Serwer

Producent: …………………………………….

Model: …………………………………….

Ilość: 1 szt.

|  |  |  |
| --- | --- | --- |
| **Nazwa** | **Wymagane parametry techniczne** | **Oferowane parametry techniczne** |
| **Obudowa** | * Obudowa Rack o wysokości max 1U z możliwością instalacji min. 8 dysków 2,5” wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych oraz organizatorem do kabli.
* 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.
* Płyta główna powinna obsługiwać do 1TB pamięci RAM.
 |  |
| **Chipset** | * Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych.
 |  |
| **Procesor** | * Zainstalowane dwa procesory min. 8-rdzeniowe, min. 2.6GHz, klasy x86 dedykowane do pracy z zaoferowanym serwerem umożliwiające osiągnięcie wyniku min. 165 w teście SPECrate2017\_int\_base, dostępnym na stronie www.spec.org dla konfiguracji dwuprocesorowej.
 |  |
| **RAM** | * Minimum 128GB DDR5 RDIMM 4800MT/s,
* Na płycie głównej powinno znajdować się minimum 16 slotów przeznaczonych do instalacji pamięci.
 |  |
| **Funkcjonalność pamięci RAM** | * Demand Scrubing,
* Patrol Scrubing,
* Permanent Fault Detection
 |  |
| **Gniazda PCI** | * minimum dwa sloty PCIe generacji 4
 |  |
| **Interfejsy sieciowe/FC/SAS** | * Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT oraz 2 interfejsy sieciowe 25Gb Ethernet w standardzie SFP28 (porty nie mogą być osiągnięte poprzez karty w slotach PCIe)
 |  |
| **Dyski twarde** | * Zainstalowane min. 4 dyski SAS o pojemności min. 2,4TB, 12Gb, 2,5“ Hot-Plug.
* Możliwość zainstalowania dwóch dysków M.2 NVMe SSDs o pojemności min. 960GB Hot-Plug z możliwością konfiguracji RAID 1.
 |  |
| **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
 |  |
| **Wbudowane porty** | * 4 x USB z czego nie mniej niż 1x USB 3.0, 2x VGA
 |  |
| **Video** | * Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1920x1200
 |  |
| **Zasilacze** | * Redundantne, Hot-Plug min. 800W każdy.
 |  |
| **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
 |  |
| **System operacyjny** | Zainstalowany na serwerze system operacyjny, kompatybilny z oferowanym serwerem, spełniający nw. wymagania minimalne:1. Możliwość wykorzystania 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym.
2. Możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności do 64TB przez każdy wirtualny serwerowy system operacyjny.
3. Możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania 7000 maszyn wirtualnych.
4. Możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci.
5. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy.
6. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy.
7. Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.
8. Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading.
9. Wbudowane wsparcie instalacji i pracy na wolumenach, które:
	1. pozwalają na zmianę rozmiaru w czasie pracy systemu,
	2. umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,
	3. umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów,
	4. umożliwiają zdefiniowanie list kontroli dostępu (ACL).
10. Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.
11. Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.
12. Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET
13. Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.
14. Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.
15. Dostępne dwa rodzaje graficznego interfejsu użytkownika:
	1. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,
	2. Dotykowy umożliwiający sterowanie dotykiem na monitorach dotykowych.
16. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe,
17. Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji.
18. Mechanizmy logowania w oparciu o:
	1. login i hasło,
	2. karty z certyfikatami (smartcard),
	3. wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM),
19. Możliwość wymuszania wieloelementowej dynamicznej kontroli dostępu dla: określonych grup użytkowników, zastosowanej klasyfikacji danych, centralnych polityk dostępu w sieci, centralnych polityk audytowych oraz narzuconych dla grup użytkowników praw do wykorzystywania szyfrowanych danych.
20. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).
21. Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.
22. Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa.
23. Pochodzący od producenta systemu serwis zarządzania polityką dostępu do informacji w dokumentach (Digital Rights Management).
24. Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach.
25. Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:
	1. Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC,
	2. Usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji:
		1. Podłączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną,
		2. Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,
		3. Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza.
		4. Bezpieczny mechanizm dołączania do domeny uprawnionych użytkowników prywatnych urządzeń mobilnych opartych o iOS i Windows 8.1 i wyższych.
	3. Zdalna dystrybucja oprogramowania na stacje robocze.
	4. Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej.
	5. Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:
		1. dystrybucję certyfikatów poprzez http,
		2. konsolidację CA dla wielu lasów domeny,
		3. automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen,
		4. automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509.
	6. Szyfrowanie plików i folderów.
	7. Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec).
	8. Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów.
	9. Serwis udostępniania stron WWW.
	10. Wsparcie dla protokołu IP w wersji 6 (IPv6),
	11. Wsparcie dla algorytmów Suite B (RFC 4869),
	12. Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows,
	13. Wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie do 1000 aktywnych środowisk wirtualnych systemów operacyjnych. Wirtualne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności. Mechanizmy wirtualizacji mają zapewnić wsparcie dla:
		1. Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych,
		2. Obsługi ramek typu jumbo frames dla maszyn wirtualnych.
		3. Obsługi 4-KB sektorów dysków
		4. Nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra
		5. Możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API.
		6. Możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk mode)
26. Możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta serwerowego systemu operacyjnego umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet.
27. Wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath).
28. Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego.
29. Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.
30. Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF.
31. Zorganizowany system szkoleń i dostępne materiały edukacyjne w języku polskim.

Zaoferowana wraz z serwerem licencja na system operacyjny:1. musi zostać tak dobrana, aby była zgodna z zasadami licencjonowania producenta i pozwalała na legalne używanie na oferowanym serwerze,
2. musi obejmować najnowszą wersję systemu dostępną na dzień składania oferty,
3. musi uprawniać do zainstalowania serwerowego systemu operacyjnego w środowisku fizycznym lub umożliwiać zainstalowanie czterech instancji wirtualnych tego serwerowego systemu operacyjnego,

Do oferty należy załączyć potwierdzenie kompatybilności serwera z oferowanym systemem operacyjnym (wydruk ze strony producenta systemu operacyjnego, dopuszcza się wydruk w języku angielskim). |  |
| **Diagnostyka** | * Możliwość wyposażenia w panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS’u, zasilaniu oraz temperaturze.
 |  |
| **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.
 |  |
| **Certyfikaty** | * Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015, ISO-50001 oraz ISO-14001
* Serwer musi posiadać deklaracja CE.
* Serwer musi spełniać wymagania normy NIST SP 800-193 ochrony przed cyberatakami – załączyć do ofert dokumentację techniczną potwierdzającą spełnienie normy lub oświadczenie producenta serwera o spełnieniu normy.
* 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** | * Min 5 lat gwarancji producenta, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii 24x7x365 poprzez ogólnopolską linię telefoniczną producenta
* 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 wykonawcy (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 wykonawcy / 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.
* 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.
 |  |