

Příloha č. 3 Smlouvy

Platforma Správy železnic

Leden 2019

Tento dokument obsahuje 32 stran

Kontrola a schválení dokumentu

Provedené revize

| Verze | Datum | Revize - komentář |
|-------|-------------|------------------------------------|
| 1.0 | 13. 9. 2019 | Úvodní verze Platformy |
| 2.0 | 1. 10. 2019 | Aktualizace |
| 3.0 | 17.10.2019 | Aktualizace |
| 4.0 | 20.11.2019 | Aktualizace |
| 5.0 | 06.12.2019 | Aktualizace |
| 6.0 | 13. 1. 2020 | Draft k připomínkám |
| 7.0 | 21. 1. 2020 | Zpracované připomínky |
| Final | 27. 1.2020 | Verze se zpracovanými připomínkami |

OBSAH

| | |
|--|-----------|
| ČÁST I. ÚVOD | 4 |
| ČÁST II. ZKRATKY A POJMY | 5 |
| ČÁST III. PLATFORMA SPRÁVY ŽELEZNIC | 6 |
| ČÁST IV. MOTIVACE | 8 |
| ČÁST V. SLUŽBY PLATFORMY SPRÁVY ŽELEZNIC..... | 9 |
| V.1 INFRASTRUKTURNÍ SLUŽBY | 10 |
| V.1.1 SLUŽBY ZABEZPEČENÝCH FYZICKÝCH SERVERŮ BEZ OPERAČNÍHO SYSTÉMU | 10 |
| V.1.2 SLUŽBY ZABEZPEČENÝCH FYZICKÝCH SERVERŮ S OPERAČNÍM SYSTÉMEM | 10 |
| V.1.3 SLUŽBY ZABEZPEČENÝCH VIRTUALIZOVANÝCH SERVERŮ BEZ OPERAČNÍHO SYSTÉMU | 11 |
| V.1.4 SLUŽBY ZABEZPEČENÝCH VIRTUALIZOVANÝCH SERVERŮ S OPERAČNÍM SYSTÉMEM..... | 11 |
| V.1.5 SLUŽBY ZABEZPEČENÝCH DATOVÝCH ÚLOŽIŠŤ | 11 |
| V.2 PLATFORMNÍ SLUŽBY | 12 |
| V.2.1 SLUŽBY ZABEZPEČENÝCH DATABÁZOVÝCH PROSTŘEDÍ | 12 |
| V.2.2 SLUŽBY ZABEZPEČENÝCH APLIKAČNÍCH SERVERŮ, SLUŽBY ZABEZPEČENÝCH WEBOVÝCH SERVERŮ .. | 12 |
| V.2.3 SLUŽBY ZABEZPEČENÝCH INTEGRAČNÍCH PLATFORM | 12 |
| V.3 PODPŮRNÉ SLUŽBY | 13 |
| V.3.1 ZAJIŠTĚNÍ SLUŽBY MONITORINGU A DOHLEDU INFRASTRUKTURY A APLIKACÍ | 13 |
| V.3.2 ZAJIŠTĚNÍ SLUŽBY ZÁLOHOVÁNÍ | 13 |
| ČÁST VI. TECHNOLOGIE PLATFORMY SPRÁVY ŽELEZNIC..... | 14 |
| ČÁST VII. ARCHITEKTONICKÉ PRINCIPY A VZORY | 18 |
| VII.1 ARCHITEKTONICKÉ PRINCIPY..... | 19 |
| VII.1.1 BEZPEČNOST A SOULAD S VNITROPODNIKOVOU LEGISLATIVOU | 19 |
| VII.1.2 PROVOZOVATELNOST ŘEŠENÍ..... | 19 |
| VII.1.3 OCHRANA DAT JAKO KLÍČOVÉHO AKTIVA SPRÁVY ŽELEZNIC..... | 20 |
| VII.1.4 ZNOVUPOUŽITELNOST ŘEŠENÍ..... | 20 |
| VII.1.5 NEZÁVISLOST NA DODAVATELÍCH | 20 |
| VII.1.6 NEZÁVISLOST NA TECHNOLOGIÍ | 20 |
| VII.1.7 ŘÍZENÍ IDENTIT | 20 |
| VII.1.8 ARCHITEKTURA, NÁKUP A VÝVOJ ŘEŠENÍ | 21 |
| VII.1.9 BUSINESS KONTINUITA JAKO ZÁSADNÍ ČINNOST | 22 |
| VII.2 ARCHITEKTONICKÉ VZORY..... | 23 |
| VII.2.1 SKUPINA 1 | 24 |
| VII.2.2 SKUPINA 2 | 27 |
| VII.2.3 SKUPINA 3 | 28 |
| ČÁST VIII. PRINCIPY APLIKOVÁNÍ PLATFORMY SPRÁVY ŽELEZNIC..... | 30 |
| ČÁST IX. PŘÍLOHY..... | 31 |

Část I. Úvod

Odbor informatiky (O22) zastává pozici integrátora IT procesů (systémových, aplikačních i infrastrukturních). Plná kontrola nad celofiremním IT prostřednictvím vyšší míry centralizace a nastavením jasných kompetencí ve vztahu k organizačním jednotkám, ostatním úsekům a dodavatelům je nezbytným předpokladem pro tuto pozici.

Platforma Správy železnic specifikuje souhrn podporovaných infrastrukturních služeb, komponent, principů a architektonických vzorů. Tímto Platforma Správy železnic definuje základní rámec aplikovatelný při dodávce a návrhu ICT řešení.

Část II. Zkratky a pojmy

| | |
|------------|--|
| O22 | Odbor informatiky |
| ZZVZ | Zákon o zadávání veřejných zakázek |
| SW | Software je sada všech počítačových programů používaných v počítači, které provádějí nějakou činnost |
| HW | Hardware označuje veškeré fyzicky existující technické vybavení počítače |

Část III. Platforma Správy železnic

Platforma Správy železnic je veřejně dostupný a publikovaný dokument, který definuje prostředí podporující návrh, implementaci a následný provoz IT systémů a řešení ve Správě železnic. Pro návrh ICT řešení ať v rámci ICT projektů nebo v rámci dodání jako součást staveb definuje základní architektonické vzory, komponenty a principy. Na jejich základě lze budovat řešení převzatelné do provozu interními týmy Správy železnic, dlouhodobě provozovatelné a rozvíjitelné a splňující požadované úrovně bezpečnosti a kvality poskytovaných služeb.

V pojetí dokumentu se jedná o Platformu odboru informatiky O22.
Dokument spravuje odbor Informatiky O22.

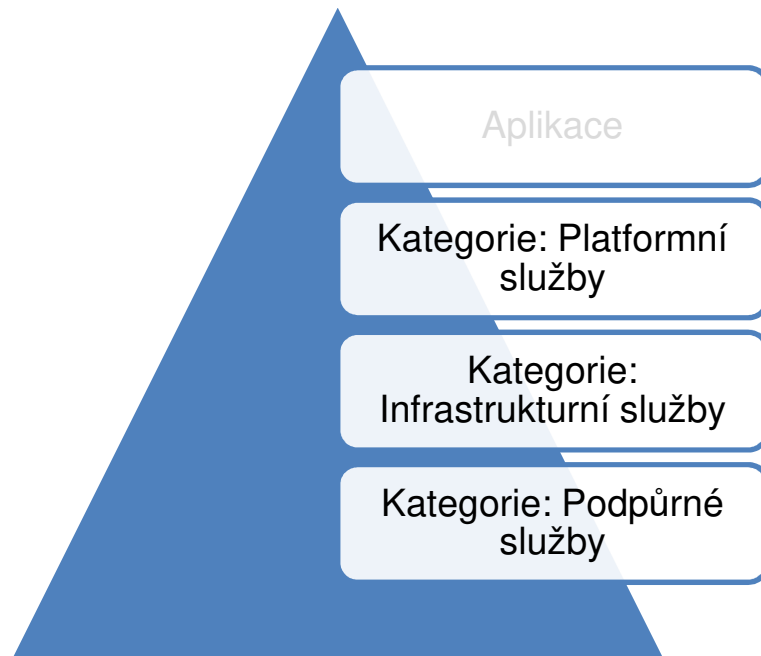
Platforma Správy železnic je pravidelně aktualizována z pohledu zajištění souladu s novými ICT trendy a standardy Správy železnic a byznys požadavky a cíli a úkoly Správy železnic.

Platforma Správy železnic obsahuje:

- Katalog dostupných služeb Platformy Správy železnic
- Technologie pro zajištění služeb
- Architektonické principy
- Architektonické vzory
- Popis principů využití Platformy Správy železnic

Katalog dostupných ICT služeb, technologií a architektonické principy a vzory je nutné respektovat při plánování využití služeb a při návrhu ICT řešení.

Služby Platformy Správy železnic jsou seskupeny do níže uvedených kategorií:



Obrázek 1: Kategorie služeb Platformy

Funkčnost jednotlivých služeb v dané kategorii je zajištěna možnými kombinacemi komponent, které jsou uvedeny v kapitole Část VI. Technologie Platformy Správy železnic.

Dodávaná komponenta musí být schopna využívat služby Platformy SŽDC na níže uvedených vrstvách.

Není-li ve výběrovém řízení uvedeno jinak, jsou jednotlivé vrstvy Platformy soutěženy samostatnými výběrovými řízeními.

Soulad s Platformou Správy železnic je využit při hodnocení nabídek v zadávacích řízeních z pohledu compatibility nově pořizovaných technologií se stávajícími.

Hodnotící kritéria Platformy se uplatňují při specifikaci zadání.

V hodnocení nabídek z pohledu souladu s Platformou jsou hodnoceny i náklady životního cyklu nových technologií a náklady jejich standardizace do prostředí Správy železnic.

Část IV. Motivace

Motivací pro Platformu Správy železnic je:

- Zajištění schopnosti převzetí řešení do provozu.
- Zajištění schopnosti dlouhodobého provozu řešení.
- Zajištění schopnosti dlouhodobého rozvoje řešení.
- Posilování interního know-how v preferovaných ICT oblastech.
- Standardizace poskytovaných ICT služeb.
- Homogenizace ICT prostředí Správy železnic.
- Nákladová efektivita.
- Maximalizace využití kapacit a funkcionalit stávajících technologií.

Uvedená motivace vede na následující definici cílů Platformy Správy železnic:

- Platforma Správy železnic je transparentní.
- Platforma Správy železnic je jednoznačná.
- Platforma Správy železnic je průběžně aktualizována.
- Platforma Správy železnic je veřejně dostupná a publikována.
- Platforma Správy železnic je zdrojem informací pro interní i externí týmy pracující na návrhu a dodávce ICT řešení.

Část V. Služby platformy Správy železnic

Tato kapitola popisuje seznam komoditních ICT služeb a jednotlivých HW/SW komponent, které tvoří standard v rámci Správy železnic.

Cílem je zajistit ve fázích přípravy poptávky, návrhu ICT řešení a realizace dodávky kompatibilitu se stávajícím ICT prostředím a v maximální míře využít již provozované komponenty a technologie.

Seznam služeb a komponent je průběžně aktualizován.

ICT služby Platformy jsou rozděleny do následujících skupin (kategorií):

- **INFRASTRUKTURNÍ**
Infrastrukturní službou je míněno poskytování IT infrastruktury na úrovni HW, virtualizace, operačních systémů a diskových úložišť.
- **PLATFORMNÍ**
Platformní služba poskytuje aplikační, databázovou či integrační platformu (middleware), který integruje ostatní aplikace a služby do jednoho spolupracujícího celku. Podporuje standardizované komunikační protokoly a formáty dat.
- **PODPŮRNÉ**
Podpůrné služby zajišťují komplexní správu a provoz IT infrastruktury. Například monitorovací systémy, zálohování, reporting.

V.1 Infrastrukturní služby

Infrastrukturní služby zajišťují poskytování IT infrastruktury na úrovni HW, virtualizace, operačních systémů, diskových úložišť a souborových serverů.

V rámci platformy Správy železnic jsou poskytovány tyto infrastrukturní služby:

- Služby zabezpečených Fyzických serverů bez operačního systému
- Služby zabezpečených Fyzických serverů s operačním systémem
- Služby zabezpečených Virtualizovaných serverů bez operačního systému
- Služby zabezpečených Virtualizovaných serverů s operačním systémem
- Služby zabezpečených Datových úložišť

V.1.1 Služby zabezpečených Fyzických serverů bez operačního systému

| Služba | Výrobce | Odkaz |
|----------------------|---------|---|
| Huawei_X86_64 | Huawei | https://e.huawei.com/en/products/servers/rh-series |
| HP_X86_64 | HP | https://buy.hpe.com/us/en/servers/mission-critical-x86-servers/c/1010550750 |

V.1.2 Služby zabezpečených Fyzických serverů s operačním systémem

| Služba | Výrobce | Odkaz |
|----------------|-----------|---|
| Windows Server | Microsoft | https://www.microsoft.com/cs-cz/cloud-platform/windows-server |
| Linux SLES | Linux | https://www.suse.com/ |
| Linux Centos | Linux | https://www.centos.org/ |
| Linux RedHat | Linux | https://www.redhat.com/en/technologies/linux-platforms/enterprise-linux |

V.1.3 Služby zabezpečených Virtualizovaných serverů bez operačního systému

| Služba | Výrobce | Odkaz |
|-----------|-----------|---|
| VMware | Vmware | https://www.vmware.com/cz.html |
| Hyper-V | Microsoft | https://docs.microsoft.com/cs-cz/windows-server/virtualization/hyper-v/hyper-v-server-2016 |
| Oracle VM | Oracle | |

V.1.4 Služby zabezpečených Virtualizovaných serverů s operačním systémem

| Služba | Výrobce | Odkaz |
|---------------------|-----------|---|
| VMware.x86_64.Win | VMware | https://www.vmware.com/ |
| HyperV.x86_64.Lnx | Microsoft | https://docs.microsoft.com/cs-cz/windows-server/virtualization/hyper-v/hyper-v-server-2016 |
| VMware.x86_64.Lnx | VMware | https://www.vmware.com/ |
| HyperV.x86_64.Win | Microsoft | https://docs.microsoft.com/cs-cz/windows-server/virtualization/hyper-v/hyper-v-server-2016 |
| Oracle VM.OracleLnx | Oracle | |

V.1.5 Služby zabezpečených Datových úložišť

| Služba | Výrobce | Odkaz |
|---|---------|---|
| Huawei.aplikační úložiště Oceanstore 5800v3 | Huawei | https://support.huawei.com/enterprise/en/enterprise-storage/oceanstor-5800-v3-pid-21041237 |
| Huawei. backup úložiště Oceanstore 5500v3 | Huawei | https://support.huawei.com/enterprise/en/enterprise-storage/oceanstor-5500-v3-pid-21122039 |
| HP | HP | https://www.hpe.com/cz/en/storage.html |

V.2 Platformní služby

Platformní služba poskytuje aplikační, webovou, databázovou či integrační platformu (middleware). Tato integruje aplikace a služby do jednoho spolupracujícího celku. Podporuje standardizované komunikační protokoly a formáty dat. Platformní služby jsou poskytovány v různých kombinacích s infrastrukturními službami HW a SW.

V rámci platformy Správy železnic jsou poskytovány tyto platformní služby:

- Služby zabezpečených Databázových prostředí
- Služby zabezpečených Aplikačních serverů, služby zabezpečených Webových serverů
- Služby zabezpečených integračních platforem

V.2.1 Služby zabezpečených Databázových prostředí

| Služba | Výrobce | Odkaz |
|-----------|-----------|---|
| Oracle DB | Oracle | https://www.oracle.com/cz/database/ |
| SAP HANA | SAP | https://www.sap.com/products/database-data-management/hana-database-management-system.html |
| MSSQL | Microsoft | https://www.microsoft.com/cs-cz/sql-server/sql-server-2019 |
| MySQL | Oracle | https://www.mysql.com/ |

V.2.2 Služby zabezpečených Aplikačních serverů, služby zabezpečených Webových serverů

| Služba | Výrobce | Odkaz |
|-----------------|-----------|---|
| Oracle WebLogic | Oracle | https://www.oracle.com/cz/middleware/technologies/weblogic.html |
| Microsoft.IIS | Microsoft | https://www.iis.net/ |
| JBoss | | https://www.redhat.com/en/technologies/jboss-middleware/application-platform |
| SAP Netweaver | SAP | https://wiki.scn.sap.com/wiki/display/ASJAVA/AS+Java+Home |

V.2.3 Služby zabezpečených integračních platforem

S výjimkou portálu Liferay Správy železnic nevyužívá žádnou technologii pro datovou, procesní či UI integraci.

| Služba | Výrobce | Odkaz |
|---------|-----------------------|---|
| Liferay | Liferay (open source) | https://www.liferay.com/ |

V.3 Podpůrné služby

Podpůrné služby zajišťují komplexní správu a provoz IT infrastruktury. Například monitorovací systémy, zálohování, reporting.

Seznam Podpůrných služeb:

- Zajištění služby monitoringu a dohledu infrastruktury a aplikací
- Zajištění služby zálohování

V.3.1 Zajištění služby monitoringu a dohledu infrastruktury a aplikací

| Služba | Výrobce | Odkaz |
|----------------------------|---------------|---|
| Zabbix | Zabbix SIA | https://www.zabbix.com/ |
| Aplikační nadstavba Zabbix | Zabbix SIA | https://www.zabbix.com/ |

V.3.2 Zajištění služby zálohování

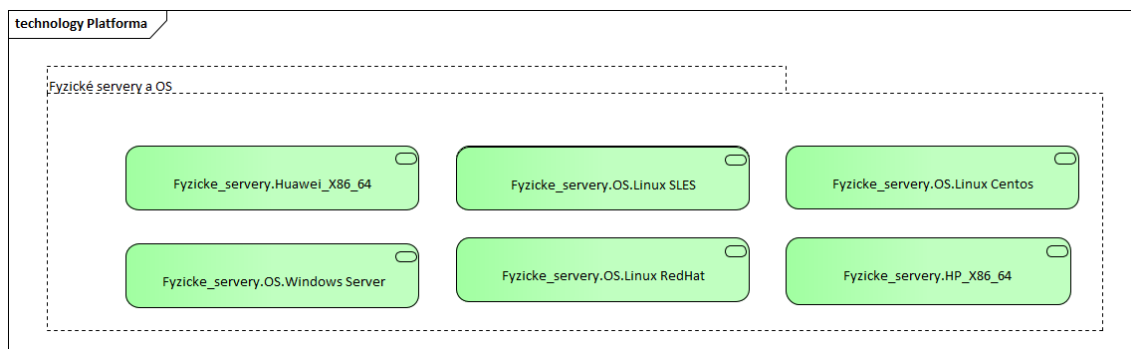
| Služba | Výrobce | Odkaz |
|-------------------------|----------|---|
| SW IBM Spectrum Protect | IBM | https://www.ibm.com/cz-en/marketplace/data-protection-and-recovery |
| SW NAS Synology | Synology | https://www.synology.com/cs-cz |

Část VI. Technologie Platformy Správy železnic

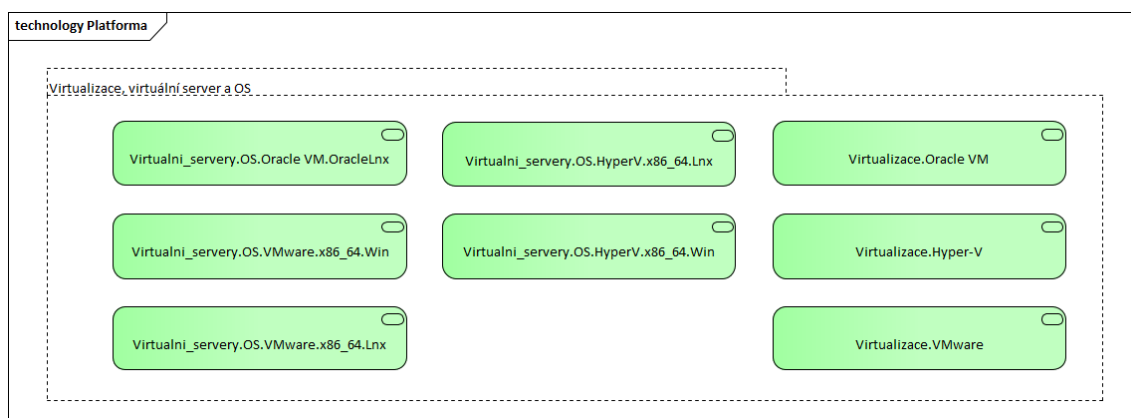
Technologie Platformy Správy železnic obsahují softwarové a hardwarové komponenty a prostředky, které jsou základním stavebním kamenem pro Služby platformy Správy železnic.

Při návrhu řešení je přípustné navrhovat využití těchto prostředků ve verzích v souladu s Architektonickými principy.

Pro nově uvolněné verze sw/hw je přípustná jejich aplikace do návrhu řešení, pokud k datu plánovaného nasazení je či bude dostupný service pack (SP) stabilizující uvolněnou verzi.

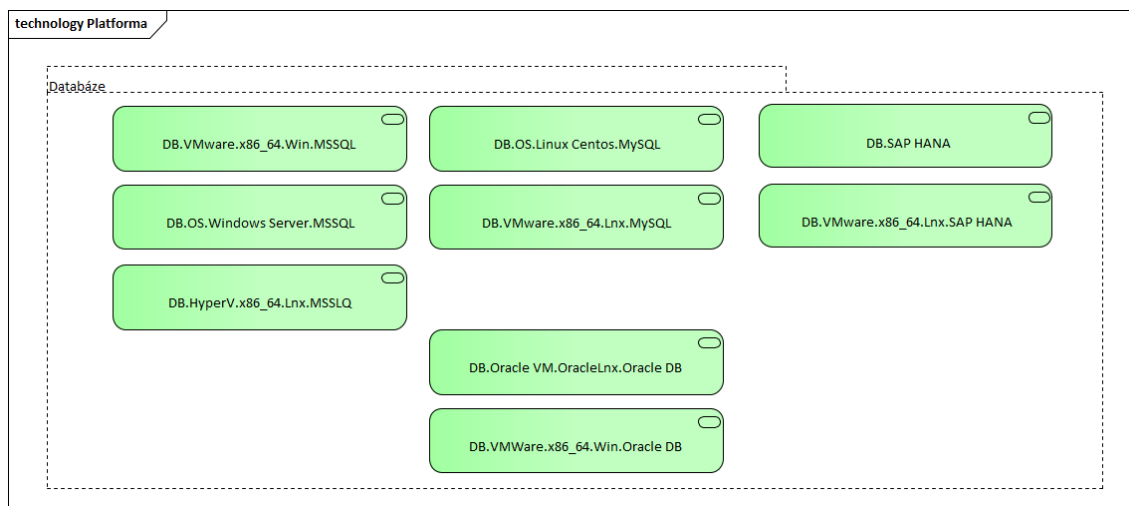


| | |
|-----------------------------------|--|
| Fyzicke_servery.Huawei_X86_64 | Výrobce: Huawei, https://e.huawei.com/en/products/servers/rh-series |
| Fyzicke_servery.HP_X86_64 | Výrobce: HP, https://buy.hpe.com/us/en/servers/mission-critical-x86-servers/c/1010550750 |
| Fyzicke_servery.OS.Windows Server | Výrobce: Microsoft, https://www.microsoft.com/cs-cz/cloud-platform/windows-server |
| Fyzicke_servery.OS.Linux SLES | Výrobce: Linux, https://www.suse.com/ |
| Fyzicke_servery.OS.Linux Centos | Výrobce: Linux, https://www.centos.org/ |
| Fyzicke_servery.OS.Linux RedHat | Výrobce: Linux, https://www.redhat.com/en/technologies/linux-platforms/enterprise-linux |

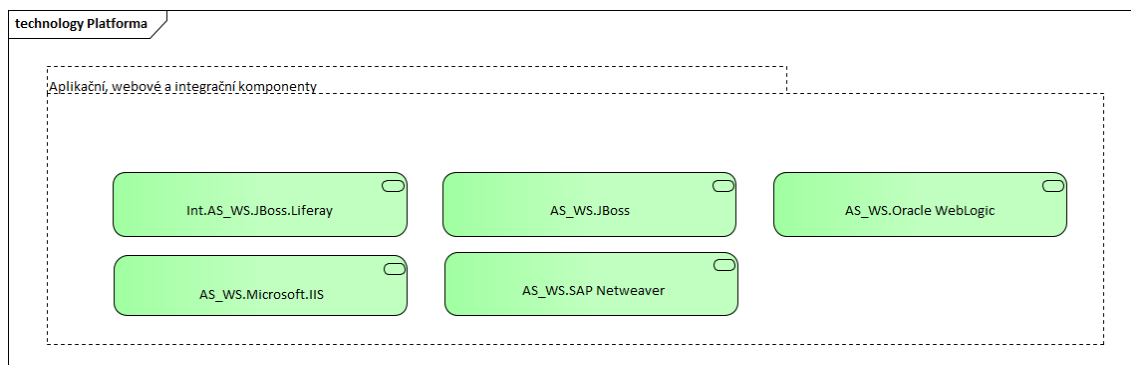


| | |
|------------------------|---|
| Virtualizace.VMware | Výrobce: Vmware, https://www.vmware.com/cz.html |
| Virtualizace.Hyper-V | Výrobce: Microsoft, https://docs.microsoft.com/cs-cz/windows-server/virtualization/hyper-v/hyper-v-server-2016 |
| Virtualizace.Oracle VM | Výrobce: Oracle |
| Virtualni_servery.OS.V | Výrobce: VMware, https://www.vmware.com/ |

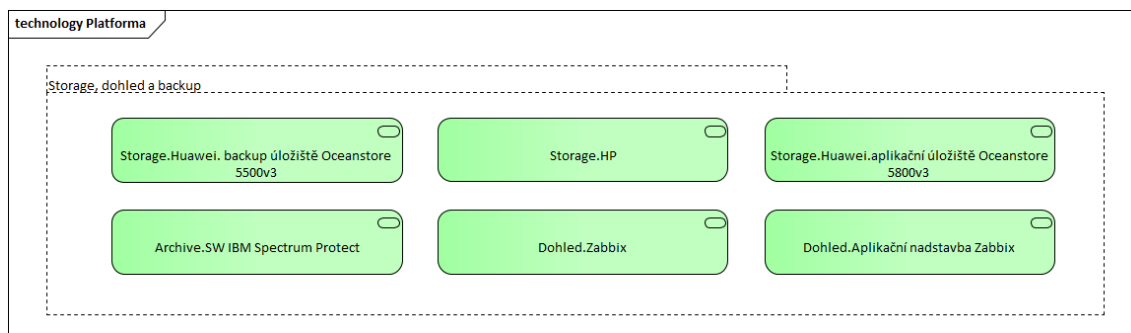
| | |
|--|---|
| Mware.x86_64.Win | |
| Virtualni_servery.OS.HyperV.x86_64.Lnx | Výrobce: Microsoft, https://docs.microsoft.com/cs-cz/windows-server/virtualization/hyper-v/hyper-v-server-2016 |
| Virtualni_servery.OS.VMware.x86_64.Lnx | Výrobce: VMware, https://www.vmware.com/ |
| Virtualni_servery.OS.HyperV.x86_64.Win | Výrobce: Microsoft, https://docs.microsoft.com/cs-cz/windows-server/virtualization/hyper-v/hyper-v-server-2016 |
| Virtualni_servery.OS.Oracle VM.OracleLnx | Výrobce: Oracle |



| | |
|--|---|
| DB.Oracle VM.OracleLnx.Oracle DB | Výrobce: Oracle, https://www.oracle.com/cz/database/ |
| DB.VMWare.x86_64.Wi n.Oracle DB | Výrobce: Oracle, https://www.oracle.com/cz/database/ |
| DB.VMware.x86_64.Ln x.SAP HANA | Výrobce: SAP, https://www.sap.com/products/database-data-management/hana-database-management-system.html |
| DB.SAP HANA | Výrobce: SAP, https://www.sap.com/products/database-data-management/hana-database-management-system.html |
| DB.OS.Windows Server.MSSQL | Výrobce: Microsoft, https://www.microsoft.com/cs-cz/sql-server/sql-server-2019 |
| DB.VMware.x86_64.Wi n.MSSQL | Výrobce: Microsoft, https://www.microsoft.com/cs-cz/sql-server/sql-server-2019 |
| DB.HyperV.x86_64.Lnx .MSSQL | Výrobce: Microsoft, https://www.microsoft.com/cs-cz/sql-server/sql-server-2019 |
| DB.VMware.x86_64.Ln x.MySQL | Výrobce: Oracle, https://www.mysql.com/ |
| DB.OS.Linux Centos.MySQL | Výrobce: Oracle, https://www.mysql.com/ |



| | |
|-----------------------------|--|
| AS_WS.Oracle WebLogic | Výrobce: Oracle, https://www.oracle.com/cz/middleware/technologies/weblogic.html |
| AS_WS.Microsoft.IIS | Výrobce: Microsoft, https://www.iis.net/ |
| AS_WS.JBoss | Výrobce: , https://www.redhat.com/en/technologies/jboss-middleware/application-platform |
| AS_WS.SAP Netweaver | Výrobce: SAP, https://wiki.scn.sap.com/wiki/display/ASJAVA/AS+Java+Home |
| Int.AS_WS.JBoss.Lifera y | Výrobce: Liferay (open source), https://www.liferay.com/ |



| | |
|--|--|
| Storage.Huawei.aplikač ní úložiště Oceanstore 5800v3 | Výrobce: Huawei, https://support.huawei.com/enterprise/en/enterprise-storage/oceanstor-5800-v3-pid-21041237 |
|--|--|

| | |
|---|---|
| Storage.Huawei. backup úložiště Oceanstore 5500v3 | Výrobce: Huawei, https://support.huawei.com/enterprise/en/enterprise-storage/oceanstor-5500-v3-pid-21122039 |
| Storage.HP | Výrobce: HP, https://www.hpe.com/cz/en/storage.html |
| Dohled.Zabbix | Výrobce: Zabbix SIA, https://www.zabbix.com/ |
| Dohled.Aplikační nastavba Zabbix | Výrobce: Zabbix SIA, https://www.zabbix.com/ |
| Archive.SW IBM Spectrum Protect | Výrobce: IBM, https://www.ibm.com/cz-en/marketplace/data-protection-and-recovery |

Část VII. Architektonické principy a vzory

Kapitola popisuje architektonická pravidla a principy, které musí být aplikovány při návrhu a realizaci ICT řešení.

Principy a vzory určují užití Služeb poskytovaných v rámci Platformy Správy železnic.

VII.1 Architektonické principy

Základní architektonické principy, které musí být uplatněny při návrhu ICT řešení.

- Bezpečnost a soulad s vnitropodnikovou legislativou
- Provozovatelnost řešení
- Ochrana dat jako klíčového aktiva Správy železnic
- Znovupoužitelnost řešení
- Nezávislost na dodavatelích
- Nezávislost na technologii
- Řízení identit
- Nákup a vývoj
- Business kontinuita jako zásadní činnost

VII.1.1 Bezpečnost a soulad s vnitropodnikovou legislativou

Navrhované řešení a procesy jím podporované musí být v souladu s legislativními a regulatorními nároky a vnitropodnikovou legislativou Správy železnic. V případě potřeby dodržovat interní předpisy budou tyto součástí zadávací dokumentace případně předány jiným způsobem oproti podpisu NDA.

Řešení musí umožnit monitorování akcí uživatelů, zejména jejich práce s daty a dokumenty.

Musí být zajištěna administrovatelnost a auditovatelnost integračních vazeb.

Vývoj a test není realizován na produkčním prostředí.

Před nasazením do produkčního prostředí je řešení prokazatelně otestováno.

Nejsou realizovány integrace mezi produkčními a neprodukčními prostředími.

Dohled je zajištěn na všech vrstvách řešení (HW, OS, DB, AS, aplikace, koncový uživatel). Musí být zajištěno napojení na centrální dohledovou konzoli.

Služby poskytované do prostředí internetu budou procházet penetračním testem.

VII.1.2 Provozovatelnost řešení

Řešení je navrženo takovým způsobem, aby bylo provozovatelné na službách a technologiích Správy železnic.

Řešení je navrženo takovým způsobem, aby bylo možné jeho převzetí do provozního prostředí Správy železnic a zajištění jeho provozu týmy a procesy Správy železnic.

Řešení je navrženo takovým způsobem, aby umožnilo škálování.

VII.1.3 Ochrana dat jako klíčového aktiva Správy železnic

Data jsou důležitým aktivem Správy železnic s významnou hodnotou.

Uživatelé řešení mají přístup pouze k datům, která nutně potřebují pro výkon své pracovní činnosti podpořené daným informačním systémem.

Řešení musí umožňovat diferencovaný přístup k datům se zohledněním uživatelských oprávnění, životního cyklu dat a jejich klasifikace.

Data se pořizují a získávají právě jednou pro všechna řešení Správy železnic.

VII.1.4 Znovupoužitelnost řešení

Řešení musí umožňovat logické oddělení dat pro současné využívání funkcionality různými subjekty (tzv. multitenant).

V rámci Správy železnic se realizuje minimalizace počtu a rozsahu používaných technologií a aplikací.

Snižováním počtu a rozsahu používaných technologií a aplikací snižujeme komplexitu správy technologického a aplikačního portfolia.

Řešení je navrhované s opakováním ověřených jednoduchých návrhových vzorů a designových principů.

Nasazování změn a nových řešení je seskupováno dle funkcionalit a cílových systémů do jednotlivých „release“. Termíny releasů jsou stanoveny jednotkou O22.

Nasazované řešení nesmí ke svému provozu vyžadovat pravidelný nutný zásah administrátora (např. restarty, čištění logů, ..)

V rámci Správy železnic usilujeme o minimalizaci počtu prostředí pro stejnou funkcionalitu.

VII.1.5 Nezavislost na dodavateli

Řešení navrhujeme s ohledem na omezení či eliminaci rizika vendor-lock.

U řešení převzatých do provozu je cíl převzetí schopnosti vytvořit build aplikace bez závislosti na dodavateli.

Usilujeme o právo zásahu do zdrojových kódů a rozvoje řešení interními kapacitami Správy železnic nebo dalšími dodavateli. Výjimku mohou tvořit jen případy, kdy by takové požadavky byly ekonomicky výrazně nevýhodné a současně by byl důvod se domnívat, že tato práva budou nadbytečná.

VII.1.6 Nezavislost na technologii

Preferujeme implementaci řešení pomocí otevřených standardů před použitím proprietárních technologií.

Preferujeme technologie s možností několika různých dodavatelů nebo implementátorů.

Usilujeme o implementaci řešení bez vazby na konkrétní produkt.

Usilujeme o implementaci aplikací bez úzké vazby na HW platformu.

Výjimku mohou tvořit jen případy, kdy by takové požadavky byly ekonomicky výrazně nevýhodné a současně by byl důvod se domnívat, že tato práva budou nadbytečná.

VII.1.7 Řízení identit

Identity jsou pro nově nasazovaná řešení centrálně řízené.

Informační systémy implementované do Správy železnic, s. o. musí podporovat zavedení jednotného přihlašování pomocí SSO (SingleSignOn). Jedná se o jednotný způsob ověřování identity oproti Active Directory.

Na produkčních prostředích nepracují uživatelé pod generickými účty.

Autorizace je řízená na základě rolí. Role jsou přiděleny k identitě uživatele. Autorizační role jsou v IDM skládány do byznys rolí.

Externí systém musí mít API pro napojení na IDM, definice požadavků je následující. Pro splnění bezpečnostního opatření dle vyhlášky Národního úřadu pro kybernetickou a informační bezpečnost č. 82/2018 Sb., o kybernetické bezpečnosti, § 20 Řízení přístupových oprávnění je nutné, aby každý informační systém implementovaný do společnosti Správa železnic splňoval požadavky na řízení přístupových oprávnění k jednotlivým aktivům informačního a komunikačního systému a pro čtení dat, zápis dat a změnu oprávnění, a § 22 Zaznamenávání událostí informačního a komunikačního systému, jeho uživatelů a administrátorů, zaznamenávání použití přístupových oprávnění v souladu s bezpečnostními potřebami a výsledky hodnocení rizik. Každý informační systém skrze integrační vrstvu tak musí poskytovat rozhraní, přes které bude možné řídit oprávnění, získávat informace o uživateli a rolích a to minimálně na této úrovni:

- Vytváření nových uživatelů
- Aktivace a deaktivace uživatelů
- Aktualizace uživatelů
- Získávání informací o uživateli
- Získávání seznamů aplikačních rolí
- Získávání seznamů uživatelů
- Získávání přesných informací o uživateli a přiřazení do konkrétních aplikačních rolí
- Přidávání uživatelů do aplikačních rolí
- Odebírání uživatelů z aplikačních rolí

VII.1.8 Architektura, nákup a vývoj řešení

U nákupu standardizovaných komerčních produktů požadujeme schopnost nastavení balíkového řešení interními kapacitami či dalšími externími dodavateli.

U standardizovaných agend preferujeme nákup a úpravu před custom vývojem nového zákaznického řešení.

Vzájemná integrace musí být realizovaná přes aplikační middleware. Integrační scénáře zajišťují, aby implementace nových funkcí v řídicí aplikaci minimalizovala vyvolané změny na straně návazných aplikací.

Preferujeme přírůstkovou integraci před přenosem kompletních informací.

Je oddělené produkční a neprodukční prostředí.

Preferujeme řešení v min. třívrstvé či vícevrstvé architektuře s min. oddělením databázové, aplikační a prezentační vrstvy.

Topologie a architektura produkčního a testovacího prostředí musí být identická, odlišovat se může ve výkonu a použitých zdrojích.

Minimalizujeme dodávku řešení s takovými úpravami, které by omezovaly nebo eliminovaly přechod na budoucí vyšší verze produktu.

V transakčních systémech preferujeme pouze základní operativní reporting. Plný reporting je implementovaný v analytických nástrojích.

Řešení je řádně dokumentované jak po stránce vývojové, provozní, uživatelské.

Případné zdrojové kódy jsou verzovány a ověřeny, že z nich je možno vytvořit interními týmy Správy železnic build aplikace. Zdrojové kódy a dokumentace jsou ukládány na standardizované úložiště Správy železnic.

Návrh prostředí reflektuje trendy technologií a zároveň business potřeby.

VII.1.9 Business kontinuita jako zásadní činnost

Navržené řešení musí odpovídat kritičnosti aplikace a požadovaným parametrům SLA.

Servisní model a parametry aplikace odpovídají bezpečnostní klasifikaci a byznysové kritičnosti aplikace.

Dle servisního modelu jsou definované plány obnovy a „disaster recovery“ postupy.

VII.2 Architektonické vzory

Architektonické vzory předepisují topologii řešení, které bude podporovat Servisní modely a dodržení SLA parametrů.

Dodavatel návrhu ICT řešení zvolí nejvhodnější architektonický vzor se znalostí konkrétních požadavků, situace a doporučení a best practices výrobce dodávaného řešení.

Základní architektonické vzory se dělí do jednotlivých skupin dle schopnosti podpořit konkrétní servisní modely.

Dostupné architektonické vzory pro návrh ICT řešení:

Skupina 1:

- V1 - Jednoúrovňové prostředí
 - prezentační vrstva na koncové stanici
 - prezentační, aplikační a datová vrstva na jednom stroji
- v2 - n-úrovňové prostředí – škálovatelné vnitřně
- V3 n-úrovňové prostředí – vnitřní škálování, vnější škálování

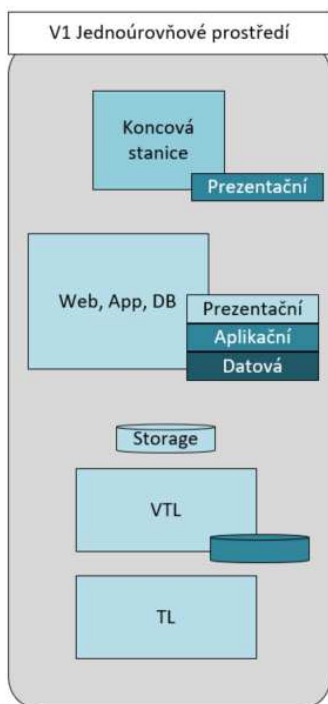
Skupina 2:

- V4 n-úrovňové prostředí – vnitřní škálování, replikace záloh
- V5 n-úrovňové prostředí – vnitřní škálování, vnější škálování, replikace záloh

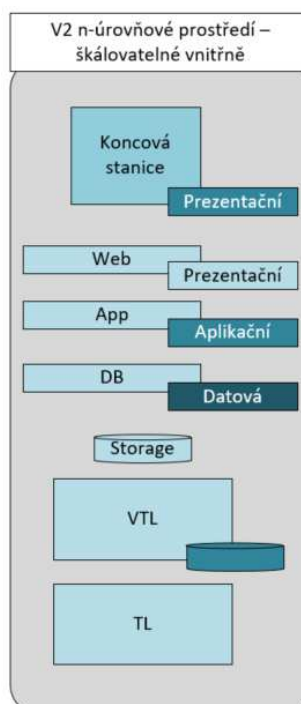
Skupina 3:

- V6 n-úrovňové prostředí – vnitřní škálování, vnější škálování, replikace storage
- V7 n-úrovňové prostředí – vnitřní škálování, vnější škálování, replikace databáze
- V8 n-úrovňové prostředí – vnitřní škálování, vnější škálování, replikace do připraveného prostředí

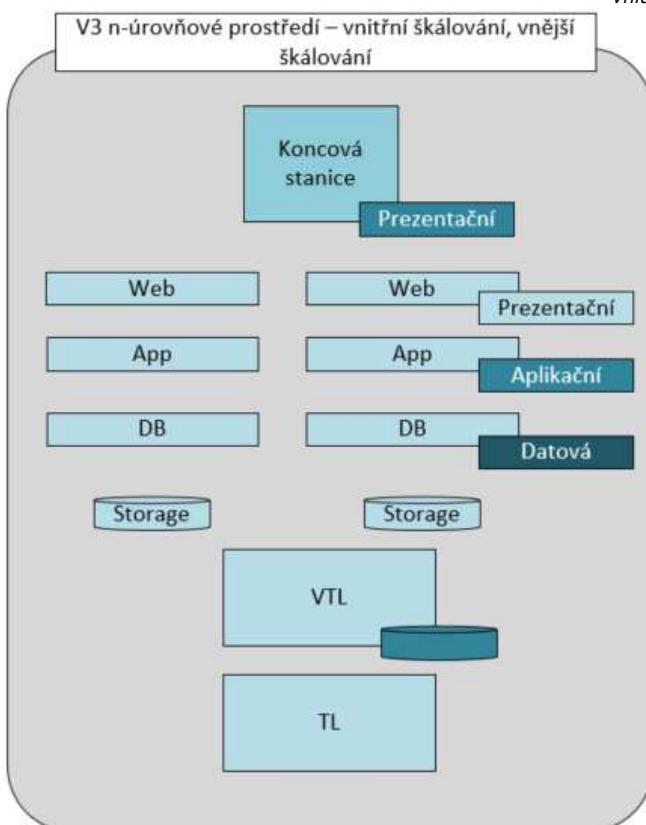
VII.2.1 Skupina 1



Obrázek 2: Jednoúrovňové prostředí



Obrázek 3: n-úrovňové prostředí - škálovatelné vnitřně



Obrázek 4: n-úrovňové prostředí - vnitřní škálování, vnější škálování

V1: Jednoduché prostředí

Jednoduché prostředí s webovým, aplikačním a databázovým serverem. Použití pro jednoduché aplikace bez požadavku na škálování a vysokou dostupnost nad rámec virtuálního prostředí.

Prostředí vhodné pro využití jako vývojové a ověřovací prostředí. Jednotlivé vrstvy odděleny na logické úrovni provozované v rámci jednoho virtuálního prostředí. Škálování scale-in (doplněním core, ram, lan, i/o)

Použitelnost pro servisní model: D

V2:n-úrovňové prostředí scale-in

n-úrovňové prostředí s webovým, aplikačním a db serverem. Použití pro jednoduché aplikace bez požadavku na škálování a vysokou dostupnost nad rámec virtuálního prostředí

Prostředí pro vývojové a ověřovací, testovací a produkční prostředí. Jednotlivé vrstvy odděleny na virtuální úrovni. Škálování scale-in (doplněním core, ram, lan, i/o)

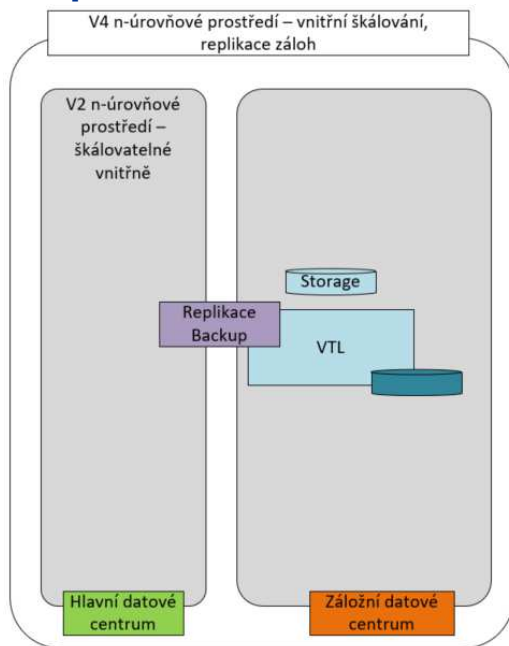
Použitelnost pro servisní model: C, D

V3:n-úrovňové prostředí scale-in, scale-out

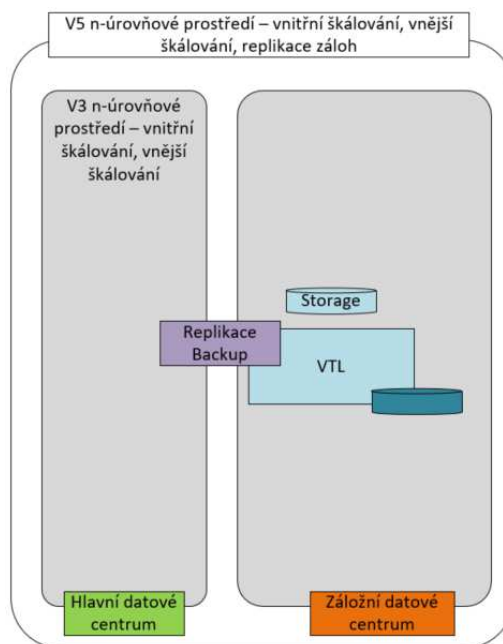
n-úrovňové prostředí s webovým, aplikačním a db serverem. Škálování na úrovni balancování webové, aplikační a db vrstvy. Vhodný pro zajištění vysoké dostupnosti.

Prostředí pro vývojové a ověřovací, testovací a produkční prostředí. Jednotlivé vrstvy odděleny na virtuální úrovni. Provozováno na samostatných virtuálních prostředích. Škálování scale-in (doplněním core, ram, lan, i/o) a scale-out s využitím balanceru. Použitelnost pro servisní model: C

VII.2.2 Skupina 2



Obrázek 5: n-úrovňové prostředí - vnitřní škálování, replikace záloh



Obrázek 6: n-úrovňové prostředí - vnitřní škálování, vnější škálování, replikace záloh

V4:n-úrovňové prostředí scale-in s replikou záloh

n-úrovňové prostředí s webovým, aplikačním a db serverem. Použití pro jednoduché aplikace bez požadavku na škálování a vysokou dostupnost nad rámec virtuálního prostředí se zabezpečením dat replikou záloh do jiné lokality.

Prostředí pro vývojové a ověřovací, testovací a produkční prostředí s požadavkem na replikaci dat. Jednotlivé vrstvy odděleny na virtuální úrovni. Škálování scale-in (doplněním core, ram, lan, i/o). Replikace záloh do záložního centra. Ověřování na úrovni obnovy dat. Použitelnost pro servisní model: B

V5:n-úrovňové prostředí scale-in, scale-out s replikou záloh

n-úrovňové prostředí s webovým, aplikačním a db serverem. Škálování na úrovni balancování webové, aplikační a db vrstvy se zabezpečením dat replikou záloh do jiné lokality. Vhodný pro zajištění vysoké dostupnosti.

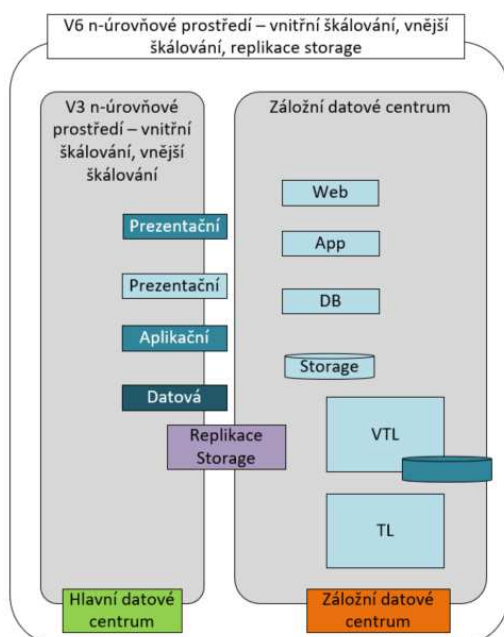
Prostředí pro vývojové a ověřovací, testovací a produkční prostředí. Jednotlivé vrstvy odděleny na virtuální úrovni. Provozováno na samostatných virtuálních prostředích.

Škálování

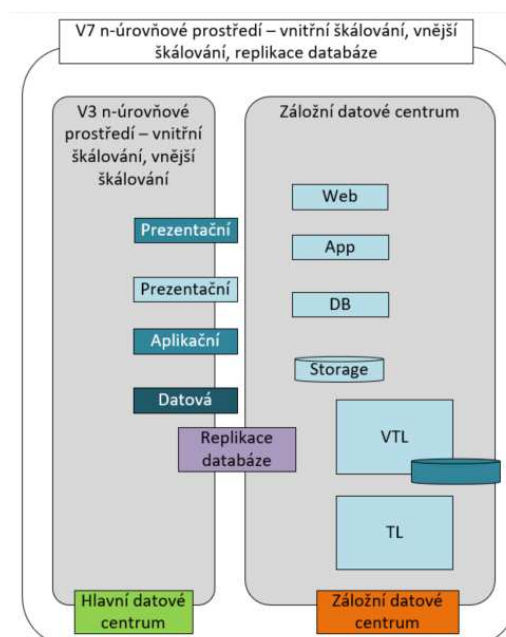
scale-in (doplněním core, ram, lan, i/o) a scale-out s využitím balanceru. Replikace záloh do záložního centra. Ověřování na úrovni obnovy dat.

Použitelnost pro servisní model: B

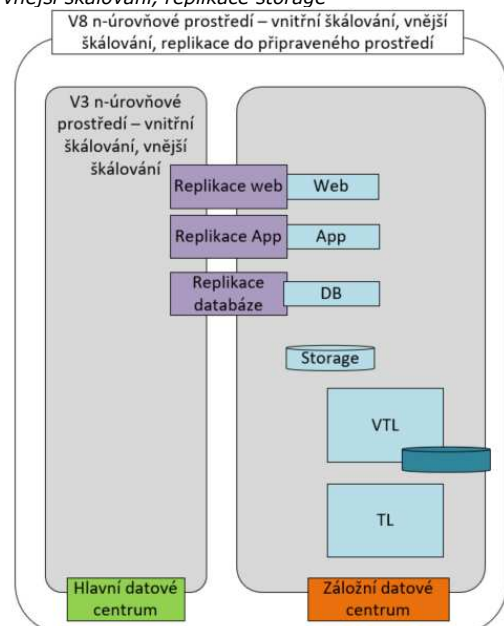
VII.2.3 Skupina 3



Obrázek 7: n-úrovňové prostředí - vnitřní škálování, vnější škálování, replikace storage



Obrázek 8: n-úrovňové prostředí - vnitřní škálování, vnější škálování, replikace databáze



Obrázek 9: n-úrovňové prostředí - vnitřní škálování, vnější škálování, replikace do připraveného prostředí

V6:n-úrovňové prostředí scale-in, scale-out s replikou storage

Řešení prostředí s webovým, aplikačním a db prostředí s požadovanou úrovní škálování a zabezpečení na jednotlivých vrstvách (farma, cluster). Zabezpečení dat replikou storage do jiné lokality. Pro zajištění Business Continuity jsou vrstvy nad storage instalovány v rámci scénáře aktivace záložního prostředí.

Prostředí pro testovací a produkční prostředí s vysokým požadavkem na dostupnost a škálovatelnost. Jednotlivé vrstvy odděleny na virtuální úrovni. Provozováno na samostatných virtuálních prostředích. Škálování scale-in (doplněním core, ram, lan, i/o) a scale-out (doplněním serverů). Replikace storage do záložní lokality. Ověřování na úrovni storage. V případě aktivace záložního prostředí dochází k doinstalování potřebných vrstev při dodržení RTO definovaného servisním modelem.

Použitelnost pro servisní model: B

V7:n-úrovňové prostředí scale-in, scale-out s replikou DB

Řešení prostředí s webovým, aplikačním a db prostředí s požadovanou úrovní škálování a zabezpečení na jednotlivých vrstvách (farma, cluster). Zabezpečení dat replikou DB do jiné lokality. Pro zajištění Business Continuity jsou vrstvy nad DB instalovány v rámci scénáře aktivace záložního prostředí.

Prostředí pro testovací a produkční prostředí s vysokým požadavkem na dostupnost a škálovatelnost. Jednotlivé vrstvy odděleny na virtuální úrovni. Provozováno na samostatných virtuálních prostředích. Škálování scale-in (doplněním core, ram, lan, i/o) a scale-out (doplněním serverů). Replikace databáze do záložní lokality. Ověřování na úrovni připraveného db prostředí. V případě aktivace záložního prostředí dochází k doinstalování potřebných vrstev při dodržení RTO definovaného servisním modelem.

Použitelnost pro servisní model: A

V8:n-úrovňové prostředí scale-in, scale-out s replikou do připraveného prostředí

Řešení prostředí s webovým, aplikačním a db prostředí s požadovanou úrovní škálování a zabezpečení na jednotlivých vrstvách (farma, cluster). Zabezpečení dat replikou do jiné lokality s připraveným prostředím v této lokalitě. Vzor je vhodný pro řešení s nejvyšším požadavkem na RTO.

Prostředí pro testovací a produkční prostředí s vysokým požadavkem na dostupnost a škálovatelnost. Jednotlivé vrstvy odděleny na virtuální úrovni. Provozováno na samostatných virtuálních prostředích. Škálování scale-in (doplněním core, ram, lan, i/o) a scale-out (doplněním serverů). Replikace do záložní lokality na potřebných vrstvách (DB, APP, WEB). Ověřování na úrovni připraveného prostředí dle zvoleného typu repliky.

Použitelnost pro servisní model: A

Část VIII. Principy aplikování platformy Správy železnic

Následující kapitola popisuje případy použití a principy aplikování platformy Správy železnic v rámci Správy železnic v konkrétních situacích.

Využití platformy Správy železnic je vyžadováno v následujících situacích:

- marketingový průzkum
- předběžná tržní konzultace
- zadávací dokumentace pro externího partnera
- žádost o informace
- poptávka / objednávka
- zpracování návrhu řešení účastníkem zadávacího řízení.
- hodnocení externích nabídek zadavatelem
- zpracování návrhu řešení interním zpracovatelem

Platforma je uveřejňována jako součást zadávacích podmínek. Služby, které jsou uvedeny v platformě jsou standardy Správy železnic, na kterých by dodávaná technologie měla být provozována.

Při hodnocení nabídek v zadávacích řízeních bude soulad s Platformou posuzován z pohledu kompatibility nově pořizovaných technologií se stávajícími.

Ve stávajícím způsobu vypisování a vyhodnocování veřejných zakázek je doporučeno, aby byla vyžadována kompatibilita s technologiemi platformy.

Část IX. Přílohy
