NixOS: Imutabilita a perzistence dat (Concept Impermanence)

V článku NixOS jako imutabilní systém jsme si ukázali, že základní systémové komponenty a aplikace jsou v NixOS uloženy v read-only úložišti `/nix/store`. Pokročilí uživatelé NixOS však tento koncept posouvají ještě dál – do stavu, kdy je **celý kořenový souborový systém (/) považován za dočasný** a při každém restartu počítače se kompletně vymaže.

Tento přístup se v komunitě označuje jako **Impermanence** (pomíjivost) nebo podle známého motta *„Erase Your Darlings“* (Vymaž své miláčky). Přináší absolutní kontrolu nad tím, jaká data v systému dlouhodobě zůstávají a která jsou perzistentní (trvalá).

Proč mazat systém při každém restartu?

V běžném operačním systému se postupem času hromadí „datový odpad“ – dočasné soubory, cache, logy aplikací, které jste jednou spustili a odinstalovali, nebo zapomenuté konfigurační soubory v `/var` a `/etc`. Systém trpí tzv. softwarovým stárnutím.

Pokud je kořenový adresář `/` při každém bootu smazán a obnoven z prázdného snapshotu:

- Máte jistotu, že v systému neběží žádný škodlivý kód (malware), který by se pokusil skrýt v systémových složkách – restart ho zlikviduje.
- Systém je po deseti letech provozu v naprosto stejně čistém stavu jako první den po instalaci.
- Pokud nějaká aplikace vyžaduje trvalé ukládání dat, musíte ji v konfiguraci explicitně definovat. Nic se neděje „za vašimi zády“.

Architektura imutabilního disku

Abychom nepřišli o osobní dokumenty, zdrojové kódy nebo databáze, musíme disk rozdělit na specifické podsvazky (subvolumes) pomocí souborových systémů jako Btrfs nebo ZFS (viz Srovnání Btrfs a ZFS).

Typické rozdělení disků vypadá takto:

- **`/` (root) – Ephemerální (dočasný):** Namontován ze subvolumů Btrfs/ZFS, který se při každém bootu promaže.
- **`/nix` – Perzistentní:** Zde sídlí `/nix/store`. Obsahuje všechny aplikace a konfigurace. Nemusí se mazat, protože Nix sám ví, co má vyčistit pomocí Garbage Collection.
- **`/persistent` – Perzistentní:** Speciální bezpečné místo na disku, kam se ukládají data, o která nechceme přijít. Sem se fyzicky mapují soubory z domovských adresářů a systémových databází.

Jak se čistí kořenový adresář?

Promazání kořenového adresáře probíhá v rané fázi startu systému (**initrd**) ještě předtím, než se namontují samotné souborové systémy.

Příklad skriptu v jazyce Nix pro souborový systém Btrfs:

```
boot.initrd.postDeviceCommands = lib.mkAfter ''
  mkdir /btrfs_tmp
  mount /dev/disk/by-uuid/VAŠE-UUID-DISKU /btrfs_tmp
  if [ -e /btrfs_tmp/root ]; then
      btrfs subvolume delete /btrfs_tmp/root
  fi
  btrfs subvolume snapshot /btrfs_tmp/root-blank /btrfs_tmp/root
  umount /btrfs_tmp
'';
```

Tento skript při každém startu smaže subvolume `root` a vytvoří jeho čistou kopii ze záložního prázdného snímku `root-blank`.

Řešení perzistence: Komunitní modul Impermanence

Abyste nemuseli ručně psát složité symbolické odkazy pro každý soubor, který chcete zachovat, vyvinula komunita NixOS modul s názvem **Impermanence**. Tento modul využívá technologii **bind mounting** (připojení adresáře do jiného adresáře) na úrovni jádra.

V konfiguraci systému pak stačí jednoduše deklarovat, které soubory a složky mají „přežít“ restart tím, že se propojí do perzistentního úložiště:

```
{ inputs, ... }: {
  imports = [
    inputs.impermanence.nixosModules.impermanence
  ];

  # Globální systémová perzistence
  environment.persistence."/persistent" = {
    hideMounts = true;
    directories = [
      "/var/log"
      "/var/lib/bluetooth"
      "/var/lib/nixos"
      "/var/lib/systemd/coredump"
      "/etc/NetworkManager/system-connections"
    ];
    files = [
      "/etc/machine-id"
      "/etc/ssh/ssh_host_rsa_key"
      "/etc/ssh/ssh_host_ed25519_key"
```

```
    ];
  };
}
```

Perzistence uživatelských dat (Home Manager)

Stejný přístup lze aplikovat i na domovský adresář uživatele prostřednictvím nástroje **Home Manager**:

```
home.persistence."/persistent/home/anna" = {
  directories = [
    "Downloads"
    "Documents"
    "Projects"
    ".config/PulseEffects"
    ".mozilla/firefox" # Zachování profilu prohlížeče
    ".local/share/Steam" # Zachování her ze Steamu
  ];
  allowOther = true;
};
```

Výzvy a na co si dát pozor

Provozování systému v tomto režimu je fascinující, ale přináší určité komplikace:

- **SSH klíče hostitele:** Pokud zapomenete perzistovat SSH klíče serveru (`/etc/ssh/ssh_host_*`), při každém restartu se vygenerují nové. Klienti se k serveru odmítnou připojit s varováním před útokem Man-in-the-Middle.
- **Machine ID:** Soubor `/etc/machine-id` je unikátní pro každou instalaci. Pokud není perzistentní, systém ho generuje znovu, což může mást logovací nástroje (journald) nebo DHCP servery v síti.
- **Aplikace třetích stran:** Některé špatně navržené aplikace ukládají důležitá data do složek jako `/tmp` nebo `/var/tmp`. V imutabilním systému tato data po restartu zmizí, což může vést k neočekávanému chování.

Související články:

- NixOS jako imutabilní systém a principy /nix/store
- Srovnání souborových systémů: Btrfs, ZFS a role v imutabilitě
- Infrastruktura jako kód (IaC) a deklarativní správa

Tagy: linux nixos immutability impermanence btrfs zfs persistence devops