|  |  |  |
| --- | --- | --- |
| **Załącznik 3 do SWZ CZĘŚĆ 2**  **OPIS PRZEDMIOTU ZAMÓWIENIA**  **ZAP.271.28.2022.ASK** | | |
| **Asortyment** | **Minimalne parametry wymagane przez Zamawiającego** | **Parametry oferowane przez Wykonawcę (Wypełnia Wykonawca)** |
| **Serwer - typ 1**  **– 1 sztuka** | **Nazwa oferowanego asortymentu spełniającego poniższe wymagania Zamawiającego - należy podać markę oraz model.** |  |
| Obudowa | Obudowa Rack o wysokości max 1U z możliwością instalacji do 4 dysków 3.5" wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie Rack i wysuwanie serwera do celów serwisowych.  Obudowa z możliwością wyposażona 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. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym. |  |
| Chipset | Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych |  |
| Procesor | Zainstalowane dwa procesory min. 8-rdzeniowe, min. 2.8GHz, klasy x86 dedykowany do pracy z zaoferowanym serwerem umożliwiający osiągnięcie wyniku min. 127 punktów w teście SPECrate2017\_int\_base, dostępnym na stronie www.spec.org dla konfiguracji dwuprocesorowej. |  |
| RAM | 64GB DDR4 RDIMM 3200MT/s, na płycie głównej powinno znajdować się minimum 16 slotów przeznaczonych do instalacji pamięci. Płyta główna powinna obsługiwać do 1TB pamięci RAM. |  |
| Funkcjonalność pamięci RAM | Memory Rank Sparing, Failed DIMM isolation, Memory Address Parity Protection, Memory Thermal Throttling |  |
| Gniazda PCI | - minimum dwa sloty PCIe x16 generacji 4 |  |
| Interfejsy sieciowe/FC/SAS | Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie Base-T oraz (porty nie mogą być osiągnięte poprzez karty w slotach PCIe) |  |
| Dyski twarde | Możliwość instalacji dysków SAS, SATA, SSD  Zainstalowane 2 dyski SSD SATA o pojemności min. 480GB, 6Gb, 2,5“ Hot-Plug.  Możliwość zainstalowania dwóch dysków M.2 SATA o pojemności min. 480GB z możliwością konfiguracji RAID 1.  Możliwość zainstalowania dedykowanego modułu dla hypervisora wirtualizacyjnego, wyposażony w 2 nośniki typu flash o pojemności min. 64GB, z możliwością konfiguracji zabezpieczenia synchronizacji pomiędzy nośnikami z poziomu BIOS serwera, rozwiązanie nie może powodować zmniejszenia ilości wnęk na dyski twarde |  |
| System operacyjny/System wirtualizacji | Licencja na serwerowy system operacyjny musi uprawniać do uruchamiania serwerowego systemu operacyjnego w środowisku fizycznym i dwóch wirtualnych środowiskach serwerowego systemu operacyjnego niezależnie od liczby rdzeni w serwerze fizycznym.  Serwerowy system operacyjny musi posiadać następujące, wbudowane cechy:  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:  a. pozwalają na zmianę rozmiaru w czasie pracy systemu,  b. umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików  i folderów,  c. umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów,  d. 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:  a. klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,  b. dotykowy umożliwiający sterowanie dotykiem na monitorach dotykowych.  16. 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:  a. login i hasło,  b. karty z certyfikatami (smartcard),  c. 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:  a. Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC,  b. 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:  I. Podłączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego  z domeną,  II. Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,  III. Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej  z mechanizmu kosza.  IV. Bezpieczny mechanizm dołączania do domeny uprawnionych użytkowników prywatnych urządzeń mobilnych opartych o iOS i Windows 8.1.  c. Zdalna dystrybucja oprogramowania na stacje robocze.  d. Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej  e. Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego umożliwiająca:  I. Dystrybucję certyfikatów poprzez http,  II. Konsolidację CA dla wielu lasów domeny,  III. Automatyczne rejestrowanie certyfikatów pomiędzy różnymi lasami domen,  IV. Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509.  f. Szyfrowanie plików i folderów.  g. Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec).  h. Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów.  i. Serwis udostępniania stron WWW.  j. Wsparcie dla protokołu IP w wersji 6 (IPv6),  k. Wsparcie dla algorytmów Suite B (RFC 4869),  l. Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows,  m. 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:  I. Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych,  II. Obsługi ramek typu jumbo frames dla maszyn wirtualnych.  III. Obsługi 4-KB sektorów dysków  IV. Nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra  V. Możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API.  VI. 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. |  |
| Wbudowane porty | Przednie: min. 1x VGA, min. 1x USB 2.0, min. 1x micro-USB dedykowane dla karty zarządzającej,  Tylne: min. 1x VGA, min. 2x USB w tym 1x USB 3.0, |  |
| Video | Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1600x900 |  |
| Wentylatory | Redundantne |  |
| Zasilacze | Redundantne, Hot-Plug maksymalnie 800W. |  |
| 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 |  |
| Certyfikaty | Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2008 oraz ISO-14001.  Serwer musi posiadać deklaracja CE. Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Microsoft Windows Server 2016, Microsoft Windows Server 2019. |  |
| Warunki gwarancji | 36 miesięczna gwarancja producenta, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii 24x7x365 poprzez ogólnopolską linię telefoniczną producenta.  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 9001:2008 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty.  Wymagane dołączenie do oferty oświadczenia Producenta potwierdzając, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta.  Możliwość rozszerzenia gwarancji przez producenta do 7 lat.  Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji serwera |  |
| Dokumentacja użytkownika | Zamawiający wymaga dokumentacji w języku polskim lub angielskim.  Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela. |  |
| **Przełącznik sieciowy**  **– 1 sztuka** | **Nazwa oferowanego asortymentu spełniającego poniższe wymagania Zamawiającego - należy podać markę oraz model.** |  |
| Interfejs | Min. 48 x 10/100/1000 RJ45 Ports  Min. 4 x 1G SFP Ethernet Ports  Ethernet In-Band |  |
| Blokowanie | 52 Gbps |  |
| Zdolność przełączania | Min. 104 Gbps |  |
| Szybkość przekazywania | Min. 77.30 Mpps |  |
| Zasilanie | 100-240VAC, 50/60 Hz |  |
| Zasilacz | AC/DC, Internal, 240W |  |
| Maksymalne zużycie energii | 45W |  |
| Diody LED | Min. Porty danych RJ45, SFP |  |
| Ochrona ESD/EMP | Air: ± 16 kV, Contact: ± 12 kV |  |
| Wstrząs i wibracje | ETSI300-019-1.4 Standard |  |
| Suma wymiarów | Max. 775 mm |  |
| Waga | Max. 5 kg |  |
| Całkowite dostępne PoE | 195W |  |
| Interfejsy PoE  Porty 1-32 | PoE+ IEEE 802.3af/at |  |
| Maks. Moc PoE na  Port przez PSE  802.3at | 32W |  |
| Gwarancja | Min. 12 miesięcy |  |
| **Oprogramowanie - typ 1 – 1 sztuka** | **Nazwa oferowanego asortymentu spełniającego poniższe wymagania Zamawiającego - należy podać markę oraz model.** |  |
| Wymagania | 1. System monitoringu pomieszczenia serwerowni umożliwiający zdalną kontrolę parametrów środowiskowych i dowolnych czujników binarnych z komunikacją IP.  2. System składa się z centrali, kompletu czujników (1x temperatura, 1x wilgotność, 1x dym), rozdzielacza magistrali 1-Wire/1Wire UNI 1x5, jednostronnego wspornika montażowego 1U do racka oraz zasilacza 12 VDC typu desktop.  3. Centrala musi oferować m.in.:  • komunikację po sieci IP (port LAN, 10/100Mbps)  • podłączenie min. 8 czujników typu 1-Wire / 1-Wire UNI z wykorzystaniem 2 portów RJ11 (np. temperatura, wilgotność, 4-20mA, zalanie, natężenie światła, napięcie, natężenie prądu itp.)  • podłączenie min. 4 czujników binarnych i systemów zewnętrznych wyposażonych w wyjścia NO/NC (np. otwarcie drzwi, dym, zalanie, zanik napięcia, ruch, wstrząs, zbicie szyby, centrala SUG, wyjście z UPS/klimatyzatora itp.)  • podłączenie systemowych akcesoriów konwertujących - rozszerzających możliwości centrali (konwersja 1-Wire UNI/binarne)  • 2 wyjścia przekaźnikowe sterowane ręcznie lub automatycznie na podstawie lokalnie zdefiniowanych reguł lub wirtualnych wyjść urządzeń zdalnych  • 8 wirtualnych wyjść sterujących zdalnymi wyjściami przekaźnikowymi  • zasięg magistrali 1-Wire / 1-Wire UNI dla każdego portu RJ11 min. 60m (całkowita długość wykorzystanego okablowania)  • metalową obudowę o klasie szczelności min. IP40,  • obudowę typu desktop z możliwością instalacji w obudowie Rack 19", na szynie DIN (w różnych pozycjach) lub na panelu za pomocą dodatkowych, oryginalnych akcesoriów montażowych pochodzących od producenta systemu  • możliwość zasilenia czujek albo wprost z portu magistrali, albo z wyjścia typu terminal block umieszczonego na obudowie centrali (wspólne zasilanie z jednego zasilacza systemowego).  • możliwość komunikacji z zewnętrznymi systemami zbierania/przetwarzania danych (oprogramowanie) z wykorzystaniem protokołów SNMP (v1/v3), Modbus/TCP, XML (http/HTTPS), MQTT  • możliwość współpracy z usługą portalu online (nie wymagającym dodatkowych opłat) archiwizującym dane pomiarowe i prezentującym je w formie strony WWW  • możliwość alarmowania na e-mail (min. 5 adresów), SMS (min. 5 numerów telefonów, po podłączeniu bramki SMS poprzez sieć IP)  • możliwość alarmowania za pomocą SNMP trap  • obsługę monitorowania komunikacji przychodzącej od zewnętrznego systemu zbierania/przetwarzania danych dla każdego z wspieranych protokołów SNMP, Modbus/TCP, HTTP  • lokalną pamięć na 250000 wpisów do logowania pomiarów i zdarzeń z możliwością cyklicznego przesyłania zawartości logu na wskazany adres e-mail oraz obsługę Syslog.  • darmowe aktualizacje oprogramowania systemowego (firmware) w całym okresie życia produktu (również po upływie terminu gwarancji)  • zunifikowane oprogramowanie systemowe (firmware) dla wszystkich modeli central w celu zapewnienia jednakowej funkcjonalności (poza różnicami wynikającymi ze sprzętowych różnic pomiędzy poszczególnymi modelami)  • oprogramowanie do wstępnej konfiguracji parametrów interfejsu LAN centrali  • kompatybilność z takimi programami firm trzecich jak: astozi systemONE, Nagios, Axence nVision  4. Czujnik temperatury na kablu 3m zgodny z 1-Wire/1-Wire UNI, 1szt.,  5. Czujnik wilgotności na kablu 3m zgodny z 1-Wire/1-Wire UNI, 1szt.,  6. Czujnik dymu zasilany z napięcia 12VDC, 1szt.,  7. Rozdzielacz magistrali 1-Wire / 1-Wire UNI 1 do 5, 1szt.,  8. Jednostronna półka montażowa 1U wyposażona w otworowanie i śruby umożliwiające montaż centralki producenta systemu w kolorze obudowy centrali,  9. Oprogramowanie HWg-PDMS z licencją na 8 wartości monitorowanych w trybie ciągłym współpracujące z oferowaną centralą,  10. System powinien posiadać gwarancję producenta na min. 2 lata.  11. Temperatura pracy centrali (zakres min.): -30°C do +85°C |  |
| Gwarancja | Min. 24 miesiące |  |
| **Oprogramowanie - typ 2 – 1 sztuka** | **Nazwa oferowanego asortymentu spełniającego poniższe wymagania Zamawiającego - należy podać markę oraz model.** |  |
| Wymagane parametry techniczne | Oferowane rozwiązanie musi znaleźć się w czołówce raportu Gartner Magic Quadrant for Data Center Backup and Reocvery Solutions. Dodatkowo musi znajdować się na liście referencyjnej Gartner https://www.gartner.com/reviews/market/data-center-backup-and-recovery-solutions |  |
| Oprogramowanie musi współpracować z hostami zarządzanymi oraz pojedynczymi hostami. |  |
| Oprogramowanie musi zapewniać tworzenie kopii zapasowych z sieciowych urządzeń plikowych |  |
| Całkowite koszty posiadania | Oprogramowanie musi być niezależne sprzętowo i umożliwiać wykorzystanie dowolnej platformy serwerowej i dyskowej |  |
| Oprogramowanie musi tworzyć “samowystarczalne” archiwa do odzyskania których nie wymagana jest osobna baza danych z metadanymi deduplikowanych bloków |  |
| Oprogramowanie musi pozwalać na tworzenie kopii zapasowych w trybach: Pełny, pełny syntetyczny, przyrostowy i odwrotnie przyrostowy (tzw. reverse-inremental) |  |
| Oprogramowanie musi mieć mechanizmy deduplikacji i kompresji w celu zmniejszenia wielkości archiwów. Włączenie tych mechanizmów nie może skutkować utratą jakichkolwiek funkcjonalności wymienionych w tej specyfikacji |  |
| Oprogramowanie nie może przechowywać danych o deduplikacji w centralnej bazie. Utrata bazy danych używanej przez oprogramowanie nie może prowadzić do utraty możliwości odtworzenia backupu. Metadane deduplikacji muszą być przechowywane w plikach backupu. |  |
| Oprogramowanie musi zapewniać warstwę abstrakcji nad poszczególnymi urządzeniami pamięci masowej, pozwalając utworzyć jedną wirtualną pulę pamięci na kopie zapasowe. Wymagane jest wsparcie dla nieograniczonej liczby pamięci masowych to takiej puli. |  |
| Oprogramowanie musi pozwalać na rozszerzenie lokalnej przestrzeni backupowej poprzez integrację. Proces migracji danych powinien być zautomatyzowany. Jedynie unikalne bloki mogą być przesyłane w celu oszczędności pasma oraz przestrzeni na przechowywane dane. Funkcjonalność ta nie może mieć wpływu na możliwości odtwarzania danych. |  |
| Oprogramowanie nie może instalować żadnych stałych agentów wymagających wdrożenia czy upgradowania wewnątrz maszyny wirtualnej dla jakichkolwiek funkcjonalności backupu lub odtwarzania |  |
| Oprogramowanie musi mieć możliwość uruchamiania dowolnych skryptów przed i po zadaniu backupowym lub przed i po wykonaniu zadania snapshota. |  |
| Oprogramowanie musi oferować portal samoobsługowy, umożliwiający odtwarzanie użytkownikom wirtualnych maszyn |  |
| Oprogramowanie musi zapewniać możliwość delegacji uprawnień do odtwarzania na portalu |  |
| Oprogramowanie musi mieć możliwość integracji z innymi systemami poprzez wbudowane RESTful API |  |
| Oprogramowanie musi mieć wbudowane mechanizmy backupu konfiguracji w celu prostego odtworzenia systemu po całkowitej reinstalacji |  |
| Oprogramowanie musi mieć wbudowane mechanizmy szyfrowania zarówno plików z backupami jak i transmisji sieciowej. Włączenie szyfrowania nie może skutkować utratą jakiejkolwiek funkcjonalności wymienionej w tej specyfikacji |  |
| Oprogramowanie musi posiadać mechanizmy chroniące przed utratą hasła szyfrowania |  |
| Oprogramowanie musi wspierać backup maszyn wirtualnych używających współdzielonych dysków VHDX na Hyper-V (shared VHDX) |  |
| Oprogramowanie musi posiadać architekturę klient/serwer z możliwością instalacji wielu instancji konsoli administracyjnych. |  |
| Wymagania RPO | Oprogramowanie musi wykorzystywać mechanizmy Change Block Tracking na wszystkich wspieranych platformach wirtualizacyjnych. Mechanizmy muszą być certyfikowane przez dostawcę platformy wirtualizacyjnej |  |
| Oprogramowanie musi wykorzystywanać mechnizmy śledzenia zmienionych plików przy zabezpieczaniu udziałów plikowych. |  |
| Oprogramowanie musi oferować możliwość sterowania obciążeniem storage'u produkcyjnego tak aby nie przekraczane były skonfigurowane przez administratora backupu poziomy latencji. Funkcjonalność ta musi być dostępna na wszystkich wspieranych platformach wirtualizacyjnych |  |
| Oprogramowanie musi oferować ten mechanizm z dokładnością do pojedynczego datastoru |  |
| Oprogramowanie musi automatycznie wykrywać i usuwać snapshoty-sieroty (orphaned snapshots), które mogą zakłócić poprawne wykonanie backupu. Proces ten nie może wymagać interakcji administratora |  |
| Oprogramowanie musi zapewniać tworzenie kopii zapasowych z bezpośrednim wykorzystaniem snapshotów macierzowych. Musi też zapewniać odtwarzanie maszyn wirtualnych z takich snapshotów. Proces wykonania kopii zapasowej nie może wymagać użycia jakichkolwiek hostów tymczasowych. |  |
| Oprogramowanie musi wspierać kopiowanie backupów na taśmy wraz z pełnym śledzeniem wirtualnych maszyn |  |
| Oprogramowanie musi posiadać wsparcie dla NDMP |  |
| Oprogramowanie musi mieć możliwość tworzenia retencji GFS (Grandfather-Father-Son) |  |
| Oprogramowanie musi mieć możliwość kopiowania backupów oraz replikacji wirtualnych maszyn z wykorzystaniem wbudowanej akceleracji WAN. |  |
| Oprogramowanie musi mieć możliwość replikacji asynchronicznej włączonych wirtualnych maszyn bezpośrednio z infrastruktury. Dodatkowo oprogramowanie musi mieć możliwość użycia plików kopii zapasowych jako źródła replikacji. |  |
| Oprogramowanie musi mieć możliwość replikacji ciągłej, włączonych wirtualnych maszyn bezpośrednio z infrastruktury. Dla replikacji ciągłej musi być możliwośc zdefiniowania dziennika pozwalającego na odzyskanie danych z dowolnego punku w ramach ustalonego parametru RPO. |  |
| Oprogramowanie musi umożliwiać przechowywanie punktów przywracania dla replik |  |
| Oprogramowanie musi umożliwiać wykorzystanie istniejących w infrastrukturze wirtualnych maszyn jako źródła do dalszej replikacji (replica seeding) |  |
| Oprogramowanie musi wykorzystywać wszystkie oferowane przez hypervisor tryby transportu (sieć, hot-add, LAN Free-SAN) |  |
| Wymagania RTO | Oprogramowanie musi umożliwiać jednoczesne uruchomienie wielu maszyn wirtualnych bezpośrednio ze zdeduplikowanego i skompresowanego pliku backupu, z dowolnego punktu przywracania, bez potrzeby kopiowania jej na storage produkcyjny. Funkcjonalność musi być oferowana dla środowisk niezależnie od rodzaju storage’u użytego do przechowywania kopii zapasowych. |  |
| Oprogramowanie musi pozwalać na migrację on-line tak uruchomionych maszyn na storage produkcyjny. Migracja powinna odbywać się mechanizmami wbudowanymi w hypervisor. Jeżeli licencja na hypervisor nie posiada takich funkcjonalności - oprogramowanie musi realizować taką migrację swoimi mechanizmami |  |
| Oprogramowanie musi pozwalać na zaprezentowanie pojedynczego dysku bezpośrednio z kopii zapasowej do wybranej działającej maszyny wirtualnej |  |
| Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny, plików konfiguracji i dysków |  |
| Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny. |  |
| Oprogramowanie musi umożliwić odtworzenie plików na maszynę operatora, lub na serwer produkcyjny bez potrzeby użycia agenta instalowanego wewnątrz wirtualnej maszyny. Funkcjonalność ta nie powinna być ograniczona wielkością i liczbą przywracanych plików |  |
| Oprogramowanie musi mieć możliwość odtworzenia plików bezpośrednio do maszyny wirtualnej poprzez sieć |  |
| Oprogramowanie musi wspierać odtwarzanie pojedynczych plików z następujących systemów plików:  o    Linux: ext2, ext3, ext4, ReiserFS, JFS, XFS, Btrfs  o    BSD: UFS, UFS2  o    Solaris: ZFS, UFS  o    Mac: HFS, HFS+  o    Windows: NTFS, FAT, FAT32, ReFS  o    Novell OES: NSS |  |
| Oprogramowanie musi wspierać przywracanie plików z partycji |  |
| Oprogramowanie musi umożliwiać szybkie granularne odtwarzanie obiektów aplikacji bez użycia jakiegokolwiek agenta zainstalowanego wewnątrz maszyny wirtualnej. |  |
| Oprogramowanie musi wspierać granularne odtwarzanie obiektów Active Directory takich jak konta komputerów, konta użytkowników oraz pozwalać na odtworzenie haseł. |  |
| Oprogramowanie musi wspierać granularne odtwarzanie dowolnych atrybutów, rekordów DNS zintegrowanych z AD |  |
| Oprogramowanie musi wspierać przywracanie danych do oryginalnego środowiska |  |
| Oprogramowanie musi wspierać odtworzenie point-in-time wraz z możliwością przywrócenia bazy do oryginalnego środowiska |  |
| Oprogramowanie musi wspierać także specyficzne metody odtwarzania w tym "reverse CBT" oraz odtwarzanie z wykorzystaniem sieci SAN |  |
| Ograniczenie ryzyka | Oprogramowanie musi dawać możliwość stworzenia laboratorium (izolowane środowisko) używając wirtualnych maszyn uruchamianych bezpośrednio z plików backupu. |  |
| Oprogramowanie musi pozwalać na uruchomienie takiego środowiska bezpośrednio ze snapshotów macierzowych stworzonych na wspieranych urządzeniach. |  |
| Oprogramowanie musi umożliwiać weryfikację odtwarzalności wielu wirtualnych maszyn jednocześnie z dowolnego backupu według własnego harmonogramu w izolowanym środowisku. Testy powinny uwzględniać możliwość uruchomienia dowolnego skryptu testującego również aplikację uruchomioną na wirtualnej maszynie. Testy muszą być przeprowadzone bez interakcji z administratorem |  |
| Oprogramowanie musi umożliwiać integrację z oprogramowaniem antywirusowym w celu wykonania skanu zawartości pliku backupowego przed odtworzeniem jakichkolwiek danych. |  |
| Oprogramowanie musi umożliwiać dwuetapowe, automatyczne, odtwarzanie maszyn wirtualnych z możliwością wstrzyknięcia dowolnego skryptu przed odtworzeniem danych do środowiska produkcyjnego. |  |
| Monitoring | System musi zapewnić możliwość monitorowania środowiska wirtualizacyjnego bez potrzeby korzystania z narzędzi firm trzecich |  |
| System musi umożliwiać kategoryzacje obiektów infrastruktury wirtualnej |  |
| System musi umożliwiać tworzenie alarmów dla całych grup wirtualnych maszyn jak i pojedynczych wirtualnych maszyn |  |
| System musi dawać możliwość układania terminarza raportów i wysyłania tych raportów przy pomocy poczty elektronicznej w formacie HTML oraz Excel |  |
| System musi dawać możliwość podłączenia się do kilku instancji jednocześnie, w celu centralnego monitorowania wielu środowisk |  |
| System musi mieć wbudowane predefiniowane zestawy alarmów wraz z możliwością tworzenia własnych alarmów i zdarzeń przez administratora |  |
| System musi mieć wbudowane połączenie z bazą wiedzy opisującą problemy z predefiniowanych alarmów |  |
| System musi mieć centralną konsolę z sumarycznym podglądem wszystkich obiektów infrastruktury wirtualnej |  |
| System musi mieć możliwość monitorowania platformy sprzętowej, na której jest zainstalowana infrastruktura wirtualna |  |
| System musi zapewnić możliwość podłączenia się do wirtualnej maszyny (tryb konsoli) bezpośrednio z narzędzia monitorującego |  |
| System musi mieć możliwość integracji z oprogramowaniem do tworzenia kopii zapasowych tego samego producenta |  |
| System musi mieć możliwość monitorowania obciążenia serwerów backupowych, ilości zabezpieczanych danych oraz statusu zadań kopii zapasowych, replikacji oraz weryfikacji odzyskiwalności maszyn wirtualnych. |  |
| System musi oferować inteligentną diagnostykę rozwiązania backupowego poprzez monitorowanie logów celem wykrycia znanych problemów oraz błędów konfiguracyjnych w celu wskazania rozwiązania bez potrzeby otwierania zgłoszenia suportowego oraz bez potrzeby wysyłania jakichkolwiek danych diagnostycznych do producenta oprogramowania backupu. |  |
| System musi mieć możliwość granularnego monitorowania infrastruktury, zależnego od uprawnień nadanym użytkownikom. |  |
| System musi mieć możliwość monitorowania instancji |  |
| Raportowanie | System raportowania musi umożliwić tworzenie raportów z infrastruktury wirtualnej |  |
| System musi wspierać wiele instancji jednocześnie bez konieczności instalowania dodatkowych modułów. |  |
| System musi być systemem bezagentowym. Nie dopuszcza się możliwości instalowania przez system agentów na monitorowanych hostach |  |
| System musi mieć możliwość eksportowania raportów. |  |
| System musi mieć możliwość ustawienia harmonogramu kolekcji danych z monitorowanych systemów jak również możliwość tworzenia zadań kolekcjonowania danych ad-hoc |  |
| System musi mieć możliwość ustawienia harmonogramu generowania raportów i dostarczania ich do odbiorców w określonych przez administratora interwałach |  |
| System w raportach musi mieć możliwość uwzględniania informacji o zmianach konfiguracji monitorowanych systemów |  |
| System musi mieć możliwość generowania raportów z dowolnego punktu w czasie zakładając, że informacje z tego czasu nie zostały usunięte z bazy danych |  |
| System musi posiadać predefiniowane szablony z możliwością tworzenia nowych jak i modyfikacji wbudowanych |  |
| System musi mieć możliwość analizowania „przeszacowanych” wirtualnych maszyn wraz z sugestią zmian w celu optymalnego wykorzystania fizycznej infrastruktury |  |
| System musi mieć możliwość generowania raportów na podstawie danych uzyskanych z oprogramowania do tworzenia kopii zapasowych tego samego producenta |  |
| System musi mieć możliwość generowania raportu dotyczącego zabezpieczanych maszyn, zdefiniowanych zadań tworzenia kopii zapasowych oraz replikacji jak również wykorzystania zasobów serwerów backupowych. |  |
| System musi mieć możliwość generowania raportu planowania pojemności (capacity planning) bazującego na scenariuszach ‘what-if’. |  |
| System musi mieć możliwość granularnego raportowania infrastruktury, zależnego od uprawnień nadanym użytkownikom dla platformy |  |
| System musi mieć możliwość generowania raportów dotyczących tzw. migawek-sierot (orphaned snapshots) |  |
| System musi mieć możliwość generowania personalizowanych raportów zawierających informacje z dowolnych predefiniowanych raportów w pojedynczym dokumencie |  |
| Gwarancja | Licencja na minimum 12 miesięcy |  |
| **Serwer - typ 2**  **– 1 sztuka** | **Nazwa oferowanego asortymentu spełniającego poniższe wymagania Zamawiającego - należy podać markę oraz model.** |  |
| Obudowa | Obudowa typu Tower z możliwością instalacji do 4 dysków twardych 3,5”. |  |
| Płyta główna | Z możliwością instalacji jednego fizycznego procesora, posiadająca minimum 4 sloty na pamięć RAM UDIMM z możliwością zainstalowania do minimum 128GB pamięci RAM, możliwe zabezpieczenia pamięci: ECC. Płyta główna zaprojektowana przez producenta serwera i oznaczona trwale jego znakiem firmowym. |  |
| Procesor | Zainstalowany jeden procesor 4-rdzeniowy klasy x86 dedykowany do pracy z zaoferowanym serwerem min. 2,8GHz, 8MB pamięci cache, 65W umożliwiający osiągnięcie wyniku min. 8000 w teście Average CPU Mark dostępnym na stronie <https://www.cpubenchmark.net/>. |  |
| Pamięć RAM | 16 GB pamięci RAM UDIMM o częstotliwości taktowania minimum 3200MHz |  |
| Sloty PCI Express | Funkcjonujące sloty PCI Express: - minimum 4 sloty PCI Express w tym przynajmniej 2 sloty Gen4 |  |
| Interfejsy sieciowe/FC/SAS | Minimum dwa interfejsy sieciowe 1Gb/s Ethernet nie zajmujące żadnego z dostępnych slotów PCI Express. |  |
| Dyski twarde | Możliwość instalacji dysków twardych 3,5” typu: SATA, NearLine SAS, SAS, SSD.  Zainstalowany 1 dysk SATA o pojemności min. 2TB, 3.5”  Możliwość instalacji dwóch dysków M.2 SATA o pojemności min. 480GB oraz możliwość konfiguracji w RAID1. |  |
| System operacyjny | Licencja na serwerowy system operacyjny musi uprawniać do uruchamiania serwerowego systemu operacyjnego w środowisku fizycznym i dwóch wirtualnych środowiskach serwerowego systemu operacyjnego niezależnie od liczby rdzeni w serwerze fizycznym.  Serwerowy system operacyjny musi posiadać następujące, wbudowane cechy:  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:  a. pozwalają na zmianę rozmiaru w czasie pracy systemu,  b. umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików  i folderów,  c. umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów,  d. 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:  a. klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,  b. dotykowy umożliwiający sterowanie dotykiem na monitorach dotykowych.  16. 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:  a. login i hasło,  b. karty z certyfikatami (smartcard),  c. 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:  a. Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC,  b. 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:  I. Podłączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego  z domeną,  II. Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,  III. Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej  z mechanizmu kosza.  IV. Bezpieczny mechanizm dołączania do domeny uprawnionych użytkowników prywatnych urządzeń mobilnych opartych o iOS i Windows 8.1.  c. Zdalna dystrybucja oprogramowania na stacje robocze.  d. Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej  e. Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego umożliwiająca:  I. Dystrybucję certyfikatów poprzez http,  II. Konsolidację CA dla wielu lasów domeny,  III. Automatyczne rejestrowanie certyfikatów pomiędzy różnymi lasami domen,  IV. Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509.  f. Szyfrowanie plików i folderów.  g. Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec).  h. Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów.  i. Serwis udostępniania stron WWW.  j. Wsparcie dla protokołu IP w wersji 6 (IPv6),  k. Wsparcie dla algorytmów Suite B (RFC 4869),  l. Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows,  m. 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:  I. Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych,  II. Obsługi ramek typu jumbo frames dla maszyn wirtualnych.  III. Obsługi 4-KB sektorów dysków  IV. Nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra  V. Możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API.  VI. 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. |  |
| Wbudowane porty | Minimum 8 portów USB z czego min. 1 w technologii 3.0  1x RS-232  1x VGA |  |
| Video | Zintegrowana karta graficzna, umożliwiająca wyświetlanie obrazu w rozdzielczości minimum 1280x1024 pikseli |  |
| Chłodzenie i zasilanie | Wentylator, zasilacz o mocy minimum 300W wraz z kablami zasilającymi. |  |
| 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 |  |
| Warunki gwarancji | 36 miesięcy gwarancji producenta, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii 24x7x365 poprzez ogólnopolską linię telefoniczną producenta.  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 9001:2008 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty.  Wymagane dołączenie do oferty oświadczenia Producenta potwierdzając, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta.  Możliwość rozszerzenia gwarancji przez producenta do 7 lat.  Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji serwera |  |
| Certyfikaty | Serwer musi być wyprodukowany zgodnie z normą ISO-9001 oraz ISO-14001 (dokumenty załączyć do oferty) Serwer musi posiadać deklaracja CE (dokument załączyć do oferty  Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Microsoft Windows Server 2019 i Microsoft Windows Server 2022 |  |