Příloha č. 1

Smlouvy:

Technická specifikace

Obsah

[1. Manažerské shrnutí výchozího stavu 4](#_Toc201050390)

[1.1 SAN síť 4](#_Toc201050391)

[1.2 LAN síť 4](#_Toc201050392)

[1.3 Datová úložiště 5](#_Toc201050393)

[1.4 Výpočetní servery pro ERP SAP 5](#_Toc201050394)

[1.5 Výpočetní servery pro virtualizaci platformy x86 5](#_Toc201050395)

[2 Požadavky na realizované řešení 6](#_Toc201050396)

[2.1 Záměr obnovy infrastruktury 6](#_Toc201050397)

[2.2 Požadavky na certifikaci dodávaných komponent 8](#_Toc201050398)

[2.3 Technické parametry dodávaných komponent 9](#_Toc201050399)

[2.4 SAN síť 9](#_Toc201050400)

[2.4.1 Popis současného stavu 9](#_Toc201050401)

[2.4.2 Požadavky na nové řešení 10](#_Toc201050402)

[2.5 LAN síť (síťové a bezpečnostní prvky) 13](#_Toc201050403)

[2.5.1 Popis současného stavu 13](#_Toc201050404)

[2.5.2 Požadavky na nové řešení 13](#_Toc201050405)

[2.5.2.1 Inicializační nastavení 14](#_Toc201050406)

[2.5.2.2 Migrace 15](#_Toc201050407)

[2.5.3 LAN - topologie 29](#_Toc201050408)

[2.5.3.1 LAN část DC – Fyzické provedení / SoC 32](#_Toc201050409)

[2.5.3.2 DC fabric 34](#_Toc201050410)

[2.5.3.3 WAN konektivita 46](#_Toc201050411)

[2.5.3.4 DCI konektivita 50](#_Toc201050412)

[2.5.4 L2-L7 security 54](#_Toc201050413)

[2.5.4.1 Požadavky na nové řešení 54](#_Toc201050414)

[2.5.4.2 Firewall 55](#_Toc201050415)

[2.5.5 Load balancer 72](#_Toc201050416)

[2.5.6 Management LAN 93](#_Toc201050417)

[2.5.6.1 Management DC Fabric 93](#_Toc201050418)

[2.5.6.2 Management přístup na síťové elementy 99](#_Toc201050419)

[2.6 Systémové skříně (Rack) 108](#_Toc201050420)

[2.6.1 Popis současného stavu 108](#_Toc201050421)

[2.6.2 Popis možností DC 110](#_Toc201050422)

[2.6.3 Požadavky na systémové skříně (Rack) 111](#_Toc201050423)

[2.6.4 Popis dodávaného řešení - Racky 112](#_Toc201050424)

[2.7 Datová úložiště 112](#_Toc201050425)

[2.7.1 Řešení pro ukládání dat 112](#_Toc201050426)

[2.7.1.1 Popis současného stavu 112](#_Toc201050427)

[2.7.1.2 Požadavky na nové řešení 112](#_Toc201050428)

[2.7.1.3 Disková pole pro produkční provoz 113](#_Toc201050429)

[2.7.1.4 Disková pole pro zálohování dat 121](#_Toc201050430)

[2.7.1.5 Páskové knihovny 127](#_Toc201050431)

[2.7.2 Řešení pro zálohování a ochranu dat 130](#_Toc201050432)

[2.7.2.1 Popis současného stavu 130](#_Toc201050433)

[2.7.2.2 Požadavky na nové řešení 130](#_Toc201050434)

[2.7.2.3 Zálohování 131](#_Toc201050435)

[2.7.2.4 Správa klonovacích (hardwarový snapshot) funkcí 134](#_Toc201050436)

[2.7.2.5 Detekce ransomware hrozeb 137](#_Toc201050437)

[2.8 Výpočetní servery pro ERP SAP 141](#_Toc201050438)

[2.8.1 Popis současného stavu 141](#_Toc201050439)

[2.8.2 Požadavky na nové řešení 141](#_Toc201050440)

[2.8.3 Požadavky na výkon 142](#_Toc201050441)

[2.9 Zálohovací a dohledové servery 149](#_Toc201050442)

[2.9.1 Popis současného stavu 149](#_Toc201050443)

[2.9.2 Požadavky na nové řešení 150](#_Toc201050444)

[2.10 Výpočetní servery pro virtualizaci platformy x86 154](#_Toc201050445)

[2.10.1 Popis současného stavu 154](#_Toc201050446)

[2.10.2 Požadavky na nové řešení 155](#_Toc201050447)

[2.11 Systémový Monitoring 167](#_Toc201050448)

[2.11.1 Popis současného stavu 167](#_Toc201050449)

[2.11.2 Požadavky na nové řešení 167](#_Toc201050450)

[2.11.3 Funkční požadavky 167](#_Toc201050451)

[2.11.4 Systémové a HW požadavky 167](#_Toc201050452)

[2.11.5 Požadavky na monitorované technologie 167](#_Toc201050453)

[2.12 Migrace IS SZIF a akceptace dodávky 168](#_Toc201050454)

[2.12.1 Požadavky na realizaci migrace 169](#_Toc201050455)

[2.12.2 Postup akceptace kompletní migrace 169](#_Toc201050456)

[2.12.3 Kontroly provozovatelů IS SZIF 169](#_Toc201050457)

[2.12.4 Postup migrací dle platformy a metody 169](#_Toc201050458)

[2.12.4.1 Dílčí blok „Storage APP“ 169](#_Toc201050459)

[2.12.4.2 Dílčí blok „PowerPC“ 170](#_Toc201050460)

[2.12.4.3 Dílčí blok „x86“ 170](#_Toc201050461)

# Manažerské shrnutí výchozího stavu

Objednatel v této části dokumentu popisuje stávající technické řešení infrastruktury, které v prostředí Státního Zemědělského Intervenčního Fondu (dále jen SZIF) provozuje.

## SAN síť

SAN síť je tvořena instalací 4 kusů Edge SAN přepínači typu Cisco MDS 9148 S a 4 kusy Cisco MDS 9396 S, které umožňují propojení zařízení.

* Přepínače Cisco MDS 9148S jsou osazeny 48x 16Gbps SW SFP pro koncová zařízení a ISL propoje.
* Přepínače Cisco MDS 9396S jsou osazeny 96x 16Gbps SW SFP pro koncová zařízení a ISL propoje.

SAN přepínače jsou zapojeny tak, aby tvořily dvě fyzicky oddělené Fabric sítě. Konektivita mezi sály je realizována v každém Fabricu pomocí 16x 16Gb propoje. Konektivita mezi Core a Edge přepínači je realizována pomocí 16x 16Gb propoje pro každý Fabric.

## LAN síť

Objednatel provozuje svou infrastrukturu v lokalitě DC Chodov, která je instalována ve dvou samostatných sálech poskytující redundantní řešení. LAN je tvořena následujícími prvky a instalací:

* Dva kusy Cisco Nexus 9K jsou umístěny ve dvou fyzických boxech na každém sálu a jsou zapojeny ve vPC (Virtual Port Channel) páru tak, aby zajistily sestavení dvou Ethernetových propojů (EthernetChannel) mezi každým z nich. Propoj mezi těmito dvěma boxy je tvořen jednou linkou s rychlostí 100GbE. Synchronizace přes vPC peer-link je zajištěna dedikovaným 1GbE mgmt0 portem mezi přepínači. Port UpLink mezi sály je tvořen dvěma 100GbE linkami v jednom logickém 200GbE kanálu.
* První dvojice Extenderů FEX101 je zapojená do master přepínačů Cisco Nexus v módu Single-home 8x10GbE kabely optického vlákna Breakout.
* Druhá dvojce Extenderů FEX102 je zapojená do master přepínačů Cisco Nexus v módu Single-home 8x10GbE kabely optického vlákna Breakout.
* Boxy Cisco FirePower 4140 jsou zapojené jako samostatná zařízení v každém sále. Do boxů FirePower jsou zapojené 4x10GbE UpLink porty (2x10GbE do každého Cisco Nexus přepínače), které jsou svázané do jednoho logického kanálu s rychlostí 40GbE.
* Na Cisco FirePower boxech je instalovaný SW modul Cisco ASA, který je nakonfigurovaný v HA (High Availability) režimu active-standby a pro datovou konektivitu používá logický kanál 40GbE svého nadřazeného prvku Cisco FirePower.
* Loadbalancer boxy BIG-IP F5 i5800 jsou zapojené jako samostatná zařízení v každém sálu. Na boxech jsou virtualizované vCMP (Virual Clustered Multiprocessing) hosti, kteří fungují jako jednotlivé balancery (dmz1-p, dmz1-t, dmz2-p, dmz2-t). Balancery jsou připojeny 4x10GbE UpLink porty do přepínačů Cisco Nexus (2x10GbE do každého přepínače), které jsou svázané do jednoho logického kanálu 40GbE. vCMP hosti poté sdílí tuto konektivitu od master boxu.

V rámci životního cyklu LAN nastaly následující skutečnosti, které vyžadují upgrade celé této struktury. Jedná se zejména o:

* End of Sale a/nebo End of Life veškerých komponent v DC;
* Současný koncept řešení, je poplatný době implementace (r. 2018), který ale již nebude schopen poskytovat optimální komunikační strukturu pro aplikačně orientované služby;
* Především se jedná o nedostatečné výkonové požadavky celé LAN struktury, a to od připojení výpočetních prostředků k navazujícím výkonům DC Fabric, FW a LB;
* Dále je to nedostatečné ošetření vysoké dostupnosti a spolehlivosti (plánované výpadky a/nebo upgrade, selhání síťových elementů či topologie;

## Datová úložiště

Jako úložiště dat jsou v každé lokalitě instalovány dva nody diskového pole IBM SVC, které tvoří HA cluster využívající technologii Hyperswap pro zajištění vysoké dostupnosti dat. Dále jsou v každé lokalitě instalovány následující diskové pole:

* 2x IBM Flashsystem 900 – 10x Medium MicroLatency flash module, 8.55 TB, efektivní kapacita 160 TiB.
* 1x IBM V7000 – 1x High density expanze, 90x 1,8TB SAS 10k, 20x 7,68TB SAS SSD.
* 1x HPE 3par 8200 – 3x 2,5 HDD expanze, 5x 3,5 HDD expanze, 8x 3,84 TB SSD, 18x 1,2TB SAS 10k, 120x 6TB NL-SAS, 40x 1,8TB SAS 10k.

Tyto diskové pole jsou virtualizovány pomocí IBM SVC, které zajištuje potřebnou vysokou dostupnost diskových polí. Část kapacity diskových polí HPE je poskytnuta přímo zálohovacímu serveru bez použití IBM SVC.

## Výpočetní servery pro ERP SAP

Aktuálně Objednatelem používané servery pro provoz SAP aplikací jsou umístěny ve dvou nezávislých datových sálech. V každém z obou sálů jsou umístěny dva servery. Jeden pro provoz SAP aplikací, druhý pro provoz zálohování, instalační server a dohled.

Oba servery jsou plně virtualizované pomocí virtualizace PowerVM. Servery pro provoz SAP využívají operačního systému AIX pro databáze Oracle a aplikační servery SAP. Dále operační systém Linux RedHat for SAP pro provoz databází SAP HANA. Pro oba operační systémy jsou využívána HA řešení. Pro AIX jde o HA klastr PowerHA, pro Linux RedHat jde o pacemaker integrovaný v RHEL for SAP.

## Výpočetní servery pro virtualizaci platformy x86

Objednatel v současné době provozuje cluster dvanácti 1U fyzických x86 serverů na platformě VMware s 10GbE konektivitou a připojenými SAN blokovými úložišti přes FC16 SAN. Tyto servery jsou rozděleny do dvou datových sálů v rámci v jednoho datového centra - O2 DC Chodov (V lomech 2339/1, 149 00 Praha 4 – Chodov) v DR (Disaster Recovery) scénáři.

# Požadavky na realizované řešení

## Záměr obnovy infrastruktury

Objednatel v této části dokumentu popisuje záměr k nahrazení stávající infrastruktury pro provoz a rozvoj informačního systému SZIF a zajištění služeb provozu této infrastruktury na 72 měsíců, kdy nezbytným předpokladem pro poskytování služeb provozu po celou požadovanou dobu plnění je kompletní obměna stávající infrastruktury.

Požadované služby jsou definované v dokumentu Katalog služeb (Příloha č. 1 Servisní smlouvy: Katalog služeb).

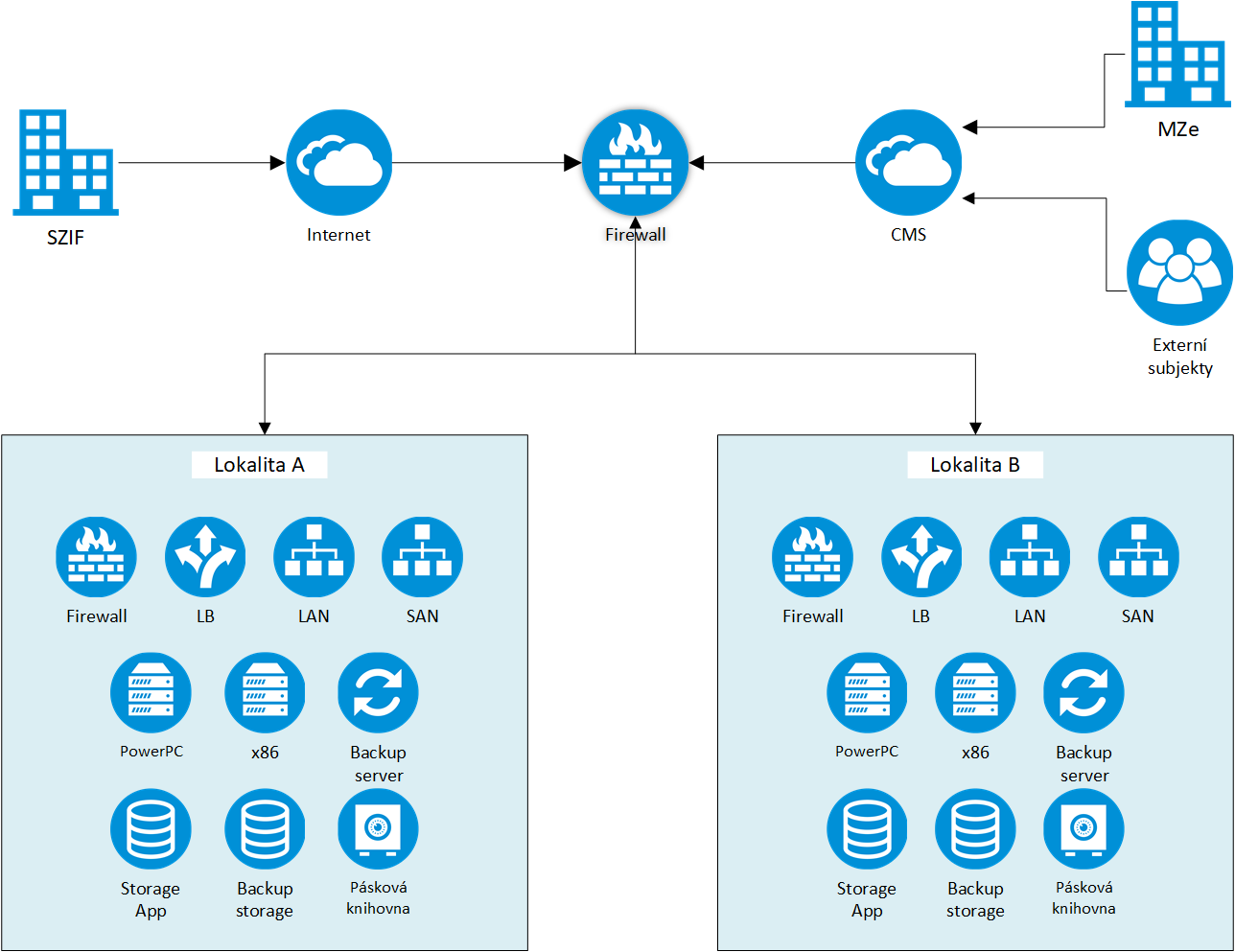
Plnění požadované dodávky v rámci tohoto projektu se musí řídit metodikou ITIL, která poskytuje strukturovaný rámec pro efektivní řízení IT projektů, produktů a IT služeb, se zaměřením na optimalizaci a zajištění kvality.

Návrh nového řešení infrastruktury musí vycházet ze standardů SAP, viz kapitola 2.2 tohoto dokumentu a respektovat veškeré požadavky na technické i provozní parametry uvedené v tomto dokumentu. Objednatel požaduje dodání řešení popsané v samostatných kapitolách jako funkční bloky. Tyto funkční bloky (oblasti) jsou dále členěny do dílčích bloků, pro které jsou uvedeny jednotlivé parametry dle požadavků Objednatele, vycházející ze znalosti provozu stávajících informačních systémů IS SZIF provozovaných na heterogenních aplikačních platformách.

Na následujícím obrázku č. 1 je schéma budoucího prostředí IS SZIF, včetně CMS (provozovaného MVČR), prostřednictvím kterého je zajištěna základní konektivita a bezpečnostní služby (pozn.: není předmětem poptávaných služeb).

Dodavatel musí počítat s realizací tohoto připojení za účelem využívání i poskytování služeb CMS, kdy propojení nesmí obsahovat slabé místo, které v případě selhání způsobí nefunkčnost celého systému (SPOF). Propoj musí být realizován plně redundantně na každé straně celkového řešení s minimální rychlostí 2x10GbE.

Dodavatel v inicializační fázi musí napojit celé dodávané řešení na stávající propoj zajištěný aktuálním poskytovatelem DC (O2 Praha Chodov).



Obrázek 1 - Architektura

Objednatel požaduje, aby veškerá nová infrastruktura byla plně redundantní a splňovala požadavky na možné zajištění provozu v režimu 7x24, viz definice služby v Katalogu služeb (viz Příloha č. 1 Servisní smlouvy: Katalog služeb). Redundance infrastruktury bude koncipovaná v módu active - active. Tedy služby jednoho systému bude možné zajistit z libovolné lokality.

Veškeré technologie, které jsou předmětem plnění, budou umístěny v lokalitě - **O2 DC Chodov (V lomech 2339/1, 149 00 Praha 4 – Chodov)**. Celé nabídnuté řešení musí být připraveno pro provoz i ve vzdálených lokalitách, kdy sál A a B budou provozovány v tzv. metroclusteru.

Z popisu řešení uvedeného v tomto dokumentu nebo vytvořeného na základě tohoto dokumentu, tj. Přílohy č. 1 Smlouvy: Technická specifikace musí být naprosto jednoznačně zřejmé, jaká je celková architektura řešení, jaké jsou použity jednotlivé komponenty pro naplnění podmínek na realizaci řešení, jaká je budoucí detailní architektura řešení s uvedenými komponentami, jaký je způsob realizace včetně harmonogramu pro instalaci, implementaci a testování funkčnosti řešení a požadovaná součinnost v podobě, jak požadovaného technického nastavení, tak personálního zajištění ze strany Objednatele a současného provozovatele informačního systému na aplikační platformě. Objednatel udává, že pokud nebude specifikováno a dohodnuto jinak v rámci definice služeb (příprava a realizace migrace), bude součinnost v podobě personálního zajištění poskytována v základní provozní době (tedy v režimu 5x12).

Řešení musí být koncipováno jako hardware, software a patřičné licence. Všechny tyto oblasti (dodané funkční celky – HW a SW) musí mít zajištěnou podporu pro dané období pro zajištění SLA dle Přílohy č. 1 Servisní smlouvy: Katalog služeb, viz kapitola 1.5 Definice SLA. Tato podpora musí být zajištěna výrobcem jednotlivých dodávaných technologii a toto musí být potvrzeno čestným prohlášením výrobce včetně toho, že odpovídá úroveň požadované podpory s úrovní podpory dodávanou s technologickými celky. Včetně požadovaných úrovní času pro reakci a opravu.

Technická specifikace řešení je rozdělena do následujících nezávislých funkčních bloků, které jsou detailněji popsány níže v jednotlivých kapitolách, včetně seznamu jejich dílčích bloků a jejich detailních specifikací a požadovaných parametrů pro všechny tyto bloky.

* Podpůrná infrastruktura:
  + Storage area network (SAN) – viz kapitola 2.3
  + Local area network (LAN) vč. Firewall – síťový, Load Balancer (LB, WAF), Antivir – viz kapitola 2.5
  + Systémové skříně (Rack) – viz kapitola 2.6
* Datová úložiště:
  + Produkční disková pole – viz kapitola 2.7.1.3
  + Zálohovací disková pole – viz kapitola 2.7.1.4
  + Páskové knihovny – viz kapitola 2.7.1.5
  + Systém pro zálohování a ochranu dat – viz kapitola 2.7.2
* Výpočetní servery pro ERP SAP – viz kapitola 2.8
* Zálohovací a dohledové servery – viz kapitola 2.9
* Výpočetní servery pro virtualizaci platformy x86 – viz kapitola 2.10
* Služby – viz Katalog služeb (Příloha č. 1 Servisní smlouvy: Katalog služeb)

## Požadavky na certifikaci dodávaných komponent

Objednatel požaduje po Dodavateli potvrzení souladu nabízeného řešení s ERP SAP podporovanými platformami. Tento soulad musí být dodavatelem doložen formou čestného prohlášení.

Dodané řešení pro zálohování musí umožnovat využívání rozhraní BACKINT a zálohovací software musí být certifikován pro zálohování platformy SAP. Pokud by nebyl zálohovací SW certifikován, může podpora SAP odmítnout spolupracovat na odstranění problému.

Dodávané řešení musí splňovat požadavky dle následujících SAP Notes a doporučení:

1. AIX/Power

* SAP Note [1578479 - SAP Support of Power Hardware with AIX](https://me.sap.com/notes/1578479/E)
* Rozcestník <https://www.ibm.com/support/docview.wss?uid=ssm1maps&wv=1>
  + [System to AIX maps (ibm.com)](https://www.ibm.com/support/pages/node/6020074)
* SAP Note [1972803 - SAP on AIX: Recommendations](https://me.sap.com/notes/1972803)
* [SAP Applications on IBM PowerVM](https://www.redbooks.ibm.com/abstracts/sg247564.html?Open) (IBM Form #: SG24-7564-01)
* [IBM Power Systems Virtualization Operation Management for SAP Applications](https://www.redbooks.ibm.com/abstracts/redp5579.html?Open) (IBM Form #: REDP-5579-00)

1. Linux

* [SAP Note 2369910](https://launchpad.support.sap.com/#/notes/2369910) – nota obsahuje ve čtvrté sekci odkazy na SAP noty o podporovaném HW
* SAP Note [1122387 - Linux: SAP Support in virtualized environments](https://me.sap.com/notes/1122387)
* SAP Note [1552925 - Linux: High Availability Cluster Solutions](https://me.sap.com/notes/1552925)

1. Linux/Power

* Rozcestník <https://www.ibm.com/support/docview.wss?uid=ssm1maps&wv=1>
  + [SAP on IBM Power Systems Running Linux | SAP Community](https://pages.community.sap.com/topics/linux/sap-on-ibm-power-systems-on-linux)

1. Oracle

* SAP Note [2478541 - Operating System Requirements for Oracle Database](https://me.sap.com/notes/2478541)
* SAP Note [2606828 - Oracle Database Roadmap for SAP NetWeaver](https://me.sap.com/notes/2606828)
* SAP Note [2799900 - Central Technical Note for Oracle Database 19c](https://me.sap.com/notes/2799900/E)

1. HANA

* HW musí být uveden v katalogu certifikovaného HW pro SAP HANA
  + [Certified and Supported SAP HANA® Hardware Directory](https://www.sap.com/dmc/exp/2014-09-02-hana-hardware/enEN/#/solutions)
* SAP Note [2188482 - SAP HANA on IBM Power Systems: Supported hardware and features](https://me.sap.com/notes/2188482/E)
* SAP Note [2055470 - HANA on IBM Power Planning and Installation Specifics](https://me.sap.com/notes/2055470)
* SAP Note [1788665 - SAP HANA Support for virtualized / partitioned (multi-tenant) environments](https://me.sap.com/notes/1788665/E)
* SAP Note [2230704 - SAP HANA on IBM Power Systems with multiple - LPARs per physical host](https://me.sap.com/notes/2230704)
* HW musí po instalaci projít SW testy dle [SAP Note 1943937](https://launchpad.support.sap.com/#/notes/1943937)

1. MaxDB + content server

* SAP Note [1178367 - SAP MaxDB: End of Support Dates](https://me.sap.com/notes/1178367)
* SAP Note [1722076 - The Future of SAP MaxDB](https://me.sap.com/notes/1722076/E)
* SAP Note [719971 - SAP Content Server release strategy](https://me.sap.com/notes/719971)
* SAP Note [2786364 - SAP Content Server and Cache Server 7.5 (and higher)](https://me.sap.com/notes/2786364)
* SAP Note [628131 - SAP MaxDB/liveCache operating system parameters on UNIX](https://me.sap.com/notes/628131/E)
* [Installation of SAP Content Server 7.5 and Higher on UNIX](https://help.sap.com/doc/1df380a7fa30410d848feb25088d4f0d/SWPM10_SP38/en-US/inst_content_server_ux_sp20.pdf)

## Technické parametry dodávaných komponent

V následujících kapitolách tohoto dokumentu jsou uvedeny popisy veškerých použitých komponent a způsob naplnění jednotlivých požadavků pro každý funkční blok uvedených v příslušných kapitolách.

## SAN síť

### Popis současného stavu

SAN infrastruktura je založená na 4x edge SAN přepínači typu Cisco MDS 9148 S a 4x core Cisco MDS 9396 S, které umožňují propojení dodávaných zařízení. Přepínače Cisco MDS 9148S jsou osazeny 48x 16Gb/s SW SFP pro koncová zařízení a ISL propoje. Přepínače Cisco MDS 9396S jsou osazeny 96x 16Gb/s SW SFP pro koncová zařízení a ISL propoje. Jsou vytvořeny a provozovány dvě fyzicky oddělené fabric sítě.

ISL propoje mezi DS jsou realizovány mezi core přepínači. Vzhledem ke vzájemné vzdálenosti stávajících DS a jejich umístění v rámci jednoho DC bylo možné v době realizace projektu dedikovat počet FC propojů mezi oběma DS bez větších omezení. Tyto propoje jsou aktuálně realizovány s využitím pasivních patchpanelů a optických, multimodových rozvodů.

FC konektivita mezi SAN přepínači v obou DS je realizována v každém fabricu pomocí 16x 16 Gb/s propoje. Konektivita mezi Core a Edge přepínači je realizována pomocí 16x 16 Gb/s FC propoj per Fabric. Celková aktuální propustnost mezi páteřními SAN přepínači je 512 Gb/s. Latence mezi SAN přepínači je vzhledem k minimální délce optických propojů (do 25 metrů) zanedbatelná a nehraje roli při FC komunikaci v rámci i mezi DS.

Veškeré prvky SAN sítě jsou prakticky na konci svého životního cyklu, a to jak ze strany morálního zastarání HW, tak i ze strany možností podpory výrobce.

### Požadavky na nové řešení

Požadavky na nové řešení vycházejí z kompletní analýzy současného stavu. Požadované řešení se kvůli zjednodušené topologii a nárokům na zprávu mění ze současné Core a Edge topologie na plně redundantní zapojení dvojice Core přepínačů do každé z lokalit. S ohledem na plánovanou životnost projektu je požadována generace SAN přepínačů postavená na technologii 64Gb/s Fiber Channel. Tato dvojice přepínačů zajistí plnohodnotnou redundanci, dostatečnou propustnost per port i pro nejnáročnější požadavky výpočetních serverů pro ERP SAP a vysokou odolnost vůči výpadku. 64Gbps technologie také umožňuje připojení stávající infrastruktury pro migraci, díky zpětné kompatibilitě s 32 resp. 16 Gb/s Fiber Channel. Toto řešení je také dostatečně flexibilní pro všechny možnosti propojení lokalit, ať se jedná o propojení dvou sálů v rámci jednoho datového centra, tak i v případě dvou oddělených datových center. Změnu lze realizovat pouhou výměnou SFP modulů.

|  |  |  |  |
| --- | --- | --- | --- |
| **SAN** | | | |
| **Číslo** | **Název komponenty** | **Part number** | **Počet kusů** |
| 1 | IBM Storage Networking SAN128B-7 | XXXXX | 4 |

Tabulka - Identifikace komponenty SAN

Zejména musí poskytovat tyto klíčové vlastnosti:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **SAN – min. 4 ks** | | | | |
| **Číslo** | **Vlastnost/komponenta** | **Požadované parametry** | **Splňuje ANO/NE** | **Skutečné parametry/Způsob splnění požadavku** |
|  | Kompatibilita | * Zařízení musí být kompatibilní s nabízenými servery a zařízeními pro ukládání dat | ANO | Nabízená zařízení jsou kompatibilní s nabízenými servery a zařízeními pro ukládání dat. |
|  | Technické vlastnosti a rozměry | * Kompatibilní s RACK 19” | ANO | Nabízená zařízení jsou kompatibilní s RACK 19“. |
|  | * Velikost v EIA (jednotek U) pro systémovou skříň 19” nesmí přesáhnout 2U. | ANO | Nabízená zařízení mají velikost 2U. |
|  | * Dodavatel uvede počet a typ napájení (C13/14 nebo C19/C20 a počet). |  | Každé z nabízených zařízení má 2 napájecí konektory C13/C14 |
|  | * Dodavatel uvede hmotnost a typický a maximální elektrický příkon. |  | Váha: 18,92 Kg  Typický elektrický příkon: 675 W  Maximální elektrický příkon: 969 W |
|  | * Dodavatel uvede, jaké jsou požadavky na elektrické jištění. |  | 1-fáze, 32A |
|  | Napájení | * Zařízení musí mít redundantní napájecí zdroje 250VAC, vyměnitelné za chodu. | ANO | Každé z nabízených zařízení má dva redundantní napájecí zdroje 250VAC, které je možné vyměnit za chodu. |
|  | Počet portů | * Min. 96 portů s rychlostí min. 64Gb/s, z toho min. 72 portů aktivních | ANO | Každé z nabízených zařízení má celkem 128 portů s rychlostí 64Gb/s. Každé z nabízených zařízení má aktivováno 72 portů s rychlostí 64Gb/s. |
| * Z 96 portů min. 49ks min. 64 Gb/s SW transceivery | ANO | Každé z nabízených zařízení je osazeno 49ks 64 Gb/s SW transceivery. |
| * Z 96 portů min. 2ks x min. 32Gb/s SW transceivery | ANO | Každé z nabízených zařízení je osazeno 15ks 32 Gb/s SW transceivery. |
| * Z 96 portů min. 13ks min. 16Gb/s SW transceivery | ANO | Každé z nabízených zařízení je osazeno 15ks 32 Gb/s SW transceivery. |
| * Z 96 portů min. 8ks min. 32Gb/s LW transceivery | ANO | Každé z nabízených zařízení je osazeno 8ks 32 Gb/s LW transceivery. |
|  | * Možnost rozšíření o dalších min. 16 SFP-DD portů pouze dokoupením licence. | ANO | Nabízené zařízení umožňuje rozšíření dalších 16 SFP-DD portů pouze dokoupením licence. |
|  | Přenosové rychlosti | * v minimálním rozsahu 8, 10, 16, 32, 64 Gb/s full duplex | ANO | Nabízená zařízení podporují následující přenosové rychlosti 8, 10, 16, 32, 64 Gb/s full duplex. |
|  | Propojovací kabely | * Odpovídající počet propojovacích kabelů pro plné zprovoznění systému. | ANO | Nabízené řešení obsahuje potřebný počet propojovacích kabelů pro plné zprovoznění systému. |
|  | Požadované vlastnosti | * ISL Trunking | ANO | Nabízená zařízení obsahují licenci na ISL Trunking. |
| * Extended Fabric – možnost propoje až do 10 km nebo více | ANO | Nabízená zařízení obsahují licenci na Extended Fabric – možnost propoje až do 10 km nebo více. |
| * Integrovaný routing mezi Fabric | ANO | Nabízená zařízení obsahují Integrovaný routing mezi Fabric. |
| * Quality of Service | ANO | Nabízená zařízení obsahují licenci na Quality of Service. |
| * Full Fabric | ANO | Nabízená zařízení obsahují licenci na Full Fabric. |
| * Vestavěná diagnostika | ANO | Nabízená zařízení obsahují licenci na vestavěnou diagnostiku. |
| * Propustnost min. 8Tb/s a latence max. 500ns | ANO | Každé z nabízených zařízení má propustnost 8,192Tb/s a latencí 460ns. |
| * Výdech ventilátorů na straně portů | ANO | Nabízená zařízení mají výdech ventilátorů na straně portů. |
|  | Záruka | * 6 let, 24x7, oprava do 24h | ANO | Nabízená zařízení mají podporu na 6 let, 24x7, s opravou do 24h. |
| * Komunikace výhradně v českém jazyce | ANO | Komunikace s podporou je výhradně v českém jazyce. |
| * Záruku garantuje přímo výrobce zařízení | ANO | Záruka je garantována přímo výrobcem |

Tabulka - Technické parametry pro SAN

## LAN síť (síťové a bezpečnostní prvky)

### Popis současného stavu

Viz kapitola 1.2 LAN síť.

### Požadavky na nové řešení

Na základě analýz trendů, současného stavu, rozvoje ICT prostředku a dlouhodobého plánování Objednatel požaduje dodat následující řešení postavené na architektuře Closovi sítě a na následujících funkcích a pravidlech.

Fabric datové centrum (dále jen DC Fabric) bude:

1. Založené na SPINE-LEAF topologii;
2. SPINE-LEAF redundance dvojité hvězdy bude pro rychlou konvergenci opřená o protokoly OSPF a iBGP;
3. SPINE-LEAF propoje budou navrženy minimálně na multiple 100GE rozhraních;
4. Připojení výpočetních prostředků bude realizováno pomocí multiple 25GE rozhraních. Tato připojení budou v režimu Dual-Homing s redundancí na L2 vrstvě s implementací tzv. multi-chassis LAG.;
5. L2/L3 služby v DC Fabric budou využívat EVPN/VXLAN technologii. Tato funkcionalita bude implementována v konfiguraci tzv. symetrického routingu, kde budou jak L2 tak i L3 VTEPy terminovány na všech „Edge zařízeních“ DC fabric, kterými jsou LEAF prvky.;
6. WAN připojení bude redundantní a provedené pomocí dedikovaných routerů;

Na základě potřeb a požadavků budou výše zmíněná pravidla realizovány v následovně:

1. Ve dvou PoDech = ve dvou sálech na jedné lokalitě;
2. Realizace musí být z hlediska HW i SW připravena na budoucí možné rozdělení ze dvou PoDů do dvou PoPů ve dvou geograficky vzdálených datových centrech včetně rozšíření o tzv. Witness site.;
3. Propojení obou PoDů bude již od startu konfigurováno s potřebnými bezpečnostnímu aspekty založené na MACsec technologii;
4. HW/SW vybavení bude již od začátku připravené pro budoucí možné rozšíření až o 30% kapacity pro připojení výpočetních prvků;
5. Na border routerech nebude provozováno full BGP = není potřeba implementace nákladných ASBR routerů. Pro WAN INET připojení tedy budou postačovat routery s výrazně nižší L3 škálovatelností a připojení bude realizováno redundantně k jednomu upstream operátorovi. Redundantně znamená jedno připojení z každého PoPu.;
6. Objednatel bude připojení za účelem využívání i poskytování služeb k CMS pomocí nejvyšší možné redundance. Tedy plně redundantně v obou PoPech datového centra;
7. L4-L7 security – NG Firewaly a Load Balancery – bude nasazenou v plně redundantních tzv. clusterech v každém z PoPů. Tento přístup poskytuje ideální řešení pro budoucí možné rozdělení do dvou geograficky oddělených PoPů.;

V rámci celého řešení musí být jednoznačně zajištěna kompatibilita mezi všemi nabízenými prvky a současně musí být poskytnuty všechny potřebné funkcionality tak, aby funkčnost celého dodaného díla byla bez vadná. Podpora řešení a aktualizace musí být zajištěna po dobu 6 let, 24x7, oprava do 24h, komunikace výhradně v českém jazyce a záruka bude garantována přímo výrobcem zařízení.

#### Inicializační nastavení

Úvodní nastavení celého systému je v detailu popsané v následujících kapitolách. Proto zde pro přehled předkládáme detailní obrázek jednoho PoDu, který popisuje tento inicializační stav včetně počtu využitých interfaců. Inicializační stav navrhujeme v následující topologii s:

* dedikovanými BORDER LEAFy pro připojení L4-L7 zařízení a připojení WAN routeru;
* dedikovanými server LEAFy pro připojení výpočetních prostředků datových center.

Topologie s využitím dedikovaných server LEAFů

**XXXXX**

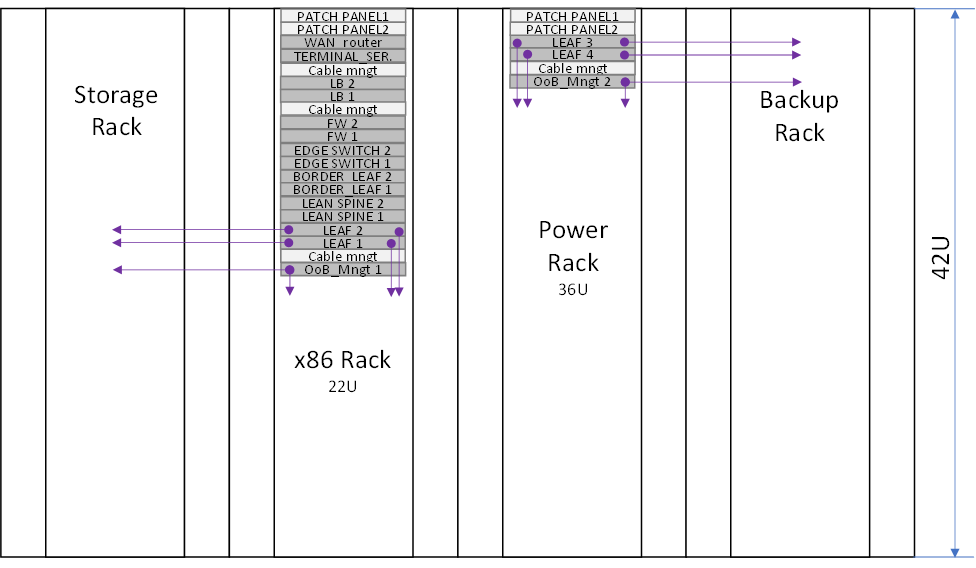
Obrázek: Úvodní nastavení systému – jeden PoD

Obrázek zahrnuje jeden PoD v inicializační fázi, druhý bude zrcadlově identický. Jsou zde dále znázorněny protokoly i terminace služeb. Terminace VXLAN je ale jasně definována jak pro L2, tak i L3 vrstvu. Dále je na obrázku definice požadavků na vzájemné propojení LAN části a počty portů pro připojení výpočetních prostředků (compute nodes) v rámci jednoho PoDu.

Nastavení celého řešení z pohledu HW a SW (licence) pro úvodní stav je již v rámci úvodní dodávky kompletní a nebude nutné dokupovat žádný dodatečný HW a SW v případě rozkročení mezi 2 datová centra, tj. při přechodu na metrocluster nebo geocluster napříč 2 datových center.

#### Migrace

Pro požadavky výše na nové řešení provedeme instalaci dle následujícího obrázku.



Obrázek: Rack s výpočetními prostředky

V rámci jednoho PoDu bude v každém ze dvou racků umístěn jeden OoB switch pro připojení jak LAN technologie, tak i výpočetních prostředků do OoB sítě. Konzolové připojení všech LAN komponent bude zajištěno přes terminálový server, který bude instalován do stojanu společně s centrální částí LAN technologie v daném PoDu. Identické rozložení technologie bude i v druhém sále/PoDu.

Celková migrace bude probíhat v následujících generických bodech:

**Postavení „parallel build“ v obou PoDech:**

* Instalace

Zahrnuje z hlediska LAN struktury:

* Instalaci LAN síťových prvků;
* Vnitřní kabeláž LAN mezi LAN síťovými prvky;
* Vnější kabeláž – na výpočetní prostředky a do WAN;
* Kabeláž Out of Band Management (dále OoB management).
* Instalace DC Fabric management systému;
* Základní Implementace a integrace

Zahrnuje z hlediska LAN struktury:

* Adresaci LAN síťových prvků;
* „přístup“ LAN síťových prvků k management nástrojům jako jsou:
* DC Fabric management systém;
* Syslog server, SNMP server, DNS server, NTP server.
* Základní konfigurace

Zahrnuje z hlediska LAN struktury:

* Fáze návrhu, plánování a nasazení datacentrové sítě (DC Fabric) a systému pro její správu;
* Základní konfigurace BGP a IGP na WAN routeru;
* Základní konfigurace a konfigurace IGP Firewallů a Load balancerů.

**Propojení současné a nové LAN struktury:**

* Instalace a konfigurace

Zahrnuje z hlediska LAN struktury:

* Propojení mezi BORDER LEAFy a Parent (Core) přepínači;
* Základní konfiguraci L2 a L3 na těchto propojích.

**Konfigurace a testy základních služeb:**

* Konfigurace

Zahrnuje z hlediska LAN struktury:

* E2E (End-to-End) příklad konfigurace L2 služby;
* E2E (End-to-End) příklad konfigurace L3 služby;
* příklad konfigurace security služby v návaznosti na L3 službu;
* příklad konfigurace load balancované služby v návaznosti na L3 službu.
* Testy

Zahrnuje z hlediska LAN struktury:

* Testy služeb vypsaných výše.

**Migrace:**

* Příprava

Vypracování migrační matice

* Detailní sepsání současného stavu;
* Definice NG (Next Generation) služeb a mapování na současné služby.
* Provedení

Zahrnuje z hlediska LAN struktury:

* Příprava služby – konfigurace;
* Migrace aplikací na nové výpočetní prostředky – není součástí Migrace LAN části infrastruktury.

Detailní návrh migrace bude stanoven v rámci realizační fáze, během analýzy a stanovení designu. Realizace migrace bude popsána v dokumentu SoW (Scope of Work) pro provedení instalace/implementace a migrace služeb a bude zahrnovat následující:

Plán migrace – Parallel Build

* + - 1. Příprava a návrh (LLD – Low Level Design).
* Analýza stávající infrastruktury (topologie, služby, závislosti).
* Návrh nové architektury včetně:
  + Rozdělení LAN technologií dle účelu;
  + Umístění LEAF (ToR) switchů, SPINE, Edge, Firewallů, LB, WAN routerů;
  + Propojení OoB a konzolového přístupu (terminálový server);
  + Propojení mezi starou a novou infrastrukturou na L2/L3 úrovni;
  + Definice NG (Next Generation) služeb a mapování na současné služby.
* Příprava testovací dokumentace.
  + - 1. Inicializace síťových prvků.
* Upgrade firmware a zahoření všech síťových zařízení;
* Předkonfigurace základních parametrů (hostname, IP, přístup).
  + - 1. Instalace infrastruktury (Parallel Build).
* Fyzická instalace do racků v obou sálech DC:
  + Montáž zařízení;
  + Napájení a kabeláž (datová i napájecí);
  + Instalace OoB switchů a terminálového serveru;
  + Redundantní rozmístění centrálních prvků (SPINE, Edge, FW, LB, WAN).

Každý rack s výpočetními prostředky bude vybaven vlastními dedikovanými LEAF (ToR) switchi, které zajistí připojení datových portů těchto technologií. Zbývající část centrální LAN technologie, včetně SPINE switchů, Edge switchů, Firewallů, Load balancerů a WAN routeru budou distribuovány redundantně, napříč stojany a PoDy, a to včetně OoB sítě a konsolového připojení všech LAN komponent přes terminálové servery.

* + - 1. Základní konfigurace a připojení.
* OoB management síť;
* In-Band přístup;
* Monitoring a management nástroje;
* Aktivace monitoringu všech boxů a sítě.
  + - 1. Instalace a implementace DC Fabric.
* Instalace Fabric Management nástroje;
* Greenfield build fáze nové DC fabric;
* Konfigurace vzorových služeb:
  + Výběr reprezentativních služeb pro testování;
  + Migrace 1:1.
    - 1. Testování vzorových služeb.
* Provedení testů a akceptace vzorových služeb;
* Vyhodnocení výsledků a případné úpravy konfigurace.
  + - 1. Migrace služeb.
* Postupná migrace služeb dle typů (typy služeb, seznam, přiřazení);
* Step-by-step procedura s testy a monitoringem každé služby;
* Zajištění plné viditelnosti a funkčnosti během migrace.
  + - 1. Odstavení staré infrastruktury.
* Odpojení staré LAN od nové (Parallel Build) po dokončení migrace všech služeb dle typů;
* Fyzické odstranění staré LAN infrastruktury.

Uvědomujeme si, že oblast LAN ovlivňuje celou migrovanou infrastrukturu SZIF, a proto nad rámec popisu migrace vrstvy LAN, uvádíme i popis migrace zbylých částí infrastruktury SZIF.

**Migrační plán celé infrastruktury SZIF**

Migrace bude probíhat po částech s cílem minimalizovat dopad na provoz.

Kritické přepojování bude probíhat po dohodě se Zadavatelem, mimo garantovanou provozní dobu.

Cílem je provést migraci bez výpadků nebo s minimálními odstávkami služeb pro koncové uživatele IS SZIF.

Architektura aplikací a SAP zůstane beze změny. Verze softwaru zůstávají stejné.

Migrace operačních systémů s IS SZIF je založena na nástrojích virtualizační platformy IBM Power a x86 VMware.

**Informační systémy a jejich vzájemné vazby nebudou migrací ovlivněny, a proto nejsou dále detailně rozebírány.**

Nová infrastruktura přinese vyšší spolehlivost, výkon (CPU, RAM, datová propustnost) a lepší možnosti škálování.

**Dopad migrace infrastruktury na aplikační architekturu SZIF:**

* Beze změn: Aplikační architektura Zadavatele vč. SAP zůstává migrací infrastruktury nedotčena;
* Zachování verzí: Verze softwaru aplikační vrstvy vč. operačních systémů, na kterých jsou provozovány zůstanou stejné;
* Virtualizace: Migrace proběhne na úrovni stávající virtualizační infrastruktury (IBM Power a x86 VMware), což zajišťuje nezávislost aplikací na konkrétním hardwaru;

Verze virtualizační infrastruktury nemá vliv na provoz OS s IS SZIF;

* Bez zásahu do IS: Vzhledem k tomu, že informační systémy a aplikace nebudou ovlivněny, jejich vnitřní vazby a architektura (včetně SAP landscape) nejsou dále rozebírány;
* Zaměření: Další popis se soustředí výhradně na migraci jednotlivých vrstev infrastruktury.

Migrační plán infrastruktury rozdělujeme do 8 základních bodů, které níže rozepisujeme.

**1. Výchozí stav (as-is) infrastruktury**

Detailní popis vychází z popisu Zadavatele, viz. kap. 1 tohoto dokumentu.

V rámci realizace projektu proběhne detailní analýza stávající infrastruktury k definici přesného postupu migrace a testovacích scénářů (topologie, seznam služeb a závislostí apod.).

Shrnutí aktuální IT infrastruktury SZIF

Datové centrum (DC)

* Umístění: O2 DC Praha Chodov;
* Struktura: 2 samostatné sály s redundantním řešením.

SAN infrastruktura

* 4× Cisco MDS 9148 S a 4× Cisco MDS 9396 S;
* Dvě fyzicky oddělené SAN Fabric sítě;
* Propojení mezi sály a přepínači: 16× 16Gb propoje.

LAN infrastruktura

* Hlavní prvky:
  + 2× Cisco Nexus 9K;
  + 2× FEX101 a 2× FEX102 (extender moduly);
  + Cisco FirePower 4140 (HA režim, 40GbE logický kanál);
  + BIG-IP F5 i5800 loadbalancery (vCMP hosti, 40GbE konektivita).

Datová úložiště

* Virtualizace polí přes IBM SVC s Hyperswap (HA cluster);
* Disková pole:
  + 2× IBM Flashsystem 900 (160 TiB efektivní kapacita);
  + 1× IBM V7000;
  + 1× HPE 3PAR 8200 (různé typy disků, část kapacity pro zálohování).
* Pásková knihovna
  + IBM TS4500 – pro dlouhodobé zálohování a archivaci.

Výpočetní servery pro ERP SAP a zálohování

* Umístění: 2 servery v každém sále (SAP + zálohování);
* Virtualizace: PowerVM;
* OS: AIX (Oracle DB, SAP), RedHat Linux (SAP HANA);
* HA řešení: PowerHA (AIX), Pacemaker (RHEL);
* Zálohování: IBM Spectrum Protect.

Výpočetní servery pro virtualizaci x86

* Rozděleny na polovinu mezi 2 sály;
* 12× 1U fyzických serverů (VMware);
* 10GbE konektivita, připojení k SAN (FC16).

**2. Cílový stav (to-be)**

Aplikační architektura včetně SAP po migraci (rozložení instancí, clustering, HA/DR) je bez změny. Cílové OS a DB (AIX/Linux, Windows, HANA/Oracle/MySQL/MSSQL/Postgres) včetně verzí budou zachovány 1:1/as-is, nemění se.

Navržená infrastruktura pro budoucí provoz a rozvoj informačního systému SZIF vychází ze standardů SAP a respektuje veškeré požadavky na technické i provozní parametry Zadavatele.

Dodání řešení obnovy infrastruktury je v souladu se všemi požadavky Zadavatele na jednotlivé funkční i dílčí bloky.

Detailní popis navržených komponent je v kap. „2 Požadavky na realizované řešení“.

Shrnutí cílového stavu infrastruktury

Lokalita a provoz:

* Infrastruktura bude umístěna v O2 DC Praha Chodov;
* 2 sály, každý vybaven 6x IBM 19" racky;
* Řešení je plně redundantní, připravené na provoz ve dvou sálech (A a B) v režimu metroclusteru, s možností rozšíření na dvě geograficky oddělená datová centra (PoPy).

Hardware, software a licence pro novou infrastrukturu budou dodány jako funkční celky.

Shrnutí komponent navržené infrastruktury:

* SAN infrastruktura s 4x IBM SAN128B-7 přepínači (64Gb/s FC);
* LAN infrastruktura:
  + Postavena na technologiích Juniper Networks a F5;
  + DC Fabric tvořen SPINE a LEAF switchi (celkem 16 switchů);
  + WAN konektivita přes INET a O2 KIVS, přímé propojení do CMS VPN;
  + DCI konektivita připravena na geografické rozdělení a „witness“ lokalitu.

Použité klíčové komponenty LAN:

* + LEAF switche: XXXXX (8 ks);
  + SPINE switche: XXXXX (4 ks);
  + WAN routery: XXXXX (2 ks);
  + Řízení přístupu a správy přes 4x OoB management switch a 2x terminálový server.

Bezpečnost (L4–L7):

* + Centralizované služby: firewall, NAT, IPsec, SSL terminace, WAF, loadbalancing;
  + 4x firewall (XXXXX), 4x loadbalancer (XXXXX).
* Datová úložiště:
  + Produkční úložiště:
* 2× IBM FlashSystem 9500 (64Gb/s FC, flash technologie);
* Výkon: až 648 759 IO/s, kapacita 1129,89 TB (dRAID6);
* Podpora detekce ransomware, kopie, zrcadlení.
  + Zálohovací úložiště:
* 2× IBM FlashSystem 5300 + 3× High Density Expansion (32Gb/s FC);
* Výkon: až 40 788 IO/s, kapacita 1273 TB (93 TB Flash, 1180 TB NL-SAS);
  + Páskové úložiště:
* LTO9 mechaniky do stávajících knihoven;
* Kompatibilita s IBM Spectrum Protect, fyzicky oddělené zálohy.
* Řešení pro zálohování a ochranu dat:
  + Koncept 3-2-1, ochrana proti ransomware a anomáliím;
  + SW: IBM Spectrum Protect + IBM Storage Defender.
* 8866 licencí pro zálohování;
* 8866 licencí pro klonování;
* 4500 licencí/měsíc pro detekci hrozeb.
  + Podpora: AIX, Linux, Windows, Oracle DB, SAP (ABAP, HANA), VMware.
* Výpočetní servery pro ERP SAP:
  + 2× IBM Power E1080 (1 na lokalitu, enterprise třída);
  + Výkon: 1 253 469 SAPs, 147 CPU, 38 912 GB RAM;
  + Virtualizace PowerVM, OS: AIX (Oracle), RHEL for SAP (HANA);
  + HA: PowerHA (AIX), Pacemaker (RHEL);
  + Zálohování: IBM Spectrum Protect.
* Zálohování a dohled:
  + 2× IBM Power S1024;
  + Výkon: 222 003 SAPs, 1 TB RAM, 8× NVMe, 25GbE + 64Gb FC;
  + Virtualizace a HA licence včetně.
* Virtualizace x86:
  + 18× Lenovo ThinkSystem SR650 V3.
* 2× Intel Xeon Gold 5520+ (28C), 1 TB RAM, 960 GB NVMe (RAID 1);
* 4× 25GbE, 2× 64Gb FC, VMware vSphere + VCF (1008 core);
  + Red Hat Enterprise Linux for Virtual Datacenters for SAP Solutions.
* Monitorovací systém GCMP for HA cluster podporuje širokou škálu technologií (OS, databáze, SAP, VMware aj.) a umožňuje flexibilní licencování.

**3. Migrace a transformace**

Migrace IS SZIF na novou infrastrukturu proběhne dle smluvního harmonogramu a dle požadavků provozovatele aplikačních vrstev.

Součástí dodávky je příprava detailního migračního plánu, harmonogramu a definice potřebné součinnosti všech stran.

Hlavní fáze migrace infrastruktury:

* Dodávka HW/SW: Pořízení a kontrola nového hardwaru a softwarových licencí v datovém centru;

Zpracování a akceptace předimplementační analýzy.

* Montáž a instalace: Fyzická instalace racků, zařízení, zapojení kabeláže dle plánu, základní oživení a aktualizace firmware.
* Konfigurace infrastruktury:
  + Síť LAN: OoBM, management LAN, nastavení VLAN, routingu, firewallů a load balancerů, WAN konektivity, síťové bezpečnosti;
  + Síť SAN a Storage: Nastavení SAN, zónování, diskových polí, replikace;
  + Úložiště a zálohování: Nastavení diskových polí, replikace, páskové knihovny a zálohovacího softwaru, ochrany dat;
  + Servery a virtualizace: Instalace VMware ESXi, konfigurace vCenter, IBM PowerVM - HMC a VIO serverů.
* Ověření migračních postupů, pilotní provoz:

Po migraci následuje pilotní provoz (30 dní) s možností odstranění závad, poté přechod do rutinního provozu;

* Migrace dat a systémů: Přesun produkčních dat a aplikací do nového prostředí ve více fázích na úrovni virtualizace pro minimalizaci rizik, bez dopadu na aplikační architekturu;
* Akceptační testy, akceptace.

Popsané činnosti budou průběžně vyhodnocovány a akceptovány dle smluvní dokumentace a předimplementační analýzy.

Typ a průběh migrace IS SZIF

* Homogenní migrace bez potřeby konverze dat;
* Zachování aplikační vrstvy 1:1, včetně SAP a databází, bez nutnosti upgradu;
* Migrace všech systémů bez vlivu na aplikační architekturu, migrace na úrovni virtualizace (VMware, PowerVM);
* Kompatibilita provozovaných IS systémů SZIF ověřena – SAP, MACH, CAAS, GTFoto a dalších IS SZIF;
* Po migraci následuje pilotní provoz (30 dní) s možností odstranění závad, poté přechod do rutinního provozu.

Postup migrace:

* Migrace proběhne po jednotlivých platformách a metodách, s jasně definovanými etapami a milníky. Postup bude detailně zpracován v rámci předimplementační analýzy;
* Testování vzorových služeb dle jednotlivých platforem
  + Provedení testů a akceptace vzorových služeb;
  + Vyhodnocení výsledků a případné úpravy konfigurace.

Dílčí bloky migrace:

* Storage APP:
  + Přesun souborových systémů na nové diskové pole Tier 0 1:1, včetně sparse souborů;
  + Zajištění konzistence dat a zamezení opětovnému připojení starých storage.
* PowerPC (IBM AIX virtualizace):
  + Migrace LPAR systémů 1:1 s využitím virtualizace PowerVM a vysoké dostupnosti PowerHA.
  + Postup:
* Konfigurace nových Power serverů (VIOS, SAN zoning, LUNy);
* Připojení nových disků do původních LPARů, přesun dat pomocí AIX nástrojů;
* Přechod VM na nové servery bez výpadku;
* Před každou migrací proběhne záloha a kontrola jejího provedení;
* SAP provede funkční kontroly po migraci.
* x86 (VMware)
  + Migrace VM / systémů 1:1 s využitím virtualizace VMware a vysoké dostupnosti
  + Postup:
* Rozšíření virtualizačního clusteru o nové hosty;
* Migrace pomocí vMotion (online) a vStorage Motion (přenos disků a celých VM);
* Hybrid Linked Mode propojí staré a nové prostředí pro snadnou správu;
* Cold migration bude použita tam, kde není online migrace možná (RDM disky);
* Před každou migrací proběhne záloha a kontrola jejího provedení;
* SAP provede funkční kontroly po migraci;

Failover / FailBack plán:

* Pokud dojde k chybě během vMotion / Storage vMotion:
  + VM zůstane běžet na původním hostu / Datastore;
  + Zkontrolujeme logy a bude investigovaná příčina;
  + Oprava chyby;
  + Opakování migrace.
* Pokud by se stalo, že VM je poškozený nebo nedostupný:
  + Obnovíme VM ze zálohy na původní nebo alternativní host/datastore.

**4. Provozní požadavky a integrace**

Provozní požadavky jsou dány smluvně a vyplývají z provozních smluv stávajících provozovatelů infrastruktury a aplikací.

V rámci navrženého řešení jsou naplněny všechny požadavky Zadavatele na vysokou dostupnost (HA) a očekávané disaster recovery (DR) řešení a to 1:1.

Jsou pokryty také všechny požadavky na ochranu dat pomocí navrženého Zálohování a obnovy dat v nové infrastruktuře. Budou implementovány všechny potřebné prvky řízení bezpečnosti toku dat v oblasti síťové konektivity (firewally, izolace subnetů - VLAN, load balancer).

Dodávka a návrh také zohledňuje napojení na služby třetích stran (monitoring, správa, zálohy, SOC/SIEM).

**5. Testovací a validační plán**

Detailní testovací a validační plán bude stanoven v rámci předimplementační analýzy, která bude podléhat akceptaci Zadavatele.

Plán hlavní kroků a testů:

* Inicializace síťové konektivity:
  + Testy vysoké dostupnosti LAN prvků, její funkčnosti, OoBM přístup, páteřních přepínačů a routingu, LB, FW, testy redundance, konektivity mezi sály A/B a připojení k internetu, CMS, latence linek;
  + Dostupnosti existujících subnetů a WAN konektivity na nové infrastruktuře.
* Konfigurace SAN, úložišť a zálohování:
  + Testy vysoké dostupnosti, funkčnosti, SAN zón, dostupnosti úložišť, latence linek, replikace úložišť, konzistence dat a funkčnosti záloh a obnov, management nástrojů.
* Instalace podpůrných systémů infrastruktury:
  + Ověření vysoké dostupnosti, funkčnosti a výkonu jako referenční bod před migrací.
* Testování virtualizačních clusterů:
  + Ověření funkčnosti VMware a PowerHA clusterů;
  + Testy vysoké dostupnosti, VM migration, failover / failback, management nástrojů.
* Bezpečnostní testy:
  + Audit firewallů, segmentace;
  + Oprava nalezených nedostatků před ostrým provozem.

Testování a validace migrace VM s IS SZIF

Po úspěšném dokončení všech testů a odstranění závad následuje ostrá migrace produkčních dat.

Před zahájením migrace proběhne:

* Pilotní test migrace na sandbox systémech (x86 a PowerPC).
* Po úspěšném ověření následuje migrace v pořadí:
  + Testovací systémy;
  + Vývojové systémy;
  + Produktivní systémy.

Testovací fáze po migraci:

* Funkční testy:
  + Ověření, že všechny aplikace fungují stejně jako před migrací;
  + Provádějí klíčoví uživatelé nebo aplikační dodavatel Zadavatele.
* Výkonnostní a zátěžové testy:
  + Porovnání kapacity zdrojů a výkonu nové a původní infrastruktury;
  + Optimalizace v případě zjištěných slabin.
* Kritéria úspěšné migrace:
  + Dodržení časového plánu a rozpočtu, případné schválení všech projektových změn;
  + Plná funkčnost systémů infrastruktury a na nich provozovaných systémů s IS SZIF;
  + Žádná ztráta dat, vše korektně přeneseno;
  + Zdroje infrastruktury a dostupnost odpovídají požadavkům nebo převyšují původní stav;
  + Dostupnost IS SZIF a formální akceptace.

**6. Plán migrace a harmonogram**

Projekt bude rozdělen do více etap s časovým plánem, dle smlouvy.

Jedná se o etapy:

* Etapa č. 1 – Dodání Nové infrastruktury;
* Etapa č. 2 – Předimplementační analýza;
* Etapa č. 3 – Implementace a konfigurace;
* Etapa č. 4 – Migrace a Pilotní provoz;
* Etapa č. 5 – Produkční provoz.

V rámci předimplementační analýzy budou specifikovány:

* Detailní rozpad dané etapy;
* Plán odstávek a strategie bezvýpadkové migrace;
* Rollback/fallback scénáře, návrh mitigací a plánů ošetření rizik;
* Termíny a závislosti;
* Akceptační kritéria, testovací scénáře;
* Registr rizik;
* Potřebné součinnost pro vlastní realizaci;
* další smluvní výstupy.

**7. Rizika a mitigace**

V rámci předimplementační analýzy je cílem identifikovat a minimalizovat rizika spojená s migrací prostřednictvím preventivních opatření a krizových scénářů.

Na základě aktuálního stavu informací vidíme tato rizika a k nim možná opatření:

* Výpadky a dlouhé odstávky:
  + Opatření: Pečlivé plánování, testování nanečisto, rollback scénáře, go/no-go milníky, paralelní provoz staré infrastruktury.
* Ztráta dat:
  + Opatření: Zálohování před migrací, ověření záloh, kontrola integrity dat po migraci (checksumy, porovnání záznamů).
* Technická nekompatibilita:
  + Opatření: Kompatibilitní analýza aplikací a prostředí, ověření podpory výrobcem před realizací migrace.
* Zpoždění harmonogramu:
  + Opatření: Rezervy v plánu, řízení dodávek, flexibilní plánování, pravidelné aktualizace a transparentní komunikace.
* Nízká kvalita po migraci:
  + Opatření: Testování a ladění výkonu, zpětná vazba od uživatelů, smluvní garance výkonu.
* Lidská chyba:
  + Opatření: Detailní scénáře, princip 4 očí, střídání směn, simulace nanečisto, krizové postupy.
* Výpadek infrastruktury:
  + Opatření: Přesun do druhého sálu, využití záložních zdrojů.
* Selhání nového prostředí:
  + Opatření: Staré prostředí v pohotovosti do úspěšného dokončení migrace a min. dalších 20 dní kvůli možnost návratu.
* Zajištění potřebných součinností 3. stran:
  + Opatření: Pečlivé plánování, včasná komunikace, smluvní zajištění 3. stran
* Komunikační krize:
  + Opatření: Připraven krizový plán pro informování vedení i veřejnosti.

**8. Organizace a odpovědnosti**

Koordinace a řízení během migrace projektu bude stanovena na kick-off projektu v souladu se smluvní dokumentací.

Organizace řízení projektu

Organizace řízení projektu bude probíhat na základě mezinárodně uznávaného standardu PRINCE2.

Tento standard zajišťuje strukturovaný přístup k projektovému řízení, který definuje jasné role a odpovědnosti v rámci projektu.

Níže je rámcově popsána tříúrovňová organizační struktura projektu a náplň jednotlivých úrovní:

* ŘV – řídící výbor projektu:
  + Řídící výbor projednává zásadní záležitosti projektu a přijímá rozhodnutí závazná pro hlavní tým programu a dále řeší problémy eskalované Projektovým manažerem Objednatele nebo Poskytovatele z úrovně Hlavního týmu projektu;
  + Řídící výbor schvaluje změny projektu, které nejsou v kompetenci HTP (eskalace, konflikty zdrojů, změny projektu s dopadem na smluvní ustanovení, rozpočet a zásadní milníky projektu).
* HTP – hlavní tým projektu:
  + Je základním výkonným orgánem projektu;
  + Úkolem HTP je každodenní řízení projektových procesů, zejména řízení činnosti a koordinace Projektových týmů, koordinace součinnosti, podrobná kontrola průběhu projektu, řízení rizik projektu, řízení rozsahu a kvality projektu a operativní řízení projektu;
  + HTP přijímá rozhodnutí v rozsahu, který nevyžaduje rozhodnutí řídícího výboru (rozsah, který nemá dopad na změny Smlouvy).
* PT – projektový/pracovní tým:
  + Třetím stupněm řízení projektu jsou projektové týmy (tematické pracovní skupiny), které zajišťují oblasti týkající se odborných a technických záležitostí vlastní realizace projektu;
  + Projektový tým je složen především z věcných odborných garantů jednotlivých tematických oblastí. Primárním cílem projektového týmu je poskytovat patřičné odborné know–how, příp. stanoviska stakeholderů, které reprezentují;
  + Zástupci projektových týmů se účastní analýz, připomínkování a testování výstupů, akceptačního testování, zpracovávají požadavky, zadání a plní úkoly projednané na jednání projektového týmu.

Níže jsou popsány jednotlivé role a jejich zodpovědnosti:

* Sponzor projektu:
  + Je nejvyšším stupněm pro eskalace;
  + Je odpovědný za zajišťování prostředků (rozpočtu) pro projekt;
  + V rámci své organizace řeší požadavky na součinnost, neshody, změnové požadavky, rizika a problémy eskalované z HTP;
  + Je odpovědný za plnění úkolů na jednání ŘV jemu uložených;
  + Je odpovědný za podporu Projektového manažera.
* Projektový manažer:
  + je odpovědný za řízení projektových procesů;
  + Je zodpovědný za řízení hlavního týmu projektu, pracovních skupin;
  + Je odpovědný za zajištění zdrojů, kapacit a součinnosti, potřebných pro řádné plnění projektu a za jejich aktivní spolupráci ve společných týmech pracujících na jednotlivých částech projektu;
  + Kontroluje průběh projektu v rámci schválených cílů a rozsahu projektu a zodpovídá za plnění ostatních závazků vyplývajících ze smlouvy.
* Sponzor projektového týmu:
  + Jeho odpovědností je prosazovat projekt v rámci struktur organizace v oblasti jeho projektového týmu;
  + Je nejvyšší autoritou v daném projektovém týmu.
* Vedoucí projektového týmu:
  + Zodpovídá za operativní řízení projektových aktivit jednotlivých pracovníků v rámci daného projektového týmu;
  + Postupuje v úzké součinnosti s Projektovým manažerem tak, aby byly v plánovaných termínech a kvalitě provedeny všechny odsouhlasené plánované projektové aktivity v daném projektovém týmu;
  + V případě potřeby eskaluje příslušné projektové záležitosti, které již nemůže v rámci své kompetence rozhodnout (změna rozsahu, rozpočtu, časového plánu projektu), na úroveň Garanta projektového týmu.
* Garant projektového týmu:
  + Zodpovídá za věcnou správnost řešení všech dohodnutých projektových aktivit;
  + Odpovídá zejména za definici technických parametrů, včetně jejich doplňujících vlastností a za přípravu a provedení dílčích testů a následně akceptačních testů dodávky dle schválených testovacích kritérií.
* Bezpečnostní manažer:
  + Zodpovídá za kontrolu, revizi i definování bezpečnostních požadavků v rámci realizace Služeb, a to jak v oblasti provozu, tak v oblasti rozvoje;
  + Společně s Analytikem bezpečnosti zodpovídá za splnění veškerých požadavků na informační a kybernetickou bezpečnost vyplývající z ISO/IEC 27001 v aktuální verzi, dále pak za soulad poskytování služeb s požadavky ZoKB včetně prováděcích předpisů.
* Člen projektového týmu:
  + Jakýkoliv člen projektového týmu (např. metodický garant, vedoucí provozu…) schválený HTP potažmo ŘV;
  + V rámci své působnosti odpovídá za věcnou a odbornou správnost kroků realizace pro danou oblast;
  + Provádí činnosti stanovené Vedoucím projektového týmu v určeném rozsahu a čase.

Po podpisu smlouvu bude společně se zadavatelem:

* Svoláno kick-off jednání projektu;
* Stanovena organizační struktura projektu, která bude navržena tak, aby vyhovovala potřebám projektu a reflektovala časový rámce projektu;
* Stanoveny role a jejich zodpovědnosti, které budou navrženy tak, aby vyhovovaly potřebám projektu a reflektovaly časový rámce projektu;
* Stanoven rozsah projektové dokumentace, který bude navržen tak, aby vyhovoval potřebám projektu a reflektoval časový rámce projektu;
* Nastaveno řízení změn, které bude navrženo tak, aby vyhovovalo potřebám projektu a reflektovalo časový rámce projektu;
* Nastaveno řízení komunikace, které bude navrženo tak, aby vyhovovalo potřebám projektu a reflektovalo časový rámce projektu;
* Nastaveno řízní rizik, které bude navrženo tak, aby vyhovovalo potřebám projektu a reflektovalo časový rámce projektu;
* Nastaveno akceptační řízení, které bude navrženo tak, aby vyhovovalo potřebám projektu a reflektovalo časový rámce projektu.

### LAN - topologie

Řešení reflektuje požadavek objednatele na zohlednění budoucího možného geografického rozdělení dvou PoDů na dva PoPy a doplnění o tzv. Witness site.

XXXXX

Obrázek: Navržená topologie DC LAN

V této topologii dle obrázku výše byly definované základní stavební bloky a to:

* DC Fabric;
* WAN konektivita;
* DCI konektivita;
* L4-L7 bezpečnost.

Kromě výše zmíněných bloků nesmíme zapomenout na management DC fabric, další důležité management nástroje pro monitoring, zálohování, logování všech komponentů a také zajištění management přístupu ke všem komponentům řešení.

**DC fabric**

DC fabric je centrálním komunikačním prvkem a skládá se ze dvou základních komponent, kterými jsou SPINE switche a LEAF switche. Z hlediska dodávané kapacity k naplnění požadavků pro vybudování DC a kapacity možného rozšíření o další výpočetní zdroje jsme navrhli komponenty tohoto stavebního bloku (dělené na půl do jednotlivých PoDů):

* 8x LEAF switch včetně všech licencí
* 4x LEAN SPINE switch včetně všech licencí
* 4x BORDER LEAF switch včetně všech licencí

**WAN konektivita**

WAN konektivitu dělíme v našem designu na:

* INET (Transit provider)
* CMS (O2 KIVS)

DC WAN INET konektivita bude realizována WAN routerem, který bude zajišťovat konektivitu k upstream providerovi na základě EBGP. Redundance WAN INET konektivity bude postavena na dvou routerech po jednom v každém PoDu. Interní propojení routerů bude postavené na IBGP. Celá tato konstrukce zajistí rychlou konvergenci v případě výpadku jedné z WAN INET konektivity. V naší topologii nazýváme router WAN router a směrem na DC fabric bude připojený přes IGP protokol.

Z hlediska dodávky pro vybudování DC jsme navrhli parametry WAN routeru (dělené na půl do jednotlivých PoDů):

* 2x WAN router včetně všech licencí pokrývajících povinné požadavky

DC WAN CMS konektivita bude realizována přímými propoji ze SPINE switchů do KIVS CMS VPNek.

**DCI konektivita**

DCI konektivita je propojení v našem scénáři mezi dvěma PoDy. Při jejím návrhu ale musíme zohlednit možné do budoucna uvažované „roztržení“ na dva PoPy v geograficky vzdálených lokalitách.

Zároveň musíme v rámci tohoto kroku uvažovat o vybudování tzv „witness“ lokality pro ošetření „split brain“ implementovaných „metro clusteru“ v rámci výpočetní infrastruktury.

Pro tento účel jsou navrženy a budou dodány dva nezávislé „Edge switche“ s podporu MACsec, který zajistí bezpečnou komunikaci a integritu dat přes konektivitu mezi PoPy realizovanou DWDM technologií poskytovatele DC.

Možná vzdálenost DC s ohledem na požadované maximální RT je pro:

* Propojení PoPů s max RTT 1ms = maximální vzdálenost až cca. 80km
* Propojení každého PoPu a Witness site s max RTT 20ms = maximální vzdálenost až cca 20.000km

Z hlediska dodávky pro vybudování DC jsme navrhli počet Edge switchů (dělené na půl do jednotlivých PoDů):

* 4x EDGE switch včetně všech licencí pokrývajících povinné požadavky

**L4-L7 bezpečnost**

Dalším stavebním kamenem, který navrhujeme je L4-L7 bezpečnost.

Vlastní návrh vychází z následujících potřeb:

* Centralizovaná služba
* L4 FW-služby z INET: NAT, terminace IPsec, Terminace SSL
* L4 FW služby v rámci DC: statefull kontrola sessions pro aplikace uvnitř DC
* L4-L7: LB služby z INET / CMS: WAF, LB služby pro aplikace přístupné přes CMS

Pro nasazení síťové bezpečnosti náš návrh opět reflektuje možnost „roztržení“ DC na dva geografický oddělené PoPy s následujícími HA scénáři.

* Plné HA na každém PoPu
* FW cluster
* LB cluster
* Cluster

= Active/Passive implementace

= plná synchronizace session na Passive node

= gracefull switchover v případě fail na Node i v případě fail na interfacech

= plný switchower = žádný traverz provozu přes Cluster data propoje

* HA per DC
* V každém PoPu plnohodnotný cluster FW a LB
* Stateless přepnutí provozu přes druhý site v případě výpadku celého clusteru v jednom PoPu
* Stateless přepnutí pomocí routingu

Výše popsané požadavky určují jasné „fyzické“ a funkční požadavky na FW boxy a LB boxy.

Z hlediska dodávky pro vybudování DC jsme navrhli parametry a počet FW boxů (dělené na půl do jednotlivých PoDů):

* 4x FW včetně všech licencí pokrývajících povinné požadavky
* 4x LB včetně všech licencí pokrývajících povinné požadavky

**Management celého řešení se dělí na následující části:**

* Management DC fabric
* Management přístup na Network Elementy

V případě našeho konceptu DC fabric založeném na EVPN/VXLAN byl navržen management systém pro DC fabric jako GUI management nástroj pro celý životní cyklus DC fabric. Tedy pro fáze výstavby, poskytování služeb a jejich provozu.

Pro management přístup na síťové elementy se bude používat několik principů.

* Tzv In-band přístup: jedná se o remote SSH/Telnet přístup přes datové propoje. Tento přístup je v našem řešení nativní, jelikož je celý DC fabric postavený na L3ECMP, je možné se připojit na loopback IPs všech network elementů
* Tzv Out-of-Band přístup: jedná se o remote SSH/Telnet přístup přes dedikovaný mngt network, ke kterému jsou všechny network elementy připojené přes dedikované OoB porty. Výhodou takového připojení je přímá cesta k CPU Network elementů, která nemůže být ovlivněná mírou datového provozu.
* Tzv. console přístup. Originálně se jedná o lokální non IP přístup, který umožňuje kontrolovat Network elementy ve všech fázích včetně boot procesu, kdy ještě není ready IP konektivita pro Inband či OoB přístup. Tento lokální přístup lze realizovat také v remote variantě pomocí tzv Terminal (Console) serverů.

Pro nasazení dostatečného MNGT přístupu na síťovou vrstvu (network) budou nasazeny následující dva elementy (dělené na půl do jednotlivých PoDů):

* OoB management switche:
* 4x OoB management switch včetně všech licencí pokrývajících povinné požadavky
* TERMINAL servery:
* 2x TERMINAL server

#### LAN část DC – Fyzické provedení / SoC

LAN část Datového centra bude poskytovat plnou flexibilitu nejenom z hlediska služeb, ale také z hlediska možného rozšíření, a to ve všech možných uvažovaných směrech. Návrh tohoto stavebního bloku LAN struktury je založený na:

* požadované kapacitě řešení specifikované v kapitole „2.5.2.1 Inicializační nastavení“.

Řešení je založené na dedikovaných BORDER a Server LEAFech a to následovně:

* LAN část Datového centra:
* 8x LEAF switch včetně všech licencí
* 128x 25GBASE-SR SFP28 transceivery pro připojení výpočetních prostředků originální od dodavatele LEAF switchů
* 16x 100GBASE-DR QSFP28 transceivery pro propojení do DC Fabric / originální od dodavatele LEAF switchů
* 4x LEAN SPINE switch včetně všech licencí
* 40x 100GBASE-DR QSFP28 transceivery / originální od dodavatele SPINE switchů.
* 4x BORDER LEAF switch včetně všech licencí
* 16x 100GBASE-DR QSFP28 transceivery pro připojení do DC Fabric / originální od dodavatele LEAF switchů
* 16x 100GBASE-SR4 QSFP28 transceivery pro připojení Firewallů a Load balancerů/ originální od dodavatele LEAF switchů
* 4x 4x40GBASE-LR4 breakout pro připojení na WAN Router a pro CMS WAN konektivitu / originální od dodavatele LEAF switchů
* 4x EDGE switch včetně všech licencí pokrývajících povinné požadavky
* 16x 100GBASE-DR QSFP28 transceivery / originální od dodavatele EDGE switchů
* 8x 10GBASE-SR SFP+ transceivery / originální od dodavatele EDGE switchů
* 2x WAN router včetně všech licencí pokrývajících povinné požadavky
* 5x 10GBASE-LR SFP+ transceivery / originální od dodavatele WAN routerů
* 4x FW včetně všech licencí pokrývajících povinné požadavky
* 8x 100GBASE-SR4 QSFP28 transceivery / originální od dodavatele Firewallů
* 4x LB včetně všech licencí pokrývajících povinné požadavky
* 8x 100GBASE-SR4 QSFP28 transceivery / originální od dodavatele Load balancerů
* 4x OoB management switch včetně všech licencí pokrývajících povinné požadavky
* 12x 10GBASE-SR SFP+ transceivery / originální od dodavatele OoB management switchů
* 2x TERMINAL server

32x RS232 kabelů kompatibilních s formou konzolových portů na dodávaných síťových prvcích v rámci tohoto zadávacího řízení.

Na základě popisu výše jsou definovány typy a počty jednotlivých síťových prvků. Příslušenství (transceivery) a detailní „rozpad“ síťových prvků na jednotlivé produkty a „Part Numbery (PN)“ je pak součástí jednotlivých následujících kapitol.

Navržené síťové prvky jsou z produktové nabídky společnosti JUNIPER Networks, která je jedním z renomovaných amerických výrobců aktivních prvků pro stavbu LAN struktury Datových Center.

|  |  |  |  |
| --- | --- | --- | --- |
| **Komponenty** | | | |
| **Číslo** | **Název komponenty** | **Part number** | **Počet kusů** |
| 1 | LEAF | XXXXX | 8 |
| 2 | LEAN SPINE | XXXXX | 4 |
| 3 | BORDER LEAF | XXXXX | 4 |
| 4 | EDGE switch | XXXXX | 4 |
| 5 | WAN router | XXXXX | 2 |
| 6 | FW (Firewall) | XXXXX | 4 |
| 7 | LB (Load balancer) | XXXXX | 4 |
| 8 | OoB MNGT switch | XXXXX | 4 |
| 9 | TERMINAL server | XXXXX | 2 |

Z popisu požadavků na novou technologii a stojany pro tzv. „parallel build“ v rámci migrace vyplývá, že nová LAN síťová infrastruktura bude umístěna následovně:

* do dvou stojanů, ve kterých budou nainstalovány výpočetní prostředky využívající LAN síťovou infrastrukturu pro datovou komunikaci
* v každém z těchto stojanů budou umístěny 2x LEAF (tzv. ToR) switche, a to do pozice „Top of the Rack) – poskytnutá redundantní (dual-homing) konektivita v rámci stojanu
* v každém z těchto stojanů bude umístěný 1x OoB management switch za účelem OoB konektivity pro všechny prvky LAN síťové infrastruktury a zároveň pro všechny výpočetní prostředky.
* V jednom ze stojanů budou umístěny zbylé síťové prvky nové LAN síťové infrastruktury a těmi budou SPINE switche, EDGE switche, Firewally, Load balancery.

|  |  |
| --- | --- |
| **Komponenta (X ks)** | |
| **Vlastnost/ komponenta** | **Parametry** | |
| N/A | Parametry výše uvedených zařízení jsou popsány v kapitolách níže. | |

#### DC fabric

Navržený DC fabric bude centrálním komunikačním prvkem LAN struktury skládá se ze tří základních komponentů, kterými jsou SPINE switche, LEAF switche a BORDER LEAF switche.

DC Fabric je „opřený“ o standardizovaný koncept, který obsahuje plně redundantní end-to-end topologie s vlastností rychlé konvergence v řádu subsekund. Což znamená:

* Dual-homed LAG/LACP pro redundantní připojení výpočetních prostředků
* Řešení poskytuje tuto funkcionalitu pomocí implementace standardizovaného řešení tzv. ESI-LAG na bázi EVPN control plane. Detail viz níže
* Plně redundantní DC Fabric core topologie založené na:
* Dual SPINE-LEAF topologii
* L3 ECMP load balancing – navržený na OSPF nebo eBGP peering. Bude případně rozhodnuto ve fázi detailního návrhu – Low Level Designu.
* Dual-homed LAG/LACP pro redundantní připojení centrální bezpečnosti, jimiž jsou centrální Firewall a centrální Load balancer
* Řešení poskytuje tuto funkcionalitu pomocí implementace standardizovaného řešení tzv. ESI-LAG na bázi EVPN controll plane. Detail viz níže.

Detail topologie LAN části v DC a jednoho PoDu je na následujícím obrázku. Obrázek zahrnuje i další stavební bloky jako připojené Firewally, Load balancery a WAN router, které jsou na obrázku se sníženým jasem, aby byl zřetelný pouze zde popsaný stavební prvek, jimž je DC Fabric. Díky tomuto komplexnímu obrázku je jasná i přesná konektivita DC Fabric k okolnímu prostředí:

XXXXX

Obrázek: DC Fabric – Požadovaná kapacita

Z obrázku je zřejmé nasazení všech moderních trendů definovaných v úvodní kapitole záměru projektu.

DC Fabric:

* je multiple 100GE;
* má topologii SPINE – LEAF;
* využívá L3 ECMP s EVPN/ VXLAN overaly;
* má EVPN/VXLAN s distribuovanou anycast Gateway = maximálně optimalizovaný provoz;
* má optimalizovanou škálovatelnost na základě 3 stage clos;
* má dedikované BORDER LEAFy, což umožňuje snazší izolaci případné chyby či problému;
* je vybavený dedikovaným WAN routerem pro optimalizaci WAN provozu do internetu.
* využívá dedikované switche pro MACsec funkcionalitu na DCI propojích.
* poskytuje vysoce výkonné HA připojení pro přístup na internet i k O2 KIVS (Komunikační infrastruktura veřejné správy) operátorovi.

Celý DC Fabric na obrázku je navržený jako velmi flexibilní z hlediska možného dalšího rozvoje, a to jak na úrovni výkonnosti, tak i na úrovni možného rozšíření za účelem nárůstu potřeby výpočetních zdrojů.

Takový nárust je možné realizovat navýšením až na dvojnásobek počtu připojených výpočetních prostředků a navýšením výkonnosti DC Fabric také až na dvojnásobek výchozího stavu.

Toto kritérium možného navýšení je v návrhu realizovatelné beze změny poptávaných Core prvků. Těmito Core prvky jsou síťové prvky typu SPINE, BORDER LEAF, EDGE switch, WAN router, Firewall, Load balancer. Návrh tedy z tohoto požadavku vychází a možný nárůst bude možné realizovat pouhým dodáním transceiverů do Core prvků a případně dodáním koncových síťových prvků DC Fabric, jimiž jsou ale pouze switche typu LEAF.

Posledním bodem architektury DC Fabric je řešení redundantního připojení výpočetní techniky. Tento tzv. Dual-homing může být v souvislosti s přístupem rozdílných vendorů řešený dvěma rozdílnými způsoby, kterými jsou tzv. MC-LAG a tzv. ESI LAG. Řešení je navrženo pomocí ESI-LAG, který má oproti MC-LAG značné výhody.

ESI LAG

XXXXX

Obrázek: ESI-LAG control plane / forwarding plane

V tomto případě není nutný vzájemný propoj mezi členy LAGu. Tento typ LAGu pak umožňuje více než dva členy a je plně otevřený (není závislý na výrobci). Na obrázku je znázorněný princip LAGu pro případ dual-homing připojených výpočetních zařízení ke dvěma LEAF switchům. Stejné principy ale budou uplatněny i pro dual-homing Firewallů a Load balancerů na BORDER LEAFy.

Dle požadavků na počet koncových připojených zařízení, zmíněnou flexibilitu a úroveň požadované vysoké dostupnosti a spolehlivosti je LAN řešení navrženo s osazením následujících prvků:

Počet LEAFů v DC (4x LEAF per PoD): 8x

Každý LEAF je:

* 1U rack mount zařízení;
* 1x 25GE SFP28 portem připojen k výpočetnímu zařízení;
* 1x 100GE QSFP28 portem připojen na SPINE1 zařízení;
* 1x 100GE QSFP28 portem připojen na SPINE2 zařízení;
* Plná redundance zdrojů (PSU) a větráků (FAN);
* Podpora MC-LAG = LAG mezi dvěma LEAFy; (založeno na ESI-LAG);
* Podpora L2 / L3;
* Podpora mBGP;
* Podpora EVPN/VXLAN;
* Podpora L2/L3 EVPN/VXLAN VTEP;
* Podpora symetrického EVPN routingu.

Počet SPINE v DC (2x SPINE per PoD): 4x

Každý SPINE je:

* 1U rack mount zařízení;
* 1x 100GE QSFP28 portem připojen s každým LEAF zařízením (4x) v rámci PoD;
* 2x 100GE QSFP28 portem připojen s jedním EDGE zařízením v rámci PoD;
* 2x 100GE QSFP28 portem připojen s BORDER LEAF1 zařízením v rámci PoD;
* 2x 100GE QSFP28 portem připojen s BORDER LEAF2 zařízením v rámci PoD;
* Plná redundance zdrojů (PSU) a větráků (FAN);
* Podpora L2 / L3;
* Podpora mBGP a iBGP RR.

Počet BORDER LEAFů v DC (2x BORDED LEAF per PoD): 4x

Každý BORDER LEAF je:

* 1U rack mount zařízení;
* Vždy v rámci PoD, 2x 100GE QSFP28 portem připojen se SPINE1 zařízením;
* Vždy v rámci PoD, 2x 100GE QSFP28 portem připojen se SPINE2 zařízením;
* Vždy v rámci PoD, 1x 100GE QSFP28 portem připojen s Firewall1 zařízením;
* Vždy v rámci PoD, 1x 100GE QSFP28 portem připojen s Loadbalancer1 zařízením;
* Vždy v rámci PoD, 1x 100GE QSFP28 portem připojen s Firewall2 zařízením;
* Vždy v rámci PoD, 1x 100GE QSFP28 portem připojen s Loadbalancer2 zařízením;
* Vždy v rámci PoD, 1x 10GE QSFP28 portem připojen s WAN router zařízením;
* Vždy v rámci PoD, 1x 10GE QSFP28 portem připojen s KIVS(CMS)router zařízením;
* Plná redundance zdrojů (PSU) a větráků (FAN);
* Podpora MC-LAG = LAG mezi dvěma LEAFy (založeno na ESI-LAG);
* Podpora L2 / L3;
* Podpora mBGP;
* Podpora L2/L3 EVPN/VXLAN VTEP;
* Podpora symetrického EVPN routingu;
* Z důvodu unifikace náhradních dílů pro tuto pozici navrhujeme stejný typ HW jako pro SPINE switche.

Z uvedených požadavků a návrhu DC Fabric v této kapitole výše jsou navrhované počty a typy síťových prvků uvedeny v následující tabulce:

|  |  |  |  |
| --- | --- | --- | --- |
| **Komponenty** | | | |
| **Číslo** | **Název komponenty** | **Part number** | **Počet kusů** |
| 1 | LEAF | XXXXX | 8 |
| 2 | LEAN SPINE | XXXXX | 4 |
| 3 | BORDER LEAF | XXXXX | 4 |

Na základě požadavků objednatele je do pozice LEAF switch navrženo zařízení s těmito vlastnostmi:

|  |  |
| --- | --- |
| **Komponenta – LEAF (8 ks)** | |
| **Vlastnost/ komponenta** | **Parametry** | |
| **SPECIFIKACE HW** | * Rack mount zařízení * Velikost (v x š x h): 4,37 x 44,09 x 52,02(57,65 s kabely) cm * Instalace do 1000 mm hlubokého stojanu * Instalace do stojanu o velikosti 19“ stojan * Maximální výška boxu - 1U * AC zdroj: 1 + 1 redundance, vyměnitelný za chodu * Větrák: 5 + 1 redundance, vyměnitelný za chodu * Aktivní chlazení (FANy) tzv. Rear-to-Front * Podpora 48x 10/25GE SFP+/SFP28 portů * Podpora 8x 100GE QSFP28 uplink * Neblokovaný výkon pro všechny požadované interface - 2Tbps * OoB Management interface - RJ45 provedení * USB * Console port - RJ45 provedení * Úložiště pro lokální logy, debug soubory atd – kapacita 50 GB SSD * Maximální spotřeba: 283 W * Maximální váha: 10,75 kg | |
| **FYZICKÝ INTERFACE** | * 1GBASE-T * 1GBASE-SX * 1GBASE-LX * 10GBASE-SR * 10GBASE-LR * 10GBASE DAC (Twinmax kabel) 3m * 25GBASE-SR * 25GBASE-LR * 25GBASE DAC (Twinmax kabel) 3m * 100GBASE-SR4 pro MC-LAG * 100GBASE-LR4 * 100GBASE-DR * 100GBASE-FR * 100GBASE DAC (Twinmax kabel) 3m | |
| **L2 VLASTNOSTI** | * Podpora jumbo frames o velikosti až 9216 B * Podpora L2 switching dle standardu IEEE 802.3 bridging * Velikost MAC tabulky = 288k * LAG/LACP * Multi chassis LAG mezi dvěma switchi MC-LAG nebo ESI LAG * Počet LAG group 80x * LAG resilient hashing * Podpora VLAN (IEEE 802.1Q) * Plný rozsah VLAN = 4094 * QinQ * Port based VLAN * Rewrite VLAN hlavičky * xSTP: * IEEE 802.1D (STP jako součást) * IEEE 802.1s (MSTP) * IEEE 802.1w (RSTP) * STP security functions * BPDU guard * Loop guard * Root guard * LLDP (802.1ab) | |
| **DCB** | * Loss-less Ethernet * Priority-based flow control (PFC)—IEEE 802.1Qbb * Explicit congestion notification (ECN) * Data Center Bridging Exchange Protocol (DCBX) * RDMA over converged Ethernet version 2 (RoCEv2) | |
| **ACLs (Access lists)** | * Podporováno v HW * Interface ACLs (ingress / egress) * VLAN ACLs (ingress / egress) * ACL match podmínky na L2 až L4 * ACL akce - discard / reject / accept / login / count / policer / instance assingment * ACL pro CPU protection | |
| **L3 FUNKCE** | * RVI (Routovaný VLAN interface), společně i s možností L3 subinterface * Podpora IP FIB kapacita: 351k záznamů pro IPv4 LPM, 172k záznamů pro IPv6 LPM * Static routing (IPv4/IPv6) * Ospf / ospfv3 * MBGP (IPv4, IPv6, EVPN) * VRRP (IPv4/6) * Virtual router - 2000 EVPN VXLAN BASE * DHCP server (IPv4/6) / relay (IPv4/6) / konfigurovatelný pod Virtual router * BFD (static, OSPF, BGP) * Policy, Filter based routing = forwarding založený na L2-L4 source a destination hlavičkách * ECMP balancing / resilient hashing – 64 ECMP cest | |
| **MCAST** | * Podporováno v HW * IGMP snooping v1/2/3 * IGMP v1/2/3 * MLD v1/2 * PIM-SM ASM / SSM | |
| **DC Fabric VLASTNOSTI** | * Podpora více než 4k VXLAN * ECMP underlay podpora - eBGP a IGP * VXLAN s EVPN control plane (DC overlay) Podpora typů route: type 2 (MAC-IP), type 3 (BUM), type 5 (IP); ARP/ND proxy, suppression. Společně s route type pro podporu ESI-LAG, jako je route type 4 a 1 * Podpora VLAN-based, VLAN-bundle, VLAN-aware-bundle servisních modelů * VXLAN L2/L3 GTW for symetrický edge routing, anycast GTW na všech edge síťových prvcích, kde jsou terminovány VXLANy, podpora type 5 route. Dále možnost konfigurace asymetrického centralizovaného routingu * EVPN Active/Active multihoming, ESI LAG (type 4 a 1 route) / konfigurovatelný ESIs | |
| **COS** | * Podpora v HW * „Trust“ traffic klasifikace založena na 802.1p, DSCP * „Untrust“ traffic klasifikace založena na L2-L4 polích hlavičky paketu * 8 front na interface * Egress Port shaping / Egress Queue shaping (sdílení provozu mezi frontami) * Priority DWRR scheduling mechanismus * 2 priority pro interface Scheduler * Strict priority implementace (LLQ) * WRED congastion mechanism * Ingres Policing single rate two colors * Rewrite mechanism 802.1p, DSCP | |
| **MANAGEMENT A TROUBLESHOOTING** | * Společné OS cli napříč kategoriemi switchů: LEAF / SPINE / BORDER LEAF / EDGE switch - JUNOS CLI * Jeden vendor napříč síťovým portfoliem v rámci tohoto projektu a to pro kategorie - LEAF / SPINE / BORDER LEAF / EDGE switch/ WAN\_router / OoB\_MNGT - JUNIPER Networks (od tohoto vendora je nabízen také centrální FW) * Cli interface: plná konfigurovatelnost a řešení problémů * local * telnet * ssh * User autentication * local * Radius, TACAC+ * RBAC pro všechny typy authentikace * Automatická záloha konfigurace - plně podporováno SCP, FTP, TFTP * Konfigurační změny přes txt file * Konfigurovatelnost přes Netconf a gRPC s podporou Yang data modelů * Lokální i vzdálený syslog server * Ping, traceroute * sFlow, Ipfix * Traffic mirroring * SNMPv2/v3 * Telemetry interface přes Netconf a gRPC s podporou Yang data modelů * Podpora Terraform a Ansible * Lokální i vzdálené spouštění skriptů - python, xslt, slax | |

|  |  |
| --- | --- |
| **Komponenta – LEAN SPINE (4 ks)** | |
| **Vlastnost/ komponenta** | **Parametry** | |
| **SPECIFIKACE HW** | * Rack mount zařízení * Velikost (v x š x h): 4,33 x 43,84 x 51,5 (55 s kabely) cm * Instalace do 1000 mm hlubokého stojanu * Instalace do stojanu o velikosti 19“ stojan * Maximální výška boxu - 1U * AC zdroj: 1 + 1 redundance, vyměnitelný za chodu * Větrák: 5 + 1 redundance, vyměnitelný za chodu * Aktivní chlazení (FANy) tzv. Rear-to-Front * 32x 100GE QSFP28 downlink portů * Neblokovaný výkon pro všechny požadované interface – 3,2Tbps * OoB Management interface - RJ45 provedení * USB * Console port - RJ45 provedení * Úložiště pro lokální logy, debug soubory atd – kapacita 64 GB SSD * Maximální spotřeba: 365 W * Maximální váha : 9,585 kg | |
| **FYZICKÝ INTERFACE** | * 100GBASE-SR4 pro MC-LAG * 100GBASE-LR4 * 100GBASE-DR * 100GBASE-FR * 100GBASE DAC (Twinmax kabel) 3m | |
| **L2 VLASTNOSTI** | * Podpora jumbo frames o velikosti až 9216 B * Podpora L2 switching dle standardu IEEE 802.3 bridging * Velikost MAC tabulky = 288k * LAG/LACP * LAG resilient hashing * Podpora VLAN (IEEE 802.1Q) * Plný rozsah VLAN = 4094 * QinQ * Port based VLAN * Rewrite VLAN hlavičky * xSTP: * IEEE 802.1D (STP jako součást) * IEEE 802.1s (MSTP) * IEEE 802.1w (RSTP) * STP security functions * BPDU guard * Loop guard * Root guard * LLDP (802.1ab) | |
| **DCB** | * Loss-less Ethernet * Priority-based flow control (PFC)—IEEE 802.1Qbb * Explicit congestion notification (ECN) * Data Center Bridging Exchange Protocol (DCBX) * RDMA over converged Ethernet version 2 (RoCEv2) | |
| **ACLs (Access lists)** | * Podporováno v HW * Interface ACLs (ingress / egress) * VLAN ACLs (ingress / egress) * ACL match podmínky na L2 až L4 * ACL akce - discard / reject / accept / login / count / policer / instance assingment * ACL pro CPU protection | |
| **L3 FUNKCE** | * RVI (Routovaný VLAN interface), včetně možností L3 subinterface * Podpora IP FIB kapacita: 351k záznamů pro IPv4 LPM, 172k záznamů pro IPv6 LPM * Static routing (IPv4/IPv6) * Ospf / ospfv3 * MBGP (IPv4, IPv6, EVPN) * BFD (static, OSPF, BGP) * Policy, Filter based routing = forwarding založený na L2-L4 source a destination hlavičkách * ECMP balancing / resilient hashing – 64 ECMP cest | |
| **MCAST** | * Podporováno v HW * IGMP snooping v1/2/3 * IGMP v1/2/3 * MLD v1/2 * PIM-SM ASM / SSM | |
| **COS** | * Podpora v HW * „Trust“ traffic klasifikace založena na 802.1p, DSCP * „Untrust“ traffic klasifikace založena na L2-L4 polích hlavičky paketu * 8 front na interface * Egress Port shaping / Egress Queue shaping (sdílení provozu mezi frontami) * Priority DWRR scheduling mechanismus * 2 priority pro interface Scheduler * Strict priority implementace (LLQ) * WRED congastion mechanism * Ingres Policing single rate two colors * Rewrite mechanism 802.1p, DSCP | |
| **MANAGEMENT A TROUBLESHOOTING** | * Společné OS cli napříč kategoriemi switchů: LEAF / SPINE / BORDER LEAF / EDGE switch - JUNOS CLI * Jeden vendor napříč síťovým portfoliem v rámci tohoto projektu a to pro kategorie - LEAF / SPINE / BORDER LEAF / EDGE switch/ WAN\_router / OoB\_MNGT - JUNIPER Networks (od tohoto vendora je nabízen také centrální FW) * Cli interface: plná konfigurovatelnost a řešení problémů * local * telnet * ssh * User autentication * local * Radius, TACAC+ * RBAC pro všechny typy authentikace * Automatická záloha konfigurace - plně podporováno SCP, FTP, TFTP * Konfigurační změny přes txt file * Konfigurovatelnost přes Netconf a gRPC s podporou Yang data modelů * Lokální i vzdálený syslog server * Ping, traceroute * Traffic mirroring * SNMPv2/v3 * Telemetry interface přes Netconf a gRPC s podporou Yang data modelů * Podpora Terraform a Ansible * Lokální i vzdálené spouštění skriptů - python, xslt, slax | |

|  |  |
| --- | --- |
| **Komponenta – BORDER LEAF (4 ks)** | |
| **Vlastnost/ komponenta** | **Parametry** | |
| **SPECIFIKACE HW** | * Rack mount zařízení * Velikost (v x š x h): 4,33 x 43,84 x 51,5 (55 s kabely) cm * Instalace do 1000 mm hlubokého stojanu * Instalace do stojanu o velikosti 19“ stojan * Maximální výška boxu - 1U * AC zdroj: 1 + 1 redundance, vyměnitelný za chodu * Větrák: 5 + 1 redundance, vyměnitelný za chodu * Aktivní chlazení (FANy) tzv. Rear-to-Front * 32x sdílených portů pro 100GE QSFP28 nebo 10GE QSFP+ rozplet * Neblokovaný výkon pro všechny požadované interface – 3,2Tbps * OoB Management interface - RJ45 provedení * USB * Console port - RJ45 provedení * Úložiště pro lokální logy, debug soubory atd – kapacita 50 GB SSD * Maximální spotřeba: 283 W * Maximální váha: 10,75 k | |
| **FYZICKÝ INTERFACE** | * 4x10GBASE-SR (Channelization 4x10GE) * 4x10GBASE-LR (Channelization 4x10GE) * 4x 10GBASE DAC (Twinmax kabel) 3m * 100GBASE-SR4 pro MC-LAG * 100GBASE-LR4 * 100GBASE-DR * 100GBASE-FR * 100GBASE DAC (Twinmax kabel) 3m | |
| **L2 VLASTNOSTI** | * Podpora jumbo frames o velikosti až 9216 B * Podpora L2 switching dle standardu IEEE 802.3 bridging * Velikost MAC tabulky = 288k * LAG/LACP * Multi chassis LAG mezi dvěma switchi * LAG resilient hashing * Podpora VLAN (IEEE 802.1Q) * Plný rozsah VLAN = 4094 * QinQ * Port based VLAN * Rewrite VLAN hlavičky * xSTP: * IEEE 802.1D (STP jako součást) * IEEE 802.1s (MSTP) * IEEE 802.1w (RSTP) * STP security functions * BPDU guard * Loop guard * Root guard * LLDP (802.1ab) | |
| **DCB** | * Loss-less Ethernet * Priority-based flow control (PFC)—IEEE 802.1Qbb * Explicit congestion notification (ECN) * Data Center Bridging Exchange Protocol (DCBX) * RDMA over converged Ethernet version 2 (RoCEv2) | |
| **ACLs (Access lists)** | * Podporováno v HW * Interface ACLs (ingress / egress) * VLAN ACLs (ingress / egress) * ACL match podmínky na L2 až L4 * ACL akce - discard / reject / accept / login / count / policer / instance assingment * ACL pro CPU protection | |
| **L3 FUNKCE** | * RVI (Routovaný VLAN interface), včetně možností L3 subinterface * Podpora IP FIB kapacita: 351k záznamů pro IPv4 LPM, 172k záznamů pro IPv6 LPM * Static routing (IPv4/IPv6) * Ospf / ospfv3 * MBGP (IPv4, IPv6, EVPN) * VRRP (IPv4/6) * Virtual router (oddělené „Routing Information Bases“) – 2000 EVPN VXLAN BASE * DHCP server (IPv4/6) / relay (IPv4/6) / konfigurovatlný pod Virtual router * BFD (static, OSPF, BGP) * Policy, Filter based routing = forwarding založený na L2-L4 source a destination hlavičkách * ECMP balancing / resilient hashing – 64 ECMP cest | |
| **MCAST** | * Podporováno v HW * IGMP snooping v1/2/3 * IGMP v1/2/3 * MLD v1/2 * PIM-SM ASM / SSM | |
| **DC Fabric VLASTNOSTI** | * Podpora více než 4k VXLAN * ECMP underlay podpora - eBGP a IGP * VXLAN s EVPN control plane (DC overlay) Podpora typů route: type 2 (MAC-IP), type 3 (BUM), type 5 (IP); ARP/ND proxy, suppression. Společně s route type pro podporu ESI-LAG, jako je route type 4 a 1 * Podpora VLAN-based, VLAN-bundle, VLAN-aware-bundle servisních modelů * VXLAN L2/L3 GTW for symetrický edge routing, anycast GTW na všech edge síťových prvcích, kde jsou terminovány VXLANy, podpora type 5 route. Dále možnost konfigurace asymetrického centralizovaného routingu * EVPN Active/Active multihoming, ESI LAG (type 4 a 1 route) / konfigurovatelný ESIs | |
| **COS** | * Podpora v HW * „Trust“ traffic klasifikace založena na 802.1p, DSCP * „Untrust“ traffic klasifikace založena na L2-L4 polích hlavičky paketu * 8 front na interface * Egress Port shaping / Egress Queue shaping (sdílení provozu mezi frontami) * Priority DWRR scheduling mechanismus * 2 priority pro interface Scheduler * Strict priority implementace (LLQ) * WRED congastion mechanism * Ingres Policing single rate two colors * Rewrite mechanism 802.1p, DSCP | |
| **MANAGEMENT A TROUBLESHOOTING** | * Společné OS cli napříč kategoriemi switchů: LEAF / SPINE / BORDER LEAF / EDGE switch - JUNOS CLI * Jeden vendor napříč síťovým portfoliem v rámci tohoto projektu a to pro kategorie - LEAF / SPINE / BORDER LEAF / EDGE switch/ WAN\_router / OoB\_MNGT - JUNIPER Networks (od tohoto vendora je nabízen také centrální FW) * Cli interface: plná konfigurovatelnost a řešení problémů * local * telnet * ssh * User autentication * local * Radius, TACAC+ * RBAC pro všechny typy authentikace * Automatická záloha konfigurace - plně podporováno SCP, FTP, TFTP * Konfigurační změny přes txt file * Konfigurovatelnost přes Netconf a gRPC s podporou Yang data modelů * Lokální i vzdálený syslog server * Ping, traceroute * Traffic mirroring * SNMPv2/v3 * Telemetry interface přes Netconf a gRPC s podporou Yang data modelů * Podpora Terraform a Ansible * Lokální i vzdálené spouštění skriptů - python, xslt, slax | |

#### WAN konektivita

Na základě definice objednatele na WAN routeru je WAN konektivita rozdělena na:

* WAN INET
* WAN CMS

Obě části konektivity včetně znázornění připojení WAN routeru k DC Fabric je ukázáno na následujícím obrázku, který reflektuje požadovanou start kapacitu i možné rozšíření:

XXXXX

Obrázek: WAN konektivita – Start kapacita a kapacita možného rozšíření

Internetová DC WAN konektivita bude realizována WAN routerem, který bude zajišťovat konektivitu k upstream poskytovateli na základě EBGP. Redundance WAN internetové konektivity bude postavena na dvou routerech po jednom v každém PoDu. Interní propojení routerů bude postavené na IBGP. Celá tato konstrukce zajistí rychlou konvergenci v případě výpadku jedné z WAN internetových konektivit. Jelikož objednatel není LIR, budou routery přijímat DGTW od upstream providera a posílat providerem přidělené závislé subnety k upstream providerovi. V navržené topologii nazýváme router WAN\_routerem. Směrem na DC Fabric bude připojený přes IBGP protokol (OSPF), do kterého bude publikována výchozí gateway. Z DC Fabric se pak bude WAN\_router učit použité LAN subnety opět přes IGP protokol (OSPF). Tento návrh protokolového stacku je znázorněný na obrázcích v předchozí kapitole.

DC WAN CMS konektivita bude realizována přímo z DC Fabric a to z BORDER LEAFů nemá vliv na vlastní WAN router.

Dle požadavků na WAN konektivitu a úroveň požadované vysoké dostupnosti a spolehlivosti je navrženo WAN řešení s následujícími prvky:

Počet WAN routerů v DC (1x WAN router per PoD): 2x

Každý WAN router je:

* 1U rack mount zařízení;
* Podpora 10GE portů (Vybavené 5x 10GBASE-LR SFP+ originálními transceivery;
* Plná redundance zdrojů (PSU) a větráků (FAN);
* Podpora L2/L3;
* Podpora BGP;
* Podpora VRF – dedikované RIB (Routing Information Base)/FIB (Forwarding Information Base) tabulky;
* Podpora FIB;

Z uvedených požadavků a návrhu WAN konektivity v této kapitole výše vyplývá navrhovaný typ network elementu a počty kusů v následující tabulce:

|  |  |  |  |
| --- | --- | --- | --- |
| **Komponenty** | | | |
| **Číslo** | **Název komponenty** | **Part number** | **Počet kusů** |
| 1 | WAN router | XXXXX | 2 |

|  |  |
| --- | --- |
| **Komponenta - WAN router (2 ks)** | |
| **Vlastnost/ komponenta** | **Parametry** | |
| **SPECIFIKACE HW** | * Rack mount zařízení * Velikost (v x š x h): 4,37 x 48,26 x 47,0 (51,87 s kabely) cm * Instalace do 1000 mm hlubokého stojanu * Instalace do stojanu o velikosti 19“ stojan * Maximální výška boxu - 1U * AC zdroj: 1 + 1 redundance, vyměnitelný za chodu * Větrák: 2 + 1 redundance, vyměnitelný za chodu * Aktivní chlazení (FANy) tzv. Rear-to-Front * 4x 40/100GE QSFP/QSFP+ * 8x 1/10GE SFP/SFP+ * Neblokovaný výkon pro všechny požadované interface – 400 Gbps * OoB Management interface - RJ45 provedení * USB * Console port - RJ45 provedení * Úložiště pro lokální logy, debug soubory o kapacitě 2x 100 GB SSD * Maximální spotřeba: 266 W * Maximální váha: 10,3 kg | |
| **FYZICKÝ INTERFACE** | * 1GBASE-T * 1GBASE-SX * 1GBASE-LX * 10GBASE-SR * 10GBASE-LR * 10GBASE DAC (Twinmax cable) 3m * 4x10GBASE-SR (Channelization 4x10GE) * 4x10GBASE-LR * 4x10GBASE DAC (Twinmax cable) 3m | |
| **L2 VLASTNOSTI** | * Podpora jumbo frames o velikosti až 9216 B * Podpora L2 switching dle standardu IEEE 802.3 bridging * Velikost MAC tabulky = 1000k * LAG/LACP * Multi chassis LAG mezi dvěma switchi * LAG resilient hashing * Podpora VLAN (IEEE 802.1Q) * Plný rozsah VLAN = 16k * QinQ * Port based VLAN * VLAN translation (swap VLAN hlavičky) * LLDP (802.1ab) | |
| **ACLs (Access lists)** | * Podporováno v HW * Interface ACLs (ingress / egress) * VLAN ACLs (ingress / egress) * ACL match podmínky na L2 až L4 * ACL akce - discard / reject / accept / login / count / policer / instance assingment * ACL pro CPU protection | |
| **L3 FUNKCE** | * RVI (Routovaný VLAN interface) * L3 subinterface („VLAN overlaping“ mezi dvěma L3 subinterfaces) * Podpora IP FIB = 8000k * Static routing (IPv4/IPv6) * Ospf / ospfv3 * MBGP (IPv4, IPv6, EVPN) * VRRP (IPv4/6) * Virtual router (oddělené „Routing Information Bases“) – 32 oddělených Routing Information Bases * DHCP server (IPv4/6) / relay (IPv4/6) / konfigurovatlný pod Virtual router * BFD (static, OSPF, BGP) * Policy, Filter based routing = forwarding založený na L2-L4 source a destination hlavičkách | |
| **COS** | * Podpora v HW * „Trust“ traffic klasifikace založena na 802.1p, DSCP * „Untrust“ traffic klasifikace založena na L2-L4 polích hlavičky paketu * 8 front na interface * Egress Port shaping / Egress Queue shaping (sdílení provozu mezi frontami) * Priority DWRR scheduling mechanismus * Podpora priority interface Scheduler: * high * low * medium-high * medium-low * Strict priority implementace (LLQ) * WRED congastion mechanism * Ingres Policing single rate two colors, také Ingress shaping * Rewrite mechanism 802.1p, DSCP | |
| **MANAGEMENT A TROUBLESHOOTING** | * Společné OS cli napříč kategoriemi switchů: LEAF / SPINE / BORDER LEAF / EDGE switch - JUNOS CLI * Jeden vendor napříč síťovým portfoliem v rámci tohoto projektu a to pro kategorie - LEAF / SPINE / BORDER LEAF / EDGE switch/ WAN\_router / OoB\_MNGT - JUNIPER Networks (od tohoto vendora je nabízen také centrální FW) * Cli interface: plná konfigurovatelnost a řešení problémů * local * telnet * ssh * User autentication * local * Radius, TACAC+ * RBAC pro všechny typy authentikace * Automatická záloha konfigurace - plně podporováno SCP, FTP, TFTP * Konfigurační změny přes txt file * Konfigurovatelnost přes Netconf a gRPC s podporou Yang data modelů * Lokální i vzdálený syslog server * Ping, traceroute * Traffic mirroring * SNMPv2/v3 * Telemetry interface přes Netconf a gRPC s podporou Yang data modelů * Podpora Terraform a Ansible * Lokální i vzdálené spouštění skriptů - python, xslt, slax | |

#### DCI konektivita

DCI konektivita je propojení mezi dvěma PoDy. Je zohledněno do budoucna uvažované „roztržení“ na dva PoPy v geograficky vzdálených lokalitách pro tento účel dedikované dva nezávislé „EDGE switche“ s podporu MACsec, který zajistí bezpečnou komunikaci a integritu dat přes konektivitu mezi PoPy realizovanou DWDM technologií poskytovatele. Na následujícím obrázku je znázorněna pozice a těchto EDGE switchů.

XXXXX

Obrázek: Role EDGE prvků

Hlavními prvky DCI ve vlastnictví a správě objednatele, jsou EDGE switche. Ty jsou pouze v L2 režimu a provádějí L2 segmentaci do jednotlivých směrů dvojitého plně redundantního trojúhelníku. Sami nedisponují žádnými redundantními mechanismy (přesně řečeno nejsou pro ně konfigurovány). O redundanci se starají mechanismy vyšších vrstev, v tomto případě IGP se spuštěným BFD v redundantní ECMP topologii.

Hlavní funkcí EDGE switchů je tedy Line Rate MACsec pro kryptování provozu i routing protokolů. DWDM vrstva je v plné správě poskytovatele a ten musí dodat požadovaný počet client interface (tzv. šedivé interface) a požadované parametry linek. Pro navrhovanou architekturu je doporučeno následující (obsahuje i detaily ohledně možného rozšíření):

PoP A/B:

* Start kapacita:

2x 100 GE client + 2x 10GE interface na dvou nezávislých DWDM zařízeních

L0: 2x 100GE Lambda + 2x 10GE Lambda na dvou nezávislých fiber párech rovnoměrně rozloženo

Max. RTT E2E (fabric, edge, DWDM, Fiber). 1ms = max. vzdálenost cca. 80 km

* Rozšíření kapacita (celková):

4x 100 GE client + 4x 10GE interface na dvou nezávislých DWDM zařízeních

L0: 4x 100GE Lambda + 4x 10GE Lambda na dvou nezávislých fiber párech rovnoměrně rozloženo

Max. RTT E2E (fabric, edge, DWDM, Fiber). 1ms = max. vzdálenost cca. 80 km

PoP A/B – Witness:

* Start kapacita:

2x 100 GE client interface na dvou nezávislých DWDM zařízeních

L0: 2x 100GE Lambda na dvou nezávislých fiber párech rovnoměrně rozloženo

Max. RTT E2E (fabric, edge, DWDM, Fiber). 20ms = max. vzdálenost cca. Až 20 000 km

* Rozšíření kapacita:

4x 100 GE client interface na dvou nezávislých DWDM zařízeních

L0: 4x 100GE Lambda na dvou nezávislých fiber párech rovnoměrně rozloženo

Max. RTT E2E (fabric, edge, DWDM, Fiber). 20ms = max. vzdálenost cca. Až 20 000 km

Dodávka linek není součástí výběrového řízení a je zde zmíněná jen pro budoucí očekávané „roztržení na dva PoPy“.

Z výše definovaných specifikací pak vyplývají následující generické fyzické a funkční požadavky na EDGE switch.

Každý EDGE switch je čistě L2 a na propojích z PoPu podporuje MACsec.

Každý EDGE switch je:

* 1U rack mount zařízení;
* až 8x 100GE NNI portů (počet reflektuje možné rozšíření DC Fabric)
* vybavené 4x 100GBASE-DR originálními transceivery;
* až 4x 10GE NNI porty (počet reflektuje možné rozšíření DC Fabric)
* vybavené 2x 10Gbase-LR originálními transceivery;
* plná redundance zdrojů (PSU) a větráků (FAN);
* podpora L2;
* MACsec pro všechny definované porty.

Z uvedených požadavků a návrhu DCI konektivity v této kapitole výše vyplývá navrhovaný typ síťového prvku a počty kusů v následující tabulce:

|  |  |  |  |
| --- | --- | --- | --- |
| **Komponenty** | | | |
| **Číslo** | **Název komponenty** | **Part number** | **Počet kusů** |
| 1 | EDGE switch | XXXXX | 4 |

|  |  |
| --- | --- |
| **Komponenta - EDGE switch (4 ks)** | |
| **Vlastnost/ komponenta** | **Parametry** | |
| **SPECIFIKACE HW** | * Rack mount zařízení * Velikost (v x š x h): 4,37 x 44,09 x 52,02 (56,9 s kabely) cm * Instalace do 1000 mm hlubokého stojanu * Instalace do stojanu o velikosti 19“ stojan * Maximální výška boxu - 1U * AC zdroj: 1 + 1 redundance, vyměnitelný za chodu * Větrák: 5 + 1 redundance, vyměnitelný za chodu * Aktivní chlazení (FANy) tzv. Rear-to-Front * 48x 10/25GE SFP+/SFP28 * 8x 100GE QSFP28 uplink * Neblokovaný výkon pro všechny požadované interface – 2Tbps * OoB Management interface – 2x RJ45 provedení * USB * Console port - RJ45 provedení * Úložiště pro lokální logy, debug soubory o kapacitě 50 GB SSD * Maximální spotřeba: 283 W * Maximální váha: 11,25 kg | |
| **FYZICKÝ INTERFACE** | * 10GBASE-SR * 10GBASE-LR * 10GBASE DAC (Twinmax kabel) 3m * 100GBASE-SR4 * 100GBASE-LR4 * 100GBASE-DR * 100GBASE-FR * 100GBASE DAC (Twinmax kabel) 3m | |
| **L2 VLASTNOSTI** | * Podpora jumbo frames o velikosti až 9216 B * Podpora L2 switching dle standardu IEEE 802.3 bridging * Velikost MAC tabulky = 288k * LAG/LACP * LAG resilient hashing * Podpora VLAN (IEEE 802.1Q) * Plný rozsah VLAN = 4094k * QinQ * Port based VLAN * VLAN translation (swap VLAN hlavičky) * xSTP: * IEEE 802.1D (STP jako součást) * IEEE 802.1s (MSTP) * IEEE 802.1w (RSTP) * STP security functions * BPDU guard * Loop guard * Root guard * LLDP (802.1ab) * MACsec * 802.1AE * AES256 | |
| **DCB** | * Loss-less Ethernet – 2 fronty * Priority-based flow control (PFC)—IEEE 802.1Qbb * Explicit congestion notification (ECN) * Data Center Bridging Exchange Protocol (DCBX) * RDMA over converged Ethernet version 2 (RoCEv2) | |
| **ACLs (Access lists)** | * Podporováno v HW * Interface ACLs (ingress / egress) * VLAN ACLs (ingress / egress) * ACL match podmínky na L2 až L4 * ACL akce - discard / reject / accept / login / count / policer / instance assingment * ACL pro CPU protection | |
| **L3 FUNKCE** | * RVI (Routovaný VLAN interface) * L3 subinterface („VLAN overlaping“ mezi dvěma L3 subinterfaces) * Podpora IP FIB - 351k záznamů pro IPv4 LPM, 172k záznamů pro IPv6 LPM * Static routing (IPv4/IPv6) | |
| **MCAST** | * Podporováno v HW * IGMP snooping v1/2/3 * MLD snooping v1/2 | |
| **COS** | * Podpora v HW * „Trust“ traffic klasifikace založena na 802.1p, DSCP * „Untrust“ traffic klasifikace založena na L2-L4 polích hlavičky paketu * 8 front na interface * Egress Port shaping / Egress Queue shaping (sdílení provozu mezi frontami) * Priority DWRR scheduling mechanismus * Podpora priority interface Scheduler * Strict priority implementace (LLQ) * WRED congastion mechanism * Ingres Policing single rate two colors, také Ingress shaping * Rewrite mechanism 802.1p, DSCP | |
| **MANAGEMENT A TROUBLESHOOTING** | * Společné OS cli napříč kategoriemi switchů: LEAF / SPINE / BORDER LEAF / EDGE switch - JUNOS CLI * Jeden vendor napříč síťovým portfoliem v rámci tohoto projektu a to pro kategorie - LEAF / SPINE / BORDER LEAF / EDGE switch/ WAN\_router / OoB\_MNGT - JUNIPER Networks (od tohoto vendora je nabízen také centrální FW) * Cli interface: plná konfigurovatelnost a řešení problémů * local * telnet * ssh * User autentication * local * Radius, TACAC+ * RBAC pro všechny typy authentikace * Automatická záloha konfigurace - plně podporováno SCP, FTP, TFTP * Konfigurační změny přes txt file * Konfigurovatelnost přes Netconf a gRPC s podporou Yang data modelů * Lokální i vzdálený syslog server * Ping, traceroute * sFlow, Ipfix * Traffic mirroring * SNMPv2/v3 * Telemetry interface přes Netconf a gRPC s podporou Yang data modelů * Podpora Terraform a Ansible * Lokální i vzdálené spouštění skriptů - python, xslt, slax | |

### L2-L7 security

#### Požadavky na nové řešení

Objednatel požaduje řešení vycházející z následujících potřeb:

* Centralizovaná služba;
* L4 FW služby z internetu: NAT, terminace IPsec;
* L4 FW služby v rámci DC: statefull kontrola relací pro aplikace uvnitř DC;
* L4-L7: LB služby z internetu (nyní přes CMS): WAF, LB služby pro aplikace přístupné přes CMS, SSL VPN;

Řešení zajištující bezpečnost musí reflektovat cílové řešení rozprostření ve dvou geograficky oddělených lokalitách (tzv. Metrocluster) s architekturou zajišťující vysokou dostupnost (HA).

* Plné HA na každé lokaci
  + FW cluster;
  + LB cluster;

Tzv. Clusterem se rozumí:

* + - Active/Passive implementace;
    - plná synchronizace session na Passive node;
    - gracefull switchover v případě fail na Node i v případě fail na interfacech;
    - plný switchower = žádný traverz provozu přes Cluster data propoje;
* HA na každé lokaci
  + V každé lokaci bude vytvořen plnohodnotný cluster FW a LB;
  + Bezstavové (tzv. stateless) přepnutí provozu v případě výpadku celého clusteru v jedné lokaci přes druhou část instalace v druhé lokaci;
  + Bezstavové (tzv. stateless) přepnutí provozu pomocí směrování (tzv. routingu);

Výše popsané požadavky určují jasnou architekturu a jasné fyzické a funkční požadavky na nabídnuté Firewally a Load Balancery.

#### Firewall

Jedná se o oddělený/samostatný hardware, který slouží pro síťovou ochranu celého prostředí. Počet FW v každé z lokací řešení jsou 2ks, tj. celkově požadováno dodat 4ks. Hardware bude připojen technologii 100Gb/s.

Jedná se o minimálně stavový firewall, rozložen přes obě lokality. Je požadován návrh řešení v módu active-active, interlink pro cluster musí být realizován na dvou nezávislých linkách prostřednictvím LAN technologií.

Firewall musí být připojen takzvaně Dual-Homing s dostatečnou propustností. Pro firewall v případě výpadku jednoho portu při Dual-Homing zapojení není povoleno degradování propustnosti/výkonu.

Firewall musí disponovat VPN technologií, součástí bezpečnostního řešení musí být systém pro detekci útoků (IDS/IPS).

Každý FW je:

* Až 2x 100GE NNI portů (počet reflektuje možné rozšíření DC fabric)
  + Vybavené 2x 100GBASE-SR4 SFP28 originálními transceivery
* Plná redundance pasivních komponentů = Napájení a chlazení;
* Podpora L4FW, NAT, IPsec, SSL VPN, L3;
* NG-FW, IDP, UMT, URL filtering, vše rozšiřitelné licencí;

|  |  |  |  |
| --- | --- | --- | --- |
| **Firewall** | | | |
| **Číslo** | **Název komponenty** | **Part number** | **Počet kusů** |
| 1 | FIREWALL | XXXXX | 4 |

Tabulka - Identifikace komponenty FW

Zejména musí poskytovat tyto klíčové vlastnosti:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Firewall – min. 4 ks** | | | | |
| **Číslo** | **Vlastnost/ komponenta** | **Požadované parametry** | **Splňuje ANO/NE** | **Skutečné parametry/Způsob splnění požadavku** |
|  | Kompatibilita | * Zařízení musí být kompatibilní s všemi nabízenými prvky a zajišťovat všechny potřebné funkcionality v rámci celého řešení | ANO | Navržené zařízení firewallu je plně kompatibilní se všemi nabízenými prvky a bude zajišťovat všechny potřebné funkcionality v rámci celého řešení. |
|  | Technické vlastnosti a rozměry | * Kompatibilní s RACK 19” | ANO | Navržené zařízení firewallu je kompatibilní s RACK 19”, rozměry zařízení jsou (š x v x h):  43,89 x 4,42 x 46,23 cm. |
|  | * Velikost v EIA (jednotek U) pro systémovou skříň 19” nesmí přesáhnout 1U. | ANO | Navržené zařízení firewallu má velikost 1U, rozměry (š x v x h): 43,89 x 4,42 x 46,23 cm. |
|  | * Dodavatel uvede počet a typ napájení (C13/14 nebo C19/C20 a počet). |  | Navržené zařízení firewallu má typ napájení C13/14, celkem 2ks na 1 zařízení. |
|  | * Dodavatel uvede hmotnost a typický a maximální elektrický příkon. |  | Navržené zařízení firewallu má hmotnost 8.8 kg s průměrným příkonem 186 W a maximálním elektrickým příkonem 229 W. |
|  | * Dodavatel uvede, jaké jsou požadavky na elektrické jištění. |  | Požadavky navrženého zařízení firewallu jsou dedikovaný jistič na min. 16A pro každý vstup zapojený na dedikovanou napájecí větev. |
|  | Napájení a chlazení | * Zařízení musí mít redundantní napájecí zdroje 250VAC, vyměnitelné za chodu. (Dodavatel také popíše řešení redundance (N+N, N+1 atd.). | ANO | Navržené zařízení firewallu má redundantní napájecí zdroje 250VAC, vyměnitelné za chodu s 1+1 redundancí. |
|  | * Zařízení musí mít redundantní chladící komponenty, vyměnitelné za chodu. (Dodavatel také popíše řešení redundance (N+N, N+1 atd.). | ANO | Navržené zařízení firewallu má redundantní chladící komponenty s 3+1 redundancí a vyměnitelných za chodu. |
|  | * Aktivní chlazení Rear-to-Front. (v případě nabídnutí zařízení, které má chlazení Front-to-Rear, je potřeba toto vzít v úvahu při montáži a počítat s delšími kabely pro vyvázání v na Patch panel) | ANO | Navržené zařízení firewallu má chlazení provedeno v režimu Front-to-Rear, při instalaci zařízení bude dle požadavku objednatele zohledněno a instalováno tak, aby směr proudění vzduchu byl jednotný pro všechny prvky v rámci stojanu. |
|  | Počet portů | * Minimálně 2ks 100GE QSFP28 portů pro data, standardně osazených * Minimálně 2ks 1GE SFP+ pro komunikaci HA clusteru, standardně osazených | ANO | Navržené zařízení firewallu obsahuje počet portů:   * 2ks 100 GbE QSFP28 pro data, standardně osazených * 2ks 1GbE SFP+ pro control link, které slouží pro HA cluster, standardně osazených.   Celkový počet portů:   * 2 x 40 GbE/100 GbE QSFP28 * 8 x 1 GbE/10 GbE SFP+ * 4 x 1 GbE/10 GbE/25 GbE SFP28   Dedikované HA porty clusteru:   * 2 x 1 GbE SFP pro control link. |
|  | Konzolový port | * Provedení RJ45 nebo USB (pozn. u USB i převodníky USB/RS-232(RJ45)) | ANO | Navržené zařízení firewallu má konzolový port v provedení RJ45. |
|  | Propojovací kabely | * Odpovídající počet propojovacích kabelů pro plné zprovoznění systému. | ANO | Navržené řešení obsahuje potřebný počet propojovacích kabelů pro plné zprovoznění systému. |
|  | Kapacita | * Minimálně 32GB SSD pro lokální logy, debug soubory atd. | ANO | Navržené zařízení firewallu má 2x120GB SSD disk pro lokální logy, debug soubory atd.. |
|  | * Podporovány musí být enterprise SSD disky, DWPD hodnota nabízených disků/modulů musí být 1 nebo vyšší. | ANO | Navržené zařízení firewallu má plnou podporu enterprise SSD disků a DWPD hodnota je 1,3. |
|  | Charakteristiky a funkce | * Podpora Jumbo Frames min. 9kB | ANO | Navržené zařízení firewallu podporuje Jumbo Frames v hodnotě 9kB. |
|  | * Podpora vytvoření tzv. subinterface s individuální konfigurací parametrů: VLAN-id, encapsulation, apod. | ANO | Navržené zařízení firewallu podporuje vytvoření subinterface s individuální konfigurací parametrů: VLAN-id, encapsulation, apod..  U JUNIPER Networks síťových prvků je tento subintreface nazývaný „unit“. |
|  | * Režim HA v módu active-passive a active-active | ANO | Navržené zařízení firewallu podporuje režim HA v módu active-passive a active-active.  Může být použitá funkce cluster nebo i Multinode HA. |
|  | * Každý HA uzel musí disponovat informacemi o probíhajícím provozu a jsou synchronizovány tak, aby při výpadku jednoho FW nedošlo ke ztrátě informací NAT a k přerušení aktivních spojení provozu TCP/UDP procházejícího skrze FW | ANO | V rámci navrženého firewall řešení každý HA uzel disponuje informacemi o probíhajícím provozu a jsou synchronizovány tak, aby při výpadku jednoho FW nedošlo ke ztrátě informací NAT a k přerušení aktivních spojení provozu TCP/UDP procházejícího skrze FW.  Synchronizace sessions je přes HA fabric propoje. |
|  | * Porpora SNMP (1v/2v/3v):   + HA musí být monitorovatelný pomocí SNMP dostupném v OoB mgmt rozhraní | ANO | Navržené zařízení firewallu podporuje SNMP (1v/2v/3v):   * HA je monitorovatelný pomocí SNMP dostupném v OoB mgmt rozhraní.   Dostupnost bude řešena MIBs pro monitoring chassis cluster status. |
|  | * HA řešení musí podporovat pro sestavení HA clusteru rozdílné rozhraní, než jsou požadované 2x100GE, min. 2x1GE (jedná se o další dva porty, které jsou nad rámec požadovaných a definovaných v bodu 10.) | ANO | V rámci navrženého HA řešení je podpora pro sestavení HA clusteru rozdílného rozhraní, než jsou požadované 2x100GE, min. 2x1GE. Bude to řešeno dalšími dvěma porty, které jsou nad rámec požadovaných a definovaných v bodu 10. - 2x10GE.  Bude řešeno v rámci HA jsou na chassis dedikované 2x 1GE SFP. |
|  | * Na HA řešení je možné provést failover na základě nedostupnosti druhého NGFW, up/down stavu interface, nebo nedostupnosti specifikované IP adresy, nebo více IP adres | ANO | V rámci navrženého HA řešení je možné provést failover na základě nedostupnosti druhého NGFW, up/down stavu interface. Je možná i konfigurace na základě nedostupnosti specifikované IP adresy, nebo více IP adres. |
|  | * Podpora na úrovni L2:   + LAG/LACP pro jakýkoliv typ interface   + LAG group = min. 64   + podpora VLAN (IEEE 802.1Q)   + plný roszah VLAN = min. 4k   + LLDP (802.1ab) | ANO | Navržené zařízení firewallu na úrovni L2:   * má podporu LAG i LACP pro jakýkoliv typ interface * má podporu až 128 LAG group * má podporu VLAN (IEEE 802.1Q) * má podporu s plným rozsahem VLAN 4,094k * má plnou podporu LLDP protokolu dle IEEE 802.1AB pro výměnu informací o sousedních zařízeních na L2. Lze konfigurovat lokálně, nebo na úrovni jednotlivých datových rozhraní. |
|  | * Podpora MBGP (IPv4, IPv6) | ANO | Navržené zařízení firewallu má plnou podporu MBGP IPv4 a IPv6, tzv. „family inet“ a „family inet6“ lze konfigurovat paralelně. |
|  | * Podpora VRRP (IPv4/6) | ANO | Navržené zařízení firewallu má plnou podporu VRRP (IPv4/6). |
|  | * Podpora IGMP (v2/v3) | ANO | Navržené zařízení firewallu má plnou podporu IGMP (v2/v3). |
|  | * Podpora ECMP (Equal-Cost Multi-Path) Load Balancing – min. 8 ECMP cest | ANO | Navržené zařízení firewallu má podporu ECMP Load Balancing, maximálně 16 ECMP cest. |
|  | * Podpora PIM (Protocol Independent Multicast) SSM/ASM | ANO | Navržené zařízení firewallu má podporu PIM (Protocol Independent Multicast) SSM/ASM. |
|  | * Podpora Policy, Filter based routing (směrování založené na L2-L4 zdrojových a cílových hlavičkách | ANO | Navržené zařízení firewallu má podporu Policy, Filter based routing (směrování založené na L2-L4 zdrojových a cílových hlavičkách. |
|  | * Podpora plnohodnotných virtuálních kontextů (virtuálních firewallů) s oddělenou správou – min. 30 | ANO | Navržené zařízení firewallu má plnou podporu plnohodnotných virtuálních kontextů (virtuálních firewallů) s oddělenou správou – 32.  Je možné použít tři úrovně oddělení. První možností je konfigurace tzv. virtuálních routerů. Další vyšší úrovní je využití tzv. logických systémů, ve kterých je možno plnohodnotně konfigurovat všechny hierarchické úrovně OS včetně Virtual-routers. Třetí úrovní je konfigurace „Tenant system“.  Je možné konfigurovat až 32x logický systém a až 500x Tenant system. |
|  | * Podpora BFD (Bi-directional Forwarding Detection) – min. static, OSPF, BGP | ANO | Navržené zařízení firewallu má plnou podporu všech požadovaných protokolů – static, OSPF i BGP. |
|  | * Podpora na úrovni L3:   + RVI (Routovaný VLAN interface)   + min. IP FIB = 20k   + Static routing (IPv4/IPv6)   + Podpora ospf / ospfv3   + ECMP balancing / resilient hashing - min. 8 ECMP cest | ANO | Navržené zařízení firewallu na úrovni L3:   * má plnou podporu RVI * má podporu max RIB/FIB = 2000k/1200k * má plnohodnotnou podporu IPv4 a IPv6 pro všechny routing protokoly * má plnou podporu OSPF i OSPFv3 * má plnou podporu ECMP balancing a resilient hashing, až na 16 ECMP cest   Je možné konfigurovat subinterface (unit) s definovaným VLAN-tag. |
|  | FW funkce | * Statický NAT, Destination NAT, Source NAT (za jednu nebo více IP adres), obousměrné překlady IPv4 a IPv6. Persistence překladu v rámci NAT poolu na úrovni IP | ANO | Navržené zařízení firewallu má plnou podporu pro Statický NAT, Destination NAT, Source NAT (za jednu nebo více IP adres), obousměrné překlady IPv4 a IPv6. Persistence překladu v rámci NAT poolu na úrovni IP.  Defaultně je IP z IP pool vybrána dynamicky = mění se source host IP. Konfigurací „persistant option“ zůstává stejná „vybraná“ IP pro každý source host. |
|  | * Souběžně aplikovatelné Source i Destination nat pravidla na jeden typ provozu | ANO | Navržené zařízení firewallu má plnou podporu pro souběžně aplikovatelné Source i Destination NAT pravidla na jeden typ provozu.  NAT může být jak statický, tak i dynamický s využitím pool IP adres. |
|  | * Podpora vyhodnocování NAT pravidel na úrovni Zdrojové zóny a IP adres zdroje a cíle, portů a protokolů pro source a destination NAT | ANO | Navržené zařízení firewallu má plnou podporu vyhodnocování NAT pravidel na úrovni Zdrojové zóny a IP adres zdroje a cíle, portů a protokolů pro source a destination NAT. |
|  | * Možnost tvorby bezpečnostních politik se specifikací source IP, destination IP, port | ANO | Navržené zařízení firewallu má možnost tvorby bezpečnostních politik se specifikací source IP, destination IP, port pomocí tzv. security policies s definicí zones a match pravidel. |
|  | * Řešení lze v případě potřeby rozšířit (tj. nyní parametr nepožadován) o parametr:   Možnost definice bezpečnostních politik s využitím user/user group, L7 aplikací | ANO | Navržené řešení lze v případě potřeby rozšířit o parametr:  Možnost definice bezpečnostních politik s využitím user/user group, L7 aplikací.  Lze splnit licencí PREMIUM1, (není požadována a není součástí nabídky).  Pomocí tzv. „User Role Firewall Security Policies = authentikace a vyhodnocení user a vyhodnocení aplikace. |
|  | * Řešení lze v případě potřeby rozšířit (tj. nyní parametr nepožadován) o parametr:   Možnost konfiguraci ochrany firewallu na síťových rozhraních – podpora IP spoofing a UDP, ICMP a SYN floods | ANO | Navržené řešení má plnou podporu konfigurace ochrany firewallu na síťových rozhraních – podpora IP spoofing a UDP, ICMP a SYN floods.  Chráněno konfigurací tzv. „screening option“. |
|  | * Řešení lze v případě potřeby rozšířit (tj. nyní parametr nepožadován) o parametr:   FW obsahuje integrovaný systém IPS systém fungující na principu signatur a anomálií. Databáze IPS signatur musí být aktualizovatelná nezávisle na OS. Aplikace IPS profilu musí být granulární, na úrovni bezpečnostního pravidla | ANO | Řešení lze v případě potřeby rozšířit o parametr:  FW obsahuje integrovaný systém IPS systém fungující na principu signatur a anomálií. Databáze IPS signatur musí být aktualizovatelná nezávisle na OS. Aplikace IPS profilu musí být granulární, na úrovni bezpečnostního pravidla.  Lze splnit licencí PREMIUM1, (není požadována a není součástí nabídky).  Výrobce FW se stará o databázi signatur a anomálií. Update na FW může být prováděn manuálně pomocí CLI příkazu a automaticky v konfigurovaném pravidelném intervalu.  IPD policy lze aplikovat na úrovni security policy. |
|  | * Min. 30 000 bezpečnostních pravidel | ANO | Navržené zařízení firewallu splňuje požadavek a to 30 000 bezpečnostních pravidel. |
|  | * Min. počet vytvořitelných zónových kontextů (párů zón) na NGFW je 4000 | ANO | Navržené zařízení firewallu splňuje požadavek, počet vytvořitelných zónových kontextů (párů zón) na NGFW je 4096. |
|  | * Řešení lze v případě potřeby rozšířit (tj. nyní parametr nepožadován) o parametr:   "Application layer Gateway" pro protokoly DNS, IKE, RPC, FTP, SIP | ANO | Navržené řešení lze v případě potřeby rozšířit o parametr: "Application layer Gateway" pro protokoly DNS, IKE, RPC, FTP, SIP a všechny uvedené parametry a další typy ALG jsou podporovány. |
|  | * Route-based site-to-site IPsec VPN | ANO | Navržené řešení má plnou podporu pro Route-based site-to-site IPsec VPN.  Také „policy“ based je podporována. |
|  | * Možnost definovat více traffic selectorů pro jeden IPsec tunel, včetně více traffic-selector pro jedno IPSEC CHILD-SA | ANO | Navržené řešení má možnost definovat více traffic selectorů pro jeden IPsec tunel, včetně více traffic-selector pro jedno IPSEC CHILD-SA. |
|  | * Min. počet IPsec tunelů na FW je 3000 (statický endpoint, IPSEC SA je počítaný jako jeden tunel) | ANO | Navržené řešení splňuje počet IPsec tunelů na FW a to v počtu 4000 (statický endpoint, IPSEC SA je počítaný jako jeden tunel). |
|  | * Řešení lze v případě potřeby rozšířit (tj. nyní parametr nepožadován) o parametr:   Podpora prioritizace a frontování provozu na základě zdrojové a cílové IP adresy, portu, uživatelské identity a aplikace, kdy je nadbytečná komunikace je zahozena, nebo frontována | ANO | Navržené řešení má plnou podporu pro prioritizace a frontování provozu na základě zdrojové a cílové IP adresy, portu, uživatelské identity a aplikace, kdy je nadbytečná komunikace je zahozena, nebo frontována.  Uvedená funkcionalita je součástí dodávky a bude implementovaná.  Je možné uplatnit Junos společný Cos na základě trusted (QoS bits v hlavičkách paketů) untrust (na základě ACL) klasifikace s následnou konfigurací schedulerů a aplikováním na konkrétní interface. Je možné také aplikovat AppCos s rule-sets na L7 match aplikace s možnou akcí DCSP přemarkování a/nebo přiřazením do traffic-class a/nebo přímou aplikací rate limit. Dále je možné nasadit „společné“ Junos CoS mechanismy na základě traffic class přiřazeného pomocí AppCoS nebo klasifikovat provoz znovu na základě AppCos DSCP markovaného provozu. |
|  | * Podpora prioritizaci provozu na základě DSCP | ANO | Navržené řešení má plnou podporu pro prioritizaci provozu na základě DSCP.  Po klasifikaci provozu (viz bod 45) je možné nasadit scheduler mechanismy, kde je možné pro jednotlivé schedulery definovat například provozní limit a prioritu. |
|  | * Podpora prioritizaci provozu na základě identifikované aplikace | ANO | Navržené řešení má plnou podporu prioritizace provozu na základě identifikované aplikace.  Popsáno u bodů 45 a 46. |
|  | * Řešení lze v případě potřeby rozšířit (tj. nyní parametr nepožadován) o parametr:   Podpora dešifrování příchozího SSL/TLS provozu, za pomoci serverového certifikátu a priv klíče (reverse proxy) | ANO | Navržené řešení má plnou podporu dešifrování příchozího SSL/TLS provozu, za pomoci serverového certifikátu a priv klíče (reverse proxy).  Konfigurace na úrovni firewall rules. |
|  | * Řešení lze v případě potřeby rozšířit (tj. nyní parametr nepožadován) o parametr:   Podpora dešifrování odchozího SSL/TLS provozu, za pomoci naimportovaného priv klíče interního serveru (forward proxy) | ANO | Navržené řešení má plnou podporu dešifrování odchozího SSL/TLS provozu, za pomoci naimportovaného priv klíče interního serveru (forward proxy).  Zařízení podporuje forward-proxy a reverse-proxy. |
|  | * Řešení lze v případě potřeby rozšířit (tj. nyní parametr nepožadován) o parametr:   Dešifrovaný provoz musí být možno definovat na základě všech typických parametrů, jako jsou zdrojová a cílová IP adresa, port, uživatelská identita | ANO | Navržené řešení má plnou podporu dešifrování provozu, které může být definováno na základě všech typických parametrů, jako jsou zdrojová a cílová IP adresa, port, uživatelská identita.  Konfigurace rules pro security policies, kde je možné definovat požadované parametry jako „match“ podmínky. |
|  | * Řešení lze v případě potřeby rozšířit (tj. nyní parametr nepožadován) o parametr:   Podpora dešifrování protokolu TLS verze 1.2 i 1.3 | ANO | Navržené řešení má plnou podporu dešifrování protokolu TLS verze 1.2 i 1.3. |
|  | * Řešení lze v případě potřeby rozšířit (tj. nyní parametr nepožadován) o parametr:   FW nebo jiné dekrypční zařízení dešifrování za pomocí ECC (Elliptical Curve Cryptography) a ECDHE pro příchozí i odchozí provoz | ANO | Navržené řešení lze v případě potřeby rozšířit o parametr:  FW nebo jiné dekrypční zařízení dešifrování za pomocí ECC (Elliptical Curve Cryptography) a ECDHE pro příchozí i odchozí provoz.  Lze splnit licencí PREMIUM1, (není požadována a není součástí nabídky). |
|  | * Řešení lze v případě potřeby rozšířit (tj. nyní parametr nepožadován) o parametr:   Podpora L7 Aplikačního Firewallu a rozpoznání aplikací nezávisle na TCP/UDP portech (update aplikačních signatur výrobcem) | ANO | Navržené řešení lze v případě potřeby rozšířit o parametr:  Podpora L7 Aplikačního Firewallu a rozpoznání aplikací nezávisle na TCP/UDP portech (update aplikačních signatur výrobcem).  Lze splnit licencí PREMIUM1, (není požadována a není součástí nabídky).  Je možné nasadit AppID modul pro rozpoznání aplikací na L7. Tento modul je společný pro nasazení IDP nebo unified AppFW policies. |
|  | * Řešení lze v případě potřeby rozšířit (tj. nyní parametr nepožadován) o parametr:   FW obsahuje mimo definovaných jednotlivých aplikací i aplikační kategorie | ANO | Navržené řešení lze v případě potřeby rozšířit o parametr:  FW obsahuje mimo definovaných jednotlivých aplikací i aplikační kategorie.  Lze splnit licencí PREMIUM1, (není požadována a není součástí nabídky).  Standardní a custom aplikace mohou být použity stejně jako tzv. application-sets (aplikační kategorie). |
|  | * Řešení lze v případě potřeby rozšířit (tj. nyní parametr nepožadován) o parametr:   Definovaná aplikace/kategorie je jedním "match" kritériem při policy lookup společně se source a destination IP | ANO | Navržené řešení lze v případě potřeby rozšířit o parametr:  Definovaná aplikace/kategorie je jedním "match" kritériem při policy lookup společně se source a destination IP.  Lze splnit licencí PREMIUM1, (není požadována a není součástí nabídky).  Kromě požadovaných „match“ podmínek je možné ještě konfigurovat „from zone“ „to-zone“ a protokol. |
|  | * Řešení lze v případě potřeby rozšířit (tj. nyní parametr nepožadován) o parametr:   Identifikace L7 aplikace musí probíhat přímo v FW | ANO | Navržené řešení lze v případě potřeby rozšířit o parametr:  Identifikace L7 aplikace musí probíhat přímo v FW.  Lze splnit licencí PREMIUM1, (není požadována a není součástí nabídky).  Podpora v rámci AppID modulu. |
|  | * Řešení lze v případě potřeby rozšířit (tj. nyní parametr nepožadován) o parametr:   FW musí umět pracovat s neznámými aplikacemi - upozornit na ně a mít možnost je zakázat | ANO | Navržené řešení lze v případě potřeby rozšířit o parametr:  FW musí umět pracovat s neznámými aplikacemi - upozornit na ně a mít možnost je zakázat.  Lze splnit licencí PREMIUM1, (není požadována a není součástí nabídky).  Může být definována akce pro tzv. „unknown-applications“. |
|  | * Řešení lze v případě potřeby rozšířit (tj. nyní parametr nepožadován) o parametr:   FW musí umožňovat tvorbu plnohodnotných, uživatelsky definovaných aplikací bez nutnosti využití externího nástroje nebo zásahu výrobce/dodavatele. Tyto uživatesky definované aplikace nejsou omezeny na specifický protokol (např. HTTP, HTTPS) | ANO | Navržené řešení lze v případě potřeby rozšířit o parametr:  FW musí umožňovat tvorbu plnohodnotných, uživatelsky definovaných aplikací bez nutnosti využití externího nástroje nebo zásahu výrobce/dodavatele. Tyto uživatesky definované aplikace nejsou omezeny na specifický protokol (např. HTTP, HTTPS).  Lze splnit licencí PREMIUM1, (není požadována a není součástí nabídky).  Je možné definovat tzv. custom applications“. |
|  | * Řešení lze v případě potřeby rozšířit (tj. nyní parametr nepožadován) o parametr:   FW umožňuje získávat Dynamické seznamy známých škodlivých IP adres přímo od výrobce, ze zdrojů třetích stran a také definovat vlastní server s dynamickými listy a jeho update interval | ANO | Navržené řešení lze v případě potřeby rozšířit o parametr:  FW umožňuje získávat Dynamické seznamy známých škodlivých IP adres přímo od výrobce, ze zdrojů třetích stran a také definovat vlastní server s dynamickými listy a jeho update interval.  Lze splnit licencí PREMIUM1, (není požadována a není součástí nabídky).  Záznamy škodlivých IP adres od výrobce Firewall jsou součástí databáze SecIntel, která je na Firewall aktualizovaná z ATP cloud. |
|  | * Řešení lze v případě potřeby rozšířit (tj. nyní parametr nepožadován) o parametr:   FW podporuje možnost odesílání souborů k dynamické analýze do sandbox prostředí jako ochranu předa škodlivým kódem | ANO | Navržené řešení lze v případě potřeby rozšířit o parametr:  FW podporuje možnost odesílání souborů k dynamické analýze do sandbox prostředí jako ochranu předa škodlivým kódem.  Lze splnit licencí PREMIUM1, (není požadována a není součástí nabídky).  Je součástí celého konceptu ATP ochrany. |
|  | * Řešení lze v případě potřeby rozšířit (tj. nyní parametr nepožadován) o parametr:   Sandbox poskytován stejným výrobcem jako FW | ANO | Navržené řešení lze v případě potřeby rozšířit o parametr:  Sandbox poskytován stejným výrobcem jako FW.  Lze splnit licencí PREMIUM1, (není požadována a není součástí nabídky).  Sandbox může být jako cloud service (multitenant prostředí) a nebo může být implementovaný onsite pomocí virtual appliance. |
|  | * Řešení lze v případě potřeby rozšířit (tj. nyní parametr nepožadován) o parametr:   Statická i dynamická analýza souborů a dokumentů na přítomnost kybernetických hrozeb ve virtuálním prostředí | ANO | Navržené řešení lze v případě potřeby rozšířit o parametr:  Statická i dynamická analýza souborů a dokumentů na přítomnost kybernetických hrozeb ve virtuálním prostředí.  Lze splnit licencí PREMIUM1, (není požadována a není součástí nabídky).  Sandbox může být jako cloud service (multitenant prostředí) a nebo může být implementovaný onsite pomocí virtual appliance. |
|  | * Řešení lze v případě potřeby rozšířit (tj. nyní parametr nepožadován) o parametr:   Monitorování chování spuštěného souboru a zaměření na pokusy o změny v systému soborů, systémových registrů, procesů a navázání síťových spojení s vyhotovením reportu | ANO | Navržené řešení lze v případě potřeby rozšířit o parametr:  Monitorování chování spuštěného souboru a zaměření na pokusy o změny v systému soborů, systémových registrů, procesů a navázání síťových spojení s vyhotovením reportu.  Lze splnit licencí PREMIUM1, (není požadována a není součástí nabídky).  V rámci sandboxu. |
|  | * Řešení lze v případě potřeby rozšířit (tj. nyní parametr nepožadován) o parametr:   Emulace a detekce na úrovni OS | ANO | Navržené řešení lze v případě potřeby rozšířit o parametr:  Emulace a detekce na úrovni OS.  Lze splnit licencí PREMIUM1, (není požadována a není součástí nabídky).  Sandbox s nainstalovanými OS. |
|  | * Řešení lze v případě potřeby rozšířit (tj. nyní parametr nepožadován) o parametr:   Sandbox analýza umí identifikovat známý i zero-day malware skrytý v souborech | ANO | Navržené řešení lze v případě potřeby rozšířit o parametr:  Sandbox analýza umí identifikovat známý i zero-day malware skrytý v souborech.  Lze splnit licencí PREMIUM1, (není požadována a není součástí nabídky).  Známý malware je mitigovaný již na úrovni Firewallu pomocí SecIntel feed a zero-day je podrobený identifikaci v sandbox. |
|  | * Řešení lze v případě potřeby rozšířit (tj. nyní parametr nepožadován) o parametr:   Logování sandboxových analýz, zaznamenané provedené operace a jejich výsledek | ANO | Navržené řešení lze v případě potřeby rozšířit o parametr:  Logování sandboxových analýz, zaznamenané provedené operace a jejich výsledek.  Lze splnit licencí PREMIUM1, (není požadována a není součástí nabídky). |
|  | * Řešení lze v případě potřeby rozšířit (tj. nyní parametr nepožadován) o parametr:   Možnost manuálního zaslání souborů pro analýzu do sandbox prostředí | ANO | Navržené řešení lze v případě potřeby rozšířit o parametr:  Možnost manuálního zaslání souborů pro analýzu do sandbox prostředí.  Lze splnit licencí PREMIUM1, (není požadována a není součástí nabídky). |
|  | Logování | * Možnost vyexportovat/poslat logy | ANO | Navržené řešení má možnost vyexportovat/poslat logy.  Definice syslog serveru. |
|  | * Posílání logů o provozu na min. 4 cílové syslog servery | ANO | Navržené řešení má plnou podporu k posílání logů o provozu na 8 cílových syslog serverů. |
|  | * Ukládání logů na interní SSD | ANO | Navržené řešení má plnou podporu ukládání logů na interní SSD.  Logování na lokální úložiště je jednou z variant ukládání logů. |
|  | * Umožňovat výběr přeposílaných logů na úrovni bezpečnostního pravidla | ANO | Navržené řešení umožňuje výběr přeposílaných logů na úrovni bezpečnostního pravidla.  Log může být akcí security policy. |
|  | * Umožnit tvorbu "Traffic mirroring" pravidel a přeposílání provozu k externímu analytickému zařízení | ANO | Navržené řešení umožňuje tvorbu "Traffic mirroring" pravidel a přeposílání provozu k externímu analytickému zařízení.  Mirroring na základě ACL. |
|  | Záruka | * Podpora řešení a aktualizace po dobu 6 let, 24x7, oprava do 24h | ANO | Navržené řešení má podporu řešení a aktualizace po dobu 6 let, 24x7, oprava do 24h. |
| * Komunikace výhradně v českém jazyce | ANO | Komunikace s podporou je výhradně v českém jazyce. |
| * Záruku garantuje přímo výrobce zařízení | ANO | Navržené řešení obsahuje garanci záruky přímo výrobcem navržených zařízení. |

Tabulka - Technické parametry pro FW

### Load balancer

Jedná se o oddělený/samostatný redundantní hardware, ve funkci Load-Balancer (rozklad zátěže) s podporou autentizace uživatelů, SSL akcelerátoru a webového aplikačního firewallu. Počet FW v každé z lokací řešení jsou 2ks, tj. celkově požadováno dodat 4ks. Hardware bude připojen technologii 100Gb/s.

Webový Aplikační Firewall (WAF) pracující na aplikační úrovni ISO OSI modelu bude poskytovat ochranu webových aplikací před kybernetickými útoky využitím pozitivní i negativní bezpečnostní logiky v bezpečnostních politikách, tj. explicitní povolení legitimního provozu (pozitivní logika) a zakázáním provozu, který je označený jako kybernetický útok. K těmto základním bezpečnostním politikám předpokládáme implementaci dalších dodatečných bezpečnostních vlastností, jako je ochrana před Brute Force útoky, detekce škodlivých robotů, ochranu před odcizením uživatelských relací. Webový aplikační firewall také bude poskytovat ochranu proti aplikačním DoS útokům zaměřeným na webové aplikace.

Webový aplikační firewall tedy přinese komplexní zabezpečení webových aplikací, především pak:

* Ochrana proti aplikačním DoS útokům (SlowLoris, R.U.D.Y, ApacheKiller, SSL útoky apod.);
* Ochrana proti "forcefull browsing", XSS, SQL-INJ, CSRF, manipulace s cookies, ochrana parametrů, URL apod.;
* Session Management – ochrana proti únosům relací;
* Brute Force Ochrana – ochrana před prolomení hrubou silou;

Součástí řešení bude také technologie/platforma pro řízení aplikačního provozu, odpovědná zejména za:

* Monitoring dostupnosti služeb;
* Rozklad zátěže provozu aplikací;
* SSL terminace vč. podpory šifer Camellia;
* HTTP/2 brána;
* Funkce reverzní proxy;
* Realizace optimalizačních funkcí pro akceleraci provozu (komprese, caching, optimalizace TCP stacku);
* Ochranu perimetru proti L3/4 DDoS útokům;
* Řízení přístupu uživatelů k aplikacím – autentizační brána.

Řešení musí umožňovat vytvoření specifické operace s procházejícím provozem např. vkládání/odebírání HTML kódu, operace manipulace s daty, manipulace s HTTP záhlavím, URI apod.

Řešení musí umožňovat požadovanou autentizaci klientů webové aplikace pomocí certifikátů s validací prostřednictvím CRL.

Navrhnuté řešení musí podporovat proaktivní monitoring klientských požadavků a jejich porovnávání se známými formami útoků a administrátorovi systému navrhovat jejich možnou eliminaci pomocí pravidel Aplikačního firewallu.

Každý LB je:

* Až 2x 100GE NNI portů (počet reflektuje možné rozšíření DC fabric)
  + vybavené 2x 100GBASE-SR4 SFP28 originálními transceivery;
* Podpora WAF, LB, L3;

|  |  |  |  |
| --- | --- | --- | --- |
| **Load Balancer** | | | |
| **Číslo** | **Název komponenty** | **Part number** | **Počet kusů** |
| 1 | Load Balancer F5 | XXXXX | 4 |

Tabulka - Identifikace komponenty LB

Zejména musí poskytovat tyto klíčové vlastnosti:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Load Balancer – min. 4 ks** | | | | |
| **Číslo** | **Vlastnost/**  **komponenta** | **Požadované parametry** | **Splňuje ANO/NE** | **Skutečné parametry/Způsob splnění požadavku** |
|  | Kompatibilita | * Zařízení musí být kompatibilní s všemi nabízenými prvky a zajišťovat všechny potřebné funkcionality v rámci celého řešení | ANO | Navržená zařízení load balanceru jsou plně kompatibilní se všemi nabízenými prvky a budou zajišťovat všechny potřebné funkcionality v rámci celého řešení.  Navržené řešení obsahuje všechny moduly F5.  LTM, GTM, aWAF, APM, AFM, DNS |
|  | Technické vlastnosti a rozměry | * Kompatibilní s RACK 19” | ANO | Navržené zařízení load balanceru jsou kompatibilní s RACK 19”. |
|  | * Velikost v EIA (jednotek U) pro systémovou skříň 19” nesmí přesáhnout 1U. | ANO | Navržené zařízení load balanceru má rozměry 1U, rozměry (v x š x h): 4,37 x 44,20 x 77,72 cm. |
|  | * Dodavatel uvede počet a typ napájení (C13/14 nebo C19/C20 a počet). |  | Navržené zařízení load balanceru má typ napájení C13/14, celkem 2ks na 1 zařízení. |
|  | * Dodavatel uvede hmotnost a typický a maximální elektrický příkon. |  | Navržené zařízení load balanceru má hmotnost 16,33 kg se dvěma zdroji.  Typický elektrický příkon 425 W a maximální elektrický příkon 650 W na zdroj. |
|  | * Dodavatel uvede, jaké jsou požadavky na elektrické jištění. |  | Pro navržené zařízení load balanceru jsou požadavky k maximálnímu příkonu na zdroje použití 16A jističe na každý napájecí přívod. |
|  | Napájení a chlazení | * Zařízení musí mít redundantní napájecí zdroje 250VAC, vyměnitelné za chodu. (Dodavatel také popíše řešení redundance (N+N, N+1 atd.). | ANO | Navržené zařízení load balanceru má redundantní napájecí zdroje 250VAC, vyměnitelné za chodu s 1+1 redundancí. |
|  | * Aktivní chlazení Rear-to-Front. (v případě nabídnutí zařízení, které má chlazení Front-to-Rear, je potřeba toto vzít v úvahu při montáži a počítat s delšími kabely pro vyvázání v na Patch panel) | ANO | Navržené zařízení load balanceru má chlazení provedeno v režimu Front-to-Rear, při instalaci zařízení bude dle požadavku objednatele zohledněno a instalováno tak, aby směr proudění vzduchu byl jednotný pro všechny prvky v rámci systémové skříně. |
|  | Počet portů | * Minimálně 2ks 100GE-SR4 QSFP28 portů pro data, standardně osazených * Minimálně 2ks 25GE SR4 SFP28 portů pro komunikaci HA clusteru, standardně osazených | ANO | Navržené zařízení load balanceru má počet portů:   * 2ks 100GE-SR4 QSFP28 portů pro data, standardně osazených * - 8ks 25GE SR4 SFP28 portů pro komunikaci HA clusteru, standardně osazených. |
|  | Konzolový port | * Provedení RJ45 nebo USB (pozn. u USB i převodníky USB/RS-232(RJ45)) | ANO | Navržené zařízení load balanceru má RJ45 provedení konzolového portu. |
|  | Management | * Rozhraní RJ45 pro mgmt OoB switche * MGMT přístup pomocí: sériový port, GUI, příkazový řádek, iLO | ANO | Navržené zařízení load balanceru má rozhraní RJ45 pro management Out-of-Band switche a management přístup pomocí sériového portu, GUI, příkazového řádku, iLO pro vzdálenou správu. |
|  | Propojovací kabely | * Odpovídající počet propojovacích kabelů pro plné zprovoznění systému | ANO | Navržené řešení obsahuje potřebný počet propojovacích kabelů pro plné zprovoznění systému. |
|  | Kapacita | * Minimálně 1TB SSD pro lokální logy, debug soubory atd. | ANO | Navržené zařízení load balanceru má 1TB M.2 SSD pro lokální logy, debug soubory atd.. |
|  | * Podporovány musí být enterprise SSD disky, DWPD hodnota nabízených disků/modulů musí být 1 nebo vyšší | ANO | Navržené zařízení load balanceru má podporu enterprise SSD disků. DWPD hodnota je vyšší než 1.  Zařízení obsahuje 1TB U.2 Enterprise-class SSD (RAID1 Mirrored). |
|  | Výkon | * Datová propustnost zařízení min. 95 Gb/s na L4 a min. 95 Gb/s na L7 | ANO | Navržené zařízení load balanceru má datovou propustnost zařízení   * na L4: 95Gb/s * na L7: 95Gb/s. |
|  | * Minimální propustnost HTTP požadavků 18 mil./s | ANO | Navržené zařízení load balanceru má propustnost HTTP požadavků 18 mil./s |
|  | * Počet souběžných L4 spojení min. 100 mil. | ANO | Navržené zařízení load balanceru má počet souběžných L4 spojení 100 mil.. |
|  | * Offload – HW komprese – propustnost min. 50 Gbps | ANO | Navržené zařízení load balanceru má Offload – HW komprese – propustnost 50 Gbps. |
|  | * SSL akcelerace v HW | ANO | Navržené zařízení load balanceru obsahuje SSL akceleraci v HW. |
|  | * Počet SSL transakcí za sekundu min. 100 000 (při použití 2K klíče) | ANO | Navržené zařízení load balanceru má počet SSL transakcí za sekundu 100 000 (při použití 2K klíče). |
|  | * Počet SSL transakcí za sekundu min. 70 000 (při použití ECDSA P-256 klíče) | ANO | Navržené zařízení load balanceru má počet SSL transakcí za sekundu 70 000 (při použití ECDSA P-256 klíče). |
|  | * Celkový šifrovací výkon min. 50 Gb/s | ANO | Navržené zařízení load balanceru má celkový šifrovací výkon 50 Gb/s. |
|  | * Virtualizace HW zdrojů | ANO | Navržené zařízení load balanceru má plnou podporu virtualizace HW zdrojů a to pomocí tzv. tenantů. |
|  | * HW podpora funkcí:   + SYN Cookie ochrana pro každou virtualizovanou službu;   + Základní DoS vektory s možností nastavení každou virtualizovanou službu;   + SIP a DNS DoS vektory; | ANO | Navržené zařízení load balanceru má HW podporu funkcí:   * SYN Cookie ochrana pro každou virtualizovanou službu; * Základní DoS vektory s možností nastavení každou virtualizovanou službu; * SIP a DNS DoS vektory; |
|  | Charakteristiky a funkce | * Podpora IPv4 | ANO | Navržené zařízení load balanceru má podporu IPv4. |
|  | * Plná podpora IPv6, IPv4/IPv6 gateway | ANO | Navržené zařízení load balanceru má plnou podporu IPv6, IPv4/IPv6 gateway. |
|  | * Podpora Spanning Tree Protokolu (STP) | ANO | Podpora Spanning Tree Protokolu (STP). |
|  | * Podpora SNMP (v1/v2c/v3) | ANO | Navržené zařízení load balanceru má plnou podporu SNMP (v1/v2c/v3). |
|  | * Podpora Active-Active a Active-Pasive módu | ANO | Navržené zařízení load balanceru má plnou podporu Active-Active a Active-Pasive módu. |
|  | * Možnost vytvoření HA clusteru mezi Virtuální a Hardware platformou | ANO | Navržené zařízení load balanceru má možnost vytvoření HA clusteru mezi Virtuální a Hardware platformou. |
|  | * Full-Proxy architektura (plné oddělení klientského a serverového spojení) | ANO | Navržené zařízení load balanceru má plnou podporu Full-Proxy architektury (plné oddělení klientského a serverového spojení). |
|  | * Podpora externích šifrovacích karet pro SSL (HSM) | ANO | Navržené zařízení load balanceru má plnou podporu externích šifrovacích karet pro SSL (HSM). |
|  | * Podpora ověření certifikátů vydaných podřízenou CA (intermediate CA) | ANO | Navržené zařízení load balanceru má plnou podporu ověření certifikátů vydaných podřízenou CA (intermediate CA). |
|  | * Možnost přidat vlastní funkce pomocí skriptování | ANO | Navržené zařízení load balanceru má možnost přidat vlastní funkce pomocí skriptování. |
|  | * Podpora HTTP/2 | ANO | Navržené zařízení load balanceru má plnou podporu HTTP/2. |
|  | * Podpora IPSec IKEv2 | ANO | Navržené zařízení load balanceru má plnou podporu IPSec IKEv2. |
|  | * Podpora konfigurace a správu zařízení přes REST API | ANO | Navržené zařízení load balanceru má plnou podporu konfigurace a správy zařízení přes REST API. |
|  | * Možnost aktivace min. následující funkcí na jedné HW platformě:   + L4-7 loadbalancing;   + ICSA certifikovaný Web aplikační firewall;   + ICSA certifikovaný síťový firewall;   + Autorizace a autentizace aplikací, SSL VPN;   + DNS služby a DNS firewall; | ANO | Navržené zařízení load balanceru má možnost aktivace následující funkcí na jedné HW platformě:   * L4-7 loadbalancing; * ICSA certifikovaný Web aplikační firewall; * ICSA certifikovaný síťový firewall; * Autorizace a autentizace aplikací, SSL VPN; * DNS služby a DNS firewall;   a to díky modulům LTM, aWAF, AFM, APM a DNS. |
|  | * Možnost používat knihovny JavaScript třetích stran k úpravě a správě provozu | ANO | Navržené zařízení load balanceru má možnost používat knihovny JavaScript třetích stran k úpravě a správě provozu.  Plná podpora pro možnost využití JAVAScriptů třetích stran díky využití node.js. |
|  | Vlastnosti a funkce WAF | * Integrace s nástrojem na detekci zranitelností webových aplikací | ANO | Navržené zařízení load balanceru má integraci s nástrojem na detekci zranitelností webových aplikací.  Plná podpora je pomocí modulu aWAF s možností integrace například s následujícími nástroji:   * Cenzic Hailstorm * WhiteHat Sentinel * IBM Rational AppScan * QualysGuard Web Application Scanning |
|  | * Detekce a blokování širokého spektra útoků na aplikační vrstvě, minimálně podle OWASP top10 | ANO | Navržené zařízení load balanceru má plnou podporu detekce a blokování širokého spektra útoků na aplikační vrstvě podle OWASP top10 a to pomocí modulu aWAF s možností kontroly souladu s OWASP Top10. |
|  | * Možnost doprogramovat si filtrovací pravidla pro aplikace | ANO | Navržené zařízení load balanceru má možnost doprogramovat si filtrovací pravidla pro aplikace.  Plná podpora je pomocí modulu aWAF s pomocí například iRules. |
|  | * Automatická korelace zranitelností do jednoho bezpečnostního incidentu | ANO | Navržené zařízení load balanceru má automatickou korelaci zranitelností do jednoho bezpečnostního incidentu a to pomocí modulu aWAF. |
|  | * Ochrana AJAX a JSON aplikací | ANO | Navržené zařízení load balanceru má ochrana AJAX a JSON aplikací a to pomocí modulu aWAF. |
|  | * Ochrana proti L7 DDoS útokům, web scrapingu a útokům pomocí hrubé síly (brute force) | ANO | Navržené zařízení load balanceru má ochranu proti L7 DDoS útokům, web scrapingu a útokům pomocí hrubé síly (brute force) a to pomocí modulu aWAF. |
|  | * Podpora Captcha metody | ANO | Navržené zařízení load balanceru má plnou podporu Captcha metody a to pomocí modulu aWAF. |
|  | * Automatické odlišení skutečných uživatelů od robotů | ANO | Navržené zařízení load balanceru má plnou podporu automatického odlišení skutečných uživatelů od robotů, a to pomocí modulu aWAF s funkcionalitou Bot Defense. |
|  | * Integrovaný XML firewall | ANO | Navržené zařízení load balanceru má plnou podporu integrovaného XML firewallu a to pomocí modulu aWAF. |
|  | * Podpora maskování/odstranění citlivých informací – čísla kreditních karet, rodné číslo, číslo pojištění apod. | ANO | Navržené zařízení load balanceru má podporu maskování/odstranění citlivých informací – čísla kreditních karet, rodné číslo, číslo pojištění apod. a to pomocí modulu aWAF. |
|  | * Automatické nahrávání a aplikování nových signatur | ANO | Navržené zařízení load balanceru má podporu automatického nahrávání a aplikování nových signatur a to pomocí modulu aWAF. |
|  | * Podpora pozitivního a negativního bezpečnostního modelu | ANO | Navržené zařízení load balanceru má podporu pozitivního a negativního bezpečnostního modelu a to pomocí modulu aWAF. |
|  | * Blokování útočníků na základě geolokace až na úroveň regionu | ANO | Navržené zařízení load balanceru má podporu blokování útočníků na základě geolokace až na úroveň regionu a to pomocí modulu LTM. |
|  | * Podpora ICAP pro antivirovou kontrolu – pro HTTP, SOAP a SMTP | ANO | Navržené zařízení load balanceru má podporu ICAP pro antivirovou kontrolu – pro HTTP, SOAP a SMTP a to pomocí modulu aWAF. |
|  | * Ochrana SMTP a FTP na aplikační úrovni | ANO | Navržené zařízení load balanceru má podporu ochrany SMTP a FTP na aplikační úrovni a to pomocí modulu aWAF. |
|  | * Podpora SSL (šifrování a dešifrování) | ANO | Navržené zařízení load balanceru má podporu SSL – šifrování i dešifrování. |
|  | * Podpora různých typů reportů – PCI, geolokační reporty | ANO | Navržené zařízení load balanceru má podporu různých typů reportů – PCI, geolokační reporty. |
|  | * Podpora standardů PCI DSS, HIPAA, Basel II a SOX | ANO | Navržené zařízení load balanceru má podporu standardů PCI DSS, HIPAA, Basel II a SOX a to pomocí modulu aWAF. |
|  | * Integrované bezpečnostní politiky pro Microsoft Outlook Web Access, Oracle Applications a Microsoft SharePoint | ANO | Navržené zařízení load balanceru má integrované bezpečnostní politiky pro Microsoft Outlook Web Access, Oracle Applications a Microsoft SharePoint a to pomocí modulu aWAF nabízející templaty pro nejčastěji používané aplikace včetně zmíněných. |
|  | * Podpora pro analýzu HTTP provozu (Top URL, Top klienti, nejpoužívanější HTTP metody, návštěvnost stránek podle geogr. regionu) | ANO | Navržené zařízení load balanceru má podporu pro analýzu HTTP provozu (Top URL, Top klienti, nejpoužívanější HTTP metody, návštěvnost stránek podle geogr. regionu). |
|  | * Podpora aplikačního firewallu ve virtuálních kontextech | ANO | Navržené zařízení load balanceru má podporu aplikačního firewallu ve virtuálních kontextech. |
|  | * Podpora aplikačního firewallu v cloudu | ANO | Navržené zařízení load balanceru má podporu aplikačního firewallu v cloudu, integrovace řešení s F5 Distributed Cloud WAAP řešením. |
|  | * Rozšířená podpora CSHUI – detekce aktivity klávesnice a myši, detekce změn URL od klienta za krátkou dobu | ANO | Navržené zařízení load balanceru má rozšířenou podporu CSHUI – detekce aktivity klávesnice a myši, detekce změn URL od klienta za krátkou dobu a to pomocí modulu aWAF. |
|  | * Ochrana proti Session Highjacking pomocí Browser Fingerprintingu | ANO | Navržené zařízení load balanceru má ochranu proti Session Highjacking pomocí Browser Fingerprintingu a to pomocí modulu aWAF. |
|  | * Detekce a ochrana před DoS útoky na specifické URL, které mohou zatížit back-end systémy (např. vyhledávácí URL apod.) | ANO | Navržené zařízení load balanceru má detekci a ochrana před DoS útoky na specifické URL, které mohou zatížit back-end systémy (např. vyhledávácí URL apod.) a to pomocí modulu aWAF s L7 DoS ochranou. |
|  | * Vynucení přístupu uživatele k chráněné aplikaci přes přihlašovací stránku aplikace | ANO | Navržené zařízení load balanceru má podporu vynucení přístupu uživatele k chráněné aplikaci přes přihlašovací stránku aplikace a to pomocí modulu aWAF funkce Login Enforcement. |
|  | * Podpora nastavení bezpečnostních politik podle IP adresy, doménového jména a URI | ANO | Navržené zařízení load balanceru má podporu nastavení bezpečnostních politik podle IP adresy, doménového jména a URI. |
|  | * Podpora a filtrování WebSocket provozu | ANO | Navržené zařízení load balanceru má podporu filtrování WebSocket provozu a to pomocí modulu aWAF. |
|  | * Blacklistování IP adres, které opakovaně snaží překonat bezpečnostní opatření v politice | ANO | Navržené zařízení load balanceru má podporu Blacklistování IP adres, které opakovaně snaží překonat bezpečnostní opatření v politice a to pomocí modulu aWAF. |
|  | * Ochrana proti Credential Stuffing útokům | ANO | Navržené zařízení load balanceru má podporu ochrany proti Credential Stuffing útokům a to pomocí modulu aWAF. |
|  | * Rozpoznání zdrojů Phishingu, Anonymních Proxy a spojení na Command and Control centra Botnetů | ANO | Navržené zařízení load balanceru má podporu ochrany rozpoznání zdrojů Phishingu, Anonymních Proxy a spojení na Command and Control centra Botnetů. Plná podpora IP Inteligence. |
|  | * Ochrana dat a přihlašovacích údajů proti Man in the Browser útokům | ANO | Navržené zařízení load balanceru má podporu ochrany dat a přihlašovacích údajů proti Man in the Browser útokům a to pomocí modulu aWAF. |
|  | * Ochrana pro DoS/DDoS útokům na aplikační úrovni pomocí průběžné analýzy stresu aplikace, analýzy povahy aplikačního provozu tzv. behaviorální analýzy a vylaďování ochrany aplikace za pomocí uplatňování dynamických signatur | ANO | Navržené zařízení load balanceru má podporu ochrany pro DoS/DDoS útokům na aplikační úrovni pomocí průběžné analýzy stresu aplikace, analýzy povahy aplikačního provozu tzv. behaviorální analýzy a vylaďování ochrany aplikace za pomocí uplatňování dynamických signatur a to pomocí modulu aWAF L7 DoS ochrany. |
|  | * Podpora importu souboru Swagger pro definici security politiky pro ochranu API | ANO | Navržené zařízení load balanceru má podporu importu souboru Swagger pro definici security politiky pro ochranu API a to pomocí modulu aWAF. |
|  | * Podpora využití CI/CD pipeline pro nasazování security politik WAF na webových aplikacích | ANO | Navržené zařízení load balanceru má podporu využití CI/CD pipeline pro nasazování security politik WAF na webových aplikacích a to pomocí modulu aWAF. |
|  | Vlastnosti řízení provozu | * Možnost připojení k monitorovacím nástrojům třetích stran prostřednictvím otevřeného API | ANO | Navržené zařízení load balanceru má možnost připojení k monitorovacím nástrojům třetích stran prostřednictvím otevřeného API. |
|  | * Podpora REST API | ANO | Navržené zařízení load balanceru má podporu REST API. |
|  | * Autentizace klientů přes LDAP/Radius | ANO | Navržené zařízení load balanceru má podporu Autentizace klientů přes LDAP/Radius. |
|  | * Povolení/zakázání ICMP a ARP pro VIP | ANO | Navržené zařízení load balanceru má podporu povolení/zakázání ICMP a ARP pro VIP a to pomocí modulu LTM. |
|  | * Podpora vysokorychlostního granulárního logování / logování per aplikace / bez omezení výkonnosti zařízení | ANO | Navržené zařízení load balanceru má podporu vysokorychlostního granulárního logování / logování per aplikace / bez omezení výkonnosti zařízení a to pomocí modulu LTM. |
|  | * Podpora různých metod rozvažování zátěže | ANO | Navržené zařízení load balanceru má podporu různých metod rozvažování zátěže a to pomocí modulu LTM, podporuje až 19 metod rozvažování zátěže. |
|  | * Podpora filtrace paketů | ANO | Navržené zařízení load balanceru má podporu filtrace paketů. |
|  | * Podpora ToS, QoS (marking/preservation/mimic) | ANO | Navržené zařízení load balanceru má podporu ToS, QoS (marking/preservation/mimic). |
|  | * Podpora rozvažování zátěže založené na poměrech (ratio) s CARP perzistencí | ANO | Navržené zařízení load balanceru má podporu rozvažování zátěže založené na poměrech (ratio) s CARP perzistencí a to pomocí modulu LTM. |
|  | * Podpora SSL certifikátů podepsaných SHA-2 algoritmem | ANO | Navržené zařízení load balanceru má podporu SSL certifikátů podepsaných SHA-2 algoritmem a to pomocí modulu LTM. |
|  | * Podpora práce s 4096-bit klíči | ANO | Navržené zařízení load balanceru má podporu práce s 4096-bit klíči a to pomocí modulu LTM. |
|  | * Současná podpora ECC a RSA certifikátu | ANO | Navržené zařízení load balanceru má současnou podporu ECC a RSA certifikátu a to pomocí modulu LTM. |
|  | * Podpora Camellia šifer SSL | ANO | Navržené zařízení load balanceru má podporu Camellia šifer SSL a to pomocí modulu LTM. |
|  | * Podpora pro TLS (v1.1/v1.2/v1.3) | ANO | Navržené zařízení load balanceru má podporu pro TLS (v1.1/v1.2/v1.3) a to pomocí LTM modulu. |
|  | * Podpora ECC a DH šifer v HW | ANO | Navržené zařízení load balanceru má podporu ECC a DH šifer v HW. |
|  | * Podpora SSL Forward proxy | ANO | Navržené zařízení load balanceru má podporu SSL Forward proxy. |
|  | * Stavové filtrované paketů (ACL) | ANO | Navržené zařízení load balanceru má podporu stavové filtrované paketů (ACL) a to pomocí modulu LTM. |
|  | * Podpora vlastních skriptů pro monitorování zdraví a dostupnosti služeb | ANO | Navržené zařízení load balanceru má podporu vlastních skriptů pro monitorování zdraví a dostupnosti služeb a to pomocí modulu LTM, tzv. Externí monitory. |
|  | * Podpora monitorování služeb na základě výkonu konkrétních hostů | ANO | Navržené zařízení load balanceru má podporu monitorování služeb na základě výkonu konkrétních hostů a to pomocí modulu LTM. |
|  | * TCP optimalizace síťových toků | ANO | Navržené zařízení load balanceru má podporu TCP optimalizace síťových toků a to pomocí modulu LTM. |
|  | * Komprese a cachování specifických služeb | ANO | Navržené zařízení load balanceru má podporu komprese a cachování specifických služeb a to pomocí modulu LTM. |
|  | * Podpora zrcadlení SSL relací a SSL spojení v HA clusteru | ANO | Navržené zařízení load balanceru má podporu zrcadlení SSL relací a SSL spojení v HA clusteru. |
|  | * Podpora optimalizace dynamické velikosti TLS bloků (TLS record size) | ANO | Navržené zařízení load balanceru má podporu optimalizace dynamické velikosti TLS bloků (TLS record size). |
|  | Řízení přístupu k aplikacím | * Podpora autentizace:   + HTTTP basic   + HTML form   + Certificate   + OCSP   + CRLDP   + Radius   + LDAP   + Active Directory   + NTLM v1/v2   + Kerberos   + SAML   + SerurID   + OAM   + Tacacs+   + Local DB | ANO | Navržené zařízení load balanceru má podporu autentizace:   * HTTTP basic * HTML form * Certificate * OCSP * CRLDP * Radius * LDAP * Active Directory * NTLM v1/v2 * Kerberos * SAML * SerurID * OAM * Tacacs+ * Local DB   Plná podpora je pomocí modulu APM pro všechny požadované metody autentizace. |
|  | * Import uživatelských identit IF-MAP | ANO | Navržené zařízení load balanceru má podporu importu uživatelských identit IF-MAP a to pomocí modulu APM. |
|  | * SAML:   + SP role   + IdP role | ANO | Navržené zařízení load balanceru má podporu SAML:   * SP role * IdP role   Plná podpora je pomocí modulu APM. |
|  | * Modifikace SAML atributů | ANO | Navržené zařízení load balanceru má podporu modifikace SAML atributů. Plná podpora je pomocí modulu APM. |
|  | * Podpora SAML 2.0 | ANO | Navržené zařízení load balanceru má podporu SAML 2.0. Plná podpora je pomocí modulu APM. |
|  | * Podpora pro vytvoření Single Sign-On (SSO):   + HTTP basic   + HTML form   + NTLM v1/v2   + Kerberos   + SAML | ANO | Navržené zařízení load balanceru má podporu pro vytvoření Single Sign-On (SSO):   * HTTP basic * HTML form * NTLM v1/v2 * Kerberos * SAML   Plná podpora je pomocí modulu APM pro všechny požadované protokoly. |
|  | * Uchování přihlašovacích údajů v paměti a jejich přeposlání k ověření (User identity credential caching, SSO proxy) | ANO | Navržené zařízení load balanceru má podporu uchování přihlašovacích údajů v paměti a jejich přeposlání k ověření (User identity credential caching, SSO proxy) a to pomocí modulu APM. |
|  | * Podpora federace (SSO napříč různými doménami, např. on-prem a SaaS) | ANO | Navržené zařízení load balanceru má podporu federace (SSO napříč různými doménami, např. on-prem a SaaS) a to pomocí modulu APM. |
|  | * Podpora Kerberos ticketing | ANO | Navržené zařízení load balanceru má podporu Kerberos ticketing a to pomocí modulu APM. |
|  | * PCoIP proxy | ANO | Navržené zařízení load balanceru má podporu PCoIP proxy a to pomocí modulu APM. |
|  | * RDP proxy | ANO | Navržené zařízení load balanceru má podporu RDP proxy a to pomocí modulu APM. |
|  | * Patching (maskování) webových portálů:   + HTML   + JavaScript   + CSS   + Java | ANO | Navržené zařízení load balanceru má podporu Patching (maskování) webových portálů:   * HTML * JavaScript * CSS * Java   Plná podpora je pomocí modulu APM pro všechny zmíněné technologie. |
|  | * Podpora L7 ACL | ANO | Navržené zařízení load balanceru má podporu L7 ACL a to pomocí modulu APM. |
|  | * Podpora zabezpečení vzdálené pracovní plochy vzdáleného uživatele | ANO | Navržené zařízení load balanceru má podporu zabezpečení vzdálené pracovní plochy vzdáleného uživatele a to pomocí modulu APM. |
|  | * Síťová SSL VPN DTLS | ANO | Navržené zařízení load balanceru má podporu SSL VPN DTLS a to pomocí modulu APM. |
|  | * Podpora minimálně 500 souběžných SSL VPN spojení | ANO | Navržené zařízení load balanceru má podporu 500 souběžných SSL VPN spojení. |
|  | * Podpora vzdáleného přístupu k aplikacím bez nutnosti použití tlustého klienta | ANO | Navržené zařízení load balanceru má podporu vzdáleného přístupu k aplikacím bez nutnosti použití tlustého klienta a to pomocí modulu APM. |
|  | * Podpora OS:   + Windows   + MAC   + Linux   + iOS   + Android | ANO | Navržené zařízení load balanceru má podporu OS:   * Windows * MAC * Linux * iOS * Android. |
|  | * Nativní podpora MDM | ANO | Navržené zařízení load balanceru má podporu MDM a to pomocí modulu APM. |
|  | * Kontrola minimálně nastavení zabezpečení koncových bodů (klientů), validace politik, detekce AV a verze, certifikátů | ANO | Navržené zařízení load balanceru má podporu kontrol nastavení zabezpečení koncových bodů (klientů), validace politik, detekce AV a verze, certifikátů a to pomocí modulu APM. |
|  | * Filtrování URL | ANO | Navržené zařízení load balanceru má podporu filtrování URL a to pomocí modulu APM. |
|  | * URL kategorizační databáze | ANO | Navržené zařízení load balanceru má podporu URL kategorizační databáze a to pomocí modulu APM. |
|  | * Podpora pro vytváření flexibilní a granulární přístupové politiky | ANO | Navržené zařízení load balanceru má podporu vytváření flexibilní a granulární přístupové politiky a to pomocí modulu APM. |
|  | * GUI pro vizuální nastavení přístupových bezpečnostních politik a logiky autentizace | ANO | Navržené zařízení load balanceru má podporu GUI pro vizuální nastavení přístupových bezpečnostních politik a logiky autentizace a to pomocí modulu APM. |
|  | DNS | * Podpora pro inspekci a filtrování DNS dotazů, ochrana před DNS DoS útoky | ANO | Navržené zařízení load balanceru má podporu pro inspekci a filtrování DNS dotazů, ochrana před DNS DoS útoky a to pomocí DNS modulu. |
|  | * Kontrola a validace DNS protokolu (normalizace) | ANO | Navržené zařízení load balanceru má podporu pro kontrolu a validace DNS protokolu (normalizace) a to pomocí DNS modulu. |
|  | * Podpora filtrování typů DNS dotazů | ANO | Navržené zařízení load balanceru má podporu filtrování typů DNS dotazů a to pomocí DNS modulu. |
|  | * Load balancing DNS provozu | ANO | Navržené zařízení load balanceru má podporu Load balancing DNS provozu a to pomocí DNS modulu. |
|  | * Podpora podpisování pomocí DNSSEC | ANO | Navržené zařízení load balanceru má podporu podpisování pomocí DNSSEC a to pomocí DNS modulu. |
|  | * Centralizované řízení a správa klíčů pro DNSSEC | ANO | Navržené zařízení load balanceru má podporu centralizované řízení a správa klíčů pro DNSSEC a to pomocí DNS modulu. |
|  | * Podpora domén nejvyššího řádu pro DNSSEC | ANO | Navržené zařízení load balanceru má podporu domén nejvyššího řádu pro DNSSEC a to pomocí DNS modulu. |
|  | * Validace DNSSEC | ANO | Navržené zařízení load balanceru má podporu validace DNSSEC a to pomocí DNS modulu. |
|  | * Mitigace DNS DDoS | ANO | Navržené zařízení load balanceru má podporu mitigace DNS DDoS a to pomocí DNS modulu. |
|  | * Potlačení přístupu k DNS doménám se špatnou reputací (domény obsahující viry, malware, phishing apod.) | ANO | Navržené zařízení load balanceru má podporu potlačení přístupu k DNS doménám se špatnou reputací (domény obsahující viry, malware, phishing apod.) a to pomocí DNS modulu. |
|  | * Zabezpečený DNS data-plane před kybernetickými útoky | ANO | Navržené zařízení load balanceru má podporu zabezpečený DNS data-plane před kybernetickými útoky a to pomocí DNS modulu. |
|  | Síťový Firewall | * Inspekce SSL relací | ANO | Navržené zařízení load balanceru má podporu inspekce SSL relací a to pomocí modulu AFM. |
|  | * Detekce a ochrana před síťovými DDoS útoky | ANO | Navržené zařízení load balanceru má podporu detekce a ochrana před síťovými DDoS útoky a to pomocí modulu AFM. |
|  | * Detekce protokolových anomálií | ANO | Navržené zařízení load balanceru má podporu detekce protokolových anomálií a to pomocí modulu AFM. |
|  | * Podpora síťových, SIP, DNS a HTTP DoS vektorů | ANO | Navržené zařízení load balanceru má podporu síťových, SIP, DNS a HTTP DoS vektorů a to pomocí modulu AFM. |
|  | * Hardwarová podpora DoS vektorů | ANO | Navržené zařízení load balanceru má hardwarovou podporu DoS vektorů a to pomocí modulu AFM. |
|  | * Podpora tvorby bezpečnostních pravidel s filtrováním IP adres se špatnou pověstí nebo přistupujících z konkrétních geografických regionů | ANO | Navržené zařízení load balanceru má podporu tvorby bezpečnostních pravidel s filtrováním IP adres se špatnou pověstí nebo přistupujících z konkrétních geografických regionů a to pomocí modulu AFM. |
|  | * Podpora pro dynamických blacklistování IP adres a jejich reporting | ANO | Navržené zařízení load balanceru má podporu pro dynamických blacklistování IP adres a jejich reporting a to pomocí modulu AFM. |
|  | * Podpora RTBH (Remote Trigger Black Hole Filtering) | ANO | Navržené zařízení load balanceru má podporu RTBH (Remote Trigger Black Hole Filtering) a to pomocí modulu AFM. |
|  | * Podpora pro ochranu SSH Proxy serverů | ANO | Navržené zařízení load balanceru má podporu pro ochranu SSH Proxy serverů a to pomocí modulu AFM. |
|  | * Detekce a ochrana proti zneužití nebo využití jiných TCP portů než běžných | ANO | Navržené zařízení load balanceru má podporu detekce a ochrany proti zneužití nebo využití jiných TCP portů než běžných a to pomocí modulu AFM. |
|  | * Napojení na globální databázi škodlivých IP adres s automatickým obnovováním a možnost jejich blokování | ANO | Navržené zařízení load balanceru má podporu napojení na globální databázi škodlivých IP adres s automatickým obnovováním a možnost jejich blokování a to pomocí licence IP Inteligence, která je součástí řešení. |
|  | Záruka | * Podpora řešení a aktualizace po dobu 6 let, 24x7, oprava do 24h | ANO | Navržené řešení obsahuje záruku s podporou řešení a aktualizace po dobu 6 let, 24x7, oprava do 24h. |
| * Komunikace výhradně v českém jazyce | ANO | Navržené řešení obsahuje záruku s komunikací výhradně v českém jazyce. |
| * Záruku garantuje přímo výrobce zařízení | ANO | Navržené řešení obsahuje záruku, kterou garantuje přímo výrobce dodávaných zařízení. |

Tabulka - Technické parametry pro LB

### Management LAN

Management celého řešení se dělí na následující části:

* Management DC Fabric;
* Management přistup na síťové elementy;

#### Management DC Fabric

Objednatel požaduje vytvoření DC Fabric založeného na EVPN-VXLAN konceptu včetně systému pro jeho profesionální management. Tento management systém musí poskytovat všechny potřebné funkce k řízení v prostředí grafického uživatelského rozhraní (GUI) a musí podporovat celý životní cyklus DC Fabricu. Tedy podporovat fáze: Návrh, Plánování, Nasazení, Provisioning a Provoz.

Musí tedy podporovat:

* Instalaci ve virtuálním prostředí – VMware, KVM;
* GUI rozhraní pro přístup uživatele přes standartní web prohlížeče včetně šifrovaní;
* Lokální a vzdálená (Radius) authentikace uživatele;
* Možnost definovat role uživatelů dle oprávnění (RBAC model);
* Interaktivní rozhraní pro fázi Návrh/Plánování;
  + ECMP underlay;
  + BGP EVPN overlay
* Interaktivní rozhraní pro fázi Deploy/Provision;
  + Provisioning L2/L3 služeb na EVPN-VXLAN;
* Rozhraní pro fázi Provozu;
  + Rozšíření, změny a monitoring všech síťových elementů a sítě;
* Možnost automatizovaného zálohování a upgrade síťových elementu a dalších provozních aktivit;
* Podpora management API pro hromadné nasazování a řízení služeb (Mass-provisioning);

|  |  |  |  |
| --- | --- | --- | --- |
| **SW pro MGMT DC Fabric** | | | |
| **Číslo** | **Název komponenty** | **Part number** | **Počet kusů** |
| 1 | APSTRA ADVANCED LICENSE | XXXXX | 20 |

Tabulka - Identifikace komponenty MGMT DC Fabric

Zejména musí poskytovat tyto klíčové vlastnosti:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **SW pro MGMT DC Fabric** | | | | |
| **Číslo** | **Vlastnost/**  **komponenta** | **Požadované parametry** | **Splňuje ANO/NE** | **Skutečné parametry/Způsob splnění požadavku** |
|  | Kompatibilita | * Nástroj musí být kompatibilní s nabídnutými síťovými elementy | ANO | Nabízený MNGT nástroj je plně kompatibilní se síťovými elementy DC Fabric a DCI konektivity. |
|  | Vlastnosti a funkcionality | * Intent-based networking – inteligentní konfigurace a orchestrace sítě | ANO | Plná podpora Intent-based networkingu – inteligentní konfigurace a orchestrace sítě.  Pro výstavbu a konfigurace sítě není potřeba znát specifické parametry síťových prvků, postačí znát záměr, který APSTRA MNGT systém zpracuje do konkrétního návrhu na konkrétním výrobci. |
|  | * Inteligentní řízení životního cyklu nabízených síťových elementů | ANO | Plná podpora životního cyklu.  Jsou dostupné všechny části „lifecycle“:  Design, Plan, Deploy, Operate. |
|  | * Správa skrze GUI dostupný přes standartní webové prohlížeče | ANO | Plná podpora.  Standardní web prohlížeče jsou podporovány pro správu skrze GUI. |
|  | * GUI musí podporovat šifrovaný přístup - min. TLS 1.2 a TLS 1.3 | ANO | Plná podpora.  Apstra GUI a API používá HTTPS on Nginx. SSL protokoly TLS 1.0 / 1.1 / 1.2 /1.3 jsou podporovány. |
|  | * Možnost definovat role admin/uživatel dle oprávnění (RBAC model); | ANO | Plná podpora možnosti definovat role admin/uživatel dle oprávnění (RBAC model).  Je možné vytvořit uživatele a přiřadit předefinované role.  Je možné definovat vlastní role s přístupy do konkrétního „blueprint“ nebo všech „blueprint“ a povolením přístupu do definovaných částí APSTRA CUI. |
|  | * Lokální a vzdálená (RADIUS nebo TACACS+ server) authentikace uživatele | ANO | Plná podpora lokální authentikace i LDAP / TACACS+ / RADIUS. |
|  | * Podpora a dostupnost REST API | ANO | Rest API Explorer plně podporován. |
|  | * Instalace jako VM   + Podpora min. VMware, Linux KVM Hypervisor   + Podpora integrace s NSX-T | ANO | Plná podpora instalace na VMware, Linux KVM Hypervisor, Hyper-V, VirtualBox.  Integrace s Vcentre a NSX-T je podporována. |
|  | * Dodavatel popíše všechny požadavky na potřebné systémové zdroje pro požadovanou architekturu (Metrocluster) a management všech síťových elementů – min. požadavky pro VM, jejich počet pro plnou správu a monitoring DC Fabric |  | Obecně platí, že jeden VM je schopný obsloužit až 25 offbox agentů. V tomto případě celkový počet switchů nepřesahuje toto číslo.  Doporučené zdroje pro VM:  Memory 64 GB RAM + 500 MB pro každého klienta  CPU 8 vCPU  Disk 160 GB  Síťový adapter s nakonfigurovaným DHCP |
|  | * Podpora „Design Tepmplates“ - min. 3-stage clos/5-stage clos/MultiPoP/MultiPoD | ANO | Plná podpora „Design Tepmplates“ - min. 3-stage clos/5-stage clos/MultiPoP/MultiPoD.  Kromě uvedených plně podporovaných Templates je možné ještě využít tzv. Freeform blueprint. |
|  | * Podpora Overlay:   + Podpora static VXLAN   + Podpora MP-BGP EVPN-VXLAN   + Podpora symetrického (Edge) routingu = L3/L2 VTEP na Edge switch   + Podpora asymetrického (Centralize) routingu = L2/L3 VTEP na SPINE switchi | ANO | Plná podpora Overlay:   * static VXLAN * MP-BGP EVPN-VXLAN * symetrického (Edge) routingu = L3/L2 VTEP na Edge switch * asymetrického (Centralize) routingu = L2/L3 VTEP na SPINE switchi. |
|  | * Podpora Multi-Tenantnosti   + Podpora VRF – oddělení tabulek pro routing a forwarding | ANO | Plná podpora Multi-Tenantnosti   * Podpora VRF – oddělení tabulek pro routing a forwarding   V APSTRA SW tzv. Routing Zones. |
|  | * Podpora definice zdrojů (Pool)   + Min. definice zdrojů pollů pro IP, IPv6, AS numbers a VNI | ANO | Plná podpora definice zdrojů (Pool) v rozsahu definice zdrojů pollů pro IP, IPv6, AS numbers a VNI.  APSTRA SW má defaultně definované pooly zdrojů, ale je možné definovat a následně použít vlastní zdroje a to pro všechny požadované proměnné. |
|  | * Podpora RACK type Templates   + Single homing, dual-homing: MC-LAG/ESI-LAG | ANO | Plná podpora RACK type Templates v rozsahu - Single homing, dual-homing: MC-LAG/ESI-LAG.  APSTRA management systém má předefinované Rack typy.  Je možné vytvořit vlastní Rack type. |
|  | * Podpora tzv. “logických devices“   + Možnost obecné definice switchů DC fabric nezávisle na výrobci   + Možnost definice typů interface / přiřazení interface   + Možnost výběru a přiřazení konkrétního HW konkrétního výrobce | ANO | Plná podpora tzv. “logických devices“ vrozsahu   * Možnost obecné definice switchů DC fabric nezávisle na výrobci * Možnost definice typů interface / přiřazení interface * Možnost výběru a přiřazení konkrétního HW konkrétního výrobce   Toto je nativní chování APSTRA management systému, který „intend“ based. Návrh DC tedy může být vendor nezávislý = není nutná znalost HW jednotlivých vendorů, postačí mít pouze „záměr/cíl“. |
|  | * Podpora vytvoření celkového DC schématu tzv. blue-print | ANO | Plná podpora vytvoření celkového DC schématu tzv. blue-print.  Řešení využívá advanced licenci, která umožňuje až 3x blueprint. |
|  | * Podpora tzv. „Devices onboarding“   + Manualně a ZTP (Zero Touch Provisioning) | ANO | Plná podpora tzv. „Devices onboarding“ v rozsahu Manualně a ZTP (Zero Touch Provisioning). |
|  | * Manuálně a ZTP (Zero Touch Provisioning)   + DHCP   + Device discovetry   + Admin root password   + Upgrade OS   + Device Connectivity | ANO | Požadavky na manuálně a ZTP (Zero Touch Provisoning) pro oblasti DHCP, Device discovetry, Admin root password, Upgrade OS, Device Connectivity“ jsou plně podporovány. |
|  | * Podpora Fabric Expansion – Links, Leaves, Racks | ANO | Plná podpora Fabric Expansion – Links, Leaves, Racks.  Prováděno konkrétním blueprintem. |
|  | * Podpora Adding New Servers – Single/Dual homed | ANO | Plná podpora Adding New Servers – Single/Dual homed.  Prováděno konkrétním blueprintem. |
|  | * Podpora změny typu a speed UNI linek | ANO | Plná podpora změny typu a speed UNI linek.  Prováděno konkrétním blueprintem. |
|  | * Podpora provisioning a management L2/L3 virtuálních sítí | ANO | Plná podpora provisioning a management L2/L3 virtuálních sítí. |
|  | * Podpora DC Fabric rollback | ANO | Plná podpora DC Fabric rollback. |
|  | * Device maintanance, upgrade | ANO | Plná podpora Device maintanance, upgrade.  APSTRA management system a provádí upgrade síťových prvků spravovaných APSTRA management systémem. |
|  | * Conectivity templates – Mass-provisioning | ANO | Plná podpora Conectivity templates – Mass-provisioning. |
|  | * Dostupnost Dashbordu v GUI s náhledem stavů min.:   + Fabric/Rack/Linky   + Topologie/Heatmapy   + Stav služeb L2/L3   + Status sítě/síťových elementů   + Detekce anomálií   + Intent Based Analytics (IBA) | ANO | Plná podpora dostupnosti Dashbordu v GUI s náhledem stavů:   * Fabric/Rack/Linky * Topologie/Heatmapy * Stav služeb L2/L3 * Status sítě/síťových elementů * Detekce anomálií * Intent Based Analytics (IBA). |
|  | Záruka | * Podpora řešení a aktualizace po dobu 6 let | ANO | Nabízený SW má podporu řešení a aktualizace po dobu 6 let. |
| * Komunikace výhradně v českém jazyce | ANO | Technický tým dodavatele má nativně mluvící techniky v českém jazyce. |
| * Záruku garantuje přímo výrobce zařízení | ANO | Navržené řešení obsahuje záruku, kterou garantuje přímo výrobce. |

Tabulka - Technické parametry SW pro MGMT DC Fabric

#### Management přístup na síťové elementy

Pro management přístupu na jednotlivé síťové elementy se budou používat tyto principy:

* Out-of-Band přístup: jedná se o vzdálený SSH/Telnet přístup přes dedikovanou mgmt síť, ke které jsou všechny síťové elementy připojené přes dedikované Out-of-Band porty. Tento způsob přístupu je Objednatelem požadován a preferován.
* In-Band přístup: jedná se o vzdálený SSH/Telnet přístup přes datové propoje. Objednatel předpokládá tento přístup za nativní.
* Přístup pomocí konzole: jedná se o lokální non-IP přístup realizovaný přes konzolový port daného síťového elementu, který umožňuje kontrolovat síťové elementy ve všech provozních fázích včetně boot-procesu, kdy ještě není připravena IP konektivita pro In-Band či Out-of-Band přístup. Tento lokální přístup lze realizovat také ve variantě vzdáleného přístupu pomocí tzv. Terminál (Console) serverů. Takový IP přístup na non-IP port patří také k Out-of-Band managementu.

Dodavatel dodá pro zajištění dostatečného mgmt přístupu do sítě dostatečně dimenzované síťové elementy pro funkci Out-of-Band switche. Jejich počet v každé z lokací řešení je 2ks, tj. celkově požadováno dodat 4ks.

Každý OoB switch je:

* min. 48x 10/100/1000BaseT portů (porty pro OoB portů Network Elementů a MNGT protů výpočetních zařízení);
* min. 2x 10GE NNI porty (pro připojení do MNGT sítě);
  + vybavené originálními 10GBASE-SR SFP+ transceivery;
* podpora stacku minimálně ze čtyřech switchů o výkonu min. 40Gbps;
* podpora L2;
* podpora L3 static routing;

|  |  |  |  |
| --- | --- | --- | --- |
| **Out-of-Band MGMT switch** | | | |
| **Číslo** | **Název komponenty** | **Part number** | **Počet kusů** |
| 1 | OoB MNGT SWITCH | XXXXX | 4 |

Tabulka - Identifikace komponenty Out-of-Band MGMT switch

Zejména musí poskytovat tyto klíčové vlastnosti:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Out-of-Band MGMT switch – min. 4ks** | | | | |
| **Číslo** | **Vlastnost/**  **komponenta** | **Požadované parametry** | **Splňuje ANO/NE** | **Skutečné parametry/Způsob splnění požadavku** |
|  | Kompatibilita | * Zařízení musí být kompatibilní s všemi nabízenými prvky a zajišťovat všechny potřebné funkcionality v rámci celého řešení | ANO | Nabízené zařízení je kompatibilní se všemi nabízenými prvky a zajišťuje všechny potřebné funkcionality v rámci celého řešení. |
|  | Technické vlastnosti a rozměry | * Kompatibilní s RACK 19” | ANO | Navržené zařízení je kompatibilní s RACK 19”. |
|  | * Dodavatel uvede velikost v EIA (jednotek U) pro systémovou skříň 19”. |  | Rozměry 1U zařízení (š x v x h): 44,17 x 4,37 x 43 cm. |
|  | * Dodavatel uvede počet a typ napájení (C13/14 nebo C19/C20 a počet). |  | Při požadované redundanci napájecích zdrojů – 2x C13. |
|  | * Dodavatel uvede hmotnost a typický a maximální elektrický příkon. |  | Hmotnost: 8,11 kg  Typický příkon: 125 W  Maximální příkon: 198 W. |
|  | * Dodavatel uvede, jaké jsou požadavky na elektrické jištění. |  | I při maximální spotřebě switche je proudový příkon tak nízký, že je potřeba se řídit při návrhu jističe spíše průměrem přívodního kabelu. Obvykle se aplikuje 10A jistič na každou napájecí větev. Přičemž přívody by měly být připojeny na dvě dedikované napájecí větve. |
|  | Napájení a chlazení | * Zařízení musí mít redundantní napájecí zdroje 250VAC, vyměnitelné za chodu. | ANO | Nabízené zařízení má redundantní napájecí zdroje 250VAC, vyměnitelné za chodu. |
|  | * Aktivní chlazení Front-to-Rear. | ANO | Nabízené zařízení má aktivní chlazení Front-to-Rear. |
|  | Propojovací kabely | * Odpovídající počet propojovacích kabelů pro plné zprovoznění systému | ANO | Nabízené řešení má odpovídající počet propojovacích kabelů pro plné zprovoznění systému. |
|  | Konektivita | * Minimálně 48ks 10/100/1000BaseT portů   + Dodavatel dodá plně dostatečný počet portů pro OoB switchi na propojení jednotlivých síťových elementů a mgmt portů specifikovaných výpočetních zařízení, a to včetně dostatečné rezervy vzhledem k ŽC 6let) | ANO | Nabízené zařízení má 48 ks 10/100/1000BaseT port.  Nabízené zařízení má dostatečný počet portů pro OoB switchi na propojení jednotlivých síťových elementů a mgmt portů specifikovaných výpočetních zařízení, a to včetně dostatečné rezervy vzhledem k ŽC 6let). |
|  | * Minimálně 2ks 10GE SFP+ (pro připojení do mgmt sítě) | ANO | Nabízené řešení obsahuje 4x 1/10GE SFP/SFP+ na uplink module. |
|  | Management | * Rozhraní RJ45 pro mgmt OoB switche | ANO | Nabízené zařízení plně podporuje rozhraní RJ45 pro mgmt OoB switche.  Switch je vybavený console porty ve formátu 1x RJ45 a 1x USB-C. |
|  | Konzolový port | * Provedení RJ45 nebo USB (pozn. u USB i převodníky USB/RS-232(RJ45)) | ANO | Nabízené zařízení má provedení RJ45 a USB (pozn. u USB i převodníky USB/RS-232(RJ45)). |
|  | Vlastnosti a funkcionality | * Podpora Jumbo Frames min. 9kB | ANO | Nabízené zařízení má podporu jumbo Frames min. 9,216 kB. |
|  | * Podpora vytvoření tzv. subinterface s individuální konfigurací parametrů: VLAN-id, encapsulation, apod. | ANO | Nabízené řešení má podporu vytvoření tzv. subinterface s individuální konfigurací parametrů: VLAN-id, encapsulation, apod.. |
|  | * Podpora na úrovni L2:   + IEEE 802.3 bridging   + min. MAC tabule size = 10k   + LAG/LACP pro jakýkoliv typ interface   + LAG group = min. 64   + počet int. na LAG group = min. 8   + podpora VLAN (IEEE 802.1Q)   + plný roszah VLAN = min. 4k   + QinQ   + port based VLAN   + VLAN translation (VLAN header swap)   + xSTP (IEEE 802.1D (STP), IEEE 802.1s (MSTP), IEEE 802.1w (RSTP))   + STP security funkce min. BPDU guard, Loop guard, Root guard   + LLDP (802.1ab) | ANO | Nabízené zařízení má podporu na úrovni L2:   * IEEE 802.3 bridging – plná podpora * Velikost MAC tabulky = 112k * LAG/LACP pro jakýkoliv typ interface – podporovány všechny interface * LAG group = 128 * počet int. na LAG group = 16 * podpora VLAN (IEEE 802.1Q) - plná podpora * plný roszah VLAN = 4,093k * QinQ – plná podpora * port based VLAN – plná podpora * VLAN translation (VLAN header swap) – plná podpora * xSTP (IEEE 802.1D (STP), IEEE 802.1s (MSTP), IEEE 802.1w (RSTP)) – plná podpora * STP security funkce BPDU guard, Loop guard, Root guard – plná podpora * Plná podpora LLDP (802.1ab) |
|  | * Podpora ACL:   + Port ACLs (ingress / egress)   + VLAN ACLs (ingress / egress)   + ACL ve vrstvách L2-L4   + ACL ackce (ermit / deny, count)   + ACL směrem na CPU (CPU protection) | ANO | Nabízené zařízení má podporu ACL:   * Port ACLs (ingress / egress) * VLAN ACLs (ingress / egress) * ACL ve vrstvách L2-L4 * ACL ackce (ermit / deny, count) * ACL směrem na CPU (CPU protection). |
|  | * Podpora na úrovni L3:   + RVI (Routovaný VLAN interface)   + min. IP FIB = 2k   + Static routing (IPv4/IPv6)   + Podpora ospf / ospfv3   + ECMP balancing / resilient hashing - min. 64 ECMP cest | ANO | Nabízené zařízení má podporu má úrovni L3:   * RVI (Routovaný VLAN interface) – plná podpora * IP FIB = 8k * Plná podpora static routingu (IPv4/IPv6) * Podpora ospf / ospfv3 – plná podpora * ECMP balancing / resilient hashing - 64 ECMP cest. |
|  | * Podpora Multicast:   + IGMP snooping v1/2/3   + MLD snooping v1/2 | ANO | Nabízené zařízení plně podporuje podporu Multicast:   * IGMP snooping v1/2/3 * MLD snooping v1/2. |
|  | Management a Troubleshooting | * Řešení musí být kompatibilní se všemi nabízenými síťovými elementy:   + LEAF / SPINE / Border LEAF / EDGE / WAN\_router / OoB\_MNGT | ANO | Nabízené řešení je kompatibilní se všemi nabízenými síťovými elementy LEAF / SPINE / Border LEAF / EDGE / WAN\_router / OoB\_MNGT. |
|  | * CLI inteface: plná konfigurovatelnost a troubleshooting:   + Local   + Telnet   + SSH | ANO | Nabízené zařízení plně podporuje CLI inteface, který je plně konfigurovatelný a lze provádět troubleshooting na úrovni:   * Local * Telnet * SSH. |
|  | * Authentikace uživatele:   + Local   + Radius, TACAC+   + RBAC | ANO | Nabízené zařízení plně podporuje authentikaci uživatele:   * Local * Radius, TACAC+ * RBAC   RBAC až na úroveň povolení/zákazu i té nejnižší vrstvy hierarchické CLI a až po jednotlivé operační příkazy. |
|  | * Konfigurační změny automaticky přes .txt file | ANO | Nabízené zařízení umožňuje konfigurační změny automaticky přes .txt file. |
|  | * Podpora syslog server   + Local   + Remote syslog server | ANO | Nabízené zařízení podporuje syslog server local (lokální) i Remote syslog server (vzdálený). |
|  | * Ping, Traceroute | ANO | Nabízené zařízení plně podporuje ping, traceroute i s dalšími možnostmi pro definici. |
|  | * sFlow a/nebo jiná adekvátní technologie | ANO | Nabízené řešení plně podporuje sFLOW i IPFIX (Telemetrie). |
|  | * Traffic mirroring | ANO | Nabízené řešení plně podporuje traffic mirroring, lokální i vzdálený. |
|  | * SNMP v2/v3 | ANO | Nabízené řešení plně podporuje SNMP v2/v3. |
|  | Záruka | * Podpora řešení a aktualizace po dobu 6 let, 24x7, oprava do 24h | ANO | Nabízené zařízení má plnou podporu řešení a aktualizace po dobu 6 let, 24x7, oprava do 24h. |
| * Komunikace výhradně v českém jazyce | ANO | Technický tým dodavatele má nativně mluvící techniky v českém jazyce. |
| * Záruku garantuje přímo výrobce zařízení | ANO | Záruku garantuje přímo výrobce zařízení. |

Tabulka - Technické parametry Out-of-Band MGMT switch

Dodavatel dodá pro zajištění dostatečného mgmt přístupu do sítě dostatečně dimenzované síťové elementy pro funkci Terminál (Console) Server. Jejich počet v každé z lokací řešení je 1ks, tj. celkově požadováno dodat 2ks.

Každý Terminál Server je:

* Min. 16x RJ45 RS-232 portů;
* Min. 2x 10/100/1000 BaseT network porty;
* Konfigurovatelnost sériových portů minimálně na úrovni „Baud Rate, Data bits, Parity, Stop bits, Flow Control;
* Možnost přímého připojení SSH na konkrétní konzolový port;
* Zabudovaný web terminal;
* Podpora násobných paralelních relaci;
* Authentikace uživatele;
* Podpora L3 static routing;
* Vestavěný FW, IPsec VPN, SSL VPN;

|  |  |  |  |
| --- | --- | --- | --- |
| **Terminal Server** | | | |
| **Číslo** | **Název komponenty** | **Part number** | **Počet kusů** |
| 1 | Terminal server | XXXXX | 2 |

Tabulka - Identifikace komponenty Terminal Server

Zejména musí poskytovat tyto klíčové vlastnosti:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Terminal Server – min. 2ks** | | | | |
| **Číslo** | **Vlastnost/**  **komponenta** | **Požadované parametry** | **Splňuje ANO/NE** | **Skutečné parametry/Způsob splnění požadavku** |
|  | Kompatibilita | * Zařízení musí být kompatibilní s všemi nabízenými prvky a zajišťovat všechny potřebné funkcionality v rámci celého řešení | ANO | Nabízené zařízení je plně kompatibilní se všemi nabízenými prvky. |
|  | Technické vlastnosti a rozměry | * Kompatibilní s RACK 19” | ANO | Navržené zařízení je kompatibilní s RACK 19”. |
|  | * Dodavatel uvede velikost v EIA (jednotek U) pro systémovou skříň 19”. |  | Rozměry 1U zařízení (h x š x v):  25,5 x 44,5 x 4,45 cm. |
|  | * Dodavatel uvede počet a typ napájení (C13/14 nebo C19/C20 a počet). |  | Navržené zařízení má typ napájení C13/14, celkem 2 kusy na zařízení. |
|  | * Dodavatel uvede hmotnost a typický a maximální elektrický příkon. |  | Hmotnost: 5,26 kg  Typický příkon: 100 W  Maximální příkon: 376 W. |
|  | * Dodavatel uvede, jaké jsou požadavky na elektrické jištění. |  | Obvykle se aplikuje 10A jistič na každou napájecí větev. Přičemž přívody by měly být připojeny na dvě dedikované napájecí větve. |
|  | Napájení a chlazení | * Zařízení musí mít redundantní napájecí zdroje 250VAC, vyměnitelné za chodu. | ANO | Nabízené zařízení má redundantní napájecí zdroje 250VAC, vyměnitelné za chodu. |
|  | * Aktivní chlazení. | ANO | Nabízené zařízení má aktivní chlazení. |
|  | Propojovací kabely | * Odpovídající počet propojovacích kabelů pro plné zprovoznění systému | ANO | Nabízené řešení má odpovídající počet propojovacích kabelů pro plné zprovoznění systému. |
|  | Konektivita | * Min. 16ks RJ45 RS-232 portů   + Dodavatel dodá plně dostatečný počet portů pro Terminal Server na propojení jednotlivých síťových elementů a mgmt portů specifikovaných výpočetních zařízení, a to včetně dostatečné rezervy vzhledem k ŽC 6let) | ANO | Nabízené zařízení má 32x RJ45 RS-232 port  Nabízené zařízení má dostatečný počet portů pro Terminal server na propojení jednotlivých síťových elementů a mgmt portů specifikovaných výpočetních zařízení, a to včetně dostatečné rezervy vzhledem k ŽC 6let). |
|  | * Min. 2ks 10/100/1000BaseT síťové porty | ANO | Nabízené zařízení má 2x 10/100/1000BaseT .  Navíc 2x SFP+. |
|  | Vlastnosti a funkcionality | * Zabudovaný web terminál dostupný přes standardní webové prohlížeče | ANO | Nabízené zařízení má zabudovaný web terminal dostupný přes standardní webové prohlížeče.  Plně podporováno.  WEB UI dostupné přes standardní webové prohlížeče, CLI UI. |
|  | * Podpora násobných paralelních relaci | ANO | Nabízené zařízení má plnou podporu násobných paralelních relaci. |
|  | * Authentikace uživatele:   + Local   + Radius, TACAC+   + RBAC | ANO | Nabízené zařízení plně podporuje authentikaci uživatele:   * Local * Radius, TACAC+ * RBAC. |
|  | * Lokální logování aktivit v systému, přístupových a komunikačních případů na seriál i stíťových portech | ANO | Nabízené zařízení plně podporuje lokální logování aktivit v systému, přístupových a komunikačních případů na seriál i síťových portech.  Micro SD pro loging. |
|  | * Podpora Static a DHCP IPv4 a IPv6 na síťových portech | ANO | Nabízené zařízení plně podporuje static a DHCP IPv4 a IPv6 na síťových portech. |
|  | * Statický routing | ANO | Nabízené zařízení plně podporuje statický routing RP, OSPF, BGP. |
|  | * Možnost konfigurace sériových portů minimálně na úrovni „Baud Rate, Data bits, Parity, Stop bits“ | ANO | Nabízené zařízení je možné konfigurace sériových portů na úrovni „Baud Rate, Data bits, Parity, Stop bits. |
|  | * Možnost přímého připojení SSH na konkrétní konzolový port | ANO | Nabízené zařízení plně podporuje možnost přímého připojení SSH na konkrétní konzolový port. |
|  | * Vestavěný Firewall / IPsec VPN / SSL VPN | ANO | Nabízené zařízení plně podporuje vestavěný Firewall / IPsec VPN / SSL VPN. |
|  | Záruka | * Podpora řešení a aktualizace po dobu 6 let, 24x7, oprava do 24h | ANO | Nabízené zařízení má podporu řešení a aktualizace po dobu 6 let, 24x7, oprava do 24h. |
| * Komunikace výhradně v českém jazyce | ANO | Komunikace s podporou je výhradně v českém jazyce. |
| * Záruku garantuje přímo výrobce zařízení. | ANO | Záruka je garantována výrobcem zařízení. |

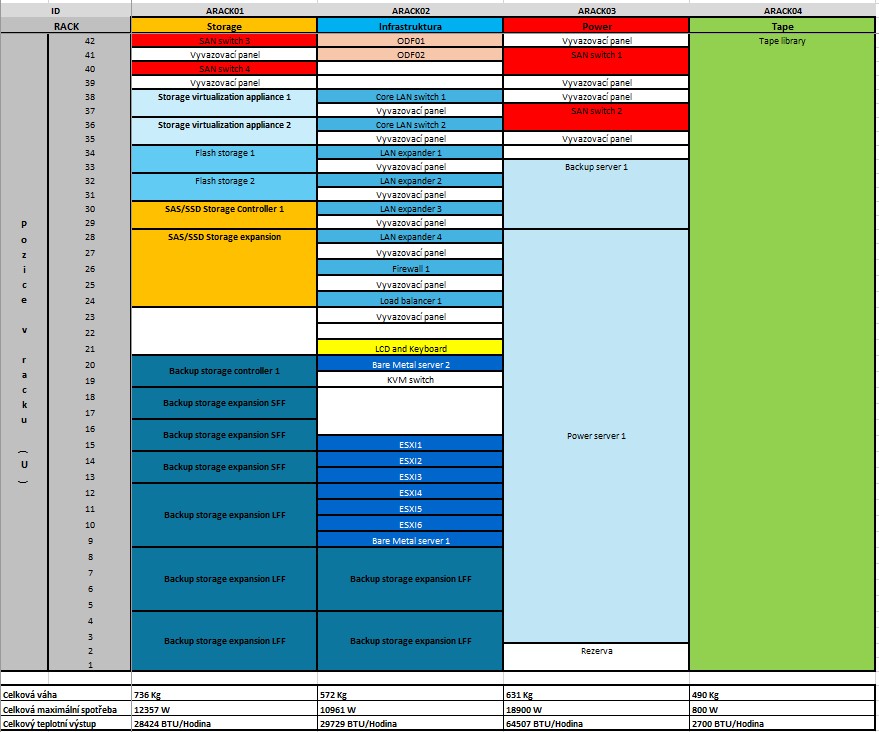
Tabulka - Technické parametry Terminal Serveru

## Systémové skříně (Rack)

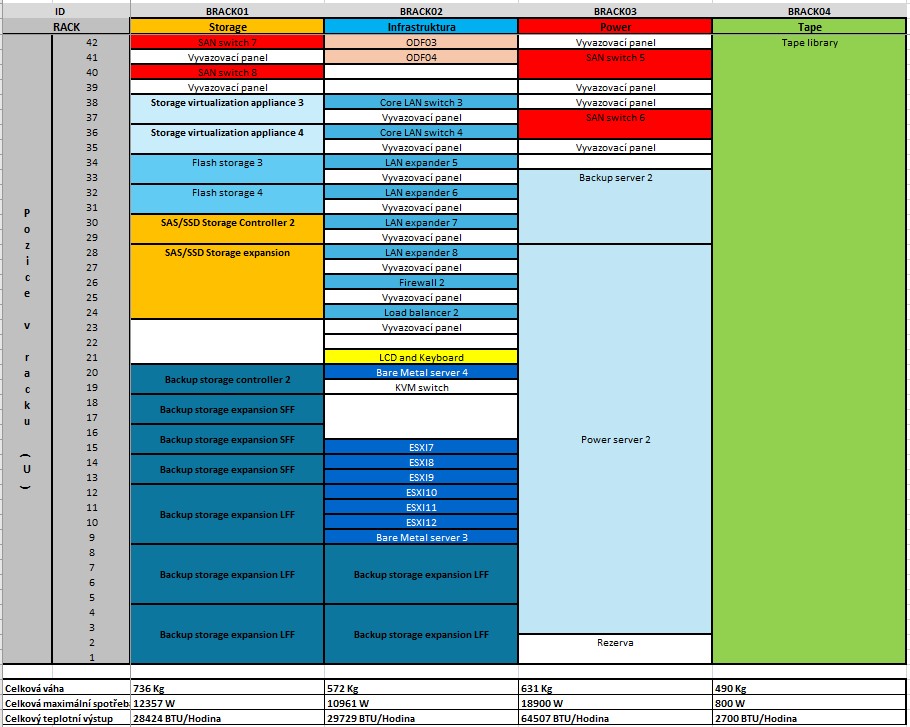
### Popis současného stavu

Veškeré technologie jsou aktuálně umístěny rovnoměrně ve dvou sálech DC Chodov (V lomech 2339/1, 149 00 Praha 4 – Chodov).

Aktuálně využívané technologie zajišťující provoz IS SZIF jsou umístěny v plně osazených šesti systémových skříních viz Obrázek 2 - Rack plán lokalita A a Obrázek 3 - Rack plán lokalita B, které jsou rovnoměrně umístěné v každém sále po třech kusem spolu s páskovou knihovnou viz Obrázek 1 - Architektura.



Obrázek 6 - Rack plán lokalita A



Obrázek 6 - Rack plán lokalita B

### Popis možností DC

Specifikace pro DC Chodov:

* Nosnost zdvojené podlahy je 2000 kg/m2 v celé ploše datového sálu.
* Standardně je poskytováno napájení v konfiguraci typicky:
  + 1F/230V/16A – cca 3 kW
  + 1F/230V/32A – cca 6 kW
  + 3F/400V/16A – cca 11 kW
  + 3F/400V/32A – cca 21 kW
* Do každého racku Objednatele vedou typicky dvě zcela nezávislé napájecí větve. Průběh napájecích větví je bez souběhu v trase vedení po celém DC. Každá větev má vlastní UPS, vlastní rozvaděč na datovém sále, vlastní jištění.
* DC má vlastní transformátory z VN na NN. Redundance N+1
* Chlazení na datových sálech je zajištěno chladícími jednotkami určenými pro datová centra. Na každém sále jsou chladící jednotky v redundanci N+1.
* Jednotlivé sály mají různou kapacitu chlazení, v závislosti na počtu chladících jednotek. Kapacita chlazení se pohybuje od 200 kW do 400 kW na jeden sál.
* Do DC je možné navážet materiál nákladním autem, vjezd pro nákladní automobil je zajištěn bránou ovládanou z recepce DC.
* Veškeré trasy v DC – přístupy do datových sálů – jsou bezbariérové.
* V DC jsou zákazníkům k dispozici manipulační vozíky a paletové vozíky.

### Požadavky na systémové skříně (Rack)

Samostatnou oblastí předmětu plnění jsou požadavky pro umístění nabízené technologie (všech funkčních celků) v jednotlivých lokalitách a příslušných Rack rozvaděčích, které definují celkovou fyzickou robustnost architektury řešení s ohledem na možné využití prostor v současném a budoucím DC Objednatele.

Součástí dodávky budou příslušné Racky, které však nesmí přesáhnout maximální povolenou hodnotu čtyř dodávaných Racků na jednu lokalitu (jeden sál) plus pásková knihovna. Tedy maximální přípustné množství dodávaných Racků je osm, s podmínkou rovnoměrného rozložení přes obě lokality.

Po provedení kompletní implementace a následní migrace a ukončení provozu stávající infrastruktury IS SZIF k 30.6.2025 budou tedy v každé lokalitě (v každém sále) umístěny 4 ks Racky a až dva kusy páskové knihovny, tzn. takto budou provozovány veškeré technologie zajišťující provoz Informačního systému SZIF na aplikační platformě SAP v jedné lokalitě.

Součástí dodávky bude zapojení PDU všech racků do DC včetně revize tohoto zapojení.

|  |  |  |  |
| --- | --- | --- | --- |
| **Rack** | | | |
| **Číslo** | **Název komponenty** | **Part number** | **Počet kusů** |
| 1 | IBM RACK | XXXXX | 6 |

Tabulka - Identifikace komponenty RACK

Nabízené Racky musí zejména poskytovat min. tyto klíčové standardy:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Rack – max 8 ks** | | | | |
| **Číslo** | **Vlastnost/komponenta** | **Požadované parametry** | **Splňuje ANO/NE** | **Skutečné parametry/Způsob splnění požadavku** |
|  | Velikost | * Kompatibilita RACK 19” s velikostí v EIA (42U) | ANO | Nabízené racky jsou kompatibilní s RACK 19“ a mají velikost v EIA 42U. |
|  | Rozměr | * Max. 65 cm šířka x max. 120 cm hloubka. | ANO | Nabízené racky mají šířku 60cm, hloubku 120cm a výšku 202cm. |
|  | Napájení | * PDU musí mít dostatečný počet konektorů C13 – C14/C19 – C20 pro připojení veškeré nabízené technologie. | ANO | PDU osazené v nabízených rack skříních obsahuje dostatečný počet konektorů C13 – C14/C19 – C20, pro připojení všech dodávaných zařízení. |

Tabulka – Vlastnosti Racku

### Popis dodávaného řešení - Racky

Dodavatel zpracuje a předloží Objednateli popis způsobu realizace osazení Racků nabízeným řešením a naplnění všech požadavků a parametrů stanovených v rack plánu ve vysokém detailu, který bude obsahovat minimálně tyto náležitosti:

* Osazení rackových skříní technologiemi.;
* Název a popis CMDB položky.;
* Rozložení technologií s uvedením počtu EIA jednotek „U“ včetně schématu.;
* Lokace PoP/PoD.;
* Definice el. spotřeby jednotlivých technologií.;
* Typ napájení a typ el. zásuvky.;
* Celkové teplotní výstupy za Rack (BTU/h).;
* Definice požadavků na chlazení jednotlivých technologií.;
* Popis dodávaných PDU a jejich zapojení do DC.;
* Definice požadavků na elektrické jištění.;
* Váha osazeného Racku.;
* atd.

## Datová úložiště

### Řešení pro ukládání dat

#### Popis současného stavu

Objednatel provozuje úložiště dat ve dvou lokalitách, kde jsou instalovány dva nody diskového pole IBM SVC, které tvoří HA cluster využívající technologii Hyperswap pro zajištění vysoké dostupnosti dat. Dále jsou v každé lokalitě instalovány další 2 diskové pole, které jsou virtualizovány pomocí IBM SVC a zajišťují potřebnou vysokou dostupnost diskových polí.

Objednatel provozuje pro účely zálohování datová úložiště HPE 3par Storserv 8200, která jsou připojena přímo k zálohovacím serverům IBM Spectrum Protect. Část kapacity z datových úložišť HPE je virtualizována pomocí IBM SVC.

Dále jsou pro ukládání záloh použity dvě páskové knihovny IBM TS4500 a LTO-8 driver. Každá z knihoven je v jiné lokalitě. Data na páskových knihovnách obsahují kopii záloh uložených na diskových polích. Dále jsou páskové knihovny používány pro ukládání záloh OFFSITE.

#### Požadavky na nové řešení

Zařízení pro ukládání dat jsou klíčová zařízení nejen z pohledu výkonu pro produkční servery a na nich provozované aplikace SAP, AMS, PF, GT Foto a další, ale také z pohledu vysoké dostupnosti, bezpečnosti a ochrany před ransomware útokem. Kromě vlastních produkčních kapacit patří mezi zařízení pro ukládání dat také zálohovací diskové a páskové systémy. Návrh pro zálohování vychází z pravidla 3-2-1 pro strategii ochrany dat. Ta doporučuje mít tři kopie dat uložené na dvou různých typech médií a jednu kopii uchovávat mimo pracoviště.

Pravidlo 3-2-1 je široce přijímanou strategií zálohování dat, která předepisuje:

1) Udržovat minimálně tři kopie dat;

2) K ukládání používat dva různé typy médií;

3) Alespoň jednu kopii uchovat v oddělené lokalitě mimo pracoviště;

Související zálohovací servery budou rozloženy do dvou lokalit pro zachování možnosti přechodu při DR situaci a pro realizaci vysoké dostupnosti. Pro uložení záloh bude využito diskových a páskových prostor.

Zařízení pro ukládání dat bude rozděleno na 3 části:

1. Vlastní produkční zařízení pro ukládání dat. Toto zařízení musí být na flash nebo obdobně výkonné technologii, podporované pro SAP HANA a splňující výkonnostní a kapacitní požadavky. Dále toto zařízení musí být integrovatelné do sw nástrojů pro detekci ransomware a musí podporovat všechny běžné provozní funkce (kopie, vzdálené zrcadlení apod.)
2. Zařízení pro ukládání dat záloh. U tohoto zařízení není kladen důraz na výkonnost, ale na kapacitu a možnost rychlé obnovy v případě jakéhokoli poškození produkčních kapacit.
3. Páskové zařízení používající zcela odlišné médium a zabezpečující poslední úroveň ochrany dat jak před selháním jakékoli hardwarové komponenty v zařízeních A) a B), tak před případným útokem na data v zařízeních A) a B). Jedná se o fyzicky bezpečně oddělené zálohy.

#### Disková pole pro produkční provoz

Nové prostředí diskových polí musí z pohledu přístupu k datům a vysoké dostupnosti odpovídat aktuální architektuře. Objednatel požaduje dvě identická disková pole s popsanými parametry.

|  |  |  |  |
| --- | --- | --- | --- |
| **Produkční disková pole** | | | |
| **Číslo** | **Název komponenty** | **Part number** | **Počet kusů** |
| 1 | IBM Flashsystem 9500 | XXXXX | 2 |

Tabulka - Identifikace komponenty Produkční diskové pole

Zejména musí poskytovat tyto klíčové vlastnosti:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Produkční disková pole (2ks)** | | | | |
| **Číslo** | **Vlastnost**  **/komponenta** | **Požadované parametry** | **Splňuje ANO/NE** | **Skutečné parametry/Způsob splnění požadavku** |
|  | Kompatibilita | * Zařízení musí být kompatibilní s OS a virtualizací: PowerVM (V3/V4), VMware (V7 a vyšší), OS AIX 7.2/7.3, OS RedHat 8.6/9, OS Suse, Windows 20 a vyšší, SAP HANA (podpora dle SAP pro minimálně 60 HANA node) | ANO | Nabízené zařízení je kompatibilní s OS a virtualizací: PowerVM (V3/V4), VMware (V7 a vyšší), OS AIX 7.2/7.3, OS RedHat 8.6/9, OS Suse, Windows 20 a vyšší, SAP HANA. Nabízené zařízení je certifikované pro provoz až 164 HANA nodes. |
|  | Technické vlastnosti a rozměry | * Kompatibilní s RACK 19” | ANO | Nabízené zařízení je kompatibilní s RACK 19“. |
|  | * Dodavatel uvede velikost v EIA (jednotek U) pro systémovou skříň 19”. |  | 4U. |
|  | * Dodavatel uvede počet a typ napájení (C13/14 nebo C19/C20 a počet). |  | 4x C19/C20. |
|  | * Dodavatel uvede hmotnost a typický a maximální elektrický příkon. |  | Maximální 3300 watt, typický: 2500 watt. |
|  | * Dodavatel uvede, jaké jsou požadavky na elektrické jištění. |  | 1 fáze, 32 A. |
|  | Napájení | * Zařízení musí mít redundantní napájecí zdroje 250VAC, vyměnitelné za chodu. | ANO | Nabízené zařízení má redundantní napájecí zdroje 250 VAC vyměnitelné za chodu. |
|  | Konektivita | * Připojena k SAN infrastruktuře je minimální 16x min. 64 Gb/s (pro každé zařízení). | ANO | Každé nabízené zařízení obsahuje 16x 64Gb/s FC port k připojení do SAN infrastruktury. |
|  | Výkon | * Řešení musí poskytnout výkon minimálně: náhodný IO výkon: 177.000 IO/s, poměr čtení:zápis 70:30, 100% náhodná zátěž při velikosti bloku 64 kB. | ANO | Nabízené zařízení poskytuje výkon až 648 759 IO/s při poměru čtení: zápis 70:30, 100% náhodná zátěž při velikosti bloku 64 kB. |
|  | * Celková velikost cache/RAM v jednom řadiči musí být minimálně 1024 GB. | ANO | Nabízené zařízení obsahují v každém řadiči cache o velikosti 1024GB. |
|  | Charakteristiky a funkce | * Plně redundantní architektura bez jediného bodu selhání (SPOF). | ANO | Nabízené zařízení jsou plně postaveny na redundantní architektura bez jediného bodu selhání (SPOF). |
|  | * Active-active přístup k diskovým prostorům (LUNům) v obou lokalitách. | ANO | Nabízené zařízení poskytují Active-active přístup k diskovým prostorům (LUNům) v obou lokalitách. |
|  | * Modulární, minimálně dvou řadičové all flash / hybridní diskové pole aktiv-aktiv designu založené na NVMe architektuře, řešení je koncipováno jako HW, SW a FW od jednoho výrobce. | ANO | Nabízené zařízení jsou modulární čtyř řadičové all flash disková pole aktiv-aktiv designu založené na NVMe architektuře. Řešení je koncipováno jako HW, SW a FW od jednoho výrobce. |
|  | * Řešení musí poskytovat nativní replikace po FC nebo IP v minimálně v synchronních a asynchronních režimech. Podpora replikace dat do třetí lokality. | ANO | Nabízené zařízení poskytují nativní replikace po FC nebo IP v synchronních a asynchronních režimech. Zařízení podporují replikaci do třetí lokality. |
|  | * Řešení musí podporovat min. následující režimy: RAID 1, 6 a 10 nebo distribuovaný RAID 1 a 6. | ANO | Nabízené zařízení podporují distribuovaný RAID 1 a 6. |
|  | * Diskový subsystém musí disponovat vytvářením virtuálních logických disků, thin provisioning (včetně detekce a reklamace prázdného prostoru). | ANO | Nabízené zařízení umožňují vytváření virtuálních logických disků, thin provisioning (včetně detekce a reklamace prázdného prostoru). |
|  | * Řešení musí poskytovat možnost vytváření snapshotů (CoW a RoW) a klonů v následujících režimech:   + a) snapshot se po určité době může automaticky stát klonem;   + b) inkrementální snapshoty, tzn. kopírují se jen rozdílová data mezi dvěma okamžiky iniciace klonu;   + c) reverzní snapshoty lze provést zpětné přesunutí dat z klonu do původního originálního Volume;   + d) lze udržovat min. 3 inkrementálně pořizované klony z jednoho originálu (s možností reverzních snapshotů). | ANO | Nabízené zařízení umožňují vytvářet snapshoty (CoW a RoW) a klony v následujících režimech:  a) snapshot se po určité době může automaticky stát klonem;  b) inkrementální snapshoty, tzn. kopírují se jen rozdílová data mezi dvěma okamžiky iniciace klonu;  c) reverzní snapshoty lze provést zpětné přesunutí dat z klonu do původního originálního Volume;  d) lze udržovat 3 inkrementálně pořizované klony z jednoho originálu (s možností reverzních snapshotů). |
|  | * Upgrade software a hardware u řadičů je musí být proveditelný za chodu a bez ztráty přístupu hostitelských serverů k datům. | ANO | Nabízené zařízení umožňují provádět upgrade software a hardware za chodu a bez ztráty přístupu hostitelských serverů k datům. |
|  | * Dodávané řešení musí obsahovat licence pro vytvoření automatického vysoce dostupného (HA Fail-over) řešení, tzn. možnost vytvoření globálního Volume, který bude dostupný i při výpadku jedné lokality. | ANO | Nabízené řešení obsahuje licence pro vytvoření automatického vysoce dostupného (HA Fail-over) řešení, tzn. možnost vytvoření globálního Volume. Volume je dostupný i při výpadku jedné lokality. |
|  | * Disková pole musí umožňovat integraci funkcí kopií dat se stávajícím zálohovacím softwarem IBM Storage Protect a s novým zálohovacím systémem. | ANO | Nabízené zařízení umožňují integraci funkcí kopií dat se stávajícím zálohovacím softwarem IBM Storage Protect a s novým zálohovacím systémem. |
|  | Ochrana proti ransomware | * Disková pole musí umožňovat vytváření aplikačně konzistentní a nesmazatelné kopie produkčních dat z důvodu zvýšené ochrany dat proti ransomware útokům. | ANO | Nabízené zařízení umožňují vytvářet aplikačně konzistentní a nesmazatelné kopie produkčních dat z důvodu zvýšené ochrany dat proti ransomware útokům. |
|  | * Aplikačně konzistentní, nesmazatelné a nemodifikovatelné kopie je nutné vytvářet minimálně pro DB Oracle nad OS AIX a prostředí SAP HANA nad RedHat. | ANO | Nabízené zařízení umožňují vytvářet konzistentní, nesmazatelné a nemodifikovatelné kopie DB Oracle, OS AIX a prostředí SAP HANA nad RedHat. |
|  | * Aplikačně konzistentní, nesmazatelné a nemodifikovatelné kopie musí být možno vytvářet bez nutnosti výpadku Oracle a SAP HANA.; | ANO | Nabízené zařízení umožňují vytvářet konzistentní, nesmazatelné a nemodifikovatelné kopie bez nutnosti výpadku Oracle a SAP HANA. |
|  | * Disková pole musí podporovat integraci do systému detekce ransomware. | ANO | Nabízené zařízení podporují integraci do systému detekce ransomware. |
|  | Kapacita | * Minimální požadovaná čistá kapacita (po RAID nebo dRAID6) **1128 TB** (kapacita bez optimalizace kompresními či deduplikačními nástroji a algoritmy). | ANO | Každé z nabízených zařízení má čistou kapacitu v dRAID6 1129,89TB. Tato kapacita je bez započítání optimalizace komprese či deduplikace. |
|  | * Počet sparedisků dle doporučení výrobce. | ANO | Každé z nabízených zařízení obsahuje 1 spare disk. |
|  | * Podporovány musí být enterprise SSD disky nebo Flash moduly, DWPD hodnota nabízených disků/modulů musí být 1 nebo vyšší. | ANO | Nabízené zařízení obsahují enterprise Flash moduly. Hodnota DWPD je 1. |
|  | Redukce dat | * Řešení musí poskytovat kompresi dat v reálném čase bez nutnosti dedikování dodatečného diskového prostoru pro post-processing pro celou nabízenou kapacitu včetně patřičného HW akcelerátoru nebo na jednotlivých modulech. | ANO | Nabízené zařízení obsahují FCM4 disky pro nabízenou kapacitu. Tyto FCM disky provádějí kompresi v reálném čase bez nutnosti dedikování dodatečného diskového prostoru pro post-processing na jednotlivých modulech. |
|  | * Řešení musí poskytovat deduplikaci dat v reálném čase bez nutnosti dedikování dodatečného diskového prostoru pro post-processing pro celou požadovanou kapacitu včetně SW licence. | ANO | Nabízené zařízení podporují využití deduplikace dat v reálném čase bez nutnosti dedikování dodatečného diskového prostoru pro post-processing pro celou požadovanou kapacitu včetně SW licence. |
|  | Šifrování | * Řešení musí poskytovat šifrování dat minimálně pro flash kapacitu ve standardu minimálně FIPS 140-2 bez nutnosti přítomnosti speciálních pevných disků včetně příslušné licence. * Pokud nabízené řešení neumožňuje šifrování dat nad úrovní disků, jsou požadovány SED disky pro celou nabízenou flash kapacitu, opět minimálně ve standardu FIPS 140-2. | ANO | Nabízené zařízení obsahují SED disky pro celou nabízenou flash kapacitu ve standardu FIPS 140-3 bez nutnosti speciálních pevných disků včetně licence. |
|  | Management/Řídící software | * MGMT rozhraní ve webové nebo grafické podobě. | ANO | Nabízené zařízení umožňuje provádět správu přes Webové rozhraní nebo CLI. |
|  | * MGMT rozhraní musí umožnit sledovat výkon systému a metriky měření. | ANO | Nabízené zařízení umožňuje v rámci MGMT Webového rozhraní sledovat výkon systému a metriky měření. |
|  | Provozní a výkonnostní monitoring | * Řešení musí umožnit sledování aktivity diskového pole v reálném čase s možností náhledu na různé výkonnostní parametry do minulosti (min. 1 rok) | ANO | Nabízené řešení umožňuje sledování aktivity diskového pole v reálném čase s možností náhledu na různé výkonnostní parametry do minulosti až 1 rok. |
|  | * Řešení musí umožňovat automatické generovaní reportů ve formátech HTML, PDF s automatickým zasíláním formou SMTP zvoleným příjemcům. | ANO | Nabízené řešení umožňuje automatické generovaní reportů ve formátech HTML, PDF s automatickým zasíláním formou SMTP zvoleným příjemcům. |
|  | * Řešení musí umožnit tvorbu reportů o vytížení pole. * Minimální požadovaná funkcionalita:   + System I/O     - Zobrazení počet operací Read, write, Total I/O   + System Latency     - Zobrazeni odezvy pro čtení a zápis (ms)   + System Bandwidth – šířka pásma     - Zobrazeni šířky pásma v (MB/s) pro čtení, zápis a celkovou   + System CPU     - Utilizace CPU v % | ANO | Nabízené řešení umožňuje tvorbu reportů o vytížení pole.  Nabízené řešení obsahuje následující funkcionalitu:  System I/O   * počet operací Read, write, Total I/O * System Latency * Zobrazeni odezvy pro čtení a zápis (ms) * System Bandwidth – šířka pásma * Zobrazeni šířky pásma v (MB/s) pro čtení, zápis a celkovou * System CPU * Utilizace CPU v %. |
|  | Rozšiřitelnost | * Dodavatel uvede počet volných pozic pro SSD/Flash disky či moduly. |  | Každé z nabízených zařízení obsahuje 12 volných pozic pro SSD/Flash disky či moduly. |
|  | * Řešení musí umožnit rozšíření o minimálně 33% (na **1500** **TB**). | ANO | Každé z nabízených zařízení umožňuje rozšíření kapacity až na 1517 TB. |
|  | * Škálování výkonnosti je prováděno nativním přidáváním dalších řadičů minimálně do čtyř řadičové konfigurace. | ANO | Nabízené zařízení umožňuje škálování výkonnosti nativním přidáváním dalších řadičů až do osmi řadičové konfigurace. |
|  | * Škálování kapacit je prováděno pomocí expanzních jednotek. | ANO | Nabízené zařízení umožňuje škálování kapacity přidáním expanzních jednotek. |
|  | * Dodavatel uvede možnosti rozšiřitelnosti a to: * A) pro Cache, * B) pro počty FC FC připojení. |  | Nabízená zařízení umožňují rozšířit cache na maximální velikost 3 TB.  Nabízené zařízení umožňují rozšířit počet FC portů až na 24x 64 Gb/s. |
|  | Záruka | * 6 let, 24x7, oprava do 24h | ANO | Nabízené zařízení mají záruku na HW komponenty 6let s dostupností 24x7 a opravou do 24h. |
| * Komunikace výhradně v českém jazyce | ANO | Podpora je dostupná výhradně v českém jazyce. |
| * Záruku garantuje přímo výrobce zařízení | ANO | Záruka je garantována výrobcem. |

Tabulka - Parametry diskového pole

#### Disková pole pro zálohování dat

Objednatel požaduje dvě identická disková pole s popsanými parametry pro potřeby zálohovacích systémů. Požadavky vychází z existující, jednoduché a provozně osvědčené architektury.

|  |  |  |  |
| --- | --- | --- | --- |
| **Zálohovací diskové pole** | | | |
| **Číslo** | **Název komponenty** | **Part number** | **Počet kusů** |
| 1 | IBM Flashsystem 5300 + 3x High Density Expansion | XXXXX | 2 |

Tabulka - Identifikaci komponenty Zálohovací diskové pole

Disková pole musí poskytovat zejména tyto klíčové vlastnosti:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Zálohovací disková pole (2ks)** | | | | |
| **Číslo** | **Vlastnost /komponenta** | **Požadované parametry** | **Splňuje ANO/NE** | **Skutečné parametry/Způsob splnění požadavku** |
|  | Kompatibilita | * Zařízení musí být kompatibilní s IBM Spectrum Protect a nově navrženým zálohovacím řešením. | ANO | Nabízené zařízení jsou kompatibilní s IBM Spectrum Protect i nabízeným zálohovacím řešení. |
|  | Technické vlastnosti a rozměry | * Kompatibilní s RACK 19”. | ANO | Nabízené zařízení je kompatibilní s RACK 19“. |
|  | * Dodavatel uvede velikost v EIA (jednotek U) pro systémovou skříň 19”. |  | 16U. |
|  | * Dodavatel uvede počet a typ napájení (C13/14 nebo C19/C20 a počet). |  | 2x C13/C14, 6x C19/C20. |
|  | * Dodavatel uvede hmotnost a typický a maximální elektrický příkon. |  | maximální 4050 watt, typický: 3200 watt. |
|  | * Dodavatel uvede, jaké jsou požadavky na elektrické jištění. |  | 1 fáze, 32 A. |
|  | Napájení | * Zařízení musí mít redundantní napájecí zdroje 250VAC, vyměnitelné za chodu. | ANO | Nabízené zařízení má redundantní napájecí zdroje 250 VAC vyměnitelné za chodu. |
|  | Konektivita | * Připojena k SAN infrastruktuře je minimální 4x min. 32 Gb/s (pro každé zařízení). | ANO | Každé nabízené zařízení obsahuje 8x 32 Gb/s FC port k připojení do SAN infrastruktury. |
|  | Výkon | * SSD/flash vrstva: Náhodný IO výkon: min. 30.000 IO/s, poměr čtení:zápis 50:50, 100% náhodná zátěž, velikost bloku 128 kB. | ANO | Nabízené zařízení poskytuje výkon až 40 788 IO/s při poměru čtení:zápis 50:50, 100% náhodná zátěž při velikosti bloku 128 kB. |
|  | * NL-SAS vrstva: Propustnost: min. 3.500 MB/s, poměr čtení:zápis 50:50, 100% sekvenční zátěž, velikost bloku 1024 kB. | ANO | Nabízené zařízení poskytuje propustnost až 5 000 MB/s při poměru čtení:zápis 50:50, 100% sekvenční zátěž při velikosti bloku 1024 kB. |
|  | * Celková velikost cache/RAM v jednom řadiči je minimálně 128 GB. | ANO | Nabízené zařízení obsahují v každém řadiči cache o velikosti 128 GB. |
|  | Charakteristiky a funkce | * Modulární, minimálně dvou řadičové all flash / hybridní diskové pole aktiv-aktiv designu založené na NVMe architektuře, řešení je koncipováno jako HW, SW a FW od jednoho výrobce. | ANO | Nabízené zařízení jsou modulární dvou řadičové all flash disková pole aktiv-aktiv designu založené na NVMe architektuře. Řešení je koncipováno jako HW, SW a FW od jednoho výrobce. |
|  | * Řešení musí poskytovat nativní replikace po FC nebo IP v minimálně v synchronních a asynchronních režimech. Podpora replikace dat do třetí lokality. | ANO | Nabízené zařízení poskytují nativní replikace po FC nebo IP v synchronních a asynchronních režimech. Zařízení podporují replikaci do třetí lokality. |
|  | * Řešení musí podporovat min. následujících režimů: RAID 1, 6 a 10 nebo distribuovaný RAID 1 a 6. | ANO | Nabízené zařízení podporují distribuovaný RAID 1 a 6. |
|  | * Diskový subsystém musí disponovat vytvářením virtuálních logických disků, thin provisioning (včetně detekce a reklamace prázdného prostoru). | ANO | Nabízené zařízení umožňují vytváření virtuálních logických disků, thin provisioning (včetně detekce a reklamace prázdného prostoru). |
|  | * Požadována je možnost vytváření snapshotů (CoW a RoW) a klonů v následujících režimech:   + a) snapshot se po určité době může automaticky stát klonem;   + b) inkrementální snapshoty, tzn. kopírují se jen rozdílová data mezi dvěma okamžiky iniciace klonu;   + c) reverzní snapshoty lze provést zpětné přesunutí dat z klonu do původního originálního Volume;   + d) lze udržovat až 4 inkrementálně pořizované klony z jednoho originálu (s možností reverzních snapshotů). | ANO | Nabízené zařízení umožňují vytvářet snapshoty (CoW a RoW) a klony v následujících režimech:  a) snapshot se po určité době může automaticky stát klonem;  b) inkrementální snapshoty, tzn. kopírují se jen rozdílová data mezi dvěma okamžiky iniciace klonu;  c) reverzní snapshoty lze provést zpětné přesunutí dat z klonu do původního originálního Volume;  d) lze udržovat 4 inkrementálně pořizované klony z jednoho originálu (s možností reverzních snapshotů). |
|  | * Upgrade software a hardware u řadičů musí být proveditelný za chodu a bez ztráty přístupu hostitelských serverů k datům. | ANO | Nabízené zařízení umožňují provádět upgrade software a hardware za chodu a bez ztráty přístupu hostitelských serverů k datům. |
|  | Kapacita | * Minimální požadovaná čistá kapacita (po RAID nebo dRAID6) **992** TB (bez optimalizace kompresními či deduplikačními nástroji a algoritmy).   + z toho: * min. 79 TB na flash/SSD; * min. 913 TB na NL-SAS; | ANO | Každé z nabízených zařízení obsahuje celkovou čistou kapacitu 1273 TB (bez optimalizace kompresními či deduplikačními nástroji a algoritmy).  Z toho:   * 93 TB v Flash/SSD tieru.   1180 TB v NL-SAS tieru. |
|  | * Počet sparedisků dle doporučení výrobce. | ANO | Každé z nabízených zařízení obsahuje následující počet spare disků:   * Flash/SSD – 1 disk   NL-SAS – 6 disky. |
|  | * Podporovány musí být enterprise SSD disky, Flash moduly a HDD disky, DWPD hodnota nabízených flash a SSD disků/modulů musí být 1 nebo vyšší. | ANO | Nabízené zařízení obsahují enterprise Flash moduly a HDD disky. Hodnota DWPD je 1 u Flash modulů. |
|  | Redukce dat | * Řešení musí poskytovat deduplikaci dat v reálném čase bez nutnosti dedikování dodatečného diskového prostoru pro post-processing pro celou požadovanou kapacitu včetně SW licence. | ANO | Nabízené zařízení podporují využití deduplikace dat v reálném čase bez nutnosti dedikování dodatečného diskového prostoru pro post-processing pro celou požadovanou kapacitu včetně SW licence. |
|  | Management /Řídící software | * MGMT rozhraní ve webové nebo grafické podobě. | ANO | Nabízené zařízení umožňuje provádět správu přes grafické webové rozhraní. |
|  | * MGMT rozhraní musí umožnit sledovat výkon systému a metriky měření. | ANO | Nabízené zařízení umožňuje v rámci MGMT Webového rozhraní sledovat výkon systému a metriky měření. |
|  | Provozní a výkonnostní monitoring | * Řešení musí umožnit sledování aktivity diskového pole v reálném čase s možností náhledu na různé výkonnostní parametry do minulosti (min. 1 rok) | ANO | Nabízené řešení umožňuje sledování aktivity diskového pole v reálném čase s možností náhledu na různé výkonnostní parametry do minulosti až 1 rok. |
|  | * Řešení musí umožňovat automatické generovaní reportů ve formátech HTML, PDF s automatickým zasíláním formou SMTP zvoleným příjemcům. | ANO | Nabízené řešení umožňuje automatické generovaní reportů ve formátech HTML, PDF s automatickým zasíláním formou SMTP zvoleným příjemcům. |
|  | * Řešení musí umožnit tvorbu reportů o vytížení pole. * Minimální požadovaná funkcionalita:   + System I/O     - Zobrazení počet operací Read, write, Total I/O   + System Latency     - Zobrazeni odezvy pro čtení a zápis (ms)   + System Bandwidth – šířka pásma     - Zobrazeni šířky pásma v (MB/s) pro čtení, zápis a celkovou   + System CPU     - Utilizace CPU v % | ANO | Nabízené řešení umožňuje tvorbu reportů o vytížení pole.  Nabízené řešení obsahuje následující funkcionalitu:  System I/O   * počet operací Read, write, Total I/O   System Latency   * Zobrazeni odezvy pro čtení a zápis (ms)   System Bandwidth – šířka pásma   * Zobrazeni šířky pásma v (MB/s) pro čtení, zápis a celkovou   System CPU   * Utilizace CPU v %. |
|  | Rozšiřitelnost | * Minimálně o 50% v obou vrstvách (SSD/flash, NL-SAS). | ANO | Nabízené zařízení je možné rozšířit o více než 50% v obou vrstvách (SSD/flash, NL-SAS). |
|  | * Škálování kapacit je prováděno pomocí expanzních jednotek. | ANO | Nabízené řešení umožňuje škálovat kapacitu pomocí přidání expanzních boxů. |
|  | * Dodavatel uvede možnosti rozšiřitelnosti cache a počty FC připojení. |  | Nabízené řešení umožňuje rozšířit cache až na 256 GB v jednom řadiči.  Nabízené řešení obsahuje maximální počet FC portů. Počet FC portů je 8x 32 GB/s. |
|  | Záruka | * 6 let, 24x7, oprava do 24h | ANO | Nabízená zařízení mají záruku na HW komponenty 6 let s dostupností 24x7 a opravou do 24h. |
| * Komunikace výhradně v českém jazyce | ANO | Podpora je dostupná výhradně v českém jazyce. |
| * Záruku garantuje přímo výrobce zařízení | ANO | Záruka je garantována výrobcem. |

Tabulka - Parametry zálohovacích diskových polí

#### Páskové knihovny

|  |  |  |  |
| --- | --- | --- | --- |
| **Pásková knihovna** | | | |
| **Číslo** | **Název komponenty** | **Part number** | **Počet kusů** |
| 1 | LTO9 mechaniky | XXXXX | 20 |
| 2 | LTO9 pásková media | XXXXX | 960 |
| 3 | LTO čistící media | XXXXX | 40 |

Tabulka - Identifikace komponenty Pásková knihovna

Páskové knihovny, musí poskytovat zejména tyto klíčové vlastnosti:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Páskové knihovny (2ks)** | | | | |
| **Číslo** | **Vlastnost /komponenta** | **Požadované parametry** | **Splňuje ANO/NE** | **Skutečné parametry/Způsob splnění požadavku** |
|  | Kompatibilita | * Zařízení musí být kompatibilní s IBM Spectrum Protect a nově navrženým zálohovacím řešením. | ANO | Nabízené mechaniky LTO9 jsou kompatibilní s IBM Spectrum Protect a nově navrženým zálohovacím řešením. |
|  | Technické vlastnosti a rozměry | * Dodavatel uvede velikost a hmotnost. |  | Dodavatel nabízí doplnění LTO9 mechaniky do stávajících páskových knihoven. Rozměry stávajících páskových knihoven se nemění.  Velikost a váha stávajících knihoven:  Váha 490 kg  Velikost 42U  Rozměry: 180cm x 78,2 cm x 121,2 cm. |
|  | * Dodavatel uvede počet a typ napájení (C13/14 nebo C19/C20 a počet). |  | Dodavatel nabízí doplnění LTO9 mechaniky do stávajících páskových knihoven. Počet a typ napájení knihoven se nemění.  Stávající knihovny napájení:  2x 230V/16A – 1 fáze. |
|  | * Dodavatel uvede typický a maximální elektrický příkon. |  | Dodavatel nabízí doplnění LTO9 mechaniky do stávajících páskových knihoven. Typický a maximální elektrický příkon knihoven se nemění.  Stávající knihovny:  Maximální: 800 W  Typický: 530 W. |
|  | * Dodavatel uvede, jaké jsou požadavky na elektrické jištění. |  | 2x 230V/16A – 1 fáze. |
|  | Napájení | * Zařízení musí mít redundantní napájecí zdroje 250VAC. | ANO | Nabízené zařízení obsahuje napájecí zdroje 250 VAC. |
|  | Konektivita | * Nové LTO mechaniky musí být připojeny pomocí FC k SAN infrastruktuře minimálně 10ks min. 8 Gb/s (pro každé zařízení). | ANO | Nabízené LTO9 mechaniky je možné připojit k SAN infrastruktuře přes 10x 8Gb/s FC port pro každé zařízení. |
|  | Charakteristiky | * Objednatel požaduje dodání nové knihovny s min. 10-ti LTO9 nebo novějšími mechanikami nebo doplnění min. 10 ks LTO9 nebo novějších mechanik do existujících páskových knihoven TS4500, 3584-L55, sériových čísel: 78BB231 a 78B230. | ANO | Je nabízeno doplnění 10ks LTO9 mechaniky do existujících páskových knihoven TS4500, 3584-L55, sériových čísel: 78BB231 a 78B230. |
|  | Kapacita | * Objednatel požaduje osazení min. 480 ks LTO9 medií. | ANO | Nabízené řešení obsahuje dodávku 480 ks LTO9 medií do každé knihovny. Celkově nabízené řešení obsahuje dodávku 960ks medii. |
|  | * Média včetně serializace dle pokynu Objednatele. | ANO | Nabízené řešení umožňuje provedení serializace medii dle pokynu Objednatele. |
|  | * Objednatel požaduje min. 480 ks aktivovaných slotů v každé knihovně. | ANO | Nabízené řešení obsahuje 730 ks aktivovaných slotů v každé knihovně. |
|  | * Objednatel požaduje min. 20 ks čistících médií pro každou knihovnu. | ANO | Nabízené řešení obsahuje dodávku 20 ks čistících medií pro každou knihovnu. |
|  | Rozšiřitelnost | * Objednatel požaduje možnost navýšit počet LTO9 mechanik min. až na 15ks. | ANO | Nabízené řešení umožňuje rozšíření počtu LTO9 mechanik až na 128 ks pomocí přidání dalších „framu“ páskové knihovny. |
|  | * Zařízení musí mít možnost rozšířit počet slotů o min. 50%. | ANO | Nabízené řešení umožňuje rozšíření počtu slotů přidáním dalších „frame“ páskové knihovny až na 23 170 slotů. |
|  | Záruka | * 6 let, 24x7, oprava do 24h | ANO | Nabízené zařízení mají záruku na HW komponenty 6let s dostupností 24x7 a opravou do 24h. |
| * Komunikace výhradně v českém jazyce | ANO | Podpora je dostupná výhradně v českém jazyce. |
| * Záruku garantuje přímo výrobce zařízení | ANO | Záruka je garantována výrobcem. |
|  | Provozní a výkonnostní monitoring | * Řešení musí poskytovat minimálně chybové a diagnostické údaje o stavu knihovny i mechanik. | ANO | Nabízené řešení umožňuje poskytovat chybové a diagnostické údaje o stavu knihovny i mechanik. |
|  | Management /Řídící software | * MGMT rozhraní ve webové nebo grafické podobě. | ANO | Nabízené řešení obsahuje MGMT ve formě webového rozhraní. |

Tabulka - Parametry páskových knihoven

### Řešení pro zálohování a ochranu dat

#### Popis současného stavu

Jako zálohovací systém prostředí Objednatele je použit nástroj IBM Storage Protect (dříve Spectrum Protect nebo také Tivoli Storage Manager) s klienty pro zálohování souborových systémů OS AIX/Linux/Windows a aplikací - Oracle DB, SAP, SAP Hana, VMware VM.

Instance IBM Storage Protect serveru (dále také jen SPS) běží na clusteru dvou IBM POWER serverů umístěných ve dvou lokalitách. Společně s IBM POWER server je na každé lokalitě jedno diskové pole pro ukládání záloh a také jedna pásková knihovna.

Celý systém zálohování je navržen tak, aby všechna data byla uložena minimálně ve dvou kopiích. Jedna kopie je na diskových polích a druhá kopie dat je uložena na LTO páskách. Nebo aby jedna kopie dat na páskách zůstávala ONSITE a další kopie dat byla uložena OFFSITE.

Pro zajištění vysoké dostupnosti instance SPS je použit clusterový systém IBM POWER HA na OS AIX 7.2 na dvou serverech POWER S824 umístěných ve dvou lokalitách v konfiguraci Active/Pasive.

Jako úložiště záloh jsou použity dva diskové systémy HP 3PAR. Každý z diskových systémů je umístěn na jiné lokalitě a obsahuje plnou kopii všech dat. Kopie dat je prováděna mirroringem na úrovni LVM OS AIX instance SPS.

Dále jsou pro ukládání záloh použity dvě páskové knihovny IBM TS4500 a LTO-8 drivy. Každá z knihoven je v jiné lokalitě. Data na páskových knihovnách obsahují kopii záloh uložených na diskových polích. Dále jsou páskové knihovny používány pro ukládání záloh OFFSITE.

#### Požadavky na nové řešení

Zálohování a ochrana dat jsou klíčové funkcionality k zabezpečení dat proti poškození.

Zálohovaní je prováděné z důvodu ochrany proti selhání hardwarových nebo softwarových komponent nebo lidské chybě. Navržené zálohování a obnova vychází z konceptu 3-2-1 popsaného v kapitole viz 2.4.1.2 Požadavky na nové řešení. Zálohování musí podporovat databáze Oracle, SAP HANA, ERP systém SAP, VMware a všechny Dodavatelem dodané platformy. Také musí podporovat nabízená zařízení pro ukládaní dat jak diskové, tak páskové technologie. Navržené zálohování navazuje na existující, dlouhodobě využívané řešení.

Ochrana proti kybernetickým útokům a detekce anomálií (ochrana proti ransomware, malware apod.). V současnosti je pravděpodobnost ransomware útoku až 10x vyšší než pravděpodobnost výpadku z důvodu HW nebo SW chyby (dáno jak vylepšeními na straně HW a SW, tak dramatickým nárůstem nepřátelských útoků na data). Poptávané řešení musí provádět skenování datových oblastí tak, aby bylo možné detektovat anomálie spojené s výskytem možné změny indikující ransomware. A to především pro kritické datové oblasti databází Oracle, SAP HANA a případně prostředí VMWare. Je nezbytné, aby tato funkcionalita byla integrovatelná s automatickou tvorbou nesmazatelných kopií a umožnila nejen detekci, ale také rychlou obnovu dat.

Objednatel požaduje, aby nabízené řešení bezpodmínečně zajišťovalo kompatibilitu se stávajícím řešením tak, aby bylo možné v případě nutnosti/havárie provést obnovu z pásek s dlouhodobou zálohou a archivem.

Objednatel umožňuje nahrazení stávajícího zálohovacího prostředí jiným řešením. V případě nahrazení stávajícího řešení, musí Dodavatel provést migraci všech dlouhodobých záloh a archivu do navrženého prostředí se zaručením zachování retencí.

#### Zálohování

Zálohování a ochrana dat jsou klíčové funkcionality k zabezpečení dat proti poškození.

|  |  |  |  |
| --- | --- | --- | --- |
| **SW pro zálohování** | | | |
| **Číslo** | **Název komponenty** | **Part number** | **Počet kusů** |
| 1 | IBM Storage Defender Resource Unit Subscription License per Month | XXXXX | 8866 |

Tabulka - Identifikace komponenty SW pro zálohování

Objednatel požaduje spolehlivé řešení, které zejména musí poskytovat tyto klíčové vlastnosti:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **SW pro zálohování** | | | | |
| **Číslo** | **Vlastnost / komponenta** | **Požadované parametry** | **Splňuje ANO/NE** | **Skutečné parametry/Způsob splnění požadavku** |
|  | Kompatibilita | * Zálohovací prostředí musí umožnit zálohovat minimálně tyto klienty a OS:   + OS AIX;   + OS Linux RedHat;   + OS Windows;   + Oracle DB;   + SAP Aplikační server;   + SAP Hana;   + VMware; | ANO | Řešení pro zálohování umožňuje zálohovat tyto klienty a OS:   * OS AIX; * OS Linux RedHat; * OS Windows; * Oracle DB; * SAP Aplikační server; * SAP Hana; * VMware; |
|  | * Zálohovací prostředí musí podporovat navržené páskové knihovny a navržená disková pole pro zálohování. | ANO | Řešení pro zálohování podporuje nabízenou páskovou knihovnu a dodávané diskové pole pro zálohování. |
|  | * Zaručená kompatibilita nástroje se stávajícím řešením založeném na produktu IBM Storage Protect.; * V případě nabídky jiného řešení, Dodavatel detailně popíše zajištění požadované kompatibility a migrace stávajících dlouhodobých záloh a archivu.; | ANO | Řešení pro zálohování je plně kompatibilní se stávajícím řešením založeném na produktu IBM Storage Protect. |
|  | Charakteristiky | * Řešení musí umožnit vytvoření aktiv-aktiv vysoce dostupného řešení zálohovacích komponent (primárního zálohovacího katalogu). | ANO | Řešení pro zálohování umožňuje vytvoření aktiv-aktiv vysoce dostupného řešení zálohovacích komponent (primárního zálohovacího katalogu). |
|  | * Řešení musí podporovat stálé inkrementální zálohování (bez ohledu na typu zálohovaných dat). | ANO | Řešení pro zálohování podporuje stálé inkrementální zálohování (bez ohledu na typu zálohovaných dat). |
|  | * Objednatel požaduje SW řešení, které je možné nasadit na OS AIX nebo Linux.; | ANO | Řešení pro zálohování obsahuje SW, který je možné nasadit na OS AIX nebo Linux. |
|  | Licenčně pokrytá kapacita | * Front-End kapacita zálohovaných dat jsou min. 66,66% z produkčních kapacit 1078 TB na jedné lokalitě - požadovaná zálohovaná kapacita musí být min.: **1438 TB** (1307 TiB). | ANO | Řešení pro zálohování má licencovanou front-end kapacitu 1438 TB (1307 TiB).  SP licence je možné licencovat na FE, nicméně BE licencování v tomto případě vychází cenově lépe. |
|  | * Back-End kapacita dle používaných retenčních period a deduplikačního poměru musí být min.: **1826 TB** (1661 TiB); | ANO | Řešení pro zálohování má licencovanou back-end kapacitu 1826 TB (1661 TiB).  SP licence je možné licencovat také na BE, BE je v tomto případě cenově výhodnější než FE kalkulace. |
|  | Šifrování | * Přenos všech dat musí probíhat pouze mezi klientem a zálohovacím serverem; | ANO | Přenos všech dat a komunikace probíhá pouze mezi klientem a zálohovacím serverem, je šifrována pomocí SSL/TLS. |
|  | * Během ukládání dat na LTO media musí být data zašifrována; | ANO | Řešení pro zálohování disponuje šifrováním dat při ukládání na LTO media.  Řešení pro zálohování také umožňuje šifrování dat na straně páskových úložišť (technologie IBM 3592 či otevřená technologie LTO Ultrium). |
|  | * Správu klíčů pro šifrování musí provádět zálohovací server; | ANO | Řešení pro zálohování má správu klíčů pro šifrování na straně zálohovacího serveru.  IBM Storage Protect podporuje šiforvání zálohovaných dat, data jsou šifrována technologií Advanced Encryption Standard (AES) 128-bit nebo 256-bit. Data mohou být šifrovaná na klientu, tak i na serveru před jejich uložením. Klíče jsou centrálně uloženy na straně SP serveru v tzv. certifikační databázi. |
|  | Redukce dat | * Řešení musí obsahovat deduplikaci a komprimaci.; | ANO | Řešení pro zálohování disponuje inline deduplikací a komprimací jak na serverové straně tak na klientské straně. |
|  | Provozní a výkonnostní monitoring | * Řešení musí poskytovat reporting a centrální správu. | ANO | Řešení pro zálohování má reporting a cetrální správu je možné zajistit nástrojem SP Operation Center, který je součásti dodávky. |
|  | Záruka | * Podpora řešení a aktualizace po dobu 6 let | ANO | Nabízené SW komponenty mají podporu na 6let včetně předplacených aktualizací a nových verzí. |
| * Komunikace výhradně v českém jazyce | ANO | Komunikace s podporou je výhradně v českém jazyce. |
| * Záruku garantuje přímo výrobce zařízení | ANO | Záruka je garantována výrobcem SW IBM. |

Tabulka - SW pro zálohování

Objednatel si je vědom složitosti licenčních podmínek a metrik u aktuálně nabízených SW pro řízení a tvorbu záloh. Objednatel proto poskytuje údaje o objemu zálohovaných dat (tzv. Front-End data) a objem dat uložených v zálohovacím řešení s ohledem na použité retenční doby a dosahovanou deduplikaci (tzv. Back-End data).

S ohledem na komplexnost a očekávané výrazné změny počtu instancí, použitých procesorů pro jednotlivá prostředí v průběhu 6-ti let není licenční mechanismus na bázi počtu CPU, typu řešení nebo počtu instancí realizovatelný.

Z tohoto důvodu si Dodavatel může zvolit vhodnější z uvedených Front-End a Back-End licenčních metrik pro jím navržený zálohovací SW.

#### Správa klonovacích (hardwarový snapshot) funkcí

|  |  |  |  |
| --- | --- | --- | --- |
| **SW pro správu klonovacích funkcí** | | | |
| **Číslo** | **Název komponenty** | **Part number** | **Počet kusů** |
| 1 | IBM Storage Defender Resource Unit Subscription License per Month | XXXXX | 8866 |

Tabulka - Identifikaci komponenty HW snapshot

Objednatel požaduje spolehlivé řešení, které zejména musí poskytovat tyto klíčové vlastnosti:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Správa klonovacích (hardware snapshot) funkcí** | | | | |
| **Číslo** | **Vlastnost /komponenta** | **Požadované parametry** | **Splňuje ANO/NE** | **Skutečné parametry/Způsob splnění požadavku** |
|  | Kompatibilita | * Řešení musí podporovat databáze Oracle, SAP HANA a virtualizaci VMware. | ANO | Nabízené řešení podporuje databáze Oracle, SAP HANA a virtualizaci VMware. |
|  | * Řešení musí podporovat nabízená produkční disková pole. | ANO | Nabízené řešení podporuje nabízená disková pole IBM Storage Systems. |
|  | Charakteristiky | * Aplikačně konzistentní snímky (snapshot) jsou požadovány minimálně pro tyto základní úlohy (workload):   + DB Oracle (19c) (aktuálně provozovány na operačním systému AIX);   + VMware (8 a vyšší);   + SAP HANA (2 a vyšší) na operačním systému RedHat; * (Crash konzistentní kopie nejsou přijatelné). | ANO | Nabízené řešení umožňuje aplikačně konzistentní snímky (snapshot) pro tyto základní úlohy (workload):   * DB Oracle (19c); * VMware (8 a vyšší); * SAP HANA (2 a vyšší) na operačním systému RedHat;   Nabízené řešení crash konzistentní kopie nepřipouští. |
|  | * Řešení musí umožnit následnou práci se snímky (snapshot) pro automatické vytvoření aktivní kopie pro potřeby selhání, vývojových prostředí, patch management nebo bezpečnostního skenování dat. | ANO | Nabízené řešení umožňuje s vytvořenými snapshoty dále pracovat, například pro vytváření záloh, vytvoření demo testovacího prostředí či pro účely bezpečnostního skenování k odhalení ransomware. |
|  | * Řešení musí podporovat nesmazatelné a nemodifikovatelné hardwarové snímky (snapshot). | ANO | Nabízené řešení podporuje nesmazatelné a nemodifikovatelné hardwarové snímky (snapshot).  CDM umí provádět Safeguarded kopie, které nelze uživatelem odstranit. |
|  | * Software pro správu snapshotů musí podporovat integraci s bezpečnostním řešením, které provádí automatické skenování variability dat mezi snapshoty, aby bylo možné detekovat anomálie a možné hrozby ransomwaru. | ANO | Nabízený software pro správu snapshotů podporuje integraci s bezpečnostním řešením, které provádí automatické skenování variability dat mezi snapshoty, pro detekci anomálií a možných hrozeb ransomwaru.  CDM podporuje integraci např s bezpečnostním řešením IBM Sentinel, snapshoty je tak možné skenovat na přítomnost ransomware hrozeb. |
|  | * Implementace nástroje pro Detekce ransomware hrozeb je požadována ve virtuálním prostředí (VMware) nebo na dedikovaném fyzickém serveru s OS Linux. | ANO | Nabízené řešení pro detekci ransomware je možné naimplementovat formou ova filu do VMware vSphere prostředí nebo instalací do OS Linux na fyzický server. |
|  | Licenčně pokrytá kapacita | * Licenčně musí být pokryta kapacita min. **1500 TB** (1365 TiB). | ANO | Nabízené řešení pokrývá licenčně kapacitu 1500 TB (1365 TiB)  Pokryto licenčním balíkem backup SW Storage Protect Suite Backend jehož je CDM součástí. |
|  | * Řešení musí umožnit vytvářet konzistentní snímky (snapshoty) na min. **66,66%** kapacity diskového pole. | ANO | Nabízené řešení nemá kapacitní limit pro vytváření snapshotů. |
|  | Záruka | * Podpora řešení a aktualizace po dobu 6 let | ANO | Nabízené SW komponenty mají podporu na 6 let včetně předplacených aktualizací a nových verzí. |
| * Komunikace výhradně v českém jazyce | ANO | Komunikace s podporou je výhradně v českém jazyce. |
| * Záruku garantuje přímo výrobce zařízení | ANO | Záruka je garantována výrobcem SW IBM. |

Tabulka - Správa klonovacích funkcí

#### Detekce ransomware hrozeb

|  |  |  |  |
| --- | --- | --- | --- |
| **Detekce ransomware** | | | |
| **Číslo** | **Název komponenty** | **Part number** | **Počet kusů** |
| 1 | IBM Storage Defender Resource Unit Subscription License per Month | XXXXX | 4500 |

Tabulka - Identifikace komponenty pro Detekci ransomware

Objednatel požaduje spolehlivé řešení, které zejména musí poskytovat tyto klíčové vlastnosti:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Detekce ransomware hrozeb** | | | | |
| **Číslo** | **Vlastnost /komponenta** | **Požadované parametry** | **Splňuje ANO/NE** | **Skutečné parametry/Způsob splnění požadavku** |
|  | Kompatibilita | * Automatizované skenování z HW snapshotů pro detekci ransomwarových útoků musí podporovat minimálně následující kritické databáze: Oracle, SAP HANA. | ANO | Nabízené řešení podporuje EPIC, SAP HANA, Oracle, od verze 1.1.9 také VMware. |
|  | * Řešení musí být kompatibilní s virtualizací: PowerVM (V3/V4), VMware (V7 a vyšší). | ANO | Nabízené řešení je kompatibilní s virtualizací: PowerVM (V3/V4), VMware (V7 a vyšší). |
|  | * Řešení musí podporovat nabízená produkční disková pole. | ANO | Řešení podporuje nabízená disková pole IBM Storage Systems. |
|  | Charakteristiky | * Objednatel požaduje automatizaci bezpečnostních skenů HW snapshotů podle typu kritické aplikace (vytvoření více SLA politik) a v případě nalezení hrozby požaduje mít možnost obnovit data z ověřeného aplikačně konzistentního snímku (snapshot). | ANO | Nabízené řešení má automatizaci bezpečnostních skenů HW snapshotů podle typu kritické aplikace (vytvoření více SLA politik) a v případě nalezení hrozby má možnost obnovit data z ověřeného aplikačně konzistentního snímku (snapshot). |
|  | * Implementace nástroje pro Detekce ransomware hrozeb je požadována ve virtuálním prostředí (VMware) nebo na dedikovaném fyzickém serveru s OS Linux. | ANO | Nabízené řešení pro detekci ransomware je možné naimplementovat do VMware vSphere prostředí nebo instalací do OS Linux na fyzický server. |
|  | * Skenování musí probíhat automaticky. | ANO | Nabízené řešení má automatické skenování.  Softwarové řešení pro skenování anomálií IBM® Storage Sentinel umožňuje komplexní automatizovaný pracovní postup kybernetické odolnosti. |
|  | * Nástroj pro detekci ransomware hrozeb musí umožnit integraci do nástroje pro správu klonovacích funkcí. | ANO | Nabízené řešení má možnost integrace do nástroje pro správu klonovacích funkcí.  Integrováno s IBM Storage Copy Data Management. |
|  | * Hlášení o pozitivní detekci/anomálii/podezřelé operaci ransomwarového útoku musí být integrovatelené softwarového řešení pro správu snapshotů (pro účely Infrastrukturního týmu). | ANO | Nabízené řešení je integrovatelné do softwarového řešení pro správu snapshotů.  Bude integrováno s IBM Storage Copy Data Management. |
|  | * Dodavatel uvede informace o možnosti případné integraci s řešením SIEM. |  | IBM Storage Sentinel je navržen s ohledem na snadnou integraci do stávajících bezpečnostních ekosystémů, včetně SIEM řešení. Tato integrace je realizována pomocí standardního syslog protokolu a umožňuje efektivní předávání alertů a bezpečnostních událostí pro centralizovaný monitoring a řízení incidentů. |
|  | Licenčně pokrytá kapacita | * Licenčně je třeba mít pokryto min. **1500 TB** (1365 TiB). | ANO | Nabízené řešení licenčně pokrývá 1500TB (1365 TiB). |
|  | * Řešení musí detekovat ransomware na min. 66,66% kapacity nabízených produkčních diskových polí. | ANO | Nabízené řešení umí detekovat ransomware v rámci celé kapacity nabízených diskových polí. |
|  | Záruka | * Podpora řešení a aktualizace po dobu 6 let | ANO | Nabízené SW komponenty mají podporu na 6let včetně předplacených aktualizací a nových verzí. |
| * Komunikace výhradně v českém jazyce | ANO | Komunikace s podporou je výhradně v českém jazyce. |
| * Záruku garantuje přímo výrobce zařízení | ANO | Záruka je garantována výrobcem SW IBM. |

Tabulka - Detekce ransomware hrozeb

## Výpočetní servery pro ERP SAP

### Popis současného stavu

V každé lokalitě jsou nainstalovány servery 1x IBM Power 880c a 1x IBM Power 824. Servery jsou spravovány HMC konzolí. Servery IBM Power 824 slouží pro účely zálohování. Mezi servery je možné využít LPM – Live Partition Mobility. Jednotlivé IBM Power servery jsou redundantně připojeny do LAN a SAN. V prostředí je provozováno v současnosti 95 LPARů:

|  |  |
| --- | --- |
| **Počet LPARů** | **Typ OS** |
| 12 | RHEL 8.6 |
| 83 | AIX 7.2 |

Tabulka – Popis LPAR

V rámci běžících LPARů je nakonfigurováno celkem 16 HACMP clusterů a 3 HANA Clustery.

V rámci IBM Power je provozována aplikace SAP s DB Oracle, MAX DB a HANA.

### Požadavky na nové řešení

Výpočetní servery pro ERP SAP jsou zařízení určená pro spolehlivý, dlouhodobý běh aplikace SAP. Jejich parametry musí splňovat specifické požadavky současného aplikačního prostředí (Oracle, SAP R/3) i budoucího aplikačního prostředí (HANA, SAP S/4). Servery musí podporovat virtualizaci a umožňovat změny parametrů virtuálních serverů v návaznosti na jednotlivé kroky migračních prací z ERP SAP R3 na ERP SAP4HANA. Parametry pro dimenzování výkonu vychází z detailní analýzy SAP systému Objednatele, které servery musí splňovat, a to jak pro současný stav, tak i s ohledem na plánovanou reimplementaci ERP a budoucí potřeby pro výkonu činnosti Objednatele. Současně je žádoucí, aby řešení nezahrnovalo dočasné servery pro potřeby migrace v cílovém stavu nevyužité (z důvodu provozních i investičních nákladů, licenčních souvislostí, nákladů na datová centra, sítě atd.), ale aby se navrhly servery využitelné co nejefektivněji pro všechny fáze projektu migrace. Servery dále musí splňovat vysoké požadavky na spolehlivost a bezpečnost a umožňovat vybudování vysoce dostupného, geograficky rozděleného prostředí. V neposlední řadě musí být servery podporovány pro běh více instancí (až 14) HANA databází.

Objednatel požaduje pro IS SZIF na platformě SAP dodat dvojici vysoce výkonných serverů kategorie enterprise, vždy 1ks na lokalitu. Servery musí být identické na obou lokalitách a plně redundantní ve všech svých hardware částech. Návrh využití serverů pro provoz SAP musí být v souladu s SAP Note 2230704.

Každý fyzický server musí být připojen k síťové infrastruktuře pomocí technologie Dual-homing (minimálně dva interface do dvou různých přepínačů v jedné lokalitě). Přenosové médium je požadováno minimálně 25Gb SFP+ LC. Pro jednotlivá prostředí (PROD, DEV, TEST, MGMT), musí být síťová vrstva oddělena na úrovni L2 pomocí VLAN. Navíc musí být k dispozici rozhraní pro HANA replikace.

Každý fyzický server musí být připojen k SAN infrastruktuře pomocí technologie Dual-homing (minimálně dva interface do dvou různých Fabriců v rámci dané lokality). Přenosové médium je požadováno minimálně 64Gb SFP+ LC.

Objednatel požaduje využití virtualizace na serverech dílčího bloku „Výpočetní servery pro ERP SAP“. Důvodem je využití sdílení procesorů a možnost mobility virtuálních serverů. Pomocí první zmíněné technologie Objednatel požaduje dynamické realokace CPU zdrojů mezi SAP systémy v rámci standardního provozu. (Bez použití této technologie je nutné navýšit výkonnostní požadavky viz kap. 2.7.3 Požadavky na výkon). Tato dynamická realokace CPU zdrojů bude řízena pomocí priorit v jednotlivých logických oblastech. Druhou zmíněnou funkcionalitou je mobilita virtuálního serveru. Tato funkcionalita zajistí plánované manuální přenesení vybraných prostředí SAP podle provozních a migračních potřeb. Tato funkcionalita musí koexistovat s HA/DR řešením pro oba plánované operační systémy.

### Požadavky na výkon

V produkčním prostředí je požadováno zajištění vysoké dostupnosti pomocí clusterware. Architektura clusterware musí umožnovat rovnoměrné využití zdrojů přes obě lokality.

V případě výpadku jedné lokality Objednatel požaduje, aby systémy prostředí PROD, TEST a MNG mohly být provozovány na jednom serveru v druhé funkční lokalitě.

S ohledem na kombinace prostředí postavené na databázi Oracle s prostředími na databázi HANA a postupnou migrací jednotlivých prostředí musí výkonnostní charakteristiky pokrýt obě tato prostředí.

V následující tabulce jsou uvedena shrnutí výkonových požadavků SAP na jednotlivé oblasti a kombinovaný běh systémů. Požadavek je stanoven s 3-letým horizontem potřeby, kdy hodnoty v tabulce jsou hodnoty předpokládané ve 3-tím roce provozu pro nová prostředí na HANA databázi:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | HANA DB část | | Aplikační část (Suite) | |
|  | *HANA SAPs* | *RAM* | *SD SAPS* | *RAM* |
| Produkce | 372 625 | 17 617 | 245 834 | 1620 |
| HA Produkce | 185 725 | 17 617 | 245 834 | 1 620 |
| Test | 411861 | 22676 | 251 991 | 2096 |
| Vývoj | 81 792 | 3 408 | 82 600 | 520 |
| Ostatní | 80 000 | 11 893 | 64 000 | 364 |
| **Celkem** | **1 132 002** | **73 211** | **870 259** | **6 219** |

Tabulka - Výkonnostní požadavky na první 3 roky

A současný běh nezbytných historických databází:

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Databázová část** | | **Aplikační část** |
|  | **SD SAPs** | **RAM (GB)** | |
| Produkce | 131 131 | 824 | |
| Test | 76 926 | 439 | |
| Vývoj | 38 000 | 202 | |
| Ostatní | 16 000 | 48 | |
| **Celkem** | **262 056** | **1 513** | |

Tabulka - Současné výkonové nároky

Pro optimální využití zdrojů serverů, s ohledem na oscilaci požadavků na zdroje, Objednatel požaduje použít virtualizaci s dynamickým přidělováním zdrojů, nejlépe v automatickém režimu. Ideálním řešením je serveru přidělit základní sadu zdrojů a v případě, kdy jsou tyto zdroje vyčerpány, může být automaticky přidělena sada dalších zdrojů, které si může systém alokovat podle pravidel virtualizační platformy. Dále je nutná možnost systémům za běhu přidávat a odebírat RAM, CPU zdroje a rozšiřovat veškeré souborové systémy, to vše bez výpadku aplikace a s dobou v řádu jednotek minut, během které je změna zdrojů realizována. Pro naplnění licenční politiky a lepší možnosti řízení přidělení zdrojů je třeba, aby bylo možno limitovat počet přidělených jader CPU.

Velikosti jednotlivých databází se budou v průběhu existence poptávané infrastruktury dynamicky měnit a navržený server musí umožňovat dynamické změny LPARů (VMs), jak co do počtu CPU, tak i do velikosti RAM i pro SAP HANA databáze (v souladu se SAP note: 3114051). Uvedené hodnoty SAPs pro aplikační část jsou za předpokladu využití technologie CPU Shared Pool.

Navržený server musí umožňovat současný běh až 14 produkčních SAP HANA databází (SAP note: 2188482).

Výsledný server za předpokladu využití sdílení procesorů musí mít následující parametry:

Celkový výkon dvojice identických serverů: 2 362 368 SD SAPs, RAM 76 026 GB. Tedy výkon 1ks serveru 1 181 184 SAPs a RAM a velikosti 38 013 GB.

Při započtení CPU a RAM zdrojů pro systémový chod je třeba tyto hodnoty navýšit o 68 000 SAPs a 512 GB RAM tedy na **1 249 319 SAPs** a **38 525 GB RAM** na jeden server.

V případě, že bude Dodavatel dodávat jinou generaci nebo variantu procesoru a serveru, tak doloží výpočet výkonu a velikost RAM. Uvedený výkon pro HANA databáze je nutné vždy navýšit o 15% pro CPU (využívající SMT4 pro HANA databáze) a jakékoli omezení možností CPU sharedpoolu musí dimenzování výkonu reflektovat v navýšení hodnot SAPs o 100% oproti uvedeným.

Pro zajištění flexibility prostředí je doporučováno použití technologie, která umožní dynamicky přesouvat logické systémy mezi jednotlivými uzly výpočetního výkonu.

Pro validaci řešení je zapotřebí SAP HANA prostředí otestovat pomocí nástroje HWCCT (SAP HANA HW Configuration Check Tool) dle SAP note: 1943937.

Obecně platí, že pro splnění výše uvedených SAP notes je nutné splnit i požadavky ze SAP note jim podřízených/referovaných.

V produkčním prostředí je požadováno HA dle specifikace níže. Pro vývojové a testovací prostředí je požadováno využití funkčnosti Mobilita Virtuálního Serveru, kde výjimku tvoří testovací systémy WAX, které budou sloužit pro testování konfigurací clusteru produkčních systémů. Je třeba s tímto faktem dále počítat při návrhu architektury řešení.

|  |  |  |  |
| --- | --- | --- | --- |
| **Výpočetní servery pro ERP SAP** | | | |
| **Číslo** | **Název komponenty** | **Part number** | **Počet kusů** |
| 1 | IBM Power E1080 | XXXXX | 2 |

Tabulka - Identifikace komponenty Výpočetní servery pro ERP SAP

Servery musí zejména poskytovat tyto klíčové vlastnosti:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Výpočetní servery pro ERP SAP (2ks)** | | | | |
| **Číslo** | **Vlastnost /komponenta** | **Požadované parametry** | **Splňuje ANO/NE** | **Skutečné parametry/Způsob splnění požadavku** |
|  | Servery Produkční | * Navržené produkční SAP servery musí být kategorie Enterprise pro potřeby kritického systému. | ANO | Nabízené servery jsou z Enterprise kategorie IBM Power serverů. Jedná se o nejvyšší model řady IBM Power a to IBM Power E1080. |
|  | * Počet serverů: 2ks identických parametrů. | ANO | Oba nabízené servery jsou identické. |
|  | * Servery musí být binárně kompatibilní se stávajícími servery Objednatele a umožňovat mobilní transfer virtuálních serverů. | ANO | Nabízené servery jsou binárně kompatibilní se stávající servery Objednatele. Nabízené servery jsou postaveny na platformě IBM Power 10, která umožňuje mobilní transfer virtuálních serverů ze stávajících serverů. |
|  | * Servery musí splňovat požadavky na zajištění provozu jak ve standardním režimu, tak v režimu při výpadku. | ANO | Nabízené servery splňují požadavky na provoz ve standardním režimu i během výpadku. |
|  | Výkon | * Objednatel požaduje min. výkon CPU pro jeden server: **1 249 319** SAPs. | ANO | Každý z nabízených serverů má výkon 1 253 469 SAPs. |
|  | Rozšiřitelnost výkonu | * Navržené řešení musí umožňovat rozšíření prostým přidáním nebo aktivací procesorů. | ANO | Nabízené servery mají osazeno 192 CPU. Aktivovaných CPU je 147. Rozšíření je možno provést pouhou aktivací procesorů. |
|  | * Objednatel požaduje min. rozšiřitelnost výkonu CPU pro jeden server: **1 584 990** SAPs. | ANO | Každý z nabízených serverů je možné rozšířit na výkon CPU 1 637 184 SAPs. |
|  | RAM kapacita | * Objednatel požaduje min. kapacitu RAM pro jeden server: **38 912** GB. | ANO | Každý z nabízených serverů je nakonfigurován s 38 912 GB. |
|  | Rozšiřitelnost RAM | * Navržené řešení musí umožňovat rozšíření prostým přidáním nebo aktivací RAM. | ANO | Nabízené servery obsahují dostatečný počet volných RAM slotů pro rozšíření prostým přidáním RAM modulů. Počet volných slotů je 104 v každém serveru. |
|  | * Objednatel požaduje min. rozšiřitelnost RAM pro jeden server: **61 440** GB. | ANO | Nabízené servery umožňují rozšíření RAM až na 65 536 GB. |
|  | * Řešení musí být rozšiřitelné bez nutnosti výměny paměťových modulů (musí zůstat dostatek volných pozic pro přidání). | ANO | Nabízené servery obsahují dostatečný počet volných DDIM slotů pro potřebné rozšíření. Počet volných slotů je 104. |
|  | IO | * Minimální počet IO PCIe pozic: 32. | ANO | Nabízené servery obsahují 32 IO PCIe pozic na jeden server. |
|  | IO – Ethernet 25Gbit | * Minimální požadovaný počet Ethernet rozhraní: 48x min. 25 Gb/s typ SR (osazeny SFP28) pro jeden server. | ANO | Každý z nabízených serverů obsahuje v konfiguraci Ethernet rozhraní 48x port s rychlostí 25Gb/s osazený SFP28 typu SR. |
|  | * Ethernet adaptéry musí být podporovány pro nabízenou virtualizaci, operační systémy a zajištění vysoké dostupnosti. | ANO | Nabízené servery obsahují Ethernet adaptéry, které podporují nabízenou virtualizaci, operační systémy a zajištění vysoké dostupnosti. |
|  | * Dodavatel uvede počet adaptérů nutných pro dosažení požadovaného počtu portů. |  | Každý z nabízených serverů obsahuje v konfiguraci 12ks čtyřportových Ethernet adaptérů. |
|  | IO – Ethernet SR-IOV | * Nabízené Ethernet 25 Gbit adaptéry musí podporovat SR-IOV virtualizační technologii. | ANO | Nabízené servery obsahuji Ethernet adaptéry o rychlosti 25Gb/s. Adaptéry podporují SR-IOV virtualizační technologii. |
|  | IO – Fibre Channel | * Minimální požadovaný počet FC rozhraní: 16 x min. 64 Gb/s (osazeny SPF+) pro jeden server. | ANO | Každý z nabízených serverů obsahuje v konfiguraci FC rozhraní 16x port s rychlostí 64Gb/s osazený SFP+. |
|  | * FC adaptéry musí být podporovány pro nabízenou virtualizaci, operační systémy a zajištění vysoké dostupnosti. | ANO | Nabízené servery obsahují FC adaptéry, které podporují nabízenou virtualizaci, operační systémy a zajištění vysoké dostupnosti. |
|  | * Dodavatel uvede počet adaptérů nutných pro dosažení požadovaného počtu portů. |  | Každý z nabízených serverů obsahuje v konfiguraci 8ks dvouportových FC adaptérů. |
|  | IO – SSD | * Server musí disponovat min. 8 ks NVMe disků o min. kapacitě 1,6 TB každý (disky pro potřeby systémových virtuálních serverů). | ANO | Každý z nabízených serverů obsahuje v konfiguraci 8ks NVME disků o velikosti 1,6TB. |
|  | Virtualizace | * Servery musí podporovat migraci virtuálních serverů ze současného HW na nově dodaný včetně příslušné licence a podpory. | ANO | Nabízené servery podporují migraci virtuálních serverů ze současného HW na nový HW. Nabízené servery obsahují všechny potřebné licence a podporu. |
|  | * Dodávka musí obsahovat licence na virtualizaci pro všechny nabízená procesorová jádra včetně příslušné licenční podpory. | ANO | Každý z nabízených serverů obsahuje v konfiguraci licenci na virtualizaci pro 147 aktivovaných jader včetně podpory na 6 let. |
|  | * Virtualizace musí podporovat současný běh různých verzi OS. | ANO | Virtualizace na nabízených serverech podporuje běh různých verzí OS současně. |
|  | OS – SAP/Oracle | * Součástí dodávky musí být licence big-endien OS (aktuálně je provozován AIX 7.2). | ANO | Každý z nabízených serverů obsahuje v konfiguraci licenci na big-endien OS (AIX) pro 80 jader. |
|  | * Licencí musí být zajištěno min. na 80ks jader pro každý server. | ANO | Každý z nabízených serverů má zajištěnu licenci na 80 ks jader. |
|  | OS – HANA | * Součástí dodávky musí být předplatné OS RHEL nebo SLES for SAP min. na 108ks jader pro každý server.   Zadavatel umožňuje rovnocenné řešení, které bude splňovat požadavky uvedené v kapitole 2.2 Požadavky na certifikaci dodávaných komponent. Dodavatel uvede v takovém případě číslo SAP Note potvrzující kompatibilitu. | ANO | Každý nabízený server obsahuje licence pro 108 jader OS RHEL for SAP. |
|  | * Licence ve verzi certifikované pro provoz SAP/HANA PROD a nonPROD. | ANO | Nabízené servery obsahují licenci Red Hat Enterprise Linux for SAP Solutions for Power LE, která je certifikovaná pro provoz SAP/HANA PROD a nonPROD. |
|  | Clusterware | * Pro zajištění vysoké dostupnosti musí být součástí nabídky licence řešení vysoké dostupnosti pro big-endien OS. | ANO | Nabízené servery obsahují licenci IBM PowerHA SystemMirror, která umožňuje zajistit vysokou dostupnost big-endien OS. |
|  | * Licencí musí být zajištěno min. na 50ks jader pro každý server. | ANO | Každý z nabízených serverů obsahuje licenci na Clusterware na 50 jader. |
|  | * Zajištění vysoké dostupnosti SAP/HANA je součástí příslušné verze RHEL nebo SLES for SAP.   Zadavatel umožňuje rovnocenné řešení, které bude splňovat požadavky uvedené v kapitole 2.2 Požadavky na certifikaci dodávaných komponent. Dodavatel v takovém případě uvede číslo SAP Note potvrzující kompatibilitu. | ANO | Vysoká dostupnost SAP/HANA je zajištěna pomocí Clusterware, který je součásti nabízené licence Red Hat Enterprise Linux for SAP Solutions for Power LE. |
|  | Management /Řídící software | * SW pro zajištění správy musí být součástí dodávky | ANO | SW pro správu je součástí dodávky. |
|  | * Řídící konzole pro virtualizaci (minimálně jedna na každý výpočetní server). | ANO | Součástí dodávky je licence na dvě Hardware Management Console Appliance, které slouží pro správu nabízených serverů. |
|  | Technické vlastnosti a rozměry | * Kompatibilní s RACK 19”. | ANO | Nabízené servery jsou kompatibilní s RACK 19“. |
|  | * Dodavatel uvede velikost v EIA (jednotek U) pro systémovou skříň 19”. |  | 22U. |
|  | * Dodavatel uvede počet a typ napájení (C13 a počet). |  | 16x C13/C14. |
|  | * Dodavatel uvede typický a maximální elektrický příkon. |  | maximální 14 400 watt, typický: 9 950 watt. |
|  | * Dodavatel uvede, jaké jsou požadavky na elektrické jištění. |  | 3 fáze, 16A. |
|  | Napájení | * Zařízení musí mít redundantní napájecí zdroje 250VAC, vyměnitelné za chodu. | ANO | Každý nabízený server má redundantní napájecí zdroje 250VAC vyměnitelné za chodu. |
|  | Provozní a výkonnostní monitoring | * Řešení musí umožnit sledování využití fyzických serverů virtuálními servery, a to minimálně v parametrech:   + Procesorový výkon a CPU shared pool;   + Operační paměť;   + Fyzické adaptéry (včetně SR-IOV); | ANO | Nabízené řešení umožňuje sledovat následující parametry:   * Procesorový výkon a CPU shared pool; * Operační paměť; * Fyzické adaptéry (včetně SR-IOV). |
|  | * Řešení musí poskytovat Alerty a agenty pro virtualizaci a nabízené operační systémy. | ANO | Nabízené řešení umožňuje sledovat, zasílat alerty a poskytuje agenty pro virtualizaci a nabízené operační systémy. |
|  | Záruka | * Na HW komponenty 6 let, 24x7, oprava do 24h | ANO | Nabízené servery mají záruku na HW komponenty 6let s dostupností 24x7 a opravou do 24h. |
| * Na SW komponenty 6 let podpora včetně předplacených aktualizací a nových verzí | ANO | Nabízené SW komponenty mají podporu na 6let včetně předplacených aktualizací a nových verzí. |
| * Komunikace výhradně v českém jazyce | ANO | Komunikace s podporou je výhradně v českém jazyce. |
| * Záruku garantuje přímo výrobce zařízení | ANO | Záruka je garantována výrobcem zařízení. |

Tabulka - Technické parametry HW pro ERP SAP

## Zálohovací a dohledové servery

### Popis současného stavu

Objednatel používá pro účely zálohování nástroj IBM Spectrum Protect s klienty pro zálohování souborových systémů OS AIX/Linux/Windows a aplikací – Oracle DB, SAP, SAP HANA, VMWARE VM instalovaný na dvou clustrovaných serverech umístěných ve dvou lokalitách.

### Požadavky na nové řešení

Objednatel dále požaduje servery pro systémové úlohy, především zálohování a dohled. Vhodné jsou 2-socketové servery s dostatečnou propustností především pro potřeby zálohování.

|  |  |  |  |
| --- | --- | --- | --- |
| **Zálohovací a dohledový server** | | | |
| **Číslo** | **Název komponenty** | **Part number** | **Počet kusů** |
| 1 | IBM Power S1024 | XXXXX | 2 |

Tabulka - Identifikace komponenty Zálohovací a dohledové servery

Požadované parametry serveru pro jednu lokalitu (celkem jsou poptávány 2 servery):

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Servery pro zálohování a dohled (2 ks)** | | | | |
| **Číslo** | **Vlastnost**  **/ komponenta** | **Požadované parametry** | **Splňuje ANO/NE** | **Skutečné parametry/Způsob splnění požadavku** |
|  | Servery Zálohovací a dohledové | * Navržené Zálohovací servery musí být dle doporučení dodavatele zálohovacího řešení. | ANO | Nabízené servery splňují doporučené požadavky zálohovacího řešení. |
|  | * Servery musí být binárně kompatibilní se stávajícími servery Objednatele a umožňovat mobilní transfer virtuálních serverů. | ANO | Nabízené servery jsou binárně kompatibilní se stávající servery Objednatele. Nabízené servery jsou postaveny na platformě IBM Power 10, která umožňuje mobilní transfer virtuálních serverů ze stávajících serverů. |
|  | * Servery musí splňovat požadavky na zajištění provozu jak ve standardním režimu, tak v režimu při výpadku. | ANO | Nabízené servery splňují požadavky na provoz ve standardním režimu i během výpadku. |
|  | Výkon | * Požadovaný výkon je min. 200000 SAPs. | ANO | Každý z nabízených serverů má výkon 222 003 SAPs. |
|  | Rozšiřitelnost výkonu | * Není vyžadována. | ANO | U nabízených serverů je možné výkon rozšířit pouze výměnou osazených CPU. |
|  | RAM kapacita | * Objednatel požaduje min. kapacitu RAM pro jeden server: **1** TB | ANO | Každý nabízených serverů obsahuje 1TB RAM. |
|  | Rozšiřitelnost RAM | * Navržené řešení musí umožňovat rozšíření prostým přidáním RAM stejného modulu. | ANO | Nabízené servery obsahují dostatečný počet volných RAM slotů pro potřebné rozšíření prostým přidáním RAM modulů. Počet volných slotů je 24. |
|  | * Objednatel požaduje min. rozšiřitelnost RAM pro jeden server: **4** TB. | ANO | Nabízené servery umožňují rozšíření RAM až na 4TB. |
|  | * Řešení musí být rozšiřitelné bez nutnosti výměny paměťových modulů (musí zůstat dostatek volných pozic pro přidání). | ANO | Nabízené servery obsahují dostatečný počet volných RAM slotů pro potřebné rozšíření prostým přidáním RAM modulů. Počet volných slotů je 24. |
|  | IO | * Minimální počet IO PCIe pozic: 10. | ANO | Nabízené servery obsahují 10 IO PCIe pozic na jeden server. |
|  | IO – Ethernet 25Gbit | * Minimální požadovaný počet Ethernet rozhraní: 8x min. 25 Gb/s typ SR (osazeny SFP28) pro jeden server. | ANO | Každý z nabízených serverů obsahuje v konfiguraci Ethernet rozhraní 8x port s rychlostí 25Gb/s osazený SFP28 typu SR. |
|  | * Ethernet adaptéry musí být podporovány pro nabízenou virtualizaci, operační systémy a zajištění vysoké dostupnosti. | ANO | Nabízené servery obsahují Ethernet adaptéry, které podporují nabízenou virtualizaci, operační systémy a zajištění vysoké dostupnosti. |
|  | * Dodavatel uvede počet adaptérů nutných pro dosažení požadovaného počtu portů. |  | Každý z nabízených serverů obsahuje v konfiguraci 4ks dvouportových Ethernet adaptérů. |
|  | IO – Ethernet SR-IOV | * Nabízené Ethernet min. 25 Gb/s adaptéry musí podporovat SR-IOV virtualizační technologii. | ANO | Nabízené servery obsahuji Ethernet adaptéry o rychlosti 25Gb/s. Adaptéry podporují SR-IOV virtualizační technologii. |
|  | IO – Fibre Channel | * Minimální požadovaný počet FC rozhraní: 8x min. 64 Gb/s (osazeny SFP+) pro jeden server. (Pozn.: použití 4-port FC adaptérů či alternativní varianty s 2-port jsou přípustné). | ANO | Každý z nabízených serverů obsahuje v konfiguraci FC rozhraní 8x port s rychlostí 64Gb/s osazený SFP+. |
|  | * FC adaptéry musí být podporovány pro nabízenou virtualizaci, operační systémy a zajištění vysoké dostupnosti. | ANO | Nabízené servery obsahují FC adaptéry, které podporují nabízenou virtualizaci, operační systémy a zajištění vysoké dostupnosti. |
|  | * Dodavatel uvede počet adaptérů nutných pro dosažení požadovaného počtu portů. |  | Každý z nabízených serverů obsahuje v konfiguraci 4ks dvouportových FC adaptérů. |
|  | IO – SSD | * Server musí disponovat min. 8 ks NVMe disků o min. kapacitě 500 GB každý (disky pro potřeby systémových virtuálních serverů). | ANO | Každý z nabízených serverů obsahuje v konfiguraci 8ks NVME disků o velikosti 800GB. |
|  | Virtualizace | * Servery musí podporovat migraci virtuálních serverů ze současného HW na nově dodaný včetně příslušné licence a podpory. | ANO | Nabízené servery podporují migraci virtuálních serverů ze současného HW na nový HW. Nabízené servery obsahují všechny potřebné licence a podporu. |
|  | * Dodávka musí obsahovat licence na virtualizaci pro všechny nabízená procesorová jádra včetně příslušné licenční podpory. | ANO | Každý z nabízených serverů obsahuje licenci na virtualizaci pro všechna jádra včetně podpory na 6 let. |
|  | * Virtualizace musí podporovat současný běh různých verzi OS. | ANO | Virtualizace na nabízených serverech podporuje běh různých verzí OS současně. |
|  | OS – Backup | * Součástí dodávky musí být licence big-endien OS (aktuálně je provozován AIX 7.2). | ANO | Nabízené servery obsahují licence na big-endien OS. Nabízené servery obsahují licenci na AIX pro 24 jader. |
|  | Clusterware | * Pro zajištění vysoké dostupnosti musí být součástí nabídky licence řešení vysoké dostupnosti pro big-endien OS. | ANO | Nabízené servery obsahují licenci IBM PowerHA SystemMirror, která umožňuje zajistit vysokou dostupnost big-endien OS. |
|  | * Licencí musí být zajištěno min. na 24ks jader pro každý server. | ANO | Každý z nabízených serverů obsahuje licenci na Clusterware na všech 24 jader. |
|  | Technické vlastnosti a rozměry | * Kompatibilní s RACK 19”. | ANO | Nabízené servery jsou kompatibilní s RACK 19“. |
|  | * Dodavatel uvede velikost v EIA (jednotek U) pro systémovou skříň 19”. |  | 4U. |
|  | * Dodavatel uvede počet a typ napájení (C13/14 nebo C19/C20 a počet). |  | 2x C13/C14. |
|  | * Dodavatel uvede typický a maximální elektrický příkon. |  | maximální 1900 watt, typický: 1370 watt. |
|  | * Dodavatel uvede, jaké jsou požadavky na elektrické jištění. |  | 3 fáze, 16A. |
|  | Napájení | * Zařízení musí mít redundantní napájecí zdroje 250VAC, vyměnitelné za chodu. | ANO | Každý nabízený server má dva redundantní zdroje 250VAC vyměnitelné za chodu. |
|  | Záruka | * Na HW komponent 6 let, 24x7, oprava do 24h. | ANO | Nabízené servery mají záruku na HW komponenty 6let s dostupností 24x7 a opravou do 24h. |
| * Na SW komponenty 6 let podpora včetně předplacených aktualizací a nových verzí. | ANO | Nabízené SW komponenty mají podporu na 6let včetně předplacených aktualizací a nových verzí. |
| * Komunikace výhradně v českém jazyce. | ANO | Komunikace s podporou je výhradně v českém jazyce. |
| * Záruku garantuje přímo výrobce zařízení. | ANO | Záruka je garantována výrobcem zařízení. |

Tabulka - Technické parametry HW pro zálohování a dohled

## Výpočetní servery pro virtualizaci platformy x86

### Popis současného stavu

Objednatel v současné době provozuje cluster dvanácti 1U fyzických x86 serverů na platformě VMware. Prostředí Intelové virtualizace je složeno ze dvou lokalit (sál A, sál B). V každé z lokalitě je umístěno šest serverů HPE sloužící k běhu virtualizační vrstvy VMware 7.0.

Konektivita mezi jednotlivými uzly clusteru je postavena na 10GbE ethernetu v redundantním zapojení. Přístup ke sdílenému VMFS datastore je prostřednictví 16Gb Fiber Channel SAN. Vysoká dostupnost celého systému je zajištěna pomoci technologie VMware High Availibility, které trvale monitoruje všechny fyzické servery a v případě detekce výpadků hardware, umožní přesunout veškerý virtualizovaný provoz na jiný fyzický uzel clusteru. Správa celého prostředí probíhá pomocí VMware vCenter serveru. Veškeré prvky této virtualizační infrastruktury jsou na konci životního cyklu v důsledku brzkého konce podpory ze strany výrobce hardware a dodavatele software.

Primární provozované operační systémy jsou postaveny na Linuxové distribuci od společnosti RedHat určené pro SAP aplikace a s neomezeným počtem provozovaných virtuálních serverů.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Zařízení** | **CPU Model** | **Počty CPU** | **Počty**  **jader**  **na**  **CPU** | **Celkový**  **počet**  **jader** | **Velikost**  **RAM** |
| HPE ProLiant DL360 Gen10 | Intel(R) Xeon(R) Gold 6152 CPU @ 2.10GHz | 2 | 22 | 44 | 523 940 |
| HPE ProLiant DL360 Gen10 | Intel(R) Xeon(R) Gold 6152 CPU @ 2.10GHz | 2 | 22 | 44 | 523 940 |
| HPE ProLiant DL360 Gen10 | Intel(R) Xeon(R) Gold 6152 CPU @ 2.10GHz | 2 | 22 | 44 | 523 940 |
| HPE ProLiant DL360 Gen10 | Intel(R) Xeon(R) Gold 6152 CPU @ 2.10GHz | 2 | 22 | 44 | 523 940 |
| HPE ProLiant DL360 Gen10 | Intel(R) Xeon(R) Gold 6258R CPU @ 2.70GHz | 2 | 28 | 56 | 1 572 516 |
| HPE ProLiant DL360 Gen10 | Intel(R) Xeon(R) Gold 6258R CPU @ 2.70GHz | 2 | 28 | 56 | 1 572 516 |
| HPE ProLiant DL360 Gen10 | Intel(R) Xeon(R) Gold 6152 CPU @ 2.10GHz | 2 | 22 | 44 | 523 940 |
| HPE ProLiant DL360 Gen10 | Intel(R) Xeon(R) Gold 6152 CPU @ 2.10GHz | 2 | 22 | 44 | 523 940 |
| HPE ProLiant DL360 Gen10 | Intel(R) Xeon(R) Gold 6152 CPU @ 2.10GHz | 2 | 22 | 44 | 523 940 |
| HPE ProLiant DL360 Gen10 | Intel(R) Xeon(R) Gold 6152 CPU @ 2.10GHz | 2 | 22 | 44 | 523 940 |
| HPE ProLiant DL360 Gen10 | Intel(R) Xeon(R) Gold 6258R CPU @ 2.70GHz | 2 | 28 | 56 | 1 572 516 |
| HPE ProLiant DL360 Gen10 | Intel(R) Xeon(R) Gold 6258R CPU @ 2.70GHz | 2 | 28 | 56 | 1 572 516 |

Tabulka - Seznam fyzického HW

Celkem je provozováno 314 virtuálních serverů ve dvou VMware clusterech a jsou rozděleny dle operačních systémů takto:

|  |  |
| --- | --- |
| **Počet VM** | **Typ OS** |
| 245 | RHEL 7.8 |
| 53 | Windows Server 2016 a 2019 |
| 4 | CentOS 7.8 |
| 1 | FreeBSD |
| 3 | Debian 6.7 |
| 5 | Linux |
| 3 | SUSE 11 |

Tabulka - Popis VM

V prostředí je provozováno 23 instancí PostgreSQL. 18 instancí je provozováno v PostgreSQL Clusteru.

### Požadavky na nové řešení

Virtualizační platforma x86 bude sloužit pro provoz všech nezbytných podpůrných systémů pro výpočetní SAP servery a další agendy Objednatele. Musí být tedy dimenzována s ohledem na dostatečný provozní výkon, včetně rezervy pro případnou automatickou aktivaci scénáře pro Failover a možné budoucí migrace nových či přesun externě provozovaných agend Objednatele a také s dostatečnou robustností a odolností proti výpadku. Objednatel počítá s instalací HW serverů do dvou fyzicky oddělených datových sálů, s možností budoucí instalace až do dvou fyzicky oddělených datových center. Minimální počet nodů je, i po započtení výše zmíněných rezerv, stanoven na osm serverů v každé lokalitě a je zároveň stanoven tak, aby bylo možné celou kritickou infrastrukturu provozovat i z jedné lokality v případě aktivace DR scénáře. S ohledem na kompatibilitu při migraci ze současné infrastruktury je požadováno osazení každého ze serverů dvěma procesory, a to v nejnovější generaci (v prostředí zadavatele jsou aktuálně používány procesory od společnosti Intel, viz tabulka Seznam fyzického HW). Dále bude každý server disponovat minimálně 1TB RAM, osazenými rovnoměrně ke každému procesoru pro nejvýkonnější konfiguraci a možnosti budoucího rozšíření. Servery budou bez interních disků pouze s dvojicí M.2 NVMe disků o kapacitě alespoň 960GB, pro okamžitý náběh libovolného virtualizačního hypervizoru. Veškerá data budou uložena na sdílených diskových polích. Přístup serverů k těmto diskovým polím bude prostřednictvím dvoucestného zapojení do SAN přes Dual-Port Host Bus Adapter o rychlosti alespoň 64Gbps. Komunikace mezi jednotlivými uzly clusteru, lokalitami a okolními prvky infrastruktury bude zajištěna redundantním 10/25Gbps ethernet konektivitou s optickým SFP rozhraním. Pro každý uzel clusteru jsou vyžadovány aspoň čtyři 10/25Gb ethernet porty na fyzicky oddělených kartách. Vzdálená správa všech serverů bude mít dedikovaný 10/100/1000 BaseT port.

S ohledem na náročnost správy infrastruktury a omezených personálních zdrojů Objednatele, Objednatel požaduje možnost integrace rozhraní vzdálené správy a dohledu do prostředí management nástroje hypervizoru a případně možnost integrace tohoto rozhraní i do dalších využívaných aplikací prostřednictvím standardizovaného aplikačního interface např. REST-API. Z důvodů snadné manipulace, poskytování servisu a rozšiřitelnosti požaduje Objednatel provedení serveru pro osazení do systémové skříně (rack) o velikosti 2U.

Z důvodu snadné migrace, návaznosti na stávající systém a požadavky SAP Notes, vyžaduje Objednatel virtualizační platformu postavenou na VMware vSphere v aktuální verzi. Součástí nové infrastruktury bude tedy i pořízení nových licencí pro virtualizační hypervizor. Veškeré prvky nabízené infrastruktury musí tedy být podporované pro běh hypervizoru VMware ESXi. Také Vysoká dostupnost prostředí x86 bude realizována pomocí nativních prostředků VMware.

Z důvodu snadné migrace a přechodu na nové prostředí doporučuje Objednatel obnovení stávajících licencí operačního systému RedHat Enterprise Linux v subscribci verze Standard. Pro SAP prostředí s neomezeným počtem virtuálních serverů v subscribci verzi **RHEL for SAP applications** a produkční podporou pro tyto licence v režimu 24x7 po dobu 6 let. Pro VM Ware prostředí je požadována subscribce **RHEL for Virtual Datacenters** včetně Add-on **Satellite** a **High Availability.** V případě, že Dodavatel využije alternativní řešení licencí operačního systému v souladu s možností uvedenou v tabulce níže, musí být produkční podpora pro tyto licence zajištěna v režimu 24x7 po dobu 6 let.

|  |  |  |  |
| --- | --- | --- | --- |
| **x86 Virtualizační infrastruktura** | | | |
| **Číslo** | **Název komponenty** | **Part number** | **Počet kusů** |
| 1 | Lenovo ThinkSystem SR650 V3 | XXXXX | 18 |

Tabulka - Identifikace komponenty x86 Virtualizační infrastruktura

Požadované parametry serverů umístěných dohromady v obou lokalitách:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **x86 Virtualizační infrastruktura (18ks)** | | | | |
| **Číslo** | **Vlastnost/komponenta** | **Požadované parametry** | **Splňuje ANO/NE** | **Skutečné parametry/Způsob splnění požadavku** |
|  | Technické vlastnosti a rozměry | * Kompatibilní s RACK 19”. | ANO | Form factor: 2U  výška: 86.5 mm  šířka: 482.0 mm  Hloubka: 763.7 mm. |
|  | * Dodavatel uvede velikost v EIA (jednotek U) pro systémovou skříň 19”. |  | 2U. |
|  | * Dodavatel uvede počet a typ napájení (C13/14 nebo C19/C20 a počet). |  | 36ks 2.8m, 13A/100-250V, C13 to C14 Jumper Cord (celkem 2ks na 1 server). |
|  | * Dodavatel uvede elektrický příkon při 70% a 100% utilizaci pro jeden server. |  | Pro navrženou konfiguraci serveru:  elektrický příkon při 70% pro jeden server: 568,4 W,  elektrický příkon při 100% utilizaci pro jeden server: 967,2 W. |
|  | * Dodavatel uvede teplotní vyzařování při 70% a 100% utilizaci pro jeden server |  | Pro navrženou konfiguraci serveru:  teplotní vyzařování při 70% pro jeden server: 1939,2 BTU/Hr,  teplotní vyzařování při 100% pro jeden server: 3300,2 BTU/Hr. |
|  | * Beznástrojové kolejnice pro montáž do racku. | ANO | Nabízené servery obsahují ThinkSystem Toolless Slide Rail Kit v2 Enhanced with 2U CMA tzn. beznástrojové kolejnice pro montáž do racku. |
|  | Výkon | * Nabízené řešení musí obsahovat min. 2 procesory nejnovější generace s 28 jádry/CPU. | ANO | Nabízené servery mají 2 procesory (CPU) Intel Xeon Gold 5520+ 28C 2.2GHz. |
|  | * Minimální výkon dle benchmarku SPEC CPU2017 (www.spec.org) sloupec Baseline ke dni zahájení zadávacího řízení:   + Integer Rates – 500   + Floating Point Rates – 630 | ANO | Nabízené servery mají tyto parametry dle benchmarku SPEC CPU2017.  Integer Rates – 509,  Floating Point Rates – 635. |
|  | RAM kapacita | * Objednatel požaduje min. kapacitu RAM pro jeden server: **1** TB. | ANO | Nabízená konfigurace jednoho serveru má 1TB RAM, složeno z  16ks ThinkSystem 64GB TruDDR5 5600MHz (2Rx4) RDIMM . |
|  | * Typ DDR5. | ANO | Nabízená konfigurace serverů má RAM typu DDR5, složeno z modulů  ThinkSystem 64GB TruDDR5 5600MHz (2Rx4) RDIMM. |
|  | * Rychlost paměťových modulů min. 5600MHz. | ANO | Nabízená konfigurace servrů má rychlost paměťových modulů 5600MHz, složeno z modulů  ThinkSystem 64GB TruDDR5 5600MHz (2Rx4) RDIMM. |
|  | Rozšiřitelnost RAM | * Navržené řešení musí umožňovat rozšíření prostým přidáním RAM stejného modulu. | ANO | Nabízené servery mají podporu až 32ks RAM modulů TruDDR5 3DS/RDIMMs.  Dodaná konfigurace bude 16ks ThinkSystem 64GB TruDDR5 5600MHz (2Rx4) RDIMM na 1 server. |
|  | * Řešení musí obsahovat min. 32 paměťových slotů s rozšiřitelností až na min. **2** TB při využití stávajících modulů. | ANO | Nabízené servery mají podporu až 32x TruDDR5 3DS/RDIMMs.  Dodaná konfigurace bude 16ks ThinkSystem 64GB TruDDR5 5600MHz (2Rx4) RDIMM na 1 server. Přidáním dalších 16ks ThinkSystem 64GB TruDDR5 5600MHz (2Rx4) RDIMM na 1 server bude cílová kapacita RAM 2TB. |
|  | IO - SSD | * Server musí disponovat min. 2 ks M.2 NVMe disků o min. kapacitě 960 GB každý v zapojení HW RAID1, umožňující boot OS nebo hypervizoru. | ANO | Nabízené servery disponují 2 ks ThinkSystem M.2 PM9A3 960GB Read Intensive NVMe PCIe 4.0 x4 NHS SSD v zapojení HW RAID 1 a umožnují boot hypervizoru nebo OS. |
|  | RAID Řadič | * Bez interního RAID řadiče. | ANO | Nabízené servery jsou bez interního RAID řadiče. |
|  | * Dedikovaný slot pro budoucí osazení řadiče. | ANO | Nabízené servery mají dedikovaný slot pro budoucí osazení RAID řadiče. |
|  | IO | * Minimální počet IO PCIe pozic: 10. | ANO | Nabízené servery disponují až 12 IO PCIe pozic. |
|  | * OCP slot. | ANO | Nabízené servery mají 1x OCP 3.0 slot. |
|  | * Dedikovaný slot pro RAID řadič. | ANO | Nabízené servery mají dedikovaný slot pro RAID řadič. |
|  | IO – Ethernet 25Gbit | * Minimální požadovaný počet Ethernet rozhraní: 4x min. 25 Gb/s typ SR (osazeny SPF28) pro jeden server. | ANO | Nabízené servery mají každý 4x 25Gb/s ethernet rozhraní pomocí 2x ThinkSystem Broadcom 57414 10/25GbE SFP28 2-Port OCP Ethernet Adapter.  Celkem tedy 4x port osazený s Lenovo 25Gb SR SFP28 Ethernet na jeden swerver. |
|  | * Řešení musí obsahovat min. 2 ks oddělených síťových karet. | ANO | Nabízené servery mají 2 ks ThinkSystem Broadcom 57414 10/25GbE SFP28 2-Port OCP Ethernet Adapter. |
|  | * Dodavatel uvede počet adaptérů nutných pro dosažení požadovaného počtu portů. |  | 2ks. |
|  | IO – Fibre Channel | * Minimální požadovaný počet FC rozhraní: 2x min. 64 Gb/s (osazeny SPF+) pro jeden server. | ANO | Nabízené servery mají každý 2x 64Gb/s FC rozhraní pomocí 1x ThinkSystem Emulex LPe36002 64Gb 2-port PCIe Fibre Channel Adapteru. |
|  | * Dodavatel uvede počet adaptérů nutných pro dosažení požadovaného počtu portů. |  | 1ks. |
|  | IO – ostatní zařízení | * VGA port, min. 3x USB generace 3.1 na zadní straně serveru. | ANO | Nabízené servery mají VGA port 1x, USB 3.1 G1 3x port na zadní stěně serveru. |
|  | * VGA port a min. 2x USB z čelní strany serveru (Pozn.: jedno z čelních USB může sloužit také pro přístup na servisní procesor serveru). | ANO | Nabízené servery mají VGA port 1x, USB 3.1 G1 1x port, USB 2.0 s XClarity Mobile support funkcí 1x port z čelní strany serveru. |
|  | * Port pro připojení diagnostického displeje. | ANO | Nabízené servery mají ThinkSystem 2U V3 EIA Latch with VGA & External Diagnostics Ports. |
|  | Virtualizace | * Servery musí podporovat hypervizor VMware vSphere ESXi. | ANO | Nabízené servery podporují hypervizor VMware vSphere ESXi. |
|  | * Dodávka musí obsahovat virtualizační licence VMware vSphere VVF pro všechny poptávané procesory na min. 6 let včetně podpory. | ANO | Dodávka obsahuje virtualizační licence VMware Cloud Foundation (VCF) v rozsahu 1008 core a včetně 6 let podpory výrobce.  1008 core = 18 (serverů) x 2 (CPU) x 28 (počet core v 1 CPU).  Licence VCF jsou nejvyšší edicí virtualizační licence VMware a mj. zahrnuje všechny produktové funkcionality licence VMware vSphere VVF a mnoho dalších, velmi užitečných funkcionalit pro budoucí rozvoj prostředí SZIF. |
|  | OS - Licence | * RHEL nebo SLES server OS pro SAP na min. 6 let včetně podpory.   Zadavatel umožňuje rovnocenné řešení, které bude splňovat požadavky uvedené v kapitole 2.2 Požadavky na certifikaci dodávaných komponent. Dodavatel uvede v takovém případě číslo SAP Note potvrzující kompatibilitu. | ANO | Dodávka obsahuje Red Hat Enterprise Linux for Virtual Datacenters for SAP Solutions, pro 18 virtualizačních serverů (VMware) x86, každý s 2 CPU@28 core na dobu 6 let a s PREMIUM subscription (je požadována 24x7 podpora), tj. 18ks.  Uvedené obsahuje tedy 18xSAP Solutions (HANA), SAP Application, RH Satellite, HA, vše pro neomezený počet virtuálů s OS RHEL na architektuře x86.   * SAP Note 2369910 – nota obsahuje ve čtvrté sekci odkazy na SAP noty o podporovaném HW * SAP Note 1122387 - Linux: SAP Support in virtualized environments * SAP Note 1552925 - Linux: High Availability Cluster Solutions. |
|  | * Aplikace, Licence na celé VMware prostředí s neomezeným množstvím virtuálních systémů. | ANO | Dodávka obsahuje virtualizační licence VMware Cloud Foundation (VCF) v rozsahu 1008 core a včetně 6 let podpory výrobce a tyto licence jsou na celé VMware prostředí s neomezeným množstvím virtuálních systémů.  1008 core = 18 (serverů) x 2 (CPU) x 28 (počet core v 1 CPU).  Licence VCF jsou nejvyšší edicí virtualizační licence VMware a mj. zahrnuje všechny produktové funkcionality licence VMware vSphere VVF a mnoho dalších, velmi užitečných funkcionalit pro budoucí rozvoj prostředí SZIF. |
|  | Napájení | * Zařízení musí mít redundantní napájecí zdroje 250VAC, vyměnitelné za chodu. | ANO | Nabízené servery mají redundantní napájecí zdroje 250VAC vyměnitelné za chodu.  Servery obsahují 2x ThinkSystem 1100W 230V Titanium Hot-Swap Gen2 Power Supply. |
|  | * Certifikace Titanium. | ANO | Nabízení servery a jejich zdroje mají certifikaci Titanium. |
|  | * Výkon jednoho zdroje minimálně 1100 W. | ANO | Nabízené servery a jejich zdroje mají 2x ThinkSystem 1100W 230V Titanium Hot-Swap Gen2 Power Supply. |
|  | Řídící software | * Vzdálené správa s dedikovaným vlastním portem RJ-45 a možností převzít plně vzdálené ovládání serveru. | ANO | Nabízené řešení podporuje Vzdálenou správa s dedikovaným vlastním portem RJ-45 a možností převzít plně vzdálené ovládání serveru a to pomocí, Lenovo XClarity (XCC2) Platinum. |
|  | * Možnost redundantního plně dedikovaného min. 1Gb RJ-45 management portu. | ANO | Nabízené řešení podporuje možnost redundantního plně dedikovaného min. 1Gb RJ-45 management portu. |
|  | * Podpora standardů IPMI (minimálně verze 2.0), SNMP (verze 3), CIM-XML, REST a RedFish. | ANO | Nabízené řešení podporuje standardy IPMI verze 2.0, SNMP verze 3.0, CIM-XML, REST a RedFish. |
|  | * Možnost nahrávání záznamu bootu serveru a pádu serveru. | ANO | Nabízené řešení podporuje možnost nahrávání záznamu bootu serveru a pádu serveru. |
|  | * Možnost vzdáleného přístupu k ISO a IMG image souborů (minimálně pomocí protokolů: HTTPS, SFTP, CIFS, a NFS). | ANO | Nabízené řešení podporuje možnost vzdáleného přístupu k ISO a IMG image souborů pomocí protokolů HTTPS, SFTP, CIFS, a NFS.  Řešení Lenovo XClarity XCC2 Platinum. |
|  | * Možnost sdílet jednu virtuální konzoli více uživateli. | ANO | Nabízené řešení podporuje možnost sdílet jednu virtuální konzoli více uživateli.  Řešení Lenovo XClarity XCC2 Platinum. |
|  | * Podpora standardních webových prohlížečů a HTML5. | ANO | Nabízené řešení podporuje standardní webové prohlížeče a HTML5.  Řešení Lenovo XClarity XCC2 Platinum. |
|  | * Možnost blokace konkrétní IP adresy. | ANO | Nabízené řešení umožňuje blokaci konkrétní IP adresy.  Řešení Lenovo XClarity XCC2 Platinum. |
|  | * Real-time sledování vytíženosti CPU, paměti a spotřeby, možnost Power cappingu (včetně historických dat). | ANO | Nabízené řešení umožňuje real-time sledování vytíženosti CPU, paměti a spotřeby, možnost Power cappingu (včetně historických dat).  Řešení Lenovo XClarity XCC2 Platinum. |
|  | * Řešení musí poskytovat možnost asistované instalace OS bez dalších nástrojů, médií, ISO apod. | ANO | Nabízené řešení poskytuje možnost asistované instalace OS bez dalších nástrojů, médií, ISO apod.  Řešení Lenovo XClarity XCC2 Platinum. |
|  | * Řešení musí poskytovat nejvyšší licence pro správu serveru bez jakéhokoli omezení funkcionalit/doby/provozu/počtu spravovaných serverů. | ANO | V rámci dodávky jsou nejvyšší licence pro správu serveru bez jakéhokoli omezení funkcionalit/doby/provozu/počtu spravovaných serverů.  Řešení Lenovo XClarity XCC2 Platinum. |
|  | * Podpora proaktivních upozornění využívající technologii S.M.A.R.T. a PFA. | ANO | Nabízené řešení podporuje proaktivní upozornění využívající technologii S.M.A.R.T. a PFA.  Řešení Lenovo XClarity XCC2 Platinum. |
|  | * Slot pro micro SD kartu o kapacitě alespoň 4GB. | ANO | Nabízené servery mají slot pro micro SD kartu o kapacitě až 4GB.  Řešení Lenovo XClarity XCC2 Platinum. |
|  | * Možnost správy a synchronizace konfigurace a úrovně firmware pro několik serverů najednou. | ANO | Nabízení řešení má možnost správy a synchronizace konfigurace a úrovně firmware pro několik serverů najednou.  Řešení Lenovo XClarity XCC2 Platinum. |
|  | Provozní a výkonnostní monitoring | * Časově neomezená licence na hromadnou správu serverů, inventarizace a alerting. | ANO | V rámci dodávky je časově neomezená licence na hromadnou správu serverů, inventarizace a alerting.  Řešení Lenovo XClarity XCC2 Platinum. |
|  | * Možnost hromadného sledováni a upgrade úrovní FW jednotlivých komponent serverů. | ANO | Nabízené řešení umožňuje hromadného sledováni a upgrade úrovní FW jednotlivých komponent serverů.  Řešení Lenovo XClarity XCC2 Platinum. |
|  | * Call Home funkce. | ANO | Nabízené řešení má Call Home funkce.  Řešení Lenovo XClarity XCC2 Platinum. |
|  | * Plug-in do management nodů virtualizačních hypervizorů (minimálně VMware vCenter, VMware Aria Suite, Microsoft Admin Center, Microsoft System Center, Nagios). | ANO | Nabízené řešení má plug-in do management nodů virtualizačních hypervizorů VMware vCenter, VMware Aria Suite, Microsoft Admin Center, Microsoft System Center, Nagios. |
|  | * Podpora REST-API a Redfish standardů. | ANO | Nabízené řešení má podporu REST-API a Redfish standardů. |
|  | * Podpora standardních Webových prohlížečů a HTML5. | ANO | Nabízené řešení má podporu standardních webových prohlížečů a HTML5. |
|  | * Software musí být bezagentový. | ANO | Nabízený software je bezagentový. |
|  | Záruka | * Na HW komponenty 6 let, 24x7, oprava do 24h. | ANO | Dodávaná záruka HW je 6 let, 24x7, oprava do 24h.  Lenovo Essential Service - 5Yr 24x7 24Hr po dobu 6 let. |
| * Na SW komponenty 6 let podpora včetně předplacených aktualizací a nových verzí. | ANO | Dodávána záruka je:  Lenovo Essential Service - 5Yr 24x7 24Hr po dobu 6 let.  VMware včetně 6 let podpory výrobce.  Red Hat na dobu 6 let a s PREMIUM subscription (je požadována 24x7 podpora). |
| * Komunikace výhradně v českém jazyce. | ANO | Komunikace s podporou je výhradně v českém jazyce. |
| * Záruku garantuje přímo výrobce zařízení. | ANO | Záruka je garantována výrobcem zařízení Lenovo, VMware, Red Hat. |

Tabulka - Technické parametry pro platformu x86

## Systémový Monitoring

### Popis současného stavu

Objednatel v současné době používá pouze systémový monitoring na platformě Zabbix, který je v jeho vlastnictví. .

### Požadavky na nové řešení

Objednatel požaduje provedení migrace a následnou konfiguraci tohoto systému na nově dodaný HW včetně všech souvisejících nastavení, kterou musí kompletně funkčně pokrývat. Monitorovací systém musí být univerzální a podporovat širší spektrum technologií, s ohledem na jejich využití do budoucna (především kontejnerové platformy).

### Funkční požadavky

* Monitorování infrastruktury a operačních systémů;
* Monitorování platformy SAP;
* Monitorování VMware vSphere;
* Monitorování kontejnerů a Kubernetes;
* Syntetické monitorování z libovolných lokalit;
* Správa událostí a upozornění dle předem stanovených pravidel;
* Vytváření vlastních dashboardů;
* Sledování úrovně služeb (SLO);
* Dynamická topologie a zobrazení závislostí mezi jednotlivými vrstvami aplikace a infrastruktury;
* Systémové REST API;
* Přehledné webové uživatelské rozhraní;

### Systémové a HW požadavky

Objednatel požaduje, aby nasazení serverové (backendové) části monitorovacího systému bylo v lokálním prostředí (on-premise) na fyzickém nebo virtuálním serveru x86 s operačním systémem Linux.

Instalace monitorovacích agentů bude podporována na těchto platformách:

* Linux;
* AIX;
* Windows;
* Kubernetes;
* RedHat OpenShift;

### Požadavky na monitorované technologie

Systém bude podporovat monitorování minimálně následujících technologií:

* Operační systémy (Linux, Windows, AIX);
* Java Virtual Machine;
* Oracle databáze;
* PostgreSQL databáze;
* IBM Power HMC;
* VMware vCenter;
* SAP Solution Manager;
* SAP with ABAP;
* SAP HANA;

Systém pro monitoring infrastruktury bude nabízet možnost provozu s vysokou dostupností.

Základní granularita měření bude min. 1 sekunda s následnou časovou agregací dle konfigurovatelných pravidel.

Řešení bude splňovat požadavky na ochranu dat dle pravidel GDPR.

S ohledem na komplexnost a očekávané změny počtu instancí Objednatel požaduje, aby monitorovací systém byl licencován tak, aby licence nebyly vázány na konkrétní systém nebo technologii a aby bylo možné je v rámci prostředí libovolně přeskupovat. Licenční metrika musí zohledňovat pouze dané monitorované prostředí (např. dle počtu virtuálních serverů) a musí v sobě zahrnovat veškerou minimálně nynější funkcionalitu současného monitorovacího systému. Nesmí být samostatně licencována a zpoplatněna serverová část monitorovacího systému, jednotlivé funkcionality, funkční moduly, množství a druh monitorovaných stavů či množství uložených dat.

|  |  |  |  |
| --- | --- | --- | --- |
| **Systémový monitoring** | | | |
| **Číslo** | **Název komponenty** | **Part number** | **Počet kusů** |
| 1. | GCMP for HA cluster, Unlimited Device | XXXXX | 1 |

Tabulka - Identifikace komponenty Systémový monitoring

## Migrace IS SZIF a akceptace dodávky

Předmětem plnění je primárně zajištění migrace IS SZIF ze stávající infrastruktury na novou infrastrukturu v termínu stanoveném ve Smlouvě. Migrace IS SZIF bude realizována jako součást dodávky nové infrastruktury. Níže jsou uvedeny požadavky současného provozovatele aplikačních vrstev na realizaci migrací dle jednotlivých oblastí a požadovaných způsobů realizace migrace.

Dodavatel v rámci tohoto plnění připraví detailní postup migrace, vypracuje harmonogram a plán migrace, definuje veškerou nezbytnou součinnost (respektive harmonogram poskytnutí součinnosti) i požadavky na realizaci migrace ze strany Objednatele i provozovatele aplikační vrstvy informačního systému SZIF. Dodavatel je v rámci tohoto povinen také splnit požadavky zadavatele a zapracovat náležitosti stanovené v Příloze č. 2 Smlouvy: Požadavky na zpracování předimplementační analýzy.

Ze strany Objednatele je zajištěna následující součinnost provozovatelů aplikací v rámci IS SZIF. Tato součinnost je limitní a způsob migrace systémů (zejména určení skupin jednotlivých systémů, které budou migrovány) musí odpovídat definované součinnosti tak, aby migrace proběhla v odpovídajícím rozsahu, kvalitě a termínech stanovených ve Smlouvě a v této Příloze č. 1 Smlouvy: Technická specifikace.

Součinnost provozovatele aplikační vrstvy IS SZIF:

Provozovatel předpokládá poskytnutí potřebné součinnosti pro každý systém v rozsahu maximálně 1MD. Pro přípravu a finální testování migrace SAP, předpokládá poskytnutí součinnosti v rozsahu 10MD. Maximálně možné souběžné čerpání služeb je 1FTE.

Součinnost bude poskytována v provozní době s výjimkou migrací produktivních systémů.

### Požadavky na realizaci migrace

Před zahájením kompletní migrace všech systémů na novou infrastrukturu bude postup migrace otestován na sandbox systémech (x86 – lx-mon + bdom02, PowerPC – WAX + SHX). Po akceptaci způsobu provedení migrace a potvrzení funkčnosti tohoto systému bude možné realizovat následně migraci všech dalších uvedených systémů v pořadí:

1. Testovací systémy
2. Vývojové systémy
3. Produktivní systémy

### Postup akceptace kompletní migrace

* Dodavatel provede migraci všech systémů dle platformy a metody migrace.;
* V rámci provádění daného plnění bude provedena kontrola ze strany provozovatelů jednotlivých aplikačních platforem (SAP, MACH, CAAS, GTFoto). Na základě potvrzení provedení migrace systému přejde jednotlivý systém do pilotního provozu.;
* Po uvedení do pilotního provozu začne běžet období 30 dnů, kdy může být dodavatel vyzván k odstranění závad, které byly zjištěny v průběhu pilotního provozu.;
* Po odstranění veškerých závad bude systém přebrán do rutinního provozu.

### Kontroly provozovatelů IS SZIF

Dodavatel umožní provedení kontroly ze strany současných provozovatelů aplikační vrstvy informačního systému v rámci provádění migrace jednotlivých systémů (skupin systémů) před přechodem do pilotního provozu, přičemž tato kontrola bude provedeno do 2 pracovních dnů ode dne, kdy Dodavatel provedení takové kontroly umožní. Bez provedení odpovídající kontroly a potvrzení ze strany provozovatelů nebude možné potvrdit provedení migrace systému a přechod systému do pilotního provozu.

### Postup migrací dle platformy a metody

#### Dílčí blok „Storage APP“

Dodavatel provede přesun všech souborových systémů na nové diskové pole Tier 0 1:1 včetně korektního přesunu sparse (<https://www.ibm.com/support/pages/about-sparse-files>) souborů. Tento přesun bude promítnut do OS (případně clusteru). Pro původní storage systémy budou provedena dostatečná opatření, aby bylo zabráněno jejich připojení do systému.

Dodavatel navrhne metody a následně provede ověření konzistence přenosu dat z diskových polí, ze kterých odevzdá objednateli protokol. V případě filesystémů použitých v systémech běžících v rámci clusteru, navrhne a provede dodavatel i testování clusteru.

#### Dílčí blok „PowerPC“

* Migrace stávajícího LPAR:
  + Stávající systémy budou přeneseny dodavatelem 1:1. Profily virtuálních serverů mohou být přenastaveny následně.;
  + Dodavatel provede migraci HW a diskových polí a následně předá SAPu k základním testům včetně přístupů na OS s administrátorským oprávněním.;
  + SAP provede „Kontroly SAP“.;
  + Dodavatel provede testy clusteru, SAP provede „Kontroly SAP“ na obou nodech clusteru.;
  + Dodavatel provede testy zálohování a obnovy, SAP provede „Kontroly SAP“.;
  + Výsledky testů budou zaznamenány do protokolu.;

#### Dílčí blok „x86“

* Migrace stávajícího VMware:
  + Dojde pouze k migraci stroje na úrovni VMware:
    - Dodavatel předá přístupy na OS s administrátorským oprávněním.;
    - SAP provede pouze relevantní „Kontroly SAP“.;
    - SAP prověří funkčnost SAP aplikací.
  + Výsledky jednotlivých testů budou zaznamenány do protokolu.