**Załącznik nr 1.1**

OPIS PRZEDMIOTU ZAMÓWIENIA

**Część 1**

1. **Serwer – 2 sztuki.**

|  |  |
| --- | --- |
| **Nazwa elementu, parametru lub cechy** | **Opis wymagań Serwerów** |
| **Ilość sztuk** | 2 |
| **Obudowa** | Do instalacji w szafie Rack 19", wysokość 2U, z zestawem szyn do mocowania w szafie i wysuwania do celów serwisowych. |
| **Procesor** | Architektura x86, maksymalny TDP dla procesora – maksymalnie 165W. Wymagana ilość rdzeni dla procesora – 8. Minimalna częstotliwość pracy procesora minimum 3.2GHz. Minimalna ilość kanałów procesora – 8.  Wynik wydajności procesora zainstalowanego w oferowanym serwerze nie powinien być niższy niż 178 punktów base w teście SPECrate 2017 Integer, opublikowanym przez SPEC.org (www.spec.org) dla konfiguracji dwuprocesorowej. Test przeprowadzony przez producenta serwera musi być zamieszczony na stronie spec.org. Obsługa minimum dwóch procesorów. |
| **Liczba procesorów** | 1 |
| **Płyta główna** | Płyta główna dedykowana do pracy w serwerach, wyprodukowana przez producenta serwera z możliwością zainstalowania przynajmniej dwóch procesorów wykonujących 64-bitowe instrukcje |
| **Pamięć operacyjna** | Zainstalowane minimum 256 pamięci RAM DDR5 o częstotliwości 4800MHz. Pamięć zainstalowana w kościach min 32GB.  Minimum 32 sloty na pamięć. Możliwość rozbudowy do 8TB RAM. |
| **Zabezpieczenie pamięci** | Mirroring, ECC, SDDC, ADDDC |
| **Procesor Graficzny** | Zintegrowana karta graficzna z minimum 16MB pamięci osiągająca rozdzielczość 1920x1200 przy 60 Hz.  1 port VGA na tylnym panelu oraz możliwość instalacji portu vga na przednim panelu serwera. |
| **Rozbudowa dysków** | W chwili dostawy każdy serwer musi posiadać zainstalowane minimum 2 dyski SSD o pojemności nie mniejszej niż 960GB, hot swap.  Obudowa ma mieć możliwość instalacji do 24 dysków 2.5. W chwili dostawy nie wymagana jest obecność zatok. |
| **Kontroler dyskowy** | Wymagana obecność w serwerze sprzętowego kontrolera RAID z obsługującego zainstalowane dyski umożłiwiającego stworzenie min. RAID 1. |
| **Zasilacz** | Minimum dwa redundantne zasilacze o mocy minimum 1100W z certyfikatem minimum Titanium. |
| **Interfejsy sieciowe** | Jeden port RJ-45 o przepustowości 1GbE dedykowany dla karty zarządzającej.  Co najmniej 1 karta czteroportowa 1Gbase-T  Zainstalowana jedna dwuportowa karta FC o prędkości przynajmniej 32Gbs wyposażone w dedykowane wkładki sfp. Zainstalowana jedna dwuportowa karta Eth o prędkości 10/25Gbs wyposażone w dedykowane wkładki optyczne 25Gb |
| **Dodatkowe sloty I/O** | W chwili dostawy serwer powinien być wyposażony min w 7 slotów PCIe 4, w tym min cztery x16, bez konieczności dokładania jakichkolwiek dodatkowych komponentów do serwera. |
| **Karty graficzne** | Możliwość przekonfigurowania serwera do jednoczesnej obsługi do 8 sztuk kart GPU pojedynczej szerokości oraz do minimum 3 kart podwójnej szerokości. |
| **Dodatkowe porty** | * z przodu obudowy: 1x USB 3.2, 1x USB 2.0 (możliwość lokalnego zarządzania serwerem przez ten port). * z tyłu obudowy: 3x USB 3.2, 1x VGA . Możliwość instalacji portu DB9. Możliwość instalacji drugiego redundantnego dedykowanego portu zarządzania * wewnątrz obudowy: 1x USB3.2   Wszystkie tylne porty USB, port RJ-45 służący do zarządzania, tylny port VGA, wewnętrzny port USB, wewnętrzny port na kartę Micro SD powinny być umieszczone na osobnej dedykowanej płytce I/O, którą łączy się bezpośrednio z płytą główną serwera. |
| **Chłodzenie** | Wentylatory wspierające wymianę Hot-Swap, zamontowane nadmiarowo minimum N+1 |
| **Zarządzanie** | Niezależny od systemu operacyjnego, posiadający dedykowany port 1Gbs base-T, sprzętowy kontroler zdalnego zarzadzania z możliwością wyposażenia w przynajmniej 4GB pamięci flash na potrzeby przechowywania oraz instalacji firmware komponentów serwera jak i plików konfiguracyjnych. Na potrzeby utrzymaniowe oraz serwisowe, wymaga się, aby kontroler zarządzania nie był integralną częścią płyty głównej serwera lecz był na osobnej płytce I/O wspomnianej w sekcji Dodatkowe Porty W przypadku awarii płyty głównej serwera, wymaga się możliwości instalacji wykorzystywanej Płytki I/O wraz z pamięcią flash (wersje firmware oraz pliki konfiguracyjne) na nowe płycie głównej. Wymaga się możliwości skonfigurowania w serwerze dwóch fizycznych portów 1Gb Base-T dedykowanych tylko na potrzeby zarządzania. Nie dopuszcza się rozwiązania w którym którykolwiek z dwóch portów miałby być portem współdzielonym na karcie LAN.  Wymagane funkcjonalności procesora serwisowego:   * Monitoring stanu systemu (komponenty objęte monitoringiem to przynajmniej: cpu, pamięć RAM, dyski, karty PCI, zasilacze, wentylatory, płyta główna * Pozyskanie następujących informacji o serwerze: nazwa, typ i model, numer seryjny, nazwa systemu, wersja UEFI oraz BMC, adres ip karty zarządzającej, utylizacja cpu, utylizacja pamięci oraz komponentów I/O * Logowanie zdarzeń systemowych oraz związanych z działaniami użytkownika. Każdy dziennik zdarzeń powinien mieć możliwość zapisu co najmniej 1024 rekordów. * Logowanie zdarzeń związanych z utrzymaniem systemu jak upgrade firmware, zmiana/instalacja sprzętu. System powinien umożliwiać zapisanie minimum 250 zdarzeń. * Możliwość zapisywania zdarzeń w formacie HTML oraz JSON * Wysylanie określonych zdarzeń poprzez SMTP oraz SNMPv3 * Update systemowego firmware * Monitoring i możliwość ograniczenia poboru prądu * Zdalne włączanie/wyłączanie/restart * Zapis video zdalnych sesji * Podmontowanie lokalnych mediów * Przekierowanie konsoli szeregowej przez IPMI oraz SSH * Zrzut ekranu w momencie zawieszenia systemu * Możliwość przejęcia zdalnego ekranu * Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera niezależne od zainstalowanego systemu operacyjnego,. * Możliwość zdalnej instalacji systemu operacyjnego * Alerty Syslog * szyfrowane połączenie (TLS min TLS 1.2) oraz autentykacje i autoryzację użytkownika; * możliwość zdefiniowania min 12 użytkowników lokalnych na karcie zarządzającej * Wyświetlanie danych aktualnych oraz historycznych dla użycia energii oraz temperatury serwera * Możliwość mapowania obrazów ISO z lokalnego dysku operatora * Możliwość mapowania obrazów ISO przez HTTPS, SFTP, CIFS oraz NFS * montowanie obrazów ISO musi być możliwe bez instalacji dodatkowych komponentów Java czy AciveX * Możliwość jednoczesnej pracy do 6 użytkowników przez wirtualną konsolę * wspierane protokoły/interfejsy: IPMI v2.0, SNMP v3, CIM, DCMI v1.5, REST API * zgodność z FIPS 140-3 oraz NIST 800-193 * zabezpieczenie przed nieautoryzowaną wymianą komponentów sprzętowych serwera. Wymaga się możliwości ustawienia zablokowania startu systemu na skutek wykrycia takiego zdarzenia. * Możliwość grupowania serwerów w kontekście synchronizacji jednolitej konfiguracji oraz wersji firmware dla całej grupy serwerów * Wymaga się możliwości wykorzystania frontowego portu USB do celów serwisowych (komunikacja portu z karta zarządzającą) bez możliwości uzyskania jakiejkolwiek funkcjonalności na poziomie zainstalowanego systemu operacyjnego. Funkcjonalność ta musi być realizowana na poziomie sprzętowym i musi być niezależna od zainstalowanego systemu operacyjnego.   Wraz z serwerem powinno zostać dostarczone dodatkowe oprogramowanie zarządzające w postaci wirtualnego appliance dla KVM, ESXi i Hyper-V, umożliwiające:  - zarzadzanie infrastruktura serwerów i storage bez udziału dedykowanego agenta - przedstawianie graficznej reprezentacji zarządzanych urządzeń  - obsługę szyfrowanej komunikacji z zarządzanymi urządzeniami, wsparcie dla NIST 800-131A oraz FIPS 140-2  - wsparcie dla certyfikatów SSL tzw self-signed oraz zewnętrznych  - udostępnianie szybkiego podgląd stanu środowiska - udostępnianie podsumowania stanu dla każdego urządzenia - tworzenie alertów przy zmianie stanu urządzenia  - monitorowanie oraz tracking zużycia energii przez monitorowane urządzenie, możliwość ustalania granicy zużycia energii,  - konsola zarzadzania oparta o HTML 5  - dostępność konsoli monitorującej na urządzeniach przenośnych ze wsparciem dla systemu Android oraz iOS, aplikacja musi umożliwiać włączenie wyłączenie oraz restart urządzenia, musi również mieć możliwość aktywowania diody lokacyjnej na urządzeniu,  - automatyczne wykrywanie dołączanych systemów oraz szczegółowa inwentaryzacja  - możliwość aktualizacji wersji oprogramowania dla komponentów zarządzanych serwerów w oparciu o repozytorium lokalne jak i zdalne dostępne na stronie producenta oferowanego rozwiązania  - definiowanie polityk zgodności wersji firmware komponentów zarządzanych urządzań (konkretne wersje firmware)  - Automatyczna polityka aktualizacji „Najnowsze dostępne”  - definiowanie roli użytkowników oprogramowania  - obsługa REST API oraz Windows PowerShell  - obsługa SNMP, SYSLOG, Email Forwarding  - autentykacja użytkowników: centralna (możliwość definiowania wymaganego poziomu skomplikowania danych autentykacyjnych) oraz integracja z MS AD oraz obsługa single sign on oraz SAML  - obsługa tzw Forward Secrecy w komunikacji z zarządzanymi urządzeniami  - przedstawianie historycznych aktywności użytkowników  -blokowanie możliwości podłączenia innego systemu zarzadzania do urządzeń zarządzanych  - tworzenie dziennika zdarzeń ukończonych sukcesem lub bledem,  oraz zdarzeń bedacych w trakcie. Możliwość definiowania filtrów wyświetlanych zdarzeń z dziennika. Możliwość eksportu dziennika zdarzeń do pliku csv  - Obsluga NTP  - przesyłanie alertów do konsoli firm trzecich |
| **Funkcje zabezpieczeń** | Możliwość instalacji czujnika otwarcia obudowy zintegrowanego z modułem zarządzania serwerem, hasło włączania, hasło administratora, moduł RoT (umieszczony na dedykowanej płytce I/O wspomnianej w sekcji Dodatkowe porty) wspierający TPM2.0 |
| **Urządzenia hot swap** | Dyski twarde, zasilacze, wentylatory. |
| **Diagnostyka** | Możliwość przewidywania awarii dla procesorów, regulatorów napięcia, pamięci, dysków wewnętrznych (włącznie z dyskami m.2), wentylatorów, zasilaczy, kontrolerów RAID  Możliwość użycia aplikacji mobilnej na telefonie, do przeglądania awarii, konfiguracji i włączenia/wyłączenia serwera.  Wymaga się aby serwer posiadał diody sygnalizacyjne awarię przy każdej kości pamięci RAM, każdej zatoce dyskowej, każdym zasilaczu. |
| **Systemy operacyjne** | Kompatybilność  Microsoft Windows Server 2019, 2022; Red Hat Enterprise Linux 8.6, 8.7, 9.0, 9.1, SUSE Linux Enterprise Server 12 SP4, 15 Xen SP4; VMware vSphere (ESXi) 7.0 U3, ESXI 8.0; Ubuntu 20.04 LTS, 22.04 LTS |
| **Waga** | maximum: 40kg |
| **Inne** | Serwer musi być wyprodukowany nie wcześniej niż w 2 kwartale 2025 roku i pochodzić z oficjalnego kanału dystrybucji producenta w Polsce. |
| **Gwarancja** | 36 miesięcy pełnego wsparcia producenta on-site w trybie 24x7 z gwarantowanym czasem naprawy 24h i usługą pozostawienia dysków. |

1. **Macierz – 2 sztuki.**

|  |  |  |
| --- | --- | --- |
| L.P. | **Nazwa elementu, parametru lub cechy** | **Szczegółowy opis wymagań** |
| 1 | Obudowa – gęstość upakowania | Macierz musi umożliwiać instalację w standardowej szafie RACK 19”. |
| 2 | Obudowa – gęstość upakowania | Macierz mieć możliwość instalacji kombinacji poniższych nośników dyskowych w ramach jednej obudowy podstawowej (zawierającej kontrolery): - Flash NVMe lub NVMe SSD, gdzie Flash NVMe oznacza dyski autorskie dostawców macierzy wykorzystujące protokół NVMe |
| 3 | Obudowa – gęstość upakowania | Możliwość zainstalowania co najmniej 12 dysków NVMe o rozmiarze 2,5” cala w obudowie o wysokości 1U. |
| 4 | Obudowa – gęstość upakowania | Kontrolery macierzowe muszą komunikować się z nośnikami dyskowymi umieszczonymi w obudowie podstawowej (zawierającej kontrolery) wyłącznie z użyciem protokołu NVMe. |
| 5 | Obudowa – gęstość upakowania | Macierz musi być zbudowana z minimum dwóch kontrolerów pracujących w trybie active-active lub dual-active. |
| 6 | Obudowa – gęstość upakowania | Architektura macierzy ma być oparta o sprawdzone i powszechnie dostępne procesory technologii x86/x64 |
| 7 | Funkcje niezawodnościowe | Wszystkie krytyczne komponenty macierzy takie jak: kontrolery dyskowe, pamięć cache, zasilacze i wentylatory muszą być zdublowane tak, aby awaria pojedynczego elementu nie wpływała na funkcjonowanie całego systemu. Komponenty te muszą być wymienialne w trakcie pracy macierzy. |
| 8 | Funkcje niezawodnościowe | Macierz musi cechować brak pojedynczego punktu awarii. |
| 9 | Funkcje niezawodnościowe | Wsparcie dla zasilania z dwóch niezależnych źródeł prądu poprzez nadmiarowe zasilacze typu Hot-Swap. Wentylatory typu Hot-Swap. |
| 10 | Funkcje niezawodnościowe | Macierz musi być odporna na zaniki napięcia, tzn. chwilowy zanik napięcia nie powinien przerywać pracy macierzy. |
| 11 | Zarządzanie | Macierz musi umożliwiać zarządzanie za pomocą interfejsu Ethernet. Możliwość zarządzania całością dostępnych zasobów dyskowych z jednej konsoli administracyjnej. |
| 12 | Zarządzanie | Funkcjonalność bezpośredniego monitoringu stanu w jakim w danym momencie macierz się znajduje. |
| 13 | Zarządzanie | Urządzenie musi składać się z pojedynczej macierzy dyskowej zarządzanej z jednego wbudowanego w macierz interfejsu GUI (interfejs graficzny), CLI (interfejs tekstowy) oraz zapewniać możliwość tworzenia skryptów użytkownika. Interfejs ten musi być natywnie dostępny na macierzy, bez zastosowania zewnętrznych urządzeń. |
| 14 | Ilość portów | Wymagane jest niemniej niż 4 x FC 32Gb/s per kontroler |
| 15 | Pojemność użytkowa | Całkowita pojemność min. 75 TiB netto (użyteczne przy założeniu konfiguracji odpornej na awarię minimum 2 dysków (typu RAID-6 lub równoważnego) oraz bez uwzględnienia technik redukcji danych takich jak kompresja, deduplikacja czy thin-provisioning) i musi być zbudowana wyłącznie w oparciu o nośniki NVMe Flash lub NVMe SSD. Pojemność musi uwzględniać dysk zapaswy (spare). |
| 16 | Pojemność użytkowa | Macierz musi pozwalać na alokację 99% pojemności użytecznej bez spadku wydajności macierzy (brak zwiększonego czasu odpowiedzi, brak spadku przepustowości macierzy). Wydajność macierzy musi być niezależna od poziomu alokacji przestrzeni macierzy w zakresie od 0% alokacji do wartości wymaganej pojemności użytecznej. Jeżeli oferowane rozwiązanie nie spełnia opisanego wymagania należy dostarczyć conajmniej 20% pojemności użytecznej więcej. |
| 17 | Obsługiwane poziomy RAID | Macierz musi obsługiwać poziomy: RAID1, RAID5 i RAID6 (dystrybuowane) i zapewniać zabezpieczenie przed awarią dwóch dysków jednocześnie w ramach jednej grupy raid. |
| 18 | bezpieczenstwo danych | Dyski/przestrzeń "spare" muszą zostać skonfigurowane/dostarczone w ilości/pojemności zgodnej z udokumentowanymi rekomendacjami producenta oferowanej macierzy. |
| 19 | bezpieczenstwo danych | Macierz musi posiadać wbudowane sprzętowo na nośnikach dyskowych NVMe szyfrowanie AES-256. |
| 20 | bezpieczenstwo danych | Kontrolery macierzowe muszą posiadać możliwość szyfrowania danych, uniemożliwiając odczyt danych z usuniętych z macierzy nośników dyskowych. Ta funkcjonalność nie jest to objęta tym postepowaniem. |
| 21 | Skalowalność rozwiązania | Macierz musi mieć możliwość obsługi min. 200 dysków poprzez dodanie półek rozszerzeń. Macierz musi mieć możliwość rozbudowy poprzez dodanie pojedynczego dysku, dodanie kontrolerów oraz półek dyskowych. |
| 22 | Skalowalność rozwiązania | Niezależnie od zastosowanych nośników danych, macierz musi umożliwiać granularną rozbudowę grupy RAID w zakresie od co najmniej od 1 do 12 nośników dyskowych, proces rozbudowy nie może powodować niedostępności do danych. |
| 23 | Kontrolery macierzy dyskowej | Macierz musi być wyposażona w minimum 2 kontrolery dyskowe z możliwością rozbudowy do 4 kontrolerów. Każdy z kontrolerów musi udostępniać co najmniej 128GB pamięci Cache. |
| 24 | Kontrolery macierzy dyskowej | Macierz musi umożliwiać rozbudowę pamięci cache do 1TB w ramach klastra macierzy składającego się z identycznych kontrolerów i zarządzanego z jednego interfejsu GUI, CLI. Zamawiający nie dopuszcza zastosowania dysków SSD/ SSD NVMe lub kart pamięci/modułów FLASH jako rozszerzenia pamięci cache. |
| 25 | Funkcjonalności | Funkcjonalność partycjonowania pamięci cache. |
| 26 | Funkcjonalności | Funkcjonalność separacji przestrzeni dyskowych pomiędzy różnymi podłączonymi hostami. |
| 27 | Funkcjonalności | Funkcjonalność dynamicznego zwiększania rozmiaru wolumenów. |
| 28 | Funkcjonalności | Funkcjonalność zarządzania maksymalną ilością operacji wejścia / wyjścia wykonywanych na danym wolumenie - zarządzanie musi być możliwe zarówno poprzez określenie ilości operacji I/O na sekundę jak również przepustowości określonej w MB/s. |
| 29 | Funkcjonalności | Macierz musi mieć możliwość kompresji i deduplikacji dla wszystkich rodzajów dysków. Licencja na tą funkcjonalność musi być zawarta w cenie i musi obejmować zaoferowaną w ramach macierzy przestrzeń dyskową Wsparcie dla kompresji danych w trybie inline („na bieżąco” bez potrzeby zapisywania danych na nośnikach danych w formie nie skompresowanej) dla dostępu blokowego. |
| 30 | Technologia optymalizacji przestrzeni zajmowanej przez dane | Macierz musi wspierać kompresję i deduplikację w trybie "inline". |
| 31 | Wysoka dostępność | Zaoferowane rozwiązanie musi posiadać możliwość implementacji klastra wysokiej dostępności. W ramach architektury klastra wysokiej dostępności musi być wspierane bezprzerwowe migrowanie maszyn wirtualnych pomiędzy ośrodkami. W przypadku awarii jednej z macierzy nastąpi bezprzerwowe przełączenie do lokalizacji zapasowej. Powyższa funkcjonalność musi być realizowana niezależnie od systemu operacyjnego na poziomie przełączania ścieżek do urządzenia logicznego. Licencja na tą funkcjonalność musi być zawarta w cenie i musi obejmować zaoferowaną w ramach macierzy przestrzeń dyskową. |
| 32 | Optymalizacja wykorzystania zasobów wewnętrznych | Macierz musi optymalizować wykorzystanie dysków SSD/ modułów Flash/ HDD, tak aby w ramach tego samego rodzaju dysków (pojemności/prędkości) wszystkie grupy dysków były utylizowane w równym stopniu. Licencja na tą funkcjonalność musi być zawarta w cenie i musi obejmować całą oferowaną pojemność macierzy. |
| 33 | Obsługa wirtualnych dysków logicznych | Macierz musi mieć możliwość rozłożenia wolumenu logicznego pomiędzy co najmniej dwoma różnymi typami macierzy dyskowych |
| 34 | Obsługa wirtualnych dysków logicznych | Macierz musi umożliwiać stworzenie mirrorowanych LUN pomiędzy różnymi macierzami, dla których awaria jednej kopii lustra musi być niezauważalna dla systemu hosta. |
| 35 | Funkcjonalność thin provisioning | Macierz musi obsługiwać funkcjonalność thin provisioning dla wszystkich wolumenów. Należy dostarczyć licencję umożliwiającą korzystanie z funkcji thin provisioning na całą oferowaną pojemność macierzy. |
| 36 | Kopie migawkowe | Kopie danych typu snapshot (PIT) muszą być tworzone w trybach incremental, multitarget, oraz kopii pełnej oraz kopii wskaźników. Licencja na tą funkcjonalność musi być zawarta w cenie i musi obejmować całą oferowaną pojemność macierzy. |
| 37 | Kopie migawkowe | Macierz musi posiadać możliwość tworzenia kopii migawkowych w trybie WORM (Write Once Read Many). Kopie powinny być tworzone za pomocą harmonogramu i mieć możliwość ustawienia retencji kopii, po upłynięciu której kopia automatycznie zostanie usunięta z macierzy. |
| 38 | Replikacja danych pomiędzy macierzami | Macierz musi mieć możliwość wykonywania replikacji synchronicznej i asynchronicznej wolumenów logicznych pomiędzy różnymi typami macierzy dyskowych. Zasoby źródłowe kopii zdalnej oraz docelowe kopii zdalnej mogą być zabezpieczone różnymi poziomami RAID i egzystować na różnych technologicznie dyskach stałych (SAS, SSD, SATA). Licencja na tą funkcjonalność musi być zawarta w cenie i musi obejmować zaoferowaną w ramach macierzy przestrzeń dyskową. |
| 39 | Inne | Macierz musi być nowa, nigdy wcześniej nie używana i pochodzić z autoryzowanego kanału dystrybucji producenta a także być objęta serwisem producenta na terenie RP. |
| 40 | Wsparcie systemów operacyjnych | Wsparcie systemów operacyjnych Macierz musi być wspierana przez systemy operacyjne i wirtualizatory: MS Windows Server 2019, 2022, Vmware vSphere 7 i nowsze, RedHat Enterprise Server 7.6 i nowsze |
| 41 | Integracja z rozwiązaniem backupu | Macierz musi zapewniać integrację z oprogramowaniem Veeam Backup & Replication na poziomie umozliwiającym na pełna współprace w zakresie: - backupu z migawek pamięci masowych - Veeam Explorer for Storage Snapshots - On-Demand Sandbox for Storage Snapshots Współpraca z oprogramowaniem Veeam Backup & Replication ma się odbywać bez konieczności instalacji dodatkowych modułów (pluginów). |
| 42 | Gwarancja | Wymagana jest gwarancja świadczona w trybie 24 godziny przez 7 dni w tygodniu na wszystkie elementy macierzy (sprzęt oraz oprogramowanie) na okres 36 miesięcy. Usługi serwisowe będą świadczone przez producenta oferowanego sprzętu. |

1. **Przełącznik SAN – 2 sztuki.**

|  |  |
| --- | --- |
| **Lp.** | **WYMAGANE PARAMETRY TECHNICZNE** |
| 1 | Przełącznik sieci SAN - FibreChannel 16/32 Gbps |
| 2 | Każdy przełącznik musi posiadać minimum 24 porty FC 16/32Gbps. Z czego minimum 16 portów musi być aktywnych (licencje), a kolejne 8 (dając razem 24 aktywne porty) może zostać aktywowane poprzez zakup licencji |
| 3 | Każdy przełącznik musi być wyposażony w 16 szt. wkładek SFP+ 32Gbps (SWL) pracujące na włóknach światłowodowych wielomodowych typu OM3/OM4 |
| 4 | Przełącznik nie może mieć więcej niż 1U |
| 5 | Z przełącznikiem należy dostarczyć elementy do instalacji urządzenia w szafie 19" |
| 6 | Przełącznik musi posiadać port Konsoli szeregowej oraz port zarządzający Ethernet |
| 7 | Przełącznik musi być zarządzany poprzez protokoły: Telnet, SSH (CLI) oraz WebGUI (http/https) |
| 8 | Wszystkie licencje muszą być dożywotnie – nie dopuszcza się subskrypcji oprogramowania |
| 9 | Przełącznik musi wspierać funkcję Ingress Rate Limiting, Traffic Isolation, QoS, BB credit recovery, F\_Port Trunking, FDMI, Frame Redirection, FSPF, IPoFC, NPIV, Simple Name Server (SNS), |
| 10 | Przełącznik musi realizować sprzętową obsługę zoningu (przez tzw. układ ASIC) na podstawie portów i adresów WWN |
| 11 | Przełącznik 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 |
| 12 | Wsparcie dla N\_Port ID Virtualization (NPIV). Obsługa, co najmniej 255 wirtualnych urządzeń na pojedynczym porcie przełącznika |
| 13 | Przełącznik musi wspierać następujące mechanizmy zwiększające poziom bezpieczeństwa: o mechanizm tzw. Fabric Binding, który umożliwia zdefiniowanie listy kontroli dostępu regulującej prawa przełączników FC do uczestnictwa w sieci fabric |
| 14 | uwierzytelnianie (autentykacja) przełączników w sieci Fabric za pomocą protokołów DH-CHAP i FCAP o uwierzytelnianie (autentykacja) urządzeń końcowych w sieci Fabric za pomocą protokołu DH-CHAP o szyfrowanie połączenia z konsolą administracyjną. Wsparcie dla SSHv2 |
| 15 | definiowanie wielu kont administratorów z możliwością ograniczenia ich uprawnień za pomocą mechanizmu tzw. RBAC (Role Based Access Control) |
| 16 | definiowane kont administratorów w środowisku RADIUS, LDAP w MS Active Directory, Open LDAP |
| 17 | obsługa SNMP v1 oraz v3 |
| 18 | wgrywanie nowych wersji firmware przełącznika z wykorzystaniem bezpiecznych protokołów SCP oraz SFTP o wykonywanie kopii bezpieczeństwa konfiguracji przełącznika FC z wykorzystaniem bezpiecznych protokołów SCP oraz SFTP |
| 19 | Przełącznik musi być dostarczony z aktywnymi następującymi narzędziami diagnostycznymi i mechanizmami obsługi ruchu FC: |
| 20 | logowanie zdarzeń poprzez mechanizm „syslog” |
| 21 | 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 |
| 22 | FCping, FC traceroute |
| 23 | Przełącznik musi być wyposażony w 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 |
| 24 | Gwarancja 3 lata na miejscu instalacji z czasem reakcji na następny dzień roboczy |

1. **Konfiguracja serwerów oraz rekonfiguracja backup.**

Przedmiotem zamówienia jest wykonanie usługi obejmującej:

1. Przygotowanie i konfiguracja dwóch serwerów Oracle Database, z których jeden pełnić będzie rolę serwera produkcyjnego (Primary), a drugi – serwera zapasowego (Standby), utrzymywanego w trybie oczekiwania na awarię. Środowisko zostanie skonfigurowane w sposób umożliwiający szybkie i bezpieczne przełączenie bazy danych na serwer zapasowy w przypadku awarii jednostki podstawowej, bez wykorzystania technologii ASM, Data Guard ani klastrów RAC. Rozwiązanie ma zapewnić wysoką dostępność systemu, minimalny czas przestoju oraz pełną spójność danych w procesie przełączenia.
2. Przepięcie datastore’ów wirtualizatorów na nową macierz
3. Rekonfigurację systemu backupu Veeam – zgodnie z najlepszymi praktykami producentów.

**Wymagania wobec wykonawcy**

1. Wykonawca musi być autoryzowanym partnerem firmy Asseco Poland S.A.
2. Wykonawca musi być autoryzowanym partnerem Oracle
3. Wykonawca musi dysponować personelem spełniającym poniższe wymagania:

* minimum dwie osoby posiadające co najmniej certyfikaty z zakresu Oracle Database 19c,
* minimum dwie osoby posiadające co najmniej certyfikat z zakresu backup i odtwarzanie baz danych Oracle

1. Osoby wykonujące prace muszą posiadać doświadczenie w:

* konfiguracji i utrzymaniu środowisk Oracle Database w architekturze redundantnej (Primary/Standby bez ASM, RAC i Data Guard),
* migracji lub przepinaniu datastore’ów w środowiskach wirtualizacyjnych (VMware / Oracle VM),
* konfiguracji i rekonfiguracji backupów w systemach Veeam Backup & Replication.

**Zakres prac**

1. Analiza bieżącej konfiguracji środowiska Oracle i wirtualizacji.
2. Przygotowanie planu migracji datastore’ów i nowej konfiguracji macierzy.
3. Konfiguracja dwóch serwerów Oracle Database – z jednym pracującym w trybie podstawowym i drugim w trybie oczekiwania na awarię, z możliwością automatycznego przełączenia w razie awarii.
4. Przełączenie datastore’ów wirtualizatorów na nową macierz z zachowaniem ciągłości pracy systemów.
5. Rekonfiguracja backupu w systemie Veeam, testy integralności kopii zapasowych.
6. Opracowanie dokumentacji powykonawczej.
7. **Usługa migracji baz danych.**

1. Przedmiot zamówienia

Przedmiotem zamówienia jest wykonanie kompleksowej usługi migracji baz danych Oracle wykorzystywanych u Zamawiającego przez systemy AMMS, Infomedica Laboratorium, Infomedica Plus, EDM, MPI (produkcji Asseco Poland S.A.) do nowego środowiska serwerowego. Migracja ma zostać przeprowadzona z zachowaniem integralności danych, ciągłości działania systemu oraz zgodności z zaleceniami i wytycznymi producenta oprogramowania Oracle oraz Asseco Poland S.A.

2. Zakres przedmiotu zamówienia

2.1. Analiza i planowanie migracji

- Inwentaryzacja istniejących baz danych (liczba, wersje Oracle, pojemność, zależności między bazami, aplikacjami i procesami).  
- Ocena wymagań nowego środowiska (wydajność, pojemność, licencje, IOPS, przepustowość).  
- Analiza ryzyka, w tym identyfikacja baz krytycznych.  
- Opracowanie szczegółowego Planu migracji, w tym planu awaryjnego (rollback planu) i harmonogramu działań.

2.2. Przygotowanie nowego środowiska

- Instalacja i konfiguracja systemu operacyjnego zgodnie z najlepszymi praktykami Oracle.  
- Konfiguracja klastra serwerów, sieci, interfejsów SAN/NAS.  
- Konfiguracja macierzy dyskowej: utworzenie wolumenów dla danych, logów i kopii zapasowych.  
- Ustalenie polityki RAID, replikacji oraz snapshotów.  
- Weryfikacja wymagań pod kątem zgodności z wersją AMMS i Oracle.

2.3. Przygotowanie i testy migracji

- Wybór i uzgodnienie metody migracji (np. RMAN backup/restore, Data Pump).  
- Wykonanie testowej migracji na środowisku testowym.  
- Weryfikacja integralności i kompletności danych.  
- Testy wydajnościowe po migracji testowej.  
- Opracowanie raportu z testów migracyjnych.

2.4. Migracja środowiska produkcyjnego

- Wykonanie pełnego backupu końcowego.  
- Przeniesienie danych na nowe środowisko.  
- Zablokowanie transakcji w bazach krytycznych (jeśli wymagane).  
- Weryfikacja poprawności działania po migracji.  
- Aktualizacja połączeń TNS, DNS, connection strings w aplikacjach współpracujących z AMMS, Infomedica Laboratorium, Infomedica Plus, EDM, MPI  
- Testy powdrożeniowe funkcjonalne i wydajnościowe.  
- Przekazanie raportu z realizacji migracji.

3. Wymagania dla Wykonawcy

- Udokumentowane doświadczenie w realizacji co najmniej dwóch projektów migracji baz danych Oracle dla systemów klasy HIS (np. AMMS, InfoMedica lub równoważnych).  
- Wykonawca zobowiązany jest do opracowania i przedstawienia: szczegółowego planu migracji i harmonogramu, planu awaryjnego (rollback), planu testów i raportu powdrożeniowego.  
- Prace muszą być prowadzone w sposób zapewniający minimalny przestój systemu AMMS.  
- Wykonawca zapewni wsparcie powdrożeniowe przez minimum 14 dni roboczych po zakończeniu migracji.

4. Kryteria odbioru usługi

Usługa migracji zostanie uznana za wykonaną prawidłowo po spełnieniu łącznie następujących warunków:  
1. Wszystkie bazy danych Oracle systemu AMMS, , Infomedica Laboratorium, Infomedica Plus, EDM, MPI zostały poprawnie przeniesione do nowego środowiska.  
2. Integralność i kompletność danych zostały potwierdzone.  
3. Systemy AMMS, , Infomedica Laboratorium, Infomedica Plus, EDM, MPI oraz powiązane aplikacje działają poprawnie po migracji (testy funkcjonalne i wydajnościowe).  
4. Wykonawca dostarczył: raport z przebiegu migracji, wyniki testów potwierdzających poprawność migracji, zaktualizowaną dokumentację konfiguracji środowiska, plan odtworzenia w razie awarii (DR plan).  
5. Przedstawiciele Zamawiającego zaakceptowali wyniki testów powdrożeniowych.  
6. Nie występują błędy krytyczne w działaniu systemów AMMS, , Infomedica Laboratorium, Infomedica Plus, EDM, MPI po migracji.

5. Dokumentacja i szkolenie

Wykonawca zobowiązany jest przekazać:  
- dokumentację techniczną nowego środowiska (schematy, konfiguracje, parametry),  
- dokumentację procedur backupu i odtworzenia,  
- krótkie szkolenie administratorów Zamawiającego w zakresie obsługi i monitorowania nowego środowiska.

1. **Archiwizacja baz danych w chmurze.**

Przedmiotem zamówienia jest: instalacja, konfiguracja środowiska backupowego w chmurze Oracle dla posiadanych przez Zamawiającego baz danych systemów: InfoMedica Laboratorium, InfoMedica Plus, AMMS, EDM i MPI produkcji Asseco SA. (usługa backupu).

2. Usługa backupu musi zapewnić automatyczne przechowywanie archiwów dla tych baz z co najmniej trzech ostatnich dni.

3. Usługa backupu świadczona będzie zgodnie z warunkami i zasadami zawartymi w dokumencie „Oracle PaaS and IaaS Universal Credits Service Descriptions”, publikowanymi przez dostawcę usługi chmurowej na stronie: http://www.oracle.com/us/corporate/contracts/paas-iaas-universal-credits-3940775.pdf

4. Usługa świadczona będzie przez okres trwałości projektu od dnia uruchomienia usługi poprzez udostępnienie na potrzeby Zamawiającego Universal Credits w ilości umożliwiającej tworzenie i przechowywanie backupu bazy danych Oracle z wykorzystaniem co najmniej narzędzia RMAN o pojemności nie mniejszej niż 5 TB.

5. Zamawiający wymaga aby Wykonawca był partnerem Oracle.

6. Usługa backupu musi umożliwiać weryfikację odtworzenia z kopii bazy na serwerach chmurowych potwierdzoną odpowiednim raportem z tej czynności.

7. Pliki muszą być chronione z wykorzystaniem technologii SSL (Secure Sockets Layer). Pliki muszą być szyfrowane zarówno w trakcie procesu wysyłania ich do chmury, jak i w samej chmurze by zapobiec ich nieautoryzowanemu użyciu.

8. Usługa backupu musi umożliwiać odtworzenie lub przeniesienia całego środowiska do chmury w przypadku awarii infrastruktury serwerowej Zamawiającego dla posiadanego systemu HIS. Wykonawca przekaże ofertę działania środowiska w chmurze z kosztem za każdy dzień jego działania.

9. Usługa backupu musi zapewnić odtworzenie zarchiwizowanych w chmurze baz danych Zamawiającego przez Wykonawcę. Po ewentualnej awarii, usługa ta musi być niezwłocznie wykonana przez certyfikowanych inżynierów Oracle tak by jak najszybciej przywrócić działanie systemu AMMS w siedzibie Zamawiającego.

Cechy wspólne systemów do archiwizacji:

1. Usługa backupu musi być świadczona na terenie Europejskiego Obszaru Gospodarczej (EOG, ang. European Economic Area) i nie jest możliwe ich przekazanie przez Wykonawcę w jakiejkolwiek formie (np. backup, logi) poza ten obszar.

2. Usługa backupu będzie współdziałać z pozostałymi systemami Zamawiającego zbudowanymi w oparciu o technologię Oracle, wdrożonymi u Zamawiającego, do których Zamawiający posiada prawa licencyjne oraz będzie zapewniać pracę tych systemów tak jak realizuje to technologia Oracle, bez konieczności zakupu dodatkowych licencji, wykonywania dodatkowych prac dostosowawczych czy migracji,

3. Usługa backupu nie będzie powodować zakłóceń pracy oprogramowania z zakresu technologii Oracle, z którym będzie współdziałało

4. Bezpieczna transmisja: połączenie pomiędzy serwerem, a usługami chmurowymi musi być szyfrowane. Transmisja danych z maszyn Zamawiającego musi odbywać się poprzez bezpieczne połączenie VPN, które jest ustanawiane za pomocą protokołów PPTP lub L2TP. Połączenie musi być szyfrowane, co ma zapewnić, że przesyłane dane są chronione przed nieautoryzowanym dostępem i potencjalnymi zagrożeniami z sieci. Cały proces transmisji musi być monitorowany, aby zapewnić integralność danych oraz bezbłędny przebieg transferu. Dzięki zastosowaniu szyfrowania, nawet w przypadku przechwycenia transmisji, dane muszą pozostać nieczytelne dla osób trzecich.

5. Usługa backupu musi być zgodna z ustawą o Cyberbezpieczeństwie.

6. Usługa backupu musi umożliwiać zabezpieczanie szyfrowaniem kopii bazy kluczem prywatnym do którego dostępu posiadają jedynie wskazani administratorzy.

7. Kopie zapasowe w chmurze muszą zapewnić zabezpieczenie danych przed utratą spowodowaną awarią sprzętu, kradzieżą, pożarem, zalaniem czy innymi katastrofami. Dane będą przechowywane na zdalnych serwerach, które są zabezpieczone i monitorowane przez profesjonalny zespół inżynierów.

8. Wykonawca zapewni łatwy dostęp do danych: Możliwość uzyskania dostępu do kopii zapasowych z dowolnego miejsca i urządzenia z dostępem do Internetu. Dzięki temu można przywrócić dane, gdy zaistnieje taka potrzeba.

9. Wykonawca utworzy harmonogram tworzenia kopii zapasowych w porozumieniu z Zamawiającym.

10. Usługi kopii zapasowych w chmurze muszą pozwalać dostosować przestrzeń przechowywania do aktualnych potrzeb. Dawać możliwość zwiększania lub zmniejszania ilości przechowywanych danych w zależności od potrzeb.

11. Kopie zapasowe w chmurze muszą stanowić dodatkową ochronę przed atakami ransomware. Jeśli lokalne dane zostaną zaszyfrowane przez złośliwe oprogramowanie, musi być możliwość ich łatwego i szybkiego przywrócenia z kopii zapasowych na dowolnym środowisku.

12. W przypadku awarii sprzętu lub zmiany środowiska, usługa musi umożliwić odtworzenie środowiska do pracy i przywrócenie danych na nowym środowisku wskazanym przez Zamawiającego.

13. Wykonawca zobowiązuje się do cyklicznego (nie rzadziej niż raz na trzy miesiąca) testowego odtworzenia. Prace te będą realizowane na żądanie administratora.

Wymagania dotyczące testowego odtwarzania kopii zapasowych baz danych

1. Wykonawca zobowiązany jest do przeprowadzania testowego odtwarzania kopii zapasowych baz danych nie rzadziej niż raz na trzy miesiące, w celu weryfikacji poprawności procesu tworzenia oraz jakości danych podlegających archiwizacji.
2. Testowe odtworzenie musi obejmować:
   * weryfikację kompletności i spójności danych,
   * możliwość odtworzenia zarówno pojedynczych elementów (np. tabel, plików), jak i całej bazy danych,
   * sprawdzenie poprawności działania mechanizmów odtwarzania oraz integralności środowiska po zakończeniu testu.
3. Wykonawca ma obowiązek dokumentowania każdego przeprowadzonego testu odtworzenia poprzez sporządzenie protokołu z testu, który powinien zawierać w szczególności:
   * datę wykonania testu,
   * identyfikator (datę) odtwarzanej kopii zapasowej,
   * opis przebiegu testu i wyniki weryfikacji danych,
   * potwierdzenie poprawności odtworzenia lub opis wykrytych nieprawidłowości,
   * wskazanie osoby odpowiedzialnej za przeprowadzenie testu.
4. Protokół z przeprowadzonego testowego odtwarzania kopii zapasowej należy przekazać Zamawiającemu w terminie do 3 dni roboczych od daty wykonania testu w formacie elektronicznym (PDF).
5. W przypadku stwierdzenia błędów lub niezgodności Wykonawca zobowiązany jest do niezwłocznego ich usunięcia oraz powtórzenia testu w terminie nie dłuższym niż 7 dni roboczych.
6. Niewykonanie testu w wymaganym terminie lub brak przekazania protokołu może zostać uznane za nienależyte wykonanie przedmiotu umowy.

Pozostałe wymagania dla Wykonawcy

* 1. Wykonawca zobowiązuje się współpracować z Inspektorem Ochrony Danych Zamawiającego zgodnie z obowiązującym porządkiem prawnym oraz uregulowaniami wewnątrzzakładowym.
  2. Wykonawca zobowiązuje się współpracować i koordynować działania ze wskazanymi osobami z działu Informatyki Zamawiającego.
  3. Wykonawca powinien być autoryzowanym partnerem producenta oprogramowania Asseco SA i dysponować wykwalifikowanym personelem posiadającym właściwe certyfikaty do obsługi określonych modułów oprogramowania aplikacyjnego, zatrudnionych na umowę o pracę przez cały okres trwania umowy.
  4. Wykonawca powinien być autoryzowanym parterem producenta baz danych Oracle i musi dysponować co najmniej dwoma specjalistami legitymującym się certyfikatem Oracle co najmniej 19c w zakresie Administrowania Bazami Danych Oracle.
  5. Wykonawca musi dysponować co najmniej dwoma specjalistami legitymującymi się certyfikatem ukończenia kursu Backup i Odtwarzanie baz danych Oracle.
  6. Wykonawca musi dysponować co najmniej dwoma specjalistami legitymującymi się certyfikatem ukończenia kursu Administracji Serwerami Linux.
  7. Wykonawca musi dysponować co najmniej jednym specjalistą legitymującym się certyfikatem Oracle Cloud Infrastructure 2025 Certified Architect Associate
  8. Wykonawca musi dysponować wykwalifikowanym personelem w postaci kierownika projektu posiadającego certyfikat PRINCE2® Foundation Certificate in Project Management zatrudnionego przez cały okres trwania umowy.
  9. Wykonawca musi dysponować opłaconą polisą od odpowiedzialności cywilnej przez cały okres obowiązywania umowy na kwotę co najmniej 300 000 zł.
  10. Wykonawca musi przedstawić na wezwanie Zamawiającego referencje dla tożsamej instalacji w okresie ostatnich 2 lat w ilości minimum 2 szt.

1. **Oprogramowanie do zarządzania bazami danych – 2 sztuki.**

**Przedmiot zamówienia:**

|  |
| --- |
| **WYMAGANIA OGÓLNE** |
| **Zamawiający wymaga licencji Oracle Database Standard Edition 2 w ilości: 2 SZT** |
| a. bezterminowej/wieczystej, |
| b. w oparciu o procesor (Processor License) – system uruchomiony będzie na dwóch serwerach jednoprocesorowych |
| c. w najnowszej dostępnej wersji wydanej przez producenta oprogramowania. |
| Oprogramowanie bazodanowe musi spełniające standardy jakościowe oraz posiadać zakres funkcjonalny i parametry oprogramowania wymaganego przez Zamawiającego oraz współpracować bez zakłóceń z bazami danych Oracle posiadanymi przez Zamawiającego - bazy danych aplikacji Infomedica Laboratorium, Infomedica Plus, AMMS, EDM, MPI firmy Asseco S.A.. |
| Oferowane oprogramowanie musi umożliwić migrację aktualnie posiadanych baz Oracle wymienionych w powyższym punkcie do swojej infrastruktury i umożliwić uruchomienie tych baz, zarządzanie nimi oraz umożliwić współpracę bez zakłóceń z aplikacjami Infomedica Laboratorium, Infomedica Plus, AMMS, EDM, MPI firmy Asseco S.A.. |
| **WYMAGANIA SZCZEGÓŁOWE** |
| 1.      Dostarczone licencje maja być dożywotnie, Zamawiający dopuszcza dostarczenie licencji umożliwiający wykorzystanie ich tylko dla oprogramowania produkcji Asseco Poland S.A. |
| 2.      Dostępność oprogramowania na współczesne 64-bitowe platformy Unix (HP-UX dla procesorów Itanium, Solaris dla procesorów SPARC i Intel/AMD, IBM AIX dla procesorów POWER, Intel/AMD Linux, MS Windows). Identyczna funkcjonalność serwera bazy danych na ww. platformach |
| 3.      Dostarczone licencje nie mogą ograniczać liczby użytkowników końcowych korzystających z oprogramowania ani liczby przetwarzanych lub przechowywanych dokumentów, plików, rekordów, żądań, wykorzystywanych systemów dziedzinowych  etc. Licencje nie mogą być ograniczone czasowo. |
| 4.      Dostępność narzędzi migracji baz danych pomiędzy platformami na poziomie fizycznym (kopiowanie / konwersja plików danych) oraz logicznym (narzędzia eksportu / importu). |
| 5.      Oprogramowanie klienckie, za pomocą którego można łączyć się do bazy danych musi być dostępne na wielu platformach systemowo-sprzętowych (minimalny zakres platform taki jak dla oprogramowania serwera bazy danych ) |
| 6.      Wsparcie protokołu XA. |
| 7.      Wsparcie standardu JDBC 3.0. |
| 8.      Zgodność ze standardem ANSI/ISO SQL 2003 lub nowszym. |
| 9.      Wbudowana obsługa wyrażeń regularnych zgodna ze standardem POSIX dostępna z poziomu języka SQL jak i procedur/funkcji składowanych w bazie danych. |
| 10.  RDBMS musi zapewniać niezależność platformy systemowej dla oprogramowania klienckiego od platformy systemowej bazy danych. |
| 11.  RDBMS musi zapewniać przetwarzanie transakcyjne wg reguł ACID z zachowaniem spójności i maksymalnego możliwego stopnia współbieżności. Mechanizm izolowania transakcji musi pozwalać na spójny odczyt modyfikowanego obszaru danych bez wprowadzania blokad, spójny odczyt nie może blokować możliwości wykonywania zmian. |
| 12.  RDBMS musi posiadać możliwość zagnieżdżania transakcji – możliwość uruchomienia niezależnej transakcji wewnątrz transakcji nadrzędnej. |
| 13.  Dostępność nieblokującego poziomu izolowania transakcji „tylko do odczytu” (Read Only) pozwalający na uzyskanie w wielu kolejnych następujących po sobie zapytaniach rezultatów odzwierciedlających stan danych z chwili rozpoczęcia ww. transakcji. |
| 14.  Dostępność poziomu serializowanego poziomu izolowania transakcji (Serializable). |
| 15.  Możliwość zmiany domyślnego trybu izolowania transakcji (Read Commited) na inny (Read Only, Serializable) za pomocą komend serwera bazy danych. |
| 16.  Wsparcie dla wielu ustawień narodowych i wielu zestawów znaków (włącznie z Unicode) zarówno po stronie serwera bazy danych jak i oprogramowania klienckiego. Wsparcie dla polskich stron kodowych – ISO-8859-2, MS Windows Code Page 1250 oraz PC 852. Automatyczna konwersja znaków pomiędzy różnymi ustawieniami stron kodowych po stronie klienta i serwera bazy danych. |
| 17.  Możliwość migracji bazy danych utrzymujących dane znakowe w 8-bitowej stronie kodowej do Unicode. |
| 18.  Możliwość definiowania w przestrzeni danych (plików) dla danych użytkownika obszarów o innym niż domyślny rozmiarze bloku. |
| 19.  Możliwość bez dodatkowych ograniczeń przechowywania wierszy, których rozmiar przekracza rozmiar bloku bazy danych. |
| 20.  Możliwość budowania indeksów o strukturze B-drzewa. Baza danych powinna umożliwiać założenie indeksu jednej lub większej liczbie kolumn tabeli, przy czym ograniczenie liczby kolumn na których założony jest 1 indeks nie powinno być mniejsze niż 16. |
| 21.  Możliwość budowania widoków zmaterializowanych odzwierciedlających stan danych zdefiniowanych przez zapytanie SQL. Widok zmaterializowany przechowuje rezultat zapytania, którego aktualizacja odbywa się w jednej z dostępnych strategii – na żądanie, okresowo bądź po każdym zatwierdzeniu transakcji modyfikującej tabele, na której oparty jest widok zmaterializowany. |
| 22.  Możliwość szybkiego odświeżania danych w widoku zmaterializowanym na podstawie mechanizmu identyfikacji zmian w danych źródłowych. |
| 23.  Brak formalnych ograniczeń na liczbę tabel i indeksów w bazie danych oraz na ich rozmiar (liczbę wierszy). |
| 24.  Kosztowy model optymalizacji instrukcji SQL. |
| 25.  Model statystyk optymalizatora kosztowego musi pozwalać na odwzorowanie nierównomierności rozkładu danych (składowanie informacji o rozkładzie wartości występujących w kolumnach za pomocą histogramu bądź porównywalnego funkcjonalnie modelu odwzorowania). |
| 26.  Możliwość uwzględnienia korelacji wartości występujących w niezależnych kolumnach tabeli w modelu statystyk optymalizatora kosztowego. |
| 27.  RDBMS 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. |
| 28.  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. |
| 29.  Procedury i funkcje składowane powinny mieć możliwość parametryzowania za pomocą parametrów prostych jak i parametrów o typach złożonych, definiowanych przez użytkownika. Funkcje powinny mieć możliwość zwracania rezultatów jako zbioru danych, możliwego do wykorzystania jako źródło danych w instrukcjach SQL (czyli występujących we frazie FROM). Ww. jednostki programowe powinny umożliwiać wywoływanie instrukcji SQL (zapytania, instrukcje DML, DDL), umożliwiać jednoczesne otwarcie wielu tzw. kursorów pobierających paczki danych (wiele wierszy za jednym pobraniem) oraz wspierać mechanizmy transakcyjne (np. zatwierdzanie bądź wycofanie transakcji wewnątrz procedury). |
| 30.  Możliwość kompilacji procedur składowanych w bazie do postaci kodu binarnego (biblioteki dzielonej). |
| 31.  Możliwość deklarowania wyzwalaczy (triggerów) na poziomie instrukcji DML (INSERT, UPDATE, DELETE) wykonywanej na tabeli, poziomie każdego wiersza modyfikowanego przez instrukcję DML oraz na poziomie zdarzeń bazy danych (np. próba wykonania instrukcji DML, start serwera, stop serwera, próba zalogowania użytkownika, wystąpienie specyficznego błędu w serwerze). Ponadto mechanizm wyzwalaczy powinien umożliwiać oprogramowanie obsługi instrukcji DML (INSERT, UPDATE, DELETE) wykonywanych na tzw. niemodyfikowalnych widokach (views). |
| 32.  W przypadku, gdy w wyzwalaczu na poziomie instrukcji DML wystąpi błąd zgłoszony przez motor bazy danych bądź ustawiony wyjątek w kodzie wyzwalacza, wykonywana instrukcja DML musi być automatycznie wycofana przez serwer bazy danych, zaś stan transakcji po wycofaniu musi odzwierciedlać chwilę przed rozpoczęciem instrukcji w której wystąpił ww. błąd lub wyjątek. |
| 33.  Możliwość wykonania równoczesnych operacji DML (Insert/Update/Delete) na tej samej tabeli . |
| 34.  Powinna istnieć możliwość autoryzowania użytkowników bazy danych za pomocą rejestru użytkowników założonego w bazie danych bądź mechanizmu zewnętrznego w stosunku do bazy danych. |
| 35.  Przywileje użytkowników bazy danych powinny być określane za pomocą przywilejów systemowych (np. prawo do podłączenia się do bazy danych - czyli utworzenia sesji, prawo do tworzenia tabel itd.) oraz przywilejów dostępu do obiektów aplikacyjnych (np. odczytu / modyfikacji tabeli, wykonania procedury). Baza danych powinna umożliwiać nadawanie ww. przywilejów za pośrednictwem mechanizmu grup użytkowników / ról bazodanowych. W danej chwili użytkownik może mieć aktywny dowolny podzbiór nadanych ról bazodanowych. |
| 36.  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, itp.). Wykonywanie kopii bezpieczeństwa powinno być możliwe w trybie offline oraz w trybie online(hot backup) |
| 37.  Odtwarzanie powinno umożliwiać odzyskanie stanu danych z chwili wystąpienia awarii bądź cofnąć stan bazy danych do punktu w czasie. W przypadku odtwarzania do stanu z chwili wystąpienia awarii odtwarzaniu może podlegać cała baza danych bądź pojedyncze pliki danych. |
| 38.  Motor bazy danych na poziomie wskazanego numeru wersji wydania musi zapewnić wbudowany, własny mechanizm umożliwiający uruchomienia środowiska w konfiguracji klastrowej wykorzystującej dwa węzły jako podstawę architektury rozwiązania |

1. **Serwer do instalacji wirtualizatora – 1 sztuka.**

|  |  |
| --- | --- |
| **Parametr** | **Charakterystyka (wymagania minimalne)** |
| **Obudowa** | * Obudowa Rack o wysokości 2U z możliwością instalacji 8/12 dysków 3.5” * Obudowa z możliwością wyposażenia w panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS’u, zasilaniu oraz temperaturze. * Obudowa z możliwością wyposażenia w kartę umożliwiającą dostęp bezpośredni poprzez urządzenia mobilne - serwer musi posiadać możliwość konfiguracji oraz monitoringu najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej min. (Android/ Apple iOS) przy użyciu jednego z protokołów BLE/ WIFI. |
| **Płyta główna** | * Płyta główna z możliwością zainstalowania do dwóch procesorów. * Obsługa procesorów 32 rdzeniowych. * Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym. * Na płycie głównej powinno znajdować się 16 slotów przeznaczonych do instalacji pamięci. * Płyta główna powinna obsługiwać do 1TB pamięci RAM. |
| **Chipset** | * Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych |
| **Procesor** | * Zainstalowane dwa procesory min. 16-rdzeniowe, min. 2.8GHz, klasy x86, dedykowane do pracy z zaoferowanym serwerem, umożliwiające osiągnięcie wyniku min. 344 w teście SPECrate2017\_int\_base, dostępnym na stronie www.spec.org dla konfiguracji dwuprocesorowej. |
| **RAM** | * 512GB DDR5 RDIMM 5600MT/s, |
| **Kontroler RAID** | * Sprzętowy kontroler dyskowy, posiadający   + Możliwość konfiguracji poziomów RAID: 0, 1, 5, 6, 10, 50, 60.   + Wsparcie dla dysków samoszyfrujących |
| **Dyski twarde** | * Zainstalowane:   2 dyski M.2 NVMe SSD o pojemności min. 480GB Hot-Plug z możliwością konfiguracji RAID 1. |
| **Gniazda PCI** | * trzy sloty PCIe |
| **Interfejsy sieciowe/FC/SAS** | * Wbudowane 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT oraz 4 interfejsy sieciowe 25Gb Ethernet w standardzie SFP28 * Dwa interfejsy FC 32Gb/s z wkładkami optycznymi |
| **Wbudowane porty** | * 4 porty USB w tym min:   + 1 port USB 3.0 z tyłu obudowy,   + 1 port micro USB z przodu obudowy * 2 port VGA z czego jeden z przodu obudowy * Możliwość rozbudowy o port RS232 |
| **Video** | * Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1280x1024 |
| **Wentylatory** | * Redundantne, Hot-Plug |
| **Zasilacze** | * Redundantne, Hot-Plug min. 1100W klasy Titanium |
| **Elementy montażowe** | * Komplet wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych * Ramię (organizer) do kabli ułatwiające wysuwanie serwera do celów serwisowych |
| **Bezpieczeństwo** | * Zatrzask górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych. * Wbudowany w serwer mechanizm pozwalający na weryfikację niezmienności konfiguracji sprzętowej serwera od momentu produkcji do dostawy do docelowej lokalizacji. Mechanizm ma również pozwalać na kontrolę otwarcia urządzenia w trakcie transportu, niezależnie od stanu zasilania. * Możliwość wyłączenia w BIOS funkcji przycisku zasilania. * BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła * Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą. * Moduł TPM 2.0 * Możliwość dynamicznego włączania i wyłączania portów USB na obudowie – bez potrzeby restartu serwera * Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem * Serwer musi być wyposażony w rozwiązanie zapewniające ochronę oprogramowania układowego przed manipulacją złośliwego oprogramowania. Ochrona taka musi być zgodna z zaleceniami NIST SP 800-147B i NIST SP 800-155. Jednocześnie Zamawiający wymaga, aby dostarczony serwer posiadał zaimplementowane sprzętowo mechanizmy kryptograficzne poświadczające integralność oprogramowania BIOS (Root of Trust). |
| **Karta Zarządzania** | * Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca:   + zdalny dostęp do graficznego interfejsu Web karty zarządzającej;   + zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera);   + szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika;   + możliwość podmontowania zdalnych wirtualnych napędów;   + wirtualną konsolę z dostępem do myszy, klawiatury;   + wsparcie dla IPv6;   + wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish;   + możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer;   + możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer;   + integracja z Active Directory;   + możliwość obsługi przez dwóch administratorów jednocześnie;   + wsparcie dla automatycznej rejestracji DNS   + wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej.   + możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera   + możliwość zarządzania do 100 serwerów bezpośrednio z konsoli karty zarządzającej pojedynczego serwera   oraz z możliwością rozszerzenia funkcjonalności o:   * + Wirtualny schowek ułatwiający korzystanie z konsoli zdalnej   + Przesyłanie danych telemetrycznych w czasie rzeczywistym   + Dostosowanie zarządzania temperaturą i przepływem powietrza w serwerze   + Automatyczna rejestracja certyfikatów (ACE) |
| **Oprogramowanie do zarządzania** | * Możliwość zainstalowania oprogramowania producenta do zarządzania, spełniającego poniższe wymagania:   + Wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych   + integracja z Active Directory   + Możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta   + Wsparcie dla protokołów SNMP, IPMI, Linux SSH, Redfish   + Możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram   + Szczegółowy opis wykrytych systemów oraz ich komponentów   + Możliwość eksportu raportu do CSV, HTML, XLS, PDF   + Możliwość tworzenia własnych raportów w oparciu o wszystkie informacje zawarte w inwentarzu.   + Grupowanie urządzeń w oparciu o kryteria użytkownika   + Tworzenie automatycznie grup urządzeń w oparciu o dowolny element konfiguracji serwera np. Nazwa, lokalizacja, system operacyjny, obsadzenie slotów PCIe, pozostałego czasu gwarancji   + Możliwość uruchamiania narzędzi zarządzających w poszczególnych urządzeniach   + Szybki podgląd stanu środowiska   + Podsumowanie stanu dla każdego urządzenia   + Szczegółowy status urządzenia/elementu/komponentu   + Generowanie alertów przy zmianie stanu urządzenia.   + Filtry raportów umożliwiające podgląd najważniejszych zdarzeń   + Integracja z service desk producenta dostarczonej platformy sprzętowej   + Możliwość przejęcia zdalnego pulpitu   + Możliwość podmontowania wirtualnego napędu   + Kreator umożliwiający dostosowanie akcji dla wybranych alertów   + Możliwość importu plików MIB   + Przesyłanie alertów „as-is” do innych konsol firm trzecich   + Możliwość definiowania ról administratorów   + Możliwość zdalnej aktualizacji oprogramowania wewnętrznego serwerów   + Aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania)   + Możliwość instalacji oprogramowania wewnętrznego bez potrzeby instalacji agenta   + Możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów   + Moduł raportujący pozwalający na wygenerowanie następujących informacji: nr seryjne sprzętu, konfiguracja poszczególnych urządzeń, wersje oprogramowania wewnętrznego, obsadzenie slotów PCI i gniazd pamięci, informację o maszynach wirtualnych, aktualne informacje o stanie i poziomie gwarancji, adresy IP kart sieciowych, występujących alertów, MAC adresów kart sieciowych, stanie poszczególnych komponentów serwera.   + Możliwość tworzenia sprzętowej konfiguracji bazowej i na jej podstawie weryfikacji środowiska w celu wykrycia rozbieżności.   + Wdrażanie serwerów, rozwiązań modularnych oraz przełączników sieciowych w oparciu o profile   + Możliwość migracji ustawień serwera wraz z wirtualnymi adresami sieciowymi (MAC, WWN, IQN) między urządzeniami.   + Tworzenie gotowych paczek informacji umożliwiających zdiagnozowanie awarii urządzenia przez serwis producenta.   + Zdalne uruchamianie diagnostyki serwera.   + Dedykowana aplikacja na urządzenia mobilne integrująca się z wyżej opisanym oprogramowaniem zarządzającym.   + Oprogramowanie dostarczane jako wirtualny appliance dla KVM, ESXi i Hyper-V. |
| **Oprogramowanie do monitorowania** | Oparta na chmurze aplikacja Producenta oferowanego urządzenia, która zapewnia proaktywne monitorowanie i rozwiązywanie problemów infrastruktury IT oraz integrację z posiadaną platformą wirtualizacji VMware. Zaproponowane rozwiązanie musi posiadać następujące funkcjonalności:   * Monitoring:   + ilość podłączonych oraz rozłączonych systemów   + stan podłączonych urządzeń   + informacje o potencjalnych zagrożeniach związanych z cyberbezpieczeństwem w oparciu o najlepsze praktyki i szczegółową analizę posiadanych systemów   + Informacje o alertach z podziałem na minimum: krytyczne, błędy, ostrzeżenia   + informacje o statusie gwarancji dla poszczególnych urządzeń   + informacje o stanie licencji na posiadane oprogramowanie rozszerzające funkcjonalności urządzeń   + informacje w oparciu o dane historyczne umożliwiające określenie trendów krótko- i długoterminowej prognozy wykorzystania przestrzeni na pamięciach masowych.   + Wykrywanie anomalii w oparciu o analizę zajętości przestrzeni na pamięciach masowych   + Wykrywanie anomalii wydajnościowych w oparciu o uczenie maszynowe oraz porównanie parametrów historycznych i bieżących. Funkcjonalność ta musi wspierać serwery, urządzenia sieciowe oraz systemy pamięci masowych.   + Monitorowanie wydajności, przepustowości oraz opóźnień dla systemy pamięci masowych.   + Zaimplementowana analityka predykcyjna umożliwiająca określenie szacowanego czasu awarii dla optyki przełączników FC.   + Szczegółowe informacje dla serwerów o modelu, konfiguracji, wersjach firmware poszczególnych komponentów adresacji IP karty zarządzającej.   + Monitoring parametrów serwerów z informacją o minimum:     - Obciążeniu procesora     - Zużyciu pamięci RAM     - Temperaturze procesorów     - Temperaturze powietrza wlotowego     - Zużyciu prądu     - Zmianach w fizycznej konfiguracji serwera     - Dla wszystkich wymienionych parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach.   + Monitoring parametrów pamięci masowych z informacją o minimum:     - Opóźnieniach     - IOPS     - Przepustowości     - Utylizacji kontrolerów     - Pojemność całkowita i dostępna     - Wszystkie informacje muszą być dostępne zarówno dla całej pamięci masowej jak i poszczególnych LUN-ów.     - Dla wszystkich wymienionych powyżej parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach.     - Dane historyczne o wykorzystaniu przestrzeni pamięci masowej muszą być przechowywane co najmniej 2 lata     - Informacje o poziomie redukcji danych     - Informacje o statusie replikacji oraz snapshotów   + Monitoring parametrów przełączników sieciowych z informacją o minimum:     - Modelu, oprogramowania, adresacji IP, MAC adres, nr seryjny     - Stanie komponentów: zasilacze, wentylatory     - Podłączonych hostach     - Ilości i statusu portów     - Utylizacji procesora     - Utylizacji poszczególnych portów     - Dla wszystkich wymienionych powyżej parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach. * Aktualizacja firmware   + możliwość aktualizacji firmware, oprogramowania zarządzającego dla systemów pamięci masowych, wraz z informacją o zalecanych wersjach oprogramowania   + możliwość aktualizacji firmware, oprogramowania zarządzającego dla serwerów, wraz z informacją o zalecanych wersjach oprogramowania   + możliwość aktualizacji firmware, oprogramowania zarządzającego dla rozwiazań HCI, wraz z informacją o zalecanych wersjach oprogramowania   + możliwość aktualizacji firmware, dla systemów przełączników FC, wraz z informacją o zalecanych wersjach oprogramowania   + możliwość aktualizacji firmware, dla deduplikatorów, wraz z informacją o zalecanych wersjach oprogramowania * Raporty   + Możliwość generowania raportów dla serwerów zawierających informację o:     - Nazwie hosta, modelu serwera, nr serwisowym, dacie końca okresu kontraktu serwisowego, zainstalowanym systemie operacyjnym, protokole komunikacyjnym z systemem pamięci masowej     - Średnim obciążeniu: procesorów, pamięci RAM, IO,   + Możliwość generowania raportów dla systemów pamięci masowych zawierających informację o:     - Nazwie, nr seryjnym, lokalizacji urządzenia, modelu urządzenia, wersji oprogramowania, zajętości systemu oraz poziomu redukcją danych, informacje o utworzonych LUN-ach i systemach pliku, status replikacji   + Generowanie raportów do plików CSV i PDF * Cyberbezpieczeństwo   + Analiza środowiska w oparciu o najlepsze praktyki dotyczące cyberbezpieczeństwa sprawdzająca stan poszczególnych urządzeń w środowisku i przypisujący im odpowiedni wynik bezpieczeństwa. System musi informować administratora o wykrytych lukach bezpieczeństwa oraz sposobie ich zabezpieczenia.   + Musi istnieć możliwość tworzenia własnych polityk bezpieczeństwa w oparciu o wzorce dla poszczególnych urządzeń.   + Stała analiza środowiska IT umożliwiająca wykrycie ataku ransomware na podstawie analizy posiadanych danych.   + Możliwość przypisania dedykowanych ról dla poszczególnych administratorów. * Wspierane urządzenia   + Urządzenie Producenta dostarczane w ramach postępowania   + Posiadane przez Zamawiającego serwery, urządzenia pamięci masowych, przełączniki sieciowe, przełączniki SAN, rozwiązania HCI, deduplikatory Producenta oferowanego urządzenia (jeśli takie są w posiadaniu Zamawiającego) * Wirtualny asystent   + Wbudowana w platformę funkcjonalność wirtualnego asystenta w oparciu o algorytmy GenAI przy dostępie do bazy wiedzy producenta urządzeń oraz analizie danych z monitoringu poszczególnych elementów infrastruktury; * Możliwość rozszerzenia funkcjonalności   + Możliwość rozbudowy systemu o zintegrowane i dodatkowe płatne moduły do monitoringu aplikacji oraz zarządzania incydentami w ramach infrastruktury IT. * Inne   + Oferowana platforma musi posiadać dedykowaną aplikację na urządzenia iOS oraz Android |
| **Certyfikaty** | * Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015, ISO-50001 oraz ISO-14001 * Serwer musi posiadać deklaracja CE. * Oferowane produkty muszą zawierać informacje dotyczące ponownego użycia i recyklingu, nie mogą zawierać farb i powłok na dużych plastikowych częściach, których nie da się poddać recyklingowi lub ponownie użyć. Wszystkie produkty zawierające podzespoły elektroniczne oraz niebezpieczne składniki powinny być bezpiecznie i łatwo identyfikowalne oraz usuwalne. Usunięcie materiałów i komponentów powinno odbywać się zgodnie z wymogami Dyrektywy WEEE 2002/96/EC. Produkty muszą składać się z co najmniej w 65% ze składników wielokrotnego użytku/zdatnych do recyklingu. We wszystkich produktach części tworzyw sztucznych większe niż 25-gramowe powinny zawierać nie więcej niż śladowe ilości środków zmniejszających palność sklasyfikowanych w dyrektywie RE 67/548/EEC. Potwierdzeniem spełnienia powyższego wymogu jest wydruk ze strony internetowej [www.epeat.net](http://www.epeat.net) potwierdzający spełnienie normy co najmniej Epeat Silver według normy wprowadzonej w 2019 roku - **Wykonawca złoży dokument potwierdzający spełnianie wymogu.** * Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Microsoft Windows Server 2019, Microsoft Windows Server 2022. |
| **Dokumentacja użytkownika** | * Zamawiający wymaga dokumentacji technicznej systemu oraz dokumentacji operacyjnej w języku polskim. Wytworzona lub aktualizowana przez Wykonawcę dokumentacja, w ramach realizacji umowy, powinna zawierać w szczególności instrukcję użytkownika, instrukcję administratora i dokumentację techniczną, w tym parametry konfiguracji sprzętowej. |
| **Warunki gwarancji** | * Zamawiający wymaga zapewnienia gwarancji Producenta z zakresu wdrażanej technologii na okres 3 lata. * Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie i przez Internet. * Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania Producenta, w tym także sprzedanego oprogramowania. * Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy. * Certyfikowany Technik Producenta z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) powinien rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym (NBD) od zakończenia diagnostyki. * Naprawa ma się odbyć w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę. * Zamawiający oczekuje nieodpłatnego udostępnienia narzędzi serwisowych i procesów wsparcia umożliwiających: Wykrywanie usterek sprzętowych z predykcją awarii, automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych, wskazówki dotyczące bezpieczeństwa produktów, samodzielne wysyłanie części, a także ocena bezpieczeństwa cybernetycznego. * Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego. * Możliwość rozszerzenia gwarancji producenta o usługę diagnostyki sprzętu na miejscu w przypadku awarii. Charakterystyka usługi diagnostyki:   + Możliwości utworzenia zgłaszania serwisowego w wyniku, którego proces diagnostyki odbędzie się na miejscu w siedzibie zamawiającego.   + Po przyjeździe do siedziby Zamawiającego, pracownik serwisu przystąpi do rozwiązywania problemu. Jeśli do rozwiązania problemu będzie konieczna dodatkowa pomoc diagnostyczna lub części, pracownik serwisu może w imieniu Zamawiającego skontaktować się z producentem w celu uzyskania pomocy.   + Reakcja na miejscu u Zamawiającego powinna nastąpić w okresie zgodnym z czasem reakcji przypisanym do urządzenia, które posiada wykupioną usługę serwisową.   + Pracownik serwisu powinien skontaktować się z Zamawiającym przed przyjazdem na miejsce w celu sprawdzenia zgłoszenia, ustalenia harmonogramu i potwierdzenia wszelkich informacji niezbędnych do realizacji wizyty technika na miejscu.   + Jeśli w trakcie wstępnego procesu rozwiązywania problemu na miejscu awarii zostanie ustalone, że do realizacji usługi jest niezbędna jakaś część, znajdujący się na miejscu pracownik serwisu zamówi nową część i przekaże dodatkowe zgłoszenie do działu obsługi technicznej. Technik pracujący na miejscu powróci do siedziby Klienta w celu wymiany wysłanej części w ciągu czasu reakcji ustalonego zgodnie z umową serwisową zakupionego produktu. * Wymagane dołączenie do oferty oświadczenia Producenta potwierdzające, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta. * Na dzień złożenia oferty, polityka producenta serwerów nie może ograniczać dostępu do poprawek oprogramowania układowego/systemowego tylko do okresu posiadania gwarancji lub kontraktu serwisowego. |

1. **Komponent serwera – 2 sztuki.**

Karta Dell BOSS PCI-E + 2 x 240GB M.2 SSD do serwerów Zamawiającego Dell PE R640 SN: H946Q53, J946Q53. Zamawiający dopuszcza równoważne rozwiązanie zgodne z serwerami posiadanymi przez Zamawiającego.

1. **Usługa wdrożenia i wsparcia technicznego.**

**Usługa wdrożenia i wsparcia technicznego przez okres 36 miesięcy.**

Zakres usługi:

* + Wdrożenie serwera i przebudowa klastra VMWare
  + Wsparcie techniczne w zakresie platformy sprzętowej IBM, Lenovo, DELL
  + Wsparcie techniczne w zakresie platformy wurtualizacyjnej VMWare
  + Wsparcie techniczne w zakresie system backup Veeam B&R
  + Konsultacje w zakresie konfiguracji
  + Konsultacje w zakresie utrzymania i rozwoju platformy
  + Wsparcie w usuwaniu awarii

Zasady realizacji usługi wsparcia technicznego

* + Usługa realizowana zdalnie
  + Wsparcie w wymiarze minimum 3 godzin miesięcznie
  + Rozliczanie ilości godzin w cyklu 6 miesięcy (niewykorzystane godziny nie przechodzą na kolejny okres)
  + Jednostka rozliczeniowa 0,5h
  + Dostępność usługi do 4h od zgłoszenia