Stav IS VZP

UPOZORNĚNÍ:

Tento dokument je zpracován Všeobecnou zdravotní pojišťovnou České republiky (dále též jen „VZP ČR“ nebo „VZP“). Všeobecná zdravotní pojišťovna České republiky jej uveřejňuje v rámci zadávací dokumentace jí zadávaných veřejných zakázek. Tento dokument umožňuje utvořit si představu o standardech informační architektury ICT VZP ČR. Účelem jeho uveřejnění je poskytnout informace nezbytné pro integraci dodávané komponenty se stávajícím informačním systémem v souladu se Standardy ICT- VZP- NIS.

Uveřejněním tohoto dokumentu není dotčena právní odpovědnost spojená s jeho zneužitím.

V tomto dokumentu bylo použito názvů subjektů a názvů produktů, které mohou být chráněny příslušnými právními předpisy.

Otevřením tohoto dokumentu berete výše uvedené skutečnosti na vědomí.

Verze dokumentu

Verze	Datum	Autor	Popis
0.9	11.3.2019	Juraj Boldiš	Založení dokumentu ze Standardu verze 1.09
1.0	22.5.2019	Roman Palkovič (OTP)	Připomínkování a zapracování úprav dokumentu
1.0.1	14.6.2019	Juraj Boldiš	Zapracovány připomínky M. Škopa

Obsah

Seznam obrázků

1. Úvod

STAV IS VZP

- **Shrnuje aktuální stav aplikačních komponent –** poskytuje přehled o aplikačních komponentách, které jsou možné využít pro, rozvoj a budování IS VZP ČR.

- **Popisuje aktuální stav infrastruktury –** dává přehled o infrastruktuře, kterou v současnosti VZP využívá

2. Aplikační komponenty

2.1.1. Integrace se stávajícím IS

Ke dni vzniku tohoto dokumentu VZP provozuje stávající IS řízený historickou verzí standardu. Způsob integrace s tímto IS je proto prováděn dle původního standardu, stav je popsán v následujících přílohách.

Příloha 3: Integrace aplikace do IDM (Identity management)
Příloha 4: Integrace aplikace s CSČ (Centrální správa číselníků)
Příloha 5: Popis integračních vazeb prostřednictvím IPF a metodika realizace integračních vazeb

3. Infrastruktura VZP

3.1. HW

3.1.1. On Premise Serverová infrastruktura

Základem serverové infrastruktury, centralizované a provozované v rámci datových center (DC), jsou servery nebo serverovými systémy založené na architektuře procesoru Intel Itanium a x86. Servery jsou certifikovány na operační systémy uvedené v kapitole 3. 3., jsou rozšířitelné, maximálně flexibilní a vysoce dostupné. Jednotlivé servery nebo serverové systémy jsou připojeny do sítě LAN a v případě komunikace s diskovými poli i do sítě SAN a vybaveny kvalitními nástroji pro správu. V případě používání virtualizace uvedené v kapitole 3. 3. je hardware management propojen s virtualizační vrstvou. Servery nebo serverové systémy jsou v provedení blade nebo rackmount a v datových centrech jsou umístěny v rackových skříních velikosti 42U. Napájení rackových skříní se odvíjí od spotřeby zařízení, která jsou v něm umístěna.

Standardem pro připojení fyzických serverů do sítě LAN v datových centrech je:

- Management konzole, 1x1GE, access
- Management interface, 2x1GE, acces, active-standby
- Datový interface, 2x10GE, trunk, active LACP

On Premise SAN infastruktura

V jednotlivých datových centrech jsou disková enterprise a midrange pole, která jsou zapojena do SAN infrastruktury pomocí SAN přepínačů. Potřebná kapacita diskových polí je řešena rozšířením těchto polí nikoliv nákupem dalších polí. Do této SAN infrastruktury jsou z důvodu vysoké propustnosti a kvalitního zabezpečení (využití alternativních cest) zapojeny všechny významné servery, zálohovací knihovny a zmíněná disková pole. Tato SAN síť využívá u všech významných komponent minimálně 2 FC rozhraní pro zajištění vysoké dostupnosti.

3.1.2. Cloudová infrastruktura

Je využíván jeden cloudový poskytovatel - Microsoft a tedy spravujeme a využíváme jedno cloudové prostředí - Azure. Do listopadu 2019 můžeme využívat pouze služby, které jsou definovány smlouvou, není tedy možné využít jakoukoliv službu, následně bude možné využívat vše. Níže jsou vyjmenovány služby, které využíváme pro provoz e-VZP aplikací a veřejného webu.

3.1.2.1. IAAS - využívané služby

Azure Virtual machine

Azure Virtual machine scale set

3.1.2.2. PAAS využívané služby

Azure Storage – blob, queue, table, files

Azure SQL database

Azure Appservice

Azure CDN

Redis Cache

Service Bus

Key Vault

Notification HUB

Log Analytics

Service Fabric

Sendgrid

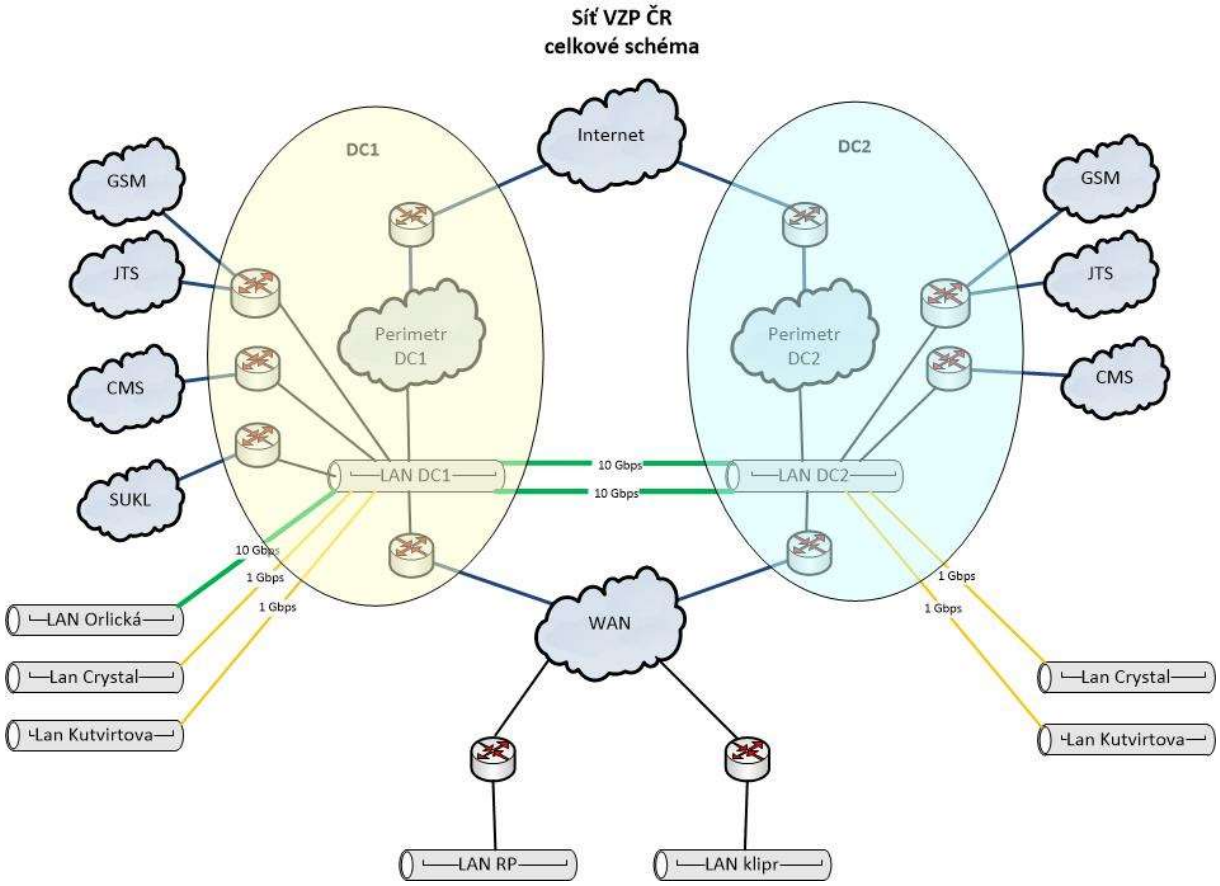
3.2. Sítě

3.2.1. Celkové schéma sítě VZP ČR

Z hlediska vztahu k uživatelům a k okolnímu světu je možné počítačovou síť VZP ČR rozdělit do několika funkčních celků:

- **Perimetr**
- **Datová centra**
- **WAN síť**
- **LAN sítě ústředí, regionálních poboček a kliprů(klientských pracovišť)**

Schematicky je síť VZP ČR znázorněna na následujícím obrázku:



Obrázek 1 - Celkové schéma sítě VZP ČR

CMS	Centrální místo služeb
GSM	Globální Systém pro Mobilní komunikaci
JTS	Jednotná telefonní síť
SUKL	Státní úřad pro kontrolu léčiv
RP	Regionální pobočka
KLIPR	Klientské pracoviště
DC1	Datové centrum 1 na adrese Orlická 4/2020, 130 00 Praha 3
DC2	Datové centrum 2 na adrese ČD Telematika, Pod Táborem 369/8a, 190 00 Praha 9
LAN Orlická	Ústředí na adrese Orlická 4/2020, 130 00 Praha 3
LAN Crystal	budova Crystal na adrese, Vinohradská 2577/178, 130 00 Praha 3
LAN Kutvirtova	Call Centrum a klipr na adrese Kutvirtova 339/5, 150 00 Praha 5

3.2.2. LAN RP a KLIPRů

LAN ve VZP ČR je rozdělena do vrstev podle hierarchického modelu:

- **Access (přístupová) vrstva** – zajišťující konektivitu koncových uživatelů
- **Distribution (distribuční) vrstva** – zajišťující vysokou dostupnost
- **Edge (hraniční) vrstva** – slouží pro připojení LAN do WAN

SLUŽBY A TECHNOLOGIE LAN

- VLAN
- QoS

VLAN

VLANy jsou implementované v přístupové vrstvě. Uživatelé z různých oddělení, rozděleni do určených VLAN, mohou přistupovat do sítě určenými přístupovými přepínači, které jsou umístěny v různých podsítích. V hraniční, případně distribuční, vrstvě je nakonfigurované směrování těchto podsítí mezi sebou a také případné omezení provozu mezi VLANami pomoci ACL – Access Control List (přístupových listů).

QoS (QUALITY OF SERVICE)

QoS zajišťuje rovnoměrné vyvažování zátěže sítě s ohledem na druh přenášených dat, spravedlivě rozděluje konektivitu mezi jednotlivé aplikace dle nastavených priorit a zabraňuje přetížení sítě.

Ve VZP ČR jsou použity následující **QoS** třídy, které jsou řazeny dle priority – od nejvyšší priority po nejnižší prioritu.

- Třída – Network support
- Třída – Real time (VoIP RTP, VoIP Signalizace)
- Třída – 3B: Interaktivní provoz (terminálová třída) – (Aplikace Interaktivní)
- Třída – 3A: Web provoz (webová třída)
- Třída – 3D: Scavenger třída (DoS, P2P, ...) – Služby UDP (Bulk)
- Třída – Zbytková třída – ostatní provoz

3.2.3. Bezdrátová síť (WIFI)

Bezdrátová síť ve VZP ČR je provozována na standardních zařízeních a technologii firmy Cisco. Bezdrátová síť poskytuje několik variant připojení:

- **WLAN_DATA** – síť určená pro standardní uživatele interní sítě VZP, je veřejně inzerovaná. Tato síť je určená pro běžného uživatele a jsou na ni implementována bezpečnostní omezení.
- **WLAN_ADMIN** – síť určená pouze pro administrátory sítě. Síť není veřejně inzerovaná (má vypnuto vysílání SSID).
- **WLAN_PHONE** – síť určená pro připojení mobilních telefonů a pro volání po bezdrátové síti. Síť není veřejně inzerovaná (má vypnuto vysílání SSID). Přístup do sítě je ověřen pomocí MAC adresy zařízení.
- **WLAN_GUEST** – síť určená pro připojení externích uživatelů s přístupem pouze do Internetu pomocí protokolu HTTP (S). Tato síť je veřejně inzerovaná.
- **WiredGuest** – jedná se o drátovou síť, která je řízená prostředky bezdrátové sítě a funguje obdobně jako síť WLAN_GUEST s tím rozdílem, že klient se místo k bezdrátové síti připojuje do portu přepínače.
  Tuto síť je možno využívat pouze v centrálních lokalitách – Orlická, Perštýn.
  Tato síť určená pro připojení externích uživatelů s přístupem pouze na Internet.

3.2.4. WAN

VZP ČR provozuje privátní datovou síť WAN na přenosových prostředcích poskytovatele datového připojení pomocí technologie MPLS. Pro zajištění bezpečnosti přenášených dat je použito šifrování na

síťové vrstvě mezi koncovými zařízeními pomocí protokolu IPSec. Pro navazování šifrované komunikace mezi směrovači v síti VZP ČR je použita technologie GET (Group Encrypted Transport) VPN.

Šířka pásma

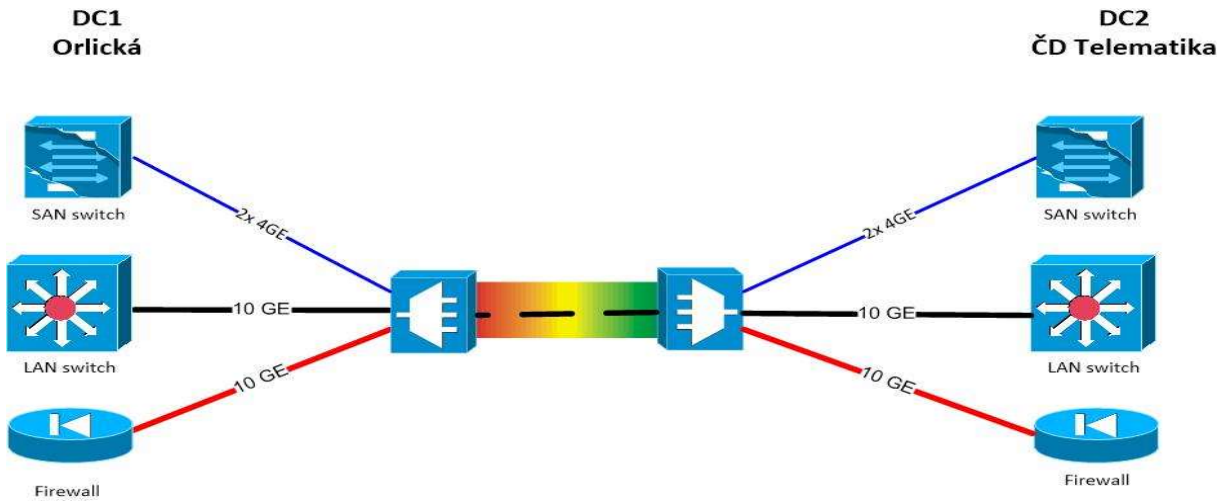
Typ pobočky	Počet uživatelů	Šířka pásma
1	1-5	0,5 Mbps
2	6 -50	4 Mbps
3	51 a více	8 Mbps

3.2.5. Datová centra On premise

VZP ČR provozuje dvě geograficky oddělená datová centra:

- DC1 na adrese Orlická 4/2020, 130 00 Praha 3
- DC2 na adrese ČD Telematika a.s., Pod Táborem 369/8a, 190 00 Praha 9

Obě datová centra jsou propojena dvěma nezávislými optickými trasami technologií DWDM. Jedna vlnová délka o kapacitě 10 Gbps je použita pro LAN provoz a druhá 10 Gbps pro propojení firewall clusteru. Pro propojení SAN přepínačů jsou multiplexovány dva kanály, každý o kapacitě 4 Gbps.



Obrázek 2 - Schéma propojení datových center

Každé z datových center VZP ČR je vytvořeno na technologii firmy Cisco Nexus dle architektury Spine and Leave a patří mezi tzv. aplikačně řízené infrastruktury (Application Centric Infrastructure ACI), které umožňují integrovat do řízení síťového provozu datového centra vlastní logiku jednotlivých aplikací z pohledu jejich požadavků na síťovou konektivitu, bezpečnost a L4-L7 služby (load balancing, firewalling atd.). Fyzické nebo virtuální aplikační servery sdílející stejnou bezpečnostní a síťovou politiku jsou konsolidovány do logických skupin a současně je definována jejich vzájemná komunikace (která aplikační komunikace je povolená, jaké vyžaduje QoS parametry a jaké vyžaduje L4-L7 služby).

Veškeré aplikační politiky jsou definovány na centrálním kontroleru (Application Policy Infrastructure Controller - APIC), který je s využitím otevřených aplikačních rozhraní automaticky distribuuje na jednotlivé komunikační prvky a systémy, které následně podle těchto aplikačních politik řídí síťový provoz.

Logická infrastruktura

Provoz datového centra je z pohledu toku dat směrem od uživatele k vlastním datům rozdělen do jednotlivých funkčních modulů neboli zón. Rozhodujícím hlediskem pro sledování toku dat je „kdo inicializuje komunikaci“.

Zóny představují zpravidla několik L3/L2 segmentů, která mají podobná bezpečnostní pravidla. Zóny jsou IP adresací příslušné k lokalitě DC. Výjimku tvoří zóna DC-DB, ta je L2 geograficky rozprostřena mezi lokalitami DC1 a DC2.

Rozdělení DC zón:

- **Síť VZP ČR (VZP NET)**

Zóna označuje síť VZP, která není součástí DC – tj. infrastrukturní část LAN/WAN včetně části koncových uživatelů.

- **Demilitarizovaná zóna (DC-DMZ)**

Zóna je dostupná z obou stran jak pro VZP, tak pro DC. Slouží k zabezpečení a poskytování služeb. Typicky Management, DNS, MS AD DC nebo LDAP, ACS. Do této zóny patří vrstva správy a administrace a vrstva infrastrukturních serverů.

- **Prezentační vrstva (DC-VIP)**

Jedná se o vrstvu, v které jsou umístěné servery zajišťující komunikaci s uživateli. Patří sem i virtuální IP adresy, které reprezentují jednotlivé aplikace pro přístup jak z VZP NET, tak z ostatních aplikací DC.

- **Aplikační vrstva (DC-APP)**

Zde jsou umístěny aplikační servery zajišťující business logiku jednotlivých aplikací.

- **Databázová vrstva DC (DC-DB)**

Umístění DB serverů. L2 vrstva rozprostřená geograficky mezi lokalitami DC1 a DC2. V databázové vrstvě je možné vytvářet clustery se společnou IP adresou mezi jednotlivými lokalitami.

- **Servisní zóna (DC-SERVIS)**

Zóna slouží jako prostředník pro výměnu dat mezi ostatními zónami a mezi prostředími produkce a test.

Zóny DC-APP a DC-DB nejsou přímo dostupné z VZP NET a obráceně. Komunikace musí být zprostřed-kována přes některou ze zón DC-DMZ, DC-VIP, DC-SERVIS .

Komunikační matice zobrazuje podporované komunikace mezi jednotlivými zónami.

	Komunikace do zóny →					
Komunikace ze zóny ↓	VZP NET	DC-DMZ	DC-VIP	DC-APP	DC-DB	DC-SERVIS
VZP NET	ANO	ANO	ANO	ϴ	ϴ	ANO
DC-DMZ	ANO	ANO	ANO	ANO	ANO	ANO
DC-VIP	ϴ	ϴ	ϴ	ANO	ϴ	ϴ
DC-APP	ϴ	ANO	ANO	ϴ	ANO	ANO
DC-DB	ϴ	ANO	ϴ	možné	možné	ANO
DC-SERVIS	ANO	ANO	ϴ	ANO	ANO	ANO

3.2.6. Perimetr

Perimetr je zabezpečená oblast podnikové sítě, která leží mezi internetem a vnitřní sítí VZP ČR. Perimetr je rozdělen pomocí bezpečnostních bran (firewallů) do několika oddělených bezpečnostních zón:

- vnější perimetr – bezpečnostní oddělení externích sítí (Internetu) od sítě VZP
- vnitřní perimetr – bezpečnostní oddělení veřejně vystavených služeb VZP od vnitřní (uživatelské) sítě VZP

Součástí řešení je i VPN přístup do VZP ČR. VPN slouží pro vzdálený přístup zaměstnanců a externích kontraktorů do sítě VZP ČR z Internetu.

3.2.7. Síťové služby

Síť VZP ČR poskytuje pro koncová zařízení, aplikace a uživatele následující služby:

- Časová synchronizace (NTP)
- Kvalita služby (QoS)
- DNS, DHCP, IPAM (DDI)
- Loadbalancing

3.2.8. Sjednocená komunikace

Sjednocená komunikace je ve VZP ČR tvořena následujícími součástmi:

- **Hlasová komunikace**
  - IP Telefonie
  - Integrované nadstavbové funkcionality
  - Spolupracující systémy
    - Call Centrum Atlantis
    - Cisco Paging
- **Elektronická komunikace**
  - Instant messaging - Cisco Jabber
  - Webová konference – Cisco WebEx

3.3. OS

3.3.1. OS pro aplikace třídy A

- HP-UX 11.31, Red Hat Enterpise Linux, Oracle Linux, CentOS (verze 6.x a 7.x)
- MS Windows Server 2012R2 EN a novější

3.3.2. OS pro aplikace třídy B

HP-UX 11.31, Red Hat Enterprise Linux, Oracle Linux, CentOS (verze 6.x a 7.x)

MS Windows Server 2012R2 EN a novější

3.3.3. Prostředí pro virtualizaci

Hostitelský systém je hypervizor nebo operační systém s hypervizorem , který umožní provoz Virtuálních serverů. Podporované platformy jsou a ve VZP mohou být nasazeny technologie, VMWare vSphere 5.5 Enterprise a vyšší, HPVM, Oracle VM 3.4 a vyšší a MS Hyper-V 2012R2 a vyšší.

Řízení Virtuálních serverů - správa VMs na VMWare nástrojem VMWare vCenter Server 5.5 Standard a vyšší. Správa VMs na Hyper-V je realizována nástrojem SCVMM 2012R2 a vyšší.

Pro zajištění vysoké dostupnosti aplikací třídy A pro a realizaci DRP plánu slouží technologie VMware DRS a HA cluster, případně VMware SRM, VMware vSAN nebo MS Hyper-V Clustering, MS Storage Spaces Direct v aktuálních verzích.

Pro aplikace třídy A využívající softwarové produkty Oracle bude použita virtualizace Oracle VM.

U aplikací třídy B lze použít i další virtualizační technologií:

KVM (Kernel-based Virtual Machine)

3.4. Middleware

3.4.1. Integrační platforma

- je založená na koncepci ESB (Enterprise Service Bus) jako podnikové sběrnice služeb
- pro realizaci integrace aplikací a služeb
- využívá centrální business rule repozitory a Business rule engine
- využívá principy servisně orientované architektury (SOA)
- využívá MOM architekturu (Message Oriented Middleware) jako podmnožinu ESB kde prostřednictvím Message brokera zajišťuje spolehlivé doručení zprávy nesoucí informaci (Message) mezi jednotlivými systémy (prostřednictvím front).
- využívá model řízení událostmi

Integrační platforma poskytuje tyto typy služeb:

- centrální řízení komunikaci mezi systémy realizované prostřednictvím ESB služeb,
- kompozice vlastních služeb a jejich publikace konzumentům
- zprostředkování a publikace sdílených služeb konzumentům,
- orchestraci služeb vnitřních i vnějších s ostatními integračními technologiemi (BPEL)
- směrování a předávání dat mezi jednotlivými službami
- transformaci formátů dat,
- konverze protokolů mezi jednotlivými službami,
- centrální business rule repozitory
- centrální repozitory služeb

3.4.2. Aplikační servery

Výčet typů AS využívaných v IS VZP:

Druh AS	Použití
Oracle Fusion Middleware WebLogic Server v nejnovější podporované verzi	Aplikace deployované v J2EE, vhodné pro aplikace třídy A
JBoss aplikační server v nejnovější podporované verzi	Pro J2EE aplikace třídy B nebo v odůvodněných případech, kde není vhodné použití Oracle Weblogic J2EE.

3.4.3. Webové servery

Výčet typů WS využívaných v IS VZP:

- Oracle Web Tier v nejnovější podporované verzi

- Apache v nejnovější podporované verzi
- IIS

3.5. Virtualizovaná infrastruktura pro hostování aplikací

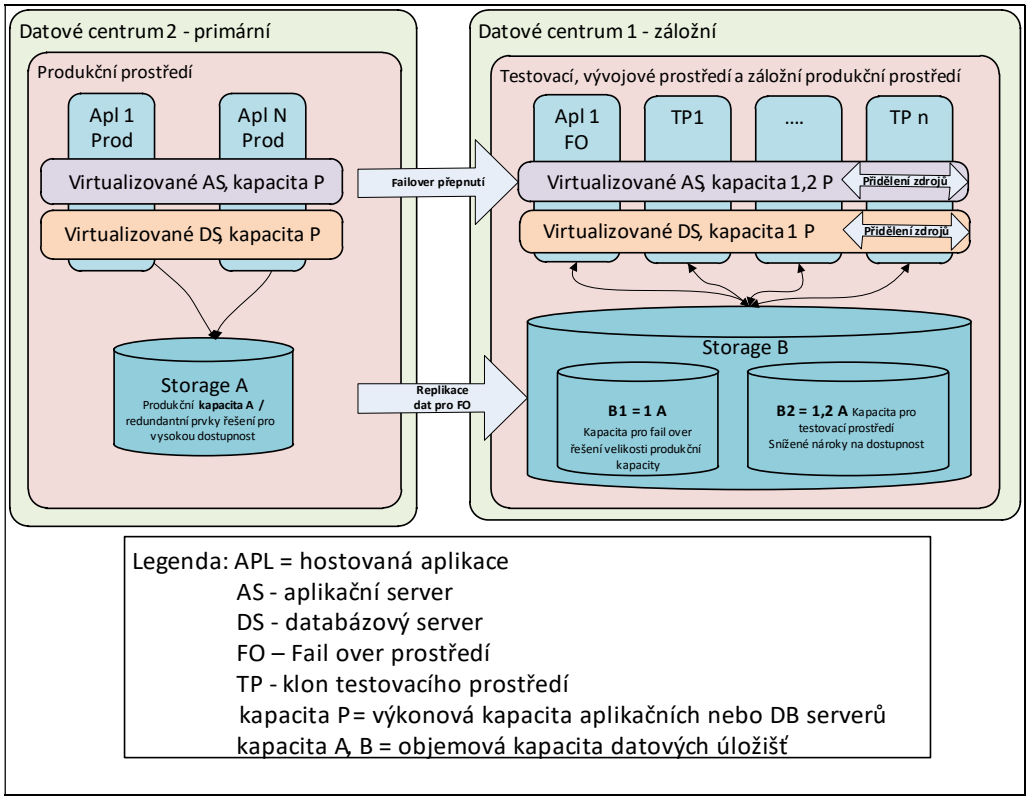
Aplikační služby jsou hostovány na virtuálních prostředí / serverech následujících parametrů:

Název služby	Popis
Server s OS	OS Windows nebo Linux (viz kap. 3.3 OS)
Aplikační server	OS Windows nebo Linux aplik. serveru Oracle Weblogic Suite
Databázový server Oracle	OS Linux, Oracle dB EE + RAC + partitioning
Databázový server MS SQL	OS MS Windows, MS SQL Server v edici Enterprise

3.6. Deployment aplikací provozovaných on-Premise do prostředí v DC

Pro zabezpečení provozu aplikací v prostředí datových center je používán standardizovaný deployment aplikací :

- Produkční instance aplikací a jejich odpovídajících dat je hostována v primárním datovém centru na zařízeních s vysokou dostupností a redundancí na virtualizované infrastruktuře.
- Záložní instance aplikací je hostována ve virtualizované infrastruktuře v záložním datovém centru s dedikovanou kapacitou úložiště o velkosti produkčních dat pro fail over primárního DC.
- Virtualizovaná infrastruktura serverů záložního centra je dimenzována jako výkonový ekvivalent zařízení v primárním datovém centru. Požadavek na dostupnost je nižší, tomu odpovídá nižší redundance prvků.
- Virtualizovaná infrastruktura záložního centra je sdílena s testovacími prostředími.
- Produkční data z primárního DC jsou asynchronně replikována do záložního DC.
- Pro účely testování je v záložním DC dedikována obecně kapacita virtualizované úložné kapacity až v rozsahu 1,2 velikosti produkčních dat sdílená pro všechny instance testovacích prostředí. Tato kapacita je alokována individuálně při návrhu systému.
- Kapacita úložiště Storage B musí být 2,2 násobkem kapacity úložiště produkčního prostředí Storage A
- Kapacita HW serverů pro databázovou a aplikační vrstvu musí být výkonově dimenzována jako 1,2 násobek produkčního prostředí (měřeno součtovým počtem jader, velikostí operační paměti virtuálních serverů a diskových úložišť pro aplikační a databázovou vrstvu). Redundance komponent není nutná.



Obrázek 3 – Schéma deploymentu datových center

3.7. Datové a databázové služby

3.5.1. Databázové technologie

Standard	Popis
Oracle DB EE v nejnovější podporované verzi, včetně databázových options	Pro aplikace třídy A nebo B.
MS SQL EN v nejnovější podporované verzi,X64bit	Podpůrné služby a pro aplikace v třídě B. V odůvodněných případech je možné použít i pro aplikace třídy A.

3.5.2. Datové a databázové standardy

Oblast standardizace	Popis
Minimum redundancí	Data jsou uložena v jediné databázi. Redundantní databáze v rámci lokality nejsou pro core business aplikace povoleny. Replikace se provádí pouze z důvodu realizace DR plánu..
Jediný zdroj informací	Data jsou uložena v místě jejich vzniku, do ostatních systémů jsou poskytována prostřednictvím integrační platformy. Platí pravidlo minima duplicit.
Datová konzistence	Datová konzistence je zachovávána již v rámci databáze, tedy nikoliv pouze aplikačně.
Modelování DB pomocí ER diagramu	Jsou zachovány normálové formy. Pouze v případech, kdy je to nutné jsou možné výjimky – v dokumentaci však je explicitně uvedeno.

Návrh datového modelu	Návrh datového modelu DB musí být akceptován datovým architektem VZP ČR. Persistentní objekty vývojář definuje bez určení: • Názvu tablespace • fyzických atributů segmentu (pctused, pctfree, storage params,...) Databázové objekty jsou považovány za privátní součást aplikace, tzn. aplikace může přistupovat k databázovým objektům jiné aplikace pouze prostřednictvím dedikovaných služeb.
Jmenné konvence databázových objektů	Všechna jména základních databázových objektů (tabulky, pohledy, balíky funkcí a procedur, fronty, sekvence, indexy, triggery apod.) začínají dvouznakovým prefixem dodavatele
Kódování	Preferované UTF16, UTF8, Definici collation – preferována Czech CI AS (case insensitive a accent sensitive) Na výjimku: ISO 8859-2, Windows 1250
Podpora anonymizace / pseudonymizace osobních údajů	Datová vrstva musí podporovat možnost anonymizace a pseudonymizace osobních údajů bez nežádoucí vlivu na chování datového engine a aplikace. Využívá se pro účely příslušné legislativy a vytváření datového derivátu pro testování z produkčních dat. Součástí dodávek je nástroj pro vytváření anonymizovaných derivátů produkčních dat (scrambling tool). Toto musí být zohledněno i v dokumentaci.
Podpora řezů dat	Datový model musí být navržen tak, aby pro účely testování bylo možno oddělit testovací derivát – vzorek dat z produkčních dat. Součástí dodávek je nástroj pro vytváření takových derivátů. Toto musí být zohledněno i v dokumentaci.
Zakázané vazby	Data v relačních databázích nesmí být provazována technologicky přes významové klíče, povolena je relační vazba pouze přes nezávislé technologické klíče záznamů. Nejsou dovoleny přímé datové vazby mezi datovými doménami.

3.6. Popis standardního koncového zařízení

- Koncová pracovní zařízení počítače a notebooky
  - Instalován OS Windows enterprise 7 x32 /Windows 10 enterprise x64
  - Nastavení OS systému a uživatelského prostředí řízeno centrálně doménovou politikou.
  - Uživatel nemá na koncové zařízení administrátorské práva
  - Vzdálený přístup je zajištěn Remote Desktop, Support Assistant
  - Bezpečnostní aktualizace OS v 6 měsíčním cyklu

- Programové vybavení koncových pracovních zařízení
  - MS Office 2010/2016 /2019 Profesionál plus
  - Google Chrome, nastavení řízené centrální doménovou politikou

  - IE aktuální verze 11, nastavení řízené centrální doménovou politikou
  - 7ZIP
  - Cisco AnyConnect Secure Mobility Client (Notebooky)
  - Adobe Reader 11/DC

- Centrální distribuce programového vybavení na pracovní stanice
  - Distribuce SW je použitím SCCM

- Zabezpečení koncových pracovních zařízení
  - Endpoint Protection , Antivirová ochrana Kaspersky Endpoint Securit (centrálně řízený)
    - AntiMalware, IDS/IPS,
    - Firewall,
    - Application control,
    - Device control,
    - Antispam

- Jednotná adresářová struktura
    - Root:
      APPL
      Archiv
      Data
      Nezalohovano
      Program Files
      Temp
      TMP
      Users
      Windows
  - Pro Root, Program Files, Windows má běžný uživatel práva pouze pro čtení

- Ostatní programové vybavení
  - JAVA 1.6.045 ,1.7.51 , 1.8. a vyšší
  - NET Framework ver. 4.0 a vyšší

- Tisková koncová zařízení
  - Tisková a multifunkční zařízení připojená přes tiskový server, výjimečně lokální připojení
  - Follow me printing se zabezpečeným tiskem.
  - Ověřování pomocí bezkontaktních karet
  - (embeded čtečka v MFDnebo externí terminál, možnost ověření PINem).
  - Scan to me (možnost naskenovat z jakékoli MFD a obdržet sken v personální složce nebo emailem).

- Ostatní koncová zřízení
  - Mobilní telefony s OS : Android 5.0 a vyšší, Windows 10 mobile

3.7. Elektronická pošta

- Elektronická pošta ve VZP ČR je realizována prostřednictvím Microsoft Exchange server 2016. enterprise. Příjem elektronické pošty z Internetu zajišťují dedikované SMTP brány v perimetru, před předáním zpráv do interního poštovního systému je provedena jejich antivirová a antispamová kontrola. Odesílání pošty mimo lokální poštovní doménu probíhá pomocí SMTP protokolu s využitím poštovních bran.

- Klientský přístup k poštovnímu systému je zajištěn pomocí MS Outlook verze 2010 nebo vyšší, případně prostřednictvím internetového prohlížeče (Outlook Web App). Poštovní systém podporuje kromě SMTP i protokoly POP3 a IMAP.

Poštovní systém je využíván pro strategické řízení firmy, a proto je implementován jako vysoce dostupný.

3.8. Active Directory

VZP ČR využívá pro ověřování uživatelů a pracovních stanic Microsoft Active Directory (dále AD). Služby AD jsou realizovány na serverech s MS Windows Server 2012 R2. V AD má každý uživatel i každá pracovní stanice svůj účet. Účty uživatelů jsou spravovány prostřednictvím Identity Managementu na základě údajů uložených v personálním systému. AD zajišťuje pomocí skupinových politik i nastavení pracovních stanic v souladu s platnými bezpečnostními standardy.

3.9. PKI

VZP ČR využívá systém interních certifikačních autorit (PKI) založený na Microsoft Windows Server 2016. Vystavované certifikáty slouží pro identifikaci pracovních stanic a serverů v interní síti VZP ČR a dále pro podpis a šifrování elektronické pošty a pro vzdálený VPN přístup uživatelů do VZP ČR.

6. Provozní prostředí

6.1. Monitoring

6.1.1. Rozsah monitoringu

Služba dohledu provozu informačního systému je centralizovaná a je zajišťována dohledovým centrem s dvousměnným provozem v pracovních dnech od 6:00 do 22:00 hod. (v režimu 5x16). V těchto časových úsecích jsou drženy pohotovosti řešitelských skupin pro síťovou infrastrukturu, operační systémy Unix, operační systémy Windows, Oracle infrastrukturu (databáze a middleware), provoz aplikací, Exchange, a pro dohledové nástroje.

Z hlediska teorie spolehlivosti IT systémů a služeb jsou sledovány a vyhodnocovány:

- chybovost, resp. dostupnost systémů a služeb (Availability) a jejich vytížení (Utilization),
- výkonnost služeb (Performance).

Z technicko-provozního hlediska je monitoring provozován ve dvou hlavních úrovních – infrastrukturní a aplikační.

- Infrastrukturní monitoring pokrývá všechny prvky produkční IT infrastruktury ZIS od síťových prvků přes servery, databáze až po middleware. Je vyhodnocována dostupnost, resp. chybovost, jakož i vytíženost sledovaných prvků.
- Aplikační monitoring je zaměřen na sledování klíčových služeb produkčních aplikací. Probíhá aktivně pravidelným spouštěním aplikačních úloh, simulujícím uživatelské akce. Zároveň jsou pasivně vyhodnocovány vybrané úlohy reálných uživatelů. Je vyhodnocována dostupnost úloh a služeb, a současně jsou zaznamenávány a vyhodnocovány odezvy takto měřených transakcí, tedy výkonost aplikací. Výstupy pasivního monitoringu jsou využitelné pro sledování vytíženosti sledovaných oblastí.

6.1.2. Používané dohledové nástroje pro On premise řešení

Centrální systém dohledu provozu informačního systému je vybudován na platformě **HP Operations Manager** (HP OM). Do dohledového centra HP OM (centrální konzole) jsou soustřeďovány všechny důležité zprávy z ostatních monitorovacích nástrojů.

HP OM – agent na úrovni OS, centrální konzole
HP OM Performance Manager (PM) – sledování vytíženosti systémů
Oracle Enterprise Manager Cloud Control (OEM) – agent, integrace vybraných událostí do HP OM
Microsoft System Center 2012 Operations Manager (SCOM) – agent na úrovni OS, integrace vybraných událostí do HP OM
Nagios – bezagentní, s integrací vybraných zpráv do HP OM
HP Business Service Management (HP BSM) – integrace do HP OM
- **Business Process Monitor (BPM)** – aktivní aplikační monitoring

HP Network Node Manager i (HP NNMi) – aktivní SNMP poll, pasivní SNMP trap, je integrován s HP OM
HP SiteScope – bezagentní, integrace do HP OM a HP BSM

Není-li možné nasadit monitoring pomocí zavedených nástrojů, poskytne dodavatel v rámci dodávky aplikace monitorovací nástroj (například skript), jehož výstup lze integrovat do HP OM.

6.2. Zálohování a archivace

Všechna DC jsou zálohována jedním společným zálohovacím subsystémem (dále jen ZS).

6.2.1. Zálohovací systém

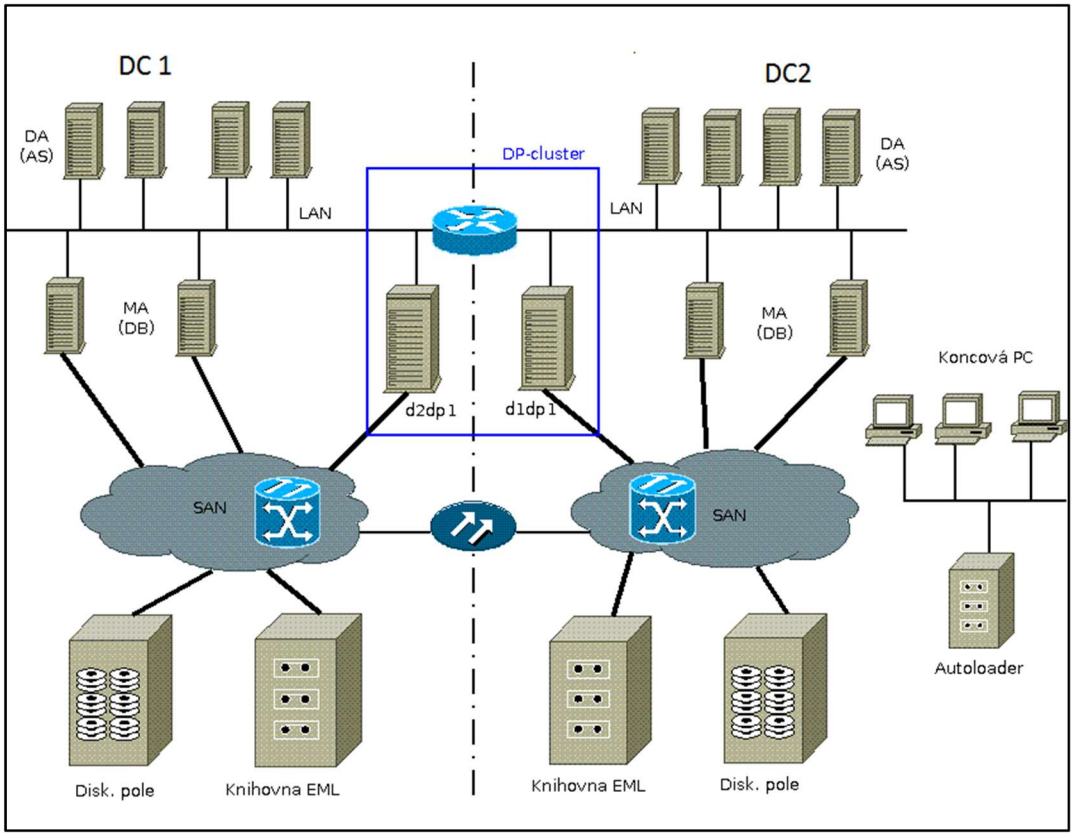
ZS je tvořen těmito komponentami:

- Řídící SW „Data Protector“.
- Cluster dvou serverů v oddělených lokalitách, na nichž je řídící SW provozován.
- HW pro ukládání zálohovaných dat, umístěný rovněž ve dvou různých lokalitách (DC), dostupný pomocí LAN a SAN infrastruktury. Jsou používány robotické páskové knihovny, které mohou být v případě potřeby doplněny o jiný HW (např. typu B2D), připojitelný pod řídící zálohovací software

Zálohování probíhá tak, aby byla respektována bezpečnostní zásada „3-2-1“ (tj. „důležitá data musí existovat 3x, ve 2 různých datových formátech, 1 kopie ve druhé lokalitě“) dle příslušné třídy aplikace.

6.2.2. Zálohovací architektura

Pro zálohování IS má VZP ČR k dispozici vysoce dostupný zálohovací systém s řídícím SW Micro Focus Data Protector. V každém datovém centru je k dispozici jedna pásková knihovna. Obě páskové knihovny jsou osazeny 8 kusy páskových mechanik (4x LTO4 + 4x LTO5, v budoucnu předpokládáme LTO7 a LTO8 a využití technologie B2D).



Obrázek 4 - Schéma zálohovacího sytému VZP ČR