**ZADANIE 2**

**Serwer nr 1**

|  |  |
| --- | --- |
| **Parametr** | **Charakterystyka (wymagania minimalne)** |
| **Obudowa** | * Obudowa Rack o wysokości max 2U z możliwością instalacji min. 12 dysków 3.5” * Obudowa wyposażona 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 56 rdzeniowych. * Płyta główna musi być zaprojektowana przez producenta serwera i   oznaczona jego znakiem firmowym.   * Na płycie głównej powinno znajdować się minimum 32 sloty przeznaczone do instalacji pamięci. * Płyta główna powinna obsługiwać do 8TB pamięci RAM. |
| **Chipset** | * Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych |
| **Procesor** | * Zainstalowane dwa procesory min. 8-rdzeniowe, min. 2.9GHz, klasy x86,   dedykowane do pracy z zaoferowanym serwerem umożliwiające  osiągnięcie wyniku min. 177 w teście SPECrate2017\_int\_base, dostępnym na stronie [www.spec.org](http://www.spec.org/) dla konfiguracji dwuprocesorowej oferowanego serwera lub „rodzinie” serwera tej samej generacji. |
| **RAM** | * Minimum 128GB DDR5 RDIMM 5600MT/s, |
| **Funkcjonalność pamięci**  **RAM** | * Demand Scrubbing, * Patrol Scrubbing, * Permanent Fault Detection (PFD) |
| **Kontroler RAID** | * Sprzętowy kontroler dyskowy, posiadający   + Min. 8GB nieulotnej pamięci cache,   + Możliwość konfiguracji poziomów RAID: 0, 1, 5, 6, 10, 50, 60.   + Wsparcie dla dysków samoszyfrujących |
| **Dyski twarde** | * Zainstalowane:   + 2x dysk SSD vSAS SED o pojemności min. 960GB, Hot-Plug   + 6x dysk SAS o pojemności min. 12TB, Hot-Plug * Zainstalowane dwa dyski M.2 NVMe SSD o pojemności min. 480GB Hot- Plug z możliwością konfiguracji RAID 1. |
| **Gniazda PCI** | * Min. osiem slotów PCIe |

|  |  |
| --- | --- |
| **Interfejsy sieciowe/FC/SAS** | * Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT oraz 4 interfejsy sieciowe 10Gb Ethernet w standardzie BaseT (porty nie   mogą być osiągnięte poprzez karty w slotach PCIe) |
| **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 |
| **System operacyjny/dodatkowe oprogramowanie** | * Windows Server 2022 Standard * 130x licencja Windows Server 2022/2019 Device CALs * 1x licencja Windows Server 2022 RDS Device * Microsoft SQL Server 2022 Standard, OEM, wraz z 5x Device DALs |
| **Bezpieczeństwo** | * Zatrzask górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych. * 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 dynamic 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 opisanymi 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 rozwiązań 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 * Rapport   + 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   + Oferowana platforma musi być zaprojektowana zgodnie ze   standardami:   * + - ISO 27001     - NIST Security and Privacy Controls for Federal Information Systems and Organization     - CSA Cloud Control Matrix |
| **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 w języku polskim lub angi*e*lskim. * Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela. |
| **Warunki gwarancji** | * Zamawiający wymaga zapewnienia gwarancji Producenta z zakresu wdrażanej technologii na okres 5 lat. * Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie, przez Internet oraz z wykorzystaniem aplikacji. |

|  |  |
| --- | --- |
|  | * Zamawiający oczekuje bezpośredniego dostępu do wykwalifikowanej kadry inżynierów technicznych a w przypadku konieczności eskalacji zgłoszenia serwisowego wyznaczonego Kierownika Eskalacji po stronie Producenta (dla krytycznych zgłoszeń serwisowych) * Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania Producenta, w tym także sprzedanego oprogramowania. * Zgłoszenie przyjęte jest potwierdzane przez zespół pomocy technicznej (mail/telefon / aplikacja / portal) przez nadanie unikalnego numeru zgłoszenia pozwalającego na identyfikację zgłoszenia w trakcie realizacji naprawy i po jej zakończeniu. * Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy. * Zamawiający oczekuje rozpoczęcia diagnostyki telefonicznej /   internetowej już w momencie dokonania zgłoszenia. 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 otrzymania zgłoszenia / 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 i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta.   * Firma serwisująca musi posiadać ISO 9001:2015 oraz ISO-27001 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty. |

**Serwer nr 2**

|  |  |
| --- | --- |
| **Parametr** | **Charakterystyka (wymagania minimalne)** |
| **Obudowa** | * Obudowa Rack o wysokości max 2U z możliwością instalacji min. 12 dysków 3.5” * Obudowa wyposażona 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 56 rdzeniowych. * Płyta główna musi być zaprojektowana przez producenta serwera i   oznaczona jego znakiem firmowym.   * Na płycie głównej powinno znajdować się minimum 32 sloty przeznaczone do instalacji pamięci. * Płyta główna powinna obsługiwać do 8TB pamięci RAM. |
| **Chipset** | * Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych |
| **Procesor** | * Zainstalowane dwa procesory min. 8-rdzeniowe, min. 2.9GHz, klasy x86,   dedykowane do pracy z zaoferowanym serwerem umożliwiające  osiągnięcie wyniku min. 177 w teście SPECrate2017\_int\_base, dostępnym na stronie [www.spec.org](http://www.spec.org/) dla konfiguracji dwuprocesorowej oferowanego serwera lub „rodzinie” serwera tej samej generacji. |
| **RAM** | * Minimum 128GB DDR5 RDIMM 5600MT/s, |
| **Funkcjonalność pamięci**  **RAM** | * Demand Scrubbing, * Patrol Scrubbing, * Permanent Fault Detection (PFD) |
| **Kontroler RAID** | * Sprzętowy kontroler dyskowy, posiadający   + Min. 8GB nieulotnej pamięci cache,   + Możliwość konfiguracji poziomów RAID: 0, 1, 5, 6, 10, 50, 60.   + Wsparcie dla dysków samoszyfrujących |
| **Dyski twarde** | * Zainstalowane:   + 2x dysk SSD vSAS SED o pojemności min. 960GB, Hot-Plug   + 6x dysk SAS o pojemności min. 12TB, Hot-Plug * Zainstalowane dwa dyski M.2 NVMe SSD o pojemności min. 480GB Hot- Plug z możliwością konfiguracji RAID 1. |
| **Gniazda PCI** | * Min. osiem slotów PCIe |

|  |  |
| --- | --- |
| **Interfejsy sieciowe/FC/SAS** | * Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT oraz 4 interfejsy sieciowe 10Gb Ethernet w standardzie BaseT (porty nie   mogą być osiągnięte poprzez karty w slotach PCIe) |
| **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 |
| **System operacyjny/dodatkowe**  **oprogramowanie** | * Windows Server 2022 Standard |
| **Bezpieczeństwo** | * Zatrzask górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych. * 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 dynamic 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 opisanymi 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 rozwiązań 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   + Oferowana platforma musi być zaprojektowana zgodnie ze   standardami:   * + - ISO 27001     - NIST Security and Privacy Controls for Federal Information Systems and Organization     - CSA Cloud Control Matrix |
| **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 w języku polskim lub angi*e*lskim. * Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela. |
| **Warunki gwarancji** | * Zamawiający wymaga zapewnienia gwarancji Producenta z zakresu wdrażanej technologii na okres 5 lat. * Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie, przez Internet oraz z wykorzystaniem aplikacji. |

|  |  |
| --- | --- |
|  | * Zamawiający oczekuje bezpośredniego dostępu do wykwalifikowanej kadry inżynierów technicznych a w przypadku konieczności eskalacji zgłoszenia serwisowego wyznaczonego Kierownika Eskalacji po stronie Producenta (dla krytycznych zgłoszeń serwisowych) * Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania Producenta, w tym także sprzedanego oprogramowania. * Zgłoszenie przyjęte jest potwierdzane przez zespół pomocy technicznej (mail/telefon / aplikacja / portal) przez nadanie unikalnego numeru zgłoszenia pozwalającego na identyfikację zgłoszenia w trakcie realizacji naprawy i po jej zakończeniu. * Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy. * Zamawiający oczekuje rozpoczęcia diagnostyki telefonicznej /   internetowej już w momencie dokonania zgłoszenia. 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 otrzymania zgłoszenia / 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 i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta.   * Firma serwisująca musi posiadać ISO 9001:2015 oraz ISO-27001 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty. |