



Příloha ZD06 – Popis stávajícího stavu centrální sdílené TI

k č. j. ČÚZK-10685/2020

1 Obsah

2.	Technologická infrastruktura	3
2.1	Logické uspořádání.....	3
2.2	Síťová vrstva	3
1.1.	Popis hardware.....	4
2.2.1	Databázová vrstva	7
2.2.2	Servery pro virtuální prostředí aplikační vrstvy	7
2.2.3	Datová vrstva.....	7
2.2.4	Databázové servery	8
2.2.5	Aplikační servery	8
2.3	Referenční, školicí a vývojové prostředí.....	8
2.4	Software	8

2 Technologická infrastruktura

2.1 Logické uspořádání

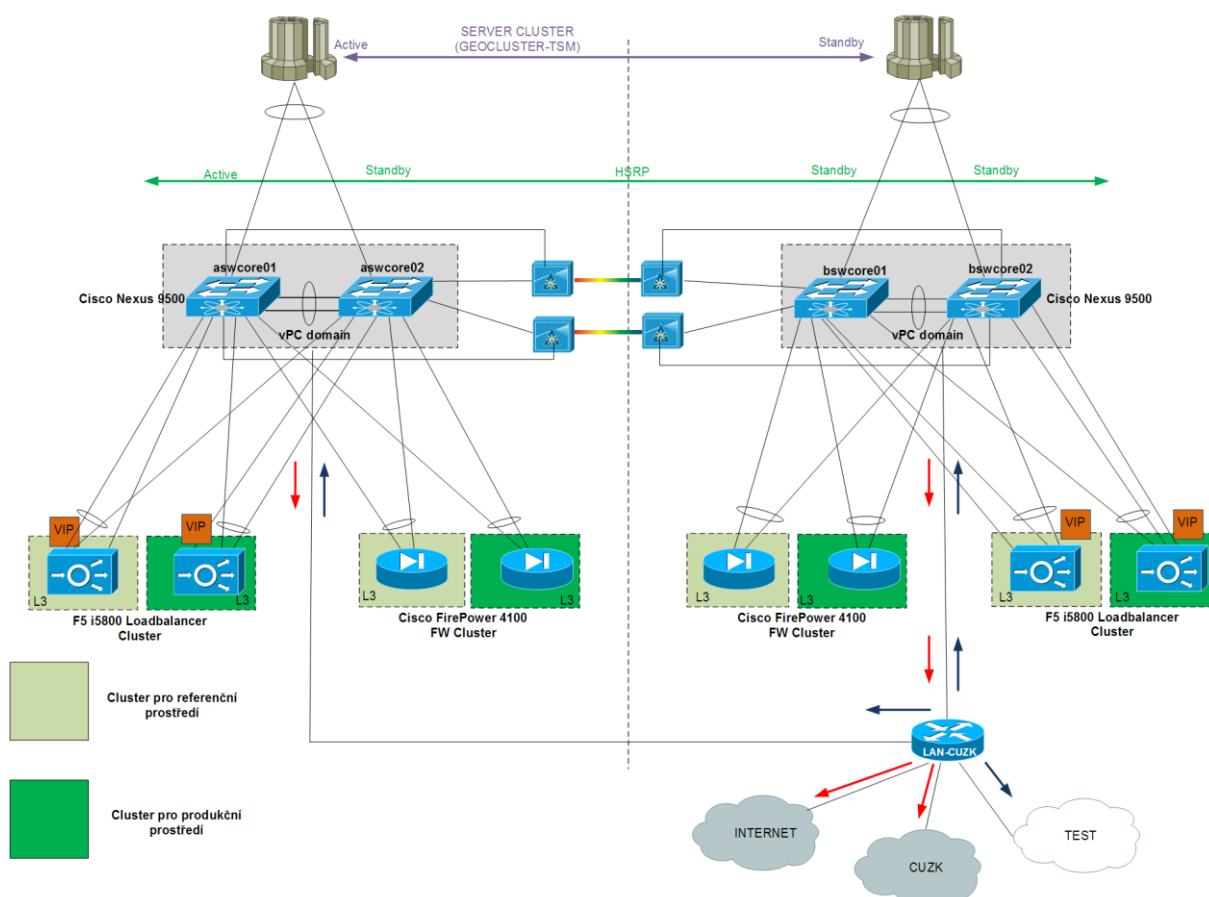
Systémy jsou provozovány ve dvou datových centrech. První z nich (dále označováno jako produkční) je umístěno v housingovém centru, druhé (dále označované jako záložní) v budově Zadavatele. Architektura je realizována jako vícevrstvá s aplikačním serverem/clusterem, který komunikuje s DB serverem/clusterem (Extended Oracle RAC). RAC cluster má přístup do SAN v obou lokalitách, k databázovým souborům se přistupuje prostřednictvím Oracle ASM, které zároveň zajišťuje synchronní replikaci dat mezi lokalitami. Nad aplikační a prezentační vrstvou je vrstva Content Switchů, které zajišťují rozdělování požadavků na všechny aplikační a prezentační severy v obou lokalitách.

Referenční a školící prostředí jsou kopií produkčního prostředí, ale mají určitá omezení, např. poloviční počet aplikačních serverů apod. Referenční a školící prostředí jsou oddělena od produkčního prostředí. Infrastruktura LAN, SAN, zálohování, datových úložišť a databázových serverů je sdílená s dalšími IS Zadavatele.

2.2 Síťová vrstva

Využívá architektury dvojité sítě GB Ethernet, zabezpečené bezpečnostními branami (firewall) a s ohledem na nároky na vyšší objemy přenášených dat redundantní strukturu SAN pro připojení subsystémů disků a pásek. Potřebné propojení lokalit po optice je realizováno redundantními DWDM zařízeními. Na globální úrovni je přístup řízen redundantními content switchi. Síťová infrastruktura včetně SAN a DWDM je z hlediska kompatibility kompletně založena na technologiích firmy CISCO.

T-Systems/Produkční lokalita CUZK/Záložní lokalita



Obrázek 1 – obecné schéma LAN a SAN propojení datových center

Základem je LAN infrastruktura, kterou tvoří dva přepínače Cisco Nexus 9500 v rámci jedné lokality, vybavené porty 10G a 1G. Firewally jsou realizovány prostřednictvím zařízení Cisco Firepower 4100, load balancing pomocí prvků F5 Big-IP i5800. V obou případech jsou prvky zapojeny v clusterovém režimu, po jednom členu clusteru v každé lokalitě.

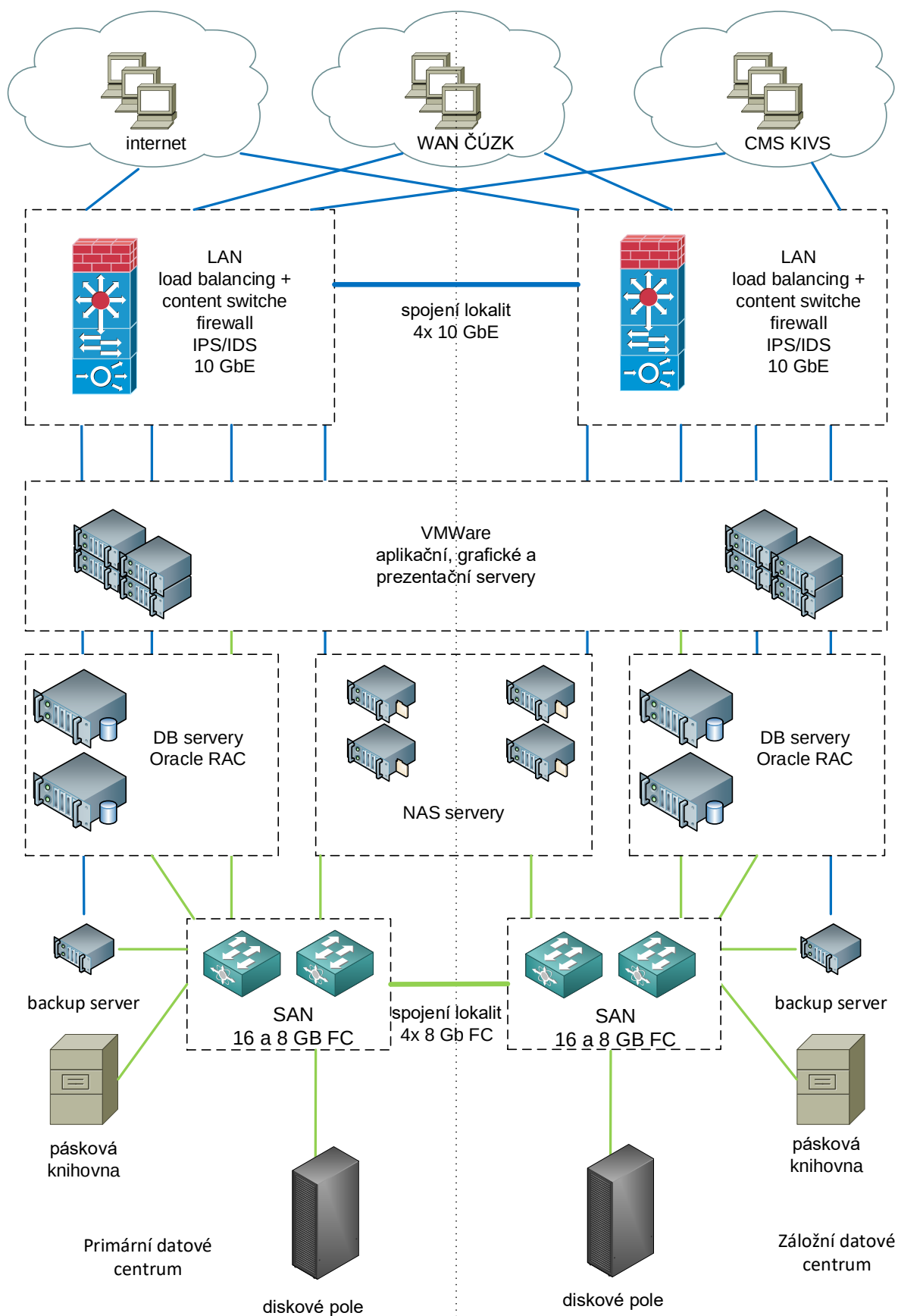
Vzhledem k velké vzdálenosti obou lokalit zajišťuje optický páteřní propoj zařízení Cisco NCS2000. Na každé lokalitě jsou dvě zařízení pro vysokou dostupnost optického páteřního propoje (celkem tedy 2 trasy, každá s kapacitou 4x 10 Gb Eth. A 4x 8 Gb FC).

K internetu je interní síť připojena z centra prostřednictvím dvou linek nezávislých poskytovatelů a třetím propojem do peeringového uzlu NIX.CZ. Pro připojení k Základním registrům, některým agentovým systémům státní správy a přístup interních uživatelů na internet se využívá linky do propojovací sítě CMS KIVS.

2.3 Popis hardware

Primární i záložní centrum jsou založena na stejných komponentech, záložní datové centrum poskytuje přibližně 2/3 výkonu produkčního datového centra. Klíčová architektura (databázové servery) je provozována na serverech IBM Power s RISC procesory POWER8 (pro rok 2021 naplánován upgrade na Power9). Aplikační a prezentační vrstva jsou kompletně virtualizované v prostředí VMWare. Architektura datového centra je flexibilní, a to především v oblasti možného dynamického přerozdělování zdrojů u databázové a aplikační vrstvy podle skutečné potřeby pomocí virtualizačních

technologií a také v oblasti rozšiřitelnosti systému, a to jak horizontální, tak vertikální. Všechny HW komponenty jsou sdíleny s dalšími centrálními systémy.



Obrázek 2 – obecné HW uspořádání datových center

Z technického hlediska se architektura řešení skládá z několika vrstev:

- síťová infrastruktura, zahrnující SAN, LAN, WAN až na úroveň přístupu do jednotlivých lokalit z Internetu nebo z interních stanic Zadavatele
- datová vrstva, obsahující systémy diskových polí a NAS
- databázové servery
- servery pro běh virtuálního prostředí aplikační vrstvy
- aplikační servery typu 1 (Red Hat EL)
- aplikační servery typu 2 (Windows Server)
- infrastruktura pro zálohování

2.3.1 Databázová vrstva

Jako databázové servery jsou použity servery IBM Power E870, u nichž je možné za běhu dynamicky měnit rozdělení výpočetního výkonu mezi jednotlivé logické servery (dále jen LPARy).

Na rok 2021 je naplánovaný upgrade serverů na model E980. V každé lokalitě jsou umístěny dva identické servery, konfigurace serverů mezi lokalitami se mírně liší v počtu aktivovaných CPU a instalované RAM. Většina databázových clusterů pracuje v konfiguraci active-active mezi lokalitami (v každé lokalitě jeden aktivní node).

Všechny servery mají připojení do LAN (několik 10G portů) i SAN (několik 16G a 8G portů).

2.3.2 Servery pro virtuální prostředí aplikační vrstvy

Jedná se o celkem 6 identických serverů (3 v každé lokalitě), na kterých je jako hypervisor provozován VMWare v edici Enterprise. Prioritizace výpočetních zdrojů pro produkční virtuální servery je zajištěna prostřednictvím resource managementu virtuálního prostředí. Vysoká dostupnost serverů je zajištěna pomocí Clusteru VMware vSphere Serverů, resp. jeho komponentami HA a vMotion.

V tomto prostředí jsou provozovány všechny virtuální servery aplikační vrstvy všech prostředí.

Konfigurace jednoho serveru (je plánována obnova serverů):

- Dell PowerEdge R730
- 2x CPU Xeon E5-2690v3 (2,6 GHz, 12-core)
- 768 GB RAM
- 2x 1Gb/s a 4x 10Gb/s porty pro Ethernet
- 4x8Gb/s porty pro FC
- 3x 300 GB pevný disk

2.3.3 Datová vrstva

Využívá pro uložení databázových dat redundantních diskových systémů HPE 3PAR 8440 a pro vytváření záloh páskové jednotky IBM TS3310 využívající technologie LTO-6 a LTO-4. Diskové pole je rovněž využíváno pro NAS gateway, která poskytuje diskovou kapacitu aplikačním serverům. Jako NAS zařízení je použit HPE 3PAR StoreServ File Controller (2 servery na každou lokalitu), v provedení „Gateway“, tj. kontroléry bez vlastní diskové kapacity, v clusterovém provedení (4-nodový cluster). Řešení je navrženo s maximální redundancí jak v rámci lokality, tak i mezi lokalitami. Mezi oběma lokalitami probíhají replikace na úrovni diskového pole.

SAN je vybudována na prvcích Cisco MDS 9148-S, pro připojení diskových polí se používají porty s rychlostí 16 Gb/s, ostatní zařízení jsou připojena přes porty s rychlostí 8 Gb/s. V každé lokalitě jsou 4 FC switche, lokality jsou spojené prostřednictvím DWDM celkem 4 kanály, každý s rychlostí 8 Gb/s.

Disková pole mají k dispozici kapacitu na discích SSD, rychlých točivých a pomalých točivých. V každé lokalitě je jedno centrální diskové pole, které má následující hlavní vlastnosti:

- Vytváření virtuálních logických disků (jednotlivé VVOLy jsou rozloženy přes všechny disky dané kategorie)
- Adaptivní optimalizace (dynamické rozložení dat na různé typy disků)
- Snapshoty
- Klony
- Replikace mezi lokalitami na úrovni polí
- Thin/full disky

2.3.4 Databázové servery

Pro databázové servery se využívají LPARy na centrálních databázových serverech (IBM Power) s operačním systémem AIX 7.2.

2.3.5 Aplikační servery

Tato vrstva je tvořena virtuálními servery v prostředí VMWare. Jednotlivé virtuální servery jsou symetricky rozděleny mezi obě lokality. Je možné využít servery s operačním systémem Windows Server 2016 a Red Hat Enterprise Linux.

2.4 Referenční, školicí a vývojové prostředí

Pro jednotlivé systémy provozuje Zhotovitel několik referenčních prostředí, technologicky shodných s produkčními systémy. Minimálně jedno z prostředí kopíruje produkční i z pohledu clusterových technologií (obsahuje cluster), ostatní prostředí jsou shodná aplikačně a neobsahují cluster.

Jednotlivé databáze odpovídají velikostí a strukturou primárnímu produkčnímu prostředí. Z hlediska používání nejsou bezprostředně závislé na primárním produkčním prostředí, tj. nedochází u nich k využívání synchronního zrcadlení dat mezi diskovými poli primární a sekundární strany. Databáze mohou pouze vznikat jako snímky primární produkční databáze v určitém čase.

2.5 Software

Zadavatel má pro své prostředí k dispozici následující licence:

- pro databázové servery dle 2.3.1 a 2.3.4:
 - o Oracle Database Enterprise Edition, včetně options: RAC, Spatial and Graph, Partitioning,
- pro aplikační servery dle 2.3.2 a 2.3.5:
 - o Microsoft Windows Server 2016 Datacenter Edition (celé VMWare prostředí),
 - o Red Hat Enterprise Linux (celé VMWare prostředí),
 - o Oracle Weblogic Suite (celé VMWare prostředí).