

12. UNIX

- Charakteristika systému
 - Srovnání s MS Windows
 - Adresářová struktura
- Uživatelský a programátorský interface
 - Základní příkazy
 - Roury
 - Tvorba skriptů
 - Systémové proměnné
 - Vrstvy
- Použití a popis služeb
 - Telnet
 - SSH
 - FTP
 - DNS
 - DHCP
- Virtualizace unixového prostředí na MS Windows

Charakteristika Systému

UNIX je v informatice ochranná známka operačního systému vytvořeného v Bellových laboratořích americké firmy AT&T v roce 1969. Většina současných operačních systémů je unixovými systémy různou měrou inspirována.

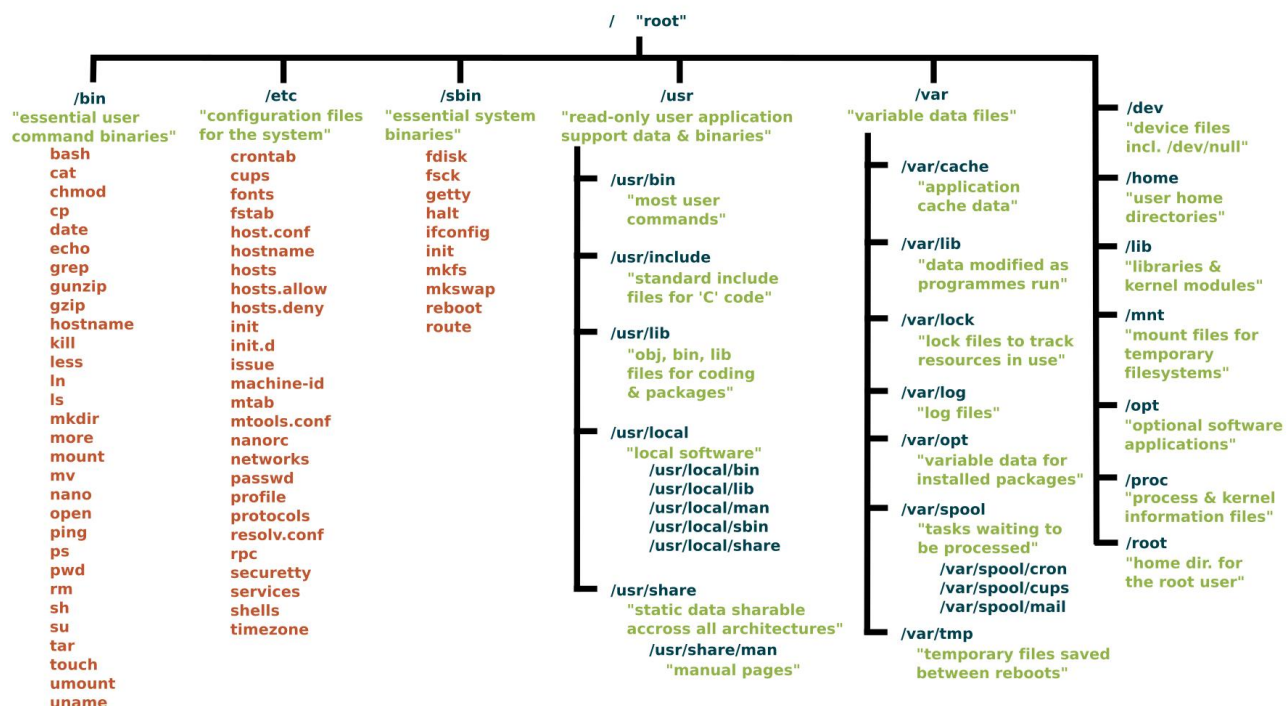
Existují různé systémy, které jsou s UNIXem v různé míře kompatibilní, ale nemohou nebo nechtějí platit licenční poplatky, a proto často používají varianty názvů, které na název UNIX odkazují (například XENIX, MINIX, Linux), ale mohou se jmenovat i jinak (například BSD varianty OpenBSD, NetBSD, ale též macOS atd.). Souhrnně je označujeme jako unixové systémy (unix-like).

- Napsán v jazyce C
- Má hierarchický souborový systém-strom adresářů s jedním kořenovým adresářem (cd /)
- Je založen na příkazech
 - Všechny příkazy malým písmenem (je case sensitive)
 - Některé příkazy mohou používat přepínače (ls -l)
- Podporuje multitasking, více uživatelů může pracovat současně
- Bez uživatelského účtu a hesla se nejde dostat do systému
- Hlavní úlohou je efektivně řídit přidělování paměti, procesoru, prostoru na disku, řídit obsluhu terminálů a všech zařízení připojených k PC
- Nabízí několik rozhraní
 - Terminál
 - GUI - KDE, GNOME nebo XFCE
- Každé fyzické zařízení, od interaktivních terminálů až po hlavní paměť je považováno za soubor, který je možno v podobě jako obyčejný soubor číst, nebo do něj zapisovat (všechno je soubor)
- Součástí je kompilátor jazyka c a řada programátorských nástrojů, jako debugger nebo profiler

Srovnání s MS Windows

- Linux je open source OS, takže uživatel může upravovat zdrojový kód podle požadavků, zatímco Windows je komerční OS, takže uživatel nemá přístup ke zdrojovému kódu
- Linux je méně náročný na HW
- Linux je velmi dobře zabezpečený, jelikož je snadné odhalit chyby a opravit díky open source zdrojovému kódu. Na druhou stranu Windows má mnohem víc uživatelů, což z něj dělá pro hackery lákavější cíl
- Soubory v linuxu jsou uspořádány do jednoho kořenového adresáře (např. připojený souborový systém najdeme v /mnt), zatímco ve Windows jsou soubory ukládány do složek na různých datových jednotkách (C:, D:, E:, F:, ...)
- V Linuxu najdete systémové a programové soubory v různých adresářích, zatímco ve Windows se obvykle nachází na jednotce C:

Adresářová struktura



- **/dev**
 - Všechny zařízení zde přístupné jako soubor, např disk `/dev/sda`
- **/lib**
 - Knihovny
 - Obrazovka napojena na STDOUT
 - Klávesnice napojena na STDIN
 - Chyby jsou napojena na STDERR
- **/usr**
 - Obsahuje uživatelské aplikace, knihovny a dokumentaci. Podadresáře jako `/usr/bin` nebo `/usr/lib` jsou domovem většiny uživatelských programů a knihoven.
- **/etc**
 - Obsahuje systémové konfigurační soubory a skripty. Najdete zde nastavení síťových rozhraní, uživatelských účtů, služeb a další.
 - DNS se nachází v `/etc/hosts`
- **/var**
 - Obsahuje proměnlivá data, která se často mění za běhu systému. Patří sem logy (`/var/log`), spool soubory pro tiskové služby, e-mail, cache a databáze.
- **/bin**
 - Obsahuje základní spustitelné soubory dostupné pro všechny uživatele, které jsou nezbytné pro chod systému. Najdete zde příkazy jako `ls`, `cp`, `mv` a další.
- **/sbin**
 - Obsahuje systémové binární soubory určené pro administraci systému, které vyžadují vyšší oprávnění. Příklady zahrnují `fdisk`, `ifconfig`, `iptables`.
- **/home**
 - Obsahuje domovské adresáře pro jednotlivé uživatele. Každý uživatel má svůj vlastní adresář, ve kterém ukládá své soubory.
- **/mnt**
 - Slouží k dočasnému připojování souborových systémů, často pro administrativní účely nebo ruční připojování.
- **/boot** - kernel image

Uživatelský a programátorský interface

- Shell - proces, který zprostředkovává provedení jiných programů

Základní příkazy

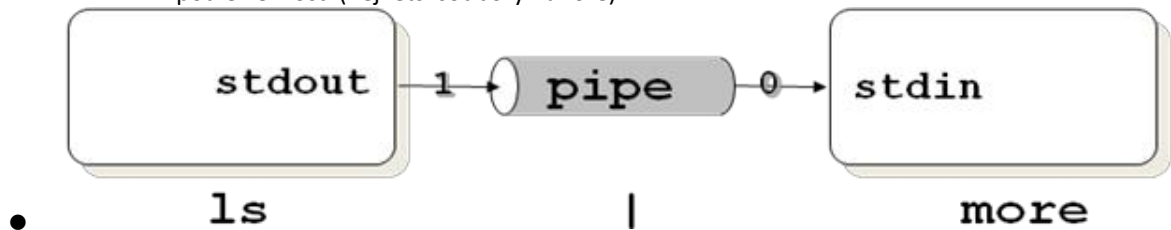
- Who - zjistí, kteří uživatelé jsou přihlášení do systému
- Whoami - vypíše informace o sobě (o svém loginu, skupině)
- Date - zobrazí systémové datum a čas
- Man - manuál
- Chmod - změna atributů
 - Change mode
 - Symbolický zápis (rwx)
 - ◆ Každá položka může mít práva pro:
 - u (user) – vlastník souboru
 - g (group) – skupina
 - o (others) – ostatní
 - a (all) – všichni
 - ◆ `chmod u+rwx,g+rx,o+r soubor.txt`
 - Číselný (oktální) zápis
 - ◆ Každé oprávnění má svou číselnou hodnotu:
 - r (read) = 4
 - w (write) = 2
 - x (execute) = 1
 - ◆ Práva se sčítají do tří číslic (uživatel, skupina, ostatní).
 - ◆ `chmod 755 soubor.txt`
- Chown - změna vlastníka (change owner)
 - `chown user soubor.txt` # Změní vlastníka na "user"
 - `chown user:group soubor.txt` # Změní vlastníka na "user" a skupinu na "group"
 - `chown :group soubor.txt` # Změní pouze skupinu na "group"
 - `chown -R user:group adresar` # Rekursivně změní vlastníka všech souborů v adresáři
- Logout / Ctrl+d - logout
- Ctrl+s - pozastaví výpis
- Ctrl+q - uvolnění výpisu
- Ctrl+c - ukončí program
- Cd (change directory) - změni aktuální adresář
 - Cd / nebo cd /- kořenový adr.
 - Cd .. - přesune uživatele do nadřazeného adresáře
 - Cd ~ - domovský adresář
- Pwd - print working directory - napíše cestu aktuálního adresáře
- Ls - vypíše obsah aktuálního adresáře
 - -a - vypíše skryté soubory
 - -l poskytne podrobný výpis (práva, velikost, ...)
- Mkdir - vytvoří nový adresář
- Rmdir - odstraní adresář
 - -r odstraní celý adresář včetně podstromů
- Touch - vytvoří soubor bez zápisu
- Cat >souborek.txt - vytvoří soubor s možností zápisu
- Cat -zabrazí obsah souboru
- Cp - kopíruje soubory
- Rm odstraní soubor/adresář

- Mv - přejmenuje nebo přesune soubor do jiného adresáře
- Du
 - Zobrazí využití diskového prostoru adresáře.
- Df
 - Zobrazí informace o využití disku.
- Find
 - Vyhledává soubory podle různých kritérií. Například `find . -name "soubor.txt"` vyhledá soubor s názvem "soubor.txt" v aktuálním adresáři a jeho podadresářích.
- Grep
 - Vyhledává text v souborech. Například `grep "slovo" soubor.txt` vyhledá slovo "slovo" v souboru "soubor.txt".
- head
 - Zobrazí prvních několik řádků souboru. Například `head -n 10 soubor.txt` zobrazí prvních 10 řádků souboru.
- Tail
 - Zobrazí posledních několik řádků souboru. Například `tail -f soubor.txt` bude neustále zobrazovat nové řádky, jakmile se v souboru objeví (užitečné pro sledování logů).
- less
 - Umožňuje interaktivní prohlížení souboru po stránkách.
- Ping
 - Otestuje dostupnost vzdáleného serveru. Například `ping google.com` otestuje, zda je server google.com dostupný.
- Ifconfig
 - Zobrazí informace o síťových rozhraních.
- Netstat
 - Zobrazí informace o síťových spojeních.
- Ssh
 - Umožňuje vzdálené přihlášení k jinému počítači.
- Man
 - Zobrazí manuálovou stránku k příkazu. Například `man ls` zobrazí manuálovou stránku k příkazu ls.
- Apropos
 - Vyhledá příkazy podle klíčového slova.
- Whatis
 - Zobrazí stručný popis příkazu.
- Alias
 - Vytvoří alias pro příkaz. Například `alias l="ls -l"` vytvoří alias l pro příkaz ls -l.
- History
 - Zobrazí historii zadaných příkazů.
- Date
 - Zobrazí aktuální datum a čas.
- Cal
 - Zobrazí kalendář.
- Echo
 - Vypíše text na obrazovku.

Roury-pipe

- Systémová vyprpvnávací paměť, do které jeden proces ukládá a další z odebírá
- Slouží pro spojování příkazů, kde se výstup z prvního příkazu zapisuje do pipy, ze které se výsledky čtou druhým příkazem na standartní výstup
 - Takové příkazy se nazývají kolona
- Příklady
 - `sort soubor.txt | uniq`

- ◆ Tento příkaz seřadí řádky v souboru "soubor.txt" pomocí příkazu sort a poté pomocí roury (|) přeměruje výstup do příkazu uniq, který odstraní duplicitní řádky.
- `ls -l | wc -l`
 - ◆ Tento příkaz vypíše všechny soubory v aktuálním adresáři pomocí příkazu ls -l (dlouhý formát výpisu) a poté pomocí roury (|) přeměruje výstup do příkazu wc -l, který spočítá počet řádků (tj. počet souborů).
- `du -h | sort -hr`
 - ◆ Tento příkaz zobrazí využití diskového prostoru pro každý adresář a soubor v aktuálním adresáři pomocí příkazu du -h (human-readable formát). Výstup tohoto příkazu je pak přeměrován pomocí roury (|) do příkazu sort -hr, který seřadí výstup podle velikosti (největší soubory nahoře).



Tvorba skriptů

- Textový spustitelný soubor, který potřebuje pro své spuštění shell
- Soubory se skripty mají přípony .sh nebo jsou bez přípony
- Každý skript je psán pro určitý shell nebo programovací jazyk (např. bash) a v jiném nemusí fungovat
 - Z toho důvodu na prvním řádku je identifikace shellu
 - `#!/bin/bash`
 - ◆ Určuje, který bash se použije (cesta k němu)
- Aby bylo možné spouštět skript v textovém režimu po napsání jeho názvu, musí mít nastaveno přístupové právo pro spuštění (x-execute)
- Pokud to neuděláme, můžeme skript spustit jako parametr interpretačního programu (bash skript.sh) ale i přes to je vhodné jej označit jako spustitelný.
- Pomocí příkazu `cat /etc/shells` zobrazíme všechny dostupné shell

```
#!/bin/bash
```

```
# Získání aktuálního data a času
```

```
datum_cas=$(date +"%Y-%m-%d %H:%M:%S")
```

```
# Název souboru, do kterého se bude zapisovat
```

```
soubor="casovy_zaznam.txt"
```

```
# Zápis data a času do souboru
```

```
echo "Aktuální datum a čas: $datum_cas" >> $soubor
```

```
# Výpis potvrzení
```

```
echo "Datum a čas byl zapsán do souboru $soubor."
```

```
#!/bin/bash
```

```
# Zeptá se uživatele na jméno
```

```
read -p "Zadej své jméno: " jmeno
```

```
# Pozdraví uživatele
```

```
echo "Ahoj, $jmeno!"
```

```
echo "Text ";
```

výpis textu

```
echo -n "Zadejte nazev souboru: ";
```

výpis textu a zadání hodnoty
v jednom řádku

```
read nazev
```

načtení hodnoty

```
echo "Vypis souboru: $nazev";
```

výpis obsahu proměnné

```
echo -e "\nVyberte jednu z moznosti: ";
```

výpis textu s odřádkováním

```
read -p "Zadejte hodnotu: " cislo
```

načtení hodnoty v jednom
řádku (lze načítat i více
hodnot)

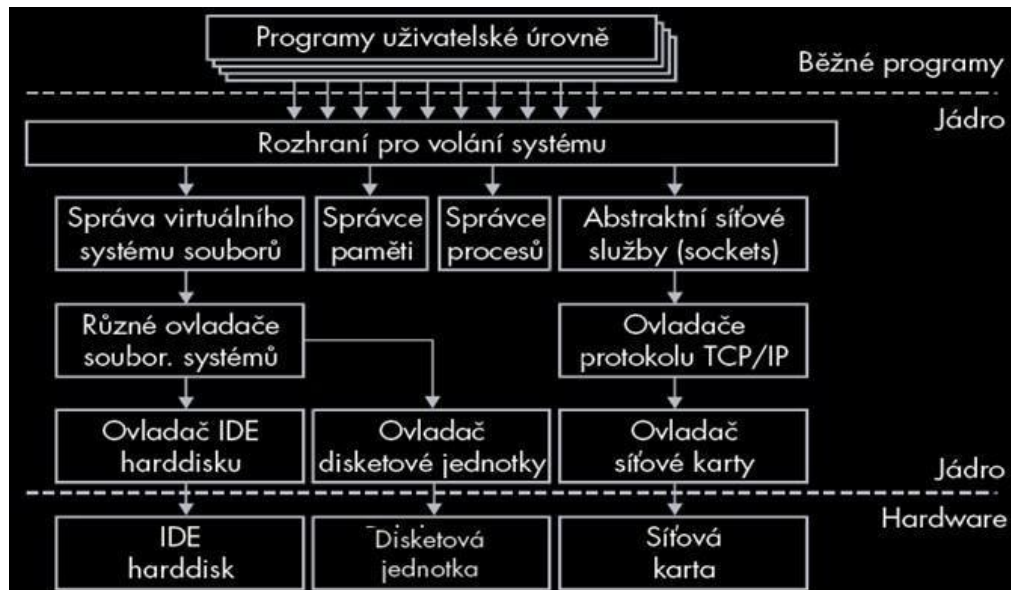
```
read -sp "Zadejte hodnotu: " heslo
```

skryté načtení hodnoty
v jednom řádku (lze načítat i
více hodnot)

Systémové proměnné

- Jedná se o parametry skriptu, které jsou přístupné přes systémové proměnné
 - \$0 - vypíše název skriptu
 - \$01 - \$09 - vypíše daný parametr skriptu nebo shellu
- Existují i proměnné předdefinované shellem. Tyto proměnné jsou využívány jak shellem, tak uživatelem, který může měnit jejich hodnotu
 - \$home - domovský adresář, při zadání příkazu cd bez parametru se použije obsah této proměnné jako cílový adresář
 - \$path - zobrazí seznam adresářů, ve kterých hledá shell spustitelné soubory v případě, že uživatel nezadá cestu k souboru
 - \$shell - cesta k interpreteru terminálu-shellu
 - \$pwd - absolutní cesta k pracovnímu adresáři
 - \$user - jméno účtu uživatele

Vrstvy



- Nejnižší - jádro(kernel)
 - Řídí komunikaci a přístup k HW
 - Spravuje procesy a zajišťuje komunikaci mezi HW a SW
 - Unix používá monolitické jádro, v 80 letech nastal odklon směrem k mikrojádru, kde obsluha souborového systému, počítačových sítí, asynchronních událostí generovaných myší a další byla přesunuta mimo jádro OS
- Systémové nástroje(utility)
 - Slouží pro správu souborového systému, operačního systému(jeho oprávněných uživatelů a jejich práv, nastavení vlastností apod.)

Správa uživatelů

- Useradd = vytvoří nového uživatele
- Userdel = vymaže uživatele a soubory
- Usermod = modifikuje uživatelský účet
- Groupadd = vytvoří novou skupinu
- Groupdel
- Groupmod
- Příklad

```
Groupadd studenti
useradd st1 -g studenti
chmod g+rx st1
Passwd st1
st1 /nastaveni hesla
st1 /potvrzeni hesla
```


Popis a použití služeb

Telnet

- TELEcommunication NETwork je síťová služba a protokol používaný k vzdálenému přístupu na jiný počítač přes síť.
- Hlavní vlastnosti
 - Opužívá TCP port 23
 - Poskytuje textový přístup k vzdálenému systému
 - Je nešifrovaný, přihlašovací údaje, příkazy a data jsou přenášeny v podobě otevřeného textu
- Používal se hlavně k administraci síťových zařízení
- Dnes kvůli bezpečnostním rizikům nahrazen SSH, který přenos šifruje

SSH

- Secure shell
- Je síťový protokol, který umožňuje šifrovaný vzdálený přístup
- Používá se hlavně ke vzdálené administraci serverů a a síťových zařízení
- Narozdíl od telnetu šifruje přenos dat
 - Odolný proti útokům typu "man-in-the-middle"
- Hlavní vlastnosti
 - Používá port 22(lze změnit)
 - Šifrovaná komunikace
 - Ověřování pomocí hesla nebo ssh klíčů
 - Podpora tunelování, přesměrovávání portů a přenosu souborů
 - ◆ Tunelování(port forwarding)
 - ◆ Data jsou obalena v jiném protokolu a bezpečně přenesena na cílovou adresu
 - Podporuje více šifrovacích algoritmů(AES, RSA, ECDSA, ...)
- Scp-secure copy protokol
- Ssh user@server
- Ssh ipadress

FTP

- File Transfer Protokol
- Síťový protokol určený k přenosu souborů mezi klientem a serverem
- Používá se ke stahování i nahrávání na vzdálený server
 - Např správa webových stránek nebo záloha dat
- Hlavní vlastnosti
 - Používá protokol TCP/IP
 - Používá TCP porty 20 a 21
 - 20 - Datové spojení(přenos souborů pokud je aktivní)
 - 21 - řídící spojení (příkazy a autentizace)
 - Nešifrovaný přenos-otevřený text
 - Podporuje anonymní přihlášení
 - ◆ Některé servery podporují přístup bez registrace
- Varianty
 - FTPS (FTP Secure) – FTP + šifrování SSL/TLS

- SFTP (SSH File Transfer Protocol) – Přenos souborů přes SSH (šifrované)

DNS

- Domain Name system
- Systém doménových jmen, který je realizován servery DNS a protokolem stejného jména, kterým si vyměňují informace
- Jeho hlavním úkolem a příčinou vzniku je překlad doménových jmen na IP adresy uzlů sítě
- Dnes složí jako distribuovaná databáze síťových informací
- Servery DNS jsou organizovány hierarchicky, stejně jako jsou hierarchicky tvořeny názvy domén
- Jména domén umožňují lepší orientaci lidem, adresy jsou pro stroje přeloženy na adresy 32 bit (IPv4) nebo 128 bit (IPv6)

DHCP

- Dynamic Host Configuration Protocol
- Protokoly z rodiny TCP/IP, který se používá pro automatické přidělení IP adres počítačům přidělených do sítě
- DHCP server přiděluje počítačům pomocí DHCP protokolu zejména IP adresu, masku sítě, výchozí bránu a adresu DNS serveru
- Platnost přidělených údajů je omezená, proto na PC běží klient, který jejich platnost prodlužuje

Virtualizace Unixu na MS Windows

- Virtualizace PC je metoda, která umožňuje spuštění libovolného OS na již zapnutém PC
- Pro použití virtualizace je nutné mít základní desku, která virtualizaci podporuje (v dnešní době téměř všechny)
- Další podmínkou je zapnout v BIOS nebo SETUP nastavení Virtual VM
- Důležitou součástí PC by měla být dostatečně velká operační paměť, alespoň 2GB
- Software pro virtualizaci
 - VirtualBox - freeware
 - Microsoft Virtual PC - freeware
 - VMware workstation
 - Parallels Workstation

Konfigurace služeb

`/var/etc/rc.d/init.d` = rozjíždí skripty pro konfiguraci
`/var/etc` = konfigurační soubory

`Chkconf`

- `--list`
- `--add`
- `--del`

`Chkconf --list | more`

Apropos = nápověda

Daemon

- Spuštěný program
- Odstřihne se od klávesnice
- Něco dělá, nastavuje, ale není vidět
- Internetový daemon = XINETD

Konfigurace FTP

- `/var/etc/vsftp/vsftp.conf`
- `/var/etc/rc.d/init.d/vsftpd reload, start, stop`