Posouzení síťového uspořádání společnosti FIRMA, spol. s r.o.

Popis uspořádání

Síť řídí router Mikrotik RB750G, který integruje role firewallu, vícenásobného NAT a IPSec tunelu do druhé pobočky. Konektivitu zajišťuje firma PODA (8/4MBit) Jednotlivé sítě:

- DMZ – k této síti jsou připojeny všechny (virtuální) servery vyžadující selektivní přístup zvenčí
- LAN – do této sítě jsou zapojeny všechny ostatní (virtuální)servery, disková úložiště, IP telefony, WiFi AP, notebooky, stanice, IP kamery, VPN klienti a záložní server
- OpenVPN – VLAN na které je poskytován VPN přístup (řídí vyhrazený virtuální server)
- EXT – jedná se o VLAN pro externisty, kteří nesmí mít přístup do lokální sítě.

Servery jsou většinou provozovány na VMWare ESXi platformě, která využívá sdíleného síťového diskového úložiště na SCSI protokolu (SAN). Výjimkou je Windows databázový server, který je nasazen z historických důvodů.

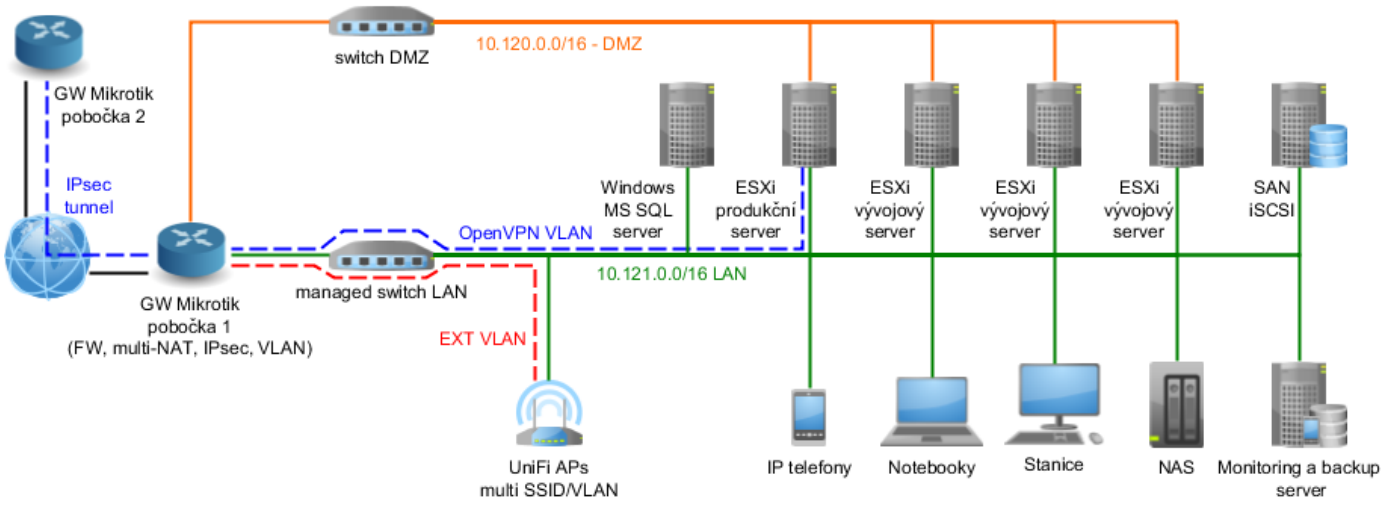
Virtuální servery jsou provozovány na jednotlivých VMWare ESXi serverech

- Chybí zde možnost live migrace virtuálního serveru mezi servery (licence na tuto možnost je finančně nákladná)
- Každý virtuální server je zapojen buď do DMZ, nebo do LAN sítě (výjimku tvoří OpenVPN server)

Bezdrátové pokrytí zajišťují centrálně spravované jednotky Ubiquiti UniFi. Jednotky poskytují dvě nezávislé WiFi sítě:

- FIRMA_LAN – přístup do lokální sítě
- FIRMA_EXT – přístup do oddělené sítě pro externisty, síť poskytuje pouze konektivitu do internetu

Mapa sítě



Zálohování

NAS

Na síťové úložiště SYNOLOGY jsou odkládány aplikační zálohy, to znamená, že se zde zálohují kritická data přímo z virtuálních serverů. Jedná se o databáze a zálohy konfigurací kritických aplikací (například webů společnosti a jejich klientů). Kromě zálohování slouží NAS i jako uživatelské sdílené úložiště pro všechny zaměstnance.

Zálohování NASu je řešeno dvěma způsoby

1. Je k němu pravidelně připojován externí USB HDD – Externí záloha dat popsaná dále.
2. IT správce jednou měsíčně v NAS fyzicky vymění jeden HDD, který se díky RAID1 automaticky synchronizuje.

Záložní server

Server je umístěn v kanceláři, jedná se bigtower který obsahuje dvě disková RAID pole. Kromě zálohování obstarává také monitoring celé sítě systémem Zabbix.

1. pole představuje iSCSI target na které jsou denně (v noci) odlévány zálohy ze SAN (formou VDMK obrazů disků virtuálních serverů a VMX konfiguračních souborů virtuálních serverů). Dále je na tomto poli sdílený prostor pro odkládání uživatelských záloh (zálohovat si zde mohou sami zaměstnanci prostřednictvím SAMBA protokolu).
2. pole obsahuje historii záloh virtuálních serverů z pole prvního. Jsou zde uloženy týdenní, 2týdenní, 3týdenní, měsíční a 2měsíční zálohy.

Externí záloha dat

Externí záloha dat probíhá pouze z NAS formou zálohy na externí HDD jednou týdně. Zálohu si nosí vedení domů. Takto zálohována jsou pouze nejkritičtější data.

Monitoring stavu sítě

Sledování stavu sítě je řešeno platformou Zabbix. Využívá se jak pasivního, tak aktivního monitoringu. Sledovány jsou aktivní prvky sítě, virtualizační platformy a virtuální servery. V případě problémů Zabbix odesílá e-mail upozornění a v případě kritických událostí může použít i SMS prostřednictvím mobilního telefonu připojeného k záložnímu serveru. Dále je možné monitorovat fyzický stav DELL serverů pomocí rozhraní iDRAC Enerprise (k dispozici je log systému, teplotní senzory, sledování napájení a vzdálená grafická konzole).

Pasivní monitoring

- Ping na servery
- Dostupnost SSH
- Funkčnost domén
- Funkčnost IPsec propojení mezi pobočkami

Aktivní monitoring

- Health status ESXi serverů
- Sledování volného místa na discích virtuálních serverů

Krizové scénáře

Výpadek konektivity do internetu - nepokryto

Připojení do internetu je od poskytovatele PODA, jedná se o stabilní službu poskytovanou standardně po optické lince. Nicméně není pokryt případný výpadek linky. V závislosti na výši SLA by bylo vhodné zřídit záložní připojení k internetu využívající jinou technologii/trasu (například VDSL).

Krátký výpadek elektřiny (do cca 15 minut) - pokryto

Výpadek pokryjí UPS, které jsou umístěny u všech serverů a klíčových síťových prvků.

Dlouhý výpadek elektřiny (hodina a více) - nepokryto

Tento případ není pokryt, je třeba zvážit riziko a jeho dopady (například při předem plánovaném výpadku dodávky elektřiny). Možné řešení je dočasný přesun kritických služeb (vysoká SLA) na jiný hosting, nebo pořízení dieselagregátu.

HW porucha SAN – částečně pokryto

SAN může být při poruše plně zastoupen záložním serverem, který obsahuje noční zálohu všech virtuálních serverů. Je třeba zvážit, zda je noční záloha v případě krizového scénáře akceptovatelná a jestli je výkon diskového pole záložního serveru dostačující.

Porucha routeru Mikrotik - pokryto

Pro případ poruchy je připraven záložní router, do kterého je možné velmi rychle obnovit konfiguraci ze záložního souboru.

Výpadek jednoho z ESXi serverů - pokryto

V případě poruchy jednoho z ESXi serverů by nebyl problém dočasně virtuální servery migrovat na zbylé ESXi servery. Diskové úložiště je umístěno externě, migrace by trvala maximálně desítky minut. Vzhledem k výkonové rezervě ESXi serverů, by výpadek nebyl citelný.

Zásah blesku – částečně pokryto

Závažnost problémů při případném úderu blesku (či jinak způsobeném výrazném přepětí v rozvodné síti) nelze předem posoudit. Všechny servery a primární síťové prvky jsou připojeny přes UPS (zajišťuje přepěťovou ochranu), to znamená, že klíčové prvky sítě jsou chráněny adekvátně.
V extrémním případě se může přepětí dostat do sítě z nechráněných stanic/notebooků (velmi malá pravděpodobnost).

Porucha záložního serveru - pokryto

Chod celé infrastruktury není ohrožen, ale je nutná velmi rychlá obnova záložního serveru (maximálně v řádu dní), zejména z důvodu nefunkčnosti monitoringu sítě.

Externí záloha dat – částečně pokryto

Externě jsou zálohována pouze klíčová data z NAS (aplikační zálohy a DB), je třeba zvážit, jestli jsou tyto zálohy dostatečné. Vzhledem k rychlosti připojení nelze zálohovat velké objemy dat on-line, ale nabízí se možnost zálohování na externí disky a odnášet data mimo firmu.

Doporučená opatření

- Zajištění sekundární konektivity do internetu od jiného poskytovatele (připojení jinou, nezávislou trasou)
- Externí záloha dat pokrývající veškerá kritická data. Vzhledem k pomalé konektivitě do internetu se nabízí dvě řešení:
    - Záloha na externí disk (prodávají se až 3TB varianty) obsahující šifrovaný kontejner se zálohami. Tento disk by se stejně jako doposud odnášel mimo firmu. Připojení bych doporučoval formou eSATA, nebo USB 3.0. Rozhodně doporučuji zálohovat kompletní sadu dat, nikoliv pouze NAS (externí disk by se připojoval přímo k záložnímu serveru, například pomocí USB 3.0).
    - Při zakoupení lepší konektivity do internetu zálohovat kritická data online (například pomocí protokolu rsync do šifrovaného kontejneru na hostovaném virtuálním serveru)
- Pravidelné (kvartální/roční) testování funkčnosti záloh
- Vytvoření protokolu o zálohování pro externí zálohy, kde by se evidovalo, kdo a kdy zálohoval
- Odstranění nekoncepčnosti zálohování (odstavit NAS jakožto místo pro zálohu dat a zálohovat pouze na záložní server)
- Připojení NAS do adresářové služby OpenLDAP, aby bylo možné centrálně řídit přístupová oprávnění.
- Nezálohovat NAS fyzickou výměnou disku v poli RAID1, je to potenciálně nebezpečné
- Vytvoření krizového scénáře pro dlouhodobý výpadek energie, aby tento problém bylo možné řešit
- Nastavení rezervace zdrojů pro jednotlivé virtuální servery dle jejich priority. Na ESXi to lze konfigurovat tak, aby jeden virtuální server neměl možnost zahltit celý ESXi server a zároveň aby každý virtuální server měl garantované minimum prostředků.
- Implementace RADIUS serveru pro WiFi připojení k LAN síti, prý již v řešení.

V Brně dne: 9. 11. 2012
Zpracoval: Mgr. Radek Šembera