Ústav zemědělské ekonomiky a informací

Rámcový popis stávajícího stavu technické infrastruktury

Obsah

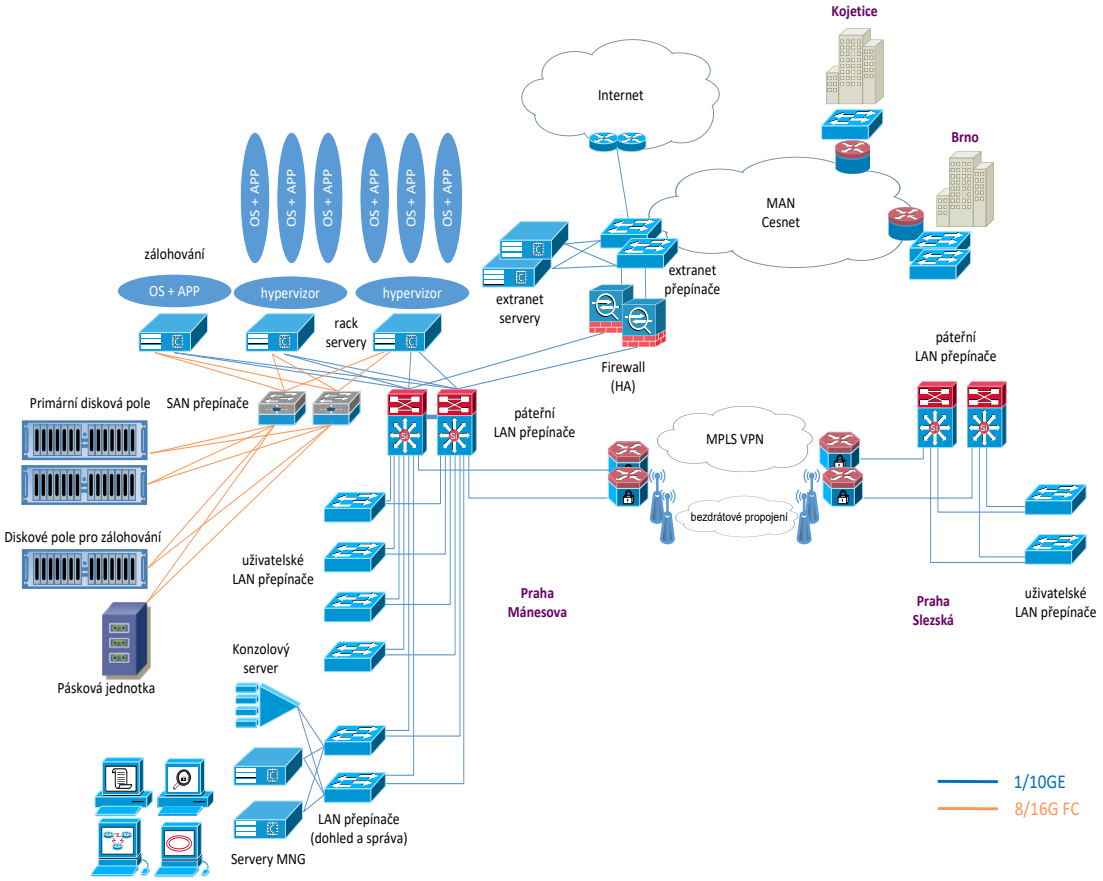
1 MANAŽERSKÝ SOUHRN

Účelem tohoto dokumentu je rámcový popis prostředí ÚZEI v návaznosti na již vypracovanou a schválenou IT Architekturu.

V dokumentu je zohledněn jak současný, tak i budoucí předpokládaný stav s výhledem na požadavky na rozšíření výpočetních a datových kapacit. Nejedná se pouze o rozšíření, ale také o návrh nových funkcionalit dle moderních trendů v daných IT oblastech.

2 STÁVAJÍCÍ ICT ARCHITEKTURA

Současný stav IT architektury je zobrazen na následujícím obrázku.



Obrázek 1 Celková IT architektura

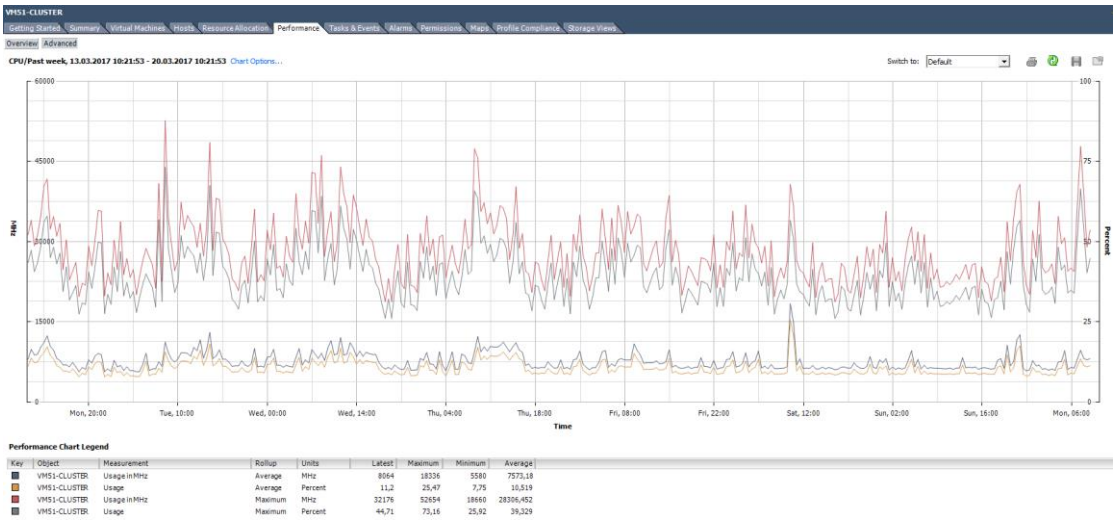
Jedním z hlavních vstupů pro celkový budoucí návrh IT architektury je také budoucí výhled ÚZEI při plánování nasazení nových aplikací případně nárůstu požadované úložné kapacity pro digitální dokumenty. Tyto budoucí požadavky mají přímý dopad na dimenzování HW zdrojů. Navržená architektura by měla být plně flexibilní a rozšiřitelná do budoucna. Budoucí požadavky z pohledu zdrojů se budou týkat zejména těchto oblastí:

- Požadavky na úložiště dat – kapacita, výkonnost, návaznost na zálohování a archivaci
- Požadavky na výpočetní výkon – CPU, RAM, návaznost na režim vysoké dostupnosti
- Požadavky na přenosovou kapacitu – odezva aplikací, návaznost zejména na přenosovou kapacitu směrem do sítě internet anebo na další lokality ÚZEI

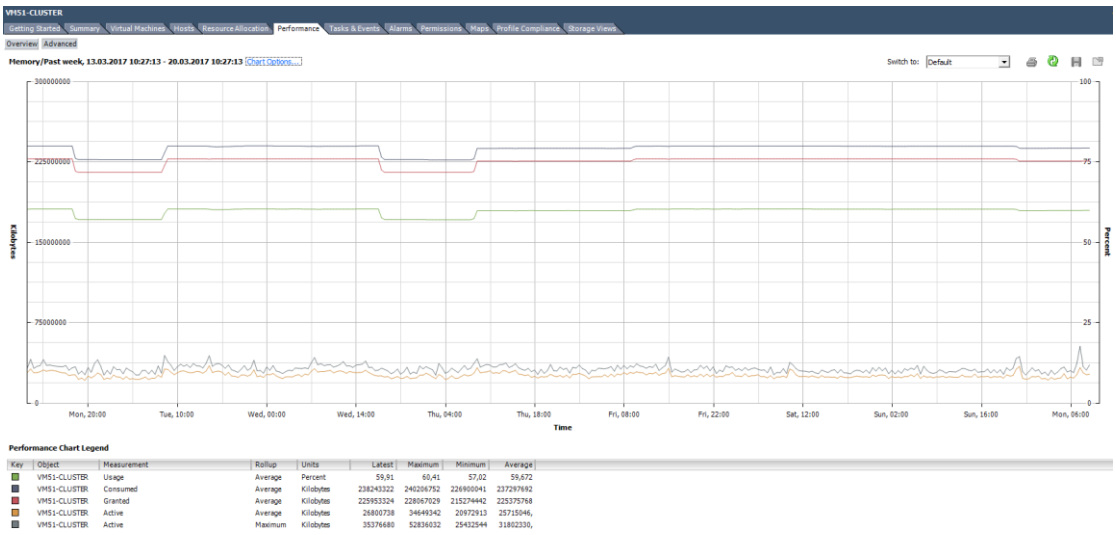
Na následujících obrázcích jsou zobrazeny grafy využití CPU a RAM v clusteru (3 servery). Statistiky zobrazují využití zdrojů v jednotlivé dny v týdnu. Monitoring se prováděl týden.

Základní parametry serverů v clusteru jsou následující:

- 3 x 12 CPU x 1,99GHz
- 3 x 128 GB RAM



Obrázek 2 Využití CPU v clusteru ÚZEI



Obrázek 3 Využití RAM v clusteru ÚZEI

V následující tabulce jsou uvedeny informace o maximálním využití CPU a RAM na jednotlivých server v clusteru v období týdenního sledováni.

	Max CPU usage:	Max RAM usage:
Host 1	38.05 %	53 %
	9 132 MHz	
Host 2	57.77 %	61 %
	13 864 MHz	
Host 2	86.55 %	66 %
	20 772 MHz	

Tabulka 1 Maximální využití zdroje jednotlivých serverů

V současnosti nelze zcela jednoznačně určit všechny předpokládané budoucí požadavky na výpočetní výkon v ÚZEI. Při dimenzování celé IT architektury na dvojnásobnou aktuální kapacitu bude i tato kapacity dostačující pro budoucí požadavky.

Z pohledu rozvoje ÚZEI očekává zajištění těchto klíčových služeb:

- DMS
- Spisovou službu
- Skenování knih v knihovně s metadaty
- digitální knihovna Kramerius

Kritickým místem je zejména predikování požadavků na diskovou kapacitu:

- Současné nároky jsou 50 TB, včetně alokace 200 GB na centrálním úložišti pro každého ze 170 uživatelů
- Roční přírůstek dat je cca 16 TB
- FADN infrastruktura disponuje kapacitou cca 5 TB

2.1 Východiska pro funkční celky

Následující kapitoly se věnují detailněji jednotlivým funkčním celkům architektury ICT. Vychází z předchozího dokumentu *Návrh architektury ICT prostředí UZEI* verze 2.0 ze dne 12.12.2016. Tyto kapitoly shrnují nejdůležitější body, které je nutné zohlednit v detailním technické návrhu.

2.1.1 Síťová infrastruktura

- Zajištění vysoké dostupnosti HA na L3 prvcích v Datacentru Mánesova. Nahradit nevyhovující 1Gbit propojení těchto prvků na přístupové switche a použít technologii 10Gbit Ethernet.

- Nahrazení stávajícího L2 stacku přístupových switchů za switche s podporou stacku na 10Gbit. Podpora PoE, IPv6, 802.1Q minimálně 4x10Gbit a 48x1Gbit o celkové kapacitě L2 minimálně 384 1Gbit portů a 32 10Gbit portů.

- Integrace infrastrukturních technologií sítě FADN na přístupové switche UZEI. Vyřazení nevyužitých IBM přístupových switchů a zajištění vysoké dostupnosti HA.

- Zřízení zabezpečené bezdrátové sítě s centrálním controllerem pro řízení a plánování celé bezdrátové sítě z jednoho místa, jedním nástrojem. Technologie 2,4GHz a 5GHz 802.11AC. Autentifikace přístupu do produkční sítě přes jednotnou správu identit (RADIUS nebo LDAP/AD). Použití captive portal pro Hostovskou síť oddělenou od produkční sítě. Zajištění monitorování a logování provozu bezdrátové sítě. Aplikace bezpečnostních technologií proti standartním útokům na bezdrátové sítě. (Rogue access point, man in the middle apod.)

- Uskutečnění optického spoje mezi lokalitou Mánesova a Slezská na technologiích T-Mobile a ponechání si záložní bezdrátové propojení na technologii SIKLU. Vyřadit bezdrátový spoj PLUTO.

- Vytvoření plánu na implementaci IPv6 a možnost budoucí realizace nasazení IPv6.

2.1.2 Perimetr s bezpečnost

- Nahrazení stávajících DMZ switchů s technologií Fast Ethernet za Gigabitové switche

- Nutná výměna stávajících nedostačujících UTM Fortigate 100D za výkonnější zařízení. Nasazení bezpečnostních pravidel zejména SSL inspekce.

- Revize firewallových pravidel, přístupů a VPN účtů. Implementace jednotné správy identit (RADIUS Server nebo LDAP) a propojení SSL-VPN a přístupových účtů s Active Directory.

- Revize a nasazení bezpečnostních funkcí a aplikace na firewallová pravidla (antivir, webfiltering, aplikační kontrola, intrusion prevention systém, DoS). Zřízení proxy a SSL inspekce pro šifrovaný provoz HTTPS, FTPS, SMTPS. Nasazení SSL certifikátu pro inspekci šifrovaného provozu.

- Revize zabezpečení emailové komunikace pomocí zařízení (emailové brány) pro zajištění účinné antispamové a antivirové kontroly příchozí a odchozí pošty.

- Realizace řešení proti Zero-Day útokům, Ransomware a dalšího škodlivého mallware v reálném čase na hardwarové platformě.

- Zajištění dlouhodobějšího ukládání logů síťového provozu s možností následné analýzy a výstupního reportingu. Zřízení Vulnerability managementu pro detekci zranitelnosti systému a předcházení bezpečnostním incidentům.

- Zajištění komunikace na protokolu IPv6 současně s IPv4. Nasazení současně pro WAN i pro vnitřní sítě.

2.1.3 Serverová infrastruktura a datové uložiště

- Konsolidace serverové infrastruktury UZEI a FADN na jednu platformu, při zachování požadavku na logické oddělení a nezávislost obou systémů s možností jednoduché migrace na samostatnou platformu v případě vzniku tohoto požadavku. Fyzické oddělení obou systémů je značně neefektivní a neúměrně zvyšuje nároky na záložní zdroje UPS, síťovou a SAN infrastrukturu a administraci.

- Pořízení serverů v zapojení ve vysoké dostupnosti HA jako Hypervizory pro virtualizační platformu (Hyper-V nebo VM-ware). Nahrazující současné 3 vmware hypervisory pro UZEI a 2 vmware hypervizory pro FADN.

- Možné vyřazení 3 VM-ware hostů z infrastruktury UZEI, jednoho standalone serveru FJS siemens spisová služba, 2 vmware hostů z infrastruktury FADN.

- Produkční datové úložiště Storwize V7000 je po 4letém provozu na konci své morální životnosti a prodloužení HW podpory je neefektivní. Datové úložiště je navíc značně poddimenzované a slouží primárně pouze pro serverový provoz a jejich aplikace. Nemá dostatečnou kapacitu na ukládání produkčních uživatelských dat. Ty jsou nechráněná a nezálohovaná na lokálních počítačích uživatelů, popřípadě nevyhovujících NAS zařízeních.

- Zálohovací datové úložiště FiberCAT je již řadu let out of sale i out of support a je osazeno nepodporovanými disky. Samotné pole vykazuje chyby jednoho controlleru a jeho další používání v infrastruktuře je nemyslitelné. Vzhledem k plnění funkce zálohování, doporučujeme nahradit stávající datové úložiště za úložiště s nižšími výkonnostními nároky bez SSD cash a rychlých SAS nebo SSD disky, naopak s vysokou hrubou kapacitou 150TB na levnějších NLSAS nebo SATA discích.

2.1.4 SAN

- Architektura SAN sítě pro zajištění vysoké spolehlivosti používá koncept dvou naprosto nezávislých SAN infrastruktur (SAN fabric A, SAN fabric B). Jednotlivé servery a systémy pro ukládání dat jsou pak připojeny na obě SAN infrastruktury. Každá SAN infrastruktura je tvořena jedním fiber channel přepínačem, který obsahuje min. 48 FC portů s volitelnou rychlostí v rozmezí 4G – 16G a s podporou virtualizačních technologií, které umožňují členit jednu fyzickou SAN infrastrukturu na několik logických – např. technologie VSAN (Virtual SAN) a s podporou technologií NPIV (N-Port Interface Virtualization) umožňujících snadnou a škálovatelnou integraci fyzických a virtualizovaných serverů do SAN infrastruktury

- Konsolidace serverové infrastruktury UZEI a FADN na jednu platformu s sebou přinese i konsolidaci SAN infrastruktury. Ze současných dvou HA řešení na jedno.

- Stávající SAN infrastruktura UZEI, má již nyní dostatečný počet portů a licencí na provoz obou systémů současně. V případě zvolení levnějšího řešení nové SAN infrastruktury na 8Gbit platformě by mohlo být současné řešení, při zajištění HW podpory výrobce, zachováno. V případě upgrade SAN infrastruktury na platformu 16Gbps je nutné pořídit dva SAN switche s podporou 16Gbps.

2.1.5 Záložní zdroje a systém napájení

- Stávající záložní zdroje napájení jsou v havarijním stavu a hrozí bezprostřední nebezpečí ztráty dat, poškození HW. Baterie v záložních zdrojích neprochází pravidelnou údržbou a nejsou ani jinak kontrolovány. Všechny baterie v záložních zdrojích v Datacentra Mánesova jsou bez několikaleté údržby a hrozí tak riziko poruchy záložního zdroje.

- Záložní zdroje nejsou vybaveny síťovým managementem a jsou schopny zajistit napájení infrastruktury, pouze při krátkodobých výpadcích v řádu několika minut. Po vyčerpání kapacity záložních zdrojů, přeruší dodávku elektrické energie do infrastruktury bez ukončení rozpracovaných transakcí, či uložení dat. Nekorektní ukončení běžících systémů může způsobit jejich nevratné poškození, nebo dokonce poškození HW.

- Rozdělení kapacit záložních zdrojů do několika samostatných UPS je neefektivní a ztěžuje tak management řízeného vypínání dle priority systému a velikosti zátěže.

- Absence monitoringu (managementu) těchto zařízení znemožňuje administrátorům rozpoznat, když dojde k výpadku elektrické energie a nemůžou tak ani reagovat na vzniklou situaci případným vzdáleným zásahem neautomatického řízeného vypnutí systémů.

- Běžné managementy záložních napájecích zdrojů zajišťují kromě napájení a automatického řízeného vypínání a zapínání, také monitorování teploty v Datacentru a v závislosti na ni reagovat. Upozorněním administrátora zasláním emailu, nebo opět řízeného vypnutí vybraných technologií, aby nedošlo k jejich poškození. Tato funkce může varovat administrátory před poruchou klimatizace, opomenutí opětovného zapnutí klimatizace při profylaxi a předejít tak poškození HW.

- Doporučujeme pořízení třífázové UPS s management modulem. Instalaci management serveru pro obsluhu. Zařazení všech zařízení pod jednotnou správu do skupin dle priorit a zátěže. Určení identit pro systém včasného varování a správce. Provázání na stávající PRTG monitoring.

- V závislosti na změny v infrastruktuře a vyřazení, nebo naopak pořízení nových aktivních prvků a serverů, doporučeno provést revizi elektrické instalace, PDU a kabeláže.

2.1.6 Systém zálohování

- Současný systém VeeamBackup and Replication, je zaměřen na virtuální prostředí s podporou souborové zálohy na pásková média. Pro současný i plánovaný systém je vhodnou volbou z důvodu nízkých provozních nákladů a snadnou administrací. Stejně jako servery UZEI, tak i servery FADN jsou na virtuální platformě je možné tento systém použít i pro zálohování FADN. Není nutné udržovat dva zálohovací systémy a lze tak opustit nákladný IBM Tivoli Storage Manager.

- Plánovaný rozvoj produkčního prostředí a navýšení kapacity produkčního datového úložiště na 100TB z důvodu převedení uživatelských dat na File-Server, vzniknou ekvivalentní nároky na zálohovací systém. Primární zálohovací datové úložiště s kapacitou 150TB na levnějších NLSAS nebo SATA discích a konektivita HBA 2x8Gbps na každý controller je plně vyhovující.

- Naopak další využití datové úložiště FiberCAT je nemyslitelné z důvodu absence podpory, použití nepodporovaných disků, nízkou kapacitou, 4Gbps HBA a častými chyby jednoho controlleru.

- Sekundární datové úložiště pro ukládání kopie záloh a měsíčních záloh je vhodné vytvořit na levnějších zařízeních typu NAS nicméně s dostatečnou hrubou kapacitou 150 TB a 8Gbit FC HBA nebo 10Gbit Ethernet konektivitou. Tato zařízení jsou cenově mnohem dostupnější a vzhledem k využití jako sekundární datové úložiště zcela vyhovující.

- Při konsolidaci infrastruktury FADN a UZEI na jednu platformu, nebude již potřeba druhé páskové knihovny původně ukládající data pro FADN. Pásková knihovna, která je součástí zálohování pro UZEI, slouží pro ukládání dlouhodobých záloh a archivu. Tuto činnost převezme sekundární datové úložiště a obě páskové knihovny bude možné dočasně využít pro offside zálohy. Hrubá kapacita jedné knihovny je 53 TB při použití LTO6 médií, je tudíž nutné použít obě knihovny pro zálohu 100 TB (hrubé kapacity) produkčního prostředí. V případě budoucího dalšího navýšení produkčního datového úložiště doporučujeme již pořídit jednu páskovou knihovnu s dostatečnou kapacitou dle velikosti produkčních dat.

- Doporučujeme zřídit postupy a proškolení odpovědné osoby pro systém zálohování a nakládání s archivními médii a jejich případnou obnovu.

- Doporučujeme zavést systém automatického upozornění do systému dohledu a správy, nejen na samotné HW komponenty systému, ale také na události zálohovacího systému, jako jsou chybová a varovná hlášení systému na různé incidenty (nedokončené zálohovací úlohy, nefunkční úlohy, odebrání médií k archivaci apod.)

- V současné době probíhá zálohování veškeré infrastruktury na datové úložiště FiberCAT, které je z důvodu absence podpory, použití nepodporovaných disků, nízkou kapacitou, 4Gbps HBA a častými chyby jednoho controlleru, velmi rizikovým úložištěm. Proto se pořizují archivní zálohy na pásková média jako sekundární zálohy s RPO 1 měsíc. Převážná většina uživatelských dat je uložena na lokálních discích uživatelů a jsou tudíž úplně bez ochrany. Hrozí tak bezprostřední nebezpečí ztráty dat!

2.1.7 Systémy dohledu a správy

- Systém dohledu a správy je provozován na výrobcem nepodporovaném serveru FJS Primergy RX100 S5. Tento server je již dlouhodobě nevyhovující, a i přes nedávno provedenou profylaxi, kdy byli odstraněny závažné chyby a upgrade operační paměti, je nutné tento server nahradit novým.

- Stávající server je provozovaný na operačním systému Microsoft Windows Server 2008R2 a slouží mimo jiné také jako svědek pro Exchange Cluster. Také míchání rolí je zcela nepřijatelné.

- V současnosti provozovaný monitorovací software PRTG má zakoupenou doživotní licenci Network Monitor 1000. Ta obsahuje 1000 sond, která je pro současnou i budoucí infrastrukturu dostačující. Limitující je absence podpory a nemožnost využívat nejnovější verze a funkcionality.

- Po upgrade software doporučujeme nastavit SNMP trap a sběr syslog zpráv, který v současné verzi není plně podporován.

- V současné době je monitorovací systém funkční a používán na detekci incidentů v síti a infrastruktuře. Výhodou je vzdálený monitoring a reporting na mobilní zařízení, spolehlivost, dobrá uživatelská přístupnost a ovládání. Doporučujeme zachovat stávající software a dokoupit podpory výrobce.