**OPIS PRZEDMIOTU ZAMÓWIENIA**

**Zadanie nr 1**

**Parametry techniczne**

Serwery klastra bazy danych - 2 szt.   
Producent: …........................................................................................   
Model:...................................................................................................

|  |  |  |  |
| --- | --- | --- | --- |
| **Lp** | **Parametr lub warunek** | **Opis parametrów technicznych / Minimalne w tym graniczne** | **PARAMETR OFEROWANY**  **(podać zakresy i opisać)** |
| 1 | Obudowa | * Typu RACK, wysokość nie więcej niż 2U; * Szyny umożliwiające wysunięcie serwera z szafy stelażowej; * Opcjonalne ramię porządkujące ułożenie przewodów z tyłu serwera; * Możliwość zainstalowania 10 dysków twardych hot plug 3,5”; * Możliwość zainstalowania fizycznego zabezpieczenia (np. na klucz lub elektrozamek) uniemożliwiającego fizyczny dostęp do dysków twardych; * Możliwość zainstalowania dedykowanego wewnętrznego napędu blu-ray. |  |
| 2 | Płyta główna | * Dwuprocesorowa; * Wyprodukowana i zaprojektowana przez producenta serwera * Możliwość instalacji procesorów 38-rdzeniowych; * Możliwość zainstalowania modułu TPM 2.0; * 7 złącz PCI Express generacji 4 w tym (minimum 3 złącza aktywne, możliwe do obsadzenia): * 4 fizyczne złącza o prędkości x16; * 3 fizyczne złącza o prędkości x8; * Opcjonalnie możliwość uzyskania 2 złącz typu pełnej wysokości; * Opcjonalnie możliwość uzyskania 8 aktywnych złącz PCI-e; * 32 gniazda pamięci RAM; * Obsługa minimum 4TB pamięci RAM DDR4; * Obsługa minimum 12TB pamięci RAM DDR4 + pamięć nieulotna * Wsparcie dla technologii: * Memory Scrubbing * SDDC * ECC * Memory Mirroring * ADDDC; * Obsługa pamięci nieulotnej instalowanej w gniazdach pamięci RAM (przez pamięć nieulotną rozumie się moduły pamięci zachowujące swój stan np. w przypadku nagłej awarii zasilania, nie dopuszcza się podtrzymania bateryjnego stanu pamięci) * Minimum 2 sloty dla dysków M.2 na płycie głównej (lub dedykowanej karcie PCI Express)  nie zajmujące klatek dla dysków hot-plug; |  |
| 3 | Procesory | * Jeden procesor 12-rdzeniowy * Taktowanie 2,1GHz * architektura x86\_64 * osiągające w teście SPEC CPU2017 Floating Point wynik SPECrate2017\_fp\_base minimum 189 pkt  (wynik osiągnięty dla zainstalowanych dla dwóch procesorów). Wynik musi być opublikowany na stronie <https://www.spec.org/cpu2017/results/cpu2017.html> |  |
| 4 | Pamięć RAM | * 256 GB pamięci RAM * DDR4 Registered * 3200Mhz |  |
| 5 | Dyski SSD | * 3 szt. dysków SSD SATA min 960GB DWPD>3,5; |  |
| 6 | Kontrolery LAN | * Karta LAN, nie zajmująca żadnego z dostępnych slotów PCI Express, wyposażona minimum w interfejsy: 4x 1Gbit Base-T, możliwość wymiany zainstalowanych interfejsów na 2x 100Gbit QSFP28 bez konieczności instalacji kart w slotach PCIe; |  |
| 7 | Kontrolery I/O | * Możliwość zainstalowania kontrolera RAID obsługującego dyski NVMe; * Możliwość zainstalowania dwóch nośników flash o pojemności 64GB w konfiguracji RAID-1, rozwiązanie dedykowane dla hypervisora oraz niezajmujące zatok dla dysków hot-plug; * Zainstalowany kontroler SAS RAID obsługujący poziomy 0,1,10,5,50,6,60 posiadający 2GB pamięci cache (opcjonalnie możliwość zabezpieczenia za pomocą baterii lub kondensatora) |  |
| 8 | Porty | * Zintegrowana karta graficzna ze złączem VGA z tyłu oraz przodu serwera; * 2 port USB 3.0 wewnętrzne; * 2 porty USB 3.0 dostępne z tyłu serwera; * Opcjonalny port serial, możliwość wykorzystania portu serial do zarządzania serwerem; * Ilość dostępnych złącz USB nie może być osiągnięta poprzez stosowanie zewnętrznych przejściówek, rozgałęziaczy czy dodatkowych kart rozszerzeń zajmujących jakikolwiek slot PCI Express i/lub USB serwera; * 2 porty USB 3.0 na panelu przednim |  |
| 9 | Zasilanie, chłodzenie | * Redundantne zasilacze hotplug o sprawności 94% (tzw. klasa Platinum) o mocy minimalnej 900W; * Redundantne wentylatory hotplug; |  |
| 10 | Zarządzanie | * Wbudowane diody informacyjne lub wyświetlacz informujące o stanie serwera - system przewidywania, rozpoznawania awarii * 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   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 do komunikacji wyłącznie z kontrolerem zdalnego zarządzania z możliwością przeniesienia tej komunikacji na inną kartę sieciową współdzieloną z systemem operacyjnym; * Dostęp poprzez przeglądarkę Web, SSH; * Zarządzanie mocą i jej zużyciem oraz monitoring zużycia energii; * Zarządzanie alarmami (zdarzenia poprzez SNMP) * Możliwość przejęcia konsoli tekstowej * Możliwość zarządzania przez 6 administratorów jednocześnie * Przekierowanie konsoli graficznej na poziomie sprzętowym oraz możliwość montowania zdalnych napędów i ich obrazów na poziomie sprzętowym (cyfrowy KVM) * Obsługa serwerów proxy (autentykacja) * Obsługa VLAN * Możliwość konfiguracji parametru Max. Transmission Unit (MTU) * Wsparcie dla protokołu SSDP * Obsługa protokołów TLS 1.2, SSL v3 * Obsługa protokołu LDAP * Integracja z HP SIM * Synchronizacja czasu poprzez protokół NTP * Możliwość backupu i odtworzenia ustawień bios serwera oraz ustawień karty zarządzającej * 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); * Dedykowana, do wbudowania w kartę zarządzającą (lub zainstalowana) pamięć flash o pojemności minimum 16 GB; * Możliwość zdalnej reinstalacji systemu lub aplikacji z obrazów zainstalowanych w obrębie dedykowanej pamięci flash bez użytkowania zewnętrznych nośników lub kopiowania danych poprzez sieć LAN; * Serwer posiadający możliwość konfiguracji i wykonania aktualizacji BIOS, Firmware, sterowników serwera bezpośrednio z GUI (graficzny interfejs) karty zarządzającej serwera bez pośrednictwa innych nośników zewnętrznych i wewnętrznych poza obrębem karty zarządzającej. * BIOS UEFI w specyfikacji 2.7; |  |
| 11 | Wspierane OS | * Microsoft Windows Server 2022, 2019, 2016 * VMWare vSphere 6.7, 7.0 * Suse Linux Enterprise Server 15 * Red Hat Enterprise Linux 7.9, 8.3 * Hyper-V Server 2016, 2019 * Oracle Linux   **Zainstalowany system Oracle Linux lub równoważny** |  |
| 12 | Gwarancja | * 84 miesiące gwarancji producenta serwera w trybie on-site z gwarantowaną skuteczną naprawą w miejscu użytkowania sprzętu do końca następnego dnia od zgłoszenia. Naprawa realizowana przez producenta serwera lub autoryzowany przez producenta serwis. * Funkcja zgłaszania usterek i awarii sprzętowych poprzez automatyczne założenie zgłoszenia w systemie helpdesk/servicedesk producenta sprzętu; * Uszkodzone dyski twarde nie podlegają zwrotowi organizacji serwisowej; * Firma serwisująca musi posiadać certyfikat ISO 9001:2000 lub równoważny na świadczenie usług serwisowych; (Za równoważne Zamawiający uzna posiadanie certyfikatu wystawionego przez niezależny uprawniony do tego pomiot potwierdzającego odpowiednie stosowanie przez firmę serwisującą środków zapewnienia norm i jakości w zakresie usług serwisowych) Bezpłatna dostępność poprawek i aktualizacji BIOS/Firmware/sterowników dożywotnio dla oferowanego serwera – jeżeli funkcjonalność ta wymaga dodatkowego serwisu lub licencji producenta serwera, takowy element musi być uwzględniony w ofercie; |  |
| 13 | Dokumentacja, inne | * Elementy, z których zbudowane są serwery muszą być produktami producenta tych serwerów lub być przez niego certyfikowane oraz całe muszą być objęte gwarancją producenta * Serwer musi być fabrycznie nowy i pochodzić z oficjalnego kanału dystrybucyjnego w UE – wymagane oświadczenie producenta dołączone do oferty * Ogólnopolska, telefoniczna infolinia/linia techniczna producenta serwera, w ofercie należy podać link do strony producenta na której znajduje się nr telefonu oraz maila na który można zgłaszać usterki; * W czasie obowiązywania gwarancji na sprzęt, możliwość, po podaniu na infolinii numeru seryjnego urządzenia, weryfikacji pierwotnej konfiguracji sprzętowej serwera, w tym model i typ dysków twardych, procesora, ilość fabrycznie zainstalowanej pamięci operacyjnej, czasu obowiązywania i typu udzielonej gwarancji; * Możliwość aktualizacji i pobrania sterowników do oferowanego modelu serwera w najnowszych certyfikowanych wersjach bezpośrednio z sieci Internet za pośrednictwem strony www producenta serwera; * Możliwość pracy w pomieszczeniach o wilgotności w zawierającej się w przedziale 10 - 85 %; * Zgodność z normami: CB, RoHS, WEEE, GS oraz CE; |  |

Macierz klastra bazy danych – 1 szt  
Producent: …........................................................................................   
Model:...................................................................................................

|  |  |  |  |
| --- | --- | --- | --- |
| **Lp** | **Parametr lub warunek** | **Opis parametrów technicznych / Minimalne w tym graniczne** | **PARAMETR OFEROWANY**  **(podać zakresy i opisać)** |
| 1 | Wymagania ogólne | System musi być dostarczony ze wszystkimi komponentami do instalacji w standardowej szafie rack 19” z zajętością maks. 2U w tej szafie. Każdy skonfigurowany moduł/obudowa musi posiadać układ nadmiarowy zasilania i chłodzenia, zapewniający bezprzerwową pracę macierzy bez ograniczeń czasowych w przypadku utraty redundancji w danym układzie (zasilania lub chłodzenia). Każdy moduł/obudowa powinien posiadać widoczne elementy sygnalizacyjne do informowania o stanie poprawnej pracy lub awarii. Rozbudowa o dodatkowe moduły dla obsługiwanych dysków powinna odbywać się wyłącznie poprzez zakup takich modułów, bez konieczności zakupu dodatkowych licencji lub specjalnego oprogramowania aktywującego proces rozbudowy lub musi być dostarczona licencja na dwukrotność dostarczanej pojemności. Dostarczana macierz musi umożliwiać takie podłączenie półek aby awaria lub/i usunięcie jednej z półek nie powodowało utraty dostępu do danych znajdujących się na pozostałych modułach. Oferowana macierz musi obsługiwać  min. 260 dysków wykonanych w technologii hot-plug. Wszystkie zainstalowane dyski hot-plug, z wyłączeniem dysków SSD stosowanych jako rozszerzenie pamięci Cache kontrolerów,  muszą być dostępne dla zapisu danych Użytkownika. Macierz musi umożliwiać rozbudowę i jednoczesne podłączenie i używanie modułów (tzw. „półek dyskowych”) w rozmiarze 2U pozwalająca umieścić do 24 dysków 2,5” typu hotplug dla dysków SAS i SSD oraz w rozmiarze 2U dla 12 dysków 3,5” typu hotplug NL-SAS i SSD oraz półki gęstego upakowania dla 60 dysków typu hotplug NL-SAS; Wymaga się aby macierz umożliwiała jednoczesne podłączenie i użycie dowolnego rodzaju i kombinacji wyżej wymienionych półek dyskowych (tj. 2,5” + 3,5” + gęstego upakowania). |  |
| 2 | Pojemność macierzy | Min 6 dysków SSD SAS pojemności min 960 GB |  |
| 3 | Kontrolery | * Kontrolery macierzy muszą obsługiwać tryb pracy w układzie active-active lub mesh-active,  macierz musi być dostarczona z zainstalowanymi minimum 2 kontrolerami; * Każdy z kontrolerów macierzy musi posiadać po minimum 32GB pamięci podręcznej Cache (z możliwością rozbudowy do 64GB) – kontrolery muszą obsługiwać między sobą mechanizm lustrzanej kopii danych (cache mirror) przeznaczonych do zapisu; * Macierz musi obsługiwać rozbudowę pamięci podręcznej cache dla operacji  odczytu o minimum 800GB poprzez instalację dodatkowych modułów pamięci w kontrolerach lub wykorzystanie pojemności zainstalowanych dysków SSD, * W przypadku awarii zasilania dane nie zapisane na dyski, przechowywane w pamięci podręcznej Cache dla zapisów muszą być zabezpieczone metodą trwałego zapisu na dysk. * Kontrolery muszą posiadać możliwość ich wymiany bez konieczności wyłączania zasilania całego urządzenia; * Kontrolery macierzy obsługują funkcjonalność kompresji danych. * Kontrolery macierzy obsługują funkcjonalność deduplikacji w trybie in-line. * Macierz musi obsługiwać wymianę kontrolera RAID bez utraty danych zapisanych na dyskach. * Każdy z kontrolerów RAID powinien posiadać dedykowany minimum 2 interfejsy RJ-45 Ethernet obsługujący połączenia z prędkością minimum 1Gb/s dla zdalnej  komunikacji z oprogramowaniem zarządzającym i konfiguracyjnym macierzy. * Kontrolery macierzy muszą być oparte o procesor wykonany w technologii wielordzeniowej z minimum 4 rdzeniami, * Kontrolery macierzy muszą obsługiwać do 130 grup dyskowych w całym rozwiązaniu, bez konieczności wymiany dostarczonych kontrolerów * Oferowana macierz musi mieć wyprowadzone 2 porty FC 16Gb/s (obsadzone modułami LC MMF) do dołączenia serwerów bezpośrednio lub do sieci san na każdy kontroler RAID. * Macierz musi umożliwiać wymianę zainstalowanych portów do transmisji danych na porty 2x 10Gb/s Base-T iSCSI * Macierz musi umożliwiać wymianę zainstalowanych portów do transmisji danych na porty 4x FC 16GB/s * Macierz musi umożliwiać wymianę zainstalowanych portów do transmisji danych na porty 2x FC 32Gb/s * Macierz musi umożliwiać dołożenie dodatkowych portów do transmisji danych 2x 10Gb/s SFP+ CIFS/NFS * Macierz musi umożliwiać dołożenie dodatkowych portów do transmisji danych 2x 12Gb/s SAS * Macierz musi umożliwiać dołożenie dodatkowych portów do transmisji danych 2x 10Gb/s SFP+ iSCSI * Wymiana oraz dołożenie portów jw. nie może powodować wymiany samych kontrolerów RAID w oferowanym rozwiązaniu a w przypadku konieczność licencjonowania tej funkcjonalności macierz ma być dostarczona z aktywną licencja na instalację i obsługę każdego z wymienionych protokołów transmisji danych * Macierz posiada obsługę operacji plikowych I/O w sieci NAS w obrębie zainstalowanych kontrolerów. Protokoły dostępu: CIFS, NFS. W przypadku obsługi protokołów CIFS i NFS wymagana jest funkcjonalność agregacji przepustowości dla interfejsów dedykowanych do obsługi tych protokołów. Obsługa protokołów CIFS i NFS musi odbywać się jednocześnie . **– nie jest wymagane dostarczenie tej funkcjonalności – opcja rozbudowy** |  |
| 4 | Poziomy RAID | * Macierz musi zapewniać poziom zabezpieczenia danych na dyskach definiowany poziomami RAID:   + Raid-1   + Raid-10   + Raid-5   + Raid-6   + Raid-50   + Raid-0 |  |
| 5 | Dyski | Oferowana macierz musi wspierać dyski hot-plug:   * dyski elektroniczne SSD i mechaniczne HDD z interfejsami SAS 12Gb/s * dyski mechaniczne HDD o prędkości obrotowej 7,2 krpm, 10 krpm, * Macierz musi obsługiwać mieszaną konfigurację dysków hot-plug SSD i HDD w rozmiarach 2,5” i 3,5” zainstalowanych w dowolnym module rozwiązania; * Wszystkie dyski wspierane przez oferowany model macierzy muszą być wykonane w technologii hot-plug i posiadać podwójne porty SAS obsługujące tryb pracy full-duplex * Macierz musi obsługiwać min. 256 dysków SAS SSD w całym rozwiązaniu, bez konieczności dokupowania/wymiany żadnych innych elementów sprzętowych czy licencyjnych innych niż same półki dyskowe wraz z dyskami; * Możliwość rozbudowy oferowanego modelu macierzy do minimum 520 dysków bez migracji i przenoszenia danych - jedynie poprzez wymianę modułu kontrolerów macierzy (bez konieczności wymiany posiadanych dysków, półek dyskowych, bez konieczności przenoszenia danych/ istniejącej struktury grup dyskowych/LUN, jak również z zachowaniem istniejącej gwarancji producenta na półki dyskowe i dyski; * Macierz musi umożliwiać skonfigurowanie każdego zainstalowanego dysku hot-plug jako dysk hot-spare (dysk zapasowy) lub wirtualna przestrzeń zapasowa: * Macierz posiada możliwość konfiguracji dysku hot-spare dla zabezpieczenia dowolnej grupy dyskowej RAID lub zapasowa przestrzeń wirtualna wielkości 33% zabezpieczanej pojemności. * Macierz posiada możliwość konfiguracji dysku hot-spare dedykowanego dla zabezpieczenia tylko wybranej grupy dyskowej RAID lub zapasowa przestrzeń wirtualna wielkości 33% zabezpieczanej pojemności. * W przypadku awarii dysku fizycznego i wykorzystania wcześniej skonfigurowanego  dysku zapasowego wymiana uszkodzonego dysku na sprawny nie może powodować powrotnego kopiowania danych z dysku hot-spare na wymieniony dysk (tzw. CopyBackLess) lub nie wymaga zwolnienia zapasowej przestrzeni wirtualnej. * Macierz musi pozwalać na zaszyfrowanie danych zapisanych na wszystkich obsługiwanych dyskach SSD-SAS, HDD-SAS oraz HDD NL-SAS minimum kluczem AES256-bit – jeżeli  w tym celu niezbędne jest zakupienie dodatkowych licencji bądź komponentów sprzętowych to należy je dostarczyć wraz z macierzą. * Macierz musi umożliwiać zaszyfrowanie całej dostępnej powierzchni użytkowej minimum kluczem AES256-bit. |  |
| 6 | **Opcje programowe** | * Macierz musi być wyposażona w system kopii migawkowych umożliwiających wykonanie minimum 2048 kopii migawkowych * Macierz musi umożliwiać zdefiniowanie min. 8000 woluminów  (LUN) * Macierz powinna umożliwiać podłączenie logiczne z serwerami i stacjami poprzez min. 1024 ścieżek logicznych FC * Macierz musi umożliwiać aktualizację oprogramowania wewnętrznego kontrolerów RAID i dysków bez konieczności wyłączania macierzy oraz bez konieczności wyłączania ścieżek logicznych FC/iSCSI dla podłączonych stacji/serwerów * Macierz musi umożliwiać dokonywanie w trybie on-line (tj. bez wyłączania zasilania i bez przerywania przetwarzania danych w macierzy) operacje: powiększanie grup dyskowych, zwiększanie rozmiaru woluminu, migrowanie woluminu na inną grupę dyskową * Macierz musi posiadać wsparcie dla systemów operacyjnych : Microsoft Windows Server 2012R2, 2016, 2019, SuSE Linux Enterprise Server, Red Hat Linux Enterprise Server, HP-UNIX, IBM AIX, SUN Solaris, Vmware Vsphere; * Macierz musi być dostarczona z licencją na oprogramowanie wspierające  technologię typu multipath (obsługa nadmiarowości dla ścieżek transmisji danych pomiędzy macierzą i serwerem)  dla połączeń FC i iSCSI. * Macierz musi posiadać możliwość uruchamiania mechanizmów zdalnej replikacji danych, w trybie synchronicznym i asynchronicznym, po protokołach FC oraz iSCSI,   bez konieczności stosowania zewnętrznych urządzeń konwersji wymienionych protokołów transmisji. Funkcjonalność replikacji danych musi być zapewniona z poziomu oprogramowania wewnętrznego macierzy, jako tzw. storage-based data replication. Replikacja danych musi być obsługiwana w połączeniu z każdą macierzą z tej samej rodziny urządzeń wspierającą obsługę zdalnej replikacji danych; **– nie jest wymagane dostarczenie tej funkcjonalności – opcja rozbudowy** * Macierz musi posiadać możliwość tworzenia lokalnych tj. w obrębie zasobów macierzy, pełnych kopii danych (tzw. klony danych), kopii przyrostowych oraz kopii lustrzanych (mirror) – **nie jest wymagane dostarczenie tej funkcjonalności – opcja rozbudowy;** * Macierz musi obsługiwać mechanizm ochrony priorytetów obsługi wybranych zasobów – za taki mechanizm uznaje się funkcję typu ‘cache partitioning’ lub ‘storage partitioning’. * Macierz musi obsługiwać adresację IP v.4 i IP v.6 * Wraz z macierzą należy dostarczyć oprogramowanie lub moduły programowe typu plug-in pozwalające na integracje macierzy w środowiskach Vmware w zakresie obsługi mechanizmów: Vmware VAAI, Vmware VVOL, Vmware MultiPath IO – z subskrypcją do bezpłatnej aktualizacji w całym okresie obowiązywania gwarancji * Macierz musi obsługiwać mechanizmy Thin Provisioning, czyli przydziału dla obsługiwanych środowisk woluminów logicznych o sumarycznej pojemności większej od sumy pojemności dysków fizycznych zainstalowanych w macierzy. * Macierz musi obsługiwać mechanizmy typu AST (Automated Storage Tiering) tj. automatycznego migrowania i realokacji bloków danych pomiędzy różnymi technologiami dyskowymi na podstawie analizy częstotliwości operacji I/O dla tych bloków oraz wg potrzeb wydajnościowych serwerów, środowisk  i aplikacji korzystających z zasobów macierzy. Mechanizm AST musi być obsługiwany przy korzystaniu zarówno z trzech jak z dwóch dostarczonych technologii dyskowych: SSD, SSAS, NLSAS. Macierz musi pozwalać na definiowanie różnych polityk i zasad migrowania danych w obrębie tej samej macierzy. Mechanizm AST musi obsługiwać funkcję Quality-of-Services pozwalająca na zagwarantowaniu wydajności dla wybranych zasobów macierzy (woluminów) mierzonej jako maksymalny czas opóźnień operacji I/O wykonywanych przez  serwer/środowisko/aplikację. Mechanizm AST musi pozwalać na definiowanie okna czasowego dla zbierania pomiarów wydajności operacji I/O oraz okna czasowego dla migrowania danych wg ustalonych zasad i polityk – minimalny definiowany czas trwania w/w operacji (długość okna czasowego) nie może być dłuższy niż 6 godzin. Mechanizm AST musi pozwalać na wykluczanie wybranych godzin i dni z pomiarów wydajności operacji I/O**. – nie jest wymagane dostarczenie tej funkcjonalności – opcja rozbudowy** * Macierz musi wspierać usługi VSS (Volume ShadowCopy Services) w systemach klasy Microsoft Windows Sever – wymagane jest dostarczenie niezbędnego oprogramowania / sterowników VSS pozwalających na obsługę VSS przy maksymalnej pojemności i liczbie dysków obsługiwanych przez oferowaną. W czasie trwania gwarancji wymaga się bezpłatnego dostępu do nowych wersji  oprogramowania  i sterowników * Macierz musi obsługiwać mechanizmy migracji danych w trybie online  z innej macierzy tej klasy, z zachowaniem obsługi operacji I/O dla serwerów podłączonych do migrowanej macierzy tj. do migrowanych zasobów LUN * Macierz wspiera rozwiązania klasy ‘klastra macierzowego’ tj. zapewnienia wysokiej dostępności zasobów dyskowych macierzy dla podłączonych platform software’owych i sprzętowych z wykorzystaniem synchronicznej replikacji danych pomiędzy minimum 2 macierzami protokołami FC oraz iSCSI. Mechanizm klastra macierzowego musi być obsługiwany dla protokołów FC oraz iSCSI, zarówno w zakresie replikacji danych jak i w zakresie sposobu podłączenia serwerów do zasobów macierzy. Pod użytym pojęciem ”wysoka dostępność zasobów dyskowych” należy rozumieć zapewnienie bezprzerwowego działania środowiska (aplikacja/ system operacyjny/ serwer) podłączonego do macierzy (macierz podstawowa) w przypadku wystąpienia awarii logicznego połączenia z tą macierzy bądź awarii samej macierzą, powodujących dla danego środowiska brak dostępu do zasobów macierzy podstawowej. Funkcjonalność ‘klastra macierzowego’ musi pozwalać na automatyczne i ręczne przełączanie obsługi środowisk produkcyjnych z macierzy podstawowej na zapasową w przypadku awarii macierzy podstawowej (tzw. Automated/manual failover). **– nie jest wymagane dostarczenie tej funkcjonalności – opcja rozbudowy** * Macierz w dostarczonej konfiguracji musi obsługiwać deduplikację i kompresję danych na dyskach wbudowanych w macierzy (nie dopuszcza się główek, kompresji zewnętrznej, programowej itp.) w następujących trybach równocześnie oraz niezależnie na poziomie każdego LUN:   + Sama deduplikacja wybranego LUN;   + Sama kompresja wybranego LUN;   + Kombinacja technologii kompresji i deduplikacji wybranego LUN;   + Brak użycia technologii kompresji i deduplikacji dla wybranego LUN; |  |
| 7 | **Zarządzanie** | * Oprogramowanie do zarządzania musi być zintegrowane z systemem operacyjnym systemu pamięci masowej * Komunikacja z wbudowanym oprogramowaniem zarządzającym macierzą musi być możliwa w trybie graficznym np. poprzez przeglądarkę WWW oraz w trybie tekstowym. * Musi być możliwe zdalne zarządzanie macierzą z wykorzystaniem standardowej przeglądarki internetowej (np. Internet Explorer, Google Chrome, Mozilla Firefox) bez konieczności instalacji  żadnych dodatkowych aplikacji na stacji administratora * Wbudowane oprogramowanie macierzy musi obsługiwać połączenia z modułem zarządzania macierzy poprzez szyfrowanie komunikacji protokołami: SSL dla komunikacji poprzez przeglądarkę WWW i protokołem SSH dla komunikacji poprzez CLI |  |
| 8 | **Gwarancja i serwis** | * Całe rozwiązanie musi być objęte minimum 84 miesięcznym okresem gwarancji z naprawą miejscu instalacji urządzenia i z gwarantowanym czasem skutecznego zakończenia naprawy do końca następnego dnia roboczego od dnia zgłoszenia awarii do organizacji serwisowej producenta macierzy. * Uszkodzone dyski twarde nie podlegają zwrotowi organizacji serwisowej; * Serwis gwarancyjny musi obejmować dostęp do poprawek i nowych wersji oprogramowania wbudowanego, które są elementem zamówienia. * Po zakończeniu okresu gwarancji musi być zapewniony przez producenta rozwiązania bezpłatny dostęp do aktualizacji oprogramowania wewnętrznego oferowanej macierzy oraz do kolejnych wersji oprogramowania zarządzającego w okresie minimum 2 lat. * System musi zapewniać możliwość samodzielnego i automatycznego powiadamiania producenta i administratorów Zamawiającego o usterkach za pomocą wiadomości wysyłanych poprzez szyfrowany protokół. Funkcjonalność musi pozwalać na automatyczne otwarcie zgłoszenia serwisowego w bazie serwisowej producenta macierzy zgodnie z wymaganym w specyfikacji poziomem SLA; Opcja ta musi być dostępna bezpłatnie w trakcie całego okresu gwarancji producenta macierzy.  Oferowana funkcjonalność musi również umożliwiać konfigurację i uruchomienie zdalnego dostępu do macierzy bezpośrednio przez Producenta – musi być do tego wykorzystany dedykowany system serwisowy macierzy. * Macierz musi pochodzić z oficjalnego kanału sprzedaży producenta w UE. Nie dopuszcza się użycia macierzy odnawianych, demonstracyjnych lub powystawowych * Urządzenie musi być wykonane zgodnie z europejskimi dyrektywami RoHS i WEEE stanowiącymi o unikaniu i ograniczaniu stosowania substancji szkodliwych dla zdrowia * Producent oferowanej macierzy musi posiadać dedykowaną, ogólnie dostępną stronę internetową, gdzie po wpisaniu numeru seryjnego macierzy można zweryfikować co najmniej: czas i poziom oferowanego serwisu gwarancyjnego producenta zarówno dla macierzy jak i dowolnej z półek dyskowych, datę zakończenia wsparcia gwarancyjnego, datę zakończenia wsparcia producenta dla oferowanego urządzenia – w formularzu ofertowym należy podać adres internetowy strony producenta macierzy,  gdzie można zweryfikować wymagane informacje; |  |

Przełączniki FC klastra bazy danych – 2 szt  
Producent: …........................................................................................   
Model:...................................................................................................

|  |  |  |  |
| --- | --- | --- | --- |
| **Lp** | **Parametr lub warunek** | **Opis parametrów technicznych / Minimalne w tym graniczne** | **PARAMETR OFEROWANY**  **(podać zakresy i opisać)** |
| 1 | Obudowa i porty | * Wysokość przełącznika 1U w systemie montażu w szafie typu rack 19” * Ilość portów SFP: 24 szt.   - porty uniwersalne o maksymalnej przepustowości 32GB/s, z obsługą przepustowości  16Gbit/s, 8Gbit/s i 4Gbit/s z automatycznym wyborem przepustowości (auto-sensing), obsługa trybu full-duplex   * 8 portów aktywnych, porty aktywne obsadzone modułami optycznymi SFP 16Gbit/s, Short Wave Length (SWL), Multi Mode Fibre (MMF) * 8 przewodów FC OM4 MMF LC/LC 5m |  |
| 2 | Funkcjonalność | * Obsługa trybów pracy portów FC: D\_port, F\_port, E\_port, M-Port * Obsługa funkcji POD (Ports on Demand) przydziału licencji dla aktywnych portów FC * Możliwość aktualizacji firmware’u switcha * Aktywne funkcje: Active Gateway, Webtools, Advanced Zoning, FullFabric (z obsługą do min. 128 przełączników FC) * Możliwość obsługi funkcjonalności (przez zakupienie odpowiednich licencji): Trunking, Extended Fabric, Fabric Vision |  |
| 3 | Zarządzanie | * RJ-45 min 10/100 Mb/s do zarządzania poprzez sieć Ethernet * RJ-45 lub DB9 do zarządzania poprzez interfejs RS232 * USB * In-band over FC |  |
| 4 | Pozostałe | * Sygnalizacja aktywnych i podłączonych portów na panelu przednim urządzenia * Zarządzanie poprzez przeglądarkę WWW z obsługą połączeń szyfrowanych 128-bit SSL oraz poprzez usługę SSH * Wsparcie dla protokołu SNMP v.3 |  |
| 5 | Gwarancja | * 84 miesiące gwarancji producenta w trybie on-site z gwarantowaną skuteczną naprawą do końca następnego roboczego dnia od zgłoszenia. Naprawa realizowana przez certyfikowanego przez producenta serwisanta. |  |

**Zakres usług**

1. **PRACE INSTALACYJNE i KONFIGURACYJNE OPROGRAMOWANIA**

Zamawiający oczekuje przeniesienia obecnej infrastruktury serwerowo-bazodanowej do nowego środowiska opartego o dostarczone dwa fizyczne serwery połączone z macierzą światłowodowym FC.

W oparciu o dostarczony przez Zamawiającego sprzęt, należy zrealizować funkcje klastra wysokiej dostępności w ramach pojedynczej serwerowni w oparciu o RAC ORACLE – wersja bazy danych 12.1.

Rozwiązanie powinno zapewnić:

1. W przypadku awarii jednego serwera w serwerowni nie powinna skutkować przerwaniem pracy jednostki,
2. całość rozwiązania powinno być odporne na awarię jednego węzła w klastrze
3. **MIGRACJA OBECNIE UŻYWANEGO ZSI DO NOWEGO ŚRODOWISKA SERWEROWEGO**
4. Przeniesienie środowiska produkcyjnego na nowe serwery może rozpocząć się w piątek od godziny 21:00 i trwać do poniedziałku do godziny 6:00. Dokładny termin przeniesienia powinien być ustalony wspólnie z Zamawiającym nie później niż 7 dni przed terminem, chyba że obie strony zgodzą się na inne terminy.
5. Migracja nie może wymuszać reinstalacji aplikacji (Kamsoft) na stacjach roboczych, dopuszczalna jest tylko rekonfiguracja aplikacji w zakresie połączenia do bazy danych, lub w związku ze zmianą wersji bazy danych (w tym dopuszczalna zmiana wersji klienta bazy danych na zgodnego z nową wersją bazy danych).
6. Wykonawca musi uwzględnić, że wszystkie prace wykonywane będą w użytkowanych obiektach przy dużym ruchu pracowników i pacjentów, tzn. organizacja prac powinna przede wszystkim zapewniać bezpieczeństwo przebywających w obiektach pracowników i pacjentów.
7. Proces migracji bazy Oracle systemów KAMSOFT oraz przeniesienia usługi ZSI-REP.
8. Zamawiający zapewni fizyczny/zdalny dostęp do dostarczonych serwerów w celu ich instalacji w sieci komputerowej Zamawiającego w celu realizacji zadania pkt 2 poniżej
9. Wykonawca dokona instalacji systemu operacyjnego i oprogramowania bazodanowego w celu wykonania migracji środowiska bazodanowego Oracle.
10. Wykonawca przygotuje odpowiednie instancje bazy danych Oracle na nowym serwerach.
11. Wykonawca dokona instalacji klastra wysokiej dostępności w ramach pojedynczej serwerowni w oparciu o RAC ORACLE
12. Zamawiający udostępni Wykonawcy dostęp do bazy produkcyjnej wraz z odpowiednimi hasłami dla danego schematu w bazie Oracle, najświeższą kopię bazy w postaci pliku „dmp” zawierającym całą bazę z wszystkimi schematami, tabelami zawartych w bazie Oracle lub kopię w postaci RMANowej. Strony ustalą sposób przekazania kopii bazy danych.
13. Wykonawca po przygotowaniu wcześniej środowiska bazodanowego wykona testową migrację, która wskaże szacunkowy czas całego procesu migracji bazy danych i pozwoli na wykrycie możliwych lecz niekoniecznych błędów, tak aby przed docelową migracją wyeliminować możliwe problemy i zminimalizować czas braku dostępu do aplikacji firmy KAMSOFT.
14. Po wykonaniu testowej migracji danych do nowego środowiska bazodanowego, Wykonawca wspólnie z Zamawiającym sprawdzi poprawność danych poprzez podłączenie minium jednej z „końcówek” do nowego środowiska serwerowego.
15. Po weryfikacji danych w aplikacjach KAMSOFT z odtworzonej testowej migracji, testowa baza zostanie usunięta i przygotowana czysta instancja bazy pod docelową migrację.
16. Po wykonaniu powyższych prac Strony ustalą wspólnie termin migracji docelowej do środowiska produkcyjnego Oracle.
17. W dniu migracji docelowej przed samą migracją zostaną poczynione następujące kroki:

* Zamawiający udostępni obecne środowisko bazodanowe w celu wykonania przez Wykonawcę zrzutu całej bazy do pliku dmp lub za pośrednictwem wbudowanego narzędzia do wykonywania kopii bazy danych tj. RMAN.
* Zostanie zatrzymane środowisko produkcyjne przez Wykonawcę tak, aby migrowana baza nie straciła spójności danych.
* Plik dmp lub RMAN zostanie przeniesiony prze Wykonawcę do nowego serwera bazodanowego i zostanie przez Wykonawcę z niego odtworzona baza danych w identyczny sposób jak miało to miejsce podczas testowego odtworzenia.

1. Zostaną zamienione przez Wykonawcę adresy IP starego i nowego środowiska bazodanowego Wykonawca dokona przeniesienia usługi
2. Wykonawca przeniesie usług systemu medycznego działające na serwerze z systemem Windows Serwer 2008r2 na inne serwery z systemem Windows Serwer 2019 wskazane przez Zamawiającego. W tym celu zamawiający udostępni zdalny dostęp - RDP do tych serwerów.

Wykaz usług do przeniesienia:

* + KSZSI-REP wraz z zasobami plikowymi dokumentów medycznych
  + Kamsoft\_HL7
  + KSPLDemon
  + KSPLIsoz (BlueHealth, Disposition, Notification, Osoz, Realisation)
  + KSWatchDog

1. Migracja usługi KS-ZSI REP z serwera wirtualnego na serwer fizyczny:
   * Przetestowanie działania usługi ZSIREP uruchomionej obecnie na serwerze wirtualnym Zamawiającego.
   * Instalacja na serwerze fizycznym usługi ZSIREP dostarczonym przez Zamawiającego. Zamawiający zapewni urządzenie o konfiguracji nie mniejszej niż Windows 10, RAM min. 8 GB
   * Migracja danych z serwera wirtualnego do serwera fizycznego,
   * Testowanie działania usługi ZSIREP po migracji.
2. Wdrożenie i uruchomienie usług indeksowania zdarzeń medycznych wraz z repozytorium udostępnianej dokumentacji medycznej w chmurze obliczeniowej z aplikacji medycznych Zamawiającego KS-Somed i KS-Medis.
   * Dostawa pakietu testowego EDM SUITE
     1. KS-EDMSUITE (c) – PAKIET ARCHIWALNY – na 12 miesięcy w jednym centrum danych (1 Data Center)
     2. KS-EDMSUITE (c) – PAKIET PODSTAWOWY - w jednym centrum danych (1 Data Center), pozwalający na zarejestrowanie w chmurze obliczeniowej - 10 tysięcy dokumentów, ale nie więcej niż 1,5GB dokumentów
   * Konfiguracja KS- EDM SUITE z poziomu aplikacji medycznych Zamawiającego KS-Somed i KS-Medis,
   * Testy zarejestrowania, modyfikacji, przeglądania testowych zdarzeń medycznych z poziomu aplikacji medycznych Zamawiającego KS-Somed i KS-Medis,
3. Na wskazanym przez Zamawiającego serwerze fizycznym z systemem operacyjnym Windows Serwer 2019, Wykonawca przygotuje środowisko służące do aktualizacji aplikacji medycznych KS-Somed i KS-Medis, które są elementami Zintegrowanego Systemu Informatycznego Zamawiającego.
4. Na wskazanym przez Zamawiającego serwerze wirtualnym Wykonawca przygotuje środowisko testowe wymienionych w p. 15 aplikacji, służące do sprawdzenia poprawności działania wykonanych aktualizacji.

Wykonawca przygotuje dokumentację powdrożeniową (zmigrowanego środowiska Oracle,) zawierającą informacje niezbędne do utrzymania poprawnej kondycji bazy danych jak i zalecenia dla administratorów po stronie Zamawiającego. Dokumentacja będzie zawierać również instrukcję odtworzenia środowiska bazodanowego z wykonywanej kopii bazy danych przy pomocy wbudowanego narzędzia RMAN.

1. **Testy akceptacyjne**

Wykonanie testów poprawnego działania wszystkich aplikacji ZSI - Wykonanie testów poprawnego działania wszystkich aplikacji na nowych serwerach - następujących produktów: KS-SOMED, KS-MEDIS, KS-ZZL, KS-FKW, KS-ESM, KS-ASW zgodnie z opisem poniżej.

**TESTY POPRAWNEGO DZIAŁANIA ZINTEGROWANEGO SYSTEMU INFORMATYCZNEGO w NOWYM ŚRODOWISKU SERWEROWYM**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Moduł/zakres** | **Lp.** | **Funkcja** | **Opis testu** | **Potwierdzić słowem TAK spełnienie** |
| **Obsługa systemu zarządzania zasobami ludzkimi KS-ZZL** | 1 | Przypisanie pracownika do struktury. | Przypisać pracownika do elementu struktury.  Zweryfikować poprawność zaktualizowanych danych.  Odpiąć w/w pracownika od elementu struktury.  Zweryfikować poprawność zaktualizowanych danych. |  |
| 2 | Dodanie urlopu dla istniejącego pracownika | Dodać absencje urlopową.  Zweryfikować poprawność działania funkcji dodawania absencji, zweryfikować poprawność funkcji rozliczenie urlopów. |  |
| 3 | Usunięcie urlopu | Usunąć wprowadzoną w poprzednim kroku absencję. Zweryfikować poprawność usunięcia danych. |  |
| 4 | Przeliczenie staży | Wywołać funkcję serwisową Przeliczanie staży.  Zweryfikować poprawność wyliczenia stażu dla wybranego pracownika. |  |
| 5 | Generowanie składników | Wywołać funkcję Generowanie składników.  Zweryfikować czy odpowiednie składniki związane z obecnościami pojawiły się na listach wynagrodzeń. |  |
| 6 | Dodanie składnika wynagrodzenia | Dodać ręcznie składnik wynagrodzenia pracownikowi i wywołać obliczanie wynagrodzeń.  Zweryfikować poprawność danych. |  |
| 7 | Otworzenie okresu rozliczeniowego | Dodać nowy okres rozliczeniowy.  Zweryfikować poprawność poprzez sprawdzenie przepisania list płac do nowego okresu. |  |
| 8 | Weryfikacja poprawności kontroli uprawnień | Dla operatora testowego dodać rolę do grafików dla wybranego elementu struktury.  Zweryfikować poprawność działania funkcji w zakresie posiadania przez operatora testowego wybranych uprawnień. |  |
| 9 | Wydruk definiowanych dokumentów | Wygenerować wydruk dowolnego definiowalnego dokumentu.  Zweryfikować poprawność wygenerowanych danych. |  |
| 10 | Wygenerowanie zestawienia listy płac | Wygenerować Zbiorczą listę płac (np. Definiowane listy XML)  Zweryfikować poprawność wygenerowanych danych. |  |
| **Integracja systemu zarządzania zasobami ludzkimi KS-ZZL z systemami medycznymi KS-SOMED** | 1 | Dodanie nowego pracownika testowego | Wprowadzić dane personalne pracownika (najlepiej lekarza) wraz z prawem wykonywania zawodu.  Zweryfikować czy dane zostały poprawnie zapisane.  Zweryfikować czy dane zostały przeniesione do systemów medycznych. |  |
| 2 | Edycja danych nowego pracownika testowego | Zmienić dane pracownika testowego – np. zmiana nazwiska.  Zweryfikować poprawność zaktualizowania danych pracownika w systemach medycznych. |  |
| 3 | Usunięcie testowego pracownika | Usunąć Kartę pracownika testowego w KS-ZZL.  Zweryfikować czy dane zostały poprawnie zmodyfikowane w systemach medycznych. |  |
| **Integracja systemu zarządzania zasobami ludzkimi KS-ZZL z systemem finansowo-księgowym KS-FKW** | 1 | Księgowanie wynagrodzeń | Po przeliczeniu listy stworzyć i zamknąć dokument księgowy.  W KS-FKW pobrać dokument, zweryfikować księgowanie.  Zwolnić dokument w KS-FKW, usunąć dokument w ZZL, otworzyć listę.  Zweryfikować czy wszystkie operacje wykonują się poprawnie. |  |
| **Obsługa finansowo-księgowa w systemie KS-FKW** | 1 | Ręczne wprowadzanie dokumentów księgowych | Wprowadzić testowy dokument zakupu kosztów, sprawdzić możliwość przypisania formuł i działanie automatu dekretacji. |  |
| 2 | Pobieranie dokumentów z systemu KS-SOMED | Pobrać dokumenty z wybranego dnia, zweryfikować dekretację, usunąć testowo pobrane dokumenty z systemu KS-FKW, usunąć blokowanie usuniętych dokumentów, sprawdzić zmianę stanu po stronie systemu źródłowego |  |
| 3 | Pobieranie dokumentów z systemu KS-ESM | Pobrać dokumenty odpisu z wybranego okresu, zweryfikować dekretację, usunąć testowo pobrane dokumenty z systemu KS-FKW, usunąć blokowanie usuniętych dokumentów, sprawdzić zmianę stanu po stronie systemu źródłowego |  |
| **System obsługi przychodni KS-SOMED** | 1 | Rejestracja wizyt pacjenta z założeniem deklaracji | Zarejestrować pacjenta na wizytę   * zlecenie zewnętrzne (umowa komercyjna oraz NFZ) * zlecenie wewnętrzne (umowa NFZ) * zlecenie prywatne   Uzupełnienie danych o kolejce oczekujących.  Dodanie deklaracji dla pacjenta POZ:   * deklaracja lekarza * deklaracja pielęgniarki * deklaracja położnej   Wydruk deklaracji dla pacjenta. |  |
| 2 | Poprawa danych wizyty zarezerwowanej | Poprawić dane zlecenia - zmiana pacjenta, kierunku i kierującego, dodanie informacji o skierowaniu, rezygnacja z badania, pobieranie informacji o ostatnim skierowaniu pacjenta. |  |
| 3 | Sprawdzenie uprawnień do świadczeń | Sprawdzenie uprawnień ewuś dla wybranego pacjenta.  Sprawdzenie uprawnień ewuś dla pacjentów posiadających rezerwację na wybrany dzień.  Sprawdzenie automatyczne uprawnień ewuś przed rozpoczęciem pracy przychodni.  Sprawdzenie podpięcia umowy komercyjnej dla wizyt zarezerwowanych. |  |
| 4 | Dodanie nowego pacjenta do bazy danych | Założenie karty pacjenta z danymi:   * Numer Pesel * Nazwisko oraz imię * Płeć * Data urodzenia * Pełny adres zamieszkania * Przypisanie firmy/zakładu pracy |  |
| 5 | Wyszukanie terminu wizyty | Wyszukanie terminu wizyty z podaniem co najmniej kryteriów:   * lekarz/gabinet wykonujący * typ godzin pracy * data od orz data do   Przejście do umówienia wizyty po wyszukaniu terminu. |  |
| 6 | Ustawienie grafiku pracy | Ustawienie grafiku pracy lekarza lub gabinetu z uwzględnieniem elementów:   * godziny pracy zależne od poradni * godziny pracy powiązane z aparatami * godziny pracy zmienne w obrębie jednego dnia |  |
| 7 | Wykonanie świadczenia w Terminarzu | Wykonanie świadczenia wcześniej zarezerwowanego z podaniem w szczególności:   * Rozpoznanie głównego oraz współistniejącego * Wprowadzenie procedury icd9 * Wybranie świadczenie za pomocą funkcji grupera * Zatwierdzenie karty wykonania usługi |  |
| 8 | Prowadzenie stanowiska kasowego | Pobranie opłaty za badanie komercyjne w tym:   * Wystawienie paragonu fiskalnego * Wystawienie faktury vat dla pacjenta * Wystawienie faktury vat dla firmy * Korekta dokumentu sprzedaży (paragon/faktura) * Przygotowane raportu dobowego |  |
| 9 | Zaplanowanie cyklu zabiegów rehabilitacyjnych | Zaplanowanie cyklu zabiegów dla pacjenta z uwzględnieniem:   * Zaplanowanie nie więcej niż pięciu zabiegów na jeden dzień zabiegowy * Zaplanowanie nie więcej niż 10 dni zabiegowych z jednym cyklu * Zaplanowanie nie więcej niż dwóch różnych cyklów w ramach tego samego skierowania * Wydrukowanie dla pacjenta planu zabiegowego |  |
| 10 | Realizacja badania diagnostyki obrazowej w module RIS | Zaplanowanie, wykonanie o opisanie badania diagnostycznego w tym:   * Zaplanowanie badania ze skierowaniem z zewnątrz * Zaplanowanie badania na podstawie elektronicznego skierowanie wewnętrznego * Wysłanie badania na listę roboczą w PACS Synektik * Wykonanie badania diagnostycznego * Opisanie badania z możliwością poprawy i usunięciem opisu * Zatwierdzenie opisu badania * Zweryfikowanie widoczności opisu badana w module Gabinet |  |
|  | 11 | Zrealizowanie wizyty lekarskiej w module Gabinet | Zrealizowanie wcześniej zaplanowanej wizyty lekarskiej z wprowadzeniem elementów takich jak:   * Wywiad główny/informacje o ogólnym stanie zdrowia * Wywiad aktualny * Badanie przedmiotowego * Rozpoznanie główne oraz trzy rozpoznania współistniejące * Elektroniczne Skierowanie do poradnia specjalistycznej * Elektroniczne Skierowanie na badanie RTG * Elektroniczne Skierowanie na badania laboratoryjne * E-Recepta wraz z dawkowaniem na pięć leków w tym jeden lek psychoaktywny wraz z wydrukiem dawkowania dla pacjenta * Zaświadczenie dla pacjenta * Wykonanie świadczenia z uwzględnienie funkcji grupera * Wygenerowanie elektronicznej historii zdrowia i choroby pacjenta z wizyty * Cyfrowe podpisanie i zarchiwizowanie elektronicznej dokumentacji medycznej z wizyty pacjenta |  |
|  | 13 | Przygotowanie zestawienia ze stanu realizacji umowy w ramach NFZ | Przygotowanie i wygenerowanie zestawienia ze stanu realizacji umowy dla umowy AOS za okres pół roku. Czas +generowanie zestawienie porównywalny z czasem generowania tego samego zestawienia z tymi samymi parametrami na obecnym serwerze. |  |
|  | 14 | Przygotowanie raportu statystycznego zawierającego 5000 zestawów świadczeń | Wykonane synchronizacji rejestru świadczeń. Oczekiwana prędkość synchronizacji na poziomie nie mniejszym niż prędkość synchronizacji na obecnej bazie danych. Wygenerowanie i zapianie do pliku raportu statystycznego do umowy rehabilitacyjnej zawierającego 5000 zestawów świadczeń. |  |
| **System Ewidencji Środków Majątkowych****KS-ESM** | 1 | ewidencja składników majątku | wprowadzanie nowych składników majątku do użytkowania |  |
| likwidacja składników majątku |  |
| zmiany osób odpowiedzialnych i miejsc użytkowania |  |
| sporządzanie dokumentów inwentaryzacyjnych |  |
| 2 | amortyzacja | sporządzanie dokumentów amortyzacyjnych (naliczanie amortyzacji) |  |
| przekazywanie naliczonej amortyzacji do programu FK (integracja między programami) |  |
| **System obsługi Gospodarki Magazynowej KS-ASW** | 1 | zamówienia | Przygotowanie zamówienia  Tworzenie norm magazynowych  Tworzenie listy braków |  |
| 2 | zakupy | Wprowadzanie dokumentów zakupu,  Wprowadzanie dokumentu na podstawie zamówienia,  Wprowadzanie dokumentu zakupu z dysku,  Poprawa zawartości bufora,  Poprawa faktur i dokumenty korygujące, |  |
| 3 | magazyn | Wydruki remanentowe,  Stany magazynowe, |  |
| 4 | wydawania | Tworzenie nowego dokumentu rozchodu  Wydanie towaru |  |
| 5 | zestawienia | Zestawienie przychodów  Zestawienie rozchodów  Rozchód do jednostek |  |
| 6 | kartoteki | Edycja baz: Dostawcy, Towary, Grupy towarów, |  |
| 7 |  | Połączenie systemów ASW i FKW w zakresie przekazywania danych |  |
| **System obsługi oddziałów Szpitalnych KS-MEDIS** | 1 | Założenie kartoteki pacjenta | Założenie karty pacjenta z danymi:   * Numer Pesel * Nazwisko oraz imię * Płeć * Data urodzenia * Pełny adres zamieszkania * Oddział NFZ |  |
| 2 | Wpis pacjenta do harmonogramu przyjęć | Wpis pacjenta do harmonogramu przyjęć:   * Wyszukanie pacjenta na liście * Kategoria świadczeniobiorcy * Data planowego przyjęcia * Oddział kolejki * Kod kolejki * Dane skierowania * Kategoria medyczna |  |
| 3 | Przyjęcie pacjenta na oddział | Przyjęcie pacjenta na oddział przez moduł Izba Przyjęć:   * Data i godzina przyjęcia * Wybór wpisu z harmonogramu przyjęć * Rozpoznanie wstępne * Lekarz podający rozpoznanie |  |
| 4 | Uzupełnienie danych medycznych po przyjęciu na oddział | Uzupełnienie danych medycznych po przyjęciu na oddział:   * Rozpoznanie zasadnicze * Rozpoznania współistniejące * Pomiary z przyjęcia * Informacje o odleżynach * Kategoria opieki pielęgniarskiej * Potwierdzenie przyjęcia do szpitala |  |
| 5 | Uzupełnienie dokumentacji medycznej | Wypełnienie dokumentacji medycznej na oddziale:   * Wywiad i badanie przedmiotowe z przyjęcia * Obserwacja lekarska * Konsultacja * Skala Norton * Karta obserwacji – indywidualna karta pielęgnowania * Dołączenie pliku pacjenta – skanu |  |
| 6 | Wpisanie procedur i świadczeń | Wpisanie procedur i świadczeń: na oddziale:   * Procedura ICD9 – przykładowa * Świadczenie - ręcznie, weryfikacja prawidłowego podpięcia umowy |  |
| 7 | Wypisanie pacjenta z oddziału | Wpis z oddziału:   * Tryb wypisu * Lekarz wypisujący * Data i godzina wypisu * Przepisanie rozpoznań do Księgi Głównej |  |
| 8 | Wygenerowanie karty informacyjnej | Wygenerowanie karty informacyjnej EDM:   * Epikryza * Zalecenia * Wygenerowanie podglądu dokumentu |  |
| 10 | Zatwierdzenie hospitalizacji | Zatwierdzenie hospitalizacji:   * Wyświetlenie hospitalizacji w Księdze Głównej w module Izba Przyjęć * Zatwierdzenie wybranych hospitalizacji * Poprawa ewentualnych błędów uniemożliwiających zatwierdzenie |  |
| **Integracja KS-SOMED z LIS Marcel** | 1 | Test integracji | * Zaplanowanie badania na podstawie elektronicznego skierowanie wewnętrznego * Wysłanie badania do systemu Marcel * Odbiór wyniku badania w module Gabinet * Dołączenie wyniku badania do wizyty Pacjenta w module Gabinet aplikacji KS-Somed i KS-Medis. |  |
| **Poprawność działania usługi HL7. Integracja systemów KS-SOMED, KS-Medis, ArPACS, Elmiko.** | 1 | Test integracji | * Obsługa Worklisty, * Zaplanowanie zlecenia medycznego, * Wysłanie zlecenia do wskazanego systemu. * Odebranie informacji o wykonaniu zlecenia. * Odbiór wyniku zlecenia w module Gabinet * Dołączenie wyniku zlecenia do wizyty Pacjenta w module Gabinet. * Test wyświetlenia obrazu diagnostycznego z modułu Gabinet w przypadku zlecenia dotyczącego diagnostyki obrazowej. |  |

**Zadanie nr 2**

Firewall UTM - 2 szt.  
Producent: …........................................................................................   
Model:...................................................................................................

|  |  |  |  |
| --- | --- | --- | --- |
| **Lp** | **Parametr lub warunek** | **Opis parametrów technicznych / Minimalne w tym graniczne** | **PARAMETR OFEROWANY**  **(podać zakresy i opisać)** |
| 1 | Parametry sprzętowe | * Urządzenie ma być wyposażone w dysk SSD o pojemności co najmniej 120 GB. * Liczba portów Ethernet 10/100/1000Mbps – min. 8. * Urządzenie musi pozwalać na podłączenie minimum jednej karty rozszerzeń z 8 miedzianymi interfejsami Ethernet 10/100/1000Mbps lub 4 miedzianymi interfejsami Ethernet 10Gbps lub 8 światłowodowymi interfejsami 1Gbps lub 4 światłowodowymi interfejsami 10Gbps. Ew. karty rozszerzeń nie są częścią postępowania przetargowego. * Urządzenie musi posiadać funkcjonalność budowania połączeń z Internetem za pomocą modemu 3G pochodzącego od dowolnego producenta. * Przepustowość Firewall – min. 30 Gbps. * Przepustowość Firewall wraz z włączonym systemem IPS – min. 15 Gbps. * Przepustowość filtrowania Antywirusowego – min. 2,9 Gbps. * Minimalna przepustowość tunelu VPN przy szyfrowaniu AES wynosi min. 4,5 Gbps. * Maksymalna liczba tuneli VPN IPSec nie może być mniejsza niż. 1000. * Maksymalna liczba tuneli typu Full SSL VPN nie może być mniejsza niż 150. * Obsługa min. VLAN 512. * Liczba równoczesnych sesji - min. 1 500 000 i nie mniej niż 80 000 nowych sesji/sekundę. * **Rozwiązanie musi być dostarczone jako klaster HA dwóch urządzeń działających co najmniej w trybie Active/Passive.** * Urządzenie jest nielimitowane na użytkowników. |  |
| 2 | Obsługa sieci | * Urządzenie ma posiadać wsparcie dla protokołu IPv4 oraz IPv6 co najmniej na poziomie konfiguracji adresów dla interfejsów, routingu, firewall, systemu IPS oraz usług sieciowych takich jak np. DHCP. |  |
| 3 | Zapora korporacyjna (firewall) | * Urządzenie ma być wyposażone w Firewall klasy Stateful Inspection. * Urządzenie ma obsługiwać translacje adresów NAT n:1, NAT 1:1 oraz PAT. * Urządzenie ma dawać możliwość ustawienia trybu pracy jako router warstwy trzeciej, jako bridge warstwy drugiej oraz hybrydowo (częściowo jako router, a częściowo jako bridge). * Interface (GUI) do konfiguracji firewall ma umożliwiać tworzenie odpowiednich reguł przy użyciu prekonfigurowanych obiektów. Przy zastosowaniu takiej technologii osoba administrująca ma mieć możliwość określania parametrów pojedynczej reguły (adres źródłowy, adres docelowy etc.) przy wykorzystaniu obiektów określających ich logiczne przeznaczenie. * Administrator musi mieć możliwość budowania reguł firewall na podstawie: interfejsów wejściowych i wyjściowych ruchu, źródłowego adresu IP, docelowego adresu IP, geolokacji hosta źródłowego bądź docelowego, reputacji hosta, użytkownika bądź grupy bazy LDAP, pola DSCP nagłówka pakietu, godziny oraz dnia nawiązywania połączenia. * Rozwiązanie musi umożliwiać między innymi filtrowanie jedynie na poziomie warstwy 2 modelu OSI tj. na podstawie adresów mac. * Administrator musi mieć możliwość zdefiniowania minimum 10 różnych, niezależnie konfigurowalnych, zestawów reguł firewall. * Edytor reguł firewall ma posiadać wbudowany analizator reguł, który eliminuje sprzeczności w konfiguracji reguł lub wskazuje na użycie nieistniejących elementów (obiektów). * Firewall ma umożliwiać uwierzytelnienie i autoryzację użytkowników w oparciu o bazę lokalną, zewnętrzny serwer RADIUS, LDAP (wewnętrzny i zewnętrzny) lub przy współpracy z uwierzytelnieniem Windows 2k (Kerberos). |  |
| 4 | Intrusion prevention system (ips) | * System detekcji i prewencji włamań (IPS) ma być zaimplementowany w jądrze systemu i ma wykrywać włamania oraz anomalia w ruchu sieciowym przy pomocy analizy protokołów, analizy heurystycznej oraz analizy w oparciu o sygnatury kontekstowe. * Moduł IPS musi być opracowany przez producenta urządzenia. Nie dopuszcza się, aby moduł IPS pochodził od zewnętrznego dostawcy. * Moduł IPS musi zabezpieczać przed co najmniej 10 000 ataków i zagrożeń. * Administrator musi mieć możliwość tworzenia własnych sygnatur dla systemu IPS. * Moduł IPS ma nie tylko wykrywać, ale również usuwać szkodliwą zawartość w kodzie HTML oraz JavaScript żądanej przez użytkownika strony internetowej. * Urządzenie umożliwia inspekcję ruchu tunelowanego wewnątrz protokołu SSL, co najmniej w zakresie analizy HTTPS, FTPS, POP3S oraz SMTPS. * Administrator urządzenia ma mieć możliwość konfiguracji jednego z trybów pracy urządzenia, to jest: IPS, IDS lub Firewall dla wybranych adresów IP (źródłowych i docelowych), użytkowników, portów (źródłowych i docelowych) oraz na podstawie pola DSCP. * Urządzenie ma mieć możliwość ochrony między innymi przed atakami typu SQL injection, Cross Site Scripting (XSS) oraz złośliwym kodem Web2.0. |  |
| 5 | Kształtowanie pasma (traffic shapping) | * Urządzenie ma mieć możliwość kształtowania pasma w oparciu o priorytetyzację ruchu oraz minimalną i maksymalną wartość pasma. * Ograniczenie pasma lub priorytetyzacja ma być określana względem reguły na firewallu w odniesieniu do pojedynczego połączenia, adresu IP lub autoryzowanego użytkownika oraz pola DSCP. * Rozwiązanie ma umożliwiać tworzenie tzw. kolejki nie mającej wpływu na kształtowanie pasma a jedynie na śledzenie konkretnego typu ruchu (monitoring). * Urządzenie ma umożliwiać kształtowanie pasma na podstawie aplikacji generującej ruch. |  |
| 6 | Ochrona antywirusowa | * Rozwiązanie zezwala na zastosowanie jednego z co najmniej dwóch skanerów antywirusowych dostarczonych przez firmy trzecie (innych niż producent rozwiązania). * Co najmniej jeden z dwóch skanerów antywirusowych jest dostarczany w ramach podstawowej licencji. * Administrator ma mieć możliwość określenia maksymalnej wielkości pliku jaki będzie poddawany analizie skanerem antywirusowym. * Administrator ma mieć możliwość zdefiniowania treści komunikatu dla użytkownika o wykryciu infekcji, osobno dla infekcji wykrytych wewnątrz protokołu POP3, SMTP i FTP. W przypadku SMTP i FTP ponadto ma być możliwość zdefiniowania 3-cyfrowego kodu odrzucenia |  |
| 7 | Ochrona antyspam | * Producent udostępnia mechanizm klasyfikacji poczty elektronicznej określający czy jest pocztą niechcianą (SPAM). * Ochrona antyspam ma działać w oparciu o: * białe/czarne listy, * DNS RBL, * heurystyczny skaner. * W przypadku ochrony w oparciu o DNS RBL administrator może modyfikować listę serwerów RBL lub skorzystać z domyślnie wprowadzonych przez producenta serwerów. Może także definiować dowolną ilość wykorzystywanych serwerów RBL. * Wpis w nagłówku wiadomości zaklasyfikowanej jako spam ma być w formacie zgodnym z formatem programu Spamassassin. |  |
| 8 | Wirtualne sieci prywante (vpn) | * Urządzenie ma posiadać wbudowany serwer VPN umożliwiający budowanie połączeń VPN typu client-to-site (klient mobilny – lokalizacja) lub site-to-site (lokalizacja-lokalizacja). * Odpowiednio kanały VPN można budować w oparciu o:  1. PPTP VPN, 2. IPSec VPN, 3. SSL VPN.  * SSL VPN musi działać w trybach Tunel i Portal. * W ramach funkcji SSL VPN producenci powinien dostarczać klienta VPN współpracującego z oferowanym rozwiązaniem. * Urządzenie ma posiadać funkcjonalność przełączenia tunelu na łącze zapasowe na wypadek awarii łącza dostawcy podstawowego (VPN Failover). * Urządzenie ma posiadać wsparcie dla technologii XAuth, Hub ‘n’ Spoke oraz modconf. * Urządzenie ma umożliwiać tworzenie tuneli w oparciu o technologię Route Based. |  |
| 9 | Filtr dostępu do stron www | * Urządzenie ma posiadać wbudowany filtr URL. * Filtr URL ma działać w oparciu o klasyfikację URL zawierającą co najmniej 50 kategorii tematycznych stron internetowych. * Administrator musi mieć możliwość dodawania własnych kategorii URL. * Urządzenie nie jest limitowane pod względem kategorii URL dodawanych przez administratora. * Moduł filtra URL, wspierany przez HTTP PROXY, musi być zgodny z protokołem ICAP co najmniej w trybie REQUEST. * Administrator posiada możliwość zdefiniowania akcji w przypadku zaklasyfikowania danej strony do konkretnej kategorii. Do wyboru jest jedna z trzech akcji:  1. blokowanie dostępu do adresu URL, 2. zezwolenie na dostęp do adresu URL, 3. blokowanie dostępu do adresu URL oraz wyświetlenie strony HTML zdefiniowanej przez administratora.  * Administrator musi mieć możliwość zdefiniowania co najmniej 4 różnych stron z komunikatem o zablokowaniu strony. * Strona blokady powinna umożliwiać wykorzystanie zmiennych środowiskowych. * Filtrowanie URL musi uwzględniać także komunikację po protokole HTTPS. * Urządzenie musi pozwalać na identyfikację i blokowanie przesyłanych danych z wykorzystaniem typu MIME. * Urządzenie posiada możliwość stworzenia białej listy stron dostępnych poprzez HTTPS, które nie będą deszyfrowane. |  |
| 10 | Uwierzytelnianie | * Urządzenie ma zezwalać na uruchomienie systemu uwierzytelniania użytkowników w oparciu o:  1. lokalną bazę użytkowników (wewnętrzny LDAP), 2. zewnętrzną bazę użytkowników (zewnętrzny LDAP), 3. usługę katalogową Microsoft Active Directory.  * Rozwiązanie musi pozwalać na równoczesne użycie co najmniej 5 różnych baz LDAP. * Rozwiązanie ma zezwalać na uruchomienie specjalnego portalu, który umożliwia autoryzacje w oparciu o protokoły:  1. SSL, 2. Radius, 3. Kerberos.  * Urządzenie ma posiadać co najmniej dwa mechanizmy transparentnej autoryzacji użytkowników w usłudze katalogowej Microsoft Active Directory. * Co najmniej jedna z metod transparentnej autoryzacji nie wymaga instalacji dedykowanego agenta. * Autoryzacja użytkowników z Microsoft Active Directory nie wymaga modyfikacji schematu domeny. |  |
| 11 | Administracja łączami do internetu (isp) | * Urządzenie ma posiadać wsparcie dla mechanizmów równoważenia obciążenia łączy do sieci Internet (tzw. Load Balancing). * Mechanizm równoważenia obciążenia łącza internetowego ma działać w oparciu o następujące dwa mechanizmy:  1. równoważenie względem adresu źródłowego, 2. równoważenie względem połączenia.  * Mechanizm równoważenia łącza musi uwzględniać wagi przypisywane osobno dla każdego z łączy do Internetu. * Urządzenie ma posiadać mechanizm przełączenia na łącze zapasowe w przypadku awarii łącza podstawowego. * Urządzenie ma posiadać mechanizm statycznego trasowania pakietów. * Urządzenie musi posiadać możliwość trasowania połączeń dla IPv6 co najmniej w zakresie trasowania statycznego oraz mechanizmu przełączenia na łącze zapasowe w przypadku awarii łącza podstawowego. * Urządzenie musi posiadać możliwość trasowania połączeń względem reguły na firewallu w odniesieniu do pojedynczego połączenia, adresu IP lub autoryzowanego użytkownika oraz pola DSCP. * Rozwiązanie powinno zapewniać obsługę routingu dynamicznego w oparciu co najmniej o protokoły: RIPv2, OSPF oraz BGP. * Rozwiązanie powinno wspierać technologię Link Aggregation. |  |
| 12 | Pozostałe usługi i funkcje rozwiązania | * Urządzenie musi posiadać wbudowany serwer DHCP z możliwością przypisywania adresu IP do adresu MAC karty sieciowej stacji roboczej w sieci. * Urządzenie musi pozwalać na przesyłanie zapytań DHCP do zewnętrznego serwera DHCP – DHCP Relay. * Konfiguracja serwera DHCP musi być niezależna dla protokołu IPv4 i IPv6. * Urządzenie musi posiadać możliwość tworzenia różnych konfiguracji dla różnych podsieci. Z możliwością określenia różnych bram, a także serwerów DNS. * Urządzenie musi być wyposażone w klienta usługi SNMP w wersji 1,2 i 3. * Urządzenie musi posiadać usługę DNS Proxy. * Urządzenie musi posiadać wsparcie dla Spanning-tree protocol (RSTP/MSTP). |  |
| 13 | Administracja urządzeniem | * Konfiguracja urządzenia ma być możliwa z wykorzystaniem polskiego interfejsu graficznego. * Interfejs konfiguracyjny musi być dostępny poprzez przeglądarkę internetową a komunikacja musi być zabezpieczona za pomocą protokołu https. * Komunikacja może odbywać się na porcie innym niż https (443 TCP). * Urządzenie ma być zarządzane przez dowolną liczbę administratorów z różnymi (także nakładającymi się) uprawnieniami. * Rozwiązanie musi mieć możliwość zarządzania poprzez dedykowaną platformę centralnego zarządzania. Komunikacja pomiędzy urządzeniem a platformą centralnej administracji musi być szyfrowana. * Interfejs konfiguracyjny platformy centralnego zarządzania musi być dostępny poprzez przeglądarkę internetową a komunikacja musi być zabezpieczona za pomocą protokołu https. * Urządzenie ma mieć możliwość eksportowania logów na zewnętrzny serwer (syslog). Wysyłanie logów powinno być możliwe za pomocą transmisji szyfrowanej (TLS). * Rozwiązanie ma mieć możliwość eksportowania logów za pomocą protokołu IPFIX. * Urządzenie musi pozwalać na automatyczne wykonywanie kopii zapasowej ustawień (backup konfiguracji) do chmury producenta lub na dedykowany serwer zarządzany przez administratora. * Urządzenie musi pozwalać na odtworzenie backupu konfiguracji bezpośrednio z serwerów chmury producenta lub z dedykowanego serwera zarządzanego przez administratora. * Urządzenie musi posiadać funkcjonalność anonimizacji logów. |  |
| 14 | Raportowanie | * Urządzenie musi posiadać wbudowany w interfejs administracyjny system raportowania i przeglądania logów zebranych na urządzeniu. * System raportowania i przeglądania logów wbudowany w system nie może wymagać dodatkowej licencji do swojego działania. * System raportowania musi posiadać predefiniowane raporty dla co najmniej ruchu WEB, modułu IPS, skanera Antywirusowego i Antyspamowego. * System raportujący musi umożliwiać wygenerowanie co najmniej 25 różnych raportów. * System raportujący ma dawać możliwość edycji konfiguracji z poziomu raportu. * W ramach podstawowej licencji zamawiający powinien otrzymać możliwość korzystania z dedykowanego systemu zbierania logów i tworzenia raportów w postaci wirtualnej maszyny. * Dodatkowy system umożliwia tworzenie interaktywnych raportów w zakresie działania co najmniej następujących modułów: IPS, URL Filtering, skaner antywirusowy, skaner antyspamowy. |  |
| 15 | Pozostałe | * Wymaga się, aby dostawa obejmowała również minimum 60-miesięczną gwarancję producentów na dostarczone elementy systemu oraz aktualizacje dla wszystkich funkcji bezpieczeństwa |  |

1 Wykonawca wykona konfigurację dostarczonych UTM-ów i dokona przeniesienia reguł  i konfiguracji z obecnie używanego UTM. W tym celu Zamawiający udostępni Wykonawcy dostęp do tego urządzenia.

2 Wykonawca we współpracy z zamawiającym wykona fizyczne przełączenie instalacji sieciowej Zamawiającego do wcześniej skonfigurowanych nowych urządzeń. Prace te będą wykonywane w sobotę lub niedzielę poza godzinami pracy Zamawiającego.

Dokładny termin przełączenia powinien być ustalony wspólnie z Zamawiającym nie później niż 7 dni przed terminem, chyba że obie strony zgodzą się na inne terminy.