**Załącznik nr 1 do SWZ - modyfikacja**

**Opis przedmiotu zamówienia**

**Wyposażenie serwerowni w sprzęt serwerowy, oprogramowane systemowe i bazodanowe**

1. **Serwer – 4 sztuki na potrzeby wirtualizacji środowisk systemów informatycznych Szpitala**

**Producent……………………..**

**Typ …………………………..**

**Model …………………………..**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **LP** | **Parametr lub warunek** | | **Minimalne wymagania – Serwery** | **Parametry oferowane** |
| 1 | Obudowa | | -Typu Rack, wysokość maksimum 1U;  - Dostarczona wraz z szynami umożliwiającymi pełne wysunięcie serwera oraz ramieniem z tyłu obudowy porządkującym ułożenie przewodów w szafie rack;  - serwer wyposażony w blokadę z przodu obudowy wyjęcia dysków zamykaną na klucz |  |
| 2 | Płyta główna | | -Dwuprocesorowa, zaprojektowana i wyprodukowana przez producenta serwera, możliwość instalacji procesorów czterdziestordzeniowych;  -wyposażona w minimum 32 gniazda pamięci RAM typu DDR4, obsługa do 4000GB pamięci RAM DDR4 3200 MHz i do 10000GB pamięci RAM DDR4 i Optane PMem  -Minimum 3 uniwersalne złącza PCI Express generacji 4, w tym minimum 3 złącza o prędkości x16;  -Wszystkie złącza PCI Express muszą być aktywne;  -Minimum 2 sloty dla dysków M.2 na płycie głównej (lub dedykowanej karcie PCI Express) nie zajmujące klatek dla dysków hot-plug; (Możliwość integracji dedykowanej, wewnętrznej pamięci flash przeznaczonej dla wirtualizatora w slocie M.2 na płycie głównej, bez zajmowania klatek dyskowych serwera)  - moduł TPM 2.0 |  |
| 3 | Procesory | | Zainstalowane dwa procesory 8-rdzeniowe w architekturze x86, pracujące z częstotliwością bazowa min 3,2 GHz, osiągające w oferowanym modelu serwera lub w innym modelu serwera 2-procesorowego tego samego producenta co serwer oferowany, w testach wydajności SPECrate2017\_int\_base minimum 145 pkt.  Wymagany wynik wydajności musi być dostępny na stronie spec.org nie później niż na dzień składania ofert; |  |
| 4 | Pamięć RAM | | -Zainstalowane 256 GB pamięci RAM typu DDR4 Registered, 3200Mhz  -Wsparcie dla technologii zabezpieczania pamięci Advanced ECC, Memory Scrubbing, lub równoważnej;  -Wsparcie serwera dla konfiguracji kopii lustrzanej pamięci RAM (memory mirror); |  |
| 5 | Dyski twarde | | -Fizyczna możliwość instalacji minimum 8-ciu dysków Hot-Plug SSD i mechanicznych z interfejsami SATA/SAS/NL-SAS o rozmiarze 2,5”  - zainstalowane 3xSSD 480GB 6G  - zainstalowane dwa dyski 240GB SSD M2 wraz z kontrolerem sprzętowym zapewniającym Raid 1  - Zainstalowany kontroler SAS RAID obsługujący poziomy 0,1,10,5,50,6,60 posiadający 8GB pamięci cache (wraz z podtrzymaniem bateryjnym) |  |
| 6 | Kontrolery LAN/FC | | Karta LAN, nie zajmująca żadnego z dostępnych slotów PCI Express, wyposażona minimum w interfejsy: 4x 1Gbit Base-T oraz 2x10G SFP, możliwość wymiany zainstalowanych interfejsów na 2x 100Gbit QSFP28 bez konieczności instalacji kart w slotach PCIe;  - zainstalowana karta 2x 10Gbit Base-T  - zainstalowana karta 2x 16Gb FC  Serwer wyposażony w 2 interfejsy 1Gbit Base-T oraz 2 x 10G SFP nie zajmujące slotów PCIe oraz umożliwiające wymianę na 2 x 100Gbit QSFP28 bez konieczności instalacji kart w slotach PCIe.” |  |
| 7. | Napędy | | - zainstalowany wewnętrzny napęd DVD-RW |  |
| 8. | Porty | | -zintegrowana karta graficzna ze złączem VGA z tyłu serwera;  -1x USB 2.0/3.0 dostępne na froncie obudowy  -1x USB 2.0/3.0 dostępne z tyłu serwera  -1x USB 2.0/3.0 wewnątrz serwera  Ilość dostępnych złącz VGA i USB nie może być osiągnięta poprzez stosowanie zewnętrznych przejściówek, rozgałęziaczy czy dodatkowych kart rozszerzeń zajmujących jakikolwiek slot PCI Express serwera; |  |
| 9 | | Zasilanie, chłodzenie | -Redundantne zasilacze hotplug o mocy minimum 900W, o sprawności 96% (tzw. klasa titanium), z kablami zasilającymi 2,5m (IEC 320 C14 -> C13)  -Redundantne wentylatory hotplug; |  |
| 10 | | Zarządzanie | -Wbudowane diody informacyjne lub wyświetlacz LCD informujący o stanie serwera (system przewidywania, rozpoznawania awarii) – co najmniej informacja o statusie pracy (poprawny/przewidywana usterka lub usterka) następujących komponentów: karty rozszerzeń zainstalowane w dowolnym slocie PCI Express, procesory CPU, pamięć RAM z dokładnością umożliwiającą jednoznaczną identyfikację uszkodzonego modułu pamięci RAM, wbudowany na płycie głównej nośnik pamięci M.2 SSD, status karty zrządzającej serwera, wentylatory, bateria podtrzymująca ustawienia BIOS/Płyty głównej, zasilacze - poprawność napięć elektrycznych płyty głównej w trybie włączonym (on) i oczekiwania (standby) serwera,  -Zintegrowany z płytą główną serwera kontroler sprzętowy zdalnego zarządzania zgodny z IPMI 2.0 o funkcjonalnościach:   * Niezależny od systemu operacyjnego, sprzętowy kontroler umożliwiający pełne zarządzanie, zdalny restart serwera; * Dedykowana karta LAN 1 Gb/s (dedykowane złącze RJ-45 z tyłu obudowy) do komunikacji wyłącznie z kontrolerem zdalnego zarządzania z możliwością przeniesienia tej komunikacji na inną kartę sieciową współdzieloną z systemem operacyjnym; * Dostęp poprzez przeglądarkę Web (także SSL, SSH) * Zarządzanie mocą i jej zużyciem oraz monitoring zużycia energii * Zarządzanie alarmami (zdarzenia poprzez SNMP) * Możliwość przejęcia konsoli tekstowej serwera * Przekierowanie konsoli graficznej na poziomie sprzętowym oraz możliwość montowania zdalnych napędów i ich obrazów na poziomie sprzętowym (cyfrowy KVM) * Sprzętowy monitoring serwera w tym stanu dysków twardych i kontrolera RAID (bez pośrednictwa agentów systemowych) * Oprogramowanie zarządzające i diagnostyczne wyprodukowane przez producenta serwera umożliwiające konfigurację kontrolera RAID, instalację systemów operacyjnych, zdalne zarządzanie, diagnostykę i przewidywanie awarii w oparciu o informacje dostarczane w ramach zintegrowanego w serwerze systemu umożliwiającego monitoring systemu i środowiska (m.in. temperatura, dyski, zasilacze, płyta główna, procesory, pamięć operacyjna itd.). * Rozwiązanie musi umożliwiać konfigurację i uruchomienie automatycznego powiadomienia serwisu o zbliżającej się lub istniejącej usterce serwera (co najmniej dyski twarde, zasilacze, pamięć RAM, procesory, wentylatory, kontrolery RAID, karty rozszerzeń); * Możliwość zapisu i przechowywania informacji i logów o pełnym stanie maszyny, w tym usterki i sytuacje krytyczne w obrębie wbudowanej pamięci karty zarządzającej - dostęp do tych informacji musi być niezależny od stanu włączenia serwera oraz stanu sprzętowego w tym np. usterki elementów poza kartą zarządzającą; * karta zarządzająca musi umożliwiać konfigurację i uruchomienie automatycznego informowania autoryzowanego serwisu producenta serwera o zaistniałej lub zbliżającej się usterce (wymagana jest możliwość automatycznego otworzenia zgłoszenia serwisowego bezpośrednio w systemie producenta serwera, nie dopuszcza się komunikacji SNMP czy email). Jeżeli są wymagane jakiekolwiek dodatkowe licencje lub pakiety serwisowe potrzebne do uruchomienia automatycznego powiadamiania autoryzowanego serwisu o usterce należy takie elementy wliczyć do oferty – czas trwania minimum równy dla wymaganego okresu gwarancji producenta serwera; |  |
| 11 | | Wspierane OS | Wspierane przez producenta serwera systemy operacyjne:  - Windows 2016, Windows 2019, Windows 2022, RedHat EL 7, RedHat EL 8, Suse ES 15, VMware vSphere 7.0 |  |
| 12 | | Gwarancja | - **min. 60 miesiące** gwarancji producenta serwera w trybie on-site z gwarantowaną naprawą w miejscu użytkowania sprzętu do końca następnego dnia od zgłoszenia. Naprawa realizowana przez producenta serwera lub autoryzowany przez producenta serwis.  -Dostępność części zamiennych co najmniej przez 5 lat od momentu zakupu serwera;  -Wymagana jest bezpłatna dostępność poprawek i aktualizacji BIOS/Firmware/sterowników dożywotnio dla oferowanego serwera – jeżeli funkcjonalność ta wymaga dodatkowego serwisu lub wsparcia wykupionego od producenta lub licencji producenta serwera koszt ten musi być uwzględniony w oferowanej konfiguracji;  -Wymagana możliwość automatycznego powiadamiania o awarii serwera centrum serwisowego producenta. Jeżeli funkcja taka jest płatna koszt ten musi być uwzględniony w oferowanej konfiguracji; | Podać: |
| 13 | | Dokumentacja, inne | -Elementy, z których zbudowane są serwery muszą być produktami producenta tych serwerów lub być przez niego certyfikowane dla oferowanego modelu serwera oraz muszą być objęte gwarancją producenta, o wymaganym w specyfikacji poziomie SLA (wymagane oświadczenie producenta serwera potwierdzające spełnienie wymagań dołączone do oferty).  -Serwer musi być fabrycznie nowy i pochodzić z oficjalnego kanału dystrybucyjnego w Polsce - Wymagane oświadczenie producenta serwera lub jego polskiego przedstawicielstwa, że oferowany sprzęt spełnia ten wymóg;  -Oferent zobowiązany jest dostarczyć wraz z ofertą kartę produktową oferowanego serwera umożliwiającą weryfikację podstawowych parametrów oferowanego sprzętu w języku polskim lub angielskim;  -Ogólnopolska, telefoniczna linia techniczna producenta serwera (ogólnopolski numer stacjonarny lub o zredukowanej odpłatności 0-800/0-801) umożliwiająca w czasie obowiązywania gwarancji na sprzęt po podaniu numeru seryjnego urządzenia: zgłoszenie usterki sprzętowej urządzenia oraz weryfikację: konfiguracji sprzętowej serwera, w tym model i typ dysków twardych, procesora, ilość fabrycznie zainstalowanej pamięci operacyjnej, czasu obowiązywania i typ udzielonej gwarancji – obsługa w języku polskim, w trybie całodobowym również w dni świąteczne;  -Wymagane jest oświadczenie Producenta oferowanego serwera lub jego polskiego przedstawicielstwa, iż wymagany w postępowaniu poziom gwarancji i wsparcia na sprzęt został zaoferowany przez Producenta serwera;  -Możliwość aktualizacji i pobrania sterowników do oferowanego modelu serwera w najnowszych certyfikowanych wersjach bezpośrednio z sieci Internet za pośrednictwem strony www producenta serwera;  -Wszystkie parametry i funkcje oferowanego serwera muszą być wspierane przez producenta i zaimplementowane fabrycznie oraz dostępne w seryjnej produkcji danego modelu urządzenia.  Zamawiający nie dopuszcza dostosowywania funkcji serwera na potrzeby niniejszego postępowania.  -Wszystkie parametry i funkcje oferowanego serwera muszą być potwierdzone w dokumentacji technicznej producenta. |  |

1. **Oprogramowanie do wirtualizacji**
2. Wymaga się dostarczenia licencji na poniższe funkcjonalności dla 4 serwerów 2 procesorowych oraz 1 instancji konsoli centralnej do zarządzania opisanej w dalszej części dokumentu. Oprogramowanie ze wsparciem na 3 lata.
3. Warstwa wirtualizacji musi być zainstalowana bezpośrednio na sprzęcie fizycznym bez dodatkowych pośredniczących systemów operacyjnych.
4. Rozwiązanie musi zapewnić możliwość obsługi wielu instancji systemów operacyjnych na jednym serwerze fizycznym i powinno się charakteryzować maksymalnym możliwym stopniem konsolidacji sprzętowej.
5. Oprogramowanie do wirtualizacji musi zapewniać możliwość stworzenia dysku maszyny wirtualnej o wielkości 62 TB.
6. Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych z możliwością przydzielenia 24 TB pamięci operacyjnej RAM.
7. Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych, z których każda może mieć 1-10 wirtualnych kart sieciowych.
8. Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych, z których każda może mieć 32 porty szeregowe.
9. Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych, z których każda może mieć 20 portów USB.
10. Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych, z których każda może mieć 4 GB pamięci graficznej.
11. Rozwiązanie musi umożliwiać łatwą i szybką rozbudowę infrastruktury o nowe usługi bez spadku wydajności i dostępności pozostałych wybranych usług.
12. Rozwiązanie powinno w możliwie największym stopniu być niezależne od producenta platformy sprzętowej.
13. Rozwiązanie musi wspierać następujące systemy operacyjne: Windows 7/8/10, Windows Server, Amazon Linux 2, macOS, OS X, Asianux, Ubuntu, CentOS, NeoKylin, CoreOS, Debian, FreeBSD, Oracle Linux, RHEL, SUSE, Photon OS.
14. Rozwiązanie musi umożliwiać przydzielenie większej ilości pamięci RAM dla maszyn wirtualnych niż fizyczne zasoby RAM serwera w celu osiągnięcia maksymalnego współczynnika konsolidacji.
15. Oprogramowanie do wirtualizacji powinno zapewnić możliwość wykonywania kopii migawkowych instancji systemów operacyjnych (tzw. snapshot) na potrzeby tworzenia kopii zapasowych bez przerywania ich pracy.
16. Rozwiązanie musi umożliwiać udostępnienie maszynie wirtualnej większej ilości zasobów dyskowych niż jest fizycznie zarezerwowane na dyskach lokalnych serwera lub na macierzy.
17. System musi posiadać funkcjonalność wirtualnego przełącznika sieciowego umożliwiającego tworzenie sieci wirtualnej w obszarze hosta i pozwalającego połączyć maszyny wirtualne w obszarze jednego hosta, a także na zewnątrz sieci fizycznej. Pojedynczy przełącznik wirtualny powinien mieć możliwość konfiguracji do 4000 portów.
18. Pojedynczy wirtualny przełącznik musi posiadać możliwość przyłączania do niego dwóch i więcej fizycznych kart sieciowych, aby zapewnić bezpieczeństwo połączenia ethernetowego w razie awarii karty sieciowej.
19. Wirtualne przełączniki musza obsługiwać wirtualne sieci lokalne (VLAN).
20. Polityka licencjonowania musi umożliwiać przenoszenie licencji na oprogramowanie do wirtualizacji pomiędzy serwerami różnych producentów z zachowaniem wsparcia technicznego i zmianą wersji oprogramowania na niższą (downgrade). Wsparcie techniczne musi być świadczone bezpośrednio przez producenta oprogramowania. Licencjonowanie nie może odbywać się w trybie OEM.
21. Oprogramowanie zarządzające musi posiadać możliwość przydzielania i konfiguracji uprawnień z możliwością integracji z usługami katalogowymi, w szczególności Microsoft Active Directory, Open LDAP.
22. Rozwiązanie musi posiadać wbudowany interfejs programistyczny (API) zapewniający pełną integrację zewnętrznych rozwiązań wykonywania kopii zapasowych z istniejącymi mechanizmami warstwy wirtualizacyjnej.
23. Rozwiązanie musi zapewniać mechanizm replikacji wskazanych maszyn wirtualnych pomiędzy różnymi systemami pamięci masowych.
24. Rozwiązanie musi zawierać funkcjonalność pozwalającą na ominięcie testów inicjalizacyjnych sprzętu fizycznego w celu szybkiego startu wirtualizatora.
25. Rozwiązanie musi zawierać możliwość zabezpieczania maszyn wirtualnych przez rozwiązania antywirusowe firm trzecich bez konieczności instalacji agenta wewnątrz maszyny wirtualnej.
26. Rozwiązanie musi mieć możliwość przenoszenia maszyn wirtualnych w czasie ich pracy, bez jakiegokolwiek przestoju i bez utraty danych, pomiędzy serwerami fizycznymi, niezależnie od dostępności współdzielonej przestrzeni dyskowej,
27. Rozwiązanie musi mieć możliwość przenoszenia maszyn wirtualnych w czasie ich pracy, bez jakiegokolwiek przestoju i bez utraty danych, pomiędzy zasobami dyskowymi, niezależnie od dostępności współdzielonej przestrzeni dyskowej,
28. Rozwiązanie musi mieć możliwość przenoszenia maszyn wirtualnych w czasie ich pracy, bez jakiegokolwiek przestoju i bez utraty danych, jednocześnie między serwerami fizycznymi oraz zasobami dyskowymi, niezależnie od dostępności współdzielonej przestrzeni dyskowej.
29. Musi zostać zapewniona odpowiednia redundancja i taki mechanizm (wysokiej dostępności HA), aby w przypadku awarii lub niedostępności serwera fizycznego wybrane przez administratora i uruchomione nim wirtualne maszyny zostały uruchomione na innych serwerach z zainstalowanym oprogramowaniem wirtualizacyjnym. Rozwiązanie musi posiadać co najmniej 2 niezależne mechanizmy wzajemnej komunikacji między serwerami oraz z serwerem zarządzającym, gwarantujące właściwe działanie mechanizmów wysokiej dostępności na wypadek izolacji sieciowej serwerów fizycznych lub partycjonowania sieci.
30. Rozwiązanie musi zapewniać wsparcie dla wirtualizacji zagnieżdżonej, w szczególności w zakresie możliwości zastosowania wszystkich funkcjonalności w tym Hyper-V systemu Windows Server na maszynie wirtualnej.
31. Rozwiązanie musi zapewniać możliwość dodawania zasobów w czasie pracy maszyny wirtualnej, w szczególności w zakresie ilości procesorów, pamięci operacyjnej i przestrzeni dyskowej.
32. Oprogramowanie do wirtualizacji musi zapewniać mechanizm takiego zabezpieczenia wybranych przez administratora wirtualnych maszyn, aby w przypadku awarii lub niedostępności serwera fizycznego maszyny, które na nim pracowały, były bezprzerwowo dostępne na innym serwerze z zainstalowanym oprogramowaniem wirtualizacyjnym. Mechanizm ten umożliwia zabezpieczenie maszyn wirtualnych wyposażonych w minimum 2 wirtualne procesory
33. Oprogramowanie musi posiadać centralną konsolę graficzną do zarządzania wieloma maszynami wirtualnymi oraz ich zasobami pracującymi na wielu serwerach fizycznych:

* globalne zarządzanie kontrolą dostępu do serwerów i maszyn wirtualnych
* wykonywanie automatycznych bądź manualnych zadań w celu optymalizacji infrastruktury dla maszyn wirtualnych.
* widok całego systemu i zbioru maszyn wirtualnych, mapy Infrastruktury.
* możliwość monitorowania dostępności i wydajności maszyn wirtualnych
* możliwość raportowania dostępności i wydajności maszyn wirtualnych
* funkcje ochrony dostępu zintegrowane z mechanizmem uwierzytelniania Windows
* planowanie zadań i ustawianie znaczników alarmów w celu generowania automatycznych powiadomień o statusie serwerów lub maszyn wirtualnych
* tworzenie obrazów maszyn wirtualnych
* klonowanie maszyn wirtualnych
* wykonywanie wielu kopii migawkowych (snapshoot) w każdym momencie pracy maszyny wirtualnej oraz możliwość powrotu do jej stanu z każdego momentu zrobienia kopii

1. **System Backup**

**Wymagania ogólne**

* Licencja na 30 systemów operacyjnych ze wsparciem na 3 lata.
* Oprogramowanie musi współpracować z infrastrukturą VMware w wersji 5.5, 6.0, 6.5 oraz 6.7 oraz Microsoft Hyper-V 2012, 2012 R2 i 2019. Wszystkie funkcjonalności w specyfikacji muszą być dostępne na wszystkich wspieranych platformach wirtualizacyjnych, chyba, że wyszczególniono inaczej
* Oprogramowanie musi współpracować z hostami zarządzanymi przez VMware vCenter oraz pojedynczymi hostami.
* Oprogramowanie musi współpracować z hostami zarządzanymi przez System Center Virtual Machine Manger, klastrami hostów oraz pojedynczymi hostami.
* Oprogramowanie musi zapewniać tworzenie kopii zapasowych wszystkich systemów operacyjnych maszyn wirtualnych wspieranych przez vSphere i Hyper-V
* Oprogramowanie musi zapewniać tworzenie kopii zapasowych z sieciowych urządzeń plikowych NAS opartych o SMB, CIFS i/lub NFS oraz bezpośrednio z serwerów plikowych opartych o Windows i Linux.
* Oprogramowanie musi być niezależne sprzętowo i umożliwiać wykorzystanie dowolnej platformy serwerowej i dyskowej
* Oprogramowanie musi tworzyć “samowystarczalne” archiwa do odzyskania których nie wymagana jest osobna baza danych z metadanymi deduplikowanych bloków
* Oprogramowanie musi pozwalać na tworzenie kopii zapasowych w trybach: Pełny, pełny syntetyczny, przyrostowy i odwrotnie przyrostowy (tzw. reverse-inremental)
* Oprogramowanie musi mieć mechanizmy deduplikacji i kompresji w celu zmniejszenia wielkości archiwów. Włączenie tych mechanizmów nie może skutkować utratą jakichkolwiek funkcjonalności wymienionych w tej specyfikacji
* Oprogramowanie musi zapewniać warstwę abstrakcji nad poszczególnymi urządzeniami pamięci masowej, pozwalając utworzyć jedną wirtualną pulę pamięci na kopie zapasowe. Wymagane jest wsparcie dla nieograniczonej liczby pamięci masowych to takiej puli.
* Oprogramowanie musi pozwalać na rozszerzenie lokalnej przestrzeni backupowej poprzez integrację z Microsoft Azure Blob, Amazon S3 oraz z innymi kompatybilnymi z S3 macierzami obiektowymi. Proces migracji danych powinien być zautomatyzowany. Jedynie unikalne bloki mogą być przesyłane w celu oszczędności pasma oraz przestrzeni na przechowywane dane. Funkcjonalność ta nie może mieć wpływu na możliwości odtwarzania danych.
* Oprogramowanie nie może przechowywać danych o deduplikacji w centralnej bazie. Utrata bazy danych używanej przez oprogramowanie nie może prowadzić do utraty możliwości odtworzenia backupu. Metadane deduplikacji muszą być przechowywane w plikach backupu.
* Oprogramowanie nie może instalować żadnych stałych agentów wymagających wdrożenia czy upgradowania wewnątrz maszyny wirtualnej dla jakichkolwiek funkcjonalności backupu lub odtwarzania
* Oprogramowanie musi mieć możliwość uruchamiania dowolnych skryptów przed i po zadaniu backupowym lub przed i po wykonaniu zadania snapshota.
* Oprogramowanie musi oferować portal samoobsługowy, umożliwiający odtwarzanie użytkownikom wirtualnych maszyn, obiektów MS Exchange i baz danych MS SQL oraz Oracle (w tym odtwarzanie point-in-time)
* Oprogramowanie musi zapewniać możliwość delegacji uprawnień do odtwarzania na portalu
* Oprogramowanie musi mieć możliwość integracji z innymi systemami poprzez wbudowane RESTful API
* Oprogramowanie musi mieć wbudowane mechanizmy backupu konfiguracji w celu prostego odtworzenia systemu po całkowitej reinstalacji
* Oprogramowanie musi mieć wbudowane mechanizmy szyfrowania zarówno plików z backupami jak i transmisji sieciowej. Włączenie szyfrowania nie może skutkować utratą jakiejkolwiek funkcjonalności wymienionej w tej specyfikacji
* Oprogramowanie musi posiadać mechanizmy chroniące przed utratą hasła szyfrowania
* Oprogramowanie musi wspierać backup maszyn wirtualnych używających współdzielonych dysków VHDX na Hyper-V (shared VHDX)
* Oprogramowanie musi posiadać architekturę klient/serwer z możliwością instalacji wielu instancji konsoli administracyjnych.

**Wymagania RPO**

* Oprogramowanie musi wykorzystywać mechanizmy Change Block Tracking na wszystkich wspieranych platformach wirtualizacyjnych. Mechanizmy muszą być certyfikowane przez dostawcę platformy wirtualizacyjnej
* Oprogramowanie musi oferować możliwość sterowania obciążeniem storage'u produkcyjnego tak aby nie przekraczane były skonfigurowane przez administratora backupu poziomy latencji. Funkcjonalność ta musi być dostępna na wszystkich wspieranych platformach wirtualizacyjnych
* Oprogramowanie musi oferować ten mechanizm z dokładnością do datastoru
* Oprogramowanie musi automatycznie wykrywać i usuwać snapshoty-sieroty (orphaned snapshots), które mogą zakłócić poprawne wykonanie backupu. Proces ten nie może wymagać interakcji administratora
* Oprogramowanie musi zapewniać tworzenie kopii zapasowych z bezpośrednim wykorzystaniem snapshotów macierzowych. Musi też zapewniać odtwarzanie maszyn wirtualnych z takich snapshotów. Proces wykonania kopii zapasowej nie może wymagać użycia jakichkolwiek hostów tymczasowych. Opisana funkcjonalność powinna działać w środowisku VMware i być dostępna dla następujących macierzy: HPE, Dell EMC, NetApp, Cisco, IBM, Lenovo, Fujitsu, Huawei, INFINIDAT, Pure Storage.
* Oprogramowanie musi posiadać wsparcie dla VMware vSAN potwierdzone odpowiednią certyfikacją VMware.
* Oprogramowanie musi wspierać kopiowanie backupów na taśmy wraz z pełnym śledzeniem wirtualnych maszyn
* Oprogramowanie musi posiadać wsparcie dla NDMP
* Oprogramowanie musi mieć możliwość tworzenia retencji GFS (Grandfather-Father-Son)
* Oprogramowanie musi umieć korzystać z protokołu DDBOOST w przypadku, gdy repozytorium backupów jest umiejscowione na Dell EMC DataDomain. Funkcjonalność powinna wspierać łącze sieciowe lub FC.
* Oprogramowanie musi umieć korzystać z protokołu Catalyst (w tym Catalyst Copy) w przypadku, gdy repozytorium backupów jest umiejscowione na HPE StoreOnce. Funkcjonalność powinna wspierać łącze sieciowe lub FC.
* Oprogramowanie musi wspierać BlockClone API w przypadku użycia Windows Server 2016 lub 2019 z systemem pliku ReFS jako repozytorium backupu. Podobna funkcjonalność musi być zapewniona dla repozytoriów opartych o linuxowy system plików XFS.
* Oprogramowanie musi mieć możliwość kopiowania backupów oraz replikacji wirtualnych maszyn z wykorzystaniem wbudowanej akceleracji WAN.
* Oprogramowanie musi mieć możliwość replikacji włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere, pomiędzy hostami ESXi, włączając asynchroniczną replikacją ciągłą. Dodatkowo oprogramowanie musi mieć możliwość użycia plików kopii zapasowych jako źródła replikacji.
* Oprogramowanie musi umożliwiać przechowywanie punktów przywracania dla replik
* Oprogramowanie musi umożliwiać wykorzystanie istniejących w infrastrukturze wirtualnych maszyn jako źródła do dalszej replikacji (replica seeding)
* Oprogramowanie musi posiadać takie same funkcjonalności replikacji dla Hyper-V
* Oprogramowanie musi wykorzystywać wszystkie oferowane przez hypervisor tryby transportu (sieć, hot-add, LAN Free-SAN)
* Oprogramowanie musi dawać możliwość tworzenia backupów ad-hoc z konsoli jak i z klienta webowego vSphere
* Oprogramowanie musi przetwarzać wiele wirtualnych dysków jednocześnie (parallel processing)

**Wymagania RTO**

* Oprogramowanie musi umożliwiać jednoczesne uruchomienie wielu maszyn wirtualnych bezpośrednio ze zdeduplikowanego i skompresowanego pliku backupu, z dowolnego punktu przywracania, bez potrzeby kopiowania jej na storage produkcyjny. Funkcjonalność musi być oferowana dla środowisk VMware oraz Hyper-V niezależnie od rodzaju storage’u użytego do przechowywania kopii zapasowych.
* Dodatkowo dla środowiska vSphere powyższa funkcjonalność powinna umożliwiać uruchomianie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna)
* Oprogramowanie musi pozwalać na migrację on-line tak uruchomionych maszyn na storage produkcyjny. Migracja powinna odbywać się mechanizmami wbudowanymi w hypervisor. Jeżeli licencja na hypervisor nie posiada takich funkcjonalności - oprogramowanie musi realizować taką migrację swoimi mechanizmami
* Oprogramowanie musi pozwalać na zaprezentowanie pojedynczego dysku bezpośrednio z kopii zapasowej do wybranej działającej maszyny wirtualnej vSpehre
* Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny, plików konfiguracji i dysków
* Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny bezpośrednio do Microsoft Azure, Microsoft Azure Stack oraz Amazon EC2.
* Oprogramowanie musi umożliwić odtworzenie plików na maszynę operatora, lub na serwer produkcyjny bez potrzeby użycia agenta instalowanego wewnątrz wirtualnej maszyny. Funkcjonalność ta nie powinna być ograniczona wielkością i liczbą przywracanych plików
* Oprogramowanie musi mieć możliwość odtworzenia plików bezpośrednio do maszyny wirtualnej poprzez sieć, przy pomocy VIX API dla platformy VMware i PowerShell Direct dla platformy Hyper-V.
* Oprogramowanie musi wspierać odtwarzanie plików z następujących systemów plików:
  + **Linux** 
    - ext2, ext3, ext4, ReiserFS, JFS, XFS, Btrfs
  + **BSD** 
    - UFS, UFS2
  + **Solaris** 
    - ZFS, UFS
  + **Mac** 
    - HFS, HFS+
  + **Windows** 
    - NTFS, FAT, FAT32, ReFS
  + **Novell OES** 
    - NSS
* Oprogramowanie musi wspierać przywracanie plików z partycji Linux LVM oraz Windows Storage Spaces.
* Oprogramowanie musi umożliwiać szybkie granularne odtwarzanie obiektów aplikacji bez użycia jakiegokolwiek agenta zainstalowanego wewnątrz maszyny wirtualnej.
* Oprogramowanie musi wspierać granularne odtwarzanie dowolnych obiektów i dowolnych atrybutów Active Directory włączając hasło, obiekty Group Policy, partycja konfiguracji AD, rekordy DNS zintegrowane z AD, Microsoft System Objects, certyfikaty CA oraz elementy AD Sites.
* Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Exchange 2010 i nowszych (dowolny obiekt w tym obiekty w folderze "Permanently Deleted Objects"),
* Oprogramowanie musi wspierać granularne odtwarzanie Microsoft SQL 2005 i nowsze włączając bazy danych z opcją odtwarzania point-in-time, tabele, schemat
* Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Sharepoint 2010 i nowsze. Opcja odtworzenia elementów, witryn, uprawnień.
* Oprogramowanie musi wspierać granularne odtwarzanie baz danych Oracle z opcją odtwarzanie point-in-time wraz z włączonym Oracle DataGuard. Funkcjonalność ta musi być dostępna dla baz uruchomionych w środowiskach Windows oraz Linux.
* Oprogramowanie musi pozwalać na zaprezentowanie baz MS SQL oraz Oracle bezpośrednio z pliku kopii zapasowej do działającego serwera bazodanowego
* Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez Oracle RMAN
* Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez SAP HANA
* Oprogramowanie musi wspierać także specyficzne metody odtwarzania w tym "reverse CBT" oraz odtwarzanie z wykorzystaniem sieci SAN

**Ograniczenie ryzyka**

* Oprogramowanie musi dawać możliwość stworzenia laboratorium (izolowane środowisko) dla vSphere i Hyper-V używając wirtualnych maszyn uruchamianych bezpośrednio z plików backupu. Dla VMware’a oprogramowanie musi pozwalać na uruchomienie takiego środowiska bezpośrednio ze snapshotów macierzowych stworzonych na wspieranych urządzeniach.
* Oprogramowanie musi umożliwiać weryfikację odtwarzalności wielu wirtualnych maszyn jednocześnie z dowolnego backupu według własnego harmonogramu w izolowanym środowisku. Testy powinny uwzględniać możliwość uruchomienia dowolnego skryptu testującego również aplikację uruchomioną na wirtualnej maszynie. Testy muszą być przeprowadzone bez interakcji z administratorem
* Oprogramowanie musi mieć podobne mechanizmy dla replik w środowisku vSphere
* Oprogramowanie musi umożliwiać integrację z oprogramowaniem antywirusowym w celu wykonania skanu zawartości pliku backupowego przed odtworzeniem jakichkolwiek danych. Integracja musi być zapewniona minimalnie dla Windows Defender, Symantec Protection Engine oraz ESET NOD32.

Oprogramowanie musi umożliwiać dwuetapowe, automatyczne, odtwarzanie maszyn wirtualnych z możliwością wstrzyknięcia dowolnego skryptu przed odtworzeniem danych do środowiska produkcyjnego.

1. **Serwer – 2 sztuki na potrzeby baz danych**

**Producent……………………..**

**Typ …………………………..**

**Model …………………………..**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **LP** | **Parametr lub warunek** | | **Minimalne wymagania – Serwery** | **Parametry oferowane** |
| 1 | Obudowa | | -Typu Rack, wysokość maksimum 1U;  - Dostarczona wraz z szynami umożliwiającymi pełne wysunięcie serwera oraz ramieniem z tyłu obudowy porządkującym ułożenie przewodów w szafie rack;  - serwer wyposażony w blokadę z przodu obudowy wyjęcia dysków zamykaną na klucz |  |
| 2 | Płyta główna | | -Dwuprocesorowa, zaprojektowana i wyprodukowana przez producenta serwera, możliwość instalacji procesorów czterdziestordzeniowych;  -wyposażona w minimum 32 gniazda pamięci RAM typu DDR4, obsługa do 4000GB pamięci RAM DDR4 3200 MHz i do 10000GB pamięci RAM DDR4 i Optane PMem  -Minimum 3 uniwersalne złącza PCI Express generacji 4, w tym minimum 3 złącza o prędkości x16;  -Wszystkie złącza PCI Express muszą być aktywne;  -Minimum 2 sloty dla dysków M.2 na płycie głównej (lub dedykowanej karcie PCI Express) nie zajmujące klatek dla dysków hot-plug; (Możliwość integracji dedykowanej, wewnętrznej pamięci flash przeznaczonej dla wirtualizatora w slocie M.2 na płycie głównej, bez zajmowania klatek dyskowych serwera)  - moduł TPM 2.0 |  |
| 3 | Procesory | | Zainstalowane dwa procesory 8-rdzeniowe w architekturze x86, pracujące z częstotliwością bazowa min 3,2 GHz, osiągające w oferowanym modelu serwera lub w innym modelu serwera 2-procesorowego tego samego producenta co serwer oferowany, w testach wydajności SPECrate2017\_int\_base minimum 145 pkt.  Wymagany wynik wydajności musi być dostępny na stronie spec.org nie później niż na dzień składania ofert; |  |
| 4 | Pamięć RAM | | -Zainstalowane 128 GB pamięci RAM typu DDR4 Registered, 3200Mhz  -Wsparcie dla technologii zabezpieczania pamięci Advanced ECC, Memory Scrubbing, lub równoważnej;  -Wsparcie serwera dla konfiguracji kopii lustrzanej pamięci RAM (memory mirror); |  |
| 5 | Dyski twarde | | -Fizyczna możliwość instalacji minimum 8-ciu dysków Hot-Plug SSD i mechanicznych z interfejsami SATA/SAS/NL-SAS o rozmiarze 2,5”  - zainstalowane 3xSSD 480GB 6G  - zainstalowane dwa dyski 240GB SSD M2 wraz z kontrolerem sprzętowym zapewniającym Raid 1  - Zainstalowany kontroler SAS RAID obsługujący poziomy 0,1,10,5,50,6,60 posiadający 8GB pamięci cache (wraz z podtrzymaniem bateryjnym) |  |
| 6 | Kontrolery LAN/FC | | Karta LAN, nie zajmująca żadnego z dostępnych slotów PCI Express, wyposażona minimum w interfejsy: 4x 1Gbit Base-T oraz 2x10G SFP, możliwość wymiany zainstalowanych interfejsów na 2x 100Gbit QSFP28 bez konieczności instalacji kart w slotach PCIe;  - zainstalowana karta 2x 10Gbit Base-T  - zainstalowana karta 2x 16Gb FC  Serwer wyposażony w 2 interfejsy 1Gbit Base-T oraz 2 x 10G SFP nie zajmujące slotów PCIe oraz umożliwiające wymianę na 2 x 100Gbit QSFP28 bez konieczności instalacji kart w slotach PCIe.” |  |
| 7. | Napędy | | - zainstalowany wewnętrzny napęd DVD-RW |  |
| 8. | Porty | | -zintegrowana karta graficzna ze złączem VGA z tyłu serwera;  -1x USB 2.0/3.0 dostępne na froncie obudowy  -1x USB 2.0/3.0 dostępne z tyłu serwera  -1xUSB 2.0/3.0 wewnątrz serwera  Ilość dostępnych złącz VGA i USB nie może być osiągnięta poprzez stosowanie zewnętrznych przejściówek, rozgałęziaczy czy dodatkowych kart rozszerzeń zajmujących jakikolwiek slot PCI Express serwera; |  |
| 9 | | Zasilanie, chłodzenie | -Redundantne zasilacze hotplug o mocy minimum 900W, o sprawności 96% (tzw. klasa titanium), z kablami zasilającymi 2,5m (IEC 320 C14 -> C13)  -Redundantne wentylatory hotplug; |  |
| 10 | | Zarządzanie | -Wbudowane diody informacyjne lub wyświetlacz LCD informujący o stanie serwera (system przewidywania, rozpoznawania awarii) – co najmniej informacja o statusie pracy (poprawny/przewidywana usterka lub usterka) następujących komponentów: karty rozszerzeń zainstalowane w dowolnym slocie PCI Express, procesory CPU, pamięć RAM z dokładnością umożliwiającą jednoznaczną identyfikację uszkodzonego modułu pamięci RAM, wbudowany na płycie głównej nośnik pamięci M.2 SSD, status karty zrządzającej serwera, wentylatory, bateria podtrzymująca ustawienia BIOS/Płyty głównej, zasilacze - poprawność napięć elektrycznych płyty głównej w trybie włączonym (on) i oczekiwania (standby) serwera,  -Zintegrowany z płytą główną serwera kontroler sprzętowy zdalnego zarządzania zgodny z IPMI 2.0 o funkcjonalnościach:   * Niezależny od systemu operacyjnego, sprzętowy kontroler umożliwiający pełne zarządzanie, zdalny restart serwera; * Dedykowana karta LAN 1 Gb/s (dedykowane złącze RJ-45 z tyłu obudowy) do komunikacji wyłącznie z kontrolerem zdalnego zarządzania z możliwością przeniesienia tej komunikacji na inną kartę sieciową współdzieloną z systemem operacyjnym; * Dostęp poprzez przeglądarkę Web (także SSL, SSH) * Zarządzanie mocą i jej zużyciem oraz monitoring zużycia energii * Zarządzanie alarmami (zdarzenia poprzez SNMP) * Możliwość przejęcia konsoli tekstowej serwera * Przekierowanie konsoli graficznej na poziomie sprzętowym oraz możliwość montowania zdalnych napędów i ich obrazów na poziomie sprzętowym (cyfrowy KVM) * Sprzętowy monitoring serwera w tym stanu dysków twardych i kontrolera RAID (bez pośrednictwa agentów systemowych) * Oprogramowanie zarządzające i diagnostyczne wyprodukowane przez producenta serwera umożliwiające konfigurację kontrolera RAID, instalację systemów operacyjnych, zdalne zarządzanie, diagnostykę i przewidywanie awarii w oparciu o informacje dostarczane w ramach zintegrowanego w serwerze systemu umożliwiającego monitoring systemu i środowiska (m.in. temperatura, dyski, zasilacze, płyta główna, procesory, pamięć operacyjna itd.). * Rozwiązanie musi umożliwiać konfigurację i uruchomienie automatycznego powiadomienia serwisu o zbliżającej się lub istniejącej usterce serwera (co najmniej dyski twarde, zasilacze, pamięć RAM, procesory, wentylatory, kontrolery RAID, karty rozszerzeń); * Możliwość zapisu i przechowywania informacji i logów o pełnym stanie maszyny, w tym usterki i sytuacje krytyczne w obrębie wbudowanej pamięci karty zarządzającej - dostęp do tych informacji musi być niezależny od stanu włączenia serwera oraz stanu sprzętowego w tym np. usterki elementów poza kartą zarządzającą; * karta zarządzająca musi umożliwiać konfigurację i uruchomienie automatycznego informowania autoryzowanego serwisu producenta serwera o zaistniałej lub zbliżającej się usterce (wymagana jest możliwość automatycznego otworzenia zgłoszenia serwisowego bezpośrednio w systemie producenta serwera, nie dopuszcza się komunikacji SNMP czy email). Jeżeli są wymagane jakiekolwiek dodatkowe licencje lub pakiety serwisowe potrzebne do uruchomienia automatycznego powiadamiania autoryzowanego serwisu o usterce należy takie elementy wliczyć do oferty – czas trwania minimum równy dla wymaganego okresu gwarancji producenta serwera; |  |
| 11 | | Wspierane OS | Wspierane przez producenta serwera systemy operacyjne:  - Windows 2016, Windows 2019, Windows 2022, RedHat EL 7, RedHat EL 8, Suse ES 15, VMware vSphere 7.0 |  |
| 12 | | Gwarancja | - **min. 60 miesiące** gwarancji producenta serwera w trybie on-site z gwarantowaną naprawą w miejscu użytkowania sprzętu do końca następnego dnia od zgłoszenia. Naprawa realizowana przez producenta serwera lub autoryzowany przez producenta serwis.  -Dostępność części zamiennych co najmniej przez 5 lat od momentu zakupu serwera;  -Wymagana jest bezpłatna dostępność poprawek i aktualizacji BIOS/Firmware/sterowników dożywotnio dla oferowanego serwera – jeżeli funkcjonalność ta wymaga dodatkowego serwisu lub wsparcia wykupionego od producenta lub licencji producenta serwera koszt ten musi być uwzględniony w oferowanej konfiguracji;  -Wymagana możliwość automatycznego powiadamiania o awarii serwera centrum serwisowego producenta. Jeżeli funkcja taka jest płatna koszt ten musi być uwzględniony w oferowanej konfiguracji; | Podać: |
| 13 | | Dokumentacja, inne | -Elementy, z których zbudowane są serwery muszą być produktami producenta tych serwerów lub być przez niego certyfikowane dla oferowanego modelu serwera oraz muszą być objęte gwarancją producenta, o wymaganym w specyfikacji poziomie SLA (wymagane oświadczenie producenta serwera potwierdzające spełnienie wymagań dołączone do oferty).  -Serwer musi być fabrycznie nowy i pochodzić z oficjalnego kanału dystrybucyjnego w Polsce - Wymagane oświadczenie producenta serwera lub jego polskiego przedstawicielstwa, że oferowany do przetargu sprzęt spełnia ten wymóg;  -Oferent zobowiązany jest dostarczyć wraz z ofertą kartę produktową oferowanego serwera umożliwiającą weryfikację podstawowych parametrów oferowanego sprzętu w języku polskim lub angielskim;  -Ogólnopolska, telefoniczna linia techniczna producenta serwera (ogólnopolski numer stacjonarny lub o zredukowanej odpłatności 0-800/0-801) umożliwiająca w czasie obowiązywania gwarancji na sprzęt po podaniu numeru seryjnego urządzenia: zgłoszenie usterki sprzętowej urządzenia oraz weryfikację: konfiguracji sprzętowej serwera, w tym model i typ dysków twardych, procesora, ilość fabrycznie zainstalowanej pamięci operacyjnej, czasu obowiązywania i typ udzielonej gwarancji – obsługa w języku polskim, w trybie całodobowym również w dni świąteczne;  -Wymagane jest oświadczenie Producenta oferowanego serwera lub jego polskiego przedstawicielstwa, iż wymagany w postępowaniu poziom gwarancji i wsparcia na sprzęt został zaoferowany przez Producenta;  -Możliwość aktualizacji i pobrania sterowników do oferowanego modelu serwera w najnowszych certyfikowanych wersjach bezpośrednio z sieci Internet za pośrednictwem strony www producenta serwera;  -Wszystkie parametry i funkcje oferowanego serwera muszą być wspierane przez producenta i zaimplementowane fabrycznie oraz dostępne w seryjnej produkcji danego modelu urządzenia.  Zamawiający nie dopuszcza dostosowywania funkcji serwera na potrzeby niniejszego postępowania.  -Wszystkie parametry i funkcje oferowanego serwera muszą być potwierdzone w dokumentacji technicznej producenta. |  |

1. **System bazodanowy 2 (dwie) licencje:**

Zamawiający korzysta ze szpitalnego systemu informatycznego ( HIS ) opartego o rozwiązania bazodanowe. Zamawiający dopuszcza tylko i wyłącznie rozwiązanie, które będzie kompatybilne oraz wspierane przez producenta obecnie użytkowanego Szpitalnego Systemu Informatycznego.)

Do obowiązków Wykonawcy należy dostarczenie licencji (dopuszcza się zastosowanie licencji typu ASFU (Application Specific Full Use) umożliwiającej legalną pracę na **dwóch procesorach,** dla potrzeb użytkowanego przez Zamawiającego oprogramowania szpitalnego systemu informatycznego (SSI) (Zamawiający posiada oprogramowanie „AMMS” i „Infomedica” firmy ASSECO, w związku z powyższym dostarczony system bazodanowy musi w 100% współgrać z wyżej wspomnianym oprogramowaniem oraz wszystkimi modułami jakie są zainstalowane u zamawiającego, w taki sposób aby nie zakłócić pracy oprogramowania SSI)

System bazodanowy musi spełniać minimalne wymagania funkcjonalne określone poniżej:

1. Możliwość uruchomienia wielu sesji bazy danych przy wykorzystaniu jednego połączenia z serwera aplikacyjnego do serwera bazy danych.
2. Oprogramowanie musi być dostępne na platformy sprzętowe i systemowe - 64-bitowe platformy Unix, Linux 32-bit i 64-bit, MS Windows 32-bit i 64-bit.
3. Oprogramowanie nie może mieć limitów na ilość przechowywanych danych – zarówno tekstowych, jak i multimedialnych.
4. Przetwarzanie transakcyjne wg reguł ACID (Atomicity, Consistency, Independency, Durability) z zachowaniem spójności i maksymalnego możliwego stopnia współbieżności. Mechanizm izolowania transakcji powinien pozwalać na spójny odczyt modyfikowanego obszaru danych bez wprowadzania blokad, z kolei spójny odczyt nie powinien blokować możliwości wykonywania zmian. Oznacza to, że modyfikowanie wierszy nie może blokować ich odczytu, z kolei odczyt wierszy nie może ich blokować do celów modyfikacji. Jednocześnie spójność odczytu musi gwarantować uzyskanie rezultatów zapytań odzwierciedlających stan danych z chwili jego rozpoczęcia, niezależnie od modyfikacji przeglądanego zbioru danych.
5. Możliwość zagnieżdżania transakcji – powinna istnieć możliwość uruchomienia niezależnej transakcji wewnątrz transakcji nadrzędnej. Przykładowo – powinien być możliwy następujący scenariusz: każda próba modyfikacji tabeli X powinna w wiarygodny sposób odłożyć ślad w tabeli dziennika operacji, niezależnie czy zmiana tabeli X została zatwierdzona czy wycofana.
6. Wsparcie dla wielu ustawień narodowych i wielu zestawów znaków (włącznie z Unicode).
7. Możliwość migracji zestawu znaków bazy danych do Unicode
8. Możliwość redefiniowania przez Zamawiającego ustawień narodowych – symboli walut, formatu dat, porządku sortowania znaków za pomocą narzędzi graficznych.
9. Skalowanie rozwiązań opartych o architekturę trójwarstwową: możliwość uruchomienia wielu sesji bazy danych przy wykorzystaniu jednego połączenia z serwera aplikacyjnego do serwera bazy danych
10. Możliwość otworzenia wielu aktywnych zbiorów rezultatów (zapytań, instrukcji DML) w jednej sesji bazy danych
11. Wsparcie protokołu XA
12. Wsparcie standardu JDBC 3.0
13. Zgodność ze standardem ANSI/ISO SQL 2003 lub nowszym.
14. Motor bazy danych powinien umożliwiać wskazywanie optymalizatorowi SQL preferowanych metod optymalizacji na poziomie konfiguracji parametrów pracy serwera bazy danych oraz dla wybranych zapytań. Powinna istnieć możliwość umieszczania wskazówek dla optymalizatora w wybranych instrukcjach SQL.
15. Brak formalnych ograniczeń na liczbę tabel i indeksów w bazie danych oraz na ich rozmiar (liczbę wierszy).
16. Możliwość wykonywania i katalogowania kopii bezpieczeństwa bezpośrednio przez serwer bazy danych. Możliwość zautomatyzowanego usuwania zbędnych kopii bezpieczeństwa przy zachowaniu odpowiedniej liczby kopii nadmiarowych - stosownie do założonej polityki nadmiarowości backup'ów. Możliwość integracji z powszechnie stosowanymi systemami backupu (Legato, Veritas, Tivoli, OmniBack, ArcServeitd). Wykonywanie kopii bezpieczeństwa powinno być możliwe w trybie offline oraz w trybie online
17. Możliwość wykonywania kopii bezpieczeństwa w trybie on-line (hot backup).

Warunki równoważności:

|  |
| --- |
| Za równoważne uważa się oprogramowanie bazodanowe spełniające standardy jakościowe oraz posiadające zakres funkcjonalny i parametry oprogramowania wymaganego przez Zamawiającego oraz współpracujące bez zakłóceń z bazami danych Oracle posiadanymi przez Zamawiającego (bazy danych aplikacji Infomedica, AMMS, EDM, MPI firmy Asseco S.A.). |
| Oferowany motor bazy danych musi być dostępny zarówno na platformy systemów operacyjnych Windows i Linux. |
| Oferowany Motor bazy danych musi mieć możliwość rozbudowy do wersji wspierającej możliwość synchronicznej replikacji danych w dwóch niezależnych centrach danych. |
| Oferowany Motor bazy danych posiada komercyjne wsparcie producenta. Nie dopuszcza się zastosowania RBD typu open-source. |
| Oferowany Motor bazy danych ma możliwość realizacji kopii bezpieczeństwa w trakcie działania (na gorąco). |
| Oferowany Motor bazy danych generuje kopie bezpieczeństwa automatycznie (o określonej porze) i na żądanie operatora oraz umożliwia odtwarzanie bazy danych z kopii archiwalnej, w tym sprzed awarii. |
| Oferowany Motor bazy danych umożliwia eksport i import danych z bazy danych w formacie tekstowym z uwzględnieniem polskiego standardu znaków. |
| Administrator posiada możliwość wyboru danych, które mają być monitorowane w logach systemu z dokładnością do poszczególnych kolumn w tabelach danych, a zarządzanie nimi może odbywać się z poziomu narzędzi do zarządzania bazami danych (dopuszcza się narzędzie na poziomie motoru bazy danych). |
| Hasła użytkowników są przechowywane w bazie danych w postaci niejawnej (zaszyfrowanej). |
| Dostępność oprogramowania na współczesne 64-bitowe platformy Unix (HP-UX dla procesorów PA-RISC i Itanium, Solaris dla procesorów SPARC i Intel/AMD, IBM AIX), Intel/AMD Linux 32-bit i 64-bit, MS Windows 32-bit i 64-bit. Identyczna funkcjonalność serwera bazy danych na ww. platformach |
| Przetwarzanie z zachowaniem spójności i maksymalnego możliwego stopnia współbieżności. Modyfikowanie wierszy nie może blokować ich odczytu, z kolei odczyt wierszy nie może ich blokować do celów modyfikacji. Jednocześnie spójność odczytu musi gwarantować uzyskanie rezultatów zapytań odzwierciedlających stan danych z chwili jego rozpoczęcia, niezależnie od modyfikacji przeglądanego zbioru danych. |
| Możliwość zagnieżdżania transakcji – powinna istnieć możliwość uruchomienia niezależnej transakcji wewnątrz transakcji nadrzędnej. Przykładowo – powinien być możliwy następujący scenariusz: każda próba modyfikacji tabeli X powinna w wiarygodny sposób odłożyć ślad w tabeli dziennika operacji, niezależnie czy zmiana tabeli X została zatwierdzona czy wycofana. |
| Wsparcie dla wielu ustawień narodowych i wielu zestawów znaków (włącznie z Unicode). |
| Możliwość migracji zestawu znaków bazy danych do Unicode |
| Możliwość redefiniowania przez klienta ustawień narodowych – symboli walut, formatu dat, porządku sortowania znaków za pomocą narzędzi graficznych. |
| Skalowanie rozwiązań opartych o architekturę trójwarstwową: możliwość uruchomienia wielu sesji bazy danych przy wykorzystaniu jednego połączenia z serwera aplikacyjnego do serwera bazy danych |
| Możliwość otworzenia wielu aktywnych zbiorów rezultatów (zapytań, instrukcji DML) w jednej sesji bazy danych |
| Wsparcie protokołu XA |
| Wsparcie standardu JDBC 3.0 |
| Zgodność ze standardem ANSI/ISO SQL 2003 lub nowszym. |
| Motor bazy danych powinien umożliwiać wskazywanie optymalizatorowi SQL preferowanych metod optymalizacji na poziomie konfiguracji parametrów pracy serwera bazy danych oraz dla wybranych zapytań. Powinna istnieć możliwość umieszczania wskazówek dla optymalizatora w wybranych instrukcjach SQL. |
| Brak formalnych ograniczeń na liczbę tabel i indeksów w bazie danych oraz na ich rozmiar (liczbę wierszy). |
| Wsparcie dla procedur i funkcji składowanych w bazie danych. Język programowania powinien być językiem proceduralnym, blokowym (umożliwiającym deklarowanie zmiennych wewnątrz bloku), oraz wspierającym obsługę wyjątków. W przypadku, gdy wyjątek nie ma zadeklarowanej obsługi wewnątrz bloku, w razie jego wystąpienia wyjątek powinien być automatycznie propagowany do bloku nadrzędnego bądź wywołującej go jednostki programu |

1. **Przełączniki FC – 4 sztuki**
2. Przełącznik FC musi być wykonany w technologii FC minimum 32 Gbs i zapewniać możliwość pracy portów FC z prędkościami 32, 16, 8, 4 Gbs w zależności od rodzaju zastosowanych wkładek SFP.
3. Dostarczony przełącznik FC musi być wyposażony w 8 aktywnych portów FC obsadzonych 8-ma wkładkami SFP+ 16Gbs SWL i jedną dodatkową wkładką SFP 16Gb/s SM LR do 10km.
4. Przełącznik musi umożliwiać w przyszłości rozbudowę do co najmniej 24 aktywnych portów w ramach tej samej obudowy. Przyszła rozbudowa musi odbywać się za pomocą aktywacji portów dodatkowa licencja i instalacji dodatkowych wkładek SFP+.
5. Wszystkie zaoferowane porty przełącznika FC muszą umożliwiać działanie bez tzw. oversubscrypcji gdzie wszystkie porty w maksymalnie rozbudowanej konfiguracji przełącznika wyposażonej we wkładki 32Gbs mogą pracować równocześnie z pełną prędkością 32Gb/s.
6. Całkowita przepustowość przełącznika FC dostępna dla maksymalnie rozbudowanej konfiguracji (24 porty) wyposażonej we wkładki 32Gbs musi wynosić minimum 768 Gb/s end-to-end.
7. Oczekiwana wartość opóźnienia przy przesyłaniu ramek FC między dowolnymi portami przełącznika nie może być większa niż 900ns.
8. Rodzaj obsługiwanych portów, co najmniej: E, D oraz F.
9. Przełącznik FC musi mieć wysokość maksymalnie 1 RU (jednostka wysokości szafy montażowej) i szerokość 19” oraz zapewniać techniczną możliwość montażu w szafie 19”. Wraz z przełącznikiem należy dostarczyć odpowiedni zestaw montażowy do szafy 19”.
10. Maksymalny dopuszczalny pobór mocy przełącznika FC wyposażonego w 24 aktywne porty 32Gbps to 77W.
11. Maksymalna ilość ciepła wydzielanego przez przełącznik FC wyposażony w 24 aktywne porty 32Gbps to 215 BTU na godzinę.
12. Przepływ powietrza chłodzącego PSAF (Port Side Exhaust Air Flow)
13. Przełącznik FC musi posiadać możliwość obsługi mechanizmu agregacji połączeń ISL między dwoma przełącznikami i tworzenia w ten sposób logicznych połączeń typu ISL Trunk o przepustowości minimum 256 Gb/s half duplex (dla wkładek 32Gbs) dla każdego logicznego połączenia. Load balancing ruchu między fizycznymi połączeniami ISL w ramach połączenia logicznego typu trunk musi być realizowany na poziomie pojedynczych ramek FC a połączenie logiczne musi zachowywać kolejność przesyłanych ramek. Nie trzeba dostarczać licencji aktywującej opisaną tu funkcjonalność.
14. Przełącznik FC musi obsługiwać mechanizm balansowania ruchu, pomiędzy co najmniej 16 różnymi połączeniami o tym samym koszcie wewnątrz wielodomenowych sieci fabric, przy czym balansowanie ruchu musi odbywać się w oparciu o 3 parametry nagłówka ramki FC: DID, SID i OXID.
15. Przełącznik FC musi posiadać możliwość jednoczesnej obsługi mechanizmów ISL Trunk oraz balansowania ruchu w oparciu o DID/SID/OXID. Nie trzeba dostarczać licencji aktywującej opisaną tu funkcjonalność.
16. Przełącznik FC musi realizować sprzętową obsługę zoningu (przez tzw. układ ASIC) na podstawie portów i adresów WWN.
17. Przełącznik FC musi mieć możliwość wymiany i aktywacji wersji firmware’u (zarówno na wersję wyższą jak i na niższą) w czasie pracy urządzenia i bez zakłócenia przesyłanego ruchu FC.
18. Przełącznik FC musi wspierać następujące mechanizmy zwiększające poziom bezpieczeństwa:
    * mechanizm tzw. Fabric Binding, który umożliwia zdefiniowanie listy kontroli dostępu regulującej prawa przełączników FC do uczestnictwa w sieci fabric
    * uwierzytelnianie (autentykacja) przełączników w sieci Fabric za pomocą protokołów DH-CHAP i FCAP
    * uwierzytelnianie (autentykacja) urządzeń końcowych w sieci Fabric za pomocą protokołu DH-CHAP
    * szyfrowanie połączenia z konsolą administracyjną. Wsparcie dla SSHv2.
    * definiowanie wielu kont administratorów z możliwością ograniczenia ich uprawnień za pomocą mechanizmu tzw. RBAC (Role Based Access Control)
    * definiowane kont administratorów w środowisku RADIUS, LDAP w MS Active Directory, Open LDAP, TACACS+
    * szyfrowanie komunikacji narzędzi administracyjnych za pomocą SSL/HTTPS
    * obsługa SNMP v1 oraz v3
    * IP Filter dla portu administracyjnego przełącznika
    * wgrywanie nowych wersji firmware przełącznika FC z wykorzystaniem bezpiecznych protokołów SCP oraz SFTP
    * wykonywanie kopii bezpieczeństwa konfiguracji przełącznika FC z wykorzystaniem bezpiecznych protokołów SCP oraz SFTP
19. Przełącznik FC musi mieć możliwość konfiguracji przez:

* polecenia tekstowe w interfejsie znakowym konsoli terminala
* przeglądarkę internetową z interfejsem graficznym lub dedykowane oprogramowanie.

1. Przełącznik FC musi być dostarczony z następującymi narzędziami diagnostycznymi i mechanizmami obsługi ruchu FC:

* logowanie zdarzeń poprzez mechanizm „syslog”,
* ciągłe monitorowanie parametrów pracy przełącznika, portów, wkładek SFP i sieci fabric z automatycznym powiadamianiem administratora, wyłączeniem pracy portu lub przesunięciem przepływów tzw. slow drain na niski priorytet w przypadku przekroczenia zdefiniowanych wartości granicznych. Powiadamianie administrator musi być możliwe za pomocą wysyłania wiadomości e-mail, pułapki SNMP lub komunikatu w logu. Nie trzeba dostarczać licencji aktywującej opisaną tu funkcjonalność.
* port diagnostyczny tzw. D\_port. Port diagnostyczny musi umożliwiać wykonanie testów sprawdzających komunikację portu przełącznika z wkładką SFP, połączenie optyczne pomiędzy dwoma przełącznikami, testowe obciążenie połączenia pełną przepustowością 16Gbps/32Gbps oraz pomiar opóźnienia i odległości między przełącznikami z dokładnością co najmniej do 5m dla wkładek SFP 16Gbps lub 32Gbps. Testy wykonywane przez port diagnostyczny nie mogą wpływać w żaden sposób na działanie pozostałych portów przełącznika i całej sieci fabric.
* FCping
* FC traceroute
* kopiowanie danych wymienianych pomiędzy dwoma wybranymi portami na inny wybrany port przełącznika
* sprzętowe monitorowanie przepływów danych dla automatycznie wykrywanych par urządzeń komunikujących się przez dany port przełącznika. Dla każdego monitorowanego przepływu muszą być gromadzone statystyki dotyczące, co najmniej liczby wysłanych i odebranych ramek, przepustowości, liczby zapisów i odczytów SCSI. Nie trzeba dostarczać licencji aktywującej opisaną tu funkcjonalność.
* sprzętowy generator ruchu umożliwiający symulowanie komunikacji w wielodomenowych sieciach SAN bez konieczności angażowania fizycznych urządzeń takich jak serwery lub macierze dyskowe. Nie trzeba dostarczać licencji aktywującej opisaną tu funkcjonalność.
* mechanizm umożliwiający kopiowanie pierwszych 64 bajtów ramek dla wybranych przepływów danych do pamięci lokalnej przełącznika w celu dalszej analizy. Nie trzeba dostarczać licencji aktywującej opisaną tu funkcjonalność.
* mechanizm umożliwiający sprzętowe identyfikowanie ramek FC oznaczonych parametrem VM ID oraz integrację tego mechanizmu z systemami monitorowania przepływów danych w szczególności w zakresie przepustowości, liczby zapisów i odczytów na sekundę oraz opóźnień operacji zapisu i odczytu. Nie trzeba dostarczać licencji aktywującej opisaną tu funkcjonalność.
* Przełącznik musi obsługiwać wysyłanie komunikatów FPIN typu: Link Integrity Notification, Delivery Notification, Peer Congestion Notification, Congestion Notification. Nie trzeba dostarczać licencji aktywującej opisaną tu funkcjonalność.

1. Przełącznik FC musi posiadać możliwość przydzielenia, co najmniej 1700 tzw. buffer credits do wybranego portu FC przełącznika. Nie trzeba dostarczać licencji aktywującej opisaną tu funkcjonalność.
2. Przełącznik FC musi zapewnić możliwość jego zarządzania przez zintegrowany port Ethernet, RS232 oraz inband IP-over-FC.
3. Przełącznik FC musi zapewniać obsługę protokołu NVMe over FC.
4. Przełącznik FC musi zapewniać obsługę interfejsu zarządzającego REST API.
5. Przełącznik FC musi realizować kategoryzację ruchu między parami urządzeń (initiator - target) oraz przydzielenie takich par urządzeń do kategorii o wysokim, średnim lub niskim priorytecie. Konfiguracja przydziału do różnych klas priorytetów musi się odbywać za pomocą standardowych narzędzi do konfiguracji zoningu.
6. Przełącznik FC musi realizować kategoryzację ruchu na podstawie wartości parametru CS\_CTL w nagłówku ramki FC oraz odpowiednie przydzielenie ramki do kategorii o wysokim, średnim lub niskim priorytecie.
7. Wsparcie dla N\_Port ID Virtualization (NPIV). Obsługa, co najmniej 255 wirtualnych urządzeń na pojedynczym porcie przełącznika.
8. Minimum 3 lata gwarancji producenta przełącznika lub jego partnera OEM wymienionego na oficjalnej stronie producenta w trybie onsite z gwarantowanym czasem reakcji w miejscu instalacji urządzenia najpóźniej w następnym dniu roboczym (Next Business Day) od zgłoszenia usterki.
9. **Macierz dyskowa – 2 sztuki**

**Producent……………………..**

**Typ …………………………..**

**Model …………………………..**

|  |  |  |  |
| --- | --- | --- | --- |
| **Macierz dyskowa** | | |  |
| Lp. | Nazwa parametru | Minimalna wartość parametru | Parametry oferowane |
|  | Obudowa | System musi być dostarczony ze wszystkimi komponentami do instalacji w szafie rack 19'’ w obudowie wysokiej gęstości, spełniającej założenia minimum 15 dysków na 1U wysokości sprzętu. |  |
|  | Pojemność: | System musi zostać dostarczony w konfiguracji zawierającej minimum:   * 21 dysków o pojemności minimum 1,8TB SAS, o prędkości obrotowej minimum 10 tyś. Obr/min. * 7 dysków SSD o pojemności minimum 1,6TB, dyski klasy nie niższej niż eMLC   Wszystkie oferowane dyski muszą być podłączone interfejsem o prędkości co najmniej 12Gb SAS.  System musi ponadto wspierać dyski o wielkościach co najmniej:   * SSD: od 800GB do 15.3TB * SAS 10k od 900GB do 1800GB * NL-SAS/SATA od 4TB do 18TB   System musi mieć możliwość rozbudowy do minimum 180 dysków oraz musi pozwalać na rozbudowę do wyższych modeli bez potrzeby migracji danych (przez rozbudowę do wyższego modelu zamawiający rozumie do modelu macierzy z większą ilością Cache, większą skalowalnością i mocniejszymi procesorami). Zamawiający dopuszcza rozwiązanie które nie pozwala na taką rozbudowę w przypadku gdy zostanie zaoferowany najwyższy z modeli macierzy skalowalny min do 500 dysków oraz pamięcią cache min 512GB. |  |
|  | Kontroler | Dwa kontrolery wyposażone w przynajmniej 32GB cache każdy.    W przypadku awarii zasilania dane nie zapisane na dyski, przechowywane w pamięci muszą być zabezpieczone za pomocą podtrzymania bateryjnego przez 72 godziny lub jako zrzut na pamięć flash. |  |
|  | Interfejsy | Oferowana macierz musi posiadać minimum   * 8 portów 32Gb FC umożliwiających podłączenie do hostów lub sieci SAN * 4 porty SAS 12 Gb/s do podłączenia półek dyskowych * 4 porty 1GbE do zarządzania dostępne dla użytkownika oraz 2 porty konsolowe (RJ45)   Macierz musi umożliwiać wymianę portów 32Gb FC porty 25GbE lub porty 12Gb SAS. Zmiana portów musi się odbywać tylko poprzez dołożenie odpowiednich kart rozszerzeń lub wymianę kart 32Gb, bez konieczności wymiany kontrolerów macierzy. |  |
|  | RAID | Wsparcie dla RAID: 0, 1, 5, 6, 10  Dodatkowo macierz musi posiadać mechanizm tworzenia wirtualnej przestrzeni na minimum 180 dyskach macierzy wraz z wyliczaniem parzystości oraz podwójnej parzystości w celu zabezpieczenia danych. Mechanizm ten musi być przygotowany do optymalizacji procesów odtwarzania dysków pojemnościowych.  Obliczanie sum kontrolnych (kodów parzystości) dla grup dyskowych RAID5 i RAID6 musi być realizowane w sposób sprzętowy przez dedykowany układ w macierzy.  Zamawiający dopuszcza zastosowanie zewnętrznego narzędzia (software, volume manager, SDS) do zbudowania RAID 0. |  |
|  | Obsługiwane protokoły | FC, iSCSI, SAS,  Macierz musi mieć możliwość wystawienia zasobów dyskowych poprzez protokoły CIFS, NFS, S3. Zamawiający dopuszcza zastosowanie rozwiązania typu SDS (Software Defined Storage). |  |
|  | Funkcjonalności | Macierz musi posiadać wsparcie dla wielościeżkowości dla systemów:  Microsoft® Windows Server®, Red Hat Enterprise Linux®, Novell SUSE Linux Enterprise Server, VMware® ESX®, Oracle® Solaris, HP HP-UX, IBM AIX,  Macierz musi posiadać funkcjonalność wykonywania snapshotów minimum 128 per wolumen oraz 512 Snapshotów na macierzy  Macierz musi posiadać funkcjonalność klonowania danych.  Macierz musi posiadać funkcjonalność replikacji danych w trybie synchronicznym i asynchronicznym, system musi pozwalać na wykonanie do 32 jednoczesnych replikacji.  Macierz musi umożliwiać dynamiczną zmianę rozmiaru wolumenów logicznych bez przerywania pracy macierzy i bez przerywania dostępu do danych znajdujących się na danym wolumenie.  Macierz musi posiadać funkcjonalność partycjonowania macierzy na odseparowane od siebie logicznie systemy na których rezydują osobne dyski logiczne dla heterogenicznych systemów. Licencja na macierzy musi pozwalać na wykonanie do 128 partycji.  Macierz musi posiadać funkcjonalność automatycznego balansowania obciążenia kontrolerów macierzy przez przełączanie w trybie online volumenów logicznych pomiędzy nimi w zależności od wygenerowanego na nich ruchu. Musi istnieć możliwość wyłączenia tej funkcjonalności z poziomu interfejsu użytkownika.  Macierz musi pozwalać na dynamiczną migrację pomiędzy poziomami RAID, czyli zmianę sposobu zabezpieczenia grupy dyskowej z jednego poziomu RAID na drugi na tych samych dyskach.  Macierz musi posiadać oprogramowanie do monitoringu stanu dysków, które pozwala na identyfikowanie potencjalnie zagrożonych awarią dysków oraz z poziomu graficznego interfejsu do zarządzania musi być możliwość sprawdzenia stanu zużycia dysków SSD.  Wraz z system musi zostać dostarczone narzędzie do monitoringu macierzy w kontekście:  - wydajności i opóźnień na wolumenach  - wydajności I/Ops, MB/s  - trafności w cache  Macierz musi posiadać możliwość integracji z Active Directory w zakresie definicji i mapowania grup i użytkowników pod kątem autentykacji.  Macierz musi posiadać oprogramowanie do aplikacji pozwalające na integrację z:  - Vmware vCenter – provisioning i monitoring macierzy z widoku vCenter  - VMware VASA  - MicrosoftVirtual Disk Service (VDS)  - Microsoft Virtual Shadow Service (VSS)  - Oracle Enterprise Manager – monitoring zasobów macierzowych  Zamawiający dopuszcza zaoferowania zewnętrznego oprogramowania do zapewnienia integracji i monitoring w/w aplikacji.  Macierz musi zapewniać możliwość szyfrowania danych, realizacja procesu szyfrowania i zarządzania kluczem może się odbywać przez kontrolery macierzy lub zewnętrzne urządzenia i oprogramowanie do zarządzania kluczami.  Wraz z macierzą musi zostać dostarczone narzędzie (w formie dedykowanej aplikacji, portalu www lub innej) do monitoringu macierzy w tym przechowywania danych historycznych z min 6 m-cy o:  - wydajności macierzy  - zajętości przestrzeni  - błędach/awariach, które wystąpiły na macierzy  Narzędzie może pochodzić od innego dostawcy niż producent macierzy.  Wszystkie licencje na funkcjonalności muszą być dostarczone na maksymalną pojemność macierzy. |  |
|  | Gwarancja i serwis | **Min. 5 lat serwisu** producenta macierzy z czasem dostawy części zamiennych na następny dzień roboczy  Dostęp do centrum serwisowego 24/7  Możliwość zgłaszania awarii 24/7  5 lat aktualizacji do oprogramowania oraz dostęp do portalu serwisowego producenta, dostęp do informacji technicznych dotyczących oferowanego urządzenia.  Uszkodzone dyski pozostają własnością zamawiającego. |  |

1. **Oprogramowanie serwerowe**

|  |  |
| --- | --- |
| Wymagane minimalne parametry techniczne | |
| Zamawiający wymaga, aby wszystkie elementy systemu oraz jego licencja pochodziły od tego samego producenta. Licencja ma umożliwiać downgrade do poprzednich wersji systemu operacyjnego oraz uprawniać do uruchamiania SSO w środowisku fizycznym i nieograniczonej liczby środowisk systemu operacyjnego za pomocą wbudowanych mechanizmów wirtualizacji.  Wymaga się dostarczenia licencji dla klastra 4 serwerów, dwuprocesorowych, każdy procesor posiada 8 rdzeni na nieograniczoną liczbę systemów OSE  Jeżeli system operacyjny wymaga licencji dostępowych należy dostarczyć licencję dla 200 urządzeń. | |
| Serwerowy system operacyjny (dalej: SSO) posiada następujące, wbudowane cechy. | |
| 1 | Posiada możliwość wykorzystania 320 logicznych procesorów oraz 4 TB pamięci RAM w środowisku fizycznym |
| 2 | Posiada możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności 64TB przez każdy wirtualny serwerowy system operacyjny. |
| 3 | Posiada możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania do 7000 maszyn wirtualnych. |
| 4 | Posiada możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci. |
| 5 | Posiada wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy. |
| 6 | Posiada wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy. |
| 7 | Posiada automatyczną weryfikację cyfrowych sygnatur sterowników w celu sprawdzenia czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego. |
| 8 | Posiada możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. |
| 9 | Wbudowane wsparcie instalacji i pracy na wolumenach, które:   * pozwalają na zmianę rozmiaru w czasie pracy systemu, * umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów, * umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów, * umożliwiają zdefiniowanie list kontroli dostępu (ACL). |
| 10 | Posiada wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość. |
| 11 | Posiada wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji. |
| 12 | Posiada możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET |
| 13 | Posiada możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów. |
| 14 | Posiada wbudowaną zaporę internetową (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych. |
| 15 | Graficzny interfejs użytkownika. |
| 16 | Zlokalizowane w języku polskim, następujące elementy:   * menu, * przeglądarka internetowa, * pomoc, * komunikaty systemowe. |
| 17 | Posiada wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play). |
| 18 | Posiada możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu. |
| 19 | Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa. |
| 20 | Pochodzący od producenta systemu serwis zarządzania polityką konsumpcji informacji w dokumentach (Digital Rights Management). |
| 21 | Posiada możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:   * Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC, * Usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji:   + Podłączenie SSO do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną,   + Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,   + Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza. * Zdalna dystrybucja oprogramowania na stacje robocze. * Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej * Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające: * Dystrybucję certyfikatów poprzez http * Konsolidację CA dla wielu lasów domeny, * Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen. * Szyfrowanie plików i folderów. * Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec). * Posiada możliwość tworzenia systemów wysokiej dostępności (klastry typu failover) oraz rozłożenia obciążenia serwerów. * Serwis udostępniania stron WWW. * Wsparcie dla protokołu IP w wersji 6 (IPv6), * Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows, * Wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie 1000 aktywnych środowisk wirtualnych systemów operacyjnych. Wirtualne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności. Mechanizmy wirtualizacji zapewniają wsparcie dla: * Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych, * Obsługi ramek typu jumbo frames dla maszyn wirtualnych, * Obsługi 4-KB sektorów dysków, * Nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra, * Posiada możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk model)   Posiada możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta SSO umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet. |
| 22 | Wsparcie dostępu do zasobu dyskowego SSO poprzez wiele ścieżek (Multipath). |
| 23 | Posiada możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego. |
| 24 | Posiada mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty. |
| 25 | Posiada możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF. |

1. **UTM Firewall**

Zapora sieciowa typu Next Generation Firewall (NGFW),

UTM Firewall powinien zawierać:

Mechanizm pozwalający na dwustronną analizę ruchu bez proxy oraz ograniczeń na rozmiar skanowanego pliku.

Minimalna ilość interfejsów:

Minimum 34 porty, w tym:

Min. 6 interfejsów 10 GbE SFP+,

Min. 24 interfejsy RJ-45 Ethernet 10/100/1000 – każdy z interfejsów musi mieć możliwość konfiguracji osobnej podsieci i strefy bezpieczeństwa.

2 interfejsy USB 3.0 dla przyszłych potrzeb i do podłączenia modemu 3G,

1 interfejs konsoli do zarządzania zaporą,

1 interfejs RJ-45 Ethernet 10/100/1000 do zarządzania zaporą,

Zapora powinna posiadać dysk M.2 o pojemności przynajmniej 128 GB z możliwością wymiany na większy.

Możliwość przypisania wielu interfejsów fizycznych do pojedynczej strefy bezpieczeństwa

Możliwość powiązania wielu interfejsów fizycznych w jeden port logiczny (agregacja portów) celem podniesienia wydajności połączeń oraz zapewnienia redundancji

Urządzenie powinno posiadać minimum dwa zasilacze.

Możliwość utworzenia przynajmniej 256 interfejsów logicznych VLAN, wsparcie dla standardu 802.1q,

Obsługa nielimitowanej ilości hostów podłączonych w sieci chronionej,

Minimalna ilość jednocześnie obsługiwanych połączeń: 2 000 000,

Możliwość obsłużenia przynajmniej 22 500 nowych połączeń w ciągu 1 sekundy.

Przepustowość urządzenia pracującego w trybie stateful firewall: 5,5 Gbps – dla ramki 1518B zgodnie z RFC 2544,

Przepustowość urządzenia pracującego z włączonym mechanizmem IPS: 3.8 Gbps,

Przepustowość urządzenia pracującego jako koncentrator VPN: 2,2 Gbps dla szyfrowania AES bez aktywnych usług UTM, zgodnie z RFC 2544,

Przepustowość urządzenia DPI/NGFW (z włączonymi wszystkimi usługami bezpieczeństwa – antivirus, antyspyware, IPS, bez buforowania i proxy i bez ograniczeń jeśli chodzi o wielkość skanowanych plików) – 3,5 Gbps,

Minimalna ilość jednocześnie zestawionych tuneli site-site VPN (urządzenie – urządzenie): 3 000,

Minimalna ilość licencji umożliwiających zestawienie połączeń client-site SSL VPN (komputer – urządzenie), dostępnych w pakiecie z urządzeniem: 25 z możliwością rozszerzenia do przynajmniej 500

Minimalna ilość licencji umożliwiających zestawienie połączeń client-site IPSec VPN (komputer – urządzenie), dostępnych w pakiecie z urządzeniem: 50 z możliwością rozszerzenia do przynajmniej 1 000.

Urządzenie powinno umożliwiać poddanie inspekcji zawartości ruchu szyfrowanego SSL/TLS poprzez jego odszyfrowanie i ponowne zaszyfrowanie zmienionym certyfikatem. Administrator powinien mieć możliwość tworzenia wyjątków do inspekcji ruchu SSL poprzez wykorzystanie kategorii stron np. wyłączenie z inspekcji kategorii zawierających strony bankowe i medyczne.

Wydajność urządzenia z włączoną funkcją inspekcji ruchu SSL/TLS powinna wynosić minimum 850 Mbps oraz obsłużyć 150 000 połączeń.

Obsługa IPSec, ISAKMP/IKE, Radius, L2TP, PPPoE, PPTP,

Zintegrowany serwer DHCP, umożliwiający przydzielanie adresów IP dla hostów znajdujących się w sieci chronionej, a także dla hostów połączonych poprzez VPN (dla tuneli nawiązanych w trybie site-site oraz client-site),

Wsparcie funkcjonalności IP Helper, lub IP Relay (przekazywanie komunikacji DHCP pomiędzy strefami bezpieczeństwa),

Uwierzytelnianie użytkowników w oparciu o wewnętrzną bazę użytkowników, oraz z wykorzystaniem zewnętrznych mechanizmów RADIUS/XAUTH, Active Directory, SSO, LDAP,

Wsparcie dla Dynamicznego DNS tzw. DDNS,

Zintegrowany mechanizm kontroli zawartości witryn pogrupowanych na kategorie tematyczne.

Mechanizm kontroli treści powinien mieć możliwość filtrowania stron tłumaczonych przez google translate (strony takie również powinny być poddane inspekcji, na takich samych zasadach jak strony na które użytkownik wchodzi bezpośrednio).

Administrator powinien mieć możliwość tworzenia różnych akcji dla stron które zostały wychwycone przez filtr treści. Powinny być dostępne takie akcje jak:

wyświetlenie strony blokady (z możliwością tworzenia kilku różnych stron),

wyświetlenie strony blokady z możliwością podania hasła odblokowującego dostęp do zablokowanej strony,

wyświetlenie informacji z polityką bezpieczeństwa organizacji podczas wchodzenia na strony z danej kategorii. Użytkownik może wejść na stronę po akceptacji polityki.

Administrator powinien mieć możliwość stworzenia polityki kontroli treści obejmującego np. strony z kategorii Multimedia i przydzielenia ograniczonego pasma dla stron w tej kategorii np. 5 Mbps,

Zintegrowany mechanizm kontroli transmisji poczty elektronicznej w oparciu o zewnętrzne serwery RBL.

Zintegrowany mechanizm zabezpieczający bezprzewodową sieć LAN, umożliwiający szyfrowanie transmisji w połączeniach bezprzewodowych realizowanych pomiędzy dodatkowymi urządzeniami Access Point a stacjami roboczymi za pomocą IPSec VPN. System wspomagania uwierzytelniania bezprzewodowych stacji roboczych, oraz użytkowników, pozwalający na wdrożenie polityki dostępowej dla sieci.

Możliwość uruchomienia minimum dwóch łączy WAN - Zintegrowane funkcje Load-Balancing oraz Failover. Funkcja Failover oparta o badanie stanu łącza i badanie dostępności hosta zewnętrznego.

Możliwość ograniczenia ruchu na zewnętrznej stacji roboczej podczas pracy zdalnej VPN (dostęp tylko do udostępnionych zasobów lub dostęp do udostępnionych zasobów oraz zasobów sieci Internet z uwzględnieniem filtrowania treści, mechanizmu IPS oraz ochrony przed wirusami i wszelkim innym oprogramowaniem złośliwym dla komputerów połączonych przez VPN),

Kontrola dostępności zestawionych tuneli VPN,

Możliwość zarządzania urządzeniem z wykorzystaniem protokołów http, https, SSH i SNMP.

Konfiguracja oparta na pracy grupowej/obiektowej. Polityka bezpieczeństwa pozwalająca na całkowitą kontrolę nad dostępem do Internetu powinna być tworzona według reguł opartych o grupy i obiekty.

Przy tworzeniu reguł dostępowych zapewniona możliwość konfiguracji trzech typów reakcji: allow, deny, discard (zezwolić, zabronić, odrzucić),

Funkcja NAT oparta o reguły bezpieczeństwa.

NAT w wersji jeden-do-jeden, jeden-do-wielu, PAT, wiele-do-wielu, wiele-do-jednego. Funkcje oparte o zaawansowaną konfigurację według reguł bezpieczeństwa (m.in. możliwość ograniczenia działania funkcji do niektórych hostów, możliwość translacji portów wyjściowych na inne docelowe),

Zintegrowany system skanowania antywirusowego na poziomie bramy internetowej – skanowanie protokołów http, ftp, pop3, smtp, imap4, tcp stream. Możliwość filtrowania załączników poczty. Skanowanie również plików skompresowanych.

Zintegrowany system skanowania antyspyware,

Zintegrowany system IPS (system wykrywania i blokowania wtargnięć) oparty o sygnatury ataków uwzględniające zagrożenia typu worm, Trojan, dziury systemowe, peer-to-peer, buffer overflow, komunikatory, niebezpieczne kody zawarte na stronach www.

System IPS musi używać algorytmu szeregowego przetwarzania.

Zintegrowany system zapory działającej w warstwie aplikacji, umożliwiający definiowanie własnych sygnatur aplikacji z wykorzystaniem ciągu znaków lub wyrażeń regularnych (regex).

Systemy skanowania IPS/Antywirus/Antyspyware muszą umożliwiać skanowanie ruchu w warstwie aplikacji,

Bazy w/w systemów muszą być aktualizowane co najmniej raz dziennie.

Administrator systemu musi mieć możliwość ręcznej aktualizacji sygnatur (online lub offline poprzez manualne zaimportowanie sygnatur,

Administrator systemu musi mieć możliwość skonfigurowania, którym portem i łączem urządzenie będzie się kontaktowało z serwerami backend w celu aktualizacji sygnatur.

System IPS/Antywirus/Antyspyware nie może posiadać ograniczeń związanych z rozmiarem skanowanych plików.

Skanowanie IPS/Antywirus/Antyspyware musi być możliwe między strefami bezpieczeństwa,

Możliwość pełnej kontroli nad programami typu P2P, IM oraz aplikacjami multimedialnymi,

Wsparcie mechanizmów QoS – Priorytet pasma, maksymalizacja pasma, gwarancja pasma, DSCP, 802.1p,

Wsparcie dla komunikacji VoIP - Pełne wsparcie dla SIP, H323v.1-5, zarządzanie pasmem (ruch wychodzący), VoIP over WLAN, śledzenie i monitorowanie połączeń,

Urządzenie powinno posiadać możliwość realizacji funkcjonalności SD-WAN bazując minimum na poniższych parametrach: Jitter, Latency, Packet Loss.

Funkcjonalność nie może wymagać zakupu dodatkowych licencji.

Urządzenie powinno mieć możliwość analizy behawioralnej (sandbox) minimum plików wykonywalnych PE, PDF, Office i aplikacji mobilnych. Sandbox powinien działać z wykorzystaniem minimum 4 silników pochodzących od różnych producentów w celu zwiększenia skuteczności analizy sandbox. Analiza powinna być wykonywana równolegle na wszystkich silnikach.

Urządzenie powinno posiadać zintegrowany kontroler sieci bezprzewodowej kompatybilny z punktami dostępowymi pochodzącymi od tego samego producenta i pozwalający na obsługę do 32 takich punktów dostępowych sieci bezprzewodowej.

Wymagane jest dostarczenie dodatkowego urządzenia pełniące funkcję standby w klastrze wysokiej dostępności (HA) z urządzeniem podstawowym. Urządzenie standby powinno mieć identyczne parametry wydajnościowe jak podstawowa jednostka.

*Gwarancja: Min. 60 m-sc, wsparcie w trybie 24x7.*

*Wymagane licencje:*

Subskrypcje pozwalające na aktualizację sygnatur aplikacji, IPS i wirusów oraz dostęp do bazy URL dla modułu kontroli aplikacji, sandboxing na okres 5 lat.

Licencja na usługę przechowywania logów z systemu firewall i generowania na ich podstawie raportów oraz oprogramowanie do zarządzania systemami firewall. Obydwie funkcjonalności muszą być obsługiwane z tej samej konsoli. Licencja powinna umożliwiać przechowywanie logów przez okres jednego roku. Eksport danych z zapory sieciowej powinien odbywać się za pomocą protokołu IPFIX. W celach zapewnienia kompatybilności oprogramowanie powinno pochodzić od tego samego producenta co system firewall. Wymagana jest licencja, która pozwoli na korzystanie z oprogramowania przez okres 5 lat. Licencja powinna umożliwiać wygenerowanie co najmniej 40 rodzajów raportów. System do zarządzania powinien umożliwiać m.in.:

wykonywania szablonów konfiguracyjnych i zarządzania nimi, obsługiwać funkcjonalność „zero-touch”, tworzenia sieci VPN oraz konfiguracji SD-WAN za pomocą kreatora, zastosowania konfiguracji o wybranej porze dnia, znajdowania różnic pomiędzy konfiguracją zapisaną na urządzeniu a nową tworzoną przez administratora.

1. **Przełącznik rdzeniowy - 2 sztuki**

- Wysokość urządzenia 1U

- Przełącznik posiadający minimum 24 porty 10GBase-X (SFP+)

- Przełącznik posiadający minimum 2 porty QSFP28

- Przełącznik posiadający miejsce na dodatkowy moduł mogący, w zależności od potrzeb, być obsadzonym:

- 4 portami 1/10GBase-X (SFP+)

- 4 portami 10/25GBase-X (SFP28)

- Nieblokującą architekturę o wydajności przełączania min. 1080 Gb/s

- Szybkość przełączania min. 800 Milionów pakietów na sekundę

- Wbudowany dodatkowy interfejs do zarządzania poza pasmem - out of band management

- Wbudowany port USB oraz port konsoli

- Przełącznik musi mieć możliwość instalacji wbudowanego, redundantnego zasilacza 230V AC

- Przełącznik musi mieć możliwość pracy w trybie tradycyjnym, czyli przełączanym/routowanym, ale również z wykorzystaniem technologii Fabric (wirtualizacja usług warstwy drugiej i trzeciej).

- Obsługa sieci wirtualnych IEEE 802.1Q – min. 4094

- Wsparcie dla ramek Jumbo Frames (min. 9216 bajtów)

- Obsługa Quality of Service (IEEE 802.1p, DiffServ, 8 kolejek priorytetów na każdym porcie wyjściowym)

- Przełącznik wyposażony w modularny system operacyjny z ochroną pamięci, procesów oraz zasobów procesora. System musi mieć możliwość dodania nowego modułu lub aktualizacji już zaimplementowanych bez konieczności restartu całego urządzenia

- Możliwość monitorowania zajętości CPU

- Routing statyczny

- Obsługa routingu dynamicznego IPv4

- RIPv1/v2, OSPFv2

- możliwość obsługi BGP, IS-IS– jeżeli funkcjonalność ta wymaga dodatkowej licencji Zamawiający nie wymaga jej dostarczenia w ramach tego postępowania

- Policy Based Routing dla IPv4

- Obsługa routingu dynamicznego dla IPv6

- RIPng, OSPFv3

- Policy Based Routing dla IPv6

- Obsługa MLDv1 oraz MLDv2, filtrowanie IGMP, obsługa MVR (Multicast VLAN Registration)

- Obsługa IGMP v1v2/v3 oraz IGMP v1/v2/v3 snooping

- Obsługa protokołu PIM-SM

- Wsparcie multicast w rozwiązaniu Fabric

- Obsługa Network Login

- IEEE 802.1x

- Web-based Network Login

- MAC based Network Login

- Funkcjonalność flexible authentication (możliwość wyboru kolejności uwierzytelniania – 802.1X/uwierzytelnianie w oparciu o MAC adres/uwierzytelnianie w oparciu o portal www)

- Obsługa wielu klientów (min. 12) Network Login na jednym porcie (Multiple supplicants)

- Możliwość integracji funkcjonalności Network Login z systemem NAC (Network Access Control) oraz obsługa funkcjonalności CoA pozwalającej na wymuszenie reautentykacji dołączonego klienta z systemu NAC

- Przydział sieci VLAN, ACL/QoS podczas logowania Network Login

- Musi działać w architekturze bezpieczeństwa opartej o role. Zapewniając ciągłe zarządzanie tożsamościami z uwierzytelnianiem opartym o role, autoryzacją, QoS i ograniczaniem poziomu pasma

- Urządzenie musi wspierać profile bezpieczeństwa definiowane per użytkownik. Profil bezpieczeństwa oznacza połączenie:

- definicji sieci VLAN,

- reguły filtrowania w warstwach L2-L4 dla IPv4 i IPv6,

- realizację zasad jakości usług w warstwach L2-L4 dla IPv4 i IPv6,

- realizację zasad ograniczania prędkości dla IPv4 i IPv6 w warstwach L2-L4.

- Obsługa TACACS+ (RFC 1492), RADIUS Authentication (RFC 2865) i Accounting (RFC 2866) – również per-command Authentication

- Bezpieczeństwo MAC adresów:

- ograniczenie liczby MAC adresów na porcie

- zatrzaśnięcie MAC adresu na porcie

- możliwość wpisania statycznych MAC adresów na port/vlan

- możliwość wyłączenia MAC learning

- Zabezpieczenie przełącznika przed atakami DoS

- Networks Ingress Filtering RFC 2267

- SYN Attack Protection

- Zabezpieczenie CPU przełącznika poprzez ograniczenie ruchu do systemu zarządzania

- Dwukierunkowe (ingress/egress) listy kontroli dostępu ACL pracujące na warstwie 2, 3 i 4 (ACL realizowane w sprzęcie bez zmniejszenia wydajności przełącznika – wire-speed)

- Obsługa Trusted DHCP Server, DHCP Snooping, DHCP Secured ARP/ARP Validation

- Obsługa Gratuitous ARP Protection, Source IP Lockdown oraz IP Source Guard

- Obsługa redundancji routingu VRRP (RFC 2338) i VRRPv2 (RFC 3768)

- Obsługa STP, RSTP, MSTP, PVST+

- Obsługa topologii Shortest Path Bridging

a. Obsługa IEEE 802.1aq Shortest Path Bridging

b. Obsługa DvR – możliwość rozszerzenia poprzez opcjonalną licencję

- Obsługa protokołu MVRP

- Obsługa EAPS (RFC 3619)

- Obsługa protokołu ERPS lub równoważnego oraz ITU G.8032

- Obsługa Link Aggregation IEEE 802.3ad wraz z LACP

- Obsługa IEEE 802.3ah Ethernet OAM

- Obsługa MLAG lub rozwiązania równoważnego - połączenie link aggregation do dwóch niezależnych przełączników

- Musi mieć możliwość zarządzania za pomocą SSH/Telnet, SNMP, oraz systemu zarządzania dostarczonego przez producenta

- Zarządzanie przez SNMP v1/v2/v3

- Obsługa SYSLOG z możliwością definiowania wielu serwerów

- Sprzętowa obsługa sFlow lub protokołu równoważnego

- Obsługa RMON (RFC 1757) i RMON2 (RFC 2021)

- Obsługa skryptów CLI (możliwość edycji skryptów i ACL bezpośrednio na urządzeniu - system operacyjny musi zawierać edytor plików tekstowych)

- Możliwość uruchamiania skryptów:

- Ręcznie

- O określonym czasie lub co wskazany okres czasu

- Na podstawie wpisów w logu systemowym

- Obsługa XML API poprzez Telnet/SSH i HTTP/HTTPS

- Obsługa Data Center Bridging

- Data Center Bridging Exchange Protocol (DCBx)

- Priority Flow Control (PFC)

- Usługi wirtualizacji warstwy L2 i L3

- Przełącznik musi udostępniać możliwość wirtualizacji usług sieciowych w warstwie L2 i L3 modelu OSI.

- Przełącznik musi zapewniać „multi-tennancy” dla usług sieciowych zarówno w L2 jak i L3. Rozumiemy przez to przypadek, w którym do przełącznika doprowadzone są nakładające się numery VLAN (vlan overlap) lub podsieci IP (subnet overlap). W takim przypadku przełącznik musi zapewniać izolację tego ruchu od siebie.

- Przełącznik musi zapewniać usługi zwirtualizowane L2 i L3 w oparciu o standardowe protokoły sieciowe (SPB 802.1aq lub EVPN)

- Przełącznik musi umożliwiać skonfigurowanie usług wirtualizacji w L2

- Przełącznik musi umożliwiać obsługę usług multicast dla L2 jak i L3 bez konieczności używania protokołu PIM.

- Przełącznik musi zapewniać możliwość zastosowania dowolnej topologii połączeń przy współpracy z innymi urządzeniami tworzącymi węzły sieci szkieletowej.

- Przełącznik musi zapewniać możliwość dokładania nowych węzłów w sieci bez wpływu na już działające usługi sieciowe.

- Dożywotnia gwarancja producenta uwzględniająca:

- wymianę uszkodzonego urządzenia z wysyłką następnego dnia roboczego,

- aktualizacje oprogramowania układowego (firmware),

- dostęp do bazy wiedzy oraz dokumentacji technicznej producenta. Każdy Przełącznik musi zawierać w zestawie:  
• 20szt. mini gibic 10G SFP  
• 20szt.paczkordów światłowodowych 3 metrowych  
• 20szt. paczkordów 1 metrowych  
• 2szt. paczkordów (stack cable) do stackowania przełączników.

1. **Przełączniki dostępowy - 5 sztuk:**

Przełącznik dostępowy – wymagania ogólne

1. Wysokość urządzenia 1U

2. Wbudowany port konsoli szeregowej RJ45 oraz USB/Micro-USB

3. Możliwość łączenia do 8 urządzeń w stos zarządzany z pojedynczego adresu IP, połączenie pomiędzy poszczególnymi urządzeniami musi być możliwe z przepustowością minimum 40Gbps

4. Wbudowany system zasilania 230VAC

5. Obsługa sieci wirtualnych IEEE 802.1Q – min. 4000

6. Wsparcie dla ramek Jumbo Frames (min. 9K bajtów)

7. Obsługa Quality of Service (IEEE 802.1p, DiffServ, 8 kolejek priorytetów na każdym porcie wyjściowym)

8. Modularny system operacyjny z ochroną pamięci, procesów oraz zasobów procesora

9. Możliwość monitorowania zajętości CPU

10. Pojemność tablicy adresów MAC: minimum 32 000 wpisów

11. Możliwość przypisania minimum 1000 ACL (sumarycznie wejściowe i wyjściowe)

12. Obsługa routingu IPv4/IPv6 minimum w zakresie tras statycznych oraz protokołów RIP i OSPF

13. Możliwość - obsługi protokołów IS-IS, BGP4, MBGP - jeżeli funkcjonalność ta wymaga dodatkowej licencji Zamawiający nie wymaga jej dostarczenia w ramach tego postępowania

14. Policy Based Routing dla IPv4 oraz IPv6

15. Obsługa MLDv1 oraz MLDv2, filtrowanie IGMP, obsługa MVR (Multicast VLAN Registration)

16. Obsługa IGMP v1v2/v3 oraz IGMP v1/v2/v3 snooping

17. Obsługa protokołu PIM-SM

18. Możliwość obsługi protokołów PIM DM oraz PIM SSM - jeżeli funkcjonalność ta wymaga dodatkowej licencji Zamawiający nie wymaga jej dostarczenia w ramach tego postępowania

19. Minimum 4000 wpisów multicast (S,G,V)

20. Obsługa uwierzytelniania do sieci z wykorzystaniem:

a. protokołu IEEE 802.1x

b. formularza www

c. adresu MAC

21. Funkcjonalność elastycznego uwierzytelniania z możliwością wyboru kolejności stosowanych mechanizmów – 802.1X/uwierzytelnianie w oparciu o MAC adres/uwierzytelnianie w oparciu o portal www)

22. Obsługa wielu sesji uwierzytelniania (min. 12) na jednym porcie (multiple supplicants)

23. Możliwość integracji funkcjonalności uwierzytelniania z systemem klasy NAC (Network Access Control) oraz obsługa funkcjonalności CoA pozwalającej na wymuszenie reautentykacji dołączonego klienta z poziomu systemu NAC

24. Przydział sieci VLAN, ACL/QoS podczas autentykacji

25. Urządzenie musi wspierać profile bezpieczeństwa definiowane per użytkownik. Profil bezpieczeństwa oznacza połączenie:

a. definicji sieci VLAN,

b. reguły filtrowania w warstwach L2-L4 dla IPv4 i IPv6,

c. realizację zasad jakości usług w warstwach L2-L4 dla IPv4 i IPv6,

d. realizację zasad ograniczania prędkości dla IPv4 i IPv6 w warstwach L2-L4.

26. Obsługa TACACS+ (RFC 1492), RADIUS Authentication (RFC 2865) i Accounting (RFC 2866) wraz z funkcjonalnością per-command authentication

27. Bezpieczeństwo adresów MAC:

a. ograniczenie liczby MAC adresów na porcie

b. zatrzaśnięcie MAC adresu na porcie

c. możliwość wpisania statycznych MAC adresów na port/vlan

d. możliwość wyłączenia uczenia MAC adresów

28. Zabezpieczenie przełącznika przed atakami DoS

a. Networks Ingress Filtering RFC 2267

b. SYN Attack Protection

c. Zabezpieczenie CPU przełącznika poprzez ograniczenie ruchu do systemu zarządzania

29. Dwukierunkowe (ingress/egress) listy kontroli dostępu ACL pracujące na warstwie 2, 3 i 4 (ACL realizowane w sprzęcie bez zmniejszenia wydajności przełącznika)

30. Obsługa Trusted DHCP Server, DHCP Snooping, DHCP Secured ARP/ARP Validation

31. Obsługa Gratuitous ARP Protection, Source IP Lockdown oraz IP Source Guard

32. Obsługa redundancji routingu VRRP (RFC 2338) i VRRPv2 (RFC 3768)

33. Wsparcie dla technologii Ethernet VPN (EVPN) oraz tunelowania GRE - jeżeli funkcjonalność ta wymaga dodatkowej licencji Zamawiający nie wymaga jej dostarczenia w ramach tego postępowania

34. Obsługa protokołów drzewa rozpinającego (spanning Tree) w zakresie STP, RSTP, MSTP, PVST+

35. Obsługa protokołu MVRP

36. Obsługa protokołu EAPS (RFC 3619), ERPS (ITU G.8032) lub równoważnego

37. Obsługa Link Aggregation IEEE 802.3ad wraz z mechanizmem LACP

38. Obsługa IEEE 802.3ah Ethernet OAM

39. Obsługa mechanizmu MC-LAG/VSS/MLAG/IRF lub równoważnego umożliwiającego agregację połączeń do dwóch niezależnych przełączników. Urządzenia dołączające się do pary przełączników muszą widzieć je jako pojedyncze urządzenie z punktu widzenia warstwy L2. Nie dopuszcza się stosowania mechanizmów łączenia w stos.

40. Zarządzany za pomocą SSH/Telnet, SNMP v1/v2/v3, oraz systemu zarządzania dostarczonego przez producenta

41. Obsługa SYSLOG z możliwością definiowania wielu serwerów

42. Sprzętowa obsługa sFlow lub protokołu równoważnego

43. Obsługa RMON (RFC 1757) i RMON2 (RFC 2021)

44. Obsługa skryptów CLI (możliwość edycji skryptów i ACL bezpośrednio na urządzeniu - system operacyjny musi zawierać edytor plików tekstowych)

45. Możliwość uruchamiania skryptów:

a. ręcznie

b. o określonym czasie lub co wskazany okres czasu

c. na podstawie wpisów w logu systemowym

46. Obsługa XML API poprzez Telnet/SSH i HTTP/HTTPS

47. Obsługa protokołu MACSEC (IEEE 802.1AE) na wszystkich portach urządzenia (zarówno porty miedziane jak i światłowodowe) – jeżeli funkcjonalność ta wymaga dodatkowych modułów lub licencji Zamawiający nie wymaga ich dostarczenia w ramach tego postępowania

48. Usługi wirtualizacji warstwy L2 i L3 (Fabric Network)

- Przełącznik musi udostępniać możliwość wirtualizacji usług sieciowych w warstwie L2 i L3 modelu OSI.

- Przełącznik musi zapewniać „multi-tennancy” dla usług sieciowych zarówno w L2 jak i L3. Rozumiemy przez to przypadek, w którym do przełącznika doprowadzone są nakładające się numery VLAN (vlan overlap) lub podsieci IP (subnet overlap). W takim przypadku przełącznik musi zapewniać izolację tego ruchu od siebie.

- Przełącznik musi zapewniać usługi zwirtualizowane L2 i L3 w oparciu o standardowe protokoły sieciowe (SPB 802.1aq lub EVPN)

- Przełącznik musi umożliwiać skonfigurowanie usług wirtualizacji w L2

- Przełącznik musi umożliwiać obsługę usług multicast dla L2 jak i L3 bez konieczności używania protokołu PIM.

- Przełącznik musi zapewniać możliwość zastosowania dowolnej topologii połączeń przy współpracy z innymi urządzeniami tworzącymi węzły sieci szkieletowej.

- Przełącznik musi zapewniać możliwość dokładania nowych węzłów w sieci bez wpływu na już działające usługi sieciowe.

49. Gwarancja producenta uwzględniająca:

a. wymianę uszkodzonego urządzenia z wysyłką następnego dnia roboczego,

b. aktualizacje oprogramowania układowego (firmware),

c. dostęp do bazy wiedzy oraz dokumentacji technicznej producenta.

Przełącznik dostępowy 48 portowy – wymagania szczegółowe

1. Przełącznik wyposażony w:

a. minimum 48 interfejsów 10/100/1000Base-T RJ45

b. minimum 4 interfejsy 1/10Gb Base-X SFP+

c. minimum 4 interfejsy 1000 Base-X SFP

d. możliwość rozbudowy (licencje – np. kosztem portów SFP, dodatkowy moduł) o dodatkowe 4 porty 10Gb SFP+.

2. Nieblokująca architektura o wydajności przełączania min. 256 Gbps i matrycy przełączającej z szybkością minimum 190 milionów pakietów na sekundę (Mpps)

3. Pojemność tablicy ARP: minimum 15 000 wpisów

4. Minimum 12 000 wpisów w tablicy routingu IPv4 oraz minimum 6 000 wpisów w tablicy routingu IPv6

„***Niniejszy dokument powinien być podpisany kwalifikowanym podpisem elektronicznym”***