EVROPSKÁ UNIE
Evropský fond pro regionální rozvoj
Integrovaný regionální operační program

MINISTERSTVO
PRO MÍSTNÍ
ROZVOJ ČR

INTEGROVANÝ REGIONÁLNÍ OPERAČNÍ PROGRAM

STUDIE PROVEDITELNOSTI

-

Město Písek

Výzva IROP 28

VERZE 1.0

BŘEZEN 2017

1 Obsah

2 Úvodní informace

Obchodní jméno, sídlo, IČ a DIČ zpracovatele studie proveditelnosti	**SmartPlan s.r.o.** Antala Staška 1859/34, Krč, 140 00 Praha 4 IČ: 02474743 DIČ: CZ02474743
Členové zpracovatelského týmu, jejich role a kontakty	
Datum vypracování	31. 3. 2017

Tabulka 1 - Úvodní informace

3 Základní informace o žadateli

Obchodní jméno, sídlo, IČ a DIČ žadatele	Město Písek Velké náměstí 114/3, 397 01, Písek - Vnitřní Město IČ: 00249998 DIČ: CZ 00249998
Jméno, příjmení a kontakt na statutárního zástupce	Mgr. Eva Vanžurová Starostka
Jméno, příjmení a kontakt na kontaktní osobu pro projekt	
Nárok na odpočet DPH na vstupu ve vztahu ke způsobilým výdajům projektu (Ano x Ne)	Ne
Název projektu	Zvyšování efektivity a transparentnosti veřejné správy prostřednictvím rozvoje využití a kvality systému IKT

Tabulka 2 - Základní informace o žadateli

Městská cloudová platforma pro centralizaci výpočetních technologií

Městská cloudová platforma pro centralizaci výpočetních technologií (MCP) představuje moderní otevřené cloudové řešení, v rámci kterého bude částečně využita stávající technologie městského technologického centra umístěného v budově Městského úřadu (formou napojení na stávající informační systémy, v oblasti bezpečnostních politik a formou integrace do stávajícího systému zálohování a monitoringu), a které bude rozšířeno o infrastrukturu potřebnou pro rozvoj nových informačních systémů, a to v budoucím horizontu. MCP představuje plně virtualizované a vysoce automatizované prostředí, které umožní:

- snadnou správu uživatelských práv nad výpočetními zdroji,
- správa chodu infrastruktury (serverů, storage, sítí, operačních systémů, aplikací, informačních systémů apod.),
- centralizaci datových zdrojů,
- propojení datového fondu úřadu,
- komplexní řízení bezpečnosti,
- automatizaci celé řady procesů jak na úrovní ICT správy technologického centra, tak na úrovni úřednické.

Implementaci a rozvoj městské cloudové platformy v rámci konceptu Smart City představuje novou alternativu, jak dosáhnout dlouhodobé udržitelnosti městské IT infrastruktury i v případě dynamického rozvoje moderních aplikací pro řízení vztahů s občany, podnikateli, návštěvníky města, ale také představuje reakci na nástup moderních Internet of Things technologií nebo implementaci nástrojů Business Intelligence a technologii pro správu, analýzu a otevírání dat.

Tato platforma zároveň představuje zásadní modernizaci stávajícího stavu a zvyšuje dostupnosti a flexibilitu komunikačních a informačních systémů a infrastruktury města a bude zásadním informačním systémem v souvislosti s centry sdílených služeb. Modernizace infrastruktury z virtualizace na plně automatizovanou cloudovou platformu nabízí řadu výhod:

- možnost výběru z řady předkonfigurovaných serverů a jejich okamžité spuštění,
- otevřená platforma poskytující snadnou migraci mezi dodavateli HW i cloud operátory (odstraňuje vendor lock-in),
- vysoká dostupnost služeb - až 99,9 %,
- proaktivní monitoring a reporting jako součást implementovaného řešení,

- možnost dedikovat HW zdroje nebo využívat propojení s cloud kapacitami třetích stran (hybridní cloud),
- nastavení vlastní síťové infrastruktury v cloudu a bezpečnostní politiky,
- plná administrace prostředí s možností správy projektů a uživatelských práv, image & instance:
    - možnost výběru z řady předpřipravených konfigurací serverů a jejich okamžité spuštění (Windows, RedHat, CentOS, Ubuntu, atd.),
    - možnost nahrání vlastních image skrz webové rozhraní v libovolném formátu (VHD, VMDK, QCOW2),
    - spuštění instancí v řádech minut včetně vlastní správy snapshotů, ○ plně funkční webová konzole nativně integrovaná v HTML5, network:
    - kompletní 10Gbit síťová infrastruktura založená na technologii SDN controlleru,
    - každý hypervisor je připojen dvěma nezávislými 10Gbit linkami (20Gbit LACP), možnost vytvářet a spravovat vlastní virtuální sítě s detailními

  bezpečnostními politikami,
    - přímé routování instancí v DC Edge routeru (BGP peering) umožňuje dosahovat reálné propustnosti (bandwidth) až 9,1Gbit mezi virtuálními instancemi v rámci interní infrastruktury,
    - možnost využití virtuálních Load Balancerů, monitoring: možnost využití monitorovacího systému, orchestrace:
    - možnost využití vlastních nebo definovaných šablon pro automatizované řízení a nasazení aplikací,
    - mohou být rozšířeny o nové aplikace popsané podrobněji dále, storage:
    - využití storage SAN,
    - možnost vytvářet datové disky (volume) podle požadované rychlosti, ○ možnost vytváření snapshotů pro zálohu systému,
    - možnost přímého mapování volume (raw disk) do virtuálních instancí skrz separátní datovou síť SAN na technologii Fibre Channel s rychlostí 8Gb/s per channel,
    - spolehlivé I/O s nízkou latencí dosahující až několik tisíc IOPS na instanci, bezpečnost:
    - vytváření vlastních bezpečnostních pravidel na úrovni základního firewallu typu UDP, TCP a ICMP,
    - import a generování vlastních SSH klíčů uvnitř webového rozhraní, ○ kompletní správa prostředí skrz API nebo Command Line, ○ umožňuje velmi pohodlnou integraci s externími aplikacemi.

- jednoduchá migrace ○ díky využití plné abstrakce je možné přenést současné virtuální stroje tak, jak jsou,
- prostředí pro moderní aplikace ○ díky vlastnostem cloudu je možné oddělit vývojové prostředí ○ vývoj nových aplikací může probíhat naprosto odděleně, ale stále na stejné platformě
    - ○ aplikace jsou na závislé pouze na API
- centralizovaná správa zdrojů všechny virtuální zdroje pod centrální správou

Popis jednotlivých informačních systémů implementovaných v rámci městské cloudové platformy

V této podkapitole následuje stručný popis jednotlivých informačních systémů včetně jejich rozřazení v rámci hlavních aktivit daných výzvou a popisu jejich nových funkcionalit. Detailní popis všech informačních systémů a jejich konkrétnější technická specifikace je, v zájmu zachování kompaktnosti studie, součástí příloh této Studie.

Nové informační systémy zohledňují implementaci nařízení GDPR. Již v přípravné fázi byly definovány jednotlivé aplikace, které se týkají přímé komunikace s občany a v rámci kterých budou využívána jejich vybraná osobní data. V rámci budoucího vypisování výběrového řízení na dodavatele definovaných aplikací bude vyžadováno splnění podmínky nakládání pouze s těmi osobními údaji, které jsou nezbytné pro úplný a funkční provoz aplikací.

Zároveň se město Písek postupně připravuje na zpracování a ukládání výše uvedených dat v plném souladu s požadavky GDPR na veřejnou správu, tj.:

- zajištění zpracovávaných údajů před jejich neoprávněným či nezákonným zpracováním či ztrátou, zničením nebo poškozením,
- řádná dokumentace,
- záměrná a standardní ochrana výše uvedených údajů, plnění informační povinnosti.

Veškerá výše uvedená data bude spravovat město Písek. Za ochranu osobních údajů bude odpovědný tým odboru informačních technologií. V nejbližší době budou zároveň realizovány aktivity, směřující k vytvoření procesů sběru, zpracování a ukládání dat, předávání dat třetím stranám, způsobu plnění informační povinnosti atd.

Přehled nových informačních systémů a aplikací pro komunikaci s veřejností

Příloha č. 1 Studie proveditelnosti

Popis technického řešení

projektu města Písek v rámci

výzvy

IROP č. 28

Verze 1.0

Březen 2017

Obsah

1. Analýza a popis vlastností nového řešení

Řešení je zaměřeno na tři základní oblasti. Tou první je rozvoj nových funkcionalit stávajících informačních systémů a implementace nových informačních systémů. Druhou je modernizace, zvýšení dostupnosti a bezpečnosti podpůrných informačních systémů a třetí oblastí je transformace infrastruktury tak, aby podporovala udržitelný rozvoj stávajících, ale především nových informačních systémů a umožnila rozvoj samoobslužných procesů díky vysoké míře automatizace na všech úrovních infrastruktury TC.

Z pohledu modernizace stávajících a implementace nových informačních systémů se projekt zaměřuje především na implementaci nových informačních systémů v oblastech elektronické spisové služby a další systémy správy dokumentů, řízení vztahů se zákazníky a business intelligence. Například informační systém pro řízení vztahu s občany a firmami umožňující přímou komunikaci s úřadem, využitelná pro zlepšení krizového řízení v území. Je plánován rozvoj nových funkcionalit stávajících systémů jako například rozšíření informačního systému pro provoz spisové služby města o modul umožňující implementaci systému elektronické úřední desky, nebo rozvoj stávajícího geografického informačního systému.

Základní myšlenkou v rámci rozvoje, modernizace a zvýšení dostupnosti komunikačních a informačních systémů a infrastruktury je doplnění stávajícího technologického centra o nové, otevřené cloudové řešení, při kterém bude částečně využita stávající technologie centra (především formou napojení na stávající informační systémy, v oblasti nastavení bezpečnostních politik a formou začlenění do stávajícího systému zálohování a monitoringu), která bude modernizována o infrastruktury potřebné pro rozvoj nových informačních systémů. Jedná se o plně virtualizované a vysoce automatizované prostředí, které umožní z libovolného internetového prohlížeče spravovat uživatelská práva nad výpočetními zdroji, spravovat chod infrastruktury (servery, storage, sítě, operační systémy, aplikace), centralizovat datové zdroje a propojovat datový fond úřadu, řídit bezpečnostní služby v rámci celé infrastruktury technologického centra a to vše ve vysoké dostupnosti a s možností automatizace řady procesů jak na úrovni ICT správy centra, tak na úrovni uživatele (úředníka).

Forma oddělení nového prostředí od stávajících systémů TC je volen především z důvodu možného provozování formou hostingu v datovém centru třetí strany. **Důvodem záměru provozovat nově zřízenou infrastrukturu v externím housingu je především aktuální stav technologického centra města Písek, které je obsazeno stávající technologií města a nedovoluje rozšíření bez zásadních stavebních úprav. Do budoucna se samozřejmě počítá s přesunem nově zřízené infrastruktury zpět do datového centra města Písek, avšak až ve chvíli, kdy bude moci město alokovat dostatečné finanční prostředky na relevantní úpravu stávajícího datového centra města Písek.**

Díky této modernizaci bude infrastruktura technologického centra vysoce flexibilní a umožní udržitelný rozvoj stávajících i nových informačních systémů, zásadně zvýší bezpečnost informačních systémů a provozovaných služeb občanům. Díky své multitenanci umožní toto řešení vytvářet zcela oddělené systémy podporující provoz informačních systémů pro řízení a podporu činností příspěvkových organizací města v rámci jednotného, centrálně monitorovaného a vysoce zabezpečeného sytému.

2. Městská cloudová platforma pro centralizaci výpočetních technologií

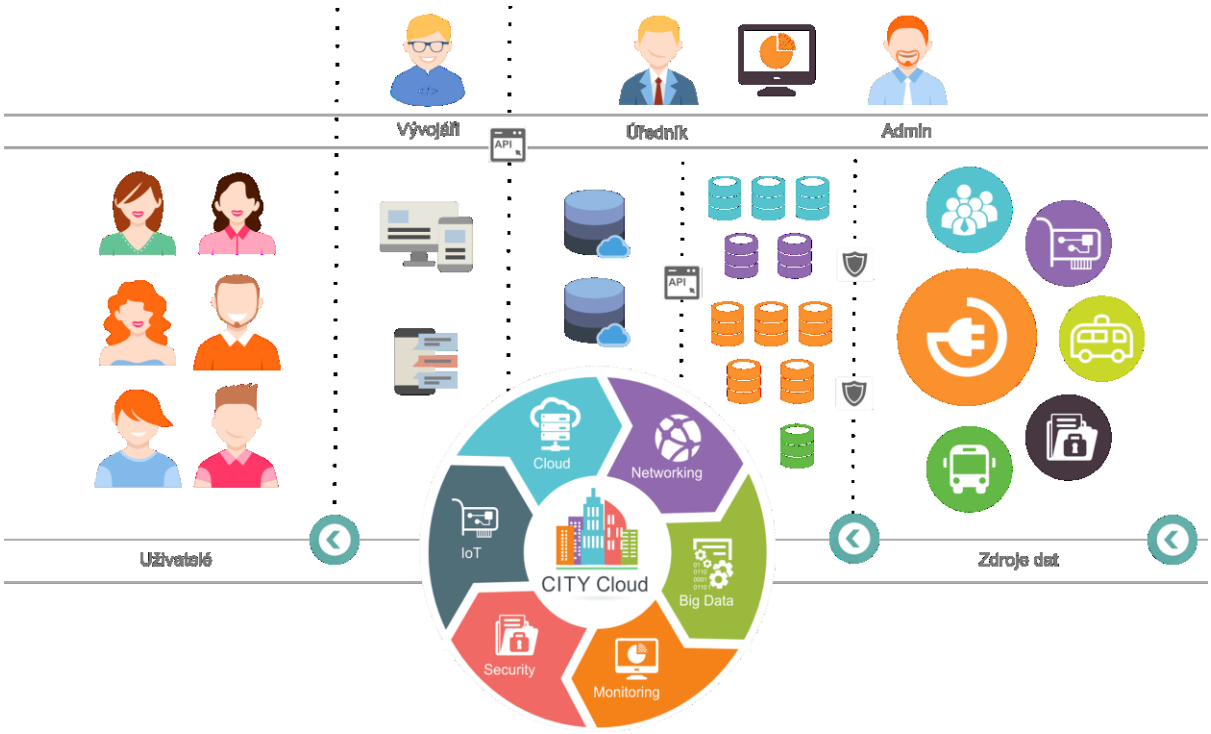
Rozvoj nových informačních systémů a aplikací v rámci konceptu Smart City Písek na Cloud řešení přestavuje novou alternativu jak dosáhnout udržitelnosti městské infrastruktury i v případě dynamického rozvoje moderních aplikací pro řízení vztahů s občany a podnikateli, nástup IoT technologií nebo implementaci nástrojů business intelligence a technologií pro správu, analýzu a otevírání dat.

Tento nový informační systém představuje zásadní modernizaci stávajícího stavu a zvyšuje dostupnosti a flexibilitu komunikačních a informačních systémů a infrastruktury města a bude zásadním informačním systémem v souvislosti s centry sdílených služeb.

Zároveň splňuje následující nové funkcionality:

- **integrace datového fondu orgánu veřejné moci (OVM) a jeho propojení s dalšími orgány, aby bylo možné data sdílet a využívat i v jiných IS veřejné správy** Navržený systém nabízí nástroje pro BigData, které zajišťují nejen integraci dat, ale také umožňují jejich další zpracování a vyhodnocování. Systém zároveň umožňuje bezpečné sdílení dat se systémy základních registrů nebo publikaci údajů z datového fondu prostřednictvím eGSB. Tuto funkcionalitu bude možné využít, ale v rámci stávajícího záměru není tato funkce relevantní.
- **interoperabilita na území státu s přesahem i např. v rámci EU**. Navržený systém disponuje univerzálním Full REST API rozhraním, které umožňuje interoperabilitu v rozsahu všech funkcí nového systému.
- **logická centralizace a celoplošná dostupnost provozních informačních systémů v rámci OVM**. Cloudový informační systém zajišťuje centralizaci všech aplikací, které jsou v ní provozovány a díky nasazení SDN (softwarově definované sítě) umožňuje plnou a bezpečnou dostupnost a možnost budoucího napojení na centrální systémy.
- **zrychlení a zjednodušení vnitřních procesů a elektronizace vnitřních procesů.** Systém automatizuje řadu standardních vnitřních procesů nejen v rámci správy a rozvoje IT, ale i v jiných oblastech. Odstraňuje nutnost předávání údajů do neelektronické formy a podporuje možnost řídit celý proces formou workflow.
- **zvýšená spolehlivost, bezpečnost a dostupnost provozních informačních systémů.** (Systém je postaven na otevřených cloud technologiích, které zásadním způsobem zvyšují flexibilitu, bezpečnost a dostupnost městské infrastruktury. Součástí systému je i pokročilý monitoring, které poskytuje komplexní informace o aktuálním stavu infrastruktury a umožňuje propojení se systémy automatizované zprávy, což napomáhá ke zrychlení a zjednodušení procesů v oblasti správy ICT infrastruktury města.

Modernizace infrastruktury z virtualizace na plně automatizovanou cloudový informační systém nabízí řadu výhod.



Obrázek 1 - CITY Cloud

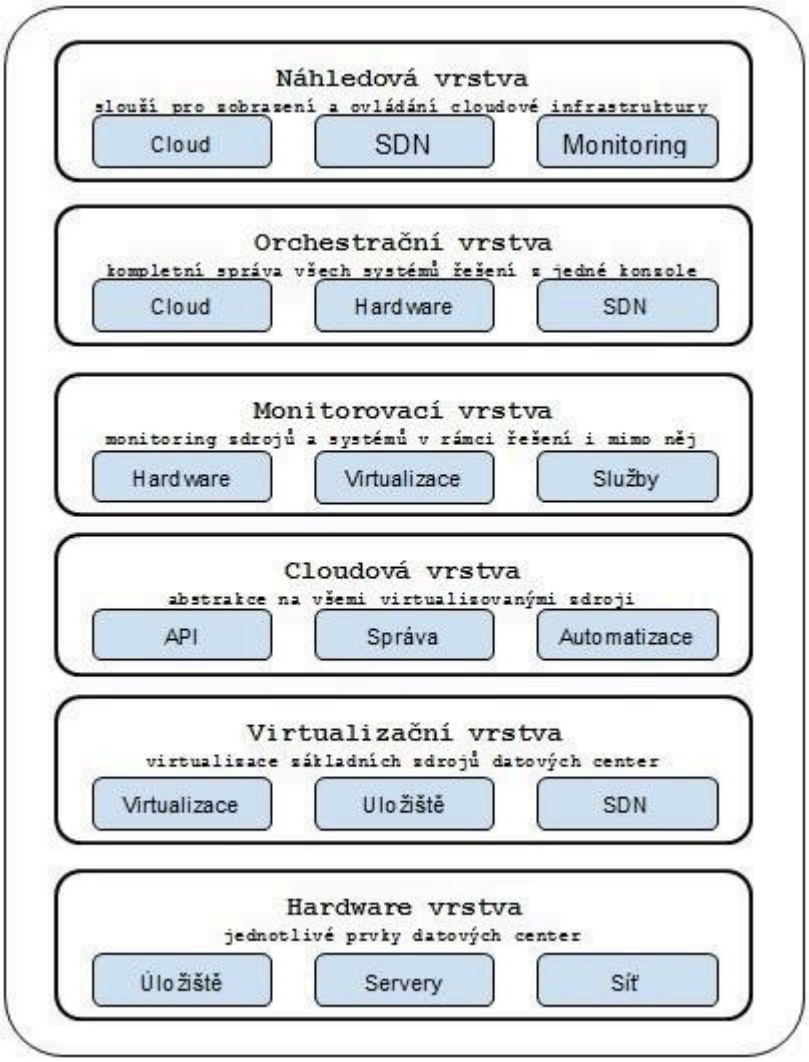
Mezi hlavní výhody tohoto řešení lze zařadit:

- možnost výběru z řady předkonfigurovaných serverů a jejich okamžité spuštění, ○ otevřená platforma poskytující snadnou migraci mezi dodavateli HW i cloud operátory (odstraňuje vendor lock-in),
- vysoká dostupnost služeb - až 99,9 %, ○ proaktivní monitoring a reporting jako součást implementovaného řešení, ○ možnost dedikovat HW zdroje nebo využívat propojení s cloud kapacitami třetích stran (hybridní cloud), ○ nastavení vlastní síťové infrastruktury v cloudu a bezpečnostní politiky, ○ plná administrace prostředí s možností správy projektů a uživatelských práv, image & instance:
  - možnost výběru z řady předpřipravených konfigurací serverů a jejich okamžité spuštění (Windows, RedHat, CentOS, Ubuntu, atd.),
  - možnost nahrání vlastních image skrz webové rozhraní v libovolném formátu (VHD, VMDK, QCOW2),
  - spuštění instancí v řádech minut včetně vlastní správy snapshotů,
  - plně funkční webová konzole nativně integrovaná v HTML5, ○ network:
  - kompletní 10Gbit síťová infrastruktura založená na technologii SDN controlleru,
  - každý hypervisor je připojen dvěma nezávislými 10Gbit linkami (20Gbit LACP),
  - možnost vytvářet a spravovat vlastní virtuální sítě s detailními bezpečnostními politikami,
  - přímé routování instancí v DC Edge routeru (BGP peering) umožňuje dosahovat reálné propustnosti

(bandwidth) až 9,1Gbit mezi virtuálními instancemi v rámci interní infrastruktury, možnost využití virtuálních Load Balancerů,

- monitoring:
  - možnost využití monitorovacího systému, orchestrace:
  - možnost využití vlastních nebo definovaných šablon pro automatizované řízení a nasazení aplikací,
  - mohou být rozšířeny o nové aplikace popsané podrobněji dále, ○ storage:
  - využití storage SAN,
  - možnost vytvářet datové disky (volume) podle požadované rychlosti,
  - možnost vytváření snapshotů pro zálohu systému,
  - možnost přímého mapování volume (raw disk) do virtuálních instancí skrz separátní datovou síť SAN na technologii Fibre Channel s rychlostí 8Gb/s per channel,
  - spolehlivé I/O s nízkou latencí dosahující až několik tisíc IOPS na instanci, ○ bezpečnost:
  - vytváření vlastních bezpečnostních pravidel na úrovni základního firewallu typu UDP, TCP a ICMP,
  - import a generování vlastních SSH klíčů uvnitř webového rozhraní,
  - kompletní správa prostředí skrz API nebo Command Line,
  - umožňuje velmi pohodlnou integraci s externími aplikacemi.
- jednoduchá migrace
  - díky využití plné abstrakce je možné přenést současné virtuální stroje tak jak jsou, ○ prostředí pro moderní aplikace
  - díky vlastnostem cloudu je možné oddělit vývojové prostředí
  - vývoj nových aplikací může probíhat naprosto odděleně, ale stále na stejné platformě
  - aplikace jsou na závislé pouze na API ○ centralizovaná správa zdrojů
  - všechny virtuální zdroje pod centrální správou
    - síť
    - výpočetní výkon
    - úložiště
    - atd…
  - přerozdělování zdrojů dle potřeb jednotlivých projektů
  - komplexní náhled na stav zdrojů a jejich aktuální využití

Následující schéma shrnuje přehled vrstev nového řešení, které je předmětem tohoto projektu.



1.1 Náhledová vrstva

Tato vrstva poskytuje přístup ke službám koncovým uživatelům především administrátorům, vývojářům, cloudovým operátorům nebo zákazníkům. Náhledová vrstva zahrnuje grafické webové rozhraní (dashboard) a FULL REST API. Dashboard je koncipován tak, aby umožnil jednotný pohled na všechny služby privátního cloudu tzv. Single Pane of Glass. Dashboard je modulárně postaven. Jeho cílem je integrace základních modulů pro identitu, správu obrazů disků, správu disků, správu sítí, orchestraci, správu instancí atd. Díky tomu umožňuje jednotný pohled na další služby jako monitoring atd.

1.2 Orchestrační vrstva

Je nástrojem pro řízení konfigurace, ale také orchestrační platformou. Ovládá fyzická zařízení, controllery a virtuální servery. Implementuje automatizované nasazení procesů s pomocí nástrojů.

Tento proces zahrnuje 2 fáze:

o Vytvoření infrastrukturních zdrojů. o Zajištění orchestrace služeb.

V první fázi klient vytvoří nutné zdroje pro úspěšné nasazení. Po úspěšném dokončení prvního kroku je možné začít s orchestrací služeb přes "aplikační stack". Nutné je vše nastavit ve správném pořadí, čili například databázová služba musí být naistalována před aplikační službou. Kromě jednoduchého zdrojového managementu, umožňuje automatickou škálovatelnost. Tato integrace se službou monitoringu zdrojů je schopna vytvořit alarmy založené na vytížení CPU serveru ve spolupráci s činnostmi jako spinning up nebo možnost ukončení instance v případě, že CPU je přetížena, příkladem je cílová aplikace, která umožňuje přidání libovolného množství přístupových webů. Tato funkce umí automaticky ukončit instanci v případě přetížení.

1.3 Monitorovací vrstva - aplikace pro automatizaci a monitoring městského informačního systému

Monitorovací vrstva se stará o nezbytné podpůrné služby jako monitoring, metering a logging. Níže jsou jednotlivé služby rozebrány.

Monitoring
Monitoring v architektuře je navržen tak, aby byl plně kompatibilní s nejrozšířenějším open source monitorovacím nástroji. Je tedy možné použít stávající monitorovací skripty a konfigurace. Řešení je založeno na open source monitoringu, který rozšiřuje standardní monitoring o další specifické kontroly (checky) a prvky automatizace. Pro sběr metrických dat a jejich další zpracování je v cloudu využíván nástroj, který je instalován na každém serveru.

Monitoring probíhá následujícím způsobem:

o server zašle žádost o vykonání monitorovacího skriptu (checku) na klientovi, o klient akceptuje lokální/vzdálené checky dle zadané funkce, o klient vrátí metriky a provede upozornění pro vykonaný check, o klient zasílá automaticky metriky bez vnějšího příkazu.

Event Processing
Tento nástroj je využíván pro sběr dat, analýzu, monitoring a následný reporting získaných informací. Hlavní prvkem tohoto nástroje je možnost zpracovávat logy z téměř jakéhokoli zařízení, které umožňuje následující činnosti:

- sběr dat prostřednictvím čtení logových souborů, monitoring stavu serveru a akceptace klientské sítě s využitím některého z široké škály nabízených protokol,
- přenos získaných dat do standardizované vnitřní podoby s konzistentními metadaty s cílem zefektivnit manipulaci a zpracování systému,
- vyhodnocení obsahu zprávy včetně metadat na základě stanoveného souboru pravidel současně nastavení veškerých procesních filtrů, na které má být zpráva doručena,

- okamžité zpracování obsahu zprávy, vykonání agregace, zpracování a monitoring, extrakce strukturovaných dat z nestrukturovaných (například: generování strukturovaných číselných statistických dat uživatelsky přátelská pro další využití) a
- generování nových zpráv jako reportované výstupy.

Metric Processing

Cloud využívá time-series databázi. Databáze je upřednostňována pro její vysokou škálovatelnost v reálném čase. Metriky získané pomocí klienta jsou poté zasílané ke zpracování na backend, který ukládá data ve specializovaném formátu databáze. Následně je možné data vizualizovat prostřednictví webového rozhraní.

Cloudová vrstva

Vrstva cloudové abstrakce umožňuje jednotný přístup na virtualizované zdroje skrze API. Platforma pro správu virtualizace a abstrakce hardwarových zdrojů skrze standardizované REST API. To umožňuje spravovat různorodé infrastruktury stejným způsobem.

Virtualizační vrstva

Virtualizační vrstva se stará o výpočetní zdroje, úložiště a síť. Výpočetní zdroje, obecně jako hypervisory poskytují virtualizační vrstvu nad hardware pro jednotlivé zdroje RAM a CPU. Starají se o virtuální instance a jejich běh. Níže je uveden přehled požadovaných funkcionalit.

Úložiště

Existuje několik typů využití úložiště, které vychází z typu uložených dat:

- persistentní úložiště - existuje zvenku instance (volume, object storage),
- dočasná úložiště - je přidělená instancím a maže se společně se smazáním instance (image instance).

Požadované typy úložišť v cílovém řešení:

- file system - používá se pro dočasné storage virtuálních strojů (vmdk, vhv, qcow2, atd.). Compute služba řídí dočasnou storage. Ve výchozím nastavení, ukládá disky virtuálních serverů jako dočasné soubory na lokálním disku Compute nodů (hypervizorů),
- bloková storage - řídí vytváření, připojování a odpojování blokových zařízení pro servery.

Networking

Cloud obsahuje NFV/SDN řešení - služba, která poskytuje NaaS (Networking as a Service). Služba má „tenant-facing API pro definování síťové konektivity v cloudu a operátorům poskytuje možnost znásobení různých síťových technologií sloužící k posílení cloudového networkingu. Každý projekt má virtuální router s jedním nebo více privátními sítěmi, které umí komunikovat s vnějším světem. To umožňuje plnou „routing“ izolaci pro každého uživatele privátní sítě.

SDN

SDN je open source síťová virtualizovaná platforma pro cloud, která je poskytovaná jako plugin v modulu. Jedná se o typ NVO SDN (Network Virtualization Overlay). V kontrastu s tím umožňuje další elementy NFV (Network Virtualization Functions jako FWaaS nebo odkaz zákazníka MPLS VPN. Jeho velkou výhodou je distribuovaná architektura, která poskytuje vysokou spolehlivost a funkčnost při výpadku napájení. Je zde i možnost kombinovat odlišné geo-lokace za použití jednoho SDN.

1.4 Předpokládaná specifikace HW pro cílové řešení

1.4.1 Datové úložiště

Pro cloudový informační systém je nutné dodat nové virtualizované úložiště na technologii iSCSI(10G), které umožňuje následující operace včetně všech potřebných licencí pro jejich provádění:

● Požadované vlastnosti ○ Create Volume ○ Delete Volume ○ Attach Volume ○ Detach Volume ○ Extend Volume ○ Create Snapshot ○ Delete Snapshot ○ List Snapshots ○ Create Volume from Snapshot ○ Create Volume from Image ○ Create Volume from Volume (Clone) ○ Create Image from Volume ○ Volume Migration (host assisted) ○ QoS ○ Volume Replication ○ Consistency Group

Úložiště má dosahovat čisté kapacity 40TB(při použití minimálně RAID6+Hot Spare) pro potřeby nového prostředí a možnosti migrace stávajícího. Dále je možné jako datové úložiště využít stávající hardware, jehož specifikace je uvedena výše.

Úložiště bude propojeno s cloudem pro management skrze LAN(1G), iSCSI minimálně 2x 10G LAN. Dále je požadovaná vysoká dostupnost úložiště, výkon disků na úrovni 10k nebo obdobné s použitím SSD cache.

1.4.2 Servery

Pro potřeby cloudového informačního systému je vyžadováno vybrat nové servery. To z důvodu nedostatečné kapacity stávajících a jejich stáří. Minimální požadavky jsou stávající:

●1x Podpůrné systémy, minimální požadavky:

- 8x SATA-3 (6 Gb/s) SW-Raid Controller on Board C612 PCH (0,1,5,10), 2x SATA-3 DOMPorts ○ Full Remote Management (KVM over LAN,

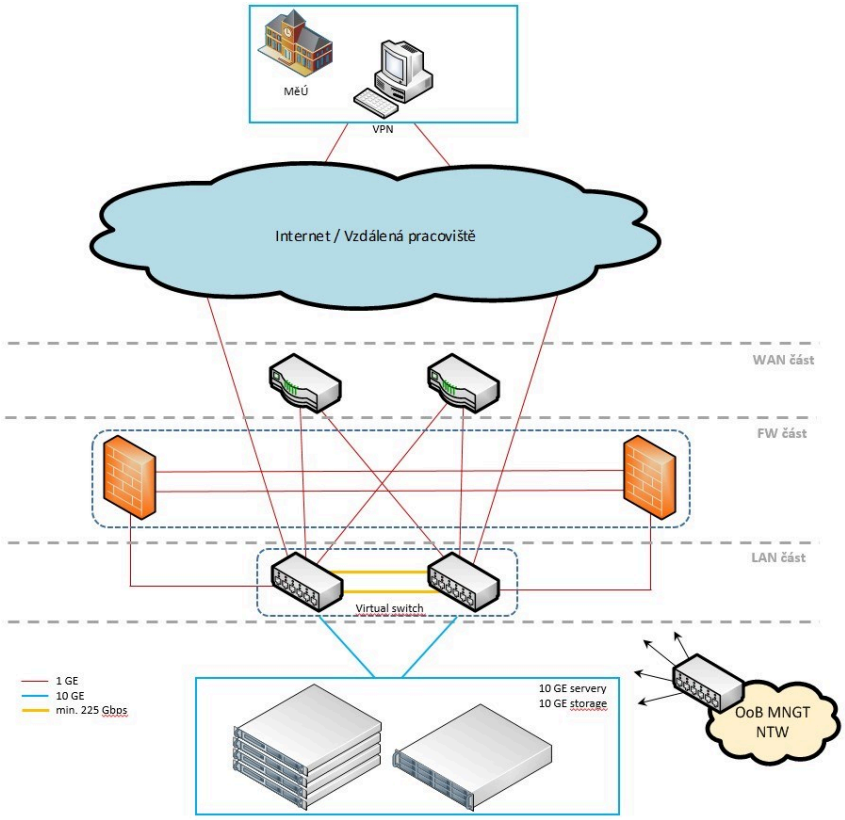
IPMI 2.0) incl. Management Software, DHCP Configuration ○ 2x Intel Xeon E5-2603v4 6-core 1.7GHz 15MB 6.4GT/s

○ 32 GB (4x 8GB) ECC Reg DDR4 2400 RAM Rank (Premium) ○ 2x 10Gbit SFP+ síťová karta umožňující jak metalické tak optické připojení ○ 480 GB SATA III SSD 2.5" ○ Extendable Mounting Rails ○ Riser Card 1x PCI-E (x8) ○ Duální napájecí zdroj vyměnitelný za chodu ○ Maximálně 1U

- 3x Controler, minimální požadavky:
  - ○ 8x SATA-3 (6 Gb/s) SW-Raid Controller on Board C612 PCH (0,1,5,10), 2x SATA-3 DOMPorts ○ Full Remote Management (KVM over LAN, IPMI 2.0) incl. Management Software, DHCP Configuration ○ 2x Intel Xeon E5-2603v4 6-core 1.7GHz 15MB 6.4GT/s ○ 192 GB (6x 32GB) ECC Reg DDR4 2133 RAM 2 Rank ○ 2x 10Gbit SFP+ síťová karta umožňující jak metalické tak optické připojení ○ 2x 2 TB SATA III WD Raid Edition 3.5" 7.2k ○ 240 GB SATA III SSD 2.5" ○ Extendable Mounting Rails ○ Riser Card 1x PCI-E (x8) ○ Duální napájecí zdroj vyměnitelný za chodu ○ Maximálně 1U
- 4x Compute, minimální požadavky:
  - ○ X10DRI: 10x SATA, 2x LAN on board ○ 8x SATA-3 (6 Gb/s) SW-Raid Controller on Board C612 PCH (0,1,5,10), 2x SATA-3 DOMPorts ○ 2x 10Gbit SFP+ síťová karta umožňující jak metalické tak optické připojení ○ Full Remote Management (KVM over LAN, IPMI 2.0) incl. Management Software, DHCP Configuration ○ 2x Intel Xeon E5-2620v4 8-core 2.10GHz 20MB 8GT/s ○ 256 GB (8x 32GB) ECC Reg DDR4 2133 RAM 4 Rank ○ 480 GB SATA III SSD 2.5" ○ Duální napájecí zdroj vyměnitelný za chodu ○ Maximálně 1U

1.4.3 Networking

Síťová vrstva je samým srdcem nové komunikační infrastruktury, a proto musí být nejenom dostatečně výkonná, ale také velmi spolehlivá, inteligentní a musí poskytnout důležité bezpečnostní funkce. Požadavky na výkon jsou dány především kapacitou připojené výpočetní technologie, která je moderně navržena na 10GE rozhraních. Spolehlivostí pak myslíme plně redundantní řešení, které spolu podporovanými HA funkcemi vytvoří prostředí pro „bezvýpadkový“ provoz aplikací. Inteligence pak znamená společné komunikační prostředí s ideálními podmínkami pro komunikaci různých aplikací a zároveň spolupráci s SDN řešením. V neposlední řadě musí network struktura poskytnou bezpečnostní kontrolu pro vybrané typy komunikace a to až po sedmou vrstvu.



1.4.3.1 LAN část

Design LAN části je středem celé síťové struktury, jak je patrno z nákresu výše, a proto musí:

1. Připojit pro start projektu 20x 10GE server/storage
2. Poskytnou double-homed připojení server/storage = připojení ke dvěma fyzicky odděleným prvkům (LAG/LACP)
3. Připojit „cluster“ Firewalů pomocí 4x1GE v opět v režimu double-homed
4. Připojit WAN část 4x1GE interface v režimu double-homed
5. Být připravena na rozšíření požadovaných server/storage o 2/3tiny počáteční kapacity = +14x 10GE portů
6. Tvořit virtuální celek, tzv. virtual switch, z hlediska managementu a běžících L2/L3 protokolů

7. Být každý fyzický box redundantní na úrovni pasivních částí, napájení chlazení
8. Být plně redundantní z hlediska připojení dalších částí= realizovaná dvěma fyzickými boxy
9. Být plně redundantní na úrovni „control plane“ = každý box musí být schopen bezvýpadkově převzít úlohu řídícího prvku a to pro L2/L3 protokoly (podpora Non-stop routing, Non-stop bridging)
10. Být plně redundantní na úrovni „forwarding plane“ = propojení do virtuálního switche musí být realizováno minimálně dvěma propojeními.

Dále musí být LAN struktura výkonná, tedy:

1) Poskytnout non-blocking architekturu z hlediska každého fyzického boxu a požadovaných připojených interface => až 34x 10GE
2) Disponovat propojení do virtuálního switche s maximální „oversubscription“ 2:1 = 225Gbps – může být realizováno násobný xGE propojením

Z hlediska podporovaných funkcí a škálovatelnosti musí podporovat v HW:

1) L2 bridging = 16k MAC adress
2) Double-homing připojených zařízení napříč fyzickými boxy = LAG/LACP
3) Virtualizaci na L2 = VLAN, QinQ
4) L3 routing = 32k route
5) IPv4/IPv6
6) L3 protokoly = minimálně statický routing a OSPF
7) L2/L3 mcast = IGMP, PIM
8) Virtualizaci na L3 = konfigurační rozdělení switche na virtuální routery tzv. vrf –lite
9) Policy based routing = konfigurace L3 protokolů pod virtuálními routery
10) Access listy na interface, VLAN
11) Data centrum funkcionality = FCoE transit switch, PFC, ETS, DCBX, iSCSI TLVs

Jelikož bude LAN struktura poskytovat komunikační prostředí pro SDN koncept je potřeba, aby byla připravena pro plnou spolupráci, což znamená:

1) Podpora VXLAN
2) Podpora OVSDB, OpenFlow
3) Podpora automatizačních nástrojů jako jsou Pupet, chef, Ansible, Python

V neposlední řadě musí být LAN část umožnit snadnou konfiguraci a správu. Za tímto účelem požadujeme společné CLI s dalšími prvky síťové infrastruktury jako je WAN část, FW část a OoB MNGT část. Boxy LAN části musí mít výšku maximálně 1U za účelem ušetření místa v DC.

1.4.3.2 FW část

Hlavním úkolem této části síťové infrastruktury je zabezpečit vybrané toky síťové komunikace, a to až po aplikační vrstvu.

FW část bude opět redundantní, tedy tvořena dvěma fyzickými boxy sestavenými z důvodu redundance do tzv. clusteru. Požadován je režim active/active, kdy jeden z FW v clusteru se stará plně o celou komunikaci, zatímco druhý se nachází se stavu „standby“ a je pouze synchronizován z hlediska session. Tento umožňuje „bezvýpadkové“ převzetí průchozího provozu standby boxem v případě výpadku aktivního boxu. Cluster bude dále umožňovat jednotnou správu obou boxů a bude se chovat navenek jako jeden network element.

Provoz, který má být kontrolovaný, bude směrovaný do FW pomocí „policy based routing“ v LAN části. Tento způsob efektivně umožní kontrolovat jenom chtěnou část provozu, a to jak uvnitř DC tak i ve směru do/z DC.

Každý box v clusteru bude připojený do LAN pomocí 2x1GE u každého boxu clusteru (s možným rozšířením na 4x1GE) a k přímým „end host“ a dalším zařízením pomocí až 6x 1GE RJ45 a 4x 1GE SFP

FW cluster bude zároveň plnit funkci ipsec koncentrátoru pro site-site VPNky se subjekty připojenými přes internet.

Z hlediska uvažovaného výkonu by jednotlivé FW měli splňovat:

- Firewall cluster připojený 3Gbps half duplex.
- IDP 400Mbps half duplex
- IPSec 600Mbps half duplex

Z hlediska logického připojení musí cluster podporovat ospf/ospfv3, vrf-lite. Kromě výše uvedených požadavků musí každý redundantní box maximální výšku 1U. FW část musí umožnit snadnou konfiguraci a správu. Za tímto účelem požadujeme společné CLI s dalšími prvky síťové infrastruktury, jako je WAN část, LAN část a OoB MNGT část.

1.4.3.3 WAN část

Úkoly WAN části můžeme rozdělit do dvou hlavních směrů.
1) Komunikace DC do WAN
2) Terminace komunikace SDN směrem z a do DC

Komunikace DC do WAN

WAN boxy dva za účelem redundance. Každý z nich bude připojení do LAN části pomocí 2x1GE v LAG/LACP režimu. Downstream a upstream komunikace bude dělena logicky na těchto LAG interfacech pomocí VLAN tagování. Mezi WAN a LAN částí poběží routing – OSPF, kde směrem do LAN (následně i na FW) bude posílána pouze default gateway.

Terminace komunikace SDN směrem z a do DC

WAN boxy kromě komunikace z LAN musí být schopni se připojit do SDN řešení. Tedy být součástí virtuální SDN sítě jak z hlediska provozu, tak i správy.

Každý z WAN boxů musí vzhledem k požadavkům výše splňovat:

1) Být vybavený 2x 1GE interface
2) Být připravený na rozšíření o minimálně 6x 1GE interface.
3) Musí být plně redundantní z hlediska pasivních prvků

Z hlediska funkcí WAN routeru je požadováno:
1) L2 bridging, 802.1Q, QinQ, IGPM/MPLD snooping, 50k MAC
2) L3: static IPv4/6, OSPFv2/3, MP-BGP (min. 2x full INET tabulka) 3) MPLS: L3VPN (i 6VPE), martiny L2VPN (EoMLS), VPLS/EVPN výhodou.
4) Access listy na interface VLAN

Z hlediska funkcí SDN routeru je požadováno:
1) L3VPN over GRE/UDP, dynamic (soft) GRE tunnel
2) VXLAN / EVPN
3) Netconf, BGP

WAN část musí umožnit snadnou konfiguraci a správu. Za tímto účelem požadujeme společné CLI s dalšími prvky síťové infrastruktury jako je LAN část, FW část a OoB MNGT část

OoB MNGT část

Tato část má pouze jeden „velmi jednoduchý“ úkol a to je připojit OoB management všech elementů v DC do jedné broadcast domény. Z hlediska počtu prvků: 2x FW, 2x LAN, 2x WAN a maximálně 40x server/storage, musí tyto/tento prvek splňovat požadavek na 44x 1GE portů.

Dále musí být tento prvek schopný komunikovat do MNGT sítě, takže je požadována minimálně 2x1GE SFP výbava. Z hlediska funkcí je nutný jen statický routing, ale pro jednoduchou správu požadujeme společné CLI s dalšími prvky síťové infrastruktury jako je LAN část, FW část a WAN část.

3. Nové informační služby a systémy provozované v cloud řešení

3.1 Přehled implementovaných aplikací

V následující tabulce jsou popsány aplikace, které budou implementovány do městského cloudového informačního systému pro centralizaci výpočetních technologií.

Navrhované aplikace	
Elektronická úřední deska	Přináší moderní a efektivní způsob zveřejňování dokumentů. Mezi hlavní přínosy tohoto řešení patří možnost nepřetržité komunikace s veřejností, pohodlný způsob vyhledávání informací ze strany veřejnosti, rychlá orientace v zobrazených informacích apod. Výhodou je, že elektronická úřední deska dokáže nahradit všechny doposud využívané vývěsky papírových dokumentů.