервне копіювання один раз" (Backup Once).*
    - *Виберіть розділ або файли для архівації.*
    - *Натисніть "Почати" (Start) і дочекайтеся завершення процесу.*

Відновлення даних

1. **Відновлення файлів або директорій**:
   - *Відкрийте "Диспетчер серверів" і натисніть "Резервне копіювання Windows Server" (Windows Server Backup).*
   - *Оберіть "Відновлення" (Restore).*
   - *Виберіть резервну копію, яку хочете відновити.*
   - *Виберіть розділ або файли для відновлення.*
   - *Натисніть "Почати" (Start) і дочекайтеся завершення процесу.*

2. **Відновлення системи**:
   - *Відкрийте "Диспетчер серверів" і натисніть "Резервне копіювання Windows Server" (Windows Server Backup).*
   - *Оберіть "Відновлення" (Restore).*
   - *Виберіть резервну копію системи.*
   - *Натисніть "Почати" (Start) і дочекайтеся завершення процесу.*

Служба архівування Windows Server допомагає забезпечити безпеку даних і забезпечити можливість відновлення в разі аварійних ситуацій.

Remote Desktop Protocol (RDP) у Windows Server дозволяє віддалено підключатися до сервера та керувати ним через графічний інтерфейс. Ось ключові моменти про RDP:

Основи RDP

1. **Що таке RDP?**
   - *RDP (Remote Desktop Protocol) - це протокол розроблений Microsoft, який дозволяє користувачам віддалено підключатися до іншого комп'ютера або сервера з графічним інтерфейсом.*

2. **Застосування RDP**:
   - *Віддалене управління сервером або робочою станцією.*

- *Віддалене виконання програм та доступ до файлів.*
- *Підтримка та технічне обслуговування на відстані.*

Налаштування RDP

1. **Увімкнення RDP**:
   - *Відкрийте "Server Manager".*
   - *Натисніть "Local Server".*
   - *У секції "Remote Desktop" натисніть "Disabled", щоб увімкнути віддалений робочий стіл.*
   - *Виберіть "Allow remote connections to this computer" та підтвердіть зміни.*

2. **Конфігурація брандмауера**:
   - *Переконайтеся, що порт 3389 відкритий у брандмауері для RDP-з'єднань.*
   - *Для цього відкрийте "Windows Firewall with Advanced Security" і додайте правило для порту 3389.*

3. **Налаштування користувачів**:
   - *Визначте користувачів, які можуть підключатися через RDP.*
   - *Для цього відкрийте "System Properties", оберіть вкладку "Remote", натисніть "Select Users" і додайте потрібних користувачів.*

Використання RDP

1. **Підключення до сервера**:
   - *На клієнтському комп'ютері відкрийте "Remote Desktop Connection" (mstsc.exe).*
   - *Введіть ім'я або IP-адресу сервера та натисніть "Connect".*
   - *Введіть облікові дані користувача з правами доступу.*

2. **Безпечне підключення**:
   - *Використовуйте протоколи безпеки, такі як TLS, щоб захистити з'єднання.*
   - *Перевірте сертифікати безпеки для захисту від атак "man-in-the-middle".*

Переваги RDP

- **Зручність**. *Доступ до серверу з будь-якого місця за наявності Інтернет-з'єднання.*
- **Ефективність**. *Швидке і легке адміністрування серверів.*
- **Безпека**. *Можливість налаштування протоколів шифрування для захисту даних.*

RDP є потужним інструментом для віддаленого адміністрування та управління серверами, що значно полегшує роботу IT-фахівців.

Дистанційне керування

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

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

Термінальний режим

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

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

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

Фізичний або *реальний термінал* – як правило мається на увазі пристрій, обчислювальні можливості якого обмежені можливістю

відображати те, що йому передано з мережі (як максимум – повноекранну графіку).

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

Типи терміналів

Текстовий термінал – це пристрій (або програма) введення/виведення, які працюють в дуплексному режимі і використовують символьно-орієнтовані протоколи передачі даних, такі як telnet. Потоки даних між терміналом і сервером представляють ASCN-символи. Спеціальні символи (або послідовність символів) представляють команди керування сервером і відповіді сервера. Існують і службові команди, які керують виводом (переведення рядка, напівжирний/похилий текст, звуковий сигнал тощо) і сеансом зв'язку (узгодження версій протоколу тощо).

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

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

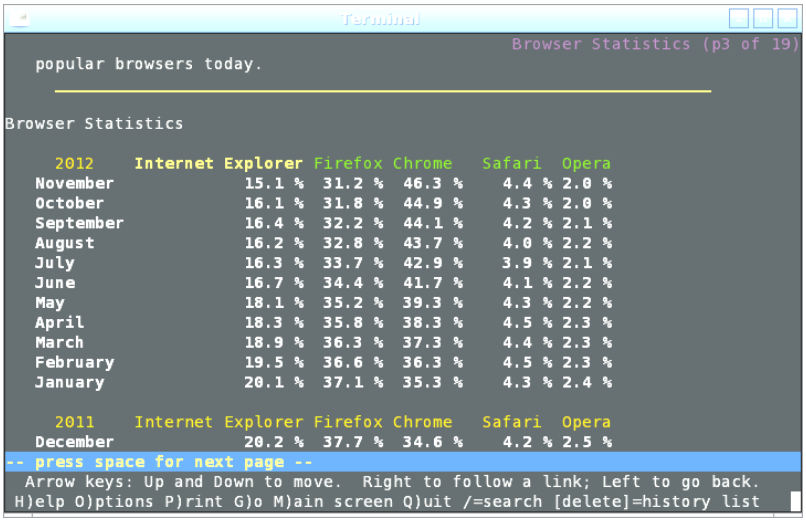


Рис. 3.2. Текстовий термінал

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

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

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

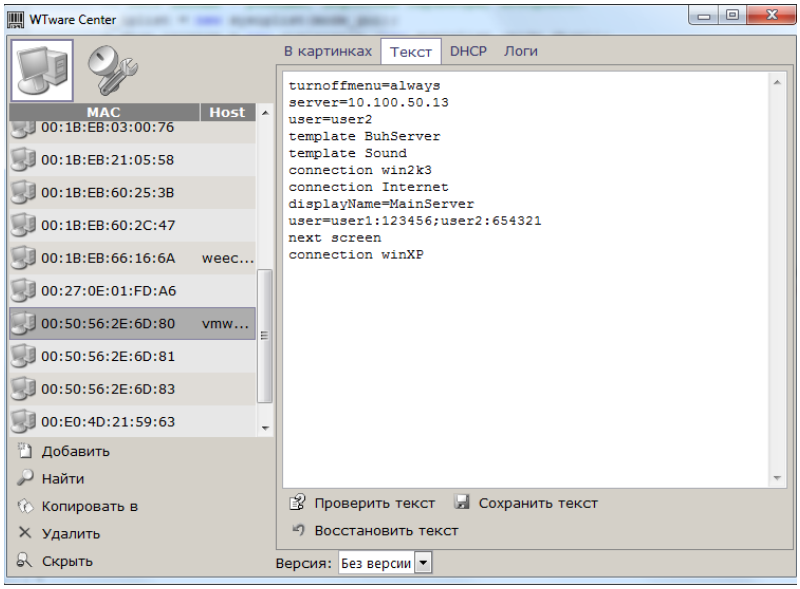


Рис. 3.3. Графічний термінал

Інтелектуальний термінал

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

Протоколи віддаленого керування

Сервіс telnet

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

Протокол rlogin

Протокол rlogin (англ. remote login – віддалений вхід в систему, RFC 1282, порт сервера – 513) дозволяє користувачам робочих станцій UNIX підключатися до віддалених серверів UNIX через Internet і працювати так само, як під час прямого підключення термінала до машини. Попри rlogin існує ще декілька подібних протоколів: rsh (remote shell), rcp (remote copy). Утиліти rlogin, rsh та rcp часто об’єднують під загальною назвою r-команд.

SSH (Secure Shell)

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

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

Remote Desktop Protocol

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

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

Remote Desktop підтримує роботу в двох режимах:

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

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

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

Веб-технології віддаленого керування

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

Застосування віддаленого керування

- ✓ *Для отримання доступу до офісного комп'ютера або файл-сервера з дому, або з іншого офісу. Ви зможете користуватися повним набором програм на своєму робочому комп'ютері з будь-якого місця, мати доступ*

до своїх документів і вести офісну роботу навіть з кафе. Подібний тип віддаленого керування комп'ютером через Інтернет активно використовується бізнесменами, що часто мають відрядження. Просто не вимикайте офісний комп'ютер – і він буде «з вами» скрізь, де є вихід в Інтернет.

- ✓ *Для керування критичними комп'ютерами, що працюють в складних мережах, наприклад, серверами. Віддалене керування комп'ютером через Інтернет дозволяє системному адміністратору постійно мати доступ до ресурсу, на збої в роботі якого повинна слідувати негайна реакція.*
- ✓ *Для роботи з віддаленими комп'ютерами і мережами через віддалений робочий стіл. Завдяки можливості керування через Інтернет, технічні фахівці мають можливість обслуговувати будь-які системи, що знаходяться в різних точках світу. Один системний адміністратор, наприклад, може налаштувати комп'ютери відразу в кількох містах: це дуже зручно для компаній, що мають велику мережу філій або складну інформаційну інфраструктуру.*
- ✓ *Для проведення веб-семінарів або дистанційного навчання. Можливість безпосередньо працювати на комп'ютері викладача або ж можливість викладача бачити всі дії учня і допомагати йому.*
- ✓ *За допомогою мобільного комп'ютера (ноутбука, нетбука, планшета IPad) з виходом в Інтернет можна здійснювати віддалене керування домашнім комп'ютером, перевіряти пошту, планувати завдання і користуватися документами та програмами.*

Організація віддаленого керування

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

Для організації віддаленого доступу та керування слід:

1) Встановити спеціальну програму на комп'ютер, який буде керованим. Ця програма дозволяє захистити дані, забезпечити конфіденційність обміну інформацією, а також правильність і надійність авторизації. Керувати своїм комп'ютером може лише власник, а інформація буде надійно захищена.

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

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

VNC-системи (Virtual Network Computing)

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

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

До одного VNC-сервера синхронно можуть поєднуватися кілька клієнтів. Найчастіше VNC-системи використовують для технічної підтримки і доступу з дому до комп'ютера на роботі.

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

Ліцензування служби терміналів у Windows Server є важливим аспектом для забезпечення правильного функціонування та відповідності правовим вимогам. Це дозволяє кільком користувачам одночасно підключатися до сервера для виконання завдань, що підвищує ефективність та гнучкість робочих процесів.

Основні кроки ліцензування

1. **Встановлення служби ліцензування**:
    - *Відкрийте "Server Manager" і додайте роль "Remote Desktop Services".*
    - *Виберіть необхідні компоненти, включаючи "Remote Desktop Licensing" та "Remote Desktop Session Host".*
    - *Встановіть вибрані компоненти.*

2. **Активація сервера ліцензій**:
    - *Використовуйте "RD Licensing Diagnoser" для активації сервера.*
    - *Відкрийте "Activation Wizard" і виберіть "Internet Explorer" як метод активації.*

- *Перейдіть на сторінку активації Microsoft і введіть ідентифікаційні дані.*
- *Вкажіть тип ліцензії та кількість придбаних ліцензій.*
- *Завершіть процес активації.*

3. **Підключення користувачів**:
   - *Після активації сервера, користувачі можуть підключатися до нього через RDP.*
   - *Користувачі повинні мати відповідні ліцензії для доступу до сервера.*

Переваги ліцензування служби терміналів

- **Економія ресурсів**. *Ліцензування дозволяє оптимізувати витрати на програмне забезпечення, зменшуючи необхідність придбання окремих ліцензій для кожного користувача.*
- **Простота управління**. *Автоматизація процесу ліцензування знижує ризик помилок та підвищує ефективність управління.*
- **Юридична відповідність**. *Правильне ліцензування гарантує, що компанія використовує програмне забезпечення відповідно до умов угоди, зменшуючи ризик юридичних проблем.*

Ліцензування служби терміналів у Windows Server є критичним аспектом для забезпечення ефективного та безпечного функціонування сервера. Відповідне ліцензування дозволяє оптимізувати витрати, підвищити продуктивність та забезпечити юридичну відповідність. Правильне налаштування та управління ліцензіями допомагає забезпечити стабільність та безперервність роботи сервера.

Для служб терміналів у Windows Server існує кілька типів ліцензій, які дозволяють користувачам підключатися до сервера та використовувати його ресурси. Ось основні типи ліцензій для служб терміналів (також відомих як Remote Desktop Services, RDS):

Типи ліцензій RDS

1. **RDS Per User CAL (Client Access License)**:
   - *Ця ліцензія надає доступ до сервера для кожного окремого користувача. Ліцензія прикріплюється до користувача, незалежно від того, з якого пристрою він підключається.*

- *Переваги: Гнучкість для користувачів, які можуть підключатися з різних пристроїв.*
- *Ідеально підходить для організацій, де користувачі часто працюють з різних пристроїв або місць.*

2. **RDS Per Device CAL**:
   - *Ця ліцензія надає доступ до сервера для кожного окремого пристрою. Ліцензія прикріплюється до пристрою, незалежно від того, скільки користувачів підключаються через цей пристрій.*
   - *Переваги: Економічність для середовищ, де кілька користувачів використовують один і той же пристрій.*
   - *Ідеально підходить для організацій з фіксованими робочими станціями або пристроями, які використовуються кількома користувачами.*

3. **RDS External Connector License**:
   - *Ця ліцензія дозволяє зовнішнім користувачам (наприклад, клієнтам або партнерам) отримувати доступ до сервера без необхідності купувати окремі ліцензії для кожного користувача або пристрою.*
   - *Переваги: Спрощення управління ліцензіями для зовнішніх користувачів.*
   - *Ідеально підходить для організацій, які надають доступ до своїх ресурсів зовнішнім користувачам.*

Вибір типу ліцензії

Вибір типу ліцензії залежить від вашої організаційної структури та способу використання серверів. Наприклад:

- *Якщо у вас багато користувачів, які підключаються з різних пристроїв, RDS Per User CAL може бути кращим варіантом.*
- *Якщо кілька користувачів використовують один і той же пристрій, RDS Per Device CAL може бути більш економічно вигідним.*
- *Якщо зовнішні користувачі регулярно підключаються до вашого сервера, RDS External Connector License може спростити управління ліцензіями.*

Правильне розуміння та вибір типу ліцензій є ключовими для забезпечення відповідності правовим вимогам та оптимізації витрат.

Virtual Private Network (VPN) у Windows Server дозволяє створювати захищені з'єднання між клієнтськими пристроями та мережею підприємства через Інтернет. Це забезпечує безпеку передачі даних і доступ до корпоративних ресурсів віддалено. Ось ключові моменти про VPN у Windows Server:

Основи VPN

1. **Що таке VPN?**
    - *VPN (Virtual Private Network) - це технологія, яка створює захищене з'єднання (тунель) через незахищену мережу, таку як Інтернет.*

2. **Переваги VPN**:
    - **Безпека**. *Шифрування даних для захисту від прослуховування.*
    - **Дистанційний доступ**. *Доступ до корпоративних ресурсів з будь-якого місця.*
    - **Приватність**. *Захист персональних даних від третіх осіб.*

Налаштування VPN у Windows Server

1. **Встановлення ролі VPN**:
    - *Відкрийте "Server Manager".*
    - *Натисніть "Add Roles and Features".*
    - *Оберіть "Role-based or feature-based installation" та оберіть сервер.*
    - *На сторінці "Select server roles" позначте "Remote Access" і натисніть "Next".*
    - *Підтвердіть вибір та натисніть "Install".*

2. **Налаштування ролі VPN**:
    - *Після встановлення ролі відкрийте "Remote Access Management Console".*
    - *Оберіть "Deploy VPN Only" для налаштування VPN.*
    - *Додайте сервер до списку серверів, які будуть використовуватися для VPN-з'єднань.*

- *Налаштуйте VPN-протоколи, такі як L2TP, SSTP або IKEv2, залежно від ваших потреб.*

3. **Налаштування мережевих політик і доступу**:
   - *Відкрийте "Routing and Remote Access" і налаштуйте політики доступу до мережі.*
   - *Налаштуйте автентифікацію користувачів та правила брандмауера для забезпечення безпеки.*

Підключення клієнтських пристроїв

1. **Налаштування клієнтського пристрою**:
   - *На клієнтському пристрої відкрийте "Network & Internet Settings".*
   - *Виберіть "VPN" і натисніть "Add a VPN connection".*
   - *Введіть потрібну інформацію (назва з'єднання, адреса сервера, тип VPN, облікові дані).*

2. **Підключення до VPN**:
   - *Виберіть створене VPN-з'єднання і натисніть "Connect".*
   - *Введіть облікові дані користувача, якщо запитується.*
   - *Після успішного з'єднання клієнтський пристрій матиме доступ до корпоративних ресурсів через захищене з'єднання.*

Переваги використання VPN у Windows Server

- **Зручність**: *Забезпечує безпечний дистанційний доступ до корпоративних ресурсів.*
- **Безпека**: *Шифрує дані, захищаючи їх від несанкціонованого доступу.*
- **Гнучкість**: *Підтримка різних протоколів VPN для різних потреб.*

VPN у Windows Server є потужним інструментом для забезпечення безпеки та доступу до корпоративних ресурсів з будь-якого місця.

Dynamic Host Configuration Protocol (DHCP) у Windows Server дозволяє автоматично призначати IP-адреси та інші налаштування мережі клієнтським пристроям у мережі. Ось основні моменти про DHCP у Windows Server:

Основи DHCP

1. **Що таке DHCP?**
   - *DHCP (Dynamic Host Configuration Protocol) - це протокол, який автоматично надає IP-адреси та інші параметри мережі (наприклад, маску підмережі, шлюз за замовчуванням та DNS-сервери) клієнтським пристроям у мережі.*

2. **Переваги DHCP**:
   - **Автоматизація**. *Автоматичне призначення IP-адрес зменшує кількість ручної роботи.*
   - **Централізоване управління**. *Легке управління та моніторинг IP-адрес з одного місця.*
   - **Зменшення конфліктів**. *Автоматичне уникнення конфліктів IP-адрес.*

Налаштування DHCP у Windows Server

1. **Встановлення ролі DHCP**:
   - *Відкрийте "Server Manager".*
   - *Натисніть "Add Roles and Features".*
   - *Виберіть "Role-based or feature-based installation" та оберіть сервер.*
   - *На сторінці "Select server roles" позначте "DHCP Server" та натисніть "Next".*
   - *Підтвердіть вибір і натисніть "Install".*

2. **Налаштування DHCP після встановлення**:
   - *Після встановлення ролі DHCP відкрийте "DHCP Manager".*
   - *Створіть новий діапазон IP-адрес (scope) для вашої мережі:*
     - *Клацніть правою кнопкою миші на "IPv4" і виберіть "New Scope".*

- *Введіть назву та опис діапазону.*
- *Вкажіть діапазон IP-адрес, який буде призначатися клієнтським пристроям.*
- *Вкажіть тривалість оренди IP-адрес.*

3. **Налаштування додаткових параметрів**:
    - *Налаштуйте параметри DHCP, такі як маска підмережі, шлюз за замовчуванням та адреси DNS-серверів.*
    - *Ви можете додати параметри вручну або скористатися майстром налаштування.*

4. **Активування діапазону (scope)**:
    - *Після створення та налаштування діапазону, активуйте його, клацнувши правою кнопкою миші на діапазоні та вибравши "Activate".*

Управління DHCP

1. **Розширене налаштування**:
    - *Ви можете створювати резервування IP-адрес для конкретних пристроїв за допомогою їх MAC-адрес.*
    - *Використовуйте політики для керування специфічними параметрами DHCP для різних груп клієнтів.*

2. **Моніторинг та звітність**:
    - *Використовуйте "DHCP Manager" для моніторингу оренди IP-адрес та стану діапазонів.*
    - *Налаштуйте журнали для відстеження подій DHCP.*

Переваги використання DHCP у Windows Server

- **Зручність**. *Автоматичне налаштування мережевих параметрів для клієнтів.*
- **Ефективність**. *Централізоване управління IP-адресами та параметрами мережі.*
- **Безпека**. *Можливість налаштування політик та резервування IP-адрес для підвищення безпеки.*

Web-сервер у Windows Server забезпечується через роль "Internet Information Services" (IIS). IIS - це гнучка, надійна та масштабована платформа для хостингу веб-сайтів та веб-додатків. Ось основні аспекти про IIS у Windows Server:

Основні функції IIS

1. **Хостинг веб-сайтів**:
   - *IIS дозволяє хостити веб-сайти на основі протоколів HTTP та HTTPS.*
   - *Підтримка статичних та динамічних веб-сторінок, включаючи ASP.NET, PHP, і JSP.*

2. **Масштабованість**:
   - *Підтримка хостингу кількох веб-сайтів на одному сервері (мультихостинг).*
   - *Використання навантажувального балансування та кластеризації для забезпечення високої доступності та продуктивності.*

3. **Безпека**:
   - *Підтримка аутентифікації, авторизації та шифрування даних.*
   - *Використання SSL/TLS сертифікатів для захисту з'єднань.*
   - *Захист від атак за допомогою модулів безпеки, таких як Request Filtering та URL Authorization.*

4. **Керування контентом**:
   - *Підтримка управління контентом через FTP та WebDAV.*
   - *Використання Application Pools для ізоляції та управління ресурсами веб-додатків.*

5. **Моніторинг та аналітика**:
   - *Інструменти для моніторингу продуктивності та аналізу журналів (Performance Monitor, Log Parser).*
   - *Підтримка розширеної аналітики та інтеграції з іншими системами моніторингу.*

Налаштування IIS у Windows Server

1. **Встановлення ролі IIS**:
    - *Відкрийте "Server Manager".*
    - *Натисніть "Add Roles and Features".*
    - *Оберіть "Role-based or feature-based installation" та виберіть сервер.*
    - *На сторінці "Select server roles" позначте "Web Server (IIS)" та натисніть "Next".*
    - *Виберіть необхідні функції та сервіси IIS, такі як ASP.NET, PHP, FTP Server, і натисніть "Install".*

2. **Налаштування веб-сайтів**:
    - *Після встановлення відкрийте "Internet Information Services (IIS) Manager".*
    - *Створіть новий веб-сайт, вказавши ім'я сайту, фізичний шлях до файлів сайту та IP-адресу або доменне ім'я.*
    - *Налаштуйте зв'язок (bindings) для сайту, включаючи порти та сертифікати SSL.*

3. **Налаштування додатків та безпеки**:
    - *Створіть та налаштуйте Application Pools для ізоляції додатків.*
    - *Налаштуйте правила безпеки, включаючи аутентифікацію та авторизацію користувачів.*

Переваги використання IIS

- **Простота у використанні**. *Інтуїтивно зрозумілий інтерфейс для налаштування та управління веб-сайтами.*
- **Масштабованість**. *Можливість розгортання веб-сайтів від малих до великих підприємств.*
- **Безпека**. *Підтримка різних методів захисту даних та доступу.*

Поширені сценарії використання IIS

- **Хостинг корпоративних сайтів та додатків**. *Веб-сервери для внутрішнього та зовнішнього використання.*
- **Розробка та тестування**. *Платформа для розробки та тестування веб-додатків.*

- **Забезпечення електронної комерції**. *Безпечні та масштабовані рішення для інтернет-магазинів.*

IIS є потужним та гнучким інструментом для хостингу веб-сайтів та додатків на платформі Windows Server.

Підведення підсумків Розділу 3.

У процесі вивчення Windows Server важливо зосередитися на кількох ключових аспектах, що забезпечують його ефективне та безпечне використання.

RDP (Remote Desktop Protocol) дозволяє адміністраторам та користувачам віддалено підключатися до серверів або робочих станцій для управління, підтримки та виконання завдань. Використання RDP надає можливість працювати з будь-якого місця, підвищуючи продуктивність та гнучкість. Важливо налаштувати безпеку з'єднань, щоб захистити дані від можливих загроз.

Ліцензування служби терміналів у Windows Server є критичним аспектом для забезпечення відповідності правовим вимогам та оптимізації витрат. Служба терміналів дозволяє кільком користувачам одночасно підключатися до одного сервера для виконання завдань. Правильне ліцензування гарантує, що компанія використовує програмне забезпечення відповідно до умов угоди, зменшуючи ризик юридичних проблем.

VPN (Virtual Private Network) забезпечує безпечний віддалений доступ до корпоративних ресурсів через Інтернет. Шифруючи дані та створюючи захищені тунелі, VPN захищає інформацію від несанкціонованого доступу та забезпечує конфіденційність. Використання VPN дозволяє віддаленим працівникам безпечно працювати з корпоративними ресурсами, підвищуючи продуктивність і гнучкість робочих процесів.

DHCP (Dynamic Host Configuration Protocol) автоматизує процес призначення IP-адрес та інших мережевих налаштувань для клієнтських пристроїв. Це знижує потребу в ручному налаштуванні, зменшуючи ймовірність помилок та покращуючи ефективність управління мережею. Правильне налаштування та моніторинг DHCP дозволяє забезпечити стабільність та безперервність роботи мережі.

WEB-сервер (Internet Information Services, IIS) у Windows Server є потужною платформою для хостингу веб-сайтів та веб-додатків. IIS забезпечує високу продуктивність, надійність та

масштабованість, підтримуючи різні технології та мови програмування. Правильне налаштування безпеки та моніторинг веб-серверу дозволяють забезпечити захист даних і стабільну роботу веб-додатків.

Ці ключові аспекти є основою для ефективного та безпечного використання Windows Server, забезпечуючи надійність та стабільність роботи в будь-якому середовищі. Вивчення та налаштування цих компонентів дозволяють максимізувати продуктивність та безпеку вашої IT-інфраструктури.

Контрольні запитання

1. Які існують основні редакції Windows Server, і чим вони відрізняються?
2. Як створити нового користувача в локальній групі та в AD?
3. Які найбільш популярні ролі в Windows Server?
4. Яке призначення служби архівування в Windows Server?
5. Які порти використовує RDP?
6. Які існують типи ліцензування служби терміналів?
7. Що таке VPN і для чого він використовується?
8. Що таке DHCP і яка його роль у мережі?
9. Як встановити та налаштувати IIS?
10. Які ключові аспекти адміністрування Windows Server?

Розділ 4. Адміністрування систем Mikrotik

Тема: Огляд продуктів Mikrotik

MikroTik - компанія з Латвії, яка займається розробкою обладнання для інтернет-мереж. Місія компанії MikroTik - зробити існуючі інтернет-технології швидшими, потужнішими та більш доступними для широкого кола користувачів.

В даний час MikroTik надає апаратне і програмне забезпечення для підключення до Інтернету в багатьох країнах світу. У компанії є реселлери в більшості країн світу і клієнти в кожній країні планети.

Ось огляд деяких популярних продуктів MikroTik:

Маршрутизатори

1. **Серія hAP ax**: *Недорогі маршрутизатори з підтримкою Wi-Fi 6, легким налаштуванням та керуванням.*
   Моделі включають:
   - ***hAP ax lite**: Компактний і доступний, підходить для малих офісів або домашнього використання.*
   - ***hAP ax²**: Трохи більший з покращеним охолодженням і підтримкою двох діапазонів.*
   - ***hAP ax³**: Покращений процесор і додаткові функції, такі як блокування реклами та підтримка USB.*
2. **Серія Chateau ax**: *Призначені для офісних середовищ, ці маршрутизатори пропонують високошвидкісні з'єднання та централізоване керування.*
3. **RB951G-2HnD**: *Компактний маршрутизатор з п'ятьма гігабітними Ethernet портами та надійною продуктивністю.*

Точки доступу

1. **Серія cAP ax**: *Двохдіапазонні точки доступу з підтримкою PoE, ідеальні для високої щільності користувачів.*
2. **Серія Chateau ax**: *Високошвидкісні точки доступу з декількома Ethernet портами та централізованим керуванням.*

Комутатори

1. **Серія hEX**: *Універсальні п'ятипортові гігабітні Ethernet комутатори з підтримкою PoE.*
2. **RB750Gr3**: *Потужний комутатор з гігабітними Ethernet портами та можливостями PoE.*

Продукти MikroTik відомі своєю надійною продуктивністю, гнучкістю та легкістю використання. Вони широко застосовуються в різних умовах, від домашніх мереж до великих корпоративних середовищ.

Mikrotik Router OS – це спеціалізована операційна система, призначена виключно для побудови багатофункціональних маршрутизаторів, фаєрволів, бриджів, базових станцій, vpn-серверів, web-серверів та інших пристроїв керування мережами. При цьому працювати операційна система може як на апаратних платформах Mikrotik RouterBoard , побудованої як правило на процесорах PowerPC і Atheros, так і на обладнанні, побудованому на базі x86 архітектури, простіше кажучи - звичайні персональні комп'ютери.

MikroTik RouterOS (або просто RouterOS) – це операційна система, розроблена для маршрутизаторів MikroTik. Вона дозволяє перетворити будь-який комп'ютер на маршрутизатор з усіма необхідними функціями, такими як маршрутизація, брандмауер, управління пропускною здатністю, точка доступу Wi-Fi, з'єднання для зворотного зв'язку, шлюз гарячої точки та сервер VPN.

RouterOS можна встановити на x86 машини (наприклад, на ПК) або на спеціалізовані пристрої MikroTik. Він також підтримує віртуальні середовища, що дозволяє використовувати його як віртуальний маршрутизатор.

MikroTik RouterOS широко використовується в різних сферах завдяки своїй гнучкості та багатофункціональності.

Розглянемо кілька основних сценаріїв, де RouterOS знаходить своє застосування:

1. Інтернет-провайдери та оператори зв'язку

RouterOS популярний серед Інтернет-провайдерів та операторів зв'язку завдяки своїм можливостям управління пропускною здатністю, маршрутизації та безпеки. Він дозволяє ефективно керувати великими мережами та надавати надійні послуги для клієнтів.

2. Малі та середні підприємства (SMB)

Малі та середні підприємства використовують RouterOS для створення надійних і безпечних мережевих інфраструктур. RouterOS підтримує різні функції, такі як VPN, фільтрація контенту та управління трафіком, що робить його ідеальним рішенням для бізнесу.

3. Освітні заклади

Багато університетів, шкіл та інших навчальних закладів використовують RouterOS для забезпечення доступу до Інтернету, управління користувачами та моніторингу мережевого трафіку. Він допомагає забезпечити безпечне та стабільне підключення для студентів і співробітників.

4. Домашні користувачі та ентузіасти

RouterOS також використовується домашніми користувачами та ентузіастами мережевих технологій для створення індивідуальних рішень. Вони цінують його за багатофункціональність і можливість налаштування під потреби користувача.

5. Готелі та підприємства гостинності

Готелі та інші підприємства гостинності використовують RouterOS для управління мережами Wi-Fi, наданням гостям доступу до Інтернету та забезпечення безпеки мережі.

MikroTik RouterOS є універсальним рішенням, яке знаходить своє застосування в багатьох сферах завдяки своїм потужним функціям та можливостям налаштування.

Розглянемо кілька основних сценаріїв, де RouterOS знаходить своє застосування:

1. Інтернет-провайдери та оператори зв'язку

RouterOS популярний серед Інтернет-провайдерів та операторів зв'язку завдяки своїм можливостям управління пропускною здатністю, маршрутизації та безпеки. Він дозволяє ефективно керувати великими мережами та надавати надійні послуги для клієнтів.

2. Малі та середні підприємства (SMB)

Малі та середні підприємства використовують RouterOS для створення надійних і безпечних мережевих інфраструктур. RouterOS підтримує різні функції,

такі як VPN, фільтрація контенту та управління трафіком, що робить його ідеальним рішенням для бізнесу.

3. Освітні заклади

Багато університетів, шкіл та інших навчальних закладів використовують RouterOS для забезпечення доступу до Інтернету, управління користувачами та моніторингу мережевого трафіку. Він допомагає забезпечити безпечне та стабільне підключення для студентів і співробітників.

4. Домашні користувачі та ентузіасти

RouterOS також використовується домашніми користувачами та ентузіастами мережевих технологій для створення індивідуальних рішень. Вони цінують його за багатофункціональність і можливість налаштування під потреби користувача.

5. Готелі та підприємства гостинності

Готелі та інші підприємства гостинності використовують RouterOS для управління мережами Wi-Fi, наданням гостям доступу до Інтернету та забезпечення безпеки мережі.

Отже, MikroTik RouterOS є універсальним рішенням, яке знаходить своє застосування в багатьох сферах завдяки своїм потужним функціям та можливостям налаштування.

Основні переваги використання обладнання MikroTik:

1. Вартість

MikroTik відомий своєю доступністю, пропонуючи високоякісні продукти за конкурентоспроможною ціною. Це особливо важливо для малих та середніх підприємств, які шукають бюджетні мережеві рішення.

2. Функціональність

MikroTik обладнання підтримує широкий спектр функцій, включаючи маршрутизацію, брандмауер, управління пропускною здатністю, VPN, QoS та багато іншого. Це дозволяє користувачам налаштовувати мережу відповідно до їхніх потреб.

3. Гнучкість

Завдяки операційній системі RouterOS, користувачі можуть налаштовувати мережу дуже детально, включаючи правила безпеки, маршрутизацію, моніторинг трафіку та інші параметри. Це робить MikroTik рішенням для різних типів мереж, від домашніх до корпоративних.

4. Надійність

Продукти MikroTik відомі своєю надійністю та стабільністю. Вони використовуються в різних умовах, від домашніх мереж до великих

корпоративних середовищ, і забезпечують стабільне підключення навіть при високих навантаженнях.

5. Підтримка спільноти

MikroTik має велику і активну спільноту користувачів по всьому світу. Це означає, що користувачі можуть легко знайти підтримку, поради та рішення для будь-яких проблем, з якими вони можуть стикнутися.

6. Програмні оновлення

Компанія MikroTik регулярно випускає оновлення для RouterOS, які додають нові функції та покращують безпеку. Це дозволяє користувачам завжди залишатися на передовій технологій.

7. Підтримка PoE

Багато пристроїв MikroTik підтримують Power over Ethernet (PoE), що дозволяє живити пристрої через Ethernet-кабелі, зменшуючи кількість необхідних кабелів і спрощуючи встановлення.

8. Центральне керування

Завдяки можливостям центрального керування, адміністратори мереж можуть легко налаштовувати, моніторити та керувати великою кількістю пристроїв з одного інтерфейсу.

Ці переваги роблять MikroTik популярним вибором серед мережевих фахівців та компаній по всьому світу.

Контрольні запитання

1. Яка місія компанії MikroTik?
2. Які типи маршрутизаторів пропонує MikroTik?
3. Як називається спеціалізована операційна система MikroTik для маршрутизаторів?
4. Які основні сценарії використання MikroTik RouterOS?
5. Які переваги обладнання MikroTik порівняно з іншими мережевими рішеннями?

Тема: Cloud Hosted Router

Cloud Hosted Router (CHR) - це версія RouterOS, яка призначена для використання як віртуальна машина. Він підтримує архітектуру x86 64-біт і може працювати на більшості популярних гіпервізорів, таких як VMWare, Hyper-V, VirtualBox, KVM та інші.

Основні переваги CHR:

- **Повна підтримка функцій RouterOS**: *CHR має усі основні функції RouterOS за замовчуванням.*
- **Різноманітність платформ**: *Він може працювати на багатьох гіпервізорах, що робить його дуже гнучким.*
- **Різні моделі ліцензування**: *CHR має інший модель ліцензування порівняно з іншими версіями RouterOS.*

Системні вимоги:

- **ОС**: *RouterOS v6.34 або новіша*
- **Процесор**: *64-біт з підтримкою віртуалізації*
- **ОП**: *128 МБ або більше*
- **Диск**: *128 МБ або більше для віртуального жорсткого диска (максимум 16 ГБ)*

Mikrotik Cloud Hosted Router (CHR): Потужний інструмент для мережевого керування

Mikrotik Cloud Hosted Router (CHR) — це віртуальний маршрутизатор, який можна використовувати для організації мережі на основі хмарних технологій. CHR є простим у використанні і може бути встановлений за рахунок кількох простих кроків.

CHR має такі переваги:

- *Простота використання: Mikrotik Cloud Hosted Router можна будувати та керувати за допомогою веб-інтерфейсу або API.*

- *Масштабність: CHR може бути масштабований до більших розмірів, щоб відповідати потребам вашого бізнесу.*
- *Гібкость: CHR можна використовувати для різних типів сетей, включаючи мережі підприємства, мережі малого бізнесу та мережі для домашніх користувачів.*

Mikrotik CHR може використовуватися для наступних цілей:

- *Організація мережі для будинку або офісу*
- *Підключення до Інтернету*
- *Обмін даних між мережами*
- *Забезпечення безпеки мережі*

CHR можна придбати в різних постачальників, включаючи Cisco, Juniper Networks і VMware.

Як встановити Cloud Hosted Router

CHR — це програмний маршрутизатор, який працює на базі програмного забезпечення. Це означає, що вона не потребує спеціального обладнання, такого як ASIC або FPGA.

CHR — це гнучкий маршрутизатор, який можна використовувати для різних типів мереж. Він може бути використаний для мереж підприємства, мереж малого бізнесу та мереж для домашніх користувачів.

Для установки CHR потрібно комп'ютер з наступними характеристиками:

- *Операційна система Windows, Linux або macOS*
- *Процесор Intel Core i3 або аналогічний*
- *4 ГБ оперативної пам'яті*
- *50 ГБ вільного місця на диску*

Налаштування mikrotik cloud hosted router:

1. *Завантажте інсталяційний файл CHR з веб-сайту Cisco*
2. *Запустіть інсталятор і дотримуйтесь інструкцій на екрані*
3. *Виберіть мову установки*
4. *Прийміть умови ліцензії*
5. *Введіть ім'я користувача і пароль для адміністратора CHR*
6. *Виберіть розташування для установки CHR*

7. *Натисніть кнопку "Встановити"*

Після завершення установки CHR буде запущений. Ви можете ввійти в систему за допомогою імені користувача і пароля, які ви ввели під час установки.

Після входу в систему ви можете налаштувати CHR відповідно до ваших потреб. Для цього використовуйте панель керування CHR.

Установка Mikrotik CHR на VPS

Це простий та швидкий процес, який може бути виконаний за кілька кроків. Для цього необхідно створити VPS за допомогою віртуалізації KVM або LXC, завантажити образ CHR на VPS, запустити CHR та налаштувати його. Після запуску CHR ви отримаєте доступ до веб-консолі CHR.

Для налаштування CHR виконайте наступні дії:

1. *Увійдіть до веб-консолі CHR за допомогою логіна admin і пароля, який ви вказали при створенні CHR*
2. *У меню System > Administration введіть ліцензію Mikrotik CHR*
3. *Налаштуйте мережеві інтерфейси CHR*
4. *Налаштуйте інші параметри CHR*

Рівні ліцензії Cloud Hosted Router та процес активації

На відміну від залізної версії RouterOS, Cloud Hosted Router не має «прив'язки» ліцензії до обладнання, а також не має певних обмежень, наприклад, немає обмежень за кількістю тунелів.

Єдине обмеження, яке накладають різні рівні ліцензій, — це швидкість кожного з інтерфейсів.

Нижче представлені різні рівні ліцензій, їх відмінності та вартість:

- *Free*
- *P1 безстрокова-1*
- *P10 безстрокова-10*
- *P-unlimited безстрокова-безлімітна*

Mikrotik CHR license — це ліцензія, яка дозволяє використовувати Mikrotik CHR. Ліцензії Mikrotik CHR доступні в декількох варіантах, які відрізняються за функціональністю і ціною.

Для домашнього використання підійде безкоштовна пробна ліцензія, яка дозволяє використовувати всі функції Mikrotik CHR протягом 60 днів. Для комерційного використання можна придбати платну ліцензію, яка забезпечує безстроковий доступ до всіх функцій Mikrotik CHR.

Висновок

Cloud Hosted Router — це хороший варіант для організації мережі на основі хмарних технологій. Він простий у використанні, економічний і має широкий спектр функцій. Однак, перед його використанням слід врахувати його обмеження.

Контрольні запитання

1. Яка архітектура підтримується Cloud Hosted Router (CHR)?
2. Які гіпервізори підтримує CHR?
3. Які основні системні вимоги для установки CHR?
4. Які рівні ліцензії доступні для Cloud Hosted Router і їхні обмеження?

Тема: Огляд інтерфейсу системи RouterOS

MikroTik Winbox 4 — це нова ера керування мережею MikroTik. Winbox 4 представляє собою сучасний, швидкий і зручний графічний інтерфейс (GUI) для роботи з RouterOS. Багато адміністраторів вже високо оцінили нову версію за її інтуїтивність і функціональність, що робить управління мережами простішим і ефективнішим. У цій статті ми детально розглянемо нові можливості Winbox 4, процес його встановлення та основні зміни в порівнянні з попередніми версіями.

Особливості MikroTik Winbox 4

Winbox 4 впроваджує низку інновацій, які значно відрізняють його від попередніх версій. Основні нововведення:

- ✓ ***Сучасний інтерфейс користувача (GUI).*** *Новий дизайн Winbox 4 став революційним у порівнянні зі старими версіями. Інтерфейс зазнав суттєвих змін, що може викликати невелику плутанину у користувачів старих версій, однак новий підхід є значно зручнішим.*
- ✓ ***Панель ресурсів.*** *У нижній частині інтерфейсу додано нову панель, яка відображає інформацію про версію RouterOS, модель пристрою, використання процесора та пам'яті, а також поточний час і дату. Ця панель може бути прихована через налаштування.*
- ✓ ***Покращення продуктивності.*** *Новий Winbox працює швидше, скорочуючи час завантаження і реагуючи на команди значно швидше.*
- ✓ ***Темний режим.*** *Для багатьох користувачів це довгоочікуване оновлення. За замовчуванням використовується світлий режим, але можна легко переключитися на темний через налаштування.*

Як завантажити та встановити Winbox 4

Winbox 4 доступний для трьох основних операційних систем: Windows, Linux та macOS. Завантажити його можна зі сторінки завантажень MikroTik (Рис. 4.1.).

1. *Перейдіть на сторінку завантажень.*
2. *Виберіть відповідну версію для вашої операційної системи.*
3. *Завантажте та запустіть файл інсталяції.*

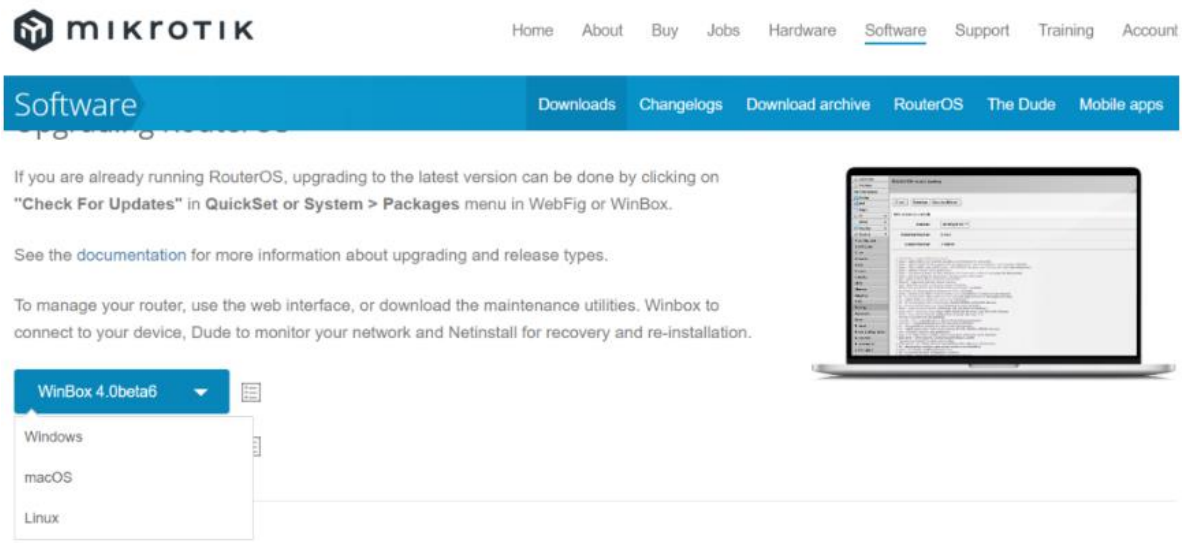


Рис. 4.1. Сторінка завантажень Mikrotik

Після встановлення відкриється вікно входу (Рис. 4.2.), в якому можна побачити новий логотип і оновлену панель Neighbours, яка тепер розташована поруч.

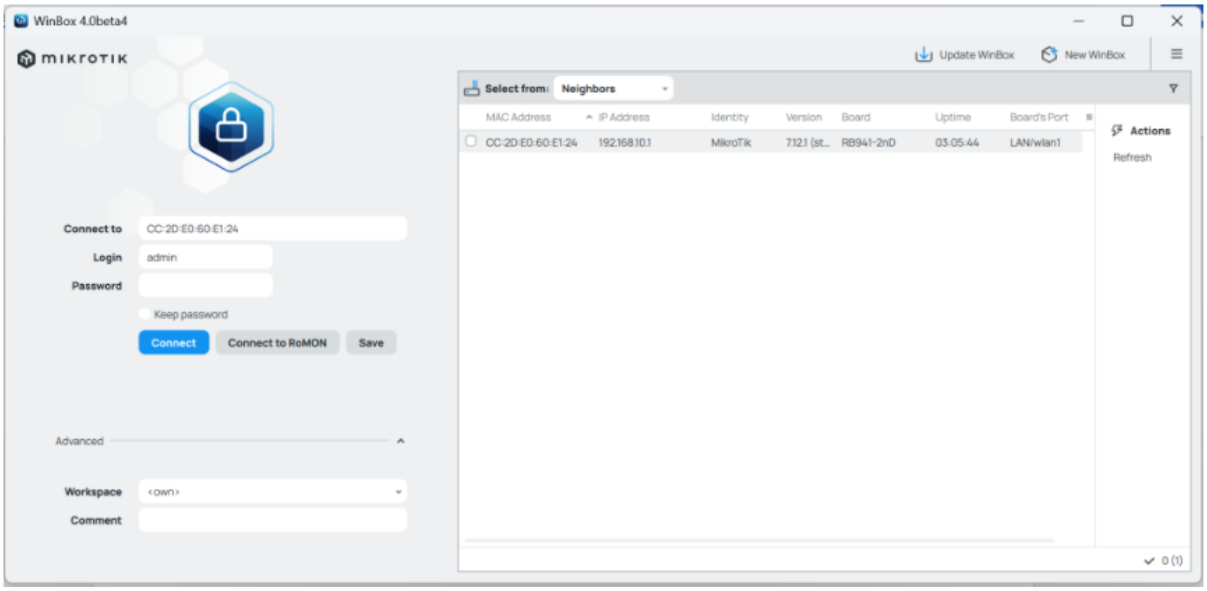


Рис. 4.2. Вікно входу Mikrotik RouterOS.

Тепер ми можемо увійти в нашу MikroTik RouterOS за допомогою Winbox 4, надавши IP-адресу/MAC-адресу, ім’я користувача та пароль.

Робота з MikroTik Winbox 4

Після входу в систему користувачі помітять оновлений дизайн інтерфейсу. Ось ключові зміни:

- ✓ ***Панель ресурсів**: Відображає важливу інформацію про пристрій.*
- ✓ ***Меню налаштувань**: Залишається схожим на попередні версії, але отримало нові іконки.*
- ✓ ***Панель дій**: Значно змінилася, включаючи новий вигляд кнопок, полів вводу та розташування елементів.*

Темний режим можна увімкнути через налаштування, що робить інтерфейс зручнішим для роботи в умовах низького освітлення.

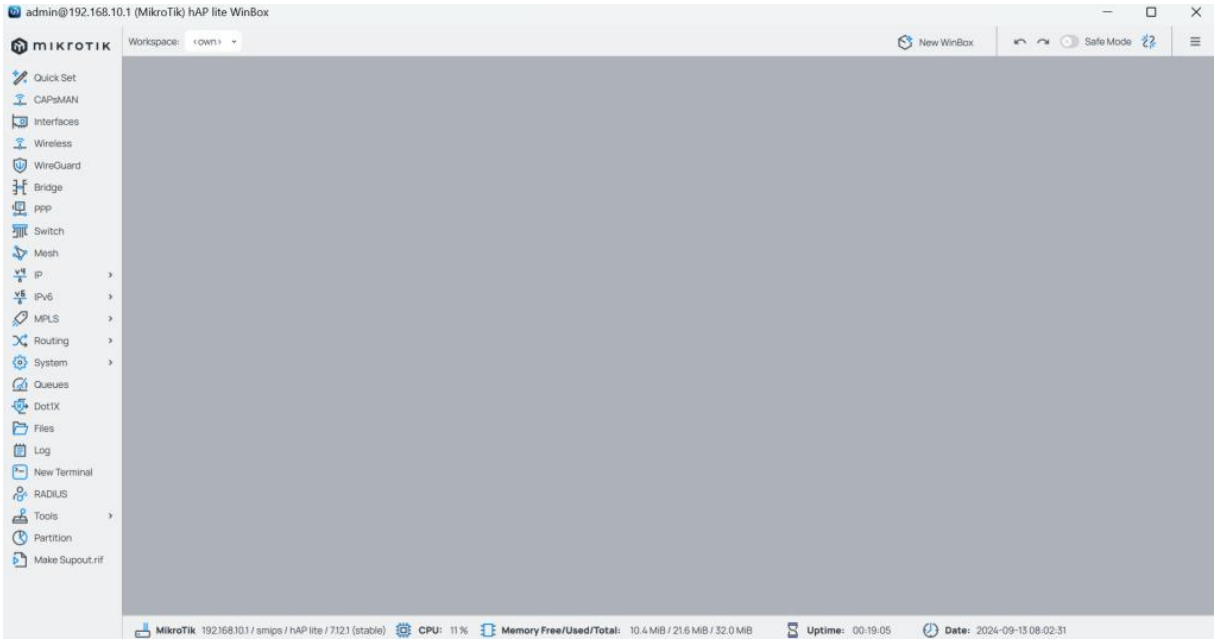


Рис. 4.3. Інтерфейс MikroTik Winbox 4

Панель меню MikroTik Winbox 4 майже така ж, як і в старій Winbox, за винятком зміни значка. З цієї панелі меню ми можемо легко керувати будь-якими послугами.

Основні зміни дизайну MikroTik Winbox 4 можна знайти на панелі дій (Action). На будь-якій панелі дій ми побачимо новий дизайн кнопки, поле введення та положення кнопки Action. Наприклад, якщо ми перейдемо до пункту меню IP > Адреси, ми побачимо новий дизайн, як на зображенні нижче (Рис. 4.4). Хто знайомий зі старою Winbox може зіткнутися з невеликою плутаниною. Але якщо звикнути, то нова версія простіше.

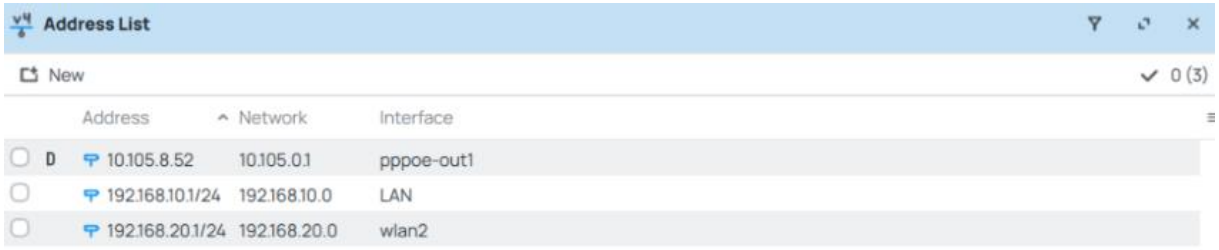


Рис. 4.4. Інтерфейс AddressList

Світлий режим є режимом за замовчуванням для MikroTik Winbox 4, але якщо ми хочемо, ми можемо легко перемкнути світлий режим на темний режим і навпаки з налаштувань.

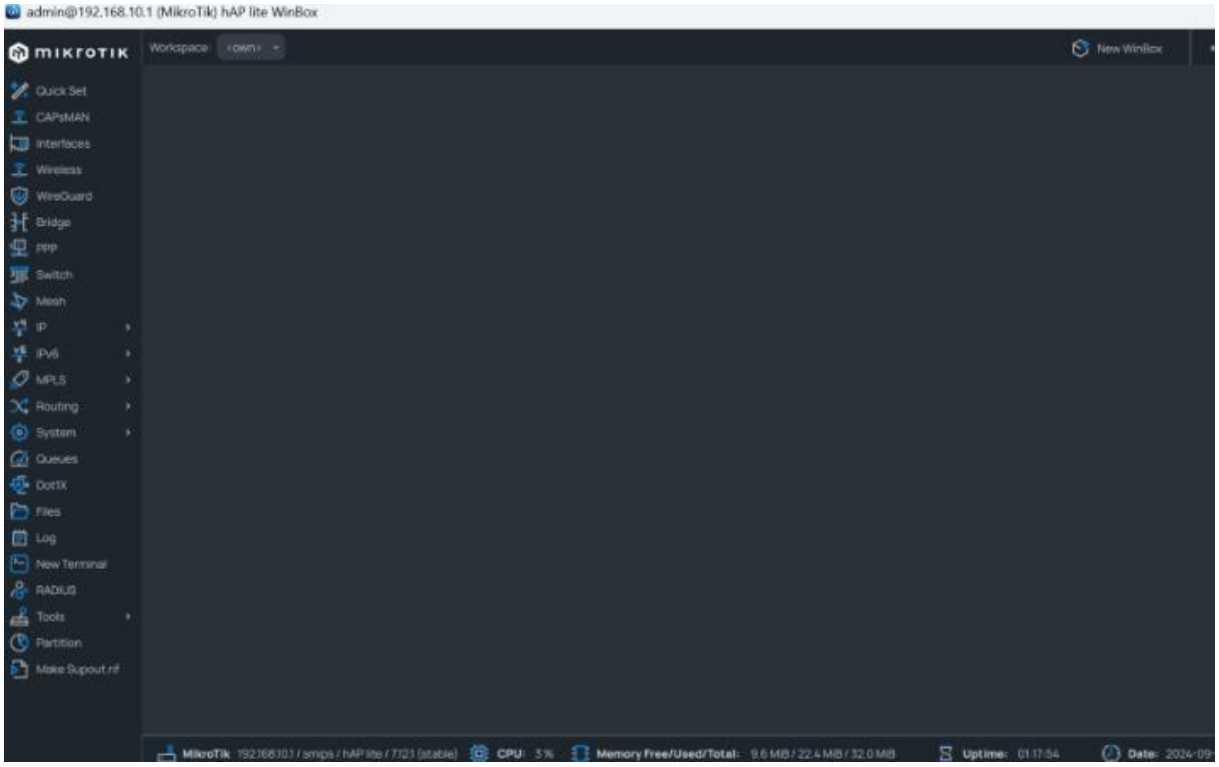


Рис. 4.5. Темний режим MikroTik Winbox 4

Швидке налаштування MikroTik RouterOS 7 за допомогою Winbox 4

Щоб наглядно побачити всі зміни графічного інтерфейсу розглянемо варіант швидкого налаштування MikroTik RouterOS 7 за допомогою Winbox 4.

Під’єднайте кабель провайдера до першого порту ether (ether1), а потім під’єднайте кабель RJ45 до ПК та будь-якого іншого порту маршрутизатора MikroTik. Відкрийте Winbox 4 і виберіть «Neighbors» на правій панелі вікна входу.

MAC підключеного інтерфейсу буде показано на панелі «Neighbors». Клацніть на ньому, і його буде призначено у полі введення Connect To на панелі входу.

Тепер введіть admin у вікні введення та залиште поле пароля порожнім, а потім натисніть кнопку «Connect». Тепер ви зможете увійти в MikroTik RouterOS 7.

Тепер виконайте наступні кроки, щоб швидко налаштувати MikroTik RouterOS 7:

- ✓ *У Winbox 4 клацніть пункт меню Quick Set на лівій панелі меню. З'явиться вікно Quick Set.*
- ✓ *Виберіть Home AP зі спадного меню Quick Set. Вікно налаштування домашньої точки доступу виглядає так, як показано нижче.*

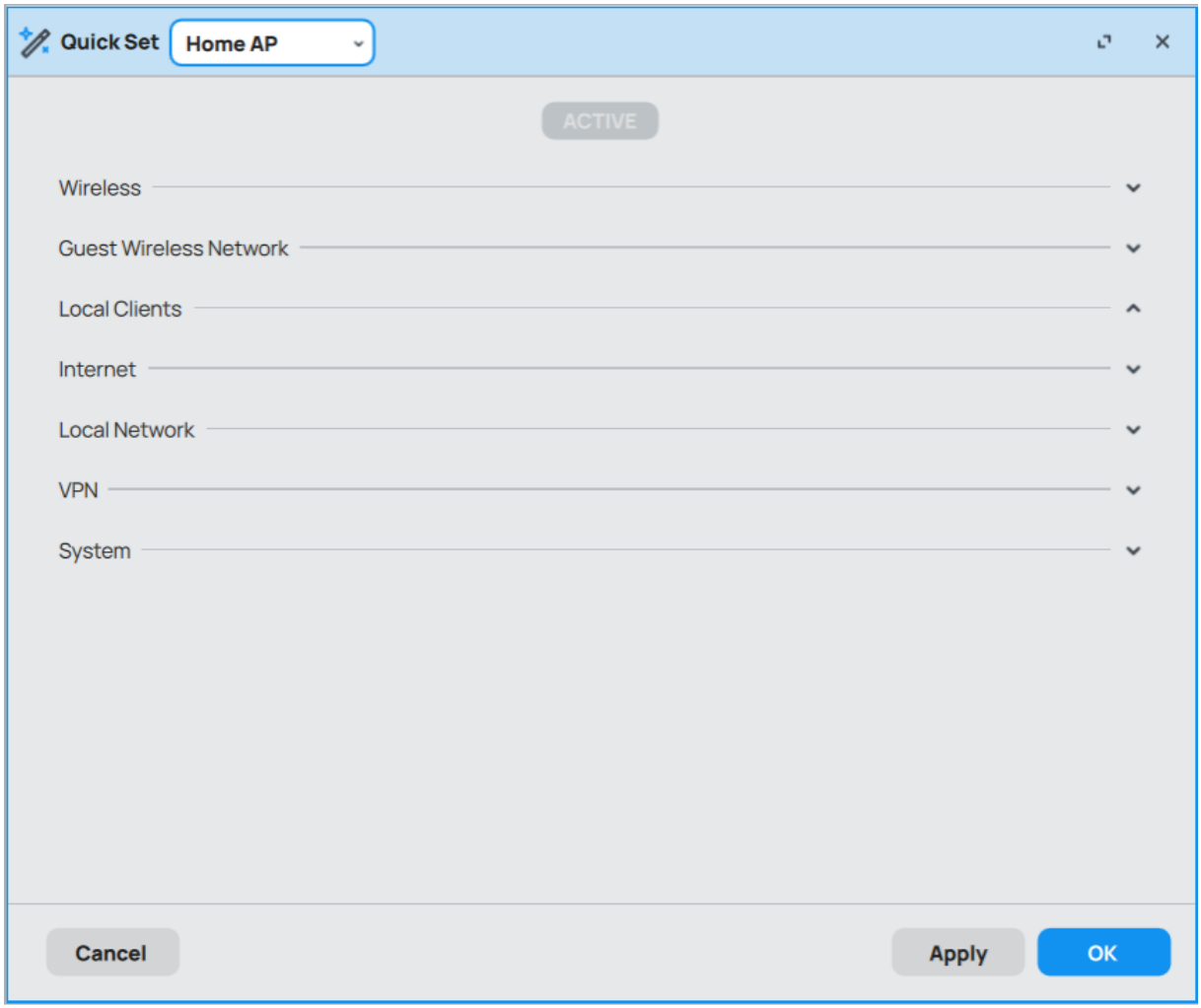


Рис. 4.6. Інтерфейс Швидкі налаштування

Швидке бездротове налаштування

- ✓ *Клацніть панель «Wireless» і введіть SSID (наприклад: MikroTik AP) у полі введення «Network Name».*
- ✓ *Клацніть на знак плюс (+) WiFi Password і введіть пароль мережі у вікні введення, що з'явилося.*

Швидке налаштування Інтернету

Тут буде налаштовано підключення провайдера. Інтернет-провайдер може надати три типи з'єднань – автоматичне (DHCP), PPPoE або статичне. Автоматично не має додаткової конфігурації, оскільки все буде призначено динамічно. Для PPPoE потрібне ім'я користувача та пароль, які будуть надані вашим Інтернет-провайдером. Статичне підключення потребує IP-адреси, маски підмережі та шлюзу за замовчуванням.

Клацніть на панелі «Internet» і виберіть тип підключення провайдера з перемикача «Address Acquisition».

- ✓ *Для автоматичного підключення: не потрібно нічого робити. Просто виберіть перемикач «Automatic», і він увімкне клієнт DHCP на порту ether1 і підключиться до DHCP-сервера провайдера.*
- ✓ *Для підключення PPPoE: введіть ім'я користувача PPPoE, пароль і назву служби PPPoE, надані провайдером, і введіть їх відповідно, а потім натисніть кнопку «Reconnect».*
- ✓ *Для статичного підключення: введіть IP-адресу, маску мережі та шлюз від провайдера та введіть їх відповідно. Також введіть IP-адресу DNS-сервера, якщо вам надає ваш провайдер, або ви можете використовувати загальнодоступну IP-адресу DNS Google: 8.8.8.8 і 8.8.4.4.*

Швидке налаштування локальної мережі

Клацніть на панелі «Local Network» та виконайте наступні дії.

- ✓ *Введіть IP-адресу шлюзу локальної мережі (наприклад: 192168.100.1) у полі введення IP-адреси.*
- ✓ *Виберіть маску мережі зі спадного меню «Netmask». Наприклад: щоб отримати доступні 256 IP-адрес у локальній мережі, виберіть параметр 255.255.255.0(/24).*
- ✓ *Установіть прапорець «Bridge All LAN Ports».*
- ✓ *Установіть прапорець DHCP Server.*
- ✓ *Введіть діапазон IP-адрес сервера DHCP (192.168.100.2-192.168.100.200) у поле введення діапазону сервера DHCP.*
- ✓ *Також натисніть прапорець NAT.*

Тепер натисніть «Apply» та кнопку «ОК».

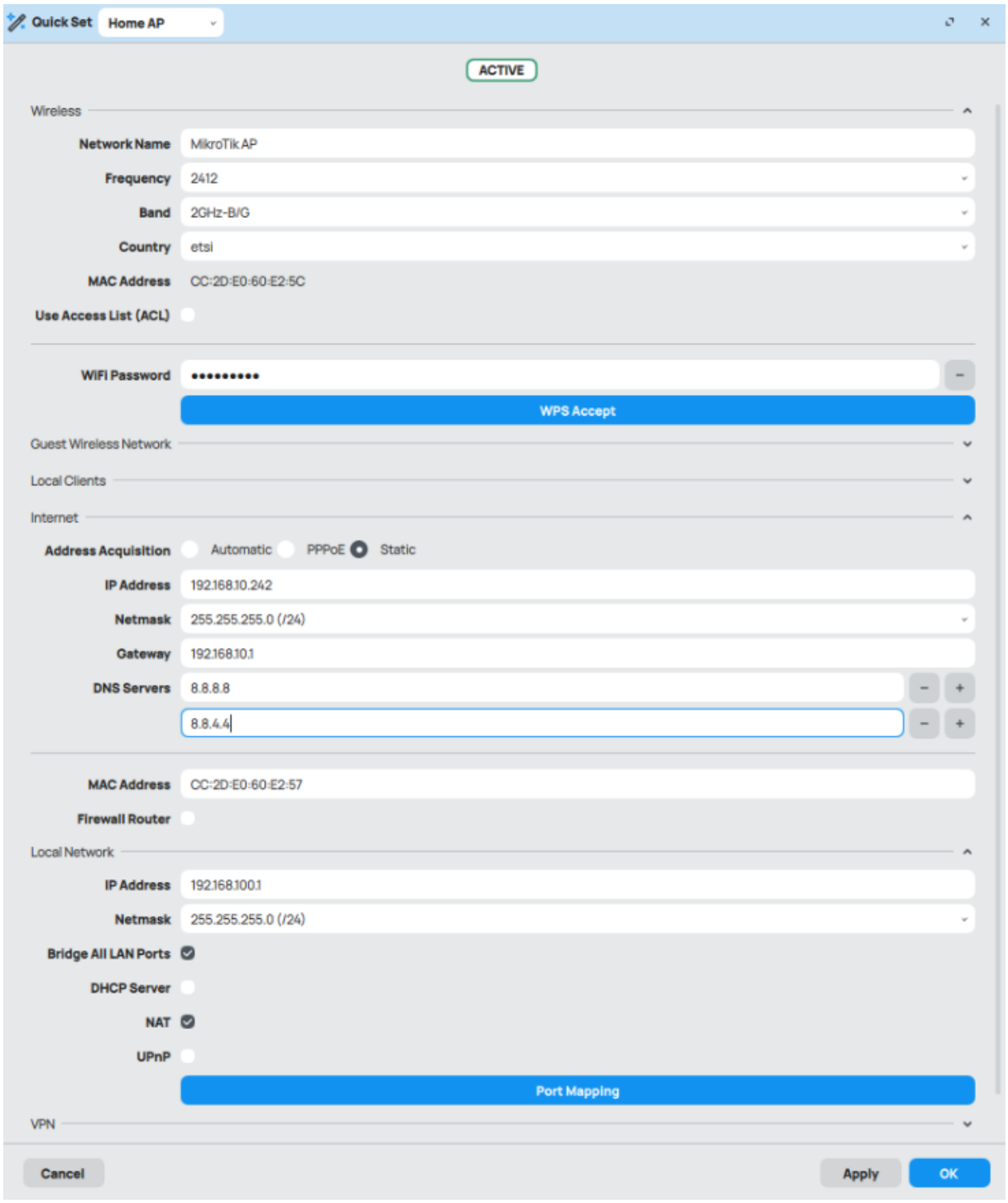


Рис. 4.7. Інтерфейс Швидкі налаштування Wireless та Internet

Тепер ваш бездротовий маршрутизатор MikroTik готовий. Ви можете підключити будь-який пристрій за допомогою кабелю або бездротового зв'язку, пристрій отримає IP-адресу від сервера LAN DHCP і матиме доступ до Інтернету.

Чи варто переходити на Winbox 4?

Без сумнівів, Winbox 4 є важливим кроком вперед для управління мережами MikroTik. Незважаючи на можливі невеликі помилки у новій версії, її функціональність постійно вдосконалюється. Знайомство з Winbox 4 вже зараз допоможе вам адаптуватися до нового інструменту, який стане основним засобом управління RouterOS.

Контрольні запитання

1. Які основні нововведення впроваджені в MikroTik Winbox 4 порівняно з попередніми версіями?
2. Які операційні системи підтримуються для завантаження та встановлення Winbox 4?
3. Які основні кроки для швидкого налаштування MikroTik RouterOS 7 за допомогою Winbox 4?
4. Як можна увімкнути темний режим в MikroTik Winbox 4?

Підсумок

Віртуалізація відіграє ключову роль у сучасних IT-інфраструктурах, забезпечуючи гнучкість і ефективність використання ресурсів. Професія системного адміністратора стала ще більш затребуваною у зв'язку з розвитком віртуалізації, оскільки ці фахівці мають навички, необхідні для управління складними віртуальними середовищами.

VMWare та VirtualBox є одними з найпопулярніших платформ для віртуалізації, пропонуючи широкий спектр функцій для створення та управління віртуальними машинами. Ці інструменти дозволяють компаніям знижувати витрати на обладнання та підвищувати продуктивність за рахунок більш ефективного використання існуючих ресурсів.

Microsoft Azure також грає важливу роль у сфері хмарних обчислень і віртуалізації, надаючи компаніям можливість масштабувати свої ресурси відповідно до потреб. Azure пропонує інструменти для створення, управління та моніторингу віртуальних машин, що дозволяє забезпечити високу доступність і продуктивність послуг.

Адміністрування Windows 10/11 та Windows Server 2016/2019/2022 вимагає детального розуміння специфікацій операційних систем, їх налаштування, оптимізації та захисту. Адміністратори повинні мати знання про мінімальні вимоги до систем і володіти навичками для ефективного розгортання та управління серверними інфраструктурами.

Огляд продуктів MikroTik та їх операційної системи RouterOS показує, що ці продукти пропонують високий рівень надійності, гнучкості та функціональності. MikroTik RouterOS забезпечує всі необхідні функції для створення багатофункціональних мереж, що робить його популярним вибором серед IT-фахівців.

Загалом, знання і навички в області віртуалізації, адміністрування Windows та використання продуктів MikroTik є важливими для сучасних системних адміністраторів. Вони дозволяють забезпечити ефективне управління IT-інфраструктурою та підвищити продуктивність і надійність мереж і систем.

Крім того, сучасні технології віртуалізації продовжують розвиватися, пропонуючи нові можливості для оптимізації роботи IT-

інфраструктури. Використання контейнеризації, зокрема Docker і Kubernetes, стає дедалі популярнішим, дозволяючи адміністраторам ефективніше розгортати та керувати програмними середовищами.

Автоматизація управління IT-інфраструктурою також є важливим аспектом, що значно спрощує адміністрування великих мережевих середовищ. Використання таких інструментів, як Ansible, Puppet та PowerShell, допомагає зменшити витрати часу та людських ресурсів на налаштування й підтримку систем.

Безпека віртуальних середовищ залишається критично важливою, оскільки кібератаки стають дедалі складнішими. Адміністраторам необхідно впроваджувати надійні заходи захисту, такі як багатофакторна автентифікація, шифрування даних та постійний моніторинг трафіку для виявлення загроз.

У майбутньому роль системного адміністратора буде продовжувати змінюватися разом із розвитком технологій. Необхідність у постійному навчанні та освоєнні нових рішень стає ключовою умовою професійного успіху в сфері IT-інфраструктури.

Список використаних джерел

Основна

1. Doug Lowe «Networking For Dummies 12th Edition». 2020. – 480 p.
2. Doug Lowe «Networking For Dummies 8th Edition». 2021. – 1433 p.
3. Oracle VirtualBox: User Guide for Release 7.1 URL: https://www.virtualbox.org/manual/
4. Windows Server 2019 Installation Guide. NEC Corporation. 2019. 65 p.
5. Windows Server® 2019 & PowerShell® All-in-One For Dummies® Published by: John Wiley & Sons, Inc., 111 River Street, Hoboken, New Jersey. 2019. 938 p.
6. Адміністрування комп'ютерних мереж та операційних систем: методичне видання для студентів за спеціальністю 121 «Інженерія програмного забезпечення» факультету інформаційних технологій УжНУ / Розробник: к.т.н., доц. Поліщук В.В. – Ужгород: 2019. – 60 с.
7. Буров Є.В. Комп'ютерні мережі. Підручник. Том перший /Є.В. Буров, М.М. Митник/ Львів: «Магнолія 2006», 2020 – 334 с.
8. Комп'ютерні мережі : навчальний посібник / А. Г. Микитишин, М. М. Митник, П. Д. Стухляк, В. В. Пасічник. – Львів : «Магнолія 2006», 2013. – 256 с.

Допоміжна

1. Смірнов О.А., Конопліцька-Слободенюк О.К., Смірнов С.А., Буравченко К.О., Смірнова Т.В., Поліщук Л.І. Інформаційна безпека в комп'ютерних мережах. Навчальний посібник – Кропивницький: вид. Лисенко В.Ф. 2020. – 294 с. Режим доступу: http://dspace.kntu.kr.ua/jspui/handle/123456789/9799
2. Технології захисту локальних мереж на основі обладнання CISCO: навч. посібник / Т.І. Коробейнікова, С.М. Захарченко. – Львів: Видавництво Львівської політехніки, 2021. – 232 с.
3. Технологія Ethernet: лабораторний практикум / М.О. Білова, С.П. Євсеєв, О.С. Жученко, І.С. Іванченко, О.В. Шматко. – Львів: «Новий Світ – 2000», 2021. – 196 с.

Інформаційні ресурси

1. Академія CISCO. – URL: https://www.netacad.com
2. Інтернет-портал Mikrotik Ukraine URL: https://www.mikrotik.ua/
3. Онлайн емулятор Mikrotik. – URL: https://demo.mt.lv/
4. Онлайн емулятор Mikrotik. – URL: https://demo2.mt.lv/
5. Онлайн ресурс Mikrotik. – URL: https://help.mikrotik.com/docs/
6. Онлайн ресурс Дія.Освіта. – URL: https://osvita.diia.gov.ua/
7. Онлайн ресурс з інформаційних технологій. – URL: https://dou.ua/
8. Онлайн ресурс перегляду відеоуроків. – URL: https://www.youtube.com
9. Онлайн-курси Coursera. – URL: https://www.coursera.org
10. Пошукова система. – URL: https://www.google.com.ua/
11. RouterOS Documentation URL: https://help.mikrotik.com/docs/

КОМП'ЮТЕРНІ НАУКИ

Олександр ХОРУНЖИЙ

АДМІНІСТРУВАННЯ ПРОГРАМНИХ СИСТЕМ І КОМПЛЕКСІВ

Конспект лекцій для здобувачів
освітньо-професійного ступеня
фаховий молодший бакалавр
спеціальності 122 Комп'ютерні науки
денної форми здобуття освіти

DTP Олександр ХОРУНЖИЙ
Редактор Олександр ХОРУНЖИЙ

Підписано до друку «28» січня 2025 р.
Формат 60x84/16. Папір офсетний. Гарнітура Tahoma.

Друк – ВСП «КПЕФК ЛНТУ»
вул. Заводська, 23, м. Ковель, Волинська обл., 45007
kpefk.com.ua, ел. пошта: info@kpefk.com.ua