

Linux a administrace serverů

Linux je open-source jádro (kernel), na kterém jsou postaveny celé operační systémy zvané **distribuce**. V serverovém světě Linux dominuje díky své efektivitě, bezpečnosti a možnosti plné kontroly nad systémem bez nutnosti grafického rozhraní (GUI).

1. Architektura a distribuce

Linuxový systém se skládá z jádra, které komunikuje s hardwarem, a uživatelského prostoru, kde běží aplikace.

Populární serverové distribuce:

- **Debian / Ubuntu Server:** Velmi oblíbené pro svou stabilitu a obrovskou komunitu. Používají balíčkovací systém apt.
- **RHEL (Red Hat Enterprise Linux) / Rocky Linux:** Standard v korporátním prostředí s dlouhou podporou. Používají dnf/yum.
- **Alpine Linux:** Extrémně lehká distribuce, ideální pro [Docker kontejnery](#).

2. Příkazová řádka (CLI) a Shell

Administrace Linuxu probíhá primárně přes **Shell** (nejčastěji **Bash** nebo **Zsh**). Pro vzdálený přístup se používá protokol **SSH** (Secure Shell).

Základní příkazy pro administrátora:

Příkaz	Význam
sudo	Spuštění příkazu s právy superuživatele (root).
ls, cd, pwd	Práce s adresářovou strukturou.
top / htop	Monitorování procesů a vytížení CPU/RAM.
systemctl	Správa systémových služeb (start, stop, restart).
tail -f /var/log/...	Sledování systémových logů v reálném čase.
chmod / chown	Změna oprávnění a vlastníka souborů.

3. Souborový systém a oprávnění

V Linuxu platí pravidlo: „**Všechno je soubor**“ (včetně pevných disků nebo síťových karet).

Adresářová struktura je hierarchická a začíná kořenem /.

Standardní oprávnění (Unix permissions):

Každý soubor má definovaná práva pro **Vlastníka**, **Skupinu** a **Ostatní**.

- **R** (Read) – čtení
- **W** (Write) – zápis
- **X** (Execute) – spuštění
- ***Příklad:** 755 znamená plná práva pro vlastníka a čtení/spouštění pro ostatní.

—

4. Síťová administrace na Linuxu

Linuxový server často slouží jako brána nebo firewall.

- **IP Adresace:** Nastavení pomocí nástroje `ip addr`.
- **Firewall:** Správa pomocí **iptables** nebo modernějšího **nftables** (často přes nadstavby jako `ufw` nebo `firewalld`).
- **Diagnostika:** Nástroje jako `ping`, `traceroute`, `netstat` nebo `ss` pro kontrolu otevřených portů.

—

5. Automatizace a Infrastructure as Code (IaC)

Moderní administrátor nespravuje servery ručně jeden po druhém, ale používá nástroje pro automatizaci:

- **Shell Scripting:** Psaní skriptů pro opakující se úlohy.
- **Ansible:** Nástroj pro hromadnou konfiguraci tisíců serverů pomocí jednoduchých YAML souborů.
- **Cron:** Plánovač úloh pro spuštění skriptů v určité časy.

—

6. Bezpečnost serveru

Základní kroky pro zabezpečení nového serveru (Hardening):

1. ****Zákaz přihlášení uživatele root**** přes SSH.
2. ****Používání SSH klíčů**** namísto hesel.
3. ****Nastavení Firewallu**** (povolit jen nutné porty).
4. ****Fail2Ban:**** Automatické blokování IP adres, které se pokoušejí o útok hrubou silou (Brute-force).

Související články:

- [Síťové protokoly a vrstvy](#)
- [Kybernetické hrozby a prevence](#)
- [Virtualizace a Hypervizory](#)

Tagy: linux sysadmin server bash ssh automation security

From:

<https://www.serviceit.cz/> - **IT ENCYKLOPEDIE**

Permanent link:

<https://www.serviceit.cz/doku.php?id=it:net:linux>

Last update: **2026/01/02 13:45**

