Instalace

- Řešení problému s neviditelným diskem při instalaci Windows

Základní nastavení

- Zobrazení sekund v dolním panelu

Klávesnicové zkratky

- Minimalizace/Maximalizace všech oken
- Skočení na adresní řádek

Chybějící klávesy na klávesnici

- Kontextová klávesa

Příkazový řádek

Batch skript obvykle obsahuje příponu `.bat` nebo `.cmd`.

SQL

▶ Spuštění všech sql skriptů ze složky

PowerShell

- Balíčky
- Změna designu

Historie

- Umístění historie

Oprávnění

- Zjistit oprávnění
- Nastavit oprávnění
- Spustit skript bez změny oprávnění

Práce se soubory

- Změna metadat
- Kopírování

Síť

- Získat název hostitele (webové adresy)
- Získat síťové adaptéry (interfaces)

VPN

VPN (Virtual Private Network) je technologie, která vytváří zabezpečené a šifrované připojení přes méně zabezpečenou síť, jako je internet.

Funguje tak, že internetové připojení vašeho zařízení je směrováno přes soukromý server, nikoli přes poskytovatele internetových služeb (ISP = Internet Service Provider).

Podrobněji jak VPN funguje:

- Šifrování

  Když se připojíte k síti VPN, zašifruje vaše data.

  To znamená, že veškeré informace odesílané přes internet jsou zakódované a nečitelné pro kohokoli, kdo by je mohl zachytit.

- Tunelování:

  Vaše data procházejí zabezpečeným `tunelem` vytvořeným sítí VPN.

  Tento tunel skrývá vaše data před hackery, poskytovateli internetových služeb a dalšími subjekty.

- Maskování IP adresy:

  Server VPN vám přidělí novou IP adresu, která maskuje vaši skutečnou IP adresu.

  To pomáhá chránit vaši identitu a polohu.

- Řízení přístupu:

  VPN vám také může umožnit přístup k obsahu omezenému na určitý region tím, že se bude zdát, že procházíte z jiného místa.

Tip

Příklad použití pro připojení do firemní sítě:

- Zabezpečení dat
  - S VPN:

    Data jsou šifrována, což znamená, že jsou chráněna před neoprávněným přístupem během přenosu. To je důležité zejména při připojení přes veřejné nebo nezabezpečené sítě.

  - Bez VPN:

    Data nejsou šifrována, což zvyšuje riziko jejich zachycení a zneužití třetími stranami, jako jsou hackeři nebo poskytovatelé internetových služeb.
- Přístup k firemním zdrojům
  - S VPN:

    Umožňuje bezpečný vzdálený přístup k interním firemním zdrojům, jako jsou servery, databáze a aplikace, které jsou jinak dostupné pouze z firemní sítě.

  - Bez VPN

    Přístup k těmto zdrojům je omezený nebo nemožný, pokud nejsou vystaveny veřejně, což může omezit produktivitu a schopnost pracovat na dálku.
- Maskování IP adresy:
  - S VPN:

    VPN server přidělí novou IP adresu, což maskuje vaši skutečnou IP adresu a chrání vaši identitu a polohu.

  - Bez VPN

    Vaše skutečná IP adresa je viditelná, což může vést k potenciálním bezpečnostním rizikům a sledování vaší aktivity.
- Tunelování:
  - S VPN

Data procházejí zabezpečeným tunelem, který skrývá vaši komunikaci před poskytovateli internetových služeb a dalšími subjekty.

- Bez VPN:

  Data procházejí přímo přes internet bez dodatečné ochrany, což zvyšuje riziko jejich zachycení a analýzy.