Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačních technologií

Teze diplomové práce

Instalace a zabezpečení serverových služeb za využití kontejnerů LXC a Docker

Bc. Michal Kružík

Souhrn

Tato diplomová práce je reakcí na snahu o vývoj a provoz serverových služeb v izolovaném prostředí z důvodu bezpečnosti, testování a přenositelnosti mezi servery. Popisuje kontejnerové technologie LXC a Docker, možnosti jejich využití, výhody, nevýhody a omezení.

Cílem této práce je instalace a konfigurace serverových linuxových služeb ve variantách bez využití kontejnerů, za využití kontejnerů LXC a Docker. Dílčím cílem je jejich porovnání z hlediska výkonu a náročnosti na systémové prostředky.

Klíčová slova

linux, server, lxc, lxd, docker, kontejnerové technologie, bezpečnost, mailserver, webserver

Ačkoli je serverová virtualizace již několik let využívána firmami k optimalizaci zátěže serverů, jejich rozdělení pro klienty a k jejich izolaci, má své omezení. Pro izolaci jednotlivých aplikací, či jejich souvisejících skupin, se nehodí. Vyžaduje pokročilé znalosti virtualizačních nástrojů, výkonnější hardware a obvykle nemalé množství místa na samotné virtualizované servery – často v řádech jednotek až desítek gigabajtů.

Diplomová práce je reakcí na rostoucí využití virtualizace softwaru na úrovni operačního systému. Ze začátku neposkytovaly virtualizační nástroje dostatečnou bezpečnost a měly znatelný vliv na výkon. Situace v současné době je již znatelně lepší a izolace procesů poskytuje dostatečnou úroveň bezpečnosti a efektivity. Vznikly nástroje pro vytváření kontejnerů, které sdílí s operačním systémem jen jádro. Mezi tyto nástroje patří LXC a Docker.

Hlavním cílem bylo vytvoření a zabezpečení plně funkční sady serverových služeb zahrnujících databázový server, webserver a mailserver za využití kontejnerových technologií Docker a LXC. Během instalace byla předpokládána jejich dostupnost v síti Internet na protokolech IPv4 i IPv6. Výjimkou je databázový server, který byl dostupný pouze v rámci virtuálního serveru. Jedná se o následující služby:

- Webserver
    - HTTP
    - HTTPS
- Mailserver
    - IMAP
    - IMAPS
- Databázový server
    - 3306

Dílčím cílem bylo porovnání náročnosti kontejnerových instalací z hlediska systémových nároků, bezpečnosti a časové náročnosti konfigurace oproti sadě služeb bez využití kontejnerů. Pro sběr dat i vytváření zátěže byly zvoleny volně dostupné nástroje.

Metodika řešené práce byla založena na studiu odborné a vědecké literatury a zkušenostech autora. Na základě získaných poznatků byly v teoretické části

charakterizovány kontejnerové technologie, jejich historie, výhody a nevýhody oproti plně virtualizovanému a nevirtualizovanému prostředí. Dále byly popsány kontejnery LXC a Docker z hlediska jejich funkcionalit a možných omezení. V praktické části byla řešena instalace a bezpečná konfigurace vybraných serverových služeb. Dále bylo provedeno měření využití systémových prostředků a testování instalací pro jejich následné porovnání.

Z analýzy v teoretické části vyplývá, že kontejnery přináší, díky izolaci procesů od hostujícího operačního systému, vyšší úroveň bezpečnosti proti některým typům útoků – zvláště při využití neprivilegovaných kontejnerů. Umožňují také vyšší kontrolu nad procesy služeb, například omezením maximálního možného využití systémových prostředků, což může chránit ostatní služby. Oba typy kontejnerů umožňují migraci na jiné OS, u LXC však tato migrace nemusí být triviální.

Náplní praktické části je instalace a bezpečná konfigurace vybraných serverových služeb. Instalace a následné testování bylo provedeno ve třech stejných virtualizovaných prostředích. Tato prostředí jsou poskytována formou plně virtualizovaných serverů. Jedno prostředí je využito pro služby běžící bez kontejnerů, přímo na hostovaném operačním systému. Dvě jsou využity pro instalaci s využitím kontejnerové technologie LXC, respektive Docker.

Pro potřeby následného porovnání byla měřena výkonová náročnost instalovaných služeb volně dostupným programem rrdtool. Během testování instalovaných služeb byl omezen nežádoucí provoz na úrovni firewallu jednotlivých instalací a před každým měřením byl proveden restart serverů pro eliminací možného ovlivnění výsledků.

Data byla měřena pro dvě situace – dlouhodobý stav bez zátěže a krátkodobý stav pod zátěží. Stav bez zátěže byl měřen po dobu jednoho dne v minutových intervalech. Zátěž byla generována HTTP požadavky na instalovanou webovou aplikaci Wordpress programem Apache jMeter. Stav pod zátěží byl měřen v desetisekundových intervalech po dobu půl hodiny. Naměřené hodnoty byly poté analyzovány a byl proveden výpočet jejich průměrů, mediánů a směrodatných odchylek.

V závěrečné části jsou vybrané služby porovnány ve všech prostředích. Porovnávanými parametry jsou paměťová, disková, výpočetní náročnost. Dalším porovnávaným parametrem byla rychlost odpovědi na HTTP požadavky, které byly

generovány v rámci testování. Na závěr byla zhodnocena vhodnost nasazení kontejnerových technologií LXC a Docker.

Výsledkem práce jsou kromě jednotlivých konfiguračních souborů k instalovaným aplikacím a kontejnerům také tři virtualizované servery poskytující zabezpečené služby webserveru, mailserveru a databáze na veřejně dostupných IPv4 i IPv6 adresách. Konfigurační soubory a instalované kontejnery jsou součástí přílohy této práce.

Výsledného stavu bylo dosaženo za využití standardně dostupných nástrojů v repositářích použitého operačního systému Linux, distribuce Ubuntu 16.04 LTS. Tato distribuce je využita ve všech kontejnerech i virtuálních serverech. Důvodem pro zvolení této distribuce byla jeho rozšířenost a velmi dobrá podpora pro běh neprivilegovaných kontejnerů. Tento typ kontejnerů je využit ve všech případech z důvodu vyšší poskytované úrovně bezpečnosti.

Testované instalace za použití kontejnerů jsou oproti instalaci bez kontejnerů v obou variantách více náročné. Zvýšení požadavků na systémové prostředky je zřejmé hlavně v případě využití CPU při běhu pod zátěží. Průměrné naměřené hodnoty byly 2 – 2,5krát vyšší než u varianty bez kontejnerů. Vyšší nároky mohou být problémem hlavně u méně výkonných serverů, protože možnosti navýšení procesorového výkonu jsou omezené.

V případě použití dostatečně výkonných serverů převažují výhody kontejnerizačních technologií, a to hlavně díky vyšší bezpečnosti a přenositelnosti. S ohledem na možnou automatizaci nasazení a správu jsou Docker kontejnery vhodnější pro produkční provoz i testování. Kontejnery LXC se hodí pro existující aplikace, které nejsou připravené na běh v Docker kontejnerech a na případné škálování. Technologie Docker i LXC předpokládají přístupnost k síti Internet na protokolu IPv4.

Vzhledem k omezení kontejnerových technologií LXC a Docker se jeví, jako další vhodný krok, využití orchestračních nadstaveb jako je Kubernetes a OpenShift. Tyto nadstavby také řeší možné škálování a spouštění kontejnerů na několika fyzických, či virtualizovaných serverech.

Seznam použitých zdrojů

[1] RUEST, Danielle. Virtualizace. Computer Press, 2010. ISBN: 978-80-251-2676-9

[2] GOASGUEN, Sébastien. Docker Cookbook: Solutions and Examples for Building Distributed Applications. O'Reilly Media, 2015. ISBN: 978-1491919712

[3] Linux Containers. *LXC – Introduction*. [online]. [cit. 2017-12-14]. Dostupné z https://linuxcontainers.org/lxc/introduction/

[4] Linux Containers Forum. *Comparing LXD vs. LXC.* [online]. [cit. 2017-12-14]. Dostupné z https://discuss.linuxcontainers.org/t/comparing-lxd-vs-lxc/24

[5] Sourceforge. *Lxc*. [online]. [cit. 2017-12-14]. Dostupné z http://lxc.sourceforge.net/man/lxc.html

[6] Docker Documentation. *Get Started, Part 1: Orientation and Setup*. [online]. [cit. 2018-01-10]. Dostupné z https://docs.docker.com/get-started/

[7] NICKOLOFF, Jeff. Docker in Action. Manning Publications, 2016. ISBN: 978 1633430235