Příloha č. 1

Smlouvy:

Technická specifikace

Obsah

[1. Manažerské shrnutí výchozího stavu 4](#_Toc177708929)

[1.1 SAN síť 4](#_Toc177708930)

[1.2 LAN síť 4](#_Toc177708931)

[1.3 Datová úložiště 5](#_Toc177708932)

[1.4 Výpočetní servery pro ERP SAP 5](#_Toc177708933)

[1.5 Výpočetní servery pro virtualizaci platformy x86 5](#_Toc177708934)

[2 Požadavky na realizované řešení 6](#_Toc177708935)

[2.1 Záměr obnovy infrastruktury 6](#_Toc177708936)

[2.2 Požadavky na certifikaci dodávaných komponent 8](#_Toc177708937)

[2.3 Technické parametry dodávaných komponent 9](#_Toc177708938)

[2.4 SAN síť 9](#_Toc177708939)

[2.4.1 Popis současného stavu 9](#_Toc177708940)

[2.4.2 Požadavky na nové řešení 10](#_Toc177708941)

[2.5 LAN síť (síťové a bezpečnostní prvky) 13](#_Toc177708942)

[2.5.1 Popis současného stavu 13](#_Toc177708943)

[2.5.2 Požadavky na nové řešení 13](#_Toc177708944)

[2.5.2.1 Inicializační nastavení 14](#_Toc177708945)

[2.5.2.2 Migrace 14](#_Toc177708946)

[2.5.3 LAN - topologie 15](#_Toc177708947)

[2.5.3.1 LAN část DC – Fyzické provedení / SoC 15](#_Toc177708948)

[2.5.3.2 DC fabric 16](#_Toc177708949)

[2.5.3.3 WAN konektivita 16](#_Toc177708950)

[2.5.3.4 DCI konektivita 17](#_Toc177708951)

[2.5.4 L2-L7 security 17](#_Toc177708952)

[2.5.4.1 Požadavky na nové řešení 17](#_Toc177708953)

[2.5.4.2 Firewall 18](#_Toc177708954)

[2.5.5 Load balancer 26](#_Toc177708955)

[2.5.6 Management LAN 37](#_Toc177708956)

[2.5.6.1 Management DC Fabric 37](#_Toc177708957)

[2.5.6.2 Management přístup na síťové elementy 41](#_Toc177708958)

[2.6 Systémové skříně (Rack) 48](#_Toc177708959)

[2.6.1 Popis současného stavu 48](#_Toc177708960)

[2.6.2 Popis možností DC 50](#_Toc177708961)

[2.6.3 Požadavky na systémové skříně (Rack) 51](#_Toc177708962)

[2.6.4 Popis dodávaného řešení - Racky 52](#_Toc177708963)

[2.7 Datová úložiště 52](#_Toc177708964)

[2.7.1 Řešení pro ukládání dat 52](#_Toc177708965)

[2.7.1.1 Popis současného stavu 52](#_Toc177708966)

[2.7.1.2 Požadavky na nové řešení 52](#_Toc177708967)

[2.7.1.3 Disková pole pro produkční provoz 53](#_Toc177708968)

[2.7.1.4 Disková pole pro zálohování dat 58](#_Toc177708969)

[2.7.1.5 Páskové knihovny 62](#_Toc177708970)

[2.7.2 Řešení pro zálohování a ochranu dat 64](#_Toc177708971)

[2.7.2.1 Popis současného stavu 64](#_Toc177708972)

[2.7.2.2 Požadavky na nové řešení 65](#_Toc177708973)

[2.7.2.3 Zálohování 65](#_Toc177708974)

[2.7.2.4 Správa klonovacích (hardwarový snapshot) funkcí 67](#_Toc177708975)

[2.7.2.5 Detekce ransomware hrozeb 69](#_Toc177708976)

[2.8 Výpočetní servery pro ERP SAP 71](#_Toc177708977)

[2.8.1 Popis současného stavu 71](#_Toc177708978)

[2.8.2 Požadavky na nové řešení 71](#_Toc177708979)

[2.8.3 Požadavky na výkon 72](#_Toc177708980)

[2.9 Zálohovací a dohledové servery 78](#_Toc177708981)

[2.9.1 Popis současného stavu 78](#_Toc177708982)

[2.9.2 Požadavky na nové řešení 78](#_Toc177708983)

[2.10 Výpočetní servery pro virtualizaci platformy x86 81](#_Toc177708984)

[2.10.1 Popis současného stavu 81](#_Toc177708985)

[2.10.2 Požadavky na nové řešení 82](#_Toc177708986)

[2.11 Aplikační a Systémový Monitoring 87](#_Toc177708987)

[2.11.1 Popis současného stavu 87](#_Toc177708988)

[2.11.2 Požadavky na nové řešení 87](#_Toc177708989)

[2.11.3 Funkční požadavky 88](#_Toc177708990)

[2.11.4 Systémové a HW požadavky 88](#_Toc177708991)

[2.11.5 Požadavky na monitorované technologie 88](#_Toc177708992)

[2.12 Migrace IS SZIF a akceptace dodávky 92](#_Toc177708993)

[2.12.1 Požadavky na realizaci migrace 92](#_Toc177708994)

[2.12.2 Postup akceptace kompletní migrace 93](#_Toc177708995)

[2.12.3 Kontroly provozovatelů IS SZIF 93](#_Toc177708996)

[2.12.4 Postup migrací dle platformy a metody 93](#_Toc177708997)

[2.12.4.1 Dílčí blok „Storage APP“ 93](#_Toc177708998)

[2.12.4.2 Dílčí blok „PowerPC“ 93](#_Toc177708999)

[2.12.4.3 Dílčí blok „x86“ 93](#_Toc177709000)

# 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
  + Aplikační monitoring – viz kapitola 2.11
* 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** |
|  |  |  |  |

Tabulka 1 - 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 |  |  |
|  | Technické vlastnosti a rozměry | * Kompatibilní s RACK 19” |  |  |
|  | * Velikost v EIA (jednotek U) pro systémovou skříň 19” nesmí přesáhnout 2U. |  |  |
|  | * Dodavatel uvede počet a typ napájení (C13/14 nebo C19/C20 a počet). |  |  |
|  | * Dodavatel uvede hmotnost a typický a maximální elektrický příkon. |  |  |
|  | * Dodavatel uvede, jaké jsou požadavky na elektrické jištění. |  |  |
|  | Napájení | * Zařízení musí mít redundantní napájecí zdroje 250VAC, vyměnitelné za chodu. |  |  |
|  | Počet portů | * Min. 96 portů s rychlostí min. 64Gb/s, z toho min. 72 portů aktivních |  |  |
| * Z 96 portů min. 49ks min. 64 Gb/s SW transceivery |  |  |
| * Z 96 portů min. 2ks x min. 32Gb/s SW transceivery |  |  |
| * Z 96 portů min. 13ks min. 16Gb/s SW transceivery |  |  |
| * Z 96 portů min. 8ks min. 32Gb/s LW transceivery |  |  |
|  | * Možnost rozšíření o dalších min. 16 SFP-DD portů pouze dokoupením licence. |  |  |
|  | Přenosové rychlosti | * v minimálním rozsahu 8, 10, 16, 32, 64 Gb/s full duplex |  |  |
|  | Propojovací kabely | * Odpovídající počet propojovacích kabelů pro plné zprovoznění systému. |  |  |
|  | Požadované vlastnosti | * ISL Trunking |  |  |
| * Extended Fabric – možnost propoje až do 10 km nebo více |  |  |
| * Integrovaný routing mezi Fabric |  |  |
| * Quality of Service |  |  |
| * Full Fabric |  |  |
| * Vestavěná diagnostika |  |  |
| * Propustnost min. 8Tb/s a latence max. 500ns |  |  |
| * Výdech ventilátorů na straně portů |  |  |
|  | Záruka | * 6 let, 24x7, oprava do 24h |  |  |
| * Komunikace výhradně v českém jazyce |  |  |
| * Záruku garantuje přímo výrobce zařízení |  |  |

Tabulka 2 - 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

**Dodavatel v rámci této kapitoly popíše detailně úvodní nastavení celého řešení umístěného do jednoho DC, za využití všech požadovaných prvků po produktivním nasazení. Po dodavateli se požaduje, aby HW a SW (licence) setup pro úvodní stav byl kompletní a při přechodu na metrocluster nebo geocluster nebylo nutné dokupovat žádný dodatečný HW a SW. Tedy kompletní řešení musí být postaveno tak, jako by se jednalo od začátku o metrocluster nebo geocluster řešení.**

#### Migrace

**Dodavatel v rámci této kapitoly popíše detailně realizaci migrace řešení formou plného „Parallel Build“. Je nezbytné vystavit novou síťovou infrastrukturu včetně výpočetní infrastruktury do nových racků v rámci každého sálu datového centra.**

**LAN technologie musí být logicky rozděleny do jednotlivých racků podle svého účelu. Každý rack s výpočetními prostředky musí mít své dedikované LEAF (ToR) switche, které budou sloužit pro připojení datových portů těchto technologií. Zbytek centrální LAN technologie, včetně SPINE switchů, Edge switchů, Firewallů, Load balancerů a WAN routeru, musí být distribuován redundantně do obou stojanů.**

**V každém racku musí být umístěn jeden z OoB switchů pro připojení jak LAN technologie, tak i výpočetních prostředků do OoB sítě. Console připojení všech LAN komponentů musí zajistit terminálový server instalovaný do stojanu společně s centrální částí LAN technologie.**

**Stejný postup musí být realizován i ve druhém PoPu datového centra.**

**Zadavatel požaduje, aby následným krokem migrace bylo propojení na L2 a L3 úrovni přes centrální switche obou sítí („staré“ a „nové“). Toto zapojení umožní postupnou migraci L2/L3 i L4-L7 služeb, s plnou viditelností služeb, které budou v té době ještě plně funkční v současné infrastruktuře.**

**Tento scénář musí zajistit realizaci migrace bez časového presu a s možností prověření každé jednotlivě přemigrované služby.**

**Dodavatel musí zpracovat detailní SoW (Scope of Work) pro provedení instalace/implementace a migraci služeb zahrnující přehledově následující:**

* **Vytvoření LLD (Low Level Design):**
  + **V této části SoW dokumentu bude detailně popsán obsah všech fází;**
  + **Zmapování a zdokumentování současného stavu na úrovni nutné pro migraci na dodaný HW a koncept nové architektury;**
* **Inicializaci všech síťových elementů = upgrade / zahoření atd.;**
* **Instalaci všech síťových elementů v Parallel Buildu = montáž do racků / připojení k napájení / kabeláž;**
* **Implementaci = základní konfiguraci síťových elementů nutnou:**
  + **pro připojení na OoB mngt síť a In-Band přístup;**
  + **pro připojení na monitoring a MGMT nástroje jako je SNMP server, NTP server, Syslog, FTP atd.;**
  + **24h monitoring boxů a sítě;**
* **Instalaci a implementaci DC:** 
  + **Instalace Fabric MNGT nástroje jako VM v VMware virtualizaci apod.;**
  + **Greenfield build fáze DC fabric;**
  + **Konfigurace vzorových služeb:**
    - **služby budou migrovány 1:1 a pak až optimalizovány;**
    - **budou vytipovány vzorové služby, které se stanou částí test fáze;**
    - **detailní dokument testů bude dodaný po ukončení výběrového řízení;**
* **Test vzorových služeb:**
  + **Test a Akceptace;**
* **Migrace:**
  + **Detailní plán migrace vepsaný do LLD zahrnuje:**
    - **typy služeb dle flow uvnitř/do/z DC LAN;**
    - **seznam všech služeb a jejich přiřazení k typům služeb;**
    - **časový plán migrace;**
  + **Propojení současné a nové LAN přes L3/L2 propoj v jednom z PoDů;**
  + **Postupná migrace služeb:**
    - **step-by-step procedura zahrnující testy přemigrovaných služeb dle typů a jejich následný monitoring – min. 24h;**
  + **Odpojení a odstavení současné LAN sítě:**
    - **odpojení současné sítě od Parallel Buildu – 24h monitoring správné funkčnosti;**
    - **odstavení současné sítě – plný „remove“ všech síťových elementu současné LAN sítě;**

### LAN - topologie

**Dodavatel v rámci této kapitoly popíše návrh řešení komplexního řešení topologie LAN včetně všech nabízených síťových elementů a zpracuje grafické znázornění architektury jednotlivých bloků, a to minimálně v rozsahu:**

* DC fabric;
* WAN konektivita;
* DCI konektivita;
* L4-L7 security;

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

**Dodavatel v rámci této kapitoly popíše fyzické provedení / SoC dle navržené LAN topologie včetně uvedení všech nabízených prvků a specifikace jejich vlastností.**

|  |  |  |  |
| --- | --- | --- | --- |
| **Komponenty** | | | |
| **Číslo** | **Název komponenty** | **Part number** | **Počet kusů** |
|  |  |  |  |

|  |  |
| --- | --- |
| **Komponenta (X ks)** | |
| **Vlastnost/ komponenta** | **Parametry** | |
|  |  | |

#### DC fabric

**Dodavatel v rámci této kapitoly popíše DC fabric dle navržené LAN topologie včetně detailního grafického schématu architektury a uvedení všech nabízených prvků a specifikace jejich vlastností.**

|  |  |  |  |
| --- | --- | --- | --- |
| **Komponenty** | | | |
| **Číslo** | **Název komponenty** | **Part number** | **Počet kusů** |
|  |  |  |  |

|  |  |
| --- | --- |
| **Komponenta (X ks)** | |
| **Vlastnost/ komponenta** | **Parametry** | |
|  |  | |

#### WAN konektivita

**Dodavatel v rámci této kapitoly popíše WAN konektivitu dle navržené LAN topologie včetně detailního grafického schématu architektury a uvedení všech nabízených prvků a specifikace jejich vlastností.**

|  |  |  |  |
| --- | --- | --- | --- |
| **Komponenty** | | | |
| **Číslo** | **Název komponenty** | **Part number** | **Počet kusů** |
|  |  |  |  |

|  |  |
| --- | --- |
| **Komponenta (X ks)** | |
| **Vlastnost/ komponenta** | **Parametry** | |
|  |  | |

#### DCI konektivita

**Dodavatel v rámci této kapitoly popíše DCI konektivitu dle navržené LAN topologie včetně detailního grafického schématu architektury a uvedení všech nabízených prvků a specifikace jejich vlastností.**

|  |  |  |  |
| --- | --- | --- | --- |
| **Komponenty** | | | |
| **Číslo** | **Název komponenty** | **Part number** | **Počet kusů** |
|  |  |  |  |

|  |  |
| --- | --- |
| **Komponenta (X ks)** | |
| **Vlastnost/ komponenta** | **Parametry** | |
|  |  | |

### 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 4x 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** |
|  |  |  |  |

Tabulka 8 - 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 |  |  |
|  | Technické vlastnosti a rozměry | * Kompatibilní s RACK 19” |  |  |
|  | * Velikost v EIA (jednotek U) pro systémovou skříň 19” nesmí přesáhnout 1U. |  |  |
|  | * Dodavatel uvede počet a typ napájení (C13/14 nebo C19/C20 a počet). |  |  |
|  | * Dodavatel uvede hmotnost a typický a maximální elektrický příkon. |  |  |
|  | * Dodavatel uvede, jaké jsou požadavky na elektrické jištění. |  |  |
|  | Napájení a chlazení | * Zařízení musí mít redundantní napájecí zdroje 250VAC, vyměnitelné za chodu. (Dodavatel také popíše řešení redundance (N+N, N+1 atd.). |  |  |
|  | * Zařízení musí mít redundantní chladící komponenty, vyměnitelné za chodu. (Dodavatel také popíše řešení redundance (N+N, N+1 atd.). |  |  |
|  | * Aktivní chlazení Rear-to-Front. |  |  |
|  | Počet portů | * Minimálně 4ks 100GE QSFP28 portů pro data, standardně osazených * Minimálně 2ks 10GE SFP+ pro komunikaci HA clusteru, standardně osazených |  |  |
|  | Konzolový port | * Provedení RJ45 nebo USB (pozn. u USB i převodníky USB/RS-232(RJ45)) |  |  |
|  | Propojovací kabely | * Odpovídající počet propojovacích kabelů pro plné zprovoznění systému. |  |  |
|  | Kapacita | * Minimálně 32GB SSD pro lokální logy, debug soubory atd. |  |  |
|  | * Podporovány musí být enterprise SSD disky, DWPD hodnota nabízených disků/modulů musí být 1 nebo vyšší. |  |  |
|  | Charakteristiky a funkce | * Podpora Jumbo Frames min. 9kB |  |  |
|  | * Podpora vytvoření tzv. subinterface s individuální konfigurací parametrů: VLAN-id, encapsulation, apod. |  |  |
|  | * Režim HA v módu active-passive a active-active |  |  |
|  | * 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 |  |  |
|  | * Porpora SNMP (1v/2v/3v):   + HA musí být monitorovatelný pomocí SNMP dostupném v OoB mgmt rozhraní |  |  |
|  | * HA řešení musí podporovat pro sestavení HA clusteru rozdílné rozhraní, než jsou požadované 4x100GE, min. 2x10GE |  |  |
|  | * 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 |  |  |
|  | * 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) |  |  |
|  | * Podpora MBGP (IPv4, IPv6) |  |  |
|  | * Podpora VRRP (IPv4/6) |  |  |
|  | * Podpora IGMP (v2/v3) |  |  |
|  | * Podpora ECMP (Equal-Cost Multi-Path) Load Balancing – min. 8 ECMP cest |  |  |
|  | * Podpora PIM (Protocol Independent Multicast) SSM/ASM |  |  |
|  | * Podpora Policy, Filter based routing (směrování založené na L2-L4 zdrojových a cílových hlavičkách |  |  |
|  | * Podpora plnohodnotných virtuálních kontextů (virtuálních firewallů) s oddělenou správou – min. 30 |  |  |
|  | * Podpora BFD (Bi-directional Forwarding Detection) – min. static, OSPF, 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. 64 ECMP cest |  |  |
|  | 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 |  |  |
|  | * Souběžně aplikovatelné Source i Destination nat pravidla na jeden typ provozu |  |  |
|  | * Podpora 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 |  |  |
|  | * Možnost definice bezpečnostních politik s využitím user/user group, L7 aplikací |  |  |
|  | * Možnost konfiguraci ochrany firewallu na síťových rozhraních – podpora IP spoofing a UDP, ICMP a SYN floods |  |  |
|  | * 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 |  |  |
|  | * Min. 50 000 bezpečnostních pravidel |  |  |
|  | * Min. počet vytvořitelných zónových kontextů (párů zón) na NGFW je 6000 |  |  |
|  | * "Application layer Gateway" pro protokoly DNS, IKE, RPC, FTP, SIP |  |  |
|  | * Route-based site-to-site IPsec VPN |  |  |
|  | * 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 5000 (statický endpoint, IPSEC SA je počítaný jako jeden tunel) |  |  |
|  | * 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 |  |  |
|  | * Podpora prioritizaci provozu na základě DSCP |  |  |
|  | * Podpora prioritizaci provozu na základě identifikované aplikace |  |  |
|  | * Podpora dešifrování příchozího SSL/TLS provozu, za pomoci serverového certifikátu a priv klíče (reverse proxy) |  |  |
|  | * Podpora dešifrování odchozího SSL/TLS provozu, za pomoci naimportovaného priv klíče interního serveru (forward proxy) |  |  |
|  | * Dešifrovaný provoz musí být možno definovat na základě všech typických parametrů, jako jsou zdrojová a cílová IP adresa, port, uživatelská identita |  |  |
|  | * Podpora dešifrování protokolu TLS verze 1.2 i 1.3 |  |  |
|  | * FW nebo jiné dekrypční zařízení dešifrování za pomocí ECC (Elliptical Curve Cryptography) a ECDHE pro příchozí i odchozí provoz |  |  |
|  | * Podpora L7 Aplikačního Firewallu a rozpoznání aplikací nezávisle na TCP/UDP portech (update aplikačních signatur výrobcem) |  |  |
|  | * FW obsahuje mimo definovaných jednotlivých aplikací i aplikační kategorie |  |  |
|  | * Definovaná aplikace/kategorie je jedním "match" kritériem při policy lookup společně se source a destination IP |  |  |
|  | * Identifikace L7 aplikace musí probíhat přímo v FW |  |  |
|  | * FW musí umět pracovat s neznámými aplikacemi - upozornit na ně a mít možnost je zakázat |  |  |
|  | * 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) |  |  |
|  | * 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 |  |  |
|  | * FW podporuje možnost odesílání souborů k dynamické analýze do sandbox prostředí jako ochranu předa škodlivým kódem |  |  |
|  | * Sandbox poskytován stejným výrobcem jako FW |  |  |
|  | * Statická i dynamická analýza souborů a dokumentů na přítomnost kybernetických hrozeb ve virtuálním prostředí |  |  |
|  | * Monitorování chování spuštěného souboru a zaměření na pokusy o změny v systému soborů, systémových registrů, procesů a navázání síťových spojení s vyhotovením reportu |  |  |
|  | * Emulace a detekce na úrovni OS |  |  |
|  | * Sandbox analýza umí identifikovat známý i zero-day malware skrytý v souborech |  |  |
|  | * Logování sandboxových analýz, zaznamenané provedené operace a jejich výsledek |  |  |
|  | * Možnost manuálního zaslání souborů pro analýzu do sandbox prostředí |  |  |
|  | Logování | * Možnost vyexportovat/poslat logy |  |  |
|  | * Posílání logů o provozu na min. 4 cílové syslog servery |  |  |
|  | * Ukládání logů na interní SSD |  |  |
|  | * Umožňovat výběr přeposílaných logů na úrovni bezpečnostního pravidla |  |  |
|  | * Umožnit tvorbu "Traffic mirroring" pravidel a přeposílání provozu k externímu analytickému zařízení |  |  |
|  | Záruka | * Podpora řešení a aktualizace po dobu 6 let, 24x7, oprava do 24h |  |  |
| * Komunikace výhradně v českém jazyce |  |  |
| * Záruku garantuje přímo výrobce zařízení |  |  |

Tabulka 9 - 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 4x 100GE NNI portů (počet reflektuje možné rozšíření DC fabric)
  + vybavené 4x 100GBASE-SR4 SFP28 originálními transceivery;
* Podpora WAF, LB, L3;

|  |  |  |  |
| --- | --- | --- | --- |
| **Load Balancer** | | | |
| **Číslo** | **Název komponenty** | **Part number** | **Počet kusů** |
|  |  |  |  |

Tabulka 10 - 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 |  |  |
|  | Technické vlastnosti a rozměry | * Kompatibilní s RACK 19” |  |  |
|  | * Velikost v EIA (jednotek U) pro systémovou skříň 19” nesmí přesáhnout 1U. |  |  |
|  | * Dodavatel uvede počet a typ napájení (C13/14 nebo C19/C20 a počet). |  |  |
|  | * Dodavatel uvede hmotnost a typický a maximální elektrický příkon. |  |  |
|  | * Dodavatel uvede, jaké jsou požadavky na elektrické jištění. |  |  |
|  | Napájení a chlazení | * Zařízení musí mít redundantní napájecí zdroje 250VAC, vyměnitelné za chodu. (Dodavatel také popíše řešení redundance (N+N, N+1 atd.). |  |  |
|  | * Aktivní chlazení Rear-to-Front. |  |  |
|  | Počet portů | * Minimálně 4ks 100GE-SR4 QSFP28 portů pro data, standardně osazených * Minimálně 2ks 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)) |  |  |
|  | Management | * Rozhraní RJ45 pro mgmt OoB switche * MGMT přístup pomocí: sériový port, GUI, příkazový řádek, iLO |  |  |
|  | Propojovací kabely | * Odpovídající počet propojovacích kabelů pro plné zprovoznění systému |  |  |
|  | Kapacita | * Minimálně 1TB SSD pro lokální logy, debug soubory atd. |  |  |
|  | * Podporovány musí být enterprise SSD disky, DWPD hodnota nabízených disků/modulů musí být 1 nebo vyšší |  |  |
|  | Výkon | * Datová propustnost zařízení min. 180 Gb/s na L4 a min. 120 Gb/s na L7 |  |  |
|  | * Minimální propustnost HTTP požadavků 32 mil./s |  |  |
|  | * Počet souběžných L4 spojení min. 135 mil. |  |  |
|  | * Offload – HW komprese – propustnost min. 75 Gbps |  |  |
|  | * SSL akcelerace v HW |  |  |
|  | * Počet SSL transakcí za sekundu min. 105 000 (při použití 2K klíče) |  |  |
|  | * Počet SSL transakcí za sekundu min. 85 000 (při použití ECDSA P-256 klíče) |  |  |
|  | * Celkový šifrovací výkon min. 70 Gb/s |  |  |
|  | * Virtualizace HW zdrojů |  |  |
|  | * HW podpora 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 |  |  |
|  | * Plná podpora IPv6, IPv4/IPv6 gateway |  |  |
|  | * Podpora Spanning Tree Protokolu (STP) |  |  |
|  | * Podpora SNMP (v1/v2c/v3) |  |  |
|  | * Podpora Active-Active a Active-Pasive módu |  |  |
|  | * Možnost vytvoření HA clusteru mezi Virtuální a Hardware platformou |  |  |
|  | * Full-Proxy architektura (plné oddělení klientského a serverového spojení) |  |  |
|  | * Podpora externích šifrovacích karet pro SSL (HSM) |  |  |
|  | * Podpora ověření certifikátů vydaných podřízenou CA (intermediate CA) |  |  |
|  | * Možnost přidat vlastní funkce pomocí skriptování |  |  |
|  | * Podpora HTTP/2 |  |  |
|  | * Podpora IPSec IKEv2 |  |  |
|  | * Podpora konfigurace a správu 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; |  |  |
|  | * Možnost používat knihovny JavaScript třetích stran k úpravě a správě provozu |  |  |
|  | Vlastnosti a funkce WAF | * Integrace s nástrojem na detekci zranitelností webových aplikací |  |  |
|  | * Detekce a blokování širokého spektra útoků na aplikační vrstvě, minimálně podle OWASP top10 |  |  |
|  | * Možnost doprogramovat si filtrovací pravidla pro aplikace |  |  |
|  | * Automatická korelace zranitelností do jednoho bezpečnostního incidentu |  |  |
|  | * Ochrana AJAX a JSON aplikací |  |  |
|  | * Ochrana proti L7 DDoS útokům, web scrapingu a útokům pomocí hrubé síly (brute force) |  |  |
|  | * Podpora Captcha metody |  |  |
|  | * Automatické odlišení skutečných uživatelů od robotů |  |  |
|  | * Integrovaný XML firewall |  |  |
|  | * Podpora maskování/odstranění citlivých informací – čísla kreditních karet, rodné číslo, číslo pojištění apod. |  |  |
|  | * Automatické nahrávání a aplikování nových signatur |  |  |
|  | * Podpora pozitivního a negativního bezpečnostního modelu |  |  |
|  | * Blokování útočníků na základě geolokace až na úroveň regionu |  |  |
|  | * Podpora ICAP pro antivirovou kontrolu – pro HTTP, SOAP a SMTP |  |  |
|  | * Ochrana SMTP a FTP na aplikační úrovni |  |  |
|  | * Podpora SSL (šifrování a dešifrování) |  |  |
|  | * Podpora různých typů reportů – PCI, geolokační reporty |  |  |
|  | * Podpora standardů PCI DSS, HIPAA, Basel II a SOX |  |  |
|  | * Integrované bezpečnostní politiky pro Microsoft Outlook Web Access, Oracle Applications a Microsoft SharePoint |  |  |
|  | * Podpora pro analýzu HTTP provozu (Top URL, Top klienti, nejpoužívanější HTTP metody, návštěvnost stránek podle geogr. regionu) |  |  |
|  | * Podpora aplikačního firewallu ve virtuálních kontextech |  |  |
|  | * Podpora aplikačního firewallu v cloudu |  |  |
|  | * Rozšířená podpora CSHUI – detekce aktivity klávesnice a myši, detekce změn URL od klienta za krátkou dobu |  |  |
|  | * Ochrana proti Session Highjacking pomocí Browser Fingerprintingu |  |  |
|  | * Detekce a ochrana před DoS útoky na specifické URL, které mohou zatížit back-end systémy (např. vyhledávácí URL apod.) |  |  |
|  | * Vynucení přístupu uživatele k chráněné aplikaci přes přihlašovací stránku aplikace |  |  |
|  | * Podpora nastavení bezpečnostních politik podle IP adresy, doménového jména a URI |  |  |
|  | * Podpora a filtrování WebSocket provozu |  |  |
|  | * Blacklistování IP adres, které opakovaně snaží překonat bezpečnostní opatření v politice |  |  |
|  | * Ochrana proti Credential Stuffing útokům |  |  |
|  | * Rozpoznání zdrojů Phishingu, Anonymních Proxy a spojení na Command and Control centra Botnetů |  |  |
|  | * Ochrana dat a přihlašovacích údajů proti Man in the Browser útokům |  |  |
|  | * 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 |  |  |
|  | * Podpora importu souboru Swagger pro definici security politiky pro ochranu API |  |  |
|  | * Podpora využití CI/CD pipeline pro nasazování security politik WAF na webových aplikacích |  |  |
|  | Vlastnosti řízení provozu | * Možnost připojení k monitorovacím nástrojům třetích stran prostřednictvím otevřeného API |  |  |
|  | * Podpora REST API |  |  |
|  | * Autentizace klientů přes LDAP/Radius |  |  |
|  | * Povolení/zakázání ICMP a ARP pro VIP |  |  |
|  | * Podpora vysokorychlostního granulárního logování / logování per aplikace / bez omezení výkonnosti zařízení |  |  |
|  | * Podpora různých metod rozvažování zátěže |  |  |
|  | * Podpora filtrace paketů |  |  |
|  | * Podpora ToS, QoS (marking/preservation/mimic) |  |  |
|  | * Podpora rozvažování zátěže založené na poměrech (ratio) s CARP perzistencí |  |  |
|  | * Podpora SSL certifikátů podepsaných SHA-2 algoritmem |  |  |
|  | * Podpora práce s 4096-bit klíči |  |  |
|  | * Současná podpora ECC a RSA certifikátu |  |  |
|  | * Podpora Camellia šifer SSL |  |  |
|  | * Podpora pro TLS (v1.1/v1.2/v1.3) |  |  |
|  | * Podpora ECC a DH šifer v HW |  |  |
|  | * Podpora SSL Forward proxy |  |  |
|  | * Stavové filtrované paketů (ACL) |  |  |
|  | * Podpora vlastních skriptů pro monitorování zdraví a dostupnosti služeb |  |  |
|  | * Podpora monitorování služeb na základě výkonu konkrétních hostů |  |  |
|  | * TCP optimalizace síťových toků |  |  |
|  | * Komprese a cachování specifických služeb |  |  |
|  | * Podpora zrcadlení SSL relací a SSL spojení v HA clusteru |  |  |
|  | * Podpora 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 |  |  |
|  | * Import uživatelských identit IF-MAP |  |  |
|  | * SAML:   + SP role   + IdP role |  |  |
|  | * Modifikace SAML atributů |  |  |
|  | * Podpora SAML 2.0 |  |  |
|  | * Podpora pro vytvoření Single Sign-On (SSO):   + HTTP basic   + HTML form   + NTLM v1/v2   + Kerberos   + SAML |  |  |
|  | * Uchování přihlašovacích údajů v paměti a jejich přeposlání k ověření (User identity credential caching, SSO proxy) |  |  |
|  | * Podpora federace (SSO napříč různými doménami, např. on-prem a SaaS) |  |  |
|  | * Podpora Kerberos ticketing |  |  |
|  | * PCoIP proxy |  |  |
|  | * RDP proxy |  |  |
|  | * Patching (maskování) webových portálů:   + HTML   + JavaScript   + CSS   + Java |  |  |
|  | * Podpora L7 ACL |  |  |
|  | * Podpora zabezpečení vzdálené pracovní plochy vzdáleného uživatele |  |  |
|  | * Síťová SSL VPN DTLS |  |  |
|  | * Podpora minimálně 500 souběžných SSL VPN spojení |  |  |
|  | * Podpora vzdáleného přístupu k aplikacím bez nutnosti použití tlustého klienta |  |  |
|  | * Podpora OS:   + Windows   + MAC   + Linux   + iOS   + Android |  |  |
|  | * Nativní podpora MDM |  |  |
|  | * Kontrola minimálně nastavení zabezpečení koncových bodů (klientů), validace politik, detekce AV a verze, certifikátů |  |  |
|  | * Filtrování URL |  |  |
|  | * URL kategorizační databáze |  |  |
|  | * Podpora pro vytváření flexibilní a granulární přístupové politiky |  |  |
|  | * GUI pro vizuální nastavení přístupových bezpečnostních politik a logiky autentizace |  |  |
|  | DNS | * Podpora pro inspekci a filtrování DNS dotazů, ochrana před DNS DoS útoky |  |  |
|  | * Kontrola a validace DNS protokolu (normalizace) |  |  |
|  | * Podpora filtrování typů DNS dotazů |  |  |
|  | * Load balancing DNS provozu |  |  |
|  | * Podpora podpisování pomocí DNSSEC |  |  |
|  | * Centralizované řízení a správa klíčů pro DNSSEC |  |  |
|  | * Podpora domén nejvyššího řádu pro DNSSEC |  |  |
|  | * Validace DNSSEC |  |  |
|  | * Mitigace DNS DDoS |  |  |
|  | * Potlačení přístupu k DNS doménám se špatnou reputací (domény obsahující viry, malware, phishing apod.) |  |  |
|  | * Zabezpečený DNS data-plane před kybernetickými útoky |  |  |
|  | Síťový Firewall | * Inspekce SSL relací |  |  |
|  | * Detekce a ochrana před síťovými DDoS útoky |  |  |
|  | * Detekce protokolových anomálií |  |  |
|  | * Podpora síťových, SIP, DNS a HTTP DoS vektorů |  |  |
|  | * Hardwarová podpora DoS vektorů |  |  |
|  | * Podpora tvorby bezpečnostních pravidel s filtrováním IP adres se špatnou pověstí nebo přistupujících z konkrétních geografických regionů |  |  |
|  | * Podpora pro dynamických blacklistování IP adres a jejich reporting |  |  |
|  | * Podpora RTBH (Remote Trigger Black Hole Filtering) |  |  |
|  | * Podpora pro ochranu SSH Proxy serverů |  |  |
|  | * Detekce a ochrana proti zneužití nebo využití jiných TCP portů než běžných |  |  |
|  | * Napojení na globální databázi škodlivých IP adres s automatickým obnovováním a možnost jejich blokování |  |  |
|  | Záruka | * Podpora řešení a aktualizace po dobu 6 let, 24x7, oprava do 24h |  |  |
| * Komunikace výhradně v českém jazyce |  |  |
| * Záruku garantuje přímo výrobce zařízení |  |  |

Tabulka 11 - 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** |
|  |  |  |  |

Tabulka 12 - 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 |  |  |
|  | Vlastnosti a funkcionality | * Intent-based networking – inteligentní konfigurace a orchestrace sítě |  |  |
|  | * Inteligentní řízení životního cyklu nabízených síťových elementů |  |  |
|  | * Správa skrze GUI dostupný přes standartní webové prohlížeče |  |  |
|  | * GUI musí podporovat šifrovaný přístup - min. TLS 1.2 a TLS 1.3 |  |  |
|  | * Možnost definovat role admin/uživatel dle oprávnění (RBAC model); |  |  |
|  | * Lokální a vzdálená (RADIUS nebo TACACS+ server) authentikace uživatele |  |  |
|  | * Podpora a dostupnost REST API |  |  |
|  | * Instalace jako VM   + Podpora min. VMware, Linux KVM Hypervisor   + Podpora integrace s NSX-T |  |  |
|  | * 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 |  |  |
|  | * Podpora „Design Tepmplates“ - min. 3-stage clos/5-stage clos/MultiPoP/MultiPoD |  |  |
|  | * 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 |  |  |
|  | * Podpora Multi-Tenantnosti   + Podpora VRF – oddělení tabulek pro routing a forwarding |  |  |
|  | * Podpora definice zdrojů (Pool)   + Min. definice zdrojů pollů pro IP, IPv6, AS numbers a VNI |  |  |
|  | * Podpora RACK type Templates   + Single homing, dual-homing: MC-LAG/ESI-LAG |  |  |
|  | * 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 |  |  |
|  | * Podpora vytvoření celkového DC schématu tzv. blue-print |  |  |
|  | * Podpora tzv. „Devices onboarding“   + Manualně a ZTP (Zero Touch Provisioning) |  |  |
|  | * Manuálně a ZTP (Zero Touch Provisioning)   + DHCP   + Device discovetry   + Admin root password   + Upgrade OS   + Device Connectivity |  |  |
|  | * Podpora Fabric Expansion – Links, Leaves, Racks |  |  |
|  | * Podpora Adding New Servers – Single/Dual homed |  |  |
|  | * Podpora změny typu a speed UNI linek |  |  |
|  | * Podpora provisioning a management L2/L3 virtuálních sítí |  |  |
|  | * Podpora DC Fabric rollback |  |  |
|  | * Device maintanance, upgrade |  |  |
|  | * 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) |  |  |
|  | Záruka | * Podpora řešení a aktualizace po dobu 6 let |  |  |
| * Komunikace výhradně v českém jazyce |  |  |
| * Záruku garantuje přímo výrobce zařízení |  |  |

Tabulka 13 - 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 10/100/100BaseT 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 SFP28 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** |
|  |  |  |  |

Tabulka 14 - 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 |  |  |
|  | Technické vlastnosti a rozměry | * Kompatibilní s RACK 19” |  |  |
|  | * Dodavatel uvede velikost v EIA (jednotek U) pro systémovou skříň 19”. |  |  |
|  | * Dodavatel uvede počet a typ napájení (C13/14 nebo C19/C20 a počet). |  |  |
|  | * Dodavatel uvede hmotnost a typický a maximální elektrický příkon. |  |  |
|  | * Dodavatel uvede, jaké jsou požadavky na elektrické jištění. |  |  |
|  | Napájení a chlazení | * Zařízení musí mít redundantní napájecí zdroje 250VAC, vyměnitelné za chodu. |  |  |
|  | * Aktivní chlazení Front-to-Rear. |  |  |
|  | Propojovací kabely | * Odpovídající počet propojovacích kabelů pro plné zprovoznění systému |  |  |
|  | Konektivita | * Minimálně 48ks 25GE SFP28 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) |  |  |
|  | * Minimálně 2ks 10GE SFP28 (pro připojení do mgmt sítě) |  |  |
|  | Management | * Rozhraní RJ45 pro mgmt OoB switche |  |  |
|  | Konzolový port | * Provedení RJ45 nebo USB (pozn. u USB i převodníky USB/RS-232(RJ45)) |  |  |
|  | Vlastnosti a funkcionality | * Podpora Jumbo Frames min. 9kB |  |  |
|  | * Podpora 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) |  |  |
|  | * 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) |  |  |
|  | * 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 |  |  |
|  | * Podpora 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 |  |  |
|  | * CLI inteface: plná konfigurovatelnost a troubleshooting:   + Local   + Telnet   + SSH |  |  |
|  | * Authentikace uživatele:   + Local   + Radius, TACAC+   + RBAC |  |  |
|  | * Konfigurační změny automaticky přes .txt file |  |  |
|  | * Podpora syslog server   + Local   + Remote syslog server |  |  |
|  | * Ping, Traceroute |  |  |
|  | * sFlow a/nebo jiná adekvátní technologie |  |  |
|  | * Traffic mirroring |  |  |
|  | * SNMP v2/v3 |  |  |
|  | Záruka | * Podpora řešení a aktualizace po dobu 6 let, 24x7, oprava do 24h |  |  |
| * Komunikace výhradně v českém jazyce |  |  |
| * Záruku garantuje přímo výrobce zařízení |  |  |

Tabulka 15 - 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** |
|  |  |  |  |

Tabulka 16 - 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 |  |  |
|  | Technické vlastnosti a rozměry | * Kompatibilní s RACK 19” |  |  |
|  | * Dodavatel uvede velikost v EIA (jednotek U) pro systémovou skříň 19”. |  |  |
|  | * Dodavatel uvede počet a typ napájení (C13/14 nebo C19/C20 a počet). |  |  |
|  | * Dodavatel uvede hmotnost a typický a maximální elektrický příkon. |  |  |
|  | * Dodavatel uvede, jaké jsou požadavky na elektrické jištění. |  |  |
|  | Napájení a chlazení | * Zařízení musí mít redundantní napájecí zdroje 250VAC, vyměnitelné za chodu. |  |  |
|  | * Pasivní chlazení. |  |  |
|  | Propojovací kabely | * 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) |  |  |
|  | * Min. 2ks 10/100/1000BaseT síťové porty |  |  |
|  | Vlastnosti a funkcionality | * Zabudovaný web terminál dostupný přes standardní webové prohlížeče |  |  |
|  | * Podpora násobných paralelních relaci |  |  |
|  | * Authentikace uživatele:   + Local   + Radius, TACAC+   + RBAC |  |  |
|  | * Lokální logování aktivit v systému, přístupových a komunikačních případů na seriál i stíťových portech |  |  |
|  | * Podpora Static a DHCP IPv4 a IPv6 na síťových portech |  |  |
|  | * Statický routing |  |  |
|  | * Možnost konfigurace sériových portů minimálně na úrovni „Baud Rate, Data bits, Parity, Stop bits“ |  |  |
|  | * Možnost přímého připojení SSH na konkrétní konzolový port |  |  |
|  | * Vestavěný Firewall / IPsec VPN / SSL VPN |  |  |
|  | Záruka | * Podpora řešení a aktualizace po dobu 6 let, 24x7, oprava do 24h |  |  |
| * Komunikace výhradně v českém jazyce |  |  |
| * Záruku garantuje přímo výrobce zařízení. |  |  |

Tabulka 17 - 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** |
|  |  |  |  |

Tabulka 18 - 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) |  |  |
|  | Rozměr | * Max. 65 cm šířka x max. 120 cm hloubka. |  |  |
|  | Napájení | * PDU musí mít dostatečný počet konektorů C13 – C14/C19 – C20 pro připojení veškeré nabízené technologie. |  |  |

Tabulka 19 – 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** |
|  |  |  |  |

Tabulka 20 - 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) |  |  |
|  | Technické vlastnosti a rozměry | * Kompatibilní s RACK 19” |  |  |
|  | * Dodavatel uvede velikost v EIA (jednotek U) pro systémovou skříň 19”. |  |  |
|  | * Dodavatel uvede počet a typ napájení (C13/14 nebo C19/C20 a počet). |  |  |
|  | * Dodavatel uvede hmotnost a typický a maximální elektrický příkon. |  |  |
|  | * Dodavatel uvede, jaké jsou požadavky na elektrické jištění. |  |  |
|  | Napájení | * Zařízení musí mít redundantní napájecí zdroje 250VAC, vyměnitelné za chodu. |  |  |
|  | Konektivita | * Připojena k SAN infrastruktuře je minimální 16x min. 64 Gb/s (pro každé zařízení). |  |  |
|  | 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. |  |  |
|  | * Celková velikost cache/RAM v jednom řadiči musí být minimálně 1024 GB. |  |  |
|  | Charakteristiky a funkce | * Plně redundantní architektura bez jediného bodu selhání (SPOF). |  |  |
|  | * 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. |  |  |
|  | * Řešení musí poskytovat nativní replikace po FC nebo IP v minimálně v synchronních a asynchronních režimech. Podpora replikace dat do třetí lokality. |  |  |
|  | * Řešení musí podporovat min. následující režimy: RAID 1, 6 a 10 nebo distribuovaný RAID 1 a 6. |  |  |
|  | * Diskový subsystém musí disponovat vytvářením 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). |  |  |
|  | * Upgrade software a hardware u řadičů je musí být proveditelný 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. |  |  |
|  | * Disková pole musí umožňovat 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. |  |  |
|  | * Aplikačně konzistentní, nesmazatelné a nemodifikovatelné kopie je nutné vytvářet minimálně pro DB Oracle nad 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.; |  |  |
|  | * Disková pole musí podporovat 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). |  |  |
|  | * Počet sparedisků dle doporučení výrobce. |  |  |
|  | * Podporovány musí být enterprise SSD disky nebo Flash moduly, DWPD hodnota nabízených disků/modulů musí být 1 nebo vyšší. |  |  |
|  | 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. |  |  |
|  | * Řešení musí poskytovat deduplikaci 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. |  |  |
|  | Management/Řídící software | * MGMT rozhraní ve webové nebo grafické podobě. |  |  |
|  | * MGMT rozhraní musí umožnit 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) |  |  |
|  | * Řešení musí umožňovat 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 % |  |  |
|  | Rozšiřitelnost | * Dodavatel uvede počet volných pozic pro SSD/Flash disky či moduly. |  |  |
|  | * Řešení musí umožnit rozšíření o minimálně 33% (na **1500** **TB**). |  |  |
|  | * Škálování výkonnosti je prováděno nativním přidáváním dalších řadičů minimálně do čtyř řadičové konfigurace. |  |  |
|  | * Škálování kapacit je prováděno pomocí expanzních jednotek. |  |  |
|  | * Dodavatel uvede možnosti rozšiřitelnosti a to: * A) pro Cache, * B) pro počty FC FC připojení. |  |  |
|  | Záruka | * 6 let, 24x7, oprava do 24h |  |  |
| * Komunikace výhradně v českém jazyce |  |  |
| * Záruku garantuje přímo výrobce zařízení |  |  |

Tabulka 21 - 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** |
|  |  |  |  |

Tabulka 22 - 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. |  |  |
|  | Technické vlastnosti a rozměry | * Kompatibilní s RACK 19”. |  |  |
|  | * Dodavatel uvede velikost v EIA (jednotek U) pro systémovou skříň 19”. |  |  |
|  | * Dodavatel uvede počet a typ napájení (C13/14 nebo C19/C20 a počet). |  |  |
|  | * Dodavatel uvede hmotnost a typický a maximální elektrický příkon. |  |  |
|  | * Dodavatel uvede, jaké jsou požadavky na elektrické jištění. |  |  |
|  | Napájení | * Zařízení musí mít redundantní napájecí zdroje 250VAC, vyměnitelné za chodu. |  |  |
|  | Konektivita | * Připojena k SAN infrastruktuře je minimální 4x min. 32 Gb/s (pro každé zařízení). |  |  |
|  | Výkon | * SSD/flash vrstva: Náhodný IO výkon: min. 30.000 IO/s, poměr čtení:zápis 50:50, 100% náhodná zátěž, velikost bloku 128 kB. |  |  |
|  | * NL-SAS vrstva: Propustnost: min. 3.500 MB/s, poměr čtení:zápis 50:50, 100% sekvenční zátěž, velikost bloku 1024 kB. |  |  |
|  | * Celková velikost cache/RAM v jednom řadiči je minimálně 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. |  |  |
|  | * Řešení musí poskytovat nativní replikace po FC nebo IP v minimálně v synchronních a asynchronních režimech. Podpora replikace dat do třetí lokality. |  |  |
|  | * Řešení musí podporovat min. následujících režimů: RAID 1, 6 a 10 nebo distribuovaný RAID 1 a 6. |  |  |
|  | * Diskový subsystém musí disponovat vytvářením 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). |  |  |
|  | * Upgrade software a hardware u řadičů musí být proveditelný 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; |  |  |
|  | * Počet sparedisků dle doporučení výrobce. |  |  |
|  | * Podporovány musí být enterprise SSD disky, Flash moduly a HDD disky, DWPD hodnota nabízených flash a SSD disků/modulů musí být 1 nebo vyšší. |  |  |
|  | 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. |  |  |
|  | Management /Řídící software | * MGMT rozhraní ve webové nebo grafické podobě. |  |  |
|  | * MGMT rozhraní musí umožnit 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) |  |  |
|  | * Řešení musí umožňovat 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 % |  |  |
|  | Rozšiřitelnost | * Minimálně o 50% v obou vrstvách (SSD/flash, NL-SAS). |  |  |
|  | * Škálování kapacit je prováděno pomocí expanzních jednotek. |  |  |
|  | * Dodavatel uvede možnosti rozšiřitelnosti cache a počty FC připojení. |  |  |
|  | Záruka | * 6 let, 24x7, oprava do 24h |  |  |
| * Komunikace výhradně v českém jazyce |  |  |
| * Záruku garantuje přímo výrobce zařízení |  |  |

Tabulka 23 - Parametry zálohovacích diskových polí

#### Páskové knihovny

|  |  |  |  |
| --- | --- | --- | --- |
| **Pásková knihovna** | | | |
| **Číslo** | **Název komponenty** | **Part number** | **Počet kusů** |
|  |  |  |  |

Tabulka 24 - 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. |  |  |
|  | Technické vlastnosti a rozměry | * Dodavatel uvede velikost a hmotnost. |  |  |
|  | * Dodavatel uvede počet a typ napájení (C13/14 nebo C19/C20 a počet). |  |  |
|  | * Dodavatel uvede typický a maximální elektrický příkon. |  |  |
|  | * Dodavatel uvede, jaké jsou požadavky na elektrické jištění. |  |  |
|  | Napájení | * Zařízení musí mít redundantní napájecí zdroje 250VAC. |  |  |
|  | Konektivita | * Nové LTO mechaniky musí být připojeny pomocí FC k SAN infrastruktuře minimálně 10ks min. 8 Gb/s (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. |  |  |
|  | Kapacita | * Objednatel požaduje osazení min. 480 ks LTO9 medií. |  |  |
|  | * Média včetně serializace dle pokynu Objednatele. |  |  |
|  | * Objednatel požaduje min. 480 ks aktivovaných slotů v každé knihovně. |  |  |
|  | * Objednatel požaduje min. 20 ks čistících médií pro každou knihovnu. |  |  |
|  | Rozšiřitelnost | * Objednatel požaduje možnost navýšit počet LTO9 mechanik min. až na 28ks. |  |  |
|  | * Zařízení musí mít možnost rozšířit počet slotů o min. 150%. |  |  |
|  | Záruka | * 6 let, 24x7, oprava do 24h |  |  |
| * Komunikace výhradně v českém jazyce |  |  |
| * Záruku garantuje přímo výrobce zařízení |  |  |
|  | Provozní a výkonnostní monitoring | * Řešení musí poskytovat minimálně chybové a diagnostické údaje o stavu knihovny i mechanik. |  |  |
|  | Management /Řídící software | * MGMT rozhraní ve webové nebo grafické podobě. |  |  |

Tabulka 25 - 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** |
|  |  |  |  |

Tabulka 26 - 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; |  |  |
|  | * Zálohovací prostředí musí podporovat navržené páskové knihovny a navržená disková 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.; |  |  |
|  | Charakteristiky | * Řešení musí umožnit vytvoření aktiv-aktiv vysoce dostupného řešení zálohovacích komponent (primárního zálohovacího katalogu). |  |  |
|  | * Řešení musí podporovat stálé inkrementální zálohování (bez ohledu na typu zálohovaných dat). |  |  |
|  | * Objednatel požaduje SW řešení, které 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). |  |  |
|  | * Back-End kapacita dle používaných retenčních period a deduplikačního poměru musí být min.: **1826 TB** (1661 TiB); |  |  |
|  | Šifrování | * Přenos všech dat musí probíhat pouze mezi klientem a zálohovacím serverem; |  |  |
|  | * Během ukládání dat na LTO media musí být data zašifrována; |  |  |
|  | * Správu klíčů pro šifrování musí provádět zálohovací server; |  |  |
|  | Redukce dat | * Řešení musí obsahovat deduplikaci a komprimaci.; |  |  |
|  | Provozní a výkonnostní monitoring | * Řešení musí poskytovat reporting a centrální správu. |  |  |
|  | Záruka | * Podpora řešení a aktualizace po dobu 6 let |  |  |
| * Komunikace výhradně v českém jazyce |  |  |
| * Záruku garantuje přímo výrobce zařízení |  |  |

Tabulka 27 - 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** |
|  |  |  |  |

Tabulka 28 - 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. |  |  |
|  | * Řešení musí podporovat nabízená produkční disková pole. |  |  |
|  | 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). |  |  |
|  | * Řešení musí umožnit následnou práci se snímky (snapshot) pro automatické vytvoření aktivní kopie pro potřeby selhání, vývojových prostředí, patch management nebo bezpečnostního skenování dat. |  |  |
|  | * Řešení musí podporovat nesmazatelné a nemodifikovatelné hardwarové snímky (snapshot). |  |  |
|  | * 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. |  |  |
|  | * Implementace nástroje pro Detekce ransomware hrozeb je požadována ve virtuálním prostředí (VMware) nebo na dedikovaném fyzickém serveru s OS Linux. |  |  |
|  | Licenčně pokrytá kapacita | * Licenčně musí být pokryta kapacita min. **1500 TB** (1365 TiB). |  |  |
|  | * Řešení musí umožnit vytvářet konzistentní snímky (snapshoty) na min. **66,66%** kapacity diskového pole. |  |  |
|  | Záruka | * Podpora řešení a aktualizace po dobu 6 let |  |  |
| * Komunikace výhradně v českém jazyce |  |  |
| * Záruku garantuje přímo výrobce zařízení |  |  |

Tabulka 29 - Správa klonovacích funkcí

#### Detekce ransomware hrozeb

|  |  |  |  |
| --- | --- | --- | --- |
| **Detekce ransomware** | | | |
| **Číslo** | **Název komponenty** | **Part number** | **Počet kusů** |
|  |  |  |  |

Tabulka 30 - 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. |  |  |
|  | * Řešení musí být kompatibilní s virtualizací: PowerVM (V3/V4), VMware (V7 a vyšší). |  |  |
|  | * Řešení musí podporovat nabízená produkční disková pole. |  |  |
|  | 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). |  |  |
|  | * Implementace nástroje pro Detekce ransomware hrozeb je požadována ve virtuálním prostředí (VMware) nebo na dedikovaném fyzickém serveru s OS Linux. |  |  |
|  | * Skenování musí probíhat automaticky. |  |  |
|  | * Nástroj pro detekci ransomware hrozeb musí umožnit integraci do nástroje pro správu klonovacích funkcí. |  |  |
|  | * Hlášení o pozitivní detekci/anomálii/podezřelé operaci ransomwarového útoku musí být integrovatelené softwarového řešení pro správu snapshotů (pro účely Infrastrukturního týmu). |  |  |
|  | * Dodavatel uvede informace o možnosti případné integraci s řešením SIEM. |  |  |
|  | Licenčně pokrytá kapacita | * Licenčně je třeba mít pokryto min. **1500 TB** (1365 TiB). |  |  |
|  | * Řešení musí detekovat ransomware na min. 66,66% kapacity nabízených produkčních diskových polí. |  |  |
|  | Záruka | * Podpora řešení a aktualizace po dobu 6 let |  |  |
| * Komunikace výhradně v českém jazyce |  |  |
| * Záruku garantuje přímo výrobce zařízení |  |  |

Tabulka 31 - 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 32 – 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 33 - 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 34 - 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** |
|  |  |  |  |

Tabulka 35 - 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. |  |  |
|  | * Počet serverů: 2ks identických parametrů. |  |  |
|  | * Servery musí být binárně kompatibilní se stávajícími servery Objednatele a umožňovat mobilní transfer virtuálních serverů. |  |  |
|  | * Servery musí splňovat požadavky na zajištění provozu jak ve standardním režimu, tak v režimu při výpadku. |  |  |
|  | Výkon | * Objednatel požaduje min. výkon CPU pro jeden server: **1 249 319** SAPs. |  |  |
|  | Rozšiřitelnost výkonu | * Navržené řešení musí umožňovat rozšíření prostým přidáním nebo aktivací procesorů. |  |  |
|  | * Objednatel požaduje min. rozšiřitelnost výkonu CPU pro jeden server: **1 584 990** SAPs. |  |  |
|  | RAM kapacita | * Objednatel požaduje min. kapacitu RAM pro jeden server: **38 912** GB. |  |  |
|  | Rozšiřitelnost RAM | * Navržené řešení musí umožňovat rozšíření prostým přidáním nebo aktivací RAM. |  |  |
|  | * Objednatel požaduje min. rozšiřitelnost RAM pro jeden server: **61 440** GB. |  |  |
|  | * Řešení musí být rozšiřitelné bez nutnosti výměny paměťových modulů (musí zůstat dostatek volných pozic pro přidání). |  |  |
|  | IO | * Minimální počet IO PCIe pozic: 32. |  |  |
|  | IO – Ethernet 25Gbit | * Minimální požadovaný počet Ethernet rozhraní: 48x min. 25 Gb/s typ SR (osazeny SFP28) pro jeden server. |  |  |
|  | * Ethernet adaptéry musí být podporovány pro nabízenou virtualizaci, operační systémy a zajištění vysoké dostupnosti. |  |  |
|  | * Dodavatel uvede počet adaptérů nutných pro dosažení požadovaného počtu portů. |  |  |
|  | IO – Ethernet SR-IOV | * Nabízené Ethernet 25 Gbit adaptéry musí podporovat SR-IOV virtualizační technologii. |  |  |
|  | IO – Fibre Channel | * Minimální požadovaný počet FC rozhraní: 16 x min. 64 Gb/s (osazeny SPF+) pro jeden server. |  |  |
|  | * FC adaptéry musí být podporovány pro nabízenou virtualizaci, operační systémy a zajištění vysoké dostupnosti. |  |  |
|  | * Dodavatel uvede počet adaptérů nutných pro dosažení požadovaného počtu portů. |  |  |
|  | IO – SSD | * Server musí disponovat min. 8 ks NVMe disků o min. kapacitě 1,6 TB každý (disky pro potřeby systémových virtuálních serverů). |  |  |
|  | Virtualizace | * Servery musí podporovat migraci virtuálních serverů ze současného HW na nově dodaný včetně příslušné licence a podpory. |  |  |
|  | * Dodávka musí obsahovat licence na virtualizaci pro všechny nabízená procesorová jádra včetně příslušné licenční podpory. |  |  |
|  | * Virtualizace musí podporovat současný běh různých verzi OS. |  |  |
|  | OS – SAP/Oracle | * Součástí dodávky musí být licence big-endien OS (aktuálně je provozován AIX 7.2). |  |  |
|  | * Licencí musí být zajištěno min. na 80ks jader pro každý server. |  |  |
|  | 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. |  |  |
|  | * Licence ve verzi certifikované pro provoz SAP/HANA PROD a nonPROD. |  |  |
|  | Clusterware | * Pro zajištění vysoké dostupnosti musí být součástí nabídky licence řešení vysoké dostupnosti pro big-endien OS. |  |  |
|  | * Licencí musí být zajištěno min. na 50ks jader pro každý server. |  |  |
|  | * 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. |  |  |
|  | Management /Řídící software | * SW pro zajištění správy musí být součástí dodávky |  |  |
|  | * Řídící konzole pro virtualizaci (minimálně jedna na každý výpočetní server). |  |  |
|  | Technické vlastnosti a rozměry | * Kompatibilní s RACK 19”. |  |  |
|  | * Dodavatel uvede velikost v EIA (jednotek U) pro systémovou skříň 19”. |  |  |
|  | * Dodavatel uvede počet a typ napájení (C13 a počet). |  |  |
|  | * Dodavatel uvede typický a maximální elektrický příkon. |  |  |
|  | * Dodavatel uvede, jaké jsou požadavky na elektrické jištění. |  |  |
|  | Napájení | * Zařízení musí mít 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); |  |  |
|  | * Řešení musí poskytovat Alerty a agenty pro virtualizaci a nabízené operační systémy. |  |  |
|  | Záruka | * Na HW komponenty 6 let, 24x7, oprava do 24h |  |  |
| * Na SW komponenty 6 let podpora včetně předplacených aktualizací a nových verzí |  |  |
| * Komunikace výhradně v českém jazyce |  |  |
| * Záruku garantuje přímo výrobce zařízení |  |  |

Tabulka 36 - 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** |
|  |  |  |  |

Tabulka 37 - 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. |  |  |
|  | * Servery musí být binárně kompatibilní se stávajícími servery Objednatele a umožňovat mobilní transfer virtuálních serverů. |  |  |
|  | * Servery musí splňovat požadavky na zajištění provozu jak ve standardním režimu, tak v režimu při výpadku. |  |  |
|  | Výkon | * Požadovaný výkon je min. 200000 SAPs. |  |  |
|  | Rozšiřitelnost výkonu | * Není vyžadována. |  |  |
|  | RAM kapacita | * Objednatel požaduje min. kapacitu RAM pro jeden server: **1** TB |  |  |
|  | Rozšiřitelnost RAM | * Navržené řešení musí umožňovat rozšíření prostým přidáním RAM stejného modulu. |  |  |
|  | * Objednatel požaduje min. rozšiřitelnost RAM pro jeden server: **4** TB. |  |  |
|  | * Řešení musí být rozšiřitelné bez nutnosti výměny paměťových modulů (musí zůstat dostatek volných pozic pro přidání). |  |  |
|  | IO | * Minimální počet IO PCIe pozic: 10. |  |  |
|  | IO – Ethernet 25Gbit | * Minimální požadovaný počet Ethernet rozhraní: 8x min. 25 Gb/s typ SR (osazeny SFP28) pro jeden server. |  |  |
|  | * Ethernet adaptéry musí být podporovány pro nabízenou virtualizaci, operační systémy a zajištění vysoké dostupnosti. |  |  |
|  | * Dodavatel uvede počet adaptérů nutných pro dosažení požadovaného počtu portů. |  |  |
|  | IO – Ethernet SR-IOV | * Nabízené Ethernet min. 25 Gb/s adaptéry musí podporovat 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). |  |  |
|  | * FC adaptéry musí být podporovány pro nabízenou virtualizaci, operační systémy a zajištění vysoké dostupnosti. |  |  |
|  | * Dodavatel uvede počet adaptérů nutných pro dosažení požadovaného počtu portů. |  |  |
|  | IO – SSD | * Server musí disponovat min. 8 ks NVMe disků o min. kapacitě 500 GB každý (disky pro potřeby systémových virtuálních serverů). |  |  |
|  | Virtualizace | * Servery musí podporovat migraci virtuálních serverů ze současného HW na nově dodaný včetně příslušné licence a podpory. |  |  |
|  | * Dodávka musí obsahovat licence na virtualizaci pro všechny nabízená procesorová jádra včetně příslušné licenční podpory. |  |  |
|  | * Virtualizace musí podporovat současný běh různých verzi OS. |  |  |
|  | OS – Backup | * Součástí dodávky musí být licence big-endien OS (aktuálně je provozován AIX 7.2). |  |  |
|  | Clusterware | * Pro zajištění vysoké dostupnosti musí být součástí nabídky licence řešení vysoké dostupnosti pro big-endien OS. |  |  |
|  | * Licencí musí být zajištěno min. na 24ks jader pro každý server. |  |  |
|  | Technické vlastnosti a rozměry | * Kompatibilní s RACK 19”. |  |  |
|  | * Dodavatel uvede velikost v EIA (jednotek U) pro systémovou skříň 19”. |  |  |
|  | * Dodavatel uvede počet a typ napájení (C13/14 nebo C19/C20 a počet). |  |  |
|  | * Dodavatel uvede typický a maximální elektrický příkon. |  |  |
|  | * Dodavatel uvede, jaké jsou požadavky na elektrické jištění. |  |  |
|  | Napájení | * Zařízení musí mít redundantní napájecí zdroje 250VAC, vyměnitelné za chodu. |  |  |
|  | Záruka | * Na HW komponent 6 let, 24x7, oprava do 24h. |  |  |
| * Na SW komponenty 6 let podpora včetně předplacených aktualizací a nových verzí. |  |  |
| * Komunikace výhradně v českém jazyce. |  |  |
| * Záruku garantuje přímo výrobce zařízení. |  |  |

Tabulka 38 - 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 39 - 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 40 - 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 pro SAP prostředí s neomezeným počtem virtuálních serverů a produkční podporou pro tyto licence v režimu 24x7 po dobu 6 let. 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** |
|  |  |  |  |

Tabulka 41 - 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”. |  |  |
|  | * Dodavatel uvede velikost v EIA (jednotek U) pro systémovou skříň 19”. |  |  |
|  | * Dodavatel uvede počet a typ napájení (C13/14 nebo C19/C20 a počet). |  |  |
|  | * Dodavatel uvede elektrický příkon při 70% a 100% utilizaci pro jeden server. |  |  |
|  | * Dodavatel uvede teplotní vyzařování při 70% a 100% utilizaci pro jeden server |  |  |
|  | * Beznástrojové kolejnice pro montáž do racku. |  |  |
|  | Výkon | * Nabízené řešení musí obsahovat min. 2 procesory nejnovější generace s 28 jádry/CPU. |  |  |
|  | * Minimální výkon dle benchmarku SPEC CPU2017 (www.spec.org) sloupec Baseline ke dni zahájení zadávacího řízení:   + Integer Rates – 500   + Floating Point Rates – 630 |  |  |
|  | RAM kapacita | * Objednatel požaduje min. kapacitu RAM pro jeden server: **1** TB. |  |  |
|  | * Typ DDR5. |  |  |
|  | * Rychlost paměťových modulů min. 5600MHz. |  |  |
|  | Rozšiřitelnost RAM | * Navržené řešení musí umožňovat rozšíření prostým přidáním RAM stejného modulu. |  |  |
|  | * Řešení musí obsahovat min. 32 paměťových slotů s rozšiřitelností až na min. **2** TB při využití stávajících modulů. |  |  |
|  | 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. |  |  |
|  | RAID Řadič | * Bez interního RAID řadiče. |  |  |
|  | * Dedikovaný slot pro budoucí osazení řadiče. |  |  |
|  | IO | * Minimální počet IO PCIe pozic: 10. |  |  |
|  | * OCP slot. |  |  |
|  | * 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. |  |  |
|  | * Řešení musí obsahovat min. 2 ks oddělených síťových karet. |  |  |
|  | * Dodavatel uvede počet adaptérů nutných pro dosažení požadovaného počtu portů. |  |  |
|  | IO – Fibre Channel | * Minimální požadovaný počet FC rozhraní: 2x min. 64 Gb/s (osazeny SPF+) pro jeden server. |  |  |
|  | * Dodavatel uvede počet adaptérů nutných pro dosažení požadovaného počtu portů. |  |  |
|  | IO – ostatní zařízení | * VGA port, min. 3x USB generace 3.1 na zadní straně 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). |  |  |
|  | * Port pro připojení diagnostického displeje. |  |  |
|  | Virtualizace | * Servery musí podporovat hypervizor VMware vSphere ESXi. |  |  |
|  | * Dodávka musí obsahovat virtualizační licence VMware vSphere VVF pro všechny poptávané procesory na min. 6 let včetně podpory. |  |  |
|  | 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. |  |  |
|  | * Aplikace, Licence na celé VMware prostředí s neomezeným množstvím virtuálních systémů. |  |  |
|  | Napájení | * Zařízení musí mít redundantní napájecí zdroje 250VAC, vyměnitelné za chodu. |  |  |
|  | * Certifikace Titanium. |  |  |
|  | * Výkon jednoho zdroje minimálně 1100 W. |  |  |
|  | Řídící software | * Vzdálené správa s dedikovaným vlastním portem RJ-45 a možností převzít plně vzdálené ovládání serveru. |  |  |
|  | * 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. |  |  |
|  | * 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). |  |  |
|  | * Možnost sdílet jednu virtuální konzoli více uživateli. |  |  |
|  | * Podpora standardních webových prohlížečů a HTML5. |  |  |
|  | * Možnost blokace konkrétní IP adresy. |  |  |
|  | * Real-time sledování vytíženosti CPU, paměti a spotřeby, možnost Power cappingu (včetně historických dat). |  |  |
|  | * Řešení musí poskytovat možnost asistované instalace OS bez dalších nástrojů, médií, ISO apod. |  |  |
|  | * Řešení musí poskytovat nejvyšší licence pro správu serveru bez jakéhokoli omezení funkcionalit/doby/provozu/počtu spravovaných serverů. |  |  |
|  | * Podpora proaktivních upozornění využívající technologii S.M.A.R.T. a PFA. |  |  |
|  | * Slot pro micro SD kartu o kapacitě alespoň 4GB. |  |  |
|  | * Možnost správy a synchronizace konfigurace a úrovně firmware pro několik serverů najednou. |  |  |
|  | Provozní a výkonnostní monitoring | * Časově neomezená licence na hromadnou správu serverů, inventarizace a alerting. |  |  |
|  | * Možnost hromadného sledováni a upgrade úrovní FW jednotlivých komponent serverů. |  |  |
|  | * Call Home funkce. |  |  |
|  | * Plug-in do management nodů virtualizačních hypervizorů (minimálně VMware vCenter, VMware Aria Suite, Microsoft Admin Center, Microsoft System Center, Nagios). |  |  |
|  | * Podpora REST-API a Redfish standardů. |  |  |
|  | * Podpora standardních Webových prohlížečů a HTML5. |  |  |
|  | * Software musí být bezagentový. |  |  |
|  | Záruka | * Na HW komponenty 6 let, 24x7, oprava do 24h. |  |  |
| * Na SW komponenty 6 let podpora včetně předplacených aktualizací a nových verzí. |  |  |
| * Komunikace výhradně v českém jazyce. |  |  |
| * Záruku garantuje přímo výrobce zařízení. |  |  |

Tabulka 42 - Technické parametry pro platformu x86

## Aplikační a Systémový Monitoring

### Popis současného stavu

Objednatel v současné době aplikační monitoring nevyužívá.

### Požadavky na nové řešení

Objednatel požaduje spolehlivou platformu pro monitoring poskytující komplexní přehled o výkonu a dostupnosti aplikací a související systémové infrastruktury. Monitoring bude primárně zaměřen na platformy Power s OS AIX a Linux a x86 s VMware. Z aplikační úrovně SAP a s tím spojené databáze Oracle, HANA a middleware komponenty. 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;
* Monitorování aplikací a trasování uživatelských transakcí;
* Monitorování mobilních aplikací a trasování uživatelských transakcí;
* Monitorování webových stránek a trasování uživatelských transakcí;
* 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 aplikací a 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 výrazné 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 požadovanou funkcionalitu monitorovacího systému. Nesmí být samostatně licencována a zpoplatněna serverová část monitorovacího systému, jednotlivé funkcionality, funkční moduly, množství a druh monitorovaných transakcí či množství uložených dat.

|  |  |  |  |
| --- | --- | --- | --- |
| **Aplikační a systémový monitoring** | | | |
| **Číslo** | **Název komponenty** | **Part number** | **Počet kusů** |
|  |  |  |  |

Tabulka 43 - Identifikace komponenty Aplikační a systémový monitoring

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

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Aplikační a systémový monitoring** | | | | |
| **Číslo** | **Vlastnost**  **/ komponenta** | **Požadované parametry** | **Splňuje ANO/NE** | **Skutečné parametry/Způsob splnění požadavku** |
|  | Komplexní monitorování | * Monitorovací systém musí monitorovat a aplikace a aplikační datové toky (transakce), služby, infrastrukturu, operační systémy, uživatelské transakce z webových prohlížečů a mobilních aplikací. |  |  |
|  | * Nakolektovaná data budou analyzována a zobrazena ve webovém nebo grafickém UI formou uživatelsky definovaných dashboardů. |  |  |
|  | * Výstupy budou formou alertů, notifikací včetně integrace s externími systémy. |  |  |
|  | Monitorování v reálném čase | * Řešení musí monitorovat aplikace a infrastrukturu v reálném čase. Bude poskytovat kontinuální viditelnost výkonu aplikací, včetně časů odezvy, propustnosti a chyb. |  |  |
|  | **Datová granularita** | * Monitorovací nástroj musí data sbírat a poskytovat s granularitou minimálně 1 sekunda po dobu 24 hodin. |  |  |
|  | **End-to-end trasování** | * Nástroj bude poskytovat trasování (zachycování jednotlivých volání) aplikačních transakcí napříč všemi komponentami. Řešení musí poskytovat podrobné transakční záznamy od uživatele směrem do monitorované aplikace. |  |  |
|  | **Sampling** | * Sampling trasovacích dat není přípustný, řešení musí sbírat a uchovat 100 % všech skutečných volání (transakcí) alespoň po dobu jednoho týdne. |  |  |
|  | **Automatické discovery** | * Řešení musí průběžně a automaticky zjišťovat a mapovat jednotlivé monitorované entity a jejich vzájemné vazby. |  |  |
|  | **Aplikační topologie** | * Monitorovací nástroj musí umět získané informace a závislosti o infrastruktuře a datových tocích mezi jednotlivými komponentami (službami) zobrazit graficky. |  |  |
|  | **Analytika** | * Nabízené řešení musí poskytovat prediktivní analýzy, které umožní předvídat a předcházet potenciálním problémům. |  |  |
|  | **Podpora systémů a platforem** | * Řešení musí podporovat minimálně: Intel x86 a Power servery, operační systémy Linux, AIX, Windows. Dále musí být monitorovány platformy VMware, PowerVM, Power HMC. Dodavatel uvede, jaké další řešení podporuje, především pro kontejnerizaci, Kubernetes/OpenShift a pro cloudová prostředí. |  |  |
|  | **Možnosti nasazení** | * Požadována je instalace monitoring serveru na x86 platformě (Linux bare metal nebo VMWare). |  |  |
|  | **Instalace agentů** | * Požadované prostředí, na kterých se bude agent instalovat: Linux, AIX, Windows. |  |  |
|  | **Podpora otevřených standardů a OpenTelemetry** | * Systém musí podporovat integraci s běžnými open-source technologiemi (Prometheus, Grafana) a nativně musí podporovat i standard OpenTelemetry. |  |  |
|  | Monitoring SAP | * Monitorovací nástroj musí umět monitorovat SAP a jeho moduly. |  |  |
|  | Monitoring VMWare | * Monitorovací nástroj musí podporovat VMWare vCenter. |  |  |
|  | Monitoring PowerVM | * Monitorovací nástroj musí podporovat PowerVM nebo PowerVM pomocí HMC. |  |  |
|  | Licencování | * Licenční metrika musí zohledňovat dané monitorované prostředí (dle počtu virtuálních serverů) a bude v sobě zahrnovat veškerou požadovanou funkcionalitu monitorovacího systému. |  |  |
|  | * Nabídka monitorovacího řešení musí pokrývat minimálně **465** virtuálních serverů. |  |  |
|  | Rozšiřitelnost | * Navržené řešení musí umožňovat rozšíření licencí min. o **200** ks. |  |  |
|  | Záruka | * Podpora řešení a aktualizace po dobu 6 let. |  |  |
| * Komunikace výhradně v českém jazyce. |  |  |
| * Záruku garantuje přímo výrobce zařízení |  |  |

Tabulka 44 - Technické parametry řešení pro aplikační 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.