Optimalizace správy a zabezpečení virtuálních strojů

Michal Švamberg

Západočeská univerzita v Plzni
Centrum informatizace a výpočetní techniky
email: svamberg@civ.zcu.cz

2. září 2015

Abstrakt

Předpokládaný projekt se zabývá analýzou možností, testováním, přípravou a nasazením systému, který by umožnil vyšší automatizaci vytváření virtuálních strojů než je na dosud používaném systému. Cílem je zlepšit bezpečnost, proto se projekt zaobírá vynucováním důležitých bezpečnostních nastavení na hostovaných systémech.

1 Současný stav řešeného problému

Virtualizace serverů byla již dříve řešena v projektech Fondu rozvoje CESNET 154R1/2005[1] a 192R2/2006[2], jejichž výsledky jsou stále používany (aktuálně přes 140 virtuálních strojů provozovaných na 6 fyzických serverech). Tato virtualizace serverů je velkým přínosem, šetří naklady na provoz serverovny a usnadňuje správu.

Ovšem vývoj ve virtualizaci pokročil a z původně zamýšleného systému pro testování se stal klíčový prvek IT infrastktury. Nyní je znát, že dlouhodobě je stávající systém neudržitelný a bude nutné jej upravit tak, aby byl ještě více automatizován, měl lepší uživatelské rozhraní a byl lépe zabezpečen.

Virtualizace na ZČU je založena na systému Xen (v srpnu 2015 ve verzi 4.4), který nyní běží na 5 provozních a jednom testovacím serveru. Tuto technologii známe po administrátorské stránce velmi dobře.

Virtuální stroje mají vlastní oddíl na FC prostoru[3], které jsou připojeny k různým typům polí[4], které jsou děleny systémem LVM (Logic Volume Manager). Zde spatřujeme

[1] http://support.zcu.cz/index.php/CIV:Granty/Ověření_migrace_Xen_virtuálních_strojů
[2] http://support.zcu.cz/index.php/CIV:Granty/Rozvoj_Xen_virtuálních_strojů
[3] Sdílený diskový prostor je jedna z podmínek pro použití migrace virtuálních strojů.
[4] Rychlé disky pro systém a databáze, pomalé kapacitní disky pro datové části.

jednu ze slabin, přestože je LVM přístupné z více strojů, není zde zaveden žádný režim clusteru a aktualizace rozdělení se po každé změně provádí na všech serverech ručně.

Po síťové stránce jsou servery připojeny etherchannelem do dvou různých přepínačů (opatření proti výpadku). Jednotlivé podsítě jsou značkovány dle standardu 802.1q a přivedeny k lokálním softwarový bridgům (brctl). O této části si myslíme, že lépe ji udělat nelze, a proto bychom ji chtěli zachovat.

Správa virtuálních strojů je prováděna výhradně ručně, není k dispozici žádné jiné rozhraní, než příkazová řádka na serverech. Chybí centrální zastřešující prvek, který by sjednotil a zjednodušil ovládání strojů. Jde zejména o základní operace životního cyklu virtuálního stroje (instalace, restart, konzole, zrušení, atd.).

Zatím jsme se vůbec nezabývali automatizací rozvážení virtuálních strojů dle generující zátěže. Toto rozvažování jsme zatím vždy prováděli ručně. Stroje, které mají odolávat velké zátěži jsou provozovány na samostatném hardware. Na virtuálních strojích provozujeme málo nebo středně náročné systémy.

Vytvoření strojů je nyní rutinní ruční práce. Je třeba stroj registrovat do systému DNS, vytvořit pro něj konfiguraci v systému FAI[5], připravit LVM oddíly a po instalaci pro něj nastavit monitoring. Dále je třeba upravit firewall a další parametry dle potřeb provozovaného systému. Věříme, že většina těchto operací lze automatizovat a zjednodušit, než je tomu nyní, kdy všechny nutné operace zkušenému správci trvají více než hodinu.

Vzhledem k tomu, že se jedná o uzavřené systémy, kam nemá přístup nikdo jiný vyjma správců (tedy ani zaměstnanci mimo CIV nebo studenti), tak jsme otázku bezpečnosti nikdy příliš neřešili. Pokud bychom ale chtěli nabídnout virtuální stroje i mimo CIV, pak je nutné se tímto zabývat. Bude třeba vymyslet způsob jak i přes oprávnění správce vynutit některá klíčová bezpečnostní opatření (např. aktivní firewall).

2 Cíle řešení

Zjednodušeně řečeno je cílem postavit novou verzi virtualizace, která zjednoduší a více automatizuje její správu. Současně se zavede lepší zabezpečení, čímž bude možno nabídnout vytvořit si virtuální stroj i mimo správce IT infrastruktury ZČU. Chtěli bychom odstranit největší současné nedostatky používaného řešení:

- těžkopádný systém rozdělování disků pro virtální stroje,
- chybějící uživatelské rozhraní pro správu virtálních strojů,
- nepřipravené zabezpečení pro širší používání,
- příliš náročné vytváření virtálního stroje.

Před nasazením do ostrého provozu nabídneme možnost vytvořit si a používat server všem zaměstnancům a studentům. Tuto možnost si doteď museli osobně domlouvat. Před-

[5] `http://fai-project.org/`

pokládáme, že existuje skupina uživatelů, kteří by tuto možnost uvítali. Od tohoto kroku si slibujeme lepší zpětnou vazbu a důkladnější otestování připraveného řešení.

Dlouhodobě zjišťujeme, že uživatelé (zaměstnanci i studenti) nejsou schopni správně zabezpečit operační systém a nejběžnější aplikace. Proto je v projektu kladen důraz na vynucenou bezpečnost, které se budou muset podřídit. Pod pojmem *vynucené bezpečnosti* plánujeme taková opatření, která nebude možné obejít bez souhlasu správců. Od tohoto opatření si slibujeme snížení počtu bezpečnostních incidentů a vylepšení zabezpečení IT infrastruktury na ZČU, protože uživatelé již nebudou nuceni provozovat své stroje někde "pod stolem". Navíc se tak podaří více centralizovat a sjednotit IT prostředí.

Předpokládáme, že je to zajímavé téma také pro studenty, které bychom chtěli do projektu zapojit. Již dříve se nám tato možnost osvědčila a rádi bychom ve spolupráci se studenty pokračovali.

3 Způsob řešení

Pro projekt předpokládáme nákup tří silných serverů[6], na kterých bude připravena nová virtualizace. K těmto strojům budou později přidány další s tím, jak postupně bude probíhat migrace ze starého systému virtualizace na nový.

Pro lepší správu diskových oddílů předpokládáme nasazení clustrového režimu LVM. Tím by měla být zajištěna synchronizace operací přes všechny servery a odstraněna ruční synchronizace metadat o volumech.

Samotnou virtualizační vrstvu předpokládáme ponechat na technologii Xen, pouze v případě významného přínosu přechodu využít jinou technologii, například KVM. Takovým přínosem by mohlo být významně lepší hostování virtuálních strojů s operačním systémem Windows nebo výrazně lepší správa a využití systémových zdrojů.

Cílem projektu není vytvořit nové rozhraní pro správu, ale implementovat nějaké již existující. Proto chceme otestovat nejpoužívanější projekty a využít jejich potenciál. Z tohoto důvodu je třeba celý systém postavit s jednotným API, za které je dnes považováno rozhraní libvirt.

Použitím obecně uznávaného API je možné vyzkoušet různá uživatelská (a administrátorská) rozhraní. Naši představu o potřebách by měl dokázat splnit OpenStack[7], OpenNebula[8] nebo oVirt[9], případně další projekty pro správu virtuálních strojů. Jedná se o nejdůležitější rozhodnutí, protože od něj se budou odvíjet možnosti škálovatelnosti, konfigurovatelnosti, ale i náročnost celé správy virtualizačního systému a nutné požadavky na znalosti systému.

Zvýšení bezpečnosti máme v plánu provést s využitím systému centrální správy konfigurace, kterou zatím používáme pouze pro základní nastavení operačního systému. Zatím jsme se nezabývali jeho využítím pro zabezpečení (vyjma konfigurace firewallu). Proto bude

[6] V konfiguraci minimálně 2 CPU, 128GB RAM, 2x10GE, duální 8Gbps FC kartou a dva lokální disky.

[7] `http://www.openstack.org/`

[8] `http://www.opennebula.org/`

[9] `http://www.ovirt.org/`

nutné rozmyslet, jak přistoupit k otázce, kdy chceme vynutit používanou bezpečnostní politiku na stroji, kde má práva administrátora také uživatel, který si o stroj požádal. K tomuto chceme využít existující systém pro správu konfigurace, předpokládáme napojení na CFEngine[10], který je na ZČU již nasazený. Toto je jediná část, kterou nelze snadno přenést do jiného výpočetního prostředí, lze se jí však inspirovat. Na druhou stranu je tato část snadno oddělitelná od zbytku systému správy virtualizace a tudíž nebrání využít informace z tohoto projektu jinde.

Uživatelům je třeba nabídnout jednoduché rozhraní, kterým si mohou požádat a nechat vytvořit virtální stroj. Zde uvidí stav stroje a budou mít přístup k základnímu ovládání. Toto rozhraní je největší problém, máme s ním jen minimální zkušenosti a znalosti. Zato máme jasnou představu, co od takového prostředí očekáváme. Proto bude nutné prozkoumat existující možnosti a najít nejvhodnější řešení, které pak nasadíme. Zpětnou vazbu uživatelů chceme využít pro zlepšení nastavení. To je důvod, proč žádáme o delší doby trvání projektu.

Za nejnáročnější považujeme úkol, kdy je třeba více napojit životní cyklus virtuálních strojů na zbytek IT infrastruktury ZČU. Jedná se o registraci v DNS systému, nastavení monitoringu, zařazení do evidence serverů. Taktéž bude nutné vyřešit způsob instalace. Zde je možnost se vydat zcela novou cestou nebo využít existující systém FAI. Rozhodnutí bude pravděpodobně odvislé od možností použitého administračního rozhraní.

Celé řešení projektu chceme provést tak, aby bylo co nejvíce použitelné také v podobných výpočetních prostředích.

4 Prezentace výsledků

Bude nutné oslovit uživatele a seznámit je s možností vytvořit si virtální stroj, který bude přednastaven a zabezpečen pro použití v IT prostředí ZČU. Proto bude připraveno setkání, kde bude prezentováno řešení a možnosti jak jej využít.

Řešení bychom chtěli prezentovat také na některé z tuzemských konferencí zabývající se otevřenými systémy nebo virtualizací. Příspěvek přihlásíme minimálně do konference OpenAlt[11] a EurOpen[12].

Všechny výsledky projektu budou k dispozici členům sdružení CESNET a zveřejněny na webu.

5 Charakteristika řešitelského týmu

Řešitelský tým je složen ze zkušených pracovníků Laboratoře počítačových systémů Centra informatizace a výpočetní techniky na Západočeské univerzitě v Plzni. Řešitelský kolektiv

[10] `http://www.cfengine.com/`
[11] `http://www.openalt.cz/`
[12] `http://www.europen.cz/`

má zkušenosti z oblasti správy operačních systémů a jejich implementace do infrastruktury distribuovaného výpočetního prostředí.

Řešitelský kolektiv tvoří:

Ing. Michal Švamberg (hlavní řešitel) vystudoval obor distribuované systémy na Fakultě aplikovaných věd na Západočeské univerzitě v Plzni. Od roku 2002 pracuje v Laboratoři počítačových systémů, Centra informatizace a výpočetní techniky, kde se účastnil návrhu a budování kolejních sítí Západočeské univerzity. Dále se zabývá správou operačního systému Linux a jeho integrací do distribuovaného výpočetního prostředí `Orion`. Spravuje diskovou FibreChannel infrastrukturu, souborový systém AFS, systém virtualizace serverů založených na technologii XEN a mnoho dalších. Na ZČU působí jako instruktor v certifikačních programech CCNA a CCNP. Podílí se na správě národní gridové infrastruktury MetaCentrum.

Ing. Jan Krčmář (spoluřešitel) je absolventem Fakulty Aplikovaných věd Západočeské univerzity v Plzni v oboru Kybernetika a řídicí technika. Od roku 2006 pracoval jako správce Linuxových učeben a automatických instalací pro Západočeskou univerzitu. Od roku 2009 pracoval jako správce *nix systémů ve společnosti ČD-Telematika, kde zajišťoval provoz systémů pro České dráhy. Jednalo se především o návrh a správu HA řešení, virtuálních prostředí a poštovních systémů s důrazem na bezpečnost. Od roku 2015 pracuje v Laboratoři počítačových systémů, Centra informatizace a výpočetní techniky. Hlavní náplní je správa souborových systémů, automatických instalací a virtuálních prostředí. Zároveň se podílí na provozu české národní gridové infrastruktury MetaCentrum. Získal certifikát IPv6 na NIC.CZ v roce 2012 a CCNA na ZČU v roce 2013.

6 Navrhovaná doba trvání projektu

Navrhovaná doba trvání projektu je plánována na 18 měsíců vzhledem k množství existujících technologií a také předpokládanému velkému objemu práce na propojení již provozovaných systémů.

7 Finanční rozvaha

Pro projekt jsou požadovány jen náklady spojené s řešením grantu, které činí 946 000,- Kč bez DPH. Z prostředků Fondu rozvoje budou čerpáno ve výši 300 000,- Kč, zbylou částku 646 000,- Kč (tj. 68,3%) včetně dalších nákladů spojených s projektem hradí řešitelská organizace.

Celkem odhadované náklady na pokrytí projektu bez DPH byly stanoveny na:

položka	cena v tis. Kč	zdroj financování
3ks výkonného serveru	360	ZČU
mzdy	224	CESNET
odměny řešitelům	129	ZČU
povinné odvody ze mzdy a odměn (34%)	76	CESNET
povinné odvody ze mzdy a odměn (34%)	44	ZČU
tuzemské cestovné, konferenčné	25	ZČU
režie (15% z NIV)	88	ZČU
celkem	946	

Tuzemské cestovné a konferenčné pokrývá náklady odhadované na prezentaci výsledků projektu na některé z národních konferencí zabývající se otevřenými systémy nebo virtualizací, případně jiným příbuzným tématem.

Cena serveru, konfigurace a dodavatel vychází z interního výběrového řízení ZČU pro roky 2014-2016 na dodávku serverů. Předpokládaná životnost serveru je minimálně 5 let, čemuž odpovídájí záruční podmínky a hardwarová konfigurace. Tři servery jsou nezbytné z důvodu použití clusterových technologií, což je doporučovaný minimální počet. Server v ceně 120 000,- Kč bez DPH byly vysoutěženy v konfiguraci:

- 2x Xeon 6C E5-2620v2 2.1GHz
- 128GB RAM, 1600MHz
- 2x 300GB HDD v HW RAID
- 2x 10Gbps síťová konfigurace
- FibreChannel duální karta 8Gbps karta
- redundantní zdroj napájeni, DVD mechanika
- vzdálený management

Výsledky výběrového řízení jsou veřejně k dispozici na profilu zadavatele[13], včetně tohoto času platné rámcové smlouvy na nákup serverů[14].

Předpokládaný rozpis prací na projektu je uveden v tabulce číslo 1 v pracovních dnech na plný úvazek (tzv. člověkodny). Jsou zde uvedeny nejdůležitější práce, které na projektu předpokládáme provést. Cenu za jeden pracovní den jsme stanovili na 2500,- Kč včetně odvodů.

[13] https://profilzadavatelezapadoceskauniverzitavplzni49777513.allycon.eu/contracts/detail/213

[14] Rámcová smlouva je ke stažení na výše uvedeném odkazu výběrového řízení v sekci *Další dokumenty veřejné zakázky* jako předposlední dokument s názvem *Rámcová smlouva* jejíž součástí je technická specifikace a ceník serverů a jeho komponent.

Instalace serverů a připojení do infrastruktury	6
Příprava a testování základního virtualizačního prostředí	12
Konfigurace clustrového režimu LVM	5
Testování a ladění konfigurace LVM	10
Analýza dostupných řešení pro uživatelské rozhraní	8
Otestování vhodných uživatelského rozhraní	20
Instalace a základní konfigurace uživatelského rozhraní	5
Nastavení autentizace a přístupových práv	3
Napojení na systém správy DNS	5
Napojení na monitoring	8
Napojení na správu serverů	2
Konfigurace instalačního mechanismu virtuálních strojů	22
Nastavení centrálního konfiguračního managementu	16
Vynucení bezpečnostních politik ve virtuálních strojích	15
Úpravy systémů na základě zpětné uživatelské vazby	20
Celkem	**157**

Tabulka 1: Tabulka rozpisu prací rozpočtena na pracovní dny