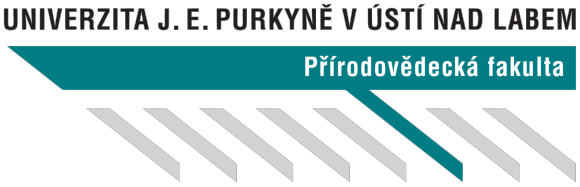
Univerzita Jana Evangelisty Purkyně
v Ústí nad Labem
Přírodovědecká fakulta



Proxmox

Seminární práce

Vypracoval: Martin Kopecký

Studijní program: Aplikovaná informatika
Studijní obor: Informační systémy

Ústí nad Labem 2024

Obsah

Kapitola 1

Historie

Proxmox je oblíbená virtualizační platforma, která kombinuje virtuální servery (Proxmox Virtual Environment, PVE) a systém pro správu clusterů a virtualizovaného úložiště (Proxmox Virtual Environment Cluster). Její historie sahá do roku 2008, kdy byla poprvé uvedena na trh společností Proxmox Server Solutions GmbH, založenou v Rakousku.

Proxmox VE byl vytvořen jako open-source řešení, které poskytuje efektivní a snadno použitelné prostředí pro správu virtuálních serverů. Od začátku byl postaven na Linuxovém jádru a využíval virtualizační technologie jako KVM (Kernel-based Virtual Machine) a kontejnerovou technologii LXC (Linux Containers), což umožňovalo uživatelům vytvářet a spravovat virtuální stroje a kontejnery z jediného rozhraní.

V průběhu let došlo k několika důležitým vývojovým krokům. Významným milníkem bylo zavedení Proxmox VE Cluster, což umožnilo správu více serverů jako jednoho celku, což výrazně zjednodušilo správu zdrojů a redundanci. Další významnou aktualizací bylo zavedení Ceph, rozšířeného open-source úložného řešení, které umožňuje vysoce škálovatelné blokové úložiště.

Proxmox se také vyznačuje svým uživatelským rozhraním založeným na webovém prohlížeči, které umožňuje jednoduché správu a monitoring virtuálních strojů a úložiště. Uživatelé oceňují jeho flexibilitu a širokou škálu konfiguračních možností, které jsou přístupné i bez hlubokých znalostí Linuxu.

Proxmox VE je také známý svou komunitou a širokou podporou. Jako open-source řešení má aktivní komunitu vývojářů a uživatelů, kteří neustále přispívají k jeho vývoji a zlepšování. To zahrnuje pravidelné aktualizace, bezpečnostní opravy a nové funkce, což udržuje Proxmox VE jako relevantní a konkurenceschopnou platformu v oblasti virtualizace.

V současnosti je Proxmox široce používán v mnoha odvětvích, od malých podniků až po velké korporace, díky své schopnosti efektivně spravovat rozsáhlé a komplexní virtualizované prostředí. Jeho kombinace výkonu, flexibility a nízkých nákladů činí z Proxmoxu atraktivní volbu pro mnoho organizací hledajících efektivní virtualizační řešení.

Kapitola 2

Jádro virtualizace

Jádrem platformy Proxmox je Proxmox VE, robustní virtualizační řešení založené na Linuxu, které kombinuje KVM (Kernel-based Virtual Machine) a LXC (Linux Containers) technologie.

2.1 LXC

LXC (Linux Containers) je technologie pro virtualizaci na úrovni operačního systému, která je implementována v Linuxovém jádře. LXC umožňuje uživatelům spouštět více izolovaných instancí operačního systému na jednom hostitelském systému. Zde je podrobnější vysvětlení, jak LXC funguje:

2.1.1 Základní Koncepty:

Namespaces: LXC využívá Linuxové namespaces pro izolaci aplikací a procesů. Namespaces oddělují systémové aspekty (jako jsou síť, uživatelé, souborový systém atd.), což umožňuje každému kontejneru mít vlastní izolované prostředí, které se jeví jako samostatný systém.

Control Groups (cgroups): Cgroups omezují a monitorují zdroje, které mohou být používány procesy. Pomocí cgroups může LXC kontrolovat a omezovat, kolik CPU, paměti, síťové kapacity a dalších zdrojů může každý kontejner využívat.

2.1.2 Izolace a Bezpečnost:

LXC poskytuje silnou izolaci mezi kontejnery a mezi kontejnery a hostitelským systémem. To je zásadní pro bezpečnost, protože procesy běžící v jednom kontejneru nemohou přistupovat k procesům nebo zdrojům jiných kontejnerů nebo hostitelského systému.

Bezpečnostní funkce, jako jsou AppArmor nebo SELinux, mohou být použity pro další zabezpečení kontejnerů, například omezují, které systémové volání

mohou kontejnery používat.

2.1.3 Architektura a Výkon:

Na rozdíl od plné virtualizace, jako je KVM nebo Xen, LXC neemuluje hardwarovou vrstvu. Místo toho všechny kontejnery sdílejí stejné jádro hostitelského systému. Tato "lehká"virtualizace vede k menší režii, vyššímu výkonu a rychlejšímu spouštění kontejnerů.

Kontejnery LXC mohou běžet různé distribuce Linuxu, což umožňuje flexibilní nasazení aplikací bez ohledu na distribuci hostitelského systému.

2.1.4 Správa a Použití:

LXC je vybaveno nástroji pro snadné vytváření, spouštění, zastavování a spravování kontejnerů. Tyto nástroje umožňují uživatelům efektivně spravovat životní cyklus kontejnerů.

Kontejnery lze použít pro širokou škálu aplikací, od izolovaných prostředí pro vývoj a testování po nasazení produkčních aplikací.

2.1.5 Integrace a Rozšiřitelnost:

LXC je často využíváno jako základ pro vyšší úrovni kontejnerových orchestrací a management nástrojů, jako je Docker a Kubernetes, i když tyto nástroje v současné době používají vlastní kontejnerové runtime.

Prostřednictvím LXC API mohou vývojáři integrovat funkce kontejnerů do svých aplikací nebo vytvářet vlastní nástroje pro správu kontejnerů.

V souhrnu, LXC poskytuje efektivní, bezpečnou a flexibilní platformu pro běh izolovaných Linuxových prostředí na jednom hostitelském systému, využívající přitom výhod Linuxového jádra a jeho schopností. Tato technologie je klíčová pro moderní cloudové a kontejnerové řešení.

2.2 KVM

KVM (Kernel-based Virtual Machine) je open-source virtualizační technologie pro Linux, která umožňuje transformovat Linux na hypervisor typu 1. Tato technologie využívá virtualizační funkce moderních procesorů, jako jsou Intel VT-x a AMD-V, a integruje se přímo do Linuxového jádra. Zde je podrobnější pohled na to, jak KVM funguje:

2.2.1 Základní Principy

KVM se stává součástí Linuxového jádra, což znamená, že každý Linuxový server s odpovídajícím jádrem a podporovaným hardwarem může fungovat jako hypervisor. KVM přidává do jádra funkce pro správu a spouštění virtuálních strojů (VM), zatímco samotné VM jsou standardní Linuxové procesy, řízené plánovačem jádra.

2.2.2 Hardwarová Virtualizace

KVM využívá hardwarovou podporu pro virtualizaci, která je poskytována moderními procesory. Tato hardwarová podpora umožňuje KVM efektivně spouštět izolované VM, každý s vlastním virtuálním hardwarem, včetně CPU, paměti, disků a síťových adaptérů. Virtualizovaný hardware VM je emulován pomocí QEMU (Quick Emulator), který poskytuje emulaci zařízení pro VM.

2.2.3 Vytváření a Správa VM

VM jsou v KVM vytvářeny a spravovány pomocí standardních nástrojů pro virtualizaci, jako je libvirt a jeho nástroj virsh, nebo grafická rozhraní jako virt-manager. Každý VM je izolován od ostatních VM a od hostitelského systému, což zajišťuje bezpečnost a stabilitu.

2.2.4 Výkon a Škálovatelnost

Díky hardwarové podpoře a úzké integraci s Linuxovým jádrem nabízí KVM vynikající výkon a škálovatelnost, což je ideální pro náročné serverové a cloudové prostředí. KVM podporuje funkce jako NUMA (Non-Uniform Memory Access), což umožňuje efektivní využívání paměti v multiprocesorových systémech.

2.2.5 Bezpečnost a Izolace

VM v KVM jsou dobře izolovány díky použití hardwarových funkcí virtualizace a bezpečnostních mechanismů Linuxu, jako jsou SELinux a cgroups. Tato izolace pomáhá chránit před škodlivým softwarem a zajišťuje, že chyba nebo selhání jednoho VM neovlivní ostatní VM nebo hostitelský systém.

2.2.6 Live Migrace

KVM podporuje live migraci, což umožňuje přesunutí běžících VM z jednoho fyzického serveru na druhý bez výpadku služby. Toto je klíčové pro údržbu a řízení zatížení v datových centrech.

2.2.7 Ekosystém a Integrace

KVM je široce podporován v rámci Linuxové komunity a integruje se s mnoha dalšími technologiemi a nástroji, což umožňuje širokou škálu použití od jednoduchých virtuálních hostů až po komplexní cloudové řešení. V souhrnu, KVM je výkonný a efektivní nástroj pro virtualizaci, který poskytuje robustní, bezpečnou a škálovatelnou platformu pro správu a provoz virtuálních strojů v Linuxovém prostředí.

2.2.8 Podporované formáty

KVM (Kernel-based Virtual Machine) podporuje různé formáty virtuálních disků, které se liší v několika klíčových aspektech, jako jsou výkon, flexibilita a podpora funkcí. Níže uvádím několik běžně používaných formátů a jejich hlavní rozdíly:

Raw

Raw formát je nejzákladnější a nejjednodušší formát virtuálního disku. Reprezentuje data bez jakékoliv metadata nebo struktury, což znamená, že soubor raw disku je přímým obrazem obsahu disku.

> **Výhody:** Vynikající výkon díky absenci dodatečného zpracování. Je také univerzálně kompatibilní s různými hypervizory a nástroji pro virtualizaci.
>
> **Nevýhody:** Chybí mu pokročilé funkce jako snímky (snapshots), dynamické alokace velikosti a komprese.

qcow2 (QEMU Copy On Write verze 2)

qcow2 je pokročilý formát disku vytvořený pro QEMU (Quick Emulator). Nabízí řadu funkcí, jako jsou snímky, komprese a šifrování.

> **Výhody:** Podporuje dynamickou alokaci velikosti, což znamená, že soubor disku roste pouze při potřebě ukládat data. Možnost vytvářet snímky (snapshots) umožňuje snadnou zálohu a obnovu stavů virtuálního stroje.
>
> **Nevýhody:** Může mít mírně nižší výkon ve srovnání s raw formátem kvůli správě dodatečných funkcí.

VMDK (Virtual Machine Disk)

Formát vytvořený společností VMware, ale podporovaný i jinými hypervizory, včetně KVM. VMDK umožňuje ukládat virtuální disky jako jeden soubor nebo sadu souborů.

> **Výhody:** Dobrá podpora v různých virtualizačních technologiích, umožňuje snadné přenášení VM mezi různými platformami. Podporuje snímky a dynamickou alokaci.
>
> **Nevýhody:** Může být méně optimalizovaný pro KVM ve srovnání s formátem qcow2 nebo raw.

VHDX (Hyper-V Virtual Hard Disk v2)

VHDX je formát zavedený Microsoftem pro Hyper-V. Je navržen tak, aby zlepšil odolnost proti poškození dat a umožnil větší maximální velikosti disku.

> **Výhody:** Vyšší odolnost proti poškození dat, podpora pro velké disky (až 64 TB) a funkce, jako je bloková alokace a interní šifrování.
>
> **Nevýhody:** Méně běžný v prostředích KVM a může vyžadovat další konfiguraci pro optimální výkon a kompatibilitu.

Každý z těchto formátů má své specifické výhody a nevýhody a vhodnost každého formátu závisí na konkrétních požadavcích a prostředí, ve kterém je KVM používán. Například pro prostředí, kde je klíčová vysoká výkonnost a jednoduchost, může být vhodnější raw formát, zatímco

Kapitola 3

Jádro

Virtualizační platforma Proxmox nabízí rozsáhlé možnosti pro efektivní správu a provoz virtualizovaných prostředí. Její funkčnost lze rozdělit do několika klíčových oblastí:

3.1 Uživatelské rozhraní a správa

Proxmox VE se vyznačuje výkonným webovým rozhraním, které umožňuje snadnou správu virtuálních strojů, kontejnerů, sítí a úložiště. Rozhraní nabízí přehledný dashboard, detailní statistiky v reálném čase, logy a možnost konfigurace různých aspektů virtualizovaného prostředí.

3.2 Clusterování a vysoká dostupnost

Proxmox podporuje vytváření clusterů z více serverů, což umožňuje centralizovanou správu a redundanci. Funkce vysoké dostupnosti (High Availability, HA) zajišťuje, že kritické virtuální stroje mohou být automaticky restartovány na jiném uzlu v případě selhání hardwaru.

3.3 Úložiště

Proxmox podporuje širokou škálu úložných řešení, včetně lokálního úložiště, NFS, iSCSI, Fiber Channel a Ceph. Ceph nabízí vysoce škálovatelné blokové, objektové a souborové úložiště, což je ideální pro velká data a cloudové úložné řešení.

3.4 Zálohování a obnova

Proxmox obsahuje integrované nástroje pro zálohování a obnovu virtuálních strojů a kontejnerů. Tyto nástroje umožňují plánovat pravidelné zálohy, což zajišťuje ochranu dat a usnadňuje obnovu v případě selhání.

3.5 Síťové funkce

Proxmox nabízí pokročilé síťové možnosti, včetně podpory VLAN, bondingu síťových rozhraní a firewallových funkcí. Umožňuje také snadnou integraci s externími síťovými službami a zařízeními.

3.6 Migrace a flexibilita

Live migrace umožňuje přesun virtuálních strojů mezi hostitelskými servery bez výpadku služby. Toto je klíčové pro údržbu hardwaru a optimalizaci zdrojů bez narušení provozu.

3.7 Rozšiřitelnost a API

Proxmox VE je vybaven REST API, které umožňuje automatizaci správy prostřednictvím skriptů a integraci s dalšími systémy. Komunita také poskytuje řadu pluginů a rozšíření pro další funkčnost.

3.8 Bezpečnost

Bezpečnostní funkce zahrnují šifrování na úrovni disku, podporu pro různé autentizační back-endy (LDAP, Active Directory, atd.) a izolaci prostředí prostřednictvím virtuáln