

Прикладний рівень моделі OSI.
Віддалене адміністрування

AGENDA

- **Поняття віддаленого адміністрування**
- **Telnet**
- **SSH**
- **Remote Desktop (віддалений робочий стіл)**

Поняття віддаленого адміністрування

- Віддалене адміністрування – це технологія, яка дозволяє здійснювати роботу з адміністрування операційної системи на віддаленому комп'ютері.
- Віддалене адміністрування підвищує оперативність вирішення завдань управління мережею та комп'ютерами, що особливо важливо для мереж великих підприємств.
- Більшість програм для віддаленого адміністрування складається з двох частин - серверу і клієнта (його ще називають “вьювер”, або “просмотрщик”). Перший встановлюється на віддаленій машині, тобто, на тій, якій потрібно управляти. Клієнтська частина ставиться на комп'ютері, з якого ви плануєте управляти іншим ПК.

Поняття віддаленого адміністрування

- Для того, щоб клієнт працював, на віддаленому ПК обов'язково повинна бути запущена серверна частина, тому при установці на віддаленому ПК програму краще відразу помістити в "Автозавантаження".
- Окрім цього, якщо на комп'ютерах використовується брандмауер, потрібно обов'язково створити правило, що дозволяє роботу з додатками для віддаленого адміністрування, інакше брандмауер може вирішити, що підключення до ПК - це атака ззовні і не допустити підключення.

Поняття віддаленого адміністрування

- Засіб віддаленого адміністрування може бути підключений до віддалених машин для виконання досить широкого кола задач, але далеко не всіх. Велика кількість проблем пов'язані з обслуговуванням, адмініструванням та управлінням робочими станціями розв'язується тільки при безпосередньому доступі до файлової системи.
- Проте, якщо комп'ютер працює, підключений до мережі, а задача полягає в зміні яких-небудь параметрів системи, або виконанні обслуговуючих операцій, то присутність адміністратора біля робочої станції не обов'язкова.

Поняття віддаленого адміністрування

- Приклади засобів для віддаленого адміністрування:
- - TELNET
- - Remote Desktop (віддалений робочий стіл)
- - SSH
- - Radmin
- - TeamViewer
- - та інші

Telnet

- Засіб віддаленого адміністрування Telnet використовує у своїй роботі протокол прикладного рівня Telnet.
- Протокол Telnet (teletype network) один з найстаріших протоколів, був розроблений в 1969 році, починаючи з RFC 15, розширений у RFC 854 і RFC 855 та інших.
- Історично Telnet забезпечував доступ до інтерфейсу командного рядка на віддаленому хості.

Telnet

- Однак через серйозні загрози безпеці при використанні Telnet через відкриту мережу, таку як Інтернет, його використання з цією метою значно зменшилось на користь SSH.
- При використовуванні Telnet для зв'язку з мережею з Інтернету паролі і імена користувачів передаються у відкритому вигляді. Тому застосовувати цей протокол краще вже усередині локальної мережі, а з Інтернету використовувати даний варіант зв'язку з не рекомендується.
- Через ці проблеми на ОС Windows 10 сервера Telnet немає і для віддаленого адміністрування рекомендується використовувати Remote Desktop.

SSH

- Протокол захищеної оболонки (SSH - Secure Shell Protocol) - це криптографічний мережевий протокол для безпечної роботи мережевих служб через незахищену мережу.
- Типові програми включають віддалений командний рядок, вхід та віддалене виконання команд, але будь-яку мережеву службу можна захистити за допомогою SSH.

SSH

- SSH забезпечує захищений канал через незахищену мережу, використовуючи архітектуру клієнт-сервер, підключаючи клієнтську програму SSH до сервера SSH.
- Специфікація протоколу розрізняє дві основні версії, які називаються SSH-1 та SSH-2. Стандартний порт TCP для SSH - 22. SSH, як правило, використовується для доступу до Unix-подібних операційних систем, але він також може використовуватися в Microsoft Windows. Windows 10 використовує OpenSSH як стандартний клієнт SSH та сервер SSH.

SSH

- У ОС Windows 10 можна встановити OpenSSH Server, запустивши Налаштування Windows, а потім перейшовши до Програми > Необов'язкові компоненти, клацнувши Додати компонент, вибравши OpenSSH Server та натиснувши Встановити.
- Щоб запустити і налаштувати серверний компонент OpenSSH для першого використання, відкрийте PowerShell від імені адміністратора і виконайте наступні команди для запуску SSHD service:

SSH

- Start-Service sshd
- # OPTIONAL but recommended:
- Set-Service -Name sshd -StartupType 'Automatic'
- # Confirm the firewall rule is configured. It should be created automatically by setup.
- Get-NetFirewallRule -Name *ssh*
- # There should be a firewall rule named "OpenSSH-Server-In-TCP", which should be enabled
- # If the firewall does not exist, create one
- New-NetFirewallRule -Name sshd -DisplayName 'OpenSSH Server (sshd)' -Enabled True -Direction Inbound -Protocol TCP -Action Allow -LocalPort 22

SSH

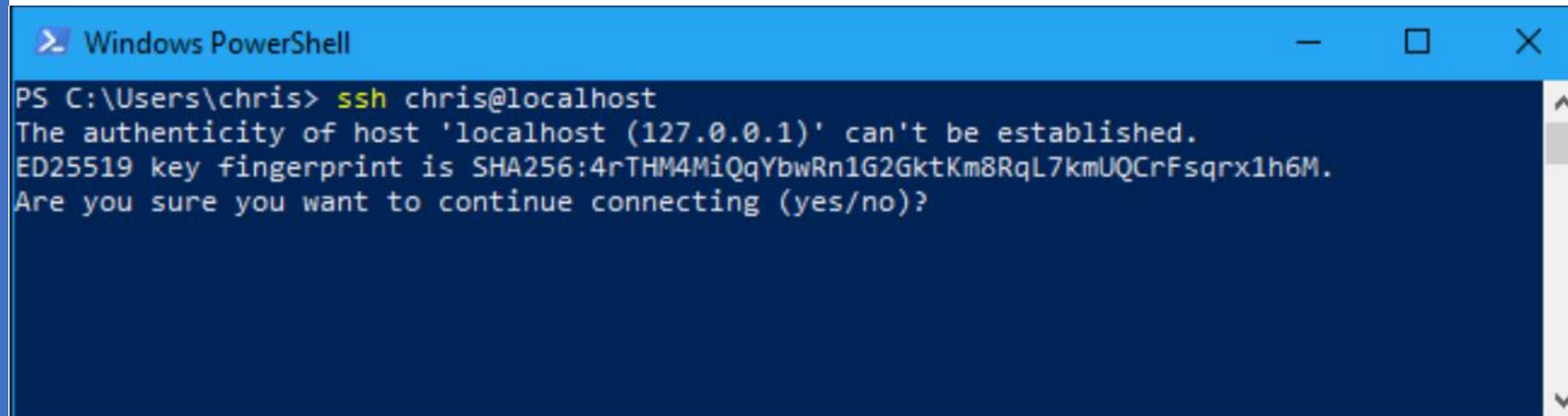
- Як встановити SSH-клієнт Windows 10:
- Клієнт SSH встановлений за замовчуванням в Windows Server 2019 і Windows 10 1809 і новіших версіях.
- Перевірте, що SSH клієнт встановлений у PowerShell від імені адміністратора :
- **Get-WindowsCapability -Online | ? Name -like 'OpenSSH.Client*'**
- Якщо клієнт встановлений, відповідь буде така:
- **Name : OpenSSH.Client~~~~0.0.1.0**
- **State : Installed**

SSH

- Якщо SSH клієнт відсутній (State: Not Present), його можна встановити аналогічно OpenSSH Server.
- SSH клієнт можна використовувати у командному рядку або у PowerShell:
- **C:\Users\Me>ssh**
- **usage: ssh [-46AaCfGgKkMNNqsTtVvXxYy] [-B bind_interface]**
- **[-b bind_address] [-c cipher_spec] [-D [bind_address:]port]**
- **[-E log_file] [-e escape_char] [-F configfile] [-I pkcs11]**
- **[-i identity_file] [-J [user@]host[:port]] [-L address]**
- **[-l login_name] [-m mac_spec] [-O ctl_cmd] [-o option] [-p port]**
- **[-Q query_option] [-R address] [-S ctl_path] [-W host:port]**
- **[-w local_tun[:remote_tun]] destination [command]**

SSH

- Для з'єднання з віддаленим сервером по SSH використовується команда:
- **ssh username@host**
- Як і у випадку з іншими клієнтами SSH, вам буде запропоновано прийняти ключ хосту при першому підключенні. Потім ви отримаєте середовище командного рядка, яке можна використовувати для запуску команд у віддаленій системі:



```
Windows PowerShell
PS C:\Users\chris> ssh chris@localhost
The authenticity of host 'localhost (127.0.0.1)' can't be established.
ED25519 key fingerprint is SHA256:4rTHM4MiQqYbwRn1G2GktKm8RqL7kmUQCrFsqrX1h6M.
Are you sure you want to continue connecting (yes/no)?
```

Задачі, доступні через SSH

- Через SSH можна виконувати всі задачі адміністрування і обслуговування, які доступні через командний рядок.
- Деякі з них:
- Дискові операції – копіювання, створення, переміщення, видалення файлів і каталогів.
- Обслуговування дисків. Наприклад, перевірка на помилки – команда `chkdsk`, дефрагментація дисків (крім дисків SSD) - команда `defrag`. Програма, що викликається цією командою, не має графічного інтерфейсу, всі звіти виводяться в текстовому вигляді на екран, або у файл. Команда може виконуватися у фоновому режимі. Це означає, що користувач продовжуватиме роботу, не підозрюючи, що в цей час проводиться обслуговування його робочого місця. Наприклад, **`defrag C:\ /a`** — виводить звіт про аналіз тому C:\ на необхідність проведення дефрагментації.

Задачі, доступні через SSH

- **Schtasks** - команда дозволяє створити “завдання” подібно тому, як це робиться в планувальнику завдань Windows.
- Мережеві команди: ping, ipconfig, tracert та інші.
- Надання диску чи каталогу у загальне користування по мережі.
Команда:
- net share
- Наприклад, створення мережевого ресурсу:
- **net share ресурс=повне_ім'я_каталогу**
- Видалення мережевого ресурсу:
- **net share ресурс /delete**

Remote Desktop (віддалений робочий стіл)

- Робота інструмента Remote Desktop базується на технології служби терміналів. Вона забезпечує доступ з локального комп'ютера (клієнта Remote Desktop) до робочого столу віддаленого комп'ютера (сервера Remote Desktop).
- Інструмент Remote Desktop являє собою "тонкий клієнт", який працює в якості емуляції терміналу (тобто клавіатури та дисплею). (Емуляція - це відтворення програмними або апаратними засобами роботи інших програм або пристроїв).

Remote Desktop (віддалений робочий стіл)

- Звичайно, Remote Desktop має велику перевагу перед telnet так як, по-перше, має віконний інтерфейс користувача, а по-друге, вся передача інформації між клієнтом і сервером зашифрована.
- Недоліком Remote Desktop можна назвати той факт, що якщо ми працюємо на комп'ютері із звичайною клієнтською версією Windows через "Віддалений робочий стіл", то інший користувач в цей час не може працювати на даному комп'ютері.

Remote Desktop (віддалений робочий стіл)

- Віддалений робочий стіл використовує для зв'язку протокол RDP (Remote Desktop Protocol). Найновіша версія протоколу - Version 10.0
- За замовчуванням сервер RDP прослуховує порт TCP 3389 та порт UDP 3389.
- Віддалений робочий стіл може працювати з наступними атрибутами віддаленого комп'ютера:
 - - файлова система
 - - звук
 - - апаратні порти – під час сеансу зв'язку можна використовувати послідовний, паралельний та USB порти.

Remote Desktop (віддалений робочий стіл)

- - принтер – комп'ютер-клієнт може використовувати принтер сервера
- - remote desktop клієнт і сервер під час сеансу зв'язку використовують спільний буфер обміну

Конфігурація сервера Remote Desktop

- Найпростіший спосіб вирішити доступ до комп'ютера з віддаленого пристрою - використовувати параметри віддаленого робочого столу в розділі "Параметри". Так як ця функціональна можливість була додана в Windows 10 Fall Creators Update (1709), також є окремий завантажуваний додаток для більш ранніх версій Windows.
- На пристрої, до якого ви збираєтеся підключитися, відкрийте меню Пуск і клацніть Налаштування.
- Виберіть групу «Система», а потім пункт «Віддалений робочий стіл».
- Увімкніть віддалений робочий стіл за допомогою повзунка.

Конфігурація сервера Remote Desktop

- Також рекомендується залишити комп'ютер в режимі неспання і видимим, щоб спростити підключення. Клацніть Показати параметри для включення.
- При необхідності додайте користувачів, які можуть віддалено підключитися, клацнувши Select users that can remotely access this PC (Вибрати користувачів, які можуть віддалено підключатися до цього комп'ютера).
- Члени групи "Адміністратори" отримують доступ автоматично.
- Запишіть ім'я цього комп'ютера, вказане в розділі How to connect to this PC (Як підключатися до цього комп'ютера). Воно буде потрібно для налаштування клієнтів

Конфігурація сервера Remote Desktop

- На Windows 7 та більш ранніх версіях установити сервер Remote Desktop можна наступним чином:
- - Відкрити “Панель керування” – “Система і безпека” – “Система” – “Додаткові параметри системи”
- - У вікні “Свойства системи” перейти на вкладку “Віддалений доступ” і у групі “Віддалений робочий стіл” вибрати один із варіантів:
- 1. “Дозволяти підключення від комп’ютерів з будь-якою версією віддаленого робочого столу”
- 2. “Дозволяти підключатися тільки з комп’ютерів, на яких працює віддалений робочий стіл з перевіркою справжності на рівні мережі”

Конфігурація сервера Remote Desktop

- Якщо доступу до віддаленого комп'ютера через Remote Desktop все рівно немає, треба переконатися чи фаєрвол (брандмауер) дозволяє вхідні підключення до Remote Desktop.
- У випадку заборони з боку брандмауера Windows , треба задіяти дозвіл:
- - відкрити брандмауер (наприклад, через Пуск або рядок пошуку), далі перейти за посиланням “Дозволити програмі працювати через брандмауер” – “Змінити параметри” і поставити значки навпроти “Віддалений робочий стіл”

Підключення до сервера Remote Desktop

- На локальному комп'ютері під керуванням Windows 10 В поле пошуку на панелі завдань введіть "Віддалений робочий стіл" і виберіть пункт "Віддалений робочий стіл" . У вікні "Підключення до віддаленого робочого столу" введіть ім'я комп'ютера, до якого потрібно підключитися, а потім натисніть кнопку Підключитися.
- Також для підключення до сервера Remote Desktop можна скористатися командою **mstsc** , яку треба ввести в поле пошуку на панелі завдань.

Керування безпекою і параметрами Remote Desktop

- Керувати безпекою і параметрами Remote Desktop можна як на стороні клієнта, так і на стороні сервера.
- На стороні клієнта всі параметри визначаються у вікні “Підключення до віддаленого робочого столу” – показати параметри.
- Наприклад, на вкладці “Екран” можна вказати розмір у пікселях та глибину кольору в бітах віддаленого робочого столу.
- На вкладці “Локальні ресурси” можна дозволити використання звуку, принтера, буфера обміну та файлової системи локального комп’ютера (тобто копіювання файлів). Для останньої можливості необхідно натиснути кнопку “Подробнее” та відмітити прапорець “Устройства” (для вступу змін у дію можливо прийдеться перезантажити віддалений комп’ютер)