Załącznik nr 1

**Opis Przedmiotu Zamówienia**

**Przedmiotem zamówienia jest dostawa infrastruktury serwerowej wraz z oprogramowaniem, usługą wdrożenia oraz szkoleniem.**

**ZADANIE 1 - MACIERZ DYSKOWA (1 SZTUKA)**

|  |  |  |  |
| --- | --- | --- | --- |
| **Lp.** | **Komponent** | **Minimalne wymagania** | **Potwierdzenie spełnienia wymagań przez oferowane produkty (skreślić TAK i wpisać NIE, jeżeli nie spełnia minimalnych wymagań), podać dane we wskazanych miejscach** |
| 1 | Zasoby dyskowe | 1. Macierz dyskowa musi być dostarczona z minimum:  1) 25 dyskami SSD 2,5” o pojemności minimum 3,84TB (w przypadku zastosowania dysków o DWPD mniejszym od 3, należy dostarczyć dwukrotnie większą pojemność na dyskach SSD),  2) zaoferowana konfiguracja powinna osiągać minimum 110000 IOPS przy operacjach blokiem 8kB i w stosunku operacji R/W 20/80. Do oferty należy dołączyć plik z aktualnym na dzień składania oferty wydrukiem z narzędzia producenta potwierdzający osiągnięty wynik.  2. Macierz dyskowa musi być dedykowana do obsługi tylko dysków SSD lub NVMe  3. Kontrolery macierzy dyskowej muszą obsługiwać minimum 450 dysków oraz pojemność surową minimum 4PB. Macierz musi mieć możliwość rozbudowy on-line do konfiguracji obsługującej minimum 750 dysków.  4. Należy dodatkowo dostarczyć dyski zapasowe lub pojemność zapasową w ilości zgodnej z zaleceniami producenta dla oferowanej konfiguracji – nie mniej niż 1 zapasowy dysk lub jego pojemność na 30 dysków danego typu.  5. Podczas awarii dysku kontroler macierzy dyskowej musi automatycznie rozpoczynać odtwarzanie danych na fizycznym dysku zapasowym lub pojemności zapasowej.  6. W przypadku stosowania dysku zapasowego proces odtwarzania danych nie może wiązać się z procesem przenoszenia danych po wymianie dysku uszkodzonego (dysk wymieniony musi być automatycznie uznany za zapasowy). | Producent oferowanej macierzy: …  Model oferowanej macierzy: …  TAK |
| 2 | Kontrolery macierzy dyskowej | 1. Macierz dyskowa musi być złożona z minimum jednej pary identycznych kontrolerów tworzących klaster wysokiej dostępności (high availability cluster). Kontrolery muszą udostępniać dane poprzez iSCSI, FCP, CIFS oraz NFS bez stosowania żadnych dodatkowych komponentów programowych lub fizycznych.  2. Obszar pamięci cache przeznaczony do zapisów danych, musi posiadać lustrzaną kopię (ang. mirror).  3. W przypadku awarii zasilania dane nie zapisane na dyskach muszą być zabezpieczone za pomocą podtrzymania bateryjnego przez minimum 72 godziny lub zachowane w pamięci nieulotnej kontrolera do momentu przywrócenia zasilania.  4. Kontrolery w klastrze wysokiej dostępności muszą oferować funkcjonalność automatycznego przejmowania funkcjonalności i zadań w przypadku awarii drugiego kontrolera w tej samej parze.  5. Każdy kontroler macierzy powinien posiadać procesory o minimalnej łącznej ilości rdzeni wynoszącej 16. Z uwagi na konieczność zachowania kompatybilności obliczeniowej w środowisku akceptowane będą jedynie rozwiązania wyposażone w procesory firmy Intel oparte o architekturę x86.  6. Macierz musi mieć minimum 192GB pamięci cache obsługującej zapis i odczyt dostępnej dla wszystkich wolumenów macierzy. Włączenie lub wyłączenie pamięci cache nie może wymagać operacji usunięcia i utworzenia na nowo wolumenów lub grup dyskowych.  7. Macierz musi mieć możliwość obsługi różnych poziomów RAID równocześnie. Minimum RAID 1 (lub 10), 5, 6. Macierz musi umożliwiać konstrukcję urządzenia LUN w taki sposób, aby zawierał dane zabezpieczone poziomami RAID 1 (lub 10), RAID 5, RAID 6 jednocześnie.  8. Awaria dowolnego pojedynczego aktywnego elementu macierzy dyskowej nie może powodować przerwy w dostępie do danych.  9. Musi być możliwe utworzenie minimum 1000 wolumenów blokowych o rozmiarze minimum 256TB, plikowych o rozmiarze minimum 256TB.  10. Macierz musi posiadać wbudowaną funkcjonalność typu thin provisioning umożliwiającą alokację wirtualnej przestrzeni dyskowej, do której fizyczne dyski mogą być dostarczone w przyszłości. | TAK |
| 3 | Interfejsy | 1. Macierz musi być wyposażona w następujące działające porty:  1) 8 portów 10 Gb SFP+ do podłączania hostów,  2) 8 portów FC 32Gb do podłączania hostów – porty muszą być obsadzone odpowiednimi wkładkami SFP+ SR,  3) 2 porty 1GbE Base-T do zdalnego zarządzania kontrolerem,  4) 4 porty SAS minimum 12Gbs do podłączania półek dyskowych.  2. Porty przeznaczone do podłączenia hostów nie mogą być wykorzystane do połączeń wewnątrz macierzy (np. pomiędzy kontrolerami).  3. Musi być możliwość rozbudowy on-line macierzy do minimum 24 portów o przepustowości 25 Gbps lub 16 portów FC o przepustowości 32Gbps jedynie poprzez instalację dodatkowych kart rozszerzeń bez konieczności instalacji dodatkowych kontrolerów (dodatkowe karty rozszerzeń nie są przedmiotem tego postępowania). | TAK |
| 4 | Kopie migawkowe | 1. System operacyjny macierzy dyskowej musi natywnie obsługiwać mechanizm kopii migawkowych, który będzie dostępny dla wszystkich rodzajów danych udostępnianych. Niedopuszczalne są rozwiązania wykonujące kopie migawkowe jedynie w trybie Copy On Write dla dowolnego rodzaju danych (blokowe lub plikowe). Licencja na wszystkie opisane funkcjonalności musi obejmować całą powierzchnię użytkową macierzy.  2. Odtwarzanie plików i folderów z kopii migawkowych wykonanych dla wolumenów plikowych udostępnionych dla systemów typu Windows i Unix musi być dostępne za pomocą wydzielonego udziału sieciowego z zachowaniem praw dostępu na poziomie użytkownika.  3. System operacyjny macierzy dyskowej zapewnia wykonywanie kopii migawkowych wolumenów plikowych w trybie on-line, bez zatrzymywania operacji odczytu i zapisu. Deklarowana przez producenta liczba kopii migawkowych musi wynosić minimum 256 na wolumen.  4. Musi być możliwe odtwarzanie danych z kopii migawkowych bezpośrednio na wolumen produkcyjny.  5. Musi być możliwe zaprezentowanie kopii migawkowej w trybie do odczytu i zapisu. | TAK |
| 5 | Obsługiwane protokoły | 1.System operacyjny macierzy dyskowej musi udostępniać dane za pomocą protokołu CIFS i FCP - jeśli do uruchomienia potrzebna jest licencja to zamawiający wymaga jej dostarczenia w ramach zaoferowanej ceny. System operacyjny macierzy dyskowej musi mieć możliwość uruchomienia udostępniania danych za pomocą protokołów NFS oraz iSCSI - licencje na protokoły CIFS, NFS, FCP oraz iSCSI są przedmiotem obecnego postępowania.  2. Jednoczesna obsługa różnych protokołów dostępu do danych nie może być zrealizowana za pomocą dodatkowego oprogramowania ani dodatkowych urządzeń pośredniczących typu wirtualizator, gateway, switch, etc. firm trzecich. | TAK |
| 6 | Pozostałe wymagania | 1. System operacyjny macierzy dyskowej musi umożliwiać dynamiczną zmianę rozmiaru wolumenów danych (zwiększanie) bez przerywania pracy i bez przerywania użytkownikom zewnętrznym dostępu do danych  2. Musi być możliwość konfiguracji macierzy dyskowej za pomocą GUI, zbieranie i wyświetlanie informacji o stanie zasobów macierzy dyskowej, prezentowanie i gromadzenie zdarzeń zachodzących w macierzy dyskowej oraz prezentowanie bieżących statystyk wydajnościowych macierzy dyskowej, podgląd parametrów wydajnościowych macierzy dyskowej w czasie rzeczywistym.  3. Dostęp do CLI systemu operacyjnego kontrolerów musi odbywać się przy użyciu połączenia szyfrowanego.  4. W systemie operacyjnym kontrolera musi być możliwość utworzenia wirtualnych serwerów plików, a każdy wirtualny serwer plików musi obsługiwać użytkowników z innej domeny Microsoft (MS Active Directory).  5. W celu zabezpieczania danych macierz dyskowa musi mieć możliwość replikacji jej zasobów na zasoby innej macierzy tej samej rodziny. Replikacja musi działać na poziomie systemu operacyjnego macierzy. Macierz musi mieć możliwość replikacji w trybie synchronicznym i asynchronicznym bez potrzeby użycia urządzeń zewnętrznych typu gateway, serwer pośredniczący, etc. Musi istnieć możliwość odwrócenia kierunku replikacji. Replikacja danych między macierzami nie może być zrealizowana zewnętrznym narzędziem software'owym. Licencja na replikację jest przedmiotem obecnego postępowania.  6. System operacyjny kontrolerów macierzy musi oferować funkcjonalność QoS (Quality of Service) dla dowolnego wolumenu blokowego, to znaczy musi być możliwość ograniczenia liczby operacji na sekundę lub przepustowości w kB (lub analogicznych jednostkach) na sekundę, jaka jest możliwa do uzyskania ze wskazanego przez administratora wolumenu. | TAK |
| 7 | Gwarancja | 1. Minimum 60 miesięcy gwarancji realizowanej w miejscu instalacji sprzętu, z czasem reakcji on-site do 4 godzin od przyjęcia zgłoszenia.  2. Możliwość zgłaszania awarii w trybie 365x7x24 poprzez ogólnopolską linię telefoniczną producenta.  3. Stałe monitorowanie macierzy przez zdalne centrum serwisowe.  4. Zamawiający wymaga od Wykonawcy dołączenia do oferty oświadczenia podmiotu realizującego serwis lub Producenta sprzętu, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego.  5. Wymagane dołączenie do oferty oświadczenia Producenta potwierdzającego, że serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta.  6. Oświadczenie producenta macierzy, potwierdzające, że sprzęt pochodzi z oficjalnego kanału dystrybucyjnego producenta. | TAK |
| 8 | Wymiana dysków | Wymiana dysków może być dokonywana przez Zamawiającego. Zamawiający zatrzymuje uszkodzone dyski. | TAK |
| 9 | Parametry dodatkowo punktowane | 1. Oprogramowanie do wykonywania kopii bezpieczeństwa. (Waga: 10 pkt)  Rozwiązanie posiada zintegrowane oprogramowanie do wykonywania spójnych kopii danych aplikacji: Exchange, SQL Server, Oracle, VMware dla blokowych i plikowych datastore.  Spójne kopie rozumiane jako funkcjonalność automatycznego przełączenia aplikacji w tryb wykonania spójnej kopii swoich danych.  Oprogramowanie to musi rozpoznać na których wolumenach logicznych aplikacja składuje swoje dane i wykonać kopie tylko tych wolumenów.  2. Szyfrowanie danych na dyskach. (Waga: 10 pkt)  Rozwiązanie posiada mechanizm umożliwiający szyfrowanie danych na dyskach. Należy dostarczyć niezbędne licencje na całą pojemność macierzy.  3. Rozbudowa pamięci cache. (Waga: 10 pkt)  Oferowane rozwiązanie posiada możliwość rozbudowania pamięci cache wspierającej odczyty o dedykowane dyski półprzewodnikowe, które pozwolą na rozbudowę do wartości minimum 1,2 TB. Jeżeli funkcjonalność wymaga zastosowania dodatkowej licencji to należy ją od razu uwzględnić na wskazanej wartości – dając możliwość Zamawiającemu na łatwiejszy proces rozbudowy w przyszłości.  4. W przypadku zaoferowania ww. funkcjonalności w pkt. 1-3 Wykonawca zapewni je w ramach zaoferowanej ceny, bez konieczności ponoszenia dodatkowych kosztów przez Zamawiającego | (zaznaczyć TAK albo NIE)  Ad 1 TAK/NIE  Ad 2 TAK/NIE  Ad 3 TAK/NIE  Ad 4 TAK |

**ZADANIE 2 – SERWER TYPU I (2 SZTUKI)**

|  |  |  |  |
| --- | --- | --- | --- |
| **Lp.** | **Komponent** | **Minimalne wymagania** | **Potwierdzenie spełnienia wymagań przez oferowane produkty (skreślić TAK i wpisać NIE, jeżeli nie spełnia minimalnych wymagań), podać dane we wskazanych miejscach** |
| 1 | Obudowa | 1. Obudowa Rack o wysokości max. 1U, umożliwiająca instalację min. 10 dysków 2,5” z kompletem wysuwanych szyn umożliwiających montaż w szafie Rack i wysuwanie serwera do celów serwisowych.  2. Obudowa wyposażona w kartę umożliwiającą dostęp bezpośredni poprzez urządzenia mobilne - serwer musi posiadać możliwość konfiguracji oraz monitoringu najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej (Android/ Apple iOS) przy użyciu jednego z protokołów BLE/ WIFI. | Producent oferowanych serwerów: …  Model oferowanych serwerów: …  TAK |
| 2 | Płyta główna | Płyta główna z możliwością zainstalowania dwóch procesorów. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym. | TAK |
| 3 | Chipset | Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych | TAK |
| 4 | Procesor | Zainstalowany jeden procesor min. szesnasto-rdzeniowy klasy x86 do pracy z zaoferowanym serwerem umożliwiający osiągnięcie wyniku min. 384 punktów w teście SPECrate2017\_int\_base dostępnym na stronie www.spec.org dla dwóch procesorów. | Podać producenta i model: …  TAK |
| 5 | Pamięć RAM | Minimum 512GB DDR4 RDIMM 4800MT/s. Na płycie głównej powinno znajdować się minimum 32 slotów przeznaczonych do instalacji pamięci. Płyta główna powinna obsługiwać do 8TB pamięci RAM. | TAK |
| 6 | Zabezpieczenia pamięci RAM | Demand Scrubbing, Patrol Scrubbing, Permanent Fault Detection | TAK |
| 7 | Gniazda PCIe | Minimum dwa sloty PCIe x8 generacji 5 i jeden slot PCIe x16 generacji 4 | TAK |
| 8 | Interfejsy sieciowe/FC/SAS | 1. Dwa interfejsy sieciowe 25Gb Ethernet ze złączami SFP28 (nie mogą zajmować gniazd PCIe zdefiniowanych w pkt 7)  2. Możliwość instalacji wymiennie modułów udostępniających:  1) dwa interfejsy sieciowe 10Gb Ethernet w standardzie SFP+,  2) dwa interfejsy sieciowe 10Gb Ethernet w standardzie BaseT,  3) cztery interfejsy sieciowe 10Gb Ethernet w standardzie SFP+,  4) cztery interfejsy sieciowe 1Gb Ethernet w standardzie BaseT,  5) cztery interfejsy sieciowe 25Gb Ethernet ze złączami SFP28.  3. Wbudowane dwa interfejsy sieciowe 1Gb Ethernet w standardzie BaseT.  4. Dodatkowo zainstalowane:  1) jedna karta dwuportowa 25Gb Ethernet ze złączami SFP28,  2) dwie karty dwuportowe FC 32Gb/s. | TAK |
| 9 | Dyski twarde | 1. Możliwość instalacji dysków SAS/SATA  2. Zainstalowane 2 dyski min. 960GB vSAS SED SSD 12Gb/s, DWPD min. 3.  3. Możliwość instalacji dwóch dysków hot-swap M.2 NVMe o pojemności min. 480GB z możliwością konfiguracji RAID 1. | TAK |
| 10 | Kontroler RAID | Sprzętowy kontroler dyskowy z pojemnością cache 8GB. Możliwe konfiguracje poziomów RAID: 0,1,5,6,10,50,60, non-RAID (JBOD). | TAK |
| 11 | Wbudowane porty | Minimum port USB 2.0 oraz port USB 3.0, port VGA | TAK |
| 12 | Video | Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1600x900 | TAK |
| 13 | Wentylatory | Redundantne Hot-Plug | TAK |
| 14 | Zasilacze | Minimum dwa zasilacze Hot-Plug min. 1100W Titanium. | TAK |
| 15 | Karta zarządzania | 1. Niezależna karta zarządzająca od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port RJ-45 Gigabit Ethernet umożliwiająca:  1) zdalny dostęp do graficznego interfejsu Web karty zarządzającej,  2) szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika,  3) podmontowanie zdalnych wirtualnych napędów,  4) wirtualną konsolę z dostępem do myszy, klawiatury,  5) wsparcie dla IPv6,  6) wsparcie dla SNMP; IPMI2.0, VLAN tagging, SSH,  7) zdalne monitorowanie w czasie rzeczywistym poboru prądu przez serwer, dane historyczne powinny być dostępne przez min. 7 dni wstecz,  8) zdalne ustawienie limitu poboru prądu przez konkretny serwer,  9) integrację z Active Directory,  10) obsługę przez czterech administratorów jednocześnie,  11) wsparcie dla automatycznej rejestracji DNS,  12) wsparcie dla LLDP,  13) wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej,  14) podłączenie lokalne poprzez złącze RS-232,  15) zarządzanie bezpośrednio poprzez złącze microUSB umieszczone na froncie obudowy,  16) monitorowanie zużycia dysków SSD,  17) monitorowanie z jednej konsoli min. 20 serwerów fizycznych,  18) automatyczne zgłaszanie alertów do centrum serwisowego producenta,  19) automatyczny update firmware dla wszystkich komponentów serwera,  20) przywrócenie poprzednich wersji firmware,  21) eksport/import konfiguracji (ustawienie karty zarządzającej, BIOSu, kart sieciowych, HBA oraz konfiguracji kontrolera RAID) serwera do pliku XML lub JSON,  22) zaimportowanie ustawień poprzez bezpośrednie podłączenie plików konfiguracyjnych,  23) automatyczne tworzenie kopii ustawień serwera w oparciu o harmonogram,  24) wykrywanie odchyleń konfiguracji na poziomie konfiguracji UEFI oraz wersji firmware serwera.  2. Karta powinna posiadać możliwość uruchomienia dodatkowych poniższych funkcjonalności:  1) kontrola stanu BIOS pod kątem naruszenia integralności oprogramowania,  2) automatyczne odświeżanie certyfikatów SSL,  3) wykorzystanie tokenu lub aplikacji SecurID do uwierzytelniania wielkoskładnikowego przy logowaniu do karty zarządzającej,  4) modyfikacja reguł chłodzenia kart w slotach PCIe, z możliwością własnych ustawień,  5) ustawienia limitu temperatury powietrza wychodzącego z serwera,  6) ustawienia dopuszczalnego wzrostu temperatury powietrza przepływającego przez serwer,  7) ustawienia maksymalnej temperatury powietrza dochodzącego do slotów PCIe,  8) monitorowanie przepływu powietrza na bieżąco. | TAK |
| 16 | Oprogramowanie do zarządzania | Zainstalowane oprogramowanie producenta do zarządzania, spełniające poniższe wymagania:  1) wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych,  2) integracja z Active Directory,  3) możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta,  4) wsparcie dla protokołów SNMP, IPMI, Linux SSH, Redfish,  5) możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram  6) szczegółowy opis wykrytych systemów oraz ich komponentów  7) możliwość eksportu raportu do CSV, HTML, XLS, PDF  8) możliwość tworzenia własnych raportów w oparciu o wszystkie informacje zawarte w inwentarzu.  9) grupowanie urządzeń w oparciu o kryteria użytkownika  10) tworzenie automatycznie grup urządzeń w oparciu o dowolny element konfiguracji serwera np. nazwa, lokalizacja, system operacyjny, obsadzenie slotów PCIe, pozostałego czasu gwarancji  11) możliwość uruchamiania narzędzi zarządzających w poszczególnych urządzeniach  12) szybki podgląd stanu środowiska  13) podsumowanie stanu dla każdego urządzenia  14) szczegółowy status urządzenia/elementu/komponentu  15) generowanie alertów przy zmianie stanu urządzenia  16) filtry raportów umożliwiające podgląd najważniejszych zdarzeń  17) integracja z service desk producenta dostarczonej platformy sprzętowej  18) możliwość przejęcia zdalnego pulpitu  19) możliwość podmontowania wirtualnego napędu  20) kreator umożliwiający dostosowanie akcji dla wybranych alertów  21) możliwość importu plików MIB  22) możliwość definiowania ról administratorów  23) możliwość zdalnej aktualizacji oprogramowania wewnętrznego serwerów  24) aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania)  25) możliwość instalacji oprogramowania wewnętrznego bez potrzeby instalacji agenta  26) możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów  27) 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  28) możliwość tworzenia sprzętowej konfiguracji bazowej i na jej podstawie weryfikacji środowiska w celu wykrycia rozbieżności  29) wdrażanie serwerów, rozwiązań modularnych oraz przełączników sieciowych w oparciu o profile  30) możliwość migracji ustawień serwera wraz z wirtualnymi adresami sieciowymi (MAC, WWN, IQN) między urządzeniami  31) tworzenie gotowych paczek informacji umożliwiających zdiagnozowanie awarii urządzenia przez serwis producenta  32) zdalne uruchamianie diagnostyki serwera  33) dedykowana aplikacja na urządzenia mobilne integrująca się z wyżej opisanymi oprogramowaniem zarządzającym  34) oprogramowanie dostarczane jako wirtualny appliance dla KVM, ESXi i Hyper-V | TAK |
| 17 | Normy środowiskowe | 1. 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 plik z wydrukiem ze strony internetowej www.epeat.net potwierdzający spełnienie normy co najmniej EPEAT Bronze według normy wprowadzonej w 2019 roku.  Do oferty należy dołączyć plik z aktualnym na dzień składania oferty wydrukiem ze strony [www.epeat.net](http://www.epeat.net) potwierdzającym spełnianie wymogu.  2. Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych, w szczególności zgodności z normą ISO 1043-4 dla płyty głównej oraz elementów wykonanych z tworzyw sztucznych o masie powyżej 25 gr.  Do oferty należy dołączyć oświadczenie producenta serwera potwierdzające spełnienie wymogu. | TAK |
| 18 | Certyfikaty | 1. Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015 oraz ISO-14001.  2. Serwer musi posiadać deklarację CE.  3. Urządzenia wyprodukowane są przez producenta zgodnie z normą PN-EN ISO 50001 lub przez producenta stosującego w fabrykach politykę zarządzania energią, która jest zgodna z obowiązującymi przepisami na terenie Unii Europejskiej.  4. Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Microsoft Windows 2019 x64, Microsoft Windows 2022 x64 .  5. Oferowany serwer musi znajdować się na liście kompatybilności produktów Oracle dostępnej na stronie https://linux.oracle.com/ords/f?p=117:1 | TAK |
| 19 | Warunki gwarancji | 1. Zamawiający wymaga min. 60 miesięcy gwarancji producenta, możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie, przez Internet oraz z wykorzystaniem aplikacji.  2. Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania producenta, w tym także dostarczonego oprogramowania.  3. Zgłoszenie przyjęte jest potwierdzane przez zespół pomocy technicznej (mail/telefon/aplikacja/portal) poprzez nadanie unikalnego numeru zgłoszenia pozwalającego na identyfikację zgłoszenia w trakcie realizacji naprawy i po jej zakończeniu.  4. Zamawiający ma możliwość samodzielnego kwalifikowania poziomu ważności naprawy.  5. Zamawiający wymaga rozpoczęcia diagnostyki telefonicznej / internetowej już w momencie dokonania zgłoszenia. Certyfikowany Technik wykonawcy / producenta z właściwym zestawem części do naprawy (potwierdzonym wstępnie na etapie diagnostyki) ma rozpocząć naprawę w siedzibie zamawiającego najpóźniej w ciągu 4 godzin od otrzymania zgłoszenia. Naprawa ma się odbywać w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę.  6. Dla najwyższego poziomu ważności zgłoszenia (awarii krytycznej) - zamawiający wymaga niezwłocznego wysłania technika serwisowego, niezależnie czy diagnostyka została już zakończona.  7. Zamawiający wymaga od Wykonawcy dołączenia do oferty oświadczenia podmiotu realizującego serwis lub producenta sprzętu, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego.  8. Wymagane dołączenie do oferty oświadczenia Producenta potwierdzającego, że serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta.  9. Oświadczenie producenta serwera, potwierdzające, że sprzęt pochodzi z oficjalnego kanału dystrybucyjnego producenta. | TAK |
| 20 | Dokumentacja użytkownika | 1. Zamawiający wymaga dokumentacji w języku polskim lub angielskim.  2. Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela. | TAK |

**ZADANIE 3 – SERWER TYPU II (3 SZTUKI)**

|  |  |  |  |
| --- | --- | --- | --- |
| **Lp.** | **Komponent** | **Minimalne wymagania** | **Potwierdzenie spełnienia wymagań przez oferowane produkty (skreślić TAK i wpisać NIE, jeżeli nie spełnia minimalnych wymagań), podać dane we wskazanych miejscach** |
| 1 | Obudowa | 1. Obudowa Rack o wysokości max. 1U, umożliwiająca instalację min. 10 dysków 2,5” z kompletem wysuwanych szyn umożliwiających montaż w szafie Rack i wysuwanie serwera do celów serwisowych.  2. Obudowa wyposażona w kartę umożliwiającą dostęp bezpośredni poprzez urządzenia mobilne - serwer musi posiadać możliwość konfiguracji oraz monitoringu najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej (Android/ Apple iOS) przy użyciu jednego z protokołów BLE/ WIFI. | Producent oferowanych serwerów: …  Model oferowanych serwerów: …  TAK |
| 2 | Płyta główna | Płyta główna z możliwością zainstalowania dwóch procesorów. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym. | TAK |
| 3 | Chipset | Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych | TAK |
| 4 | Procesor | Zainstalowany jeden procesor min. trzydziestodwu-rdzeniowy klasy x86 do pracy z zaoferowanym serwerem umożliwiający osiągnięcie wyniku min. 668 punktów w teście SPECrate2017\_int\_base dostępnym na stronie www.spec.org dla dwóch procesorów. | Podać producenta i model: …  TAK |
| 5 | Pamięć RAM | Minimum 512GB DDR4 RDIMM 4800MT/s. Na płycie głównej powinno znajdować się minimum 32 slotów przeznaczonych do instalacji pamięci. Płyta główna powinna obsługiwać do 8TB pamięci RAM. | TAK |
| 6 | Zabezpieczenia pamięci RAM | Demand Scrubbing, Patrol Scrubbing, Permanent Fault Detection | TAK |
| 7 | Gniazda PCIe | Minimum dwa sloty PCIe x8 generacji 5 i jeden slot PCIe x16 generacji 4 | TAK |
| 8 | Interfejsy sieciowe/FC/SAS | 1. Dwa interfejsy sieciowe 25Gb Ethernet ze złączami SFP28 (nie mogą zajmować gniazd PCIe zdefiniowanych w pkt 7)  2. Możliwość instalacji wymiennie modułów udostępniających:  1) dwa interfejsy sieciowe 10Gb Ethernet w standardzie SFP+  2) dwa interfejsy sieciowe 10Gb Ethernet w standardzie BaseT  3) cztery interfejsy sieciowe 10Gb Ethernet w standardzie SFP+  4) cztery interfejsy sieciowe 1Gb Ethernet w standardzie BaseT  5) cztery interfejsy sieciowe 25Gb Ethernet ze złączami SFP28  3. Wbudowane dwa interfejsy sieciowe 1Gb Ethernet w standardzie BaseT.  4. Dodatkowo zainstalowane:  1) jedna karta dwuportowa 25Gb Ethernet ze złączami SFP28  2) dwie karty dwuportowe FC 32Gb/s | TAK |
| 9 | Dyski twarde | 1. Możliwość instalacji dysków SAS/SATA.  2. Zainstalowane dwa dyski hot-swap M.2 NVMe o pojemności min. 960GB z możliwością konfiguracji RAID 1. | TAK |
| 10 | Kontroler RAID/HBA | Karta HBA | TAK |
| 11 | Wbudowane porty | Minimum port USB 2.0 oraz port USB 3.0, port VGA | TAK |
| 12 | Video | Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1600x900 | TAK |
| 13 | Wentylatory | Redundantne Hot-Plug | TAK |
| 14 | Zasilacze | Minimum dwa zasilacze Hot-Plug min. 1100W Titanium. | TAK |
| 15 | Karta zarządzania | 1. Niezależna karta zarządzająca od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port RJ-45 Gigabit Ethernet umożliwiająca:  1) zdalny dostęp do graficznego interfejsu Web karty zarządzającej  2) szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika  3) podmontowanie zdalnych wirtualnych napędów  4) wirtualną konsolę z dostępem do myszy, klawiatury  5) wsparcie dla IPv6  6) wsparcie dla SNMP; IPMI2.0, VLAN tagging, SSH  7) zdalne monitorowanie w czasie rzeczywistym poboru prądu przez serwer, dane historyczne powinny być dostępne przez min. 7 dni wstecz  8) zdalne ustawienie limitu poboru prądu przez konkretny serwer  9) integrację z Active Directory  10) obsługę przez czterech administratorów jednocześnie  11) wsparcie dla automatycznej rejestracji DNS  12) wsparcie dla LLDP  13) wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej  14) podłączenie lokalne poprzez złącze RS-232  15) zarządzanie bezpośrednio poprzez złącze microUSB umieszczone na froncie obudowy  16) monitorowanie zużycia dysków SSD  17) monitorowanie z jednej konsoli min. 20 serwerów fizycznych  18) automatyczne zgłaszanie alertów do centrum serwisowego producenta  19) automatyczny update firmware dla wszystkich komponentów serwera  20) przywrócenie poprzednich wersji firmware  21) eksport/import konfiguracji (ustawienie karty zarządzającej, BIOSu, kart sieciowych, HBA oraz konfiguracji kontrolera RAID) serwera do pliku XML lub JSON  22) zaimportowanie ustawień poprzez bezpośrednie podłączenie plików konfiguracyjnych  23) automatyczne tworzenie kopii ustawień serwera w oparciu o harmonogram  24) wykrywanie odchyleń konfiguracji na poziomie konfiguracji UEFI oraz wersji firmware serwera  2. Karta powinna posiadać możliwość uruchomienia dodatkowych poniższych funkcjonalności:  1) kontrola stanu BIOS pod kątem naruszenia integralności oprogramowania  2) automatyczne odświeżanie certyfikatów SSL  3) wykorzystanie tokenu lub aplikacji SecurID do uwierzytelniania wielkoskładnikowego przy logowaniu do karty zarządzającej  4) modyfikacja reguł chłodzenia kart w slotach PCIe, z możliwością własnych ustawień  5) ustawienia limitu temperatury powietrza wychodzącego z serwera  6) ustawienia dopuszczalnego wzrostu temperatury powietrza przepływającego przez serwer  7) ustawienia maksymalnej temperatury powietrza dochodzącego do slotów PCIe  8) monitorowanie przepływu powietrza na bieżąco | TAK |
| 16 | Oprogramowanie do zarządzania | Zainstalowane oprogramowanie producenta do zarządzania, spełniające poniższe wymagania:  1) wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych  2) integracja z Active Directory  3) możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta  4) wsparcie dla protokołów SNMP, IPMI, Linux SSH, Redfish  5) możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram  6) szczegółowy opis wykrytych systemów oraz ich komponentów  7) możliwość eksportu raportu do CSV, HTML, XLS, PDF  8) możliwość tworzenia własnych raportów w oparciu o wszystkie informacje zawarte w inwentarzu.  9) grupowanie urządzeń w oparciu o kryteria użytkownika  10) tworzenie automatycznie grup urządzeń w oparciu o dowolny element konfiguracji serwera np. nazwa, lokalizacja, system operacyjny, obsadzenie slotów PCIe, pozostałego czasu gwarancji  11) możliwość uruchamiania narzędzi zarządzających w poszczególnych urządzeniach  12) szybki podgląd stanu środowiska  13) podsumowanie stanu dla każdego urządzenia  14) szczegółowy status urządzenia/elementu/komponentu  15) generowanie alertów przy zmianie stanu urządzenia  16) filtry raportów umożliwiające podgląd najważniejszych zdarzeń  17) integracja z service desk producenta dostarczonej platformy sprzętowej  18) możliwość przejęcia zdalnego pulpitu  19) możliwość podmontowania wirtualnego napędu  20) kreator umożliwiający dostosowanie akcji dla wybranych alertów  21) możliwość importu plików MIB  22) możliwość definiowania ról administratorów  23) możliwość zdalnej aktualizacji oprogramowania wewnętrznego serwerów  24) aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania)  25) możliwość instalacji oprogramowania wewnętrznego bez potrzeby instalacji agenta  26) możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów  27) 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  28) możliwość tworzenia sprzętowej konfiguracji bazowej i na jej podstawie weryfikacji środowiska w celu wykrycia rozbieżności  29) wdrażanie serwerów, rozwiązań modularnych oraz przełączników sieciowych w oparciu o profile  30) możliwość migracji ustawień serwera wraz z wirtualnymi adresami sieciowymi (MAC, WWN, IQN) między urządzeniami  31) tworzenie gotowych paczek informacji umożliwiających zdiagnozowanie awarii urządzenia przez serwis producenta  32) zdalne uruchamianie diagnostyki serwera  33) dedykowana aplikacja na urządzenia mobilne integrująca się z wyżej opisanymi oprogramowaniem zarządzającym  34) oprogramowanie dostarczane jako wirtualny appliance dla KVM, ESXi i Hyper-V | TAK |
| 17 | System operacyjny | 1. Z uwagi na posiadane przez Zamawiającego oprogramowanie systemowe i konieczność jego pełnej integracji z nowo dostarczanymi serwerami, należy je dostarczyć z poniższymi wersjami oprogramowania w pełnym zakresie licencji:  1) Microsoft Windows Server 2022 Datacenter  2) Microsoft Server 2022 Device CAL (550 urządzeń – dotyczy całości przedmiotu zamówienia)  3) VMware vSphere 8 Enterprise Plus (licencja z supportem na 5 lat)  4) VMware vCenter Server 8 Standard for vSphere 8 (licencja z supportem na 5 lat)  2. Powyższe licencje muszą pokrywać ilość procesorów/rdzeni oferowanej konfiguracji sprzętu (klaster 3 serwerów). | TAK |
| 18 | Normy środowiskowe | 1. 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 plik z wydrukiem ze strony internetowej www.epeat.net potwierdzający spełnienie normy co najmniej EPEAT Bronze według normy wprowadzonej w 2019 roku.  Do oferty należy dołączyć plik z aktualnym na dzień składania oferty wydrukiem ze strony www.epeat.net potwierdzającym spełnianie wymogu.  2. Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych, w szczególności zgodności z normą ISO 1043-4 dla płyty głównej oraz elementów wykonanych z tworzyw sztucznych o masie powyżej 25 gr.  Do oferty należy dołączyć oświadczenie producenta serwera potwierdzające spełnienie wymogu. | TAK |
| 19 | Certyfikaty | 1. Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015 oraz ISO-14001.  2. Serwer musi posiadać deklarację CE.  3. Urządzenia wyprodukowane są przez producenta zgodnie z normą PN-EN ISO 50001 lub przez producenta stosującego w fabrykach politykę zarządzania energią, która jest zgodna z obowiązującymi przepisami na terenie Unii Europejskiej.  4. Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Microsoft Windows 2019 x64, Microsoft Windows 2022 x64.  5. Oferowany serwer musi znajdować się na liście kompatybilności produktów VMware dostępnej na stronie http://www.vmware.com/resources/compatibility/ | TAK |
| 20 | Warunki gwarancji | 1. Zamawiający wymaga min. 60 miesięcy gwarancji producenta, możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie, przez Internet oraz z wykorzystaniem aplikacji.  2. Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania producenta, w tym także dostarczonego oprogramowania.  3. Zgłoszenie przyjęte jest potwierdzane przez zespół pomocy technicznej (mail/telefon/aplikacja/portal) poprzez nadanie unikalnego numeru zgłoszenia pozwalającego na identyfikację zgłoszenia w trakcie realizacji naprawy i po jej zakończeniu.  4. Zamawiający ma możliwość samodzielnego kwalifikowania poziomu ważności naprawy.  5. Zamawiający wymaga rozpoczęcia diagnostyki telefonicznej / internetowej już w momencie dokonania zgłoszenia. Certyfikowany Technik wykonawcy / producenta z właściwym zestawem części do naprawy (potwierdzonym wstępnie na etapie diagnostyki) ma rozpocząć naprawę w siedzibie zamawiającego najpóźniej w ciągu 4 godzin od otrzymania zgłoszenia. Naprawa ma się odbywać w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę.  6. Dla najwyższego poziomu ważności zgłoszenia (awarii krytycznej) - zamawiający wymaga niezwłocznego wysłania technika serwisowego, niezależnie czy diagnostyka została już zakończona.  7. Zamawiający wymaga od Wykonawcy dołączenia do oferty oświadczenia podmiotu realizującego serwis lub producenta sprzętu, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego.  8. Wymagane dołączenie do oferty oświadczenia Producenta potwierdzającego, że serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta.  9. Oświadczenie producenta serwera, potwierdzające, że sprzęt pochodzi z oficjalnego kanału dystrybucyjnego producenta. | TAK |
| 21 | Dokumentacja użytkownika | 1. Zamawiający wymaga dokumentacji w języku polskim lub angielskim.  2. Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela. | TAK |

**ZADANIE 4 – SERWER TYPU III (1 SZTUKA)**

|  |  |  |  |
| --- | --- | --- | --- |
| **Lp.** | **Komponent** | **Minimalne wymagania** | **Potwierdzenie spełnienia wymagań przez oferowane produkty (skreślić TAK i wpisać NIE, jeżeli nie spełnia minimalnych wymagań), podać dane we wskazanych miejscach** |
| 1 | Obudowa | Obudowa Rack o wysokości max. 1U, umożliwiająca instalację min. 8 dysków 2,5” z kompletem wysuwanych szyn umożliwiających montaż w szafie Rack i wysuwanie serwera do celów serwisowych. | Producent oferowanego serwera: …  Model oferowanego serwera: …  TAK |
| 2 | Płyta główna | Płyta główna z możliwością zainstalowania dwóch procesorów. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym. | TAK |
| 3 | Chipset | Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych | TAK |
| 4 | Procesor | Zainstalowany jeden procesor min. dwunasto-rdzeniowy klasy x86 do pracy z zaoferowanym serwerem umożliwiający osiągnięcie wyniku min. 214 punktów w teście SPECrate2017\_int\_base dostępnym na stronie www.spec.org dla dwóch procesorów. | Podać producenta i model: …  TAK |
| 5 | Pamięć RAM | Minimum 64GB DDR4 RDIMM 4800MT/s. Na płycie głównej powinno znajdować się minimum 16 slotów przeznaczonych do instalacji pamięci. Płyta główna powinna obsługiwać do 1TB pamięci RAM. | TAK |
| 6 | Zabezpieczenia pamięci RAM | Demand Scrubbing, Patrol Scrubbing, Permanent Fault Detection | TAK |
| 7 | Gniazda PCIe | Minimum jeden slot PCIe x16 generacji 4 i minimum jeden slot PCIe x8 generacji 5 | TAK |
| 8 | Interfejsy sieciowe/FC/SAS | 1. Dwa interfejsy sieciowe 25Gb Ethernet ze złączami SFP28 (nie mogą zajmować gniazd PCIe zdefiniowanych w pkt 7)  2. Cztery interfejsy 1Gb Ethernet w standardzie BaseT  3. Jedna karta dwuportowa FC 32Gb/s | TAK |
| 9 | Dyski twarde | 1. Zainstalowane 2x 480GB SSD SATA, DWPD min. 3  2. Możliwość instalacji dwóch dysków hot-swap M.2 o pojemności min. 960GB z możliwością konfiguracji RAID 1. | TAK |
| 10 | Kontroler RAID | Sprzętowy kontroler dyskowy z pojemnością cache 8GB, możliwe konfiguracje poziomów RAID: 0,1,5,6,10,50,60. | TAK |
| 11 | Wbudowane porty | Minimum port USB 2.0 oraz port USB 3.0, port VGA | TAK |
| 12 | Video | Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1600x900 | TAK |
| 13 | Wentylatory | Redundantne | TAK |
| 14 | Zasilacze | Minimum dwa zasilacze Hot-Plug min. 700W Titanium. | TAK |
| 15 | Karta zarządzania | 1. Niezależna karta zarządzająca od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port RJ-45 Gigabit Ethernet umożliwiająca:  1) zdalny dostęp do graficznego interfejsu Web karty zarządzającej  2) szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika  3) podmontowanie zdalnych wirtualnych napędów  4) wirtualną konsolę z dostępem do myszy, klawiatury  5) wsparcie dla IPv6  6) wsparcie dla SNMP; IPMI2.0, VLAN tagging, SSH  7) zdalne monitorowanie w czasie rzeczywistym poboru prądu przez serwer, dane historyczne powinny być dostępne przez min. 7 dni wstecz  8) zdalne ustawienie limitu poboru prądu przez konkretny serwer  9) integrację z Active Directory  10) obsługę przez czterech administratorów jednocześnie  11) wsparcie dla automatycznej rejestracji DNS  12) wsparcie dla LLDP  13) wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej  14) podłączenie lokalne poprzez złącze RS-232  15) zarządzanie bezpośrednio poprzez złącze microUSB umieszczone na froncie obudowy  16) monitorowanie zużycia dysków SSD  17) monitorowanie z jednej konsoli min. 20 serwerów fizycznych  18) automatyczne zgłaszanie alertów do centrum serwisowego producenta  19) automatyczny update firmware dla wszystkich komponentów serwera  20) przywrócenie poprzednich wersji firmware  21) eksport/import konfiguracji (ustawienie karty zarządzającej, BIOSu, kart sieciowych, HBA oraz konfiguracji kontrolera RAID) serwera do pliku XML lub JSON  22) zaimportowanie ustawień poprzez bezpośrednie podłączenie plików konfiguracyjnych  23) automatyczne tworzenie kopii ustawień serwera w oparciu o harmonogram  24) wykrywanie odchyleń konfiguracji na poziomie konfiguracji UEFI oraz wersji firmware serwera | TAK |
| 16 | Oprogramowanie do zarządzania | Zainstalowane oprogramowanie producenta do zarządzania, spełniające poniższe wymagania:  1) wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych  2) integracja z Active Directory  3) możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta  4) wsparcie dla protokołów SNMP, IPMI, Linux SSH, Redfish  5) możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram  6) szczegółowy opis wykrytych systemów oraz ich komponentów  7) możliwość eksportu raportu do CSV, HTML, XLS, PDF  8) możliwość tworzenia własnych raportów w oparciu o wszystkie informacje zawarte w inwentarzu.  9) grupowanie urządzeń w oparciu o kryteria użytkownika  10) tworzenie automatycznie grup urządzeń w oparciu o dowolny element konfiguracji serwera np. nazwa, lokalizacja, system operacyjny, obsadzenie slotów PCIe, pozostałego czasu gwarancji  11) możliwość uruchamiania narzędzi zarządzających w poszczególnych urządzeniach  12) szybki podgląd stanu środowiska  13) podsumowanie stanu dla każdego urządzenia  14) szczegółowy status urządzenia/elementu/komponentu  15) generowanie alertów przy zmianie stanu urządzenia  16) filtry raportów umożliwiające podgląd najważniejszych zdarzeń  17) integracja z service desk producenta dostarczonej platformy sprzętowej  18) możliwość przejęcia zdalnego pulpitu  19) możliwość podmontowania wirtualnego napędu  20) kreator umożliwiający dostosowanie akcji dla wybranych alertów  21) możliwość importu plików MIB  22) możliwość definiowania ról administratorów  23) możliwość zdalnej aktualizacji oprogramowania wewnętrznego serwerów  24) aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania)  25) możliwość instalacji oprogramowania wewnętrznego bez potrzeby instalacji agenta  26) możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów  27) 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  28) możliwość tworzenia sprzętowej konfiguracji bazowej i na jej podstawie weryfikacji środowiska w celu wykrycia rozbieżności  29) wdrażanie serwerów, rozwiązań modularnych oraz przełączników sieciowych w oparciu o profile  30) możliwość migracji ustawień serwera wraz z wirtualnymi adresami sieciowymi (MAC, WWN, IQN) między urządzeniami  31) tworzenie gotowych paczek informacji umożliwiających zdiagnozowanie awarii urządzenia przez serwis producenta  32) zdalne uruchamianie diagnostyki serwera  33) dedykowana aplikacja na urządzenia mobilne integrująca się z wyżej opisanymi oprogramowaniem zarządzającym  34) oprogramowanie dostarczane jako wirtualny appliance dla KVM, ESXi i Hyper-V | TAK |
| 18 | Normy środowiskowe | 1. 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 plik z wydrukiem ze strony internetowej www.epeat.net potwierdzający spełnienie normy co najmniej EPEAT Bronze według normy wprowadzonej w 2019 roku.  Do oferty należy dołączyć plik z aktualnym na dzień składania oferty wydrukiem ze strony www.epeat.net potwierdzającym spełnianie wymogu.  2. Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych, w szczególności zgodności z normą ISO 1043-4 dla płyty głównej oraz elementów wykonanych z tworzyw sztucznych o masie powyżej 25 gr.  Do oferty należy dołączyć oświadczenie producenta serwera potwierdzające spełnienie wymogu. | TAK |
| 19 | Certyfikaty | 1. Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015 oraz ISO-14001.  2. Serwer musi posiadać deklarację CE.  3. Serwer wyprodukowany przez producenta zgodnie z normą PN-EN ISO 50001 lub przez producenta stosującego w fabrykach politykę zarządzania energią, która jest zgodna z obowiązującymi przepisami na terenie Unii Europejskiej.  4. Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Microsoft Windows 2019 x64, Microsoft Windows 2022 x64.  5. Oferowany serwer musi znajdować się na liście kompatybilności produktów VMware dostępnej na stronie http://www.vmware.com/resources/compatibility/ | TAK |
| 20 | Warunki gwarancji | 1. Zamawiający wymaga min. 60 miesięcy gwarancji producenta, możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie, przez Internet oraz z wykorzystaniem aplikacji.  2. Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania producenta, w tym także dostarczonego oprogramowania.  3. Zgłoszenie przyjęte jest potwierdzane przez zespół pomocy technicznej (mail/telefon/aplikacja/portal) poprzez nadanie unikalnego numeru zgłoszenia pozwalającego na identyfikację zgłoszenia w trakcie realizacji naprawy i po jej zakończeniu.  4. Zamawiający ma możliwość samodzielnego kwalifikowania poziomu ważności naprawy.  5. Zamawiający wymaga rozpoczęcia diagnostyki telefonicznej / internetowej już w momencie dokonania zgłoszenia. Certyfikowany Technik wykonawcy / producenta z właściwym zestawem części do naprawy (potwierdzonym wstępnie na etapie diagnostyki) ma rozpocząć naprawę w siedzibie zamawiającego najpóźniej w ciągu 4 godzin od otrzymania zgłoszenia. Naprawa ma się odbywać w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę.  6. Dla najwyższego poziomu ważności zgłoszenia (awarii krytycznej) - zamawiający wymaga niezwłocznego wysłania technika serwisowego, niezależnie czy diagnostyka została już zakończona.  7. Zamawiający wymaga od Wykonawcy dołączenia do oferty oświadczenia podmiotu realizującego serwis lub producenta sprzętu, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego.  8. Wymagane dołączenie do oferty oświadczenia Producenta potwierdzającego, że serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta.  9. Oświadczenie producenta serwera, potwierdzające, że sprzęt pochodzi z oficjalnego kanału dystrybucyjnego producenta. | TAK |
| 21 | Dokumentacja użytkownika | 1. Zamawiający wymaga dokumentacji w języku polskim lub angielskim.  2. Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela. | TAK |

**ZADANIE 5 – SERWER TYPU IV (2 SZTUKI)**

|  |  |  |  |
| --- | --- | --- | --- |
| **Lp.** | **Komponent** | **Minimalne wymagania** | **Potwierdzenie spełnienia wymagań przez oferowane produkty (skreślić TAK i wpisać NIE, jeżeli nie spełnia minimalnych wymagań), podać dane we wskazanych miejscach** |
| 1 | Obudowa | Obudowa Rack o wysokości max. 1U, umożliwiająca instalację min. 8 dysków 2,5” z kompletem wysuwanych szyn umożliwiających montaż w szafie Rack i wysuwanie serwera do celów serwisowych. | Producent oferowanych serwerów: …  Model oferowanych serwerów: …  TAK |
| 2 | Płyta główna | Płyta główna z możliwością zainstalowania dwóch procesorów. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym. | TAK |
| 3 | Chipset | Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych | TAK |
| 4 | Procesor | Zainstalowany jeden procesor min. ośmio-rdzeniowy klasy x86 do pracy z zaoferowanym serwerem umożliwiający osiągnięcie wyniku min. 176 punktów w teście SPECrate2017\_int\_base dostępnym na stronie www.spec.org dla dwóch procesorów. | Podać producenta i model: …  TAK |
| 5 | Pamięć RAM | Minimum 64GB DDR4 RDIMM 4800MT/s. Na płycie głównej powinno znajdować się minimum 16 slotów przeznaczonych do instalacji pamięci. Płyta główna powinna obsługiwać do 1TB pamięci RAM. | TAK |
| 6 | Zabezpieczenia pamięci RAM | Demand Scrubbing, Patrol Scrubbing, Permanent Fault Detection | TAK |
| 7 | Gniazda PCIe | Minimum jeden slot PCIe x16 generacji 4 i minimum jeden slot PCIe x8 generacji 5 | TAK |
| 8 | Interfejsy sieciowe/FC/SAS | 1. Dwa interfejsy sieciowe 25Gb Ethernet ze złączami SFP28 (nie mogą zajmować gniazd PCIe zdefiniowanych w pkt 7)  2. Dwa wbudowane interfejsy sieciowe 1Gb Ethernet w standardzie BaseT.  3. Dodatkowo zainstalowane:  1) jedna karta czteroportowa 1Gb Ethernet w standardzie BaseT  2) jedna karta dwuportowe 25Gb Ethernet SFP28 | TAK |
| 9 | Dyski twarde | 1. Zainstalowane 2x 480GB SSD SATA, DWPD min. 3 oraz 4x 2,4TB SAS 10k  2. Możliwość instalacji dwóch dysków hot-swap M.2 o pojemności min. 960GB z możliwością konfiguracji RAID 1. | TAK |
| 10 | Kontroler RAID | Sprzętowy kontroler dyskowy z pojemnością cache 8GB, możliwe konfiguracje poziomów RAID: 0,1,5,6,10,50,60. | TAK |
| 11 | Wbudowane porty | Minimum port USB 2.0 oraz port USB 3.0, port VGA | TAK |
| 12 | Video | Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1600x900 | TAK |
| 13 | Wentylatory | Redundantne | TAK |
| 14 | Zasilacze | Minimum dwa zasilacze Hot-Plug min. 700W Titanium. | TAK |
| 15 | Karta zarządzania | 1. Niezależna karta zarządzająca od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port RJ-45 Gigabit Ethernet umożliwiająca:  1) zdalny dostęp do graficznego interfejsu Web karty zarządzającej  2) szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika  3) podmontowanie zdalnych wirtualnych napędów  4) wirtualną konsolę z dostępem do myszy, klawiatury  5) wsparcie dla IPv6  6) wsparcie dla SNMP; IPMI2.0, VLAN tagging, SSH  7) zdalne monitorowanie w czasie rzeczywistym poboru prądu przez serwer, dane historyczne powinny być dostępne przez min. 7 dni wstecz  8) zdalne ustawienie limitu poboru prądu przez konkretny serwer  9) integrację z Active Directory  10) obsługę przez czterech administratorów jednocześnie  11) wsparcie dla automatycznej rejestracji DNS  12) wsparcie dla LLDP  13) wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej  14) podłączenie lokalne poprzez złącze RS-232  15) zarządzanie bezpośrednio poprzez złącze microUSB umieszczone na froncie obudowy  16) monitorowanie zużycia dysków SSD  17) monitorowanie z jednej konsoli min. 20 serwerów fizycznych  18) automatyczne zgłaszanie alertów do centrum serwisowego producenta  19) automatyczny update firmware dla wszystkich komponentów serwera  20) przywrócenie poprzednich wersji firmware  21) eksport/import konfiguracji (ustawienie karty zarządzającej, BIOSu, kart sieciowych, HBA oraz konfiguracji kontrolera RAID) serwera do pliku XML lub JSON  22) zaimportowanie ustawień poprzez bezpośrednie podłączenie plików konfiguracyjnych  23) automatyczne tworzenie kopii ustawień serwera w oparciu o harmonogram  24) wykrywanie odchyleń konfiguracji na poziomie konfiguracji UEFI oraz wersji firmware serwera | TAK |
| 16 | Oprogramowanie do zarządzania | Zainstalowane oprogramowanie producenta do zarządzania, spełniające poniższe wymagania:  1) wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych  2) integracja z Active Directory  3) możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta  4) wsparcie dla protokołów SNMP, IPMI, Linux SSH, Redfish  5) możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram  6) szczegółowy opis wykrytych systemów oraz ich komponentów  7) możliwość eksportu raportu do CSV, HTML, XLS, PDF  8) możliwość tworzenia własnych raportów w oparciu o wszystkie informacje zawarte w inwentarzu.  9) grupowanie urządzeń w oparciu o kryteria użytkownika  10) tworzenie automatycznie grup urządzeń w oparciu o dowolny element konfiguracji serwera np. nazwa, lokalizacja, system operacyjny, obsadzenie slotów PCIe, pozostałego czasu gwarancji  11) możliwość uruchamiania narzędzi zarządzających w poszczególnych urządzeniach  12) szybki podgląd stanu środowiska  13) podsumowanie stanu dla każdego urządzenia  14) szczegółowy status urządzenia/elementu/komponentu  15) generowanie alertów przy zmianie stanu urządzenia  16) filtry raportów umożliwiające podgląd najważniejszych zdarzeń  17) integracja z service desk producenta dostarczonej platformy sprzętowej  18) możliwość przejęcia zdalnego pulpitu  19) możliwość podmontowania wirtualnego napędu  20) kreator umożliwiający dostosowanie akcji dla wybranych alertów  21) możliwość importu plików MIB  22) możliwość definiowania ról administratorów  23) możliwość zdalnej aktualizacji oprogramowania wewnętrznego serwerów  24) aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania)  25) możliwość instalacji oprogramowania wewnętrznego bez potrzeby instalacji agenta  26) możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów  27) 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  28) możliwość tworzenia sprzętowej konfiguracji bazowej i na jej podstawie weryfikacji środowiska w celu wykrycia rozbieżności  29) wdrażanie serwerów, rozwiązań modularnych oraz przełączników sieciowych w oparciu o profile  30) możliwość migracji ustawień serwera wraz z wirtualnymi adresami sieciowymi (MAC, WWN, IQN) między urządzeniami  31) tworzenie gotowych paczek informacji umożliwiających zdiagnozowanie awarii urządzenia przez serwis producenta  32) zdalne uruchamianie diagnostyki serwera  33) dedykowana aplikacja na urządzenia mobilne integrująca się z wyżej opisanymi oprogramowaniem zarządzającym  34) oprogramowanie dostarczane jako wirtualny appliance dla KVM, ESXi i Hyper-V | TAK |
| 18 | Normy środowiskowe | 1. 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 plik z wydrukiem ze strony internetowej www.epeat.net potwierdzający spełnienie normy co najmniej EPEAT Bronze według normy wprowadzonej w 2019 roku.  Do oferty należy dołączyć plik z aktualnym na dzień składania oferty wydrukiem ze strony www.epeat.net potwierdzającym spełnianie wymogu.  2. Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych, w szczególności zgodności z normą ISO 1043-4 dla płyty głównej oraz elementów wykonanych z tworzyw sztucznych o masie powyżej 25 gr.  Do oferty należy dołączyć oświadczenie producenta serwera potwierdzające spełnienie wymogu. | TAK |
| 19 | Certyfikaty | 1. Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015 oraz ISO-14001.  2. Serwer musi posiadać deklarację CE.  3. Urządzenia wyprodukowane przez producenta zgodnie z normą PN-EN ISO 50001 lub przez producenta stosującego w fabrykach politykę zarządzania energią, która jest zgodna z obowiązującymi przepisami na terenie Unii Europejskiej.  4. Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Microsoft Windows 2019 x64, Microsoft Windows 2022 x64.  5. Oferowany serwer musi znajdować się na liście kompatybilności produktów VMware dostępnej na stronie http://www.vmware.com/resources/compatibility/ | TAK |
| 20 | Warunki gwarancji | 1. Zamawiający wymaga min. 60 miesięcy gwarancji producenta, możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie, przez Internet oraz z wykorzystaniem aplikacji.  2. Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania producenta, w tym także dostarczonego oprogramowania.  3. Zgłoszenie przyjęte jest potwierdzane przez zespół pomocy technicznej (mail/telefon/aplikacja/portal) poprzez nadanie unikalnego numeru zgłoszenia pozwalającego na identyfikację zgłoszenia w trakcie realizacji naprawy i po jej zakończeniu.  4. Zamawiający ma możliwość samodzielnego kwalifikowania poziomu ważności naprawy.  5. Zamawiający wymaga rozpoczęcia diagnostyki telefonicznej / internetowej już w momencie dokonania zgłoszenia. Certyfikowany Technik wykonawcy / producenta z właściwym zestawem części do naprawy (potwierdzonym wstępnie na etapie diagnostyki) ma rozpocząć naprawę w siedzibie zamawiającego najpóźniej w ciągu 4 godzin od otrzymania zgłoszenia. Naprawa ma się odbywać w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę.  6. Dla najwyższego poziomu ważności zgłoszenia (awarii krytycznej) - zamawiający wymaga niezwłocznego wysłania technika serwisowego, niezależnie czy diagnostyka została już zakończona.  7. Zamawiający wymaga od Wykonawcy dołączenia do oferty oświadczenia podmiotu realizującego serwis lub producenta sprzętu, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego.  8. Wymagane dołączenie do oferty oświadczenia Producenta potwierdzającego, że serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta.  9. Oświadczenie producenta serwera, potwierdzające, że sprzęt pochodzi z oficjalnego kanału dystrybucyjnego producenta. | TAK |
| 21 | Dokumentacja użytkownika | 1. Zamawiający wymaga dokumentacji w języku polskim lub angielskim.  2. Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela. | TAK |

**ZADANIE 6 – BIBLIOTEKA TAŚMOWA (1 SZTUKA)**

|  |  |  |  |
| --- | --- | --- | --- |
| **Lp.** | **Komponent** | **Minimalne wymagania** | **Potwierdzenie spełnienia wymagań przez oferowane produkty (skreślić TAK i wpisać NIE, jeżeli nie spełnia minimalnych wymagań), podać dane we wskazanych miejscach** |
| 1 | Obudowa | Do zamontowania w szafie Rack, maksymalnie 3U, wbudowany czytnik kodów kreskowych, redundantne zasilanie wraz z kablami zasilającymi | Producent oferowanej biblioteki: …  Model oferowanej biblioteki: …  TAK |
| 2 | Napęd | 1 x LTO9 | TAK |
| 3 | Interfejs | 1x FC min. 8Gb/s | TAK |
| 4 | Liczba slotów | 40 w tym minimum pięć slotów we/wy, jeżeli licencjonowana jest liczba slotów - wymagane aktywowanie wszystkich slotów | TAK |
| 5 | Zasilacze | Minimum 2 zasilacze | TAK |
| 6 | Wymagania dodatkowe | 1. Wsparcie dla nośników LTO WORM (Write Once, Read Many), umożliwiających spełnienie norm prawnych dotyczących odpowiednio długiego przechowywania nienaruszonych danych (archiwizacja).  2. Wsparcie dla technologii szyfrowania backupowanych danych. | TAK |
| 7 | Taśmy | 1. Taśma czyszcząca – 1 sztuka  2. Taśma LTO-9 – 20 sztuk  3. Taśma LTO-9 WORM – 10 sztuk | TAK |
| 8 | Warunki gwarancji | 1. Min. 60 miesięcy gwarancji realizowanej w miejscu instalacji sprzętu, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii w trybie 365x7x24 poprzez ogólnopolską linię telefoniczną producenta.  2. Zamawiający wymaga od Wykonawcy dołączenia do oferty oświadczenia podmiotu realizującego serwis lub producenta sprzętu, że w przypadku wystąpienia awarii nośnika danych w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony nośnik pozostaje u Zamawiającego.  3. Wymagane dołączenie do oferty oświadczenia Producenta potwierdzającego, że serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta.  4. Oświadczenie producenta serwera, potwierdzające, że sprzęt pochodzi z oficjalnego kanału dystrybucyjnego producenta.  5. W czasie obowiązywania gwarancji Zamawiający musi mieć możliwość nieodpłatnego pobierania nowych wersji BIOS, firmware i sterowników poprzez stronę www. | TAK |

**ZADANIE 7 – PRZEŁĄCZNIKI FC (2 SZTUKI)**

|  |  |  |  |
| --- | --- | --- | --- |
| **Lp.** | **Komponent** | **Minimalne wymagania** | **Potwierdzenie spełnienia wymagań przez oferowane produkty (skreślić TAK i wpisać NIE, jeżeli nie spełnia minimalnych wymagań), podać dane we wskazanych miejscach** |
| 1 | Wymagania ogólne | 1. Przełącznik FC musi być wykonany w technologii FC minimum 64 Gb/s i zapewniać możliwość pracy portów FC z prędkościami 64, 32, 16, 10, 8 Gb/s w zależności od rodzaju zastosowanych wkładek SFP.  2. Dostarczony przełącznik FC musi być wyposażony, w co najmniej 24 aktywne porty FC obsadzone wkładkami SFP+ typu shortwave obsługujące prędkość 32/16/8 Gb/s z możliwością rozbudowy do co najmniej 64 portów przez zakup odpowiednich licencji i wkładek optycznych (licencje oraz wkładki optyczne służące do rozbudowy ilości portów nie są przedmiotem tego postępowania).  3. Wszystkie zaoferowane porty przełącznika FC muszą umożliwiać działanie bez tzw. oversubscrypcji gdzie wszystkie porty w maksymalnie rozbudowanej konfiguracji przełącznika mogą pracować równocześnie z pełną prędkością 64Gb/s.  4. Całkowita przepustowość przełącznika FC w konfiguracji z 64 aktywnymi portami wyposażonej we wkładki 64Gb/s musi wynosić minimum 4096 Gb/s end-to-end.  5. Oczekiwana wartość opóźnienia przy przesyłaniu ramek FC między dowolnymi portami przełącznika nie może być większa niż 460ns dla portów pracujących z prędkością 64Gbps.  6. Rodzaj obsługiwanych portów, co najmniej: E, EX, D, F oraz N.  7. Przełącznik FC musi mieć wysokość maksymalnie 1 RU (jednostka wysokości szafy montażowej) i szerokość 19” oraz zapewniać techniczną możliwość montażu w szafie 19”.  8. Maksymalny dopuszczalny pobór mocy przełącznika FC wyposażonego w 64 aktywne porty obsadzone optyką 64Gbps SWL to 349W.  9. Maksymalna ilość ciepła wydzielanego przez przełącznik FC wyposażony w 64 aktywne porty obsadzone optyką 64Gbps SWL to 1192 BTU na godzinę.  10. Przełącznik FC musi posiadać nadmiarowe zasilacze i wentylatory, których wymiana musi być możliwa w trybie „na gorąco” bez przerywania pracy przełącznika.  11. Przełącznik FC musi wydmuchiwać gorące powietrze od strony portów.  12. Przełącznik FC musi być wyposażony w obsługę agregacji do 8 fizycznych połączeń ISL między dwoma przełącznikami i tworzenia w ten sposób logicznych połączeń typu ISL Trunk o przepustowości minimum 512 Gb/s half duplex (dla wkładek 64Gbps) dla każdego logicznego połączenia. Load balancing ruchu między fizycznymi połączeniami ISL w ramach połączenia logicznego typu ISL Trunk musi być realizowany na poziomie pojedynczych ramek FC a połączenie logiczne musi zachowywać kolejność przesyłanych ramek.  13. Przełącznik FC musi być wyposażony w mechanizm balansowania ruchu, pomiędzy co najmniej 16 różnymi połączeniami o tym samym koszcie wewnątrz wielodomenowych sieci fabric, przy czym balansowanie ruchu musi odbywać się w oparciu o 3 parametry nagłówka ramki FC: DID, SID i OXID.  14. Przełącznik FC musi być wyposażony w mechanizm jednoczesnej obsługi ISL Trunk oraz balansowania ruchu w oparciu o DID/SID/OXID.  15. Przełącznik FC musi być dostarczony z aktywnym mechanizmem routingu FC (FCR) zapewniającym możliwość komunikacji wybranych urządzeń z różnych izolowanych sieci fabric.  16. Przełącznik FC musi realizować sprzętową obsługę zoningu (przez tzw. układ ASIC) na podstawie portów i adresów WWN.  17. Przełącznik FC musi mieć możliwość wymiany i aktywacji wersji firmware’u (zarówno na wersję wyższą jak i na niższą) w czasie pracy urządzenia i bez zakłócenia przesyłanego ruchu FC.  18. Przełącznik FC musi obsługiwać sprzętową kompresję ramek FC dla wybranych połączeń ISL na co najmniej 4 portach przełącznika.  19. Przełącznik FC musi wspierać następujące mechanizmy zwiększające poziom bezpieczeństwa:  1) mechanizm szyfrowania i kompresji wybranych połączeń ISL wspierany, na co najmniej 4 portach przełącznika FC. Symetryczny klucz szyfrujący nie może być krótszy niż 256-bitów,  2) mechanizm tzw. Fabric Binding, który umożliwia zdefiniowanie listy kontroli dostępu regulującej prawa przełączników FC do uczestnictwa w sieci fabric,  3) uwierzytelnianie (autentykacja) przełączników w sieci Fabric za pomocą protokołów DH-CHAP i FCAP,  4) uwierzytelnianie (autentykacja) urządzeń końcowych w sieci Fabric za pomocą protokołu DH-CHAP,  5) szyfrowanie połączenia z konsolą administracyjną. Wsparcie dla SSHv2,  6) definiowanie wielu kont administratorów z możliwością ograniczenia ich uprawnień za pomocą mechanizmu tzw. RBAC (Role Based Access Control),  7) definiowane kont administratorów w środowisku RADIUS, LDAP w MS Active Directory, Open LDAP, TACACS+,  8) szyfrowanie komunikacji narzędzi administracyjnych za pomocą SSL/HTTPS,  9) obsługa SNMP v1 oraz v3,  10) IP Filter dla portu administracyjnego przełącznika,  11) wgrywanie nowych wersji firmware przełącznika FC z wykorzystaniem bezpiecznych protokołów SCP oraz SFTP,  12) wykonywanie kopii bezpieczeństwa konfiguracji przełącznika FC z wykorzystaniem bezpiecznych protokołów SCP oraz SFTP.  20. Przełącznik FC musi mieć możliwość konfiguracji przez:  1) polecenia tekstowe w interfejsie znakowym konsoli terminala,  2) przeglądarkę internetową z interfejsem graficznym lub dedykowane oprogramowanie.  21. Przełącznik FC być wyposażony w następujące narzędzia diagnostyczne i mechanizmy obsługi ruchu FC:  1) logowanie zdarzeń poprzez mechanizm „syslog”,  2) ciągłe monitorowanie parametrów pracy przełącznika, portów, wkładek SFP i sieci fabric z automatycznym powiadamianiem administratora, wyłączeniem pracy portu lub przesunięciem przepływów tzw. slow drain na niski priorytet w przypadku przekroczenia zdefiniowanych wartości granicznych. Powiadamianie administrator musi być możliwe za pomocą wysyłania wiadomości e-mail, pułapki SNMP lub komunikatu w logu,  3) port diagnostyczny tzw. D\_port. Port diagnostyczny musi umożliwiać wykonanie testów sprawdzających komunikację portu przełącznika z wkładką SFP, połączenie optyczne pomiędzy dwoma przełącznikami, testowe obciążenie połączenia pełną przepustowością 16/32/64Gbps oraz pomiar opóźnienia i odległości między przełącznikami z dokładnością co najmniej do 5m dla wkładek SFP 16/32/64Gbps. Testy wykonywane przez port diagnostyczny nie mogą wpływać w żaden sposób na działanie pozostałych portów przełącznika i całej sieci fabric,  4) FCping,  5) FC traceroute,  6) kopiowanie danych dla wybranych przepływów danych na wskazany lokalny port przełącznika do którego podłączony jest analizator FC,  7) przełącznik musi być wyposażony w mechanizm sprzętowego monitorowania przepływów danych automatycznie wykrywanych par komunikujących się urządzeń (przepływów danych). Dla każdego monitorowanego przepływu muszą być gromadzone statystyki dotyczące, co najmniej liczby wysłanych i odebranych ramek, przepustowości, liczby zapisów i odczytów, liczby IOPS, pending IO, IO exchange completion time, IO first response time dla protokołów SCSI oraz NVMe over FC,  8) przełącznik musi być wyposażony w mechanizm sprzętowego generatora ruchu umożliwiającego symulowanie komunikacji w wielodomenowych sieciach SAN bez konieczności angażowania fizycznych urządzeń takich jak serwery lub macierze dyskowe,  9) przełącznik musi być wyposażony w mechanizm umożliwiający kopiowanie pierwszych 64 bajtów ramek dla wybranych przepływów danych do pamięci lokalnej przełącznika w celu dalszej analizy,  10) przełącznik musi być wyposażony w mechanizm umożliwiający sprzętowe identyfikowanie ramek FC oznaczonych parametrem VM ID oraz integrację tego mechanizmu z systemami monitorowania przepływów danych w szczególności w zakresie przepustowości, liczby zapisów i odczytów na sekundę oraz opóźnień operacji zapisu i odczytu (first response time, exchange completion time). Mechanizm musi być obsługiwany dla dowolnego typu macierzy FC, z którą komunikują się monitorowane maszyny wirtualne,  11) przełącznik musi obsługiwać wysyłanie komunikatów FPIN typu: Link Integrity Notification, Delivery Notification, Peer Congestion Notification, Congestion Notification do zarejestrowanych urządzeń końcowych,  12) przełącznik musi obsługiwać wysyłanie sprzętowych sygnałów typu End Device Congestion za pomocą mechanizmu prymitywów FC typu ARB.  22. Przełącznik FC musi być dostarczony z aktywną możliwością przydzielenia co najmniej 22000 tzw. buffer credits do wybranego portu FC przełącznika.  23. Przełącznik FC musi zapewnić możliwość jego zarządzania przez zintegrowany port Ethernet RJ45, konsolowy miniUSB oraz inband IP-over-FC.  24. Przełącznik FC musi zapewniać obsługę protokołu NVMe over FC.  25. Przełącznik FC musi zapewniać obsługę interfejsu zarządzającego REST API.  26. W przełączniku FC musi istnieć możliwość wydzielenia logicznych, izolowanych od siebie przełączników. Każdy z logicznych przełączników musi mieć własny Domain ID, własne usługi fabric (tzw. fabric services), niezależną bazę zoningu oraz możliwość przypisanie dedykowanego administratora.  27. Musi istnieć możliwość połączenia wybranych logicznych przełączników wydzielonych w różnych fizycznych przełącznikach FC za pomocą dedykowanych połączeń ISL. Połączone w ten sposób przełączniki muszą tworzyć pojedynczą sieć fabric.  28. Przełącznik FC musi realizować kategoryzację ruchu między parami urządzeń (initiator - target) oraz przydzielenie takich par urządzeń do kategorii o wysokim, średnim lub niskim priorytecie. Konfiguracja przydziału do różnych klas priorytetów musi się odbywać za pomocą standardowych narzędzi do konfiguracji zoningu.  29. Przełącznik FC musi być wyposażony w mechanizm automatycznej kategoryzacji przepływów danych na podstawie prędkości pracy portu docelowego z przydziałem przepływów o prędkościach 16/8/4Gbps, 32Gbps i 64Gbps do różnych grup. Przepływy danych przydzielone do różnych grup muszą posiadać niezależny flow control i nie mogą wpływać wzajemnie na swoją gospodarkę tzw. buffer credits.  30. Przełącznik FC musi realizować kategoryzację ruchu na podstawie wartości parametru CS\_CTL w nagłówku ramki FC oraz odpowiednie przydzielenie ramki do kategorii o wysokim, średnim lub niskim priorytecie.  31. Wsparcie dla N\_Port ID Virtualization (NPIV). Obsługa, co najmniej 255 wirtualnych urządzeń na pojedynczym porcie przełącznika.  32. Przełącznik FC musi jednocześnie obsługiwać protokoły FCP i NVMe over FC na dowolnych portach przełącznika.  33. Wsparcie dla zarządzania in-band z poziomu mainframe’a poprzez emulację urządzenia kontrolnego ESA/390 lub z-Series I/O Device (czyli Control Unit Port). W ramach zarządzania in-band CUP możliwość konfigurowania FICON Prohibit Dynamic Connectivity Mask (PDCM), Port Address Name, Switch Name, czasu na przełączniku, wyłączenie przełącznika. | Producent oferowanych przełączników: …  Model oferowanych przełączników: …  TAK |
| 2 | Warunki gwarancji | 1. Min. 60 miesięcy gwarancji realizowanej w miejscu instalacji sprzętu, z czasem reakcji do 4 godzin od przyjęcia zgłoszenia, możliwość zgłaszania awarii w trybie 365x7x24 poprzez ogólnopolską linię telefoniczną producenta.  2. Wymagane dołączenie do oferty oświadczenia Producenta potwierdzającego, że serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta.  3. Oświadczenie producenta przełącznika, potwierdzające, że sprzęt pochodzi z oficjalnego kanału dystrybucyjnego producenta.  4. W czasie obowiązywania gwarancji Zamawiający musi mieć możliwość nieodpłatnego pobierania nowych wersji BIOS, firmware i sterowników poprzez stronę www. | TAK |

**ZADANIE 8 – OPROGRAMOWANIE WRAZ Z DEDUPLIKATOREM (1 SZTUKA)**

|  |  |  |  |
| --- | --- | --- | --- |
| **Lp.** | **Komponent** | **Minimalne wymagania** | **Potwierdzenie spełnienia wymagań przez oferowane produkty (skreślić TAK i wpisać NIE, jeżeli nie spełnia minimalnych wymagań), podać dane we wskazanych miejscach** |
| 1 | Wymagania ogólne | 1. Rozwiązanie przeznaczone do zabezpieczenia danych, składające się z:  1) oprogramowania,  2) deduplikatora (przeznaczonego do składowania zabezpieczonych danych).  2. Oprogramowanie będące przedmiotem postępowania musi umożliwiać:  1) realizację backupów w DataCenter,  2) realizację backupów środowisk wirtualnych oraz zdalnych lokalizacji,  3) realizację monitoringu oraz raportowania środowiska backupowego,  4) zabezpieczanie danych w trybie Continuous Data Protection środowisk VMware vSphere.  3. Oferowane oprogramowanie musi licencjonować się na sumaryczną ilość CPU (min. 7 szt.) zabezpieczanego środowiska (bez względu na rozmiar backupowanego wolumenu danych, ilości serwerów, baz danych, wykorzystywanych urządzeń taśmowych czy dyskowych), musi również być zintegrowane z oferowanym deduplikatorem (szczegółowe wymagania dotyczące oprogramowania oraz deduplikatora przedstawione zostały w dalszej części opisu). | Producent oferowanego:  - oprogramowania: ….  - deduplikatora: …  Wersja oferowanego:  - oprogramowania: …  - deduplikatora: …  TAK |
| 2 | Oprogramowanie - wymagania dotyczące backupu serwerów (Data Center) | 1. Wymagana jest możliwość wyboru miejsca deduplikacji w przypadku składowania danych na oferowanym deduplikatorze:  1) na źródle,  2) na medium backupowym.  2. Backup z deduplikacją na źródle (przy składowaniu danych na oferowanym deduplikatorze) musi być dostępny dla wszystkich typów danych w ramach oferowanego rozwiązania: pliki, bazy danych, obrazy maszyn wirtualnych.  3. Oprogramowanie backupowe musi zapewniać bezpośredni backup z każdej zabezpieczanej maszyny bezpośrednio na oferowany deduplikator bez pośrednictwa jakichkolwiek innych serwerów w trybie z deduplikacją na źródle oraz bez deduplikacji na źródle - wymagane obie opcje z możliwością dowolnego użycia oraz możliwością przełączania. Powyższa funkcjonalność nie może wymagać dodatkowej licencji poza zwykłą licencja kliencką. Funkcjonalność musi dostępna dla minimum następujących platform: Windows, RedHat, SuSE.  4. Wymagane jest aby oprogramowanie backupowe zapewniało szybki backup blokowy wielomilionowych systemów plików na maszynach Windows oraz Linux  5. W trakcie backupu oprogramowanie backupowe musi wykonywać kopie zapasowe fizycznych bloków a nie plików. Wymagana możliwość odtworzenia pojedynczego pliku z tak zrealizowanego backupu.  6. W celu minimalizacji czasu backupu oprogramowanie backupowe nie może indeksować plików znajdujących się na zabezpieczanym wolumenie (zaindeksowanie wielu milionów plików powoduje duże wydłużenie czasu backupu).  7. Wymagane jest aby oprogramowanie backupowe zapewniało szybki inkrementalny backup blokowy wielomilionowych systemów plików na maszynach Windows oraz Linux.  8. W trakcie backupu inkrementalnego wielomilionowych systemów plików na maszynach Windows oraz Linux oprogramowanie backupowe musi odczytywać tylko te fragmenty dysku które zmieniły się od ostatniego backupu.  9. W celu minimalizacji czasu backupu oprogramowanie backupowe nie może indeksować plików backupu inkrementalnego znajdujących się na zabezpieczanym wolumenie (zaindeksowanie wielu milionów plików powodowałoby duże wydłużenie czasu backupu).  10. Oprogramowanie backupowe musi mieć możliwość łączenia backupu blokowego pełnego i inkrementalnego w jeden pełen backup. Łączenie backupów musi odbywać się na oferowanym deduplikatorze bez fizycznego odczytu łączonych danych (łączeniu muszą podlegać tylko metadane opisujące backup pełny oraz inkrementalny).  11. Po połączeniu backupu pełnego i inkrementalnego muszą być dostępne dwa backupy pełne: dotychczas dostępny backup pełny i nowy backup pełny uzyskany w drodze łączenia z backupem inkrementalnym.  12. Wymagana możliwość automatycznego łączenia backupu blokowego pełnego i inkrementalnego po wykonaniu blokowego backupu inkrementalnego w celu uzyskania aktualnego backupu pełnego.  13. Oferowane rozwiązanie backupowe musi przechowywać całość własnych informacji (informacje o backupach, napędach taśmowych, mediach) w centralnym pojedynczym katalogu, skopiowanie centralnego katalogu systemu backupu na inną maszynę musi pozwolić na uruchomienie na drugiej maszynie serwera backupu identycznego z oryginalnym.  14. Ze względów bezpieczeństwa rozwiązanie backupowe musi mieć możliwość wykonania kopii wewnętrznej bazy danych w trakcie pracy systemu bez konieczności ograniczania jego funkcjonalności.  15. Oprogramowanie backupowe musi mieć możliwość backupu własnej bazy danych na następujące nośniki:  1) urządzenie dyskowe,  2) deduplikator będący przedmiotem zapytania,  3) nośniki taśmowe.  16. W przypadku backupu na nośniki taśmowe wymagana możliwość zdefiniowania puli taśm (zawierającej jedną lub więcej taśm) na którą będą zapisywane tylko i wyłącznie backupy wewnętrznej bazy danych systemu backupowego.  17. Oprogramowanie backupowe musi mieć możliwość automatycznego wykonywania backupu własnej bazy danych.  18. Oprogramowanie backupowe po każdorazowym backupie wewnętrznej bazy danych musi raportować miejsce, w którym znajduje się ostatni backup wewnętrznej bazy danych oprogramowania backupowego.  19. Backup własnej bazy danych musi pozwalać na odtworzenie wszystkich ustawień systemu backupowego na zupełnie nowej, świeżo zainstalowanej instancji oprogramowania backupowego.  20. W przypadku backupu systemów produkcyjnych (klientów systemu backupu) na nośniki taśmowe, oferowane oprogramowanie backupowe musi umożliwiać zapisywanie backupów o tym samym terminie ważności na jednej, tej samej, z góry zdefiniowanej puli taśm (zawierającej jedną lub więcej taśm).  21. System musi zapisywać dane na taśmach - zoptymalizowane w sposób eliminujący potrzebę wykonywania dodatkowych działań (nawet automatycznych) w celu ich optymalizacji.  22. W przypadku gdy w puli taśmowej zabraknie taśm na których można zapisywać nowe backupy, oprogramowanie backupowe musi mieć możliwość automatycznego przyporządkowania:  1) wolnych, nieprzyporządkowanych taśm znajdujących się w bibliotece,  2) nieużywanych lub przeterminowanych taśm z innych pul taśmowych.  23. W przypadku użycia biblioteki taśmowej (backup, replikacja z oferowanego deduplikatora sprzętowego na taśmę), oferowany system musi generować samoopisujące się taśmy dla całości zapisywanych taśm, co oznacza to, że wyjęcie jakiejkolwiek taśmy z biblioteki i włożenie jej do zupełnie innej biblioteki zarządzanej przez zupełnie inną instancję oferowanego oprogramowania backupowego (w tym również działającą na innym systemie operacyjnym) musi pozwolić na odtworzenie danych znajdujących się na ww. taśmie.  24. Oferowane rozwiązanie musi generować somoopisujące się zbiory danych zarówno na oferowanym deduplikatorze jak i na taśmach. Utrata wewnętrznych danych oprogramowania backupowego nie może powodować braku możliwości odtworzenia jakichkolwiek zbiorów z oferowanego deduplikatora bądź taśm.  25. Oprogramowanie backupowe musi umożliwiać łączenie strumieni backupowych z wielu zabezpieczanych serwerów w sieci LAN i bezpośredni zapis na napędzie taśmowym (multiplexing).  26. Oprogramowanie backupowe musi umożliwiać zarządzanie bezpośrednią replikacją backupów między deduplikatorami oferowanego typu (replikacja realizowana na poziomie deduplikatorów) - bezpośrednio z poziomu interfejsu oprogramowania backupowego przy spełnieniu wszystkich poniższych wymagań  1) replikacji podlegają tylko te bloki które nie znajdują się na docelowym oferowanym deduplikatorze  2) replikacja między deduplikatorami może nastąpić zarówno bezpośrednio po zakończeniu backupu jak również zgodnie z kalendarzem  3) oferowane oprogramowanie backupowe przechowuje informacje o wszystkich kopiach danych znajdujących się na deduplikatorach m.in. źródłowych jak i po replikacji  27. GUI oferowanego oprogramowania backupowego powinien umożliwiać wybór urządzenia deduplikacyjnego z którego zostanie wykonane odtwarzanie - w efekcie umożliwiając odtworzenie z oryginalnej kopii backupowej bądź ze zreplikowanej kopii backupowej.  28. Oprogramowanie backupowe musi mieć możliwość kopiowania backupów między dowolnymi mediami:  1) deduplikatorami oferowanego typu,  2) dyskowymi (CIFS, NFS),  3) taśmowymi.  29. Oprogramowanie backupowe musi zapewniać różny czas ważności danych na podstawowym nośniku i nośniku zawierającym kopię (replikę backupu). Definicja czasu przechowywania kopii (repliki) powinna być określenia w momencie definiowania zadania duplikacji/kopiowania zarówno z interfejsu graficznego jak i z command line.  30. Oprogramowanie backupowe musi pozwalać na następujące rodzaje backupu systemu plików:  1) pełny,  2) różnicowy,  3) inkrementalny.  31. Oprogramowanie backupowe musi pozwalać na łączenie backupów pełnych i inkrementalnych w jeden pełen backup. Proces ten musi być niewidoczny dla systemu plików którego dotyczą backupy pełne i inkrementalne. Proces odtworzenia danych z połączonego backupu pełnego i inkrementalnego musi być identyczny z odtworzeniem danych z normalnie wykonanego backupu pełnego w zakresie:  1) zarządzania,  2) wydajności.  32. Oprogramowanie backupowe musi pozwalać na łączenie backupów pełnych i inkrementalnych bez odczytu danych z oferowanego deduplikatora.  33. Łączenie backupów pełnych i inkrementalnych musi być realizowane przez oferowany deduplikator, jedynie zarządzanie (start, kalendarz łączenia) procesem łączenia backupów pełnych i inkrementalnych musi być realizowany przez aplikację backupową.  34. Oprogramowanie backupowe musi pozwalać na zatrzymanie procesu backupu oraz jego wznowienie od momentu zatrzymania.  35. W przypadku nieudanego backupu dla systemu plików (na przykład zerwanie łączności), oprogramowanie backupowe musi pozwalać na wznowienie backupu od ostatnio poprawnie zbackupowanego:  1) katalogu,  2) pliku.  36. W przypadku awarii fragmentu zapisanej taśmy, oprogramowanie backupowe musi umożliwiać odtworzenie całości plików, które znajdują się na nieuszkodzonej części nośnika.  37. W przypadku konsoli oprogramowania backupowego wymagana możliwość definiowania ważności danych (backupów) na podstawie kryteriów czasowych (dni, miesiące, lata). Po okresie ważności backupy muszą być automatycznie usunięte.  38. Oprogramowanie backupowe musi wspierać (wymagane wsparcie producenta) następujące systemy operacyjne: Windows (także Microsoft Cluster) , Linux (Red Hat, SUSE).  39. Oprogramowanie backupowe musi wspierać (wymagane wsparcie producenta) backup online następujących baz danych i aplikacji: MS Exchange, MS SQL, Oracle, IBM DB2, PostgreSQL, mySQL, SharePoint.  40. W przypadku zabezpieczania baz danych, oferowany system backupowy musi umożliwiać inicjalizację backupu poprzez określone zdarzenie: np. ilość logów, czas który upłynął od ostatniego zdarzenia lub inne zdarzenie zdefiniowane przez użytkownika.  41. Dla baz danych MSSQL wymagana możliwość inicjowania backupów przez administratora MSSQL przy spełnieniu wszystkich poniższych wymagań:  1) backup jest wykonywany przez oferowane oprogramowanie backupowe,  2) inicjowanie backupu z graficznego interfejsu będącego częścią MSSQL Management Studio,  3) możliwość wyboru backupu pełnego, różnicowego oraz logów,  4) backup inicjowany przez administratora MSSQL bez konieczności zaangażowania administratora oferowanego rozwiązania backupowego.  42. Dla baz danych MSSQL wymagana możliwość odtworzenia backupów przez administratora MSSQL przy spełnieniu wszystkich poniższych wymagań:  1) odtworzenie dowolnego backupu wykonanego przez oferowane rozwiązanie backupowe,  2) zarządzanie odtwarzaniem z graficznego interfejsu będącego częścią MSSQL Management Studio,  3) możliwość odtworzenia do dowolnego punktu w czasie wybranego przez administratora MSSQL w ramach przechowywanych przez oferowane oprogramowanie backupowe logów MSSQL,  4) odtworzenie bazy danych przez administratora MSSQL bez konieczności zaangażowania administratora oferowanego rozwiązania backupowego.  43. Oferowane rozwiązanie backupowe musi integrować się funkcjonalnością FRA (Fast Recovery Area) bazą danych Oracle. Wymagane spełnienie wszystkie poniższych funkcjonalności:  1) administrator Oracle wykonuje backupy narzędziami RMAN do przestrzeni FRA,  2) oferowane rozwiązanie backupowe automatycznie kopiuje backupy z przestrzeni Oracle FRA na media zarządzane przez oferowane rozwiązanie backupowe,  3) definiowanie parametrów zadania kopiowania backupów przestrzeni FRA na media zarządzane przez oferowane rozwiązanie backupowe z poziomu interfejsu graficznego,  4) odtworzenie danych możliwe przez administratora Oracle.  44. Oprogramowanie backupowe musi mieć możliwość odtwarzania pojedynczego serwera Windows bez ponownej instalacji systemu operacyjnego.  45. Rozwiązanie backupowe musi mieć możliwość odtworzenia plików na docelową maszynę w oddziale z poziomu centralnej konsoli systemu backupowego. Nie może być wymagane logowanie się na odtwarzaną maszynę w celu odtworzenia danych z systemu backupowego.  46. Wymagana możliwość odtworzenia danych  1) z zabezpieczanego serwera / komputera,  2) z konsoli systemu backupowego. | TAK |
| 3 | Oprogramowanie - wymagania dotyczące backupu zdalnych lokalizacji oraz środowisk wirtualnych | 1. Oprogramowanie backupowe musi wspierać (wymagane wsparcie producenta) następujące systemy operacyjne: Windows (także Microsoft Cluster) , Linux (Red Hat, SUSE).  2. Backup zasobów plików w przypadku powyższych systemów musi podlegać deduplikacji ze zmiennym blokiem na zabezpieczanej maszynie zgodnie z przedstawionymi wymaganiami.  3. Oprogramowanie backupowe musi wspierać (wymagane wsparcie producenta) backup online następujących baz danych, aplikacji i środowisk: MS Exchange, MS SQL, Oracle, IBM DB2, SharePoint, VM na VMware vSphere, Hyper-V.  4. Backup powyższych baz danych i aplikacji musi podlegać deduplikacji ze zmiennym blokiem na zabezpieczanej maszynie zgodnie z przedstawionymi wymaganiami.  5. W przypadku zabezpieczania baz danych i aplikacji wymagana możliwość realizacji kopii zapasowej kilkoma strumieniami jednocześnie (minimum 10 jednoczesnych strumieni).  6. Zabezpieczane serwery muszą być backupowane bezpośrednio na dyski oferowanego deduplikatora bez pośrednictwa jakichkolwiek innych urządzeń / serwerów.  Dotyczy to backupów lokalnych oraz zdalnych.  7. Oprogramowanie backupowe musi umożliwiać dla sieci lokalnej:  1) backup pojedynczych plików,  2) backup całych systemów plików,  3) backup baz danych w trakcie ich normalnej pracy,  4) backup ustawień systemu operacyjnego Windows,  5) backup całych obrazów maszyn wirtualnych systemu VMware vSphere,  6) backup całych obrazów maszyn wirtualnych systemu Hyper-V.  8. Rozwiązanie backupowe musi umożliwiać transfer danych bezpośrednio z innych lokalizacji do oferowanego deduplikatora bez konieczności instalacji dodatkowego sprzętu w innej lokalizacji. Powyższa funkcjonalność wymagana jest dla następujących typów danych:  1) backup pojedynczych plików,  2) backup całych systemów plików,  3) backup baz danych w trakcie ich normalnej pracy.  9. Wymaga się aby oferowane rozwiązanie backupowe było w pełni konfigurowalne z konsoli znajdującej się w lokalizacji centralnej, w szczególności backupy maszyn w innych lokalizacjach (bazy, pliki) czy też backupy laptopów muszą być konfigurowalne z poziomu centralnej konsoli bez konieczności logowania się na zabezpieczaną maszynę.  10. Oferowane rozwiązanie backupowe musi umożliwiać odtworzenie plików, baz danych na docelową maszynę w innej lokalizacji - z poziomu centralnej konsoli systemu backupowego. Wymagany scenariusz nie może wymagać logowania się na odtwarzaną maszynę celem odtworzenia danych z systemu backupowego.  11. W celu minimalizacji ilości przesyłanych danych, oferowane rozwiązanie musi mieć możliwość przesyłania odtwarzanych danych z medium backupowego do docelowego serwera w postaci skompresowanej, odtwarzane dane powinny zostać rozkompresowane na docelowym serwerze przez agenta oferowanego systemu.  12. Oprogramowanie backupowe musi posiadać funkcjonalność podziału danych (plików, baz danych, obrazów maszyn wirtualnych) na bloki o zmiennej długości. System musi się dopasowywać do struktury dokumentu zapewniając podział na bloki o różnej długości w ramach pojedynczego dokumentu w celu polepszenia efektywności deduplikacji.  13. Podział na bloki musi następować bezpośrednio na zabezpieczanym serwerze.  14. Używany algorytm deduplikacji musi generować zmienny blok w przypadku backupu pojedynczego dokumentu. Bloki wysyłane w trakcie backupu pojedynczego dokumentu z zabezpieczanej maszyny do oferowanego deduplikatora muszą wynikać i odpowiadać rozmiarem - długości bloków używanych przez oferowany deduplikator.  15. Wymaga się aby oprogramowanie backupowe przesyłało na oferowany deduplikator tylko unikalne bloki nie znajdujące się na tym urządzeniu, w efekcie skracając czas backupu, obciążenie procesora i zmniejszając ruch w sieci WAN / LAN.  16. Funkcjonalność deduplikacji nie może wymagać instalacji dodatkowych modułów programowych po stronie klienckiej lub serwera backupowego.  17. Oprogramowanie backupowe nie może odczytywać tych plików z systemu dyskowego, które się nie zmieniły w stosunku do ostatniego backupu. Raz zbackupowany plik nie może być ponownie odczytywany, chyba, że zmieni się jego zawartość.  18. Wymaga się aby oprogramowanie backupowe realizowało wyłącznie - logicznie pełne backupy systemu plików. Z zabezpieczanego systemu plików muszą odczytywane tylko nowe lub zmienione pliki, do oferowanego deduplikatora powinny być przesyłane dane po deduplikacji, jednak każdy finalny backup musi być logicznie pełnym backupem. W wewnętrznej strukturze systemu musi być przechowywana informacja o każdym backupie i należących do niego danych (blokach), dzięki czemu odtworzenie jakichkolwiek danych plikowych musi być pojedynczym zadaniem identycznym z odtworzeniem danych z pełnego backupu.  19. Wymagana możliwość definiowania w konsoli oprogramowania backupowego ważności (retencji) danych (backupów) na podstawie kryteriów czasowych (dni, miesiące, lata). Po okresie ważności backupy musza być automatycznie usunięte.  20. Wymagana możliwość tworzenia z poziomu GUI (konsoli graficznej) w przypadku oferowanego oprogramowania backupowego, polityk w których zdefiniowano:  1) czas przechowywania backupów dziennych,  2) czas przechowywania backupów tygodniowych,  3) czas przechowywania backupów miesięcznych,  4) czas przechowywania backupów rocznych.  21. Oferowane rozwiązanie musi umożliwiać tworzenie wykluczeń, czyli elementów nie podlegających backupowi w ramach zadania backupowego. Wymagana możliwość tworzenia wykluczeń dla dowolnej kombinacji następujących elementów:  1) wybranych typów plików, np. dla plików z rozszerzeniem mp3,  2) dla całych katalogów (np.: c:\windows),  3) dla pojedynczych plików.  22. Oferowane rozwiązanie musi mieć możliwość zdefiniowania aby ostatni backup dowolnego zbioru danych nigdy się nie przeterminował. Oznacza to, że jeśli dany zasób nie jest backupowany to automatycznie ostatni ważny backup tego zasobu będzie przechowywany bezterminowo, jedynie administrator może zdecydować o jego usunięciu.  23. Konsola zarządzająca systemem backupowym musi integrować się z Active Directory. Musi być możliwość przydzielania użytkownikom i grupom Active Directory dostępnych ról (min. administrator, monitoring, tylko wykonywanie odtworzeń) w systemie backupowym.  24. Wymagana możliwość generowania (poprzez konsolę) raportów określających zajętość przestrzeni przeznaczonej na składowanie deduplikatów.  25. Bloki przesyłane z zabezpieczanych serwerów do oferowanego deduplikatora muszą być kompresowane i szyfrowane algorytmem z kluczem minimum 256-bitowym.  26. Oprogramowanie backupowe musi pozwalać na odtwarzanie danych poprzez: wybór odtwarzanych danych, odtworzenie danych w jednym kroku.  27. Wymagana możliwość limitowania wielkości zadania backupowego, jeśli zadanie backupowe przekroczy zdefiniowaną wielkość wówczas nie może być zapisane w systemie backupowym.  28. Rozwiązanie backupowe musi wspierać backup i odtwarzanie środowisk VMware vSphere 7.x, 8.x  29. Oprogramowanie backupowe musi umożliwiać w przypadku środowisk VMware następujące typy backupu:  1) backup całych maszyn wirtualnych,  2) backup pojedynczych, wybranych dysków maszyny wirtualnej vmdk,  3) musi istnieć możliwość zastosowania wyrażeń regularnych do określenia które wirtualne dyski VMware mają być backupowane,  4) w trakcie backupu odczytowi z systemu dyskowego mają podlegać tylko zmienione bloki wirtualnych maszyn systemu VMware (wymagane wykorzystanie mechanizmu CBT systemu VMware),  5) wykonywanie backupu obrazów maszyn wirtualnych VMware nie może wymagać bufora dyskowego na kopię obrazów maszyn wirtualnych (plików vmdk).  30. Powyższe metody backupu maszyn wirtualnych muszą podlegać deduplikacji ze zmiennym blokiem przed wysłaniem danych do medium backupowego zgodnie z wymaganiami dla deduplikacji powyżej.  31. Powyższe metody backupu muszą być wbudowane w oferowany system backupu, nie mogą wymagać tworzenia skryptów/dodatkowych komend.  32. Oferowany system musi pozwalać na szybkie odtworzenie  1) całych obrazów maszyn wirtualnych,  2) pojedynczych dysków maszyny wirtualnej z backupu całej maszyny wirtualnej.  33. Wymaga się aby oferowane rozwiązanie backupowe umożliwiało odtwarzanie obrazów maszyn wirtualnych VMware z następującymi funkcjonalnościami:  1) odtwarzanie całych maszyn wirtualnych musi wykorzystywać mechanizm CBT systemu VMware – odtwarzane są tylko te bloki wirtualnej maszyny/dysku które uległy zmianie od ostatniego backupu,  2) odtwarzanie pojedynczych dysków maszyn wirtualnych musi wykorzystywać mechanizm CBT systemu VMware – odtwarzane są tylko te bloki wirtualnej maszyny/dysku które uległy zmianie od ostatniego backupu,  3) odtworzenie pojedynczych plików z backupu obrazu maszyny wirtualnej bez konieczności odtworzenia całej maszyny wirtualnej, funkcjonalność ta musi być dostępna dla obrazów maszyn wirtualnych z zainstalowanym systemem operacyjnym Windows oraz Linux,  4) możliwość zamontowania na dowolnym serwerze (fizycznym lub wirtualnym) zbackupowanych obrazów maszyn wirtualnych Windows (plików vmdk maszyny wirtualnej Windows), w efekcie metoda ta nie odtwarza backupów a jedynie umożliwia na przeglądanie zawartości plików vmdk w backupie z poziomu Eksploratora Plików Windows na dowolnej maszynie.  34. Oferowane rozwiązanie backupowe musi umożliwiać uruchomienie maszyn wirtualnych bezpośrednio z oferowanego dedupliktora w oparciu o zrealizowany backup, bez konieczności odtwarzania backupu (tzw. Instant Access) – wymagane formalne wsparcie tej funkcjonalności zarówno od strony oferowanej aplikacji backup’owej jak i oferowanego deduplikatora.  35. Oferowane oprogramowanie backupowe musi mieć możliwość prezentacji (bez konieczności odtworzenia) zbackupowanych obrazów maszyn wirtualnych VMware (plików vmdk) jako katalogów na maszynie fizycznej w celu ich przeszukiwania (wymagane przeszukiwanie po nazwach plików jak również zawartości plików) z poziomu systemu operacyjnego maszyny fizycznej.  36. Oferowane oprogramowanie backupowe musi mieć możliwość backupu/odtworzenia w trybie „image backup” (backup plików vmdk) maszyn wirtualnych znajdujących się na serwerach VMware ESX bez udziału vCenter.  37. Wymagana skalowalność rozwiązania dla środowisk VMware na poziomie minimum 2000 maszyn wirtualnych w ramach pojedynczej instancji systemu backupu.  38. Oferowane oprogramowanie backupowe musi mieć możliwość automatycznego sprawdzania (weryfikacji) zbackupowanych maszyn wirtualnych VMware, wymagana możliwość ustawienia kalendarza weryfikacji maszyn wirtualnych VMware.  39. Weryfikacja maszyn wirtualnych musi zapewniać minimum:  1) odtworzenie maszyny wirtualnej na zdefiniowanym Data Center/Data Store,  2) weryfikację podstawowych procesów,  3) możliwość dołączenia własnego skryptu weryfikującego wybrane elementy maszyny wirtualnej.  Wymagana dostępność informacji w konsoli systemu backupu o statusie (poprawna/niepoprawna) weryfikacji maszyny wirtualnej.  40. Administrator (właściciel) danej maszyny wirtualnej VMware musi mieć możliwość samodzielnego (bez konieczności kontaktu z administratorem backupu czy tez administratorem VMware) odtworzenia pojedynczych plików z dowolnego backupu obrazu jego maszyny wirtualnej.  41. Oprogramowanie backupowe musi zawsze przechowywać pełne backupy obrazów maszyn wirtualnych środowiska VMware dla każdej wykonanej w przeszłości kopii zapasowej. Każdy backup obrazu maszyny wirtualnej musi być backupem pełnym.  42. Oferowane rozwiązanie backupowe musi umożliwiać na tworzenie automatycznych polityk backupowych dla folderu, resource pool, systemu VMware. Oznacza to, że dodanie maszyny wirtualnej do folderu, hosta czy resource pooli w systemie VMware vSphere spowoduje automatyczne backupowanie dodanej maszyny wirtualnej zgodnie z polityka zdefiniowana dla folderu hosta czy resource pooli w systemie VMware.  43. Rozwiązanie backupowe musi umożliwiać zdefiniowanie polityk backupowych dostępnych dla administratora systemu VMware z poziomu vCenter. Administrator VMware musi mieć możliwość przyporządkowania nowo tworzonych maszyn wirtualnych do polityk backupowych.  44. Wymaga się aby inicjowanie backupu oraz odtwarzanie maszyn wirtualnych VMware dostępne było z poziomu graficznego interfejsu, linii komend oraz przez REST API.  45. Oferowane oprogramowanie backupowe musi umożliwiać dla środowisk Hyper-V:  1) backup pojedynczych plików i baz danych z maszyny wirtualnej ze środka maszyny wirtualnej Hyper-V,  2) backup całych maszyn wirtualnych (czyli plików vhd reprezentujących wirtualną maszynę), takie wykonanie backupu nie może wymagać bufora dyskowego na kopię obrazów maszyn wirtualnych (plików vhd),  3) wykonywanie backupu jak w punkcie 2) musi umożliwiać na odtworzenie pojedynczych plików z obrazu maszyny wirtualnej bez konieczności odtworzenia całej maszyny wirtualnej, funkcjonalność ta musi być dostępna dla obrazów maszyn wirtualnych z zainstalowanym systemem operacyjnym Windows.  a) dopuszcza się wykonywanie snapshotów vss maszyn wirtualnych i użycie ich w trakcie backupu obrazów maszyn wirtualnych,  b) powyższe metody backupu muszą być wbudowane w system backupu i w pełni automatyczne bez wykorzystania skryptów/dodatkowych komend,  c) powyższe metody backupu maszyn wirtualnych muszą podlegać deduplikacji ze zmiennym blokiem w momencie odczytu danych zgodnie z wymaganiami powyżej.  46. Oferowane oprogramowanie backupowe musi zapewniać spójny backup Exchange / MSSQL przy backupie obrazów maszyn wirtualnych środowiska Hyper-V  47. Wymagana możliwość odtworzenia danych  1) z zabezpieczanego serwera / komputera,  2) z konsoli systemu backupowego.  48. Wymagana możliwość odtworzenia:  1) pojedynczego pliku,  2) zabezpieczanej bazy danych.  49. W przypadku odtwarzania istniejącego systemu plików (systemu plików który utracił część zasobów) oprogramowanie backupowe musi samo, automatycznie sprawdzać których plików znajdujących się w backupie, brakuje na odtwarzanej maszynie a następnie odczytać z backupu i przesłać tylko te pliki które znajdują się w backupie i których brakuje na odtwarzanej maszynie.  50. Oferowany system backupu musi być dostępny (dla backupu i odtwarzania) przez 24h na dobę 7 dni w tygodniu, wyklucza się istnienie okresów w przypadku których system backupowy nie może wykonywać backupu lub odtwarzania (tzw. BLACKOUT WINDOWS).  51. Wymaga się aby oferowany system backupu posiadał możliwość bezpośredniego raportowania o błędach do serwisu producenta.  52. Oferowany system backupu powinien mieć możliwość instalacji agentów jako plików msi. Wymagana możliwość automatyzacji instalacji agentów poprzez uruchomienie skryptu na zabezpieczanej maszynie, przyporządkowującego maszynę automatycznie do określonej polityki backupowej.  53. Oferowany system backupu musi mieć możliwość automatycznej aktualizacji oprogramowania agentów wykonywanej bezpośrednio z serwera backupu.  54. Oferowany system musi pozwalać na backup serwerów NAS z następującymi funkcjonalnościami:  1) w trakcie backupu z systemu NAS muszą być wysyłane do medium backupowego tylko zmienione pliki od ostatniego backupu,  2) w przypadku odtwarzania danych z backupu, uprawnienia użytkowników również są odtwarzane,  3) integracja z protokołem NDMP systemów NAS,  4) odtwarzanie plików z backupu NDMP bezpośrednio na platformę Windows/Linux. | TAK |
| 4 | Oprogramowanie – wymagania dotyczących monitorowania, raportowania oraz przeszukiwania backupów | 1. W ramach dostarczonych licencji musi być zapewniona możliwość monitorowania, raportowania, szczegółowego rozliczania z użycia komponentów systemu backupowego oraz analizy błędów dla środowiska kopii zapasowej Zamawiającego. Wymagana dostępność następujących raportów:  1) podsumowanie zadań backupowych (liczba backupów udanych, nieudanych, aktywnych, łączny rozmiar zbackupowanych danych),  2) podsumowanie zadań odtworzeniowych (liczba odtworzeń udanych, nieudanych, aktywnych, łączny rozmiar odtworzonych danych danych),  3) zbiorcze procentowe zestawienie udanych zadań backupowych z poszczególnych serwerów,  4) zbiorcze zestawienie zabezpieczanych serwerów które w sposób ciągły (kilka razy pod rząd) maja problem z backupami,  5) zestawienie zabezpieczanych systemów plików które w ogóle nie są backupowane,  6) spodziewany czas odtwarzania zabezpieczanego serwera oraz potencjalnej utraty danych (czas między ostatnim backupem a chwilą awarii),  7) najmniej wiarygodne zabezpieczanych serwery (procent nieudanych backupów),  8) lista najwolniejszych/najszybszych zabezpieczanych maszyn,  9) poziom SLA (procentowa liczba udanych backupów) w odniesieniu do poziomu założonego,  10) mierzenie poziomu SLA dla poszczególnych zabezpieczanych serwerów przy uwzględnieniu założonego okna backupowego i RPO (punktu do którego się odtwarzamy),  11) liczba danych backupowanych dziennie,  12) liczba zadań backupowych dziennie,  13) zużycie zasobów na serwerach backupowych (procesor, pamięć, karty sieciowe LAN, SAN),  14) zużycie mediów backupowych i napędów taśmowych,  15) aktualna konfiguracja systemu backupowego,  16) historia zmian konfiguracji systemu backupowego,  17) posiadane licencje systemu backupowego,  18) wykorzystanie systemu backupowego przez poszczególne działy / grupy użytkowników (chargeback per cost center).  2. W ramach dostarczonych licencji wymagana możliwość zaindeksowania oraz przeszukiwania backupów z poziomu graficznego interface’u (GUI), wymagana również możliwość wyszukania dowolnych fraz w nazwach plików. | TAK |
| 5 | Oprogramowanie – wymagania dotyczące ochrony w trybie Continuous Data Protection dla środowisk VMware vSphere | 1. Integracja na poziomie VMware vCenter Plug-in (ORCHESTRATION, MANAGEMENT), vSphere Web Client GUI.  2. Wsparcie dla HA, DRS, S-DRS, VMotion, S-VMotion.  3. Możliwość integracji z VMware vRealize Operations Manager.  4. Rozwiązanie dostarczane w postaci oprogramowania instalowanego na platformie ESXi.  5. Skalowalność zapewniająca wsparcie dla 8000 VM w obrębie poj. vCenter.  6. Zabepieczenie dowolnej maszyny wirtualnej wraz z aplikacjami w trybie ciągłym tzn. umożliwiającym odtworzenie do dowolnego punktu w czasie (tzw. PIT – Point In Time), wymagane wsparcie dla VMware ESXi 7.x, 8.x.  7. możliwość tworzenia tzw. CONSISTENCY GROUP zapewniających identyczną konsystencję dla przynależących do danej grupy maszyn wirtualnych (VM), wymagane wsparcie dla min. 250 CONSISTENCY GROUP.  8. Zabezpieczenie realizowane za pośrednictwem ciągłej replikacji (a nie za pomocą SNAPSHOT’ów ) na poziomie VMDK oraz RDM, niezależnie od użytego storage’u (tzw. Storage Agnostic - warunkiem jest wsparcie przez VMware), wymagane wsparcie dla połączeń: FC, FCoE, iSCSI, NAS oraz DAS.  9. Wsparcie dla replikacji (bi-directional) asynchronicznej oraz synchronicznej (realizowanej na poziomie dostarczanego oprogramowania), połączonych z mechanizmem tzw. JOURNALING umożliwiającego odnotowanie wszystkich zmian zabezpieczanego środowiska.  10. Odporność na krótkotrwałe problemy (przeciążenie, zaniki) związane z siecią WAN.  11. Wbudowana funkcjonalność deduplikacji oraz kompresji w przypadku transmisji danych poprzez WAN.  12. Wsparcie dla równoległej replikacji zabezpieczanego środowiska do różnych ośrodków docelowych (min. 3-ech), wsparcie dla replikacji równoległej musi być zapewnione również na poziomie grup konsystencji (CONSISTENCY GROUP).  13. Oferowane rozwiązanie musi umożliwiać:  1) stworzenia DISASTER RECOVERY dla całego zabezpieczanego wirtualnego środowiska zbudowanego w oparciu o VMware,  2) operacyjne odtwarzanie dowolnej maszyny VM wraz z aplikacjami,  3) migracji danych w trybie on-line na inne zasoby dyskowe.  14. Równoległe wsparcie środowisk lokalnych oraz zdalnych, wymagana możliwość pracy w 3-ech trybach, tzw.: CDP (Continuous Data Protection - tryb replikacji lokalnej), CRR (Continuous Remote Replication - tryb replikacji zdalnej), CLR (Continuous Local and Remote Replication, połączenie CDP oraz CLR - tryb replikacji lokalnej oraz zdalnej) w ramach dostarczonych licencji.  15. Granularność umożliwiająca pominięcie określonych plików VMDK związanych z wirtualnymi serwerami VM objętych protekcją  architektura FAULT-TOLERANT, brak pojedynczego punktu awarii  16. Wyskalowanie systemu powinno gwarantować RPO (Recovery Point Objective) w przypadku codziennej pracy ciągłej na poziomie pojedynczych sekund.  17. Oferowana konfiguracja systemu powinna zapewnić następującą retencję przechowywanych kopii bezpieczeństwa:  1) RPO=30s z ostatnich 24h,  2) RPO=24h z ostatniego tygodnia,  3) RPO=1tydzień z ostatniego miesiąca  18. Możliwość odtworzenia zabezpieczanego środowiska do dowolnego punktu w czasie.  19. Możliwość trybu pracy umożliwiającego objęciem protekcją w sposób automatyczny nowo dodanych maszyn wirtualnych (VM).  20. Rozwiązanie powinno dopuszczać zmiany HW na poziomie infrastruktury zabezpieczanego środowiska bez negatywnego wpływu na działanie systemu.  21. Możliwość użycia mechanizmu typu BOOKMARK dla oznaczenia konsystentnych kopii zabezpieczanych aplikacji.  22. Wsparcie dla VSS, zapewnienie konsystencji aplikacji na poziomie VSS.  23. Możliwość automatycznego przeprowadzania operacji typu FAILOVER/FAILBACK do dowolnego punktu w czasie dla określonych produkcyjnych serwerów wirtualnych (VM), w tym: odtworzenie, uruchomienie (z zachowaniem wymaganej sekwencji), konfigurację.  24. Możliwość automatycznego przeprowadzania operacji typu FAILOVER/FAILBACK do dowolnego punktu w czasie określonych testowych maszyn wirtualnych (VM).  25. Możliwość automatycznego zainicjowania procesu REVERSE REPLICATION w przypadku procesów FAILOVER/FAILBACK.  26. Możliwość przeprowadzania testów DR bez wpływu na zabezpieczane serwery produkcyjne oraz bez konieczności zmian w działaniu replikacji (np.: PAUSE, REVERSE).  27. Możliwość skryptowego tworzenia planów RECOVERY. | TAK |
| 6 | Deduplikator sprzętowy | 1. Urządzenie musi być przeznaczone do deduplikacji i przechowywania kopii zapasowych.  2. Dostarczone urządzenie musi oferować przestrzeń min. 32TB netto (powierzchni użytkowej) bez uwzględniania mechanizmów protekcji – przestrzeń dedykowana do gromadzenia deduplikatów, wymagana skalowalność do min. 170TB netto (powierzchni użytkowej widocznej po założeniu systemu plików)  3. Dostarczone urządzenie umożliwia rozbudowę o warstwę typu CLOUD dedykowaną do długotrwałego przechowywania danych (tzw. Long Term Retention) – dane o określonej retencji (zgodnie z założoną polityka retencyjną), bez pośrednictwa dodatkowych urządzeń (typu GATEWAY) powinny zostać przemigrowane (w postaci zdeduplikowanej) na dodatkową warstwę, wymagane wsparcie dla AWS, Microsoft Azure oraz Google GCP. Wymagana enkrypcja danych przechowywanych na warstwie typu CLOUD. Wymagane dostarczenie licencji na przestrzeń min. 60TB netto dla warstwy CLOUD w ramach zaoferowanej ceny. Wymagana funkcjonalność jest oficjalnie wspierana w przypadku oferowanej aplikacji backup’owej. (Waga: 10 pkt)  4. Oferowane urządzenie musi posiadać minimum:  1) 4 porty Eth 10Gb/s OP (wraz z 4-a wkładkami SFP+),  wymagana możliwość obsługi każdym z ww. portów protokołów CIFS, NFS, deduplikacja na źródle.  2) 2 porty FC 16Gb/s, wymagana możliwość obsługi poprzez porty FC protokołów VTL oraz deduplikacja na źródle.  5. Oferowane pojedyncze urządzenie musi osiągać zagregowaną wydajność (dla maksymalnej konfiguracji) protokołami: NFS co najmniej 10 TB/h (dane podawane przez producenta) oraz co najmniej 20 TB/h z wykorzystaniem deduplikacji na źródle (dane podawane przez producenta).  6. Urządzenie musi pozwalać na jednoczesną obsługę minimum 250 strumieni w tym jednocześnie:  1) zapis danych minimum 150 strumieniami,  2) odczyt danych minimum 50 strumieniami,  3) replikacja minimum 50 strumieniami,  pochodzących z różnych aplikacji oraz dowolnych protokołów (CIFS, NFS, VTL, deduplikacja na źródle) oraz dowolnych interfejsów (FC, LAN) w tym samym czasie.  Wymienione wartości 250 jednoczesnych strumieni dla wszystkich protokołów (czyli jednocześnie 150 dla zapisu i jednocześnie 50 strumieni dla odczytu i jednocześnie 50 strumieni dla replikacji) musi mieścić w przedziale oficjalnie rekomendowanym i wspieranym przez producenta urządzenia.  Wszystkie zapisywane strumienie muszą podlegać globalnej deduplikacji przed zapisem na dysk (in-line) jak opisano w niniejszej specyfikacji.  7. Oferowane urządzenie musi mieć możliwość emulacji bibliotek taśmowych StorageTek L180 lub IBM TS 3500.  8. Oferowane urządzenie musi mieć możliwość emulacji napędów taśmowych min. LTO5 oraz LTO7.  9. Urządzenie musi umożliwiać (w przypadku VTL’a) emulację minimum 250 napędów, emulację min. 30 000 slotów w przypadku poj. biblioteki taśmowej oraz emulację sumarycznie min. 60 000 slotów.  10. Technologia deduplikacji musi wykorzystywać algorytm bazujący na zmiennym, dynamicznym bloku jednak o wielkości nie większej niż 12 kB.  Algorytm ten musi samoczynnie i automatycznie dopasowywać się do otrzymywanego strumienia danych co oznacza, że urządzenie musi dzielić otrzymany pojedynczy strumień danych na bloki o różnej długości, bez konieczności podejmowania czynności mających na celu ustalenie predefiniowanej długości bloków używanych do deduplikacji danych określonego typu. Deduplikacja zmiennym, dynamicznym blokiem oznacza, że wielkość każdego bloku (na jaki są dzielone dane pojedynczego strumienia backupowego) może być inna niż poprzedniego oraz jest indywidualnie ustalana przez algorytm deduplikacji zastosowany w urządzeniu, oferowane urządzenie nie może dzielić jakiegokolwiek pojedynczego strumienia danych backupowych na bloki o ustalonej, tej samej długości.  11. Oferowane urządzenie musi posiadać obsługę mechanizmów globalnej deduplikacji dla danych otrzymywanych jednocześnie wszystkimi protokołami (CIFS, NFS, VTL, deduplikacja na źródle) przechowywanych w obrębie całej przestrzeni oferowanego urządzenia co oznacza, że przechowywany na urządzeniu fragment danych nie może być ponownie zapisany bez względu na to, jakim protokołem zostanie ponownie otrzymany. Wszystkie emulowane jednocześnie w obrębie urządzenia biblioteki wirtualne (VTL) oraz udziały NFS/CIFS również muszą podlegać globalnej deduplikacji – blok danych otrzymany i zapisany w wirtualnej bibliotece „A”, nie może zostać ponownie zapisany jeśli trafi do innej wirtualnej biblioteki „B” w obrębie tego samego urządzenia (to samo dotyczy udziałów NFS/CIFS). Przestrzeń składowania zdeduplikowanych danych musi być jedna dla wszystkich protokołów dostępowych, co oznacza zastosowanie pojedynczej bazy deduplikatów bez względu na ilość/rodzaj używanych jednocześnie protokołów dostępowych.  12. Proces deduplikacji musi odbywać się in-line – w pamięci urządzenia, przed zapisem danych na nośnik dyskowy. Zapisowi na system dyskowy muszą podlegać tylko unikalne bloki danych nie zapisane jeszcze na system dyskowy urządzenia. Dotyczy to każdego fragmentu przychodzących do urządzenia danych. Wymaganie nie będzie spełnione jeżeli deduplikacja in-line realizowana będzie przez zewnętrzną aplikację backup’ową. Wymaganie deduplikacji in-line dotyczy zapisu danych przez każdy z wymaganych intefejsów, w przypadku interfejsów: NFS, CIFS oraz VTL realizacja deduplikacji in-line nie może w żadnym stopniu zależeć od konkretnej aplikacji backu’owej, dane zapisywane poprzez interfejsy NFS CIFS bez użycia jakiejkolwiek aplikacji backup’owej również muszą być deduplikowane w sposób in-line  13. Proponowane rozwiązanie nie może w żadnej fazie korzystać (w całości lub częściowo) z bufora na składowanie danych w postaci oryginalnej (niezdeduplikowanej) w celu ich późniejszej deduplikacji (wymagana deduplikacja in-line)  14. Wszystkie unikalne bloki przed zapisaniem na dysk muszą być dodatkowo kompresowane.  15. Tryb zapisu zabezpieczanych danych nie może umożliwiać nadpisywania danych, dane mogą być zapisywane jedynie w trybie append-only, dane dla których wygasła retencja muszą zostać usunięte podczas procesu czyszczenia tzw. Cleaning, wymaganie dotyczy wszystkich danych zapisanych na urządzeniu a nie wybranych grup danych objętych działaniem blokad zabezpieczających przed usunięciem/modyfikacją danych.  16. Oferowane urządzenie musi wspierać (wymagane formalne wsparcie producenta urządzenia), co najmniej następujące aplikacje: oferowana aplikacja backup’owa, RMAN, Microsoft SQL Server Management Studio.  17. W przypadku współpracy z każdą z poniższych aplikacji:  1) oferowana aplikacja backup’owa,  2) RMAN (dla ORACLE),  3) Microsoft SQL Server Management Studio (dla Microsoft SQL),  urządzenie musi realizować deduplikację na źródle oraz przesłanie jedynie nowych, nie znajdujących się jeszcze na urządzeniu bloków poprzez sieć LAN.  Deduplikacja w wyżej wymienionych przypadkach musi zapewniać aby z zabezpieczanych serwerów do urządzenia były transmitowane poprzez sieć LAN jedynie fragmenty danych (bloki o wymaganej długości) nie znajdujące się dotychczas na urządzeniu.  18. W przypadku przyjmowania backupów z oferowanej aplikacji backup’owej, urządzenie musi realizować deduplikację na źródle i przesłać jedynie nowe, nieznajdujące się jeszcze na urządzeniu bloki poprzez sieć FC.  Deduplikacja w wyżej wymienionych przypadkach musi zapewniać aby z zabezpieczanych serwerów do urządzenia były transmitowane poprzez sieć FC tylko fragmenty danych (bloki o wymganej długości) nie znajdujące się dotychczas na urządzeniu.  19. Oferowane urządzenie musi umożliwiać uruchamianie maszyn wirtualnych VMware bezpośrednio z danych backupowych bez konieczności odtwarzania danych – funkcjonalność ta musi być oficjalnie wspierana i zintegrowana z oferowaną aplikacją backupową. Spełnienie wymagania nie może być ograniczone dla wybranych grup danych ze względu na miejsce składowania czy konkretną retencję.  20. Wymagana funkcjonalność Load Balancing oraz Link Failover w obrębie portów wykorzystywanych przez aplikację backupową, wymagane wsparcie tej funkcjonlaności dla oferowanej aplikacji backup’owej.  21. W przypadku deduplikacji na źródle poprzez sieć IP (LAN oraz WAN), wymagana możliwość szyfrowania komunikacji kluczem minimum 256 bitów.  22. Urządzenie musi umożliwiać zaszyfrowanie przechowywanych danych, wymagane licencje umożliwiające zaszyfrowanie i przechowywanie zaszyfrowanych danych w obrębie maksymalnej pojemności oferowanego urządzenia.  23. Urządzenie musi wspierać deduplikację na źródle poprzez sieć FC (SAN) minimum dla systemów operacyjnych Windows, Linux (RedHat, SuSE).  24. Oferowane urządzenie musi umożliwiać bezpośrednią replikację danych do drugiego urządzenia takiego samego typu.  25. Konfiguracja replikacji musi być możliwa w każdym z trybów:  1) jeden do jednego,  2) wiele do jednego,  3) jeden do wielu,  4) kaskadowej (urządzenie A replikuje dane do urządzenia B, które te same dane replikuje do urządzenia C).  26. Replikacja musi się odbywać w trybie asynchronicznym. Transmitowane mogą być tylko te fragmenty danych (bloki), które nie znajdują się na docelowym urządzeniu. Ewentualna licencja na replikację jest przedmiotem postępowania.  27. Urządzenie musi umożliwiać wydzielenie określonych portów Ethernet dedykowanych do replikacji.  28. W przypadku wykorzystania portów Ethernet do replikacji urządzenie musi umożliwiać przyjmowanie backupów, odtwarzanie danych, przyjmowanie strumienia replikacji, wysyłanie strumienia replikacji tymi samymi portami.  29. W przypadku replikacji danych między dwoma urządzeniami oferowanego typu, wymagana możliwość kontroli przez: oferowaną aplikację backup’ową, muszą być możliwe do uzyskania jednocześnie wszystkie następujące funkcjonalności:  1) replikacja odbywa się bezpośrednio między dwoma urządzeniami bez udziału serwerów pośredniczących,  2) replikacji podlegają tylko te fragmenty danych (na poziomie bloków używanych do deduplikacji), które nie znajdują się na docelowym urządzeniu,  3) replikacja zarządzana jest z poziomu wymaganej aplikacji,  4) aplikacja posiada informację o obydwu kopiach zapasowych znajdujących się w obydwu urządzeniach bez konieczności przeprowadzania procesu inwentaryzacji.  30. Oferowane urządzenie musi działać poprawnie przy zapełnieniu danymi na poziomie co najmniej 90%. Dokumentacja urządzenia nie może wskazywać na ew. problemy, obostrzenia, które są efektem zapełnieniu urządzenia zabezpieczanymi danymi, na poziomie mniejszym niż 90%.  31. Wymagana możliwość ograniczenia pasma używanego do replikacji między dwoma urządzeniami – oferowane urządzenie musi być wyposażone w mechanizm umożliwiający zarządzaniem stopnia wykorzystania pasma na potrzeby replikacji.  32. Zdeduplikowane i skompresowane dane przechowywane w obrębie podsystemu dyskowego urządzenia muszą być chronione za pomocą technologii RAID 6 bądź równoważnej.  33. Oferowane urządzenie musi umożliwiać wykonywanie SnapShot’ów, czyli umożliwiać zamrożenie obrazu danych (stanu backupów) w urządzeniu na określoną chwilę. Oferowane urządzenie musi również umożliwiać odtworzenie danych ze Snapshot’u.  34. Odtworzenie danych ze Snapshot’u nie może wymagać konieczności nadpisania danych produkcyjnych jak również nie może oznaczać przerwy w normalnej pracy urządzenia (przyjmowania/odtwarzania backupów).  35. Urządzenie musi pozwalać na realizację oraz przechowywanie minimum 500 Snapshotów jednocześnie w obrębie oferowanej przestrzeni, przy zachowaniu globalnej deduplikacji oraz standardowego trybu pracy urządzenia – umożliwiającego wykorzystanie wszystkich dostępnych funkcjonalności.  36. Urządzenie musi umożliwiać podział na logiczne części. Dane znajdujące się w każdej logicznej części muszą być między sobą deduplikowane (globalna deduplikacja między logicznymi częściami urządzenia).  37. Urządzenie musi mieć możliwość podziału na minimum 10 logicznych części pracujących równolegle.  38. Dla każdej z ww. logicznych części oferowanego urządzenia musi być możliwość zdefiniowania oddzielnego użytkownika zarządzającego daną logiczną częścią deduplikatora. Użytkownicy zarządzający logiczną częścią A muszą widzieć tylko i wyłącznie zasoby logicznej części A i nie mogą widzieć żadnych innych zasobów oferowanego urządzenia.  39. Wymagana możliwość zaprezentowania każdej z logicznych części oferowanego urządzenia, jako niezależnego urządzenia dostępnego za pośrednictwem:  1) CIFS,  2) NFS,  3) VTL,  4) deduplikacja na źródle.  40. Urządzenie musi umożliwiać zdefiniowanie blokady skasowania danych (funkcjonalność WORM). Blokada skasowania danych musi chronić plik w zdefiniowanym czasie przed usunięciem pliku oraz modyfikacją pliku.  41. Blokada skasowania danych musi działać w dwóch trybach (do wyboru przez administratora):  1) możliwość zdjęcia blokady przed upływem ważności danych,  2) brak możliwości zdjęcia blokady przed upływem ważności danych (COMPLIANCE), w tym wypadku wymagane wsparcie norm SEC 17a-4(f) oraz ISO Standard 15489-1 w zakresie ochrony danych.  Licencje na blokadę WORM muszą być dostarczone wraz z urządzeniem.  42. W przypadku braku wymaganej funkcjonalności WORM, wymagana dostawa dodatkowej macierzy typu NAS (NFS/CIFS) o pojemności netto dwukrotnie większej od wymaganej pojemności netto deduplikatora (32TB x 2 = 64TB netto), o wydajności nie mniejszej od deduplikatora będącego przedmiotem postępowania. Wyposażona w funkcjonalność WORM macierz musi oficjalnie spełniać wymagania dot. ochrony danych określone normami SEC 17a-4(f) oraz ISO Standard 15489-1.  43. Blokada WORM (zarówno w przypadku deduplikatora jak i macierzy NAS) musi być zintegrowana z oferowaną aplikacją backup’ową co oznacza:  1) możliwość uruchomienia blokady WORM dla określonych danych z poziomu oferowanej aplikacji backup’owej,  2) możliwość określenia/wymuszenia czasu blokady z poziomu oferowanej aplikacji backup’owej,  3) możliwość raportowania od strony oferowanej aplikacji backup’owej danych zabezpieczonych przed usunięciem wymaganą blokadą WORM.  W każdym przypadku wymagana możliwość automatycznego uruchamiania blokady (podczas zapisu) WORM dla danych zapisywanych na obszar objęty działaniem wspomnianej blokady. W każdym przypadku wymagana również możliwość używania blokady WORM dla obrazu danych uzyskanych poprzez użycie wymaganej funkcjonalności SnapShot.  Zamawiający zastrzega możliwość prośby o dostarczenie ogólnodostępnej dokumentacji oferowanego produktu potwierdzającego spełnienie wymaganej funkcjonalności.  44. Urządzenie musi mieć możliwość przechowywania danych niezmienialnych: video, grafika, nagrania dźwiękowe, pliki pdf na udziałach CIFS/NFS.  45. Urządzenie musi weryfikować dane po zapisie (nie chodzi o ew. weryfikację danych indeksowych generowanych przez urządzenie ale o weryfikację wszystkich zabezpieczanych danych backup’owych). Każda zapisana na dyskach porcja danych musi być odczytana i porównana z danymi otrzymanymi przez urządzenie. Powyższa weryfikacja musi być realizowana w locie, czyli przed usunięciem z pamięci oryginalnych danych (otrzymanych z aplikacji backupowej), musi być realizowana w trybie ciągłym (a nie ad-hoc), wymagane parametry wydajnościowe urządzenia muszą uwzględniać tę funkcjonalność.  Wymagane potwierdzenie opisanej funkcjonalności w oficjalnej dokumentacji producenta oferowanego urządzenia. Zamawiający zastrzega możliwość prośby o dostarczenie ogólnodostępnej dokumentacji oferowanego produktu potwierdzającego spełnienie wymaganej funkcjonalności.  46. Urządzenie musi automatycznie usuwać przeterminowane dane (bloki danych nie należące do backupów o aktualnej retencji) w procesie czyszczenia.  Proces usuwania przeterminowanych danych (czyszczenia) nie może uniemożliwiać pracy procesów backupu / odtwarzania danych (zapisu / odczytu danych z zewnątrz do systemu).  47. Wymagana możliwość zdefiniowania maksymalnego obciążenia urządzenia procesem usuwania przeterminowanych danych (poziomu obciążenia procesora), wymagane potwierdzenie w ogólnodostępnej dokumentacji. Zamawiający zastrzega możliwość prośby o dostarczenie ogólnodostępnej dokumentacji oferowanego produktu potwierdzającego spełnienie wymaganej funkcjonalności.  48. Wymagana możliwość zdefiniowania harmonogramu wg. którego wykonywany jest proces usuwania przeterminowanych danych (czyszczenia), realizowany równolegle z procesami backup/restore/replication.  49. Standardowa częstotliwość usuwania przeterminowanych danych (czyszczenie) nie powinna być większa niż 1 raz na tydzień - minimalizując czas w którym backupy/odtworzenia narażone są na spowolnienie (weryfikacja wymagania na podstawie dokumentacji typu DOBRE PRAKTYKI publikowanej przez producenta).  50. Urządzenie musi umożliwiać systemowo (wbudowana funkcjonalnośc) - realizację procesu pierwszego czyszczenia dopiero po przekroczeniu 75% zajętości oferowanej przestrzeni.  51. Urządzenie musi mieć możliwość zarządzania poprzez:  1) interfejs graficzny dostępny z przeglądarki internetowej,  2) poprzez linię komend (CLI) dostępną z poziomu ssh (secure shell).  52. Oprogramowanie do zarządzania musi rezydować na oferowanym na urządzeniu deduplikacyjnym.  53. Urządzenie musi być rozwiązaniem kompletnym, appliancem sprzętowym pochodzącym od jednego producenta. Zamawiający nie dopuszcza stosowania rozwiązań typu gateway. | (zaznaczyć TAK albo NIE)  Ad 3 TAK/NIE  Ad 1,2,4-53 TAK |
| 7 | Warunki gwarancji | 1. Min. 60 miesięcy gwarancji realizowanej w miejscu instalacji sprzętu, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii w trybie 365x7x24 poprzez ogólnopolską linię telefoniczną producenta.  2. Zamawiający wymaga od Wykonawcy dołączenia do oferty oświadczenia podmiotu realizującego serwis lub producenta sprzętu, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony nośnik pozostaje u Zamawiającego.  3. Wymagane dołączenie do oferty oświadczenia Producenta potwierdzającego, że serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta.  4. Oświadczenie producenta deduplikatora, potwierdzające, że sprzęt pochodzi z oficjalnego kanału dystrybucyjnego producenta.  5. W czasie obowiązywania gwarancji Zamawiający musi mieć możliwość nieodpłatnego pobierania nowych wersji oferowanego oprogramowania oraz firmware (w przypadku deduplikatora) poprzez stronę www. | TAK |

**ZADANIE 9 – POZOSTAŁE WYMAGANIA**

|  |  |  |  |
| --- | --- | --- | --- |
| **Lp.** | **Element** | **Minimalne wymagania** | **Potwierdzenie spełnienia wymagań (skreślić TAK i wpisać NIE, jeżeli nie spełnia minimalnych wymagań), podać dane we wskazanych miejscach** |
| 1 | Okablowanie i akcesoria | 1. Należy dostarczyć:  1) 2 sztuki – moduł EX4600-EM-8F do przełączników Juniper EX4600 posiadanych przez Zamawiającego,  2) 10 sztuk – wkładka SFP+ LC 10Gb multimode, kompatybilna z przełącznikami Juniper posiadanymi przez Zamawiającego,  3) 50 sztuk – wkładka SFP+ LC 10Gb multimode, kompatybilna z oferowanym sprzętem w niniejszym postępowaniu,  4) 50 sztuk – wkładka SFP28 LC 25Gb multimode, kompatybilna z oferowanym sprzętem w niniejszym postępowaniu,  5) 2 sztuki – kabel DAC SFP28 25Gbe o długości 0,5 metra, kompatybilny z oferowanym sprzętem w niniejszym postępowaniu,  6) 48 sztuk - kabel FC LC OM4 - 1 metr,  7) 12 sztuk - kabel FC LC OM4 – 0,5 metra,  8) 24 sztuki - kabel FC LC OM4 - 1 metr,  9) 24 sztuki - kabel FC LC OM4 - 2 metry,  10) 24 sztuki - kabel FC LC OM4 - 3 metry,  11) 24 sztuki - kabel FC LC OM4 - 4 metry,  12) 6 sztuk – listwa dystrybucji zasilania RACK 1U (wtyczka wejściowa C20, min. 12 gniazd wyjściowych C13),  13) 4 sztuki – listwa dystrybucji zasilania RACK 1U (wtyczka wejściowa C20, min. 8 gniazd C19),  14) 26 sztuk – przewód zasilający o długości 2 metrów C13/C14,  15) 6 sztuk - przewód zasilający o długości 2 metrów C19/C20. | TAK |
| 2 | Plan wdrożenia | 1. Wykonawca po zawarciu umowy przy współpracy z Zamawiającym zapozna się ze specyfiką infrastruktury sprzętowej i programowej Zamawiającego. Zamawiający udzieli Wykonawcy wszelkich niezbędnych informacji do przygotowania planu i przeprowadzenia wdrożenia. Na tej podstawie Wykonawca opracuje i dostarczy plan wdrożenia w postaci elektronicznej lub papierowej. Plan powinien zawierać w szczególności:  1) harmonogram realizacji przedmiotu zamówienia (terminy dostaw, terminy realizacji poszczególnych etapów prac itd.),  2) opis oraz schemat montażu i połączeń dostarczanego sprzętu we wskazanej przez Zamawiającego szafie RACK,  3) opis podłączenia do infrastruktury Zamawiającego,  4) opis instalacji i konfiguracji dostarczanych urządzeń oraz oprogramowania (konfiguracja serwerów, macierzy, wirtualizacja, system backupu itp.),  5) opis procesu migracji wskazanych przez Zamawiającego zasobów do dostarczanej infrastruktury będącej przedmiotem niniejszego postępowania,  6) plan testów akceptacyjnych realizowanego zamówienia.  2. Plan wymaga akceptacji przez Zamawiającego przed przystąpieniem do dalszego etapu realizacji przedmiotu umowy. | TAK |
| 3 | Dostawa | 1. Wykonawca powiadomi Zamawiającego o terminie dostawy z wyprzedzeniem co najmniej 3 dni roboczych. Niezbędna jest akceptacja tego terminu przez Zamawiającego.  2. Dostawa możliwa jest w godzinach 8:00 – 16:00, poniedziałek – piątek (z wyłączeniem dni ustawowo wolnych od pracy).  3. Wykonawca zobowiązany jest do dostarczenia oraz wniesienia dostarczanych urządzeń do pomieszczeń wskazanych przez Zamawiającego. Miejsce dostawy: ul. Karola Szajnochy 8, 01-637 Warszawa.  4. Dostarczany sprzęt powinien być zapakowany w oryginalne opakowania transportowe producenta sprzętu i nie powinien być rozpakowywany bez obecności Zamawiającego. Opakowania nie mogą nosić śladów widocznych uszkodzeń.  5. Po dostawie urządzeń do miejsca dostawy sporządzony zostanie Protokół Odbioru Ilościowego.  6. Zamawiający zastrzega sobie prawo otwarcia opakowań w obecności przedstawiciela Wykonawcy w celu weryfikacji dostarczanych urządzeń. | TAK |
| 4 | Montaż, instalacja i konfiguracja | 1. Wykonawca zobowiązany jest do instalacji i konfiguracji przedmiotu umowy zgodnie z opracowanym planem wdrożenia, wytycznymi Zamawiającego oraz dobrymi praktykami producenta dostarczonych rozwiązań.  2. Dostarczony przedmiot zamówienia musi być kompleksowo wdrożony w zakresie platformy serwerowej oraz systemów operacyjnych z nią związanych, w tym również warstwy wirtualizacyjnej.  3. Każdy z dostarczonych w ramach zamówienia elementów musi zostać w pełni zintegrowany na etapie wdrożenia ze środowiskiem Zamawiającego. Wdrożenie musi obejmować:  1) Wdrożenie serwerów zgodnie z ich założeniem i pełnioną funkcją:  a) serwery dedykowane do baz danych Oracle,  b) serwery dedykowane dla systemu wirtualizacji,  c) serwery dedykowane do obsługi systemu NAC,  d) serwer dedykowany do środowiska backupu i obsługi biblioteki taśmowej.  2) Wdrożenie pamięci masowej (przeprowadzone przez inżyniera autoryzowanego przez producenta sprzętu):  a) konfiguracja przestrzeni dyskowej zgodnie z dobrymi praktykami producenta,  b) konfiguracja sieciowa w zakresie szkieletu LAN oraz SAN z zapewnieniem dostępu dla wdrażanych serwerów,  c) konfiguracja mechanizmu kopii bezpieczeństwa krytycznych wolumenów (snapshoty).  3) Wdrożenie środowiska backupu (przeprowadzone przez inżyniera autoryzowanego przez producenta sprzętu):  a) implementacja oprogramowania do wykonywania kopii bezpieczeństwa środowiska oraz odpowiednie wdrożenie polityk czasowych realizacji zadań,  b) implementacja urządzenia do składowania danych backupowych zgodnie z dobrymi praktykami producenta rozwiązania i jego integracja z oprogramowaniem do realizacji kopii bezpieczeństwa,  c) implementacja biblioteki taśmowej i jej pełna integracja z dedykowanym serwerem do backupu oraz resztą środowiska, co pozwoli na realizację polityki archiwizacji danych.  4) Wdrożenie warstwy wirtualizacyjnej:  a) implementacja systemu operacyjnego pozwalającego na dostęp do warstwy wirtualnej środowiska,  b) implementacja polityk dostępowych zgodnie z dobrymi praktykami producenta dostarczonego rozwiązania.  4. Oprogramowanie układowe urządzeń oraz oprogramowanie standardowe musi być zaktualizowane do najwyższej rekomendowanej przez danego producenta wersji (na dzień instalacji) zgodnej dla dostarczanego środowiska.  5. Zadania opisane w niniejszym etapie muszą być prowadzone w siedzibie Zamawiającego, w godzinach 8:00 – 16:00, poniedziałek – piątek (z wyłączeniem dni ustawowo wolnych od pracy). Za zgodą Zamawiającego możliwe będzie prowadzenie prac również poza wskazanymi godzinami.  6. Wykonawca powiadomi Zamawiającego o planowanym terminie realizacji zadań z wyprzedzeniem co najmniej 2 dni roboczych. Niezbędna jest akceptacja tego terminu przez Zamawiającego.  7. Zamawiający przy udziale Wykonawcy zweryfikuje licencje/oprogramowanie oraz parametry techniczne dostarczonego sprzętu w odniesieniu do niniejszej specyfikacji. | TAK |
| 5 | Testy akceptacyjne | 1. Scenariusze testów akceptacyjnych opracowuje Wykonawca na podstawie poniższych wytycznych:  1) fizyczne uruchomienie każdego z dostarczonych urządzeń,  2) wyłączenie/włączenie jednych z linii zasilania w przypadku urządzeń wyposażonych w redundantne zasilacze,  3) utworzenie testowej maszyny wirtualnej,  4) weryfikacja widoczności zasobów dyskowych z poziomu systemu operacyjnego wirtualizatora oraz systemu operacyjnego z zainstalowanymi bazami Oracle,  5) wykonanie kopii bezpieczeństwa testowej maszyny wirtualnej oraz zapisanie jej zarówno na urządzeniu typu deduplikator oraz bibliotece taśmowej,  6) odtworzenie przykładowej maszyny,  7) uruchomienie backupu maszyny wirtualnej z poziomu odseparowanego środowiska deduplikatora.  2. Podstawą przejścia do kolejnego etapu (migracja zasobów) będzie przeprowadzenie z pozytywnym skutkiem testów akceptacyjnych oraz sporządzenie i podpisanie przez obie strony umowy Protokołu Odbioru Sprzętu i Oprogramowania. | TAK |
| 6 | Migracja zasobów | 1. Wykonawca zobowiązany jest do migracji wskazanych przez Zamawiającego zasobów do dostarczonej i skonfigurowanej infrastruktury będącej przedmiotem niniejszego postępowania, zgodnie z opracowanym planem wdrożenia – element nr 2, Zadanie 9.  2. Proces migracji musi odbywać się ze szczególnym uwzględnieniem zachowania ciągłości pracy Zamawiającego i w ramach tego procesu wszelkie przestoje systemu muszą być zaplanowane i uzgodnione z Zamawiającym.  3. Wszelkie prace związane z migracją danych muszą się odbywać w siedzibie Zamawiającego.  4. Wykonawca przez okres 5 dni od ukończenia migracji zobowiązany jest prowadzić asystę techniczną w siedzibie Zamawiającego. W ramach tej asysty zobowiązany jest zapewnić wsparcie techniczne (co najmniej 8h) specjalisty w zakresie zgodnym z niniejszym przedmiotem zamówienia. Osoba/osoby te zobowiązane będą do bieżącego wsparcia Zamawiającego w identyfikacji i usuwaniu usterek, które mogą powstać po procesie migracji. Zamawiający zastrzega sobie prawo skrócenia tego okresu, jeżeli uzna, że stabilność systemu po migracji jest wystarczająca. | TAK |
| 7 | Dokumentacja powdrożeniowa | 1. Wykonawca zobowiązany jest do przygotowania i przekazania Zamawiającemu w postaci elektronicznej dokumentacji powdrożeniowej, składającej się z opisu rozwiązania, w tym w szczególności:  1) wykorzystywane skróty i pojęcia,  2) zestawienie ilościowe infrastruktury i oprogramowania standardowego:  a) infrastruktura:  - producent,  - nazwa,  - ilość,  - pełniona funkcja,  - numery seryjne,  - data rozpoczęcia i zakończenia gwarancji,  b) oprogramowanie standardowe:  - producent,  - nazwa,  - ilość licencji,  - rodzaj licencjonowania (per procesor, użytkownik itp.),  - data rozpoczęcia i zakończenia subskrypcji (o ile ma zastosowanie),  3) topologia fizyczna - logiczny schemat zaproponowanego rozwiązania,  4) adresacja zarządzająca (nazwa urządzenia, adres IP do zarządzania),  5) konfiguracja portów LAN (logiczny schemat połączeń),  6) konfiguracja portów SAN (logiczny schemat połączeń),  7) pamięci masowe:  a) typ dysku, poziom zabezpieczeń, szacowana pojemność,  b) nazwa wolumenów, grupa zabezpieczeń, szacowana pojemność,  c) mapowanie wolumenów do hostów: urządzenie, nazwa wolumenu, nazwa hosta,  8) wirtualizacja:  a) parametry instalacyjne,  b) wysoka dostępność,  c) wirtualne przełączniki (jeżeli istnieje taka konieczność na bazie najlepszych praktyk producenta rozwiązania),  d) zasoby dyskowe,  9) Oprogramowanie kopii zapasowych:  a) wykaz ról i uprawnień użytkowników,  b) infrastruktura systemu kopii zapasowych,  c) integracja systemu kopii zapasowych z warstwą wirtualizacji,  10) Loginy oraz hasła dostępowe (dane zabezpieczone przed nieautoryzowanym dostępem).  2. Dodatkowo, Wykonawca opracuje i utworzy procedurę wykonywania kopii zapasowych utworzonego środowiska, zawierającą w szczególności:  1) cel i zakres backupu,  2) metody wykonywania backupu,  3) harmonogram backupów,  4) wybór lokalizacji przechowywania,  5) automatyzacja backupów,  6) testowanie i weryfikacja backupów,  7) zabezpieczenie dostępu do kopii,  8) monitorowanie procesu oraz aktualizacje procedury.  3. Dokumentacja musi być wykonana w sposób spójny, zgodnie z dobrymi praktykami i zaleceniami budowy tego typu dokumentów.  4. Dokumentacja, o której mowa powyżej, wymaga akceptacji przez Zamawiającego. | TAK |
| 8 | Szkolenie | 1. Szkolenie z administracji dostarczonym rozwiązaniem (backup, deduplikator, wirtualizacja, macierz) dla pracowników Działu IT wskazanych przez Zamawiającego.  2. Szkolenie w siedzibie Zamawiającego w terminie ustalonym z Zamawiającym. Czas trwania szkolenia 10 godzin, przy czym nie muszą to być godziny następujące po sobie.  3. Po zakończeniu całości przedmiotu zamówienia zostanie sporządzony Protokół Odbioru Końcowego. | TAK |

Wskazany powyżej w OPZ zapis typu: musi mieć możliwość, musi być możliwe, musi być możliwość, zapewnia możliwość, umożliwia, należy rozumieć jako obowiązek zapewnienia danej funkcji w ramach zaoferowanej ceny, bez konieczności ponoszenia dodatkowych kosztów przez zamawiającego, z wyjątkiem przypadków, gdzie jednoznacznie określono inaczej.