Katalog služeb společnosti EPOFIS IT

Verze 20170921

OBSAH

1 Úvod

Hlavním cílem naší společnosti EPOFIS IT s.r.o. je stát se stabilní a neustále se rozvíjející firmou, která nabídne svým zákazníkům kvalitní a spolehlivé služby v oblasti kompletní správy IT. Veškeré práce jsou vykonávány týmem zkušených odborníků s dlouholetou praxí jak v oblasti Linuxové tak Windows infrastruktury. Hlavní důraz při všech pracích pro naše zákazníky klademe na kvalitu a inovativnost za dodržení rozumných nákladů a maximální přidané hodnoty.

Hlavními obory naší činnosti jak v oblasti serverové, tak oblasti stolních počítačů či notebooků jsou:

1. Analýza infrastruktury
2. Návrh infrastruktury
3. Realizace infrastruktury
4. Správa infrastruktury
5. Vybudování a ochrana zabezpečení síťové infrastruktury

Naše dlouholeté zkušenosti z různých oblastí IT nám umožňují pro každého zákazníka vybrat optimální řešení, které zohledňuje jeho preference, klientské prostředí, funkcionalitu a samozřejmě také cenové předpoklady.

Správná volba mezi platformou Linux a MS Windows závisí na více atributech a nedílnou součástí spolupráce se zákazníky jsou tak konzultace a analýza prostředí. To vše nám umožní hlubší náhled do zákaznické problematiky a v konečném důsledku je náš tým schopen zvolit nejoptimálnější řešení pro každého zákazníka.

Naši technici jsou dostupní v Praze, Brně, Ostravě a Zlíně.

V kapitolách níže najdete detailní informace o nabízených službách v oblasti Linuxové a Windows infrastruktury.

Věříme, že se naše společnost může stát zajímavým partnerem pro Vaše IT.

Za tým společnosti EPOFIS IT s.r.o.
Ing. Michal Fiala, jednatel společnosti

2 Linux

2.1 Úvod

Našim zákazníkům nabízíme řešení, která pokrývají jejich požadavky, zohledňují jejich možnosti a kryjí možná rizika.

Máme velmi dobré znalosti operačního systému Linux a aktivně se zapojujeme do jeho ladění, kooperujeme s komunitou kolem operačního systému Linux. Máme zkušenosti s provozem distribucí Gentoo, Debian, Ubuntu LTS, CentOS, Red Hat, SuSE.

Díky hlubokým znalostem a zkušenostem s operačním systémem Linux, jsme schopni zákazníkům nabídnout řešení na míru dle jeho potřeb a maximalizovat užitek z komunitního software.

Máme zkušenosti s provozem různě náročných aplikací:

- **Základní**, kde aplikační služby běží pouze na jednom operačním systému.
- **Pokročilé**, kde jsou aplikační služby odděleny v rámci více operačních systémů, služby však běží pouze v jedné instanci.
- **Náročné**, aplikace náročné na výkon a vysokou dostupnost, kde aplikační služby běží ve více instancích na více serverech. Tyto aplikace vyžadují distribuci zátěže, replikaci dat, automatickou detekci a následné řešení problémů, horizontální škálovatelnost, provádění údržby za provozu.

2.2 Síťová brána

- Linux tvoří bránu pro příchozí síťový provoz. Základní funkcionalitou je zabezpečení provozu, aplikace firewall pravidel, přesměrování provozu, zaznamenávání podezřelého provozu.
- Neméně důležitou rolí je brána pro odchozí síťový provoz, neboli default gateway.
- **VPN** přístup do privátní sítě postavený na nástroji **OpenVPN**.
- Služby pro privátní síť jako **DHCP** či **DNS**.
- Linux plní velmi dobře roli distributora provozu (loadbalancer), je to zajímavá alternativa vůči zásadně finančně nákladnějším HW řešením. Využíváme nástroj **Haproxy** (síťová vrstva L4/L7, SSL offloading). Pokud klient požaduje cachování HTTP provozu, můžeme nasadit reverse proxy **Varnish.** Námi používaná řešení lze horizontálně škálovat, můžeme navýšit výkon přidáním dalšího serveru.

2.3 Webový, aplikační server

- Dle dohody s vývojáři volíme mezi web servery **Apache**, **Nginx** či **Lighttpd**. V případě zájmu o cachování HTTP obsahu můžeme nasadit reverse proxy **Varnish**.
- Vývojáři mohou využít interprety **PHP**, **Python**, **Perl**, **Ruby**, **Mono**. Můžeme provozovat více majoritních verzí PHP, Python, Ruby na jednom operačním systému. Pro vývojáře jsme schopni postavit vývojové prostředí na míru, využijeme vysoké úrovně volnosti, škálovatelnosti Linux distribuce **Gentoo**.
- Máme zkušenosti s provozem aplikací na platformě **Node.js**.
- Pro zabezpečení webových projektů v rámci jednoho operačního systému používáme jemné řízení práv pomocí **Posix ACL**. Projekt standardně nemůže číst, zapisovat data jiného projektu. Vývojáři mají

personifikované účty a lze stanovit, k jakým projektům má daný vývojář přístup. Vývojář tedy spravuje jemu přiřazené projekty jedním účtem.

2.4 Poštovní server

- Jako základní kámen poštovních serverů využíváme **Postfix** nebo **Exim**. Poštovní server využívá pro příchozí poštu antispamovou ochranou využívající balíky **Clamav**, **Spamassassin**, **Amavis**, **Opendkim** – kombinací těchto balíků dosahujeme vysoké efektivity ochrany proti spamu. Se schránkou lze pracovat pomocí **šifrovaných** protokolů **SMTP**, **IMAP**, **POP3**.

- Pro zákazníky provozujeme poštovní servery zaměřené na odesílání velkého množství emailů, kde je potřeba doručit co nejvíce emailů v co nejkratším čase.

2.5 SQL databáze

- Máme zkušenosti s provozem obsáhlých relačních databází **Mysql**, **Mariadb**, kde zákazník vyžaduje automatické sledování dostupnosti, sledování zpoždění replik, řízení replikace, případné automatické řešení problému (automatický failover). Pro automatické řízení využíváme cluster **Corosync, Pacemaker**.

- Provozujeme i databáze typu **Postgresql**.

2.6 Non-SQL databáze

- Provozujeme key-value databázi **Memcached** u aplikací, kde je vyžadován vysoký výkon, ale nikoliv perzistence dat. Databázi **Redis** provozujeme u aplikací, kde je vyžadován výkon, perzistence dat, vysoká dostupnost. Pro automatické řízení Redis replikace využíváme cluster **Corosync, Pacemaker**.

- Pro klienty vyžadující databázi umožňující horizontální škálovatelnost, vysokou úroveň ochrany vůči výpadku, provozujeme distribuované databáze **Mongodb**.

2.7 Datová úložiště

- Pro vybudování vysoce dostupného, škálovatelného úložiště využíváme **Glusterfs, Cephfs.** Tyto nástroje nám umožňují stavět pro zákazníky modely, kde všechny servery odbavují produkční provoz a tak efektivně využíváme zdroje zákazníka.

- Pro budování lokálních úložišť, kde je kladen důraz na efektivitu, výkon nad mnoha malými soubory, využíváme **DRBD**, **NFS**, **CIFS**, **ZFS** (**ZFSonLinux**). Pro řízení blokové replikace DRBD používáme cluster **Pacemaker, Corosync**.

2.8 Vysoká dostupnost a replikace dat

- Klienti vyžadují pro své kritické aplikace vysokou ochranu vůči výpadku. Aplikace chráníme pomocí různých modelů vysoké dostupnosti, zohledňujeme nároky na ochranu, výkon, škálovatelnost.
- Základním pilířem vysoké dostupnosti je replikace. Preferujeme aplikační replikace, která jsou dostupná u nástrojů jako redis, mysql, mongodb, riak. Lze využít i datovou replikaci na úrovni souborů, kterou plní nástroje glusterfs, cephfs. Univerzální datovou replikaci na úrovni bloků zprovozníme nástrojem drbd.
- Přístup k exkluzivním prostředkům řídíme pomocí corosync/pacemaker clusteru. Jedná se o plně distribuovaný nástroj, který vyhodnocuje nastavenou politiku řízení služeb a dle aktuální situace provádí změny.
- Zátěž distribuujeme pomocí nástrojů haproxy, varnish či nginx.

2.9 Virtualizace

- Pomocí hypervisorů **KVM, XEN** budujeme virtualizační řešení pro naše zákazníky. Využíváme primárně režimu PVHVM, případně PV, kde dosahujeme vysoké výkonnosti a těžíme z kooperace hypervisoru a virtualizovaného systému. Jsme schopni navyšovat, snižovat počet procesorů, paměti, diskové kapacity za běhu systému, tedy bez nutnosti restartovat virtualizovaný systém. Námi používané hypervisory zákazníka neomezují v max. počtu procesorů, pamětí či úložiště na virtuální server.

- V prostředí, kde je třeba oddělit výpočetní prostředky různých služeb na úrovni jednoho operačního systému, využíváme kontejnerové virtualizace **LXC.** Kontejnery se vyznačují vysokou efektivitou využití výpočetních prostředků, ale oproti hypervisorům XEN, KVM nenabízí tak vysokou úroveň oddělení virtualizovaných systémů.

2.10 Monitoring

- Monitoring považujeme za klíčový prvek infrastruktury. Dle potřeby využíváme několik nástrojů. Pro sledování dostupnosti serverů, služeb využíváme **Nagios**, který máme doplněn o vlastní metody sledování vysoce dostupných služeb.

- Využití systémových prostředků sledujeme pomocí nástroje **Munin**, kde oceňujeme jeho jednoduchost a snadnost rozšíření.

- Kombinací předchozích dvou nástrojů je **Zabbix**. Služby nástroje Zabbix mohou využít vývojáři, mohou sledovat a nechat kreslit grafy postavené na aplikační metrice.

- Pro monitoring a řízení aplikačních služeb vyžadující vysokou dostupnost a používající exkluzivní zdroje využíváme cluster **Corosync, Pacemaker.** Cluster sleduje v pravidelných krátkých intervalech službu, pokud detekuje problém, dle stanovené politiky provede nápravu.

- Nástroj **Monit** využíváme pro monitoring služeb, které jsou klíčové pro běh aplikace a neběží v clusteru. Nástroj Monit má velmi dobře propracovanou detekci problému a navazující operace.

2.11 Backup

- Využíváme open source zálohovací řešení **Bacula**. Nástroj umožňuje centrálně spravovat zálohovací politiku. Díky katalogu zálohovaných dat je možné porovnat data v záloze a na zálohovaném systému, nástroj je možné použít při ověření integrity dat (např. při podezření na zneužití systému). Efektivně využíváme možnosti napojit Baculu na operace před/po odkopírováním dat, tímto snižujeme chybovost a dobu zálohování.

- U menších projektů provádíme zálohování za pomocí nástrojů postavených na protokolu Rsync **- Rdiff-backup, Rsnapshot**.

2.12 Další role

- Máme zkušenosti s provozem systému obsluhy **RabbitMQ** v clusteru (inbuild).

- Zákazníkům vyžadující škálovatelný full text engine můžeme nabídnout řešení postavené na enginu **Sphinx** či **Elastic Search**.

- U početných serverových farem je vhodné nasadit centrální správu účtů postavenou na **OpenLDAP** – Single Sign On. Centrální evidence umožňuje efektivní správu uživatelských účtů a skupin, jednotné přihlašování na systémy podporující OpenLDAP či PAM.

3 Microsoft Windows

3.1 Úvod

Náš tým zdobí bohaté zkušenosti a znalosti rovněž ve světě Windows. Ochrana sítě, firewall, VPN a jiné služby lze postavit také na technologiích společnosti Microsoft, ovšem oproti komunitnímu linuxovému řešení je nákladnější (vliv licencí) a výsledek pro koncového zákazníka může být totožný. Rozdíly bývají spíše v administračním rozhraní použitého software, se kterým koncový zákazník v případě Outsourcingu ani nepřijde do styku.

Společnost Microsoft ovšem vlastní řešení, které v současnosti nemá plnohodnotné zastoupení žádným jiným konkurenčním operačním systémem, a jsou tedy špičkou v této oblasti. Jedná se o tzv. **doménu** (neboli **Active Directory** nebo také **Doménový řadič**), kdy servery nebo klientské stanice zařazené do této domény jsou centrálně spravovány přes jednu konzoli. Klientské stanice (nebo servery) je možné rozčlenit do **organizačních jednotek -** neboli skupin (např. Účtárna, Ekonomický odbor, Vrcholné vedení) a jedním zásahem do tzv. **skupinové politiky** je možno ovlivnit chování všech serverů nebo klientských stanic (např. oprávnění pro file server), které patří do dané organizační jednotky. O funkcích doménového řadiče více v kapitole „Doménový řadič a jeho funkce“.

Katalog služeb na platformě Windows je možné rozdělit do dvou základních skupin: servery a klientské stanice. Každá skupina má rozdílné zaměření.

U serverů (konkrétně Active Directory) provádíme konfiguraci způsobem, kdy uživatelé na klientských stanicích mají co nejvyšší komfort v kombinaci s nastavením vhodné bezpečnostní politiky. Servery a klientské stanice jsou dva protipóly, mezi kterými je třeba vhodnou konfigurací vybudovat komunikační most.

3.2 Active Directory a jeho funkce

Active Directory, často nazývaná jako **AD**, je velmi obsáhlá. Jedná se o implementaci adresářových služeb LDAP, vyvinutou firmou Microsoft. AD umožňuje administrátorům nastavovat politiku, instalovat programy na mnoho počítačů nebo centrálně aplikovat kritické aktualizace v celé organizační struktuře.

AD zdobí hodně funkcí, které administrátor maximálně ocení, ty nejpoužívanější jsou například:

- **Deployment software –** jedná se o nastavení jakéhokoliv programu, který umožňuje instalaci přes příkazový řádek pomocí parametrů. Můžeme nastavit například instalaci všech programů, které jsou rutinní pro zprovoznění jakékoliv klientské stanice. Na každou novou klientskou stanici je nutné např. instalovat software jako antivir, Adobe Flash Player, Acrobat Reader, nastavení automatických aktualizací atd. Nastavení tohoto deploymentu zajistí, že každý nový počítač zařazený do domény ihned po restartu nainstaluje všechny nadefinované programy. Odpadá tak rutinní zavádění počáteční instalace software. Administrátor musí pouze držet potřebné (nikoliv pouze aktuální) verze balíčků.

- **Centrální správa účtů –** zavedení nových uživatelů, aktivace nebo deaktivace účtů (při deaktivaci účtu se uživatel nebude moct přihlásit do MS Windows, tudíž ani na žádný sdílený disk, který je součástí firemní infrastruktury), vkládání uživatelů do skupin, definice uživatele v organizační struktuře společnosti, spouštění BAT skriptů (po zálohování konkrétního uživatele se spustí BAT skript, který např. může namapovat všechny sdílené disky, na které má uživatel udělená oprávnění). Nastavení takového profilu je pak shodné na všech klientských stanicích napříč společností. Nezáleží tedy na tom, na kterém PC se uživatel přihlásí, na všech PC bude mít oprávnění shodná.

- **VPN PPTP -** Point-to-Point Tunneling Protocol je způsob realizace Virtuální privátní sítě (VPN). Obvyklými náhradami za PPTP jsou Layer 2 Tunneling Protocol (L2TP) nebo IPsec. Na konci července 2012 byl ovšem prolomen šifrovací protokol MS-CHAPv2 a od té doby nelze použití PPTP VPN považovat za bezpečné. Dodnes se ovšem tento protokol pro účely nemající dopad na společnost hojně využívá.

3.3 Active Directory a jeho role

V rámci jedné zakoupené licence nám AD nabízí mimo jiné následující role:

- **DHCP SERVER -** používá se pro automatickou konfiguraci počítačů připojených do počítačové sítě. DHCP server přiděluje počítačům pomocí DHCP protokolu zejména IP adresu, masku sítě, implicitní bránu a adresu DNS serveru. Platnost přidělených údajů je omezená, proto je na počítači spuštěn DHCP klient, který jejich platnost prodlužuje.

- **DNS SERVER -** jeho hlavním úkolem a příčinou vzniku jsou vzájemné převody doménových jmen a IP adres. Později ale přibral další funkce (např. pro elektronickou poštu či IP telefonii) a slouží dnes jako distribuovaná databáze síťových informací.

- **AD CS –** Active Directory Certificate Services je role serveru, která umožňuje budovat infrastrukturu veřejných klíčů (PKI) a poskytují kryptografie s veřejným klíčem, digitální certifikáty a možností digitálního podpisu pro vaši organizaci.

- **SOUBOROVÝ SERVER –** Souborový server (**File Server, FS**) je v informatice označení pro počítač (server), který je připojen k počítačové síti a jeho hlavním úkolem je poskytovat přístup k souborům, které jsou na něm uloženy (model klient-server). Výhodou souborového serveru je centralizovaná správa, údržba, podpora sdílení dat a podobně. Je možné nastavovat kvóty pro konkrétní adresáře a omezit tak uživatele na požadovanou kapacitu. Díky souborovému serveru se vytváří tzv. „sdílené disky“, které se pak každému uživateli mohou namapovat.

- **IIS -** Internet Information Services, nebo také IIS (dříve nazvaný Internet Information Server), je softwarový webový server s kolekcí rozšiřujících modulů, vytvořený společností Microsoft pro operační systém Windows. Jedná se o nejpoužívanější webový server po serveru Apache.

- **TISKOVÝ SERVER -** Tiskový server (print server) je zařízení, které propojuje tiskárnu s klientem přes počítačovou síť. Na print server se nainstalují ovladače na všechny tiskárny ve společnosti. To má za následek velmi snadnou instalaci každé tiskárny ve společnosti na jakoukoliv klientskou stanici. Print server dokáže rozlišit ovladače také dle architektury (32/64 bit).

- **WSUS -** Windows Server Update Services je služba zajišťující aktualizaci softwaru pro operační systémy Microsoft Windows. WSUS je lokálně spravovaná alternativa ke službě Microsoft Update. Používáním služby Windows Server Update Services mohou administrátoři plně spravovat distribuci aktualizací uvolněných prostřednictvím Automatických aktualizací do počítačů ve firemní síti. V této roli je možné přesně nastavit, které aktualizace povolit a které nikoliv.

3.4 Microsoft Exchange

Microsoft Exchange Server je softwarový produkt společnosti Microsoft, který slouží k výměně e-mailových zpráv a sdílení zdrojů. Tvoří jeden ze základů portfolia Microsoftu v oblasti nabídky firemních systémů. Mezi jeho hlavní vlastnosti patří příjem a odesílání poštovních zpráv, správa kalendáře a kontaktů, sdílení veřejných složek, možnost přístupu do poštovních schránek přes webové rozhraní, přístup k systému pomocí mobilních zařízení a vlastnost datového úložiště.

Jedná se o nákladnější ekvivalent linuxového řešení, popsaného v kapitole 2.4 Poštovní server. Zatímco u linuxového řešení je využito také antispamové ochrany, zde by bylo nutné tuto ochranu zajistit dalším softwarem.

3.5 Skype for Business Server (dříve Microsoft Lync)

Aplikace **Skype for Business** (dříve známá jako **Microsoft Lync**) je online komunikátor, který se využívá interně ve společnostech mezi zaměstnanci. Jedná se o bezpečnější formu komunikace, protože veškerá komunikace probíhá na interních serverech společnosti. Pro zprovoznění je potřebný Skype for Business Server, který je licencován separátně. Pro využívání aplikace Skype for Business veřejně (tedy i mimo interní síť) je

navíc potřeba licence tzv. EDGE serveru.

3.6 Microsoft Sharepoint

Microsoft SharePoint je aplikační platforma pro web vyvinutá společností Microsoft. Poskytuje služby typu CMS (Systém pro správu obsahu) a integraci s dalšími službami. Zároveň poskytuje také prostředí pro tvorbu a chod aplikací od jiných dodavatelů. Jedná se o modulární systém, lze tedy tento systém doplnit o další moduly, např. o vytváření pracovních postupů od společnosti Nintex.

3.7 Microsoft SQL Server

Microsoft SQL Server je relační databázový a analytický systém např. pro internetové obchody, byznys a řešení datových skladů vyvinutý společností Microsoft. Jedná se opět o komerční řešení, kde je třeba zaplatit potřebnou licenci, nicméně existuje také bezplatná, omezená verze – Microsoft SQL Server Express.

Microsoft SQL je konkurenční nástroj vůči Linuxovému řešení zmíněnému v kapitole 2.5 SQL databáze.

3.8 Vysoká dostupnost a replikace dat

Na aplikacích typu Active Directory, MS Exchange nebo MS SQL je možné využít replikace dat, potažmo nastavit režim vysoké dostupnosti. Vysoká dostupnost (**HA**- **High Availability**) znamená chod dvou a více instancí na jednu službu.

Tedy například doménový řadič (případně Exchange nebo SQL) poběží na dvou geograficky oddělených serverech. Ve chvíli, kdy primární server vypoví službu, automaticky přebírá funkci server záložní. Tyto funkce je možné využít při zakoupení potřebného množství licencí u požadované služby.

3.9 Klientské stanice

U klientských stanic provádíme pravidelně údržbu softwaru ve smyslu aktualizací. Dále se soustředíme na licence používaného software, tedy kontrolu expirace např. u antivirových programů.

U notebooků, kde je vyšší riziko ztráty/krádeže, doporučujeme šifrování celého pevného disku. Výsledkem je snížení rizika zneužití dat při krádeži notebooku.

Naším cílem je udržovat všechny klientské stanice v takové kondici, aby uživatel nebyl omezen pomalým chodem a nestabilitou operačního systému.

Staráme se o software i hardware. Homogennost prostředí má zásadní vliv na efektivitu řešení případných potíží. Snažíme se tedy po dohodě s klientem dodávat klientské stanice od jednoho výrobce.

EPOFIS IT

EPOFIS IT s.r.o.

Nové sady 988/2, Staré Brno
602 00 Brno
info@epofis-it.cz
www.epofis-it.cz