Virtualizace serverů pomocí LXC

Jak to děláme v projektu Turris

Lukáš Jelínek • lukas.jelinek@nic.cz • 7. 10. 2023

TURRIS

K čemu v Turrisu potřebujeme servery

- Kompilace & build (Jenkins, master/slave)
- Repozitář balíčků, instalačních obrazů, dalších souborů
- Podpora výroby (firmware, testování)
- Sentinel (zpracování detekcí, analýza, databáze, dynamický firewall, zobrazování, vstupy, výstupy…)
- E-mailová infrastruktura (notifikace)
- Dokumentace, wikistránky, fórum
- Měření rychlosti (LibreSpeed)
- Monitoring serverů a softwaru (Zabbix)
- Pomocné věci (DNS master, zálohování, logy, VPN…)
- (GitLab, Mattermost, RT, e-mail a kancelářskou VPN využíváme v rámci CZ.NIC)

TURRIS

Co je LXC

- LXC = Linux Containers
- Virtualizace na úrovni OS (společné jádro)
- Využívá standardní technologie linuxového jádra (cgroups, jmenné prostory)
- Možnost omezovat a prioritizovat prostředky
- Privilegované vs. neprivilegované kontejnery
- Low-level nástroje, LXD, ProxMox…

TURRIS

Výhody a nevýhody LXC

- Výhody
  - Zanedbatelná režie
  - Využívá standardní technologie linuxového jádra
  - Je součástí všech hlavních linuxových distribucí
  - Různé možnosti ovládání a správy
  - Aktivní vývoj
- Nevýhody
  - V kontejneru může běžet jen linuxový systém
  - Je potřeba mít systém připraven (distrobuilder)
  - Některé systémové prostředky nelze jednoduše řídit
  - Občasné problémy s technologií AppArmor
  - Problémy s kombinací vzdálených verzí hostitelského systému a kontejneru

TURRIS

Proč používáme LXC

- Zanedbatelná režie – hodně kontejnerů na jednom HW
- Snadná správa automatizovaně i ručně
- Všechny servery běží na Linuxu
- Máme nástroje v Ansiblu (vytváření, úprava, migrace)
- Máme monitoring v Zabbixu
- Možné využití dalších nástrojů (ProxMox)

TURRIS

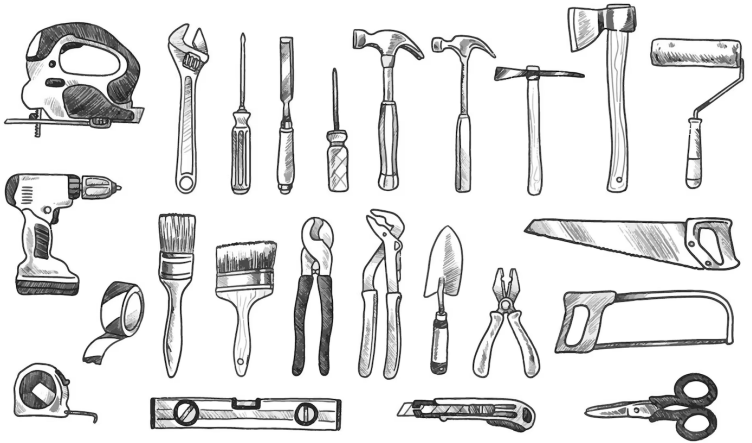
LXC a Ansible – vytváření kontejneru

- Vytvoření kontejneru pomocí modulu lxc_container
- Vytvoření konfigurace kontejneru ze šablony (podpora LXC 2 a 3)
- Konfigurace síťových rozhraní (většinou statická)
- Restart kontejneru
- Příprava a spuštění SSH serveru
- Specifická konfigurace systemd
- Nasazení standardních rolí Ansible

TURRIS

LXC a Ansible – úprava kontejneru

- Běžné úpravy pomocí rolí Ansible
- Úpravy základu LXC – úpravy prostřednictvím hostitele (modul lxc_container a další)



TURRIS

LXC a Ansible – migrace kontejneru (požadavky)

- Migrace jedním příkazem
- Musí proběhnout s minimálním výpadkem
- Data musí téct přímo mezi hostiteli
- Pokud dojde k přerušení, musí jít bezpečně navázat
- Musí podporovat určení zdroje i cíle nebo jen jednoho z nich
- Na zdrojovém hostiteli musí být kontejner archivován

TURRIS

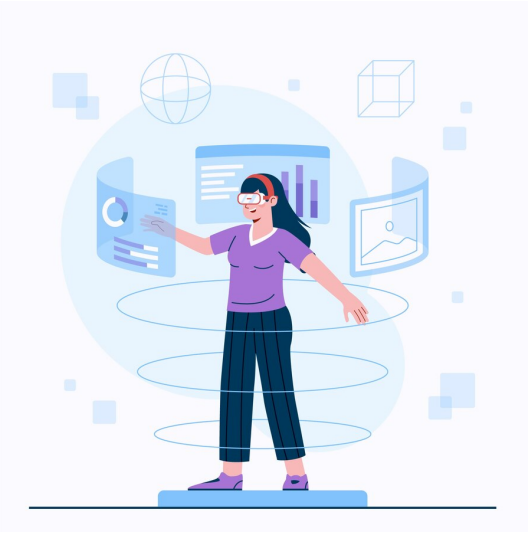
LXC a Ansible – migrace kontejneru (řešení)

- Přenos pomocí rsync skrz SSH spojení
- Příprava: předání klíčů, nastavení SSH, otevření firewallu
- Vlastní přenos: 2x synchronizace za běhu, vypnutí, dosynchronizace, změna konfigurace
- Úklid: zavření firewallu, vrácení konfigurace, smazání klíčů
- Lze udělat i jen přípravu (synchronizaci za běhu)
- Úmyslně se kontejner nezapíná na cílovém hostiteli (chceme ruční kontrolu a spuštění)
- Doba výpadku – podle souborového systému, typicky < 1 min

TURRIS

LXC a Ansible – co dál?

- Chceme to dělat ještě lépe ;-)
- Zvažujeme nasadit ProxMox
  - Kromě LXC podporuje i KVM (někdy se může hodit – větší izolace, nelinuxové systémy, Docker…)
  - Webové rozhraní, konzolové utility
  - REST API, moduly pro Ansible
- LXD? Něco dalšího?
- Nebo jít cestou Kubernetes apod.?



TURRIS

Děkuji za pozornost!

Lukáš Jelínek • lukas.jelinek@nic.cz

TURRIS