Chroot (Change Root)

Chroot je jedním z nejstarších mechanismů pro izolaci procesů v systémech Unix (představen již v roce 1979). Umožňuje spustit program tak, aby si „myslel“, že vybraný adresář je kořenem celého systému (/).

Pokud například zavřete aplikaci do adresáře `/home/uzivatel/jail`, bude pro ni soubor `/etc/passwd` ve skutečnosti souborem `/home/uzivatel/jail/etc/passwd`.

Hlavní využití Chrootu

1. Izolace rizikových služeb (Sandboxing)

Pokud provozujete veřejnou službu (např. webový server nebo DNS), můžete ji „zavřít“ do chrootu. Pokud by útočník tuto službu ovládl, zůstane uvězněn v daném adresáři a nedostane se k citlivým systémovým souborům.

2. Oprava systému (Rescue Mode)

Chroot je nepostradatelný při opravě nefunkčního Linuxu. Nabootujete z USB, připojíte disk s poškozeným systémem a pomocí `chroot` se do něj „přepnete“. Poté můžete opravit zavaděč (GRUB), změnit zapomenuté heslo nebo přeinstalovat balíčky, jako byste v daném systému přímo byli.

3. Testování a vývoj

Umožňuje vytvořit testovací prostředí (např. jinou distribuci Linuxu) uvnitř vašeho stávajícího systému bez nutnosti virtualizace.

Jak se chroot vytváří?

Aby program v chrootu fungoval, musí mít uvnitř „vězení“ vše, co potřebuje k běhu:

- **Binární soubory:** Samotný program (např. `/bin/bash`).
- **Knihovny:** Sdílené knihovny (např. v `/lib` a `/usr/lib`), bez kterých se program nespustí.
- **Zařízení:** Speciální soubory jako `/dev/null` nebo `/dev/random`.

Omezení a bezpečnost

Je důležité pochopit, že **chroot není plnohodnotný bezpečnostní kontejner**.

- **Útěk z vězení (Chroot Escape):** Uživatel s právy **root** může z chrootu poměrně snadno uniknout (například pomocí dvojitého volání chroot nebo připojením externích zařízení).
- **Sdílené jádro:** Proces v chrootu stále sdílí stejné jádro operačního systému, síťové rozhraní a další prostředky s hostitelem.

Technologie	Úroveň izolace	Hlavní rozdíl
Chroot	Nízká	Izoluje pouze souborový systém.
Docker / Kontejnery	Střední	Využívá „Namespaces“ k izolaci sítě, procesů a uživatelů.
Virtuální stroj	Vysoká	Emuluje celý hardware a běží v něm vlastní jádro OS.

Moderní nástupci

Dnes je chroot považován za základní stavební kámen, na kterém staví pokročilejší technologie:

- **LXC (Linux Containers):** Přidává izolaci sítě a zdrojů (CPU/RAM).
- **Docker:** Automatizuje správu izolovaných prostředí pomocí obrazů.
- **Systemd-nspawn:** Moderní „chroot na steroidech“ v systémech se systemd.

Související pojmy: Docker, Virtualizace, Linux, Root, Filesystem, Sandbox, Kontejnerizace.