**Opis przedmiotu zamówienia – Załącznik nr 2 do SWZ**

1. **Sewer (typ 1)**

|  |  |  |
| --- | --- | --- |
| **Parametr** | **Charakterystyka (wymagania minimalne lub równoważne)\*** | **Parametry oferowane** |
| **Obudowa** | Obudowa rack o wysokości max. 1U z możliwością instalacji min. 8 dysków 2,5” z organizatorem okablowania oraz kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych. Wentylatory redundantne „hot-plug”, wbudowany czujnik otwarcia obudowy współpracujący z kartą zarządzającą |  |
| **Płyta główna** | Płyta główna z możliwością zainstalowania jednego procesora. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym. |  |
| **Procesor** | Zainstalowany jeden procesor min. 32-rdzeniowy klasy x86 dedykowany do pracy z zaoferowanym serwerem umożliwiający osiągnięcie wyniku min. 220 punktów w teście SPECrate2017\_int\_base dostępnym na stronie www.spec.org. |  |
| **RAM** | Zainstalowane minimum 512GB pamięci RDIMM 3200MT/s. Na płycie głównej powinno znajdować się minimum 16 slotów przeznaczonych do instalacji pamięci RAM. Płyta główna powinna obsługiwać do 1TB pamięci RAM. |  |
| **Gniazda PCI** | Minimum dwa sloty PCIe low-profile, w tym jeden generacji 4. |  |
| **Interfejsy sieciowe/FC/SAS** | Zainstalowane min. cztery interfejsy sieciowe 10/25Gb Ethernet w standardzie SFP28. |  |
| **Dyski twarde** | Możliwość instalacji dysków SAS, SATA, SSD.  Zainstalowane dwa dyski M.2 o pojemności min. 480GB z możliwością konfiguracji RAID 1.  Zainstalowane dwa 800GB SSD SAS ISE Write Intensive 12Gbps 512e 2.5in Hot-plug, 10 DWPD. Dysk musi być wspierany przez producenta rozwiązania SDS w kategorii dysków przeznaczonych pod zastosowania Cache.  Zainstalowane sześć dysków 3.84TB SSD SATA Read Intensive 6Gbps 512 2.5in Hot-plug, 1 DWPD. Dyski muszą być wspierane przez producenta rozwiązania SDS w kategorii dysków przeznaczonych pod zastosowania Capacity. |  |
| **Kontroler RAID** | Zainstalowany wewnętrzny kontroler bez obsługi RAID (pass through). |  |
| **Wbudowane porty** | Minimum 4 porty USB z czego nie mniej niż jeden USB 2.0 na przednim panelu obudowy, jeden USB 3.0 wewnętrzny, jeden USB 3.0 z tyłu obudowy. Dwa porty VGA z czego jeden na panelu przednim, jeden port RS-232. |  |
| **Video** | Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1920x1200. |  |
| **Wentylatory** | Redundantne. |  |
| **Zasilacze** | Redundantne, Hot-Plug min. 550W każdy. |  |
| **Bezpieczeństwo** | Zintegrowany moduł TPM.  Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą. |  |
| **Karta zarządzania** | Karta zarządzająca niezależna od zainstalowanego na serwerze systemu operacyjnego, posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca:  - zdalny dostęp do graficznego interfejsu Web karty zarządzającej;  - zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera);  - szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika;  - możliwość podmontowania zdalnych wirtualnych napędów;  - wirtualną konsolę z dostępem do myszy, klawiatury;  - wsparcie dla IPv6;  - wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish;  - możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer;  - możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer;  - integracja z Active Directory;  - możliwość obsługi przez dwóch administratorów jednocześnie;  - wsparcie dla dynamic DNS;  - wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej.  - możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera  - możliwość zarządzania do 50 serwerów bezpośrednio z konsoli karty zarządzającej pojedynczego serwera  Dodatkowe oprogramowanie umożliwiające zarządzanie poprzez sieć, spełniające minimalne wymagania:  - wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych;  - możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta;  - wsparcie dla protokołów – WMI, SNMP, IPMI, WSMan, Linux SSH;  - możliwość oskryptowywania procesu wykrywania urządzeń;  - możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram;  - szczegółowy opis wykrytych systemów oraz ich komponentów;  - możliwość eksportu raportu do CSV, HTML, XLS;  - grupowanie urządzeń w oparciu o kryteria użytkownika;  - automatyczne skrypty CLI umożliwiające dodawanie i edycję grup urządzeń;  - szybki podgląd stanu środowiska;  - podsumowanie stanu dla każdego urządzenia;  - szczegółowy status urządzenia/elementu/komponentu;  - generowanie alertów przy zmianie stanu urządzenia;  - filtry raportów umożliwiające podgląd najważniejszych zdarzeń;  - integracja z service desk producenta dostarczonej platformy sprzętowej;  - możliwość przejęcia zdalnego pulpitu;  - możliwość podmontowania wirtualnego napędu;  - automatyczne zaplanowanie akcji dla poszczególnych alertów w tym automatyczne tworzenie zgłoszeń serwisowych w oparciu o standardy przyjęte przez producentów oferowanego w tym postępowaniu serwerów;  - kreator umożliwiający dostosowanie akcji dla wybranych alertów;  - możliwość importu plików MIB;  - przesyłanie alertów „as-is” do innych konsol firm trzecich;  - aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania);  - możliwość instalacji sterowników i oprogramowania wewnętrznego bez potrzeby instalacji agenta;  - możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów;  - moduł raportujący pozwalający na wygenerowanie następujących informacji: nr seryjny sprzętu, konfiguracja poszczególnych urządzeń, wersje oprogramowania wewnętrznego, obsadzenie slotów PCIe i gniazd pamięci, informację o maszynach wirtualnych, aktualne informacje o stanie gwarancji, adresy IP kart sieciowych |  |
| **Oprogramowanie do tworzenia kopii zapasowej maszyn wirtualnych w środowisku wirtualnym** | * Wykonywanie kopii musi być możliwe z poziomu konsoli zarządzania środowiskiem wirtualnym. * Oprogramowanie musi mieć możliwość wykonywania kopii i odtwarzania dla pojedynczej maszyny wirtualnej. * Nie dopuszcza się rozwiązań wymagających instalację dodatkowych serwerów czy fizycznych appliance. * Oprogramowanie musi być niezależne od rodzaju systemów dyskowych, na których zainstalowane są maszyny wirtualne (wymagane wsparcie dla zasobów dyskowych SAN/NFS/DAS/iSCSI/FC/vSAN). * Wymagana jest możliwość bezpośredniego wykonywania kopii maszyny wirtualnej w ośrodku lokalnym (kopie lokalne) i zdalnym (replikacja). * Wymagana jest możliwość tworzenia grup konsystencji dla grupy zabezpieczanych maszyn wirtualnych. * Oprogramowanie musi mieć możliwość wykonywania kopii bezpieczeństwa maszyn wirtualnych skonfigurowanych w oparciu o RDM. * Oprogramowanie musi umożliwiać:   + stworzenia DISASTER RECOVERY dla całego zabezpieczanego wirtualnego środowiska zbudowanego w oparciu o VMware   + operacyjne ODTWARZANIE dowolnej maszyny VM wraz z aplikacjami   + MIGRACJI danych w trybie ON-LINE na inne zasoby dyskowe * Działanie oprogramowania nie może mieć negatywnego wpływu na wydajność zabezpieczanych maszyn wirtualnych i aplikacji. * Oprogramowanie musi mieć możliwość pominięcia wybranych plików VMDK podczas wykonywania kopii maszyny wirtualnej. * Oprogramowanie musi zapewniać wsparcie dla VSS, zapewnienie konsystencji aplikacji na poziomie VSS. * Wymagana jest możliwość replikacji dwukierunkowej (bi-directional). * Wymagana jest funkcjonalność kompresji i deduplikacji danych wysyłanych po sieci WAN. * Testy DR muszą być możliwe bez konieczności zmian w działaniu replikacji (np. PAUSE, REVERSE). * Oprogramowanie musi mieć możliwość automatycznego zainicjowania procesu REVERSE REPLICATION w przypadku procesów FAILOVER/FAILBACK. * Wymagana jest możliwość ciągłego wykonywania kopii (bez wykorzystania mechanizmu kopii migawkowych VMware) podczas pracy maszyny wirtualnej. Wymagane jest RPO na poziomie pojedynczych sekund. * Wymagana jest możliwość wyboru dowolnego punktu w czasie (z ostatnich 5 dni), z którego chcemy odtworzyć dane lub całe środowisko. * Wymagana jest możliwość przeprowadzania testów DR bez zatrzymywania przetwarzania produkcyjnego. * Wymagana jest możliwość tworzenia własnych scenariuszy odtwarzania w przypadku awarii. * Oprogramowanie musi mieć możliwość automatycznego wykonywania kopii maszyn wirtualnych pracujących w środowisku wykorzystującym technologie VMware vMotion, VMware Storage vMotion, VMware DRS, VMware HA. * Oprogramowanie musi być odporne na krótkotrwałe problemy związane z siecią WAN. * Oprogramowanie musi być odporne na zmiany sprzętowe środowiska (zmiany w warstwie sprzętowej nie mogą mieć negatywnego wpływu na działanie systemu). * Rozwiązanie musi posiadać pełną redundancję bez pojedynczego punktu awarii. * Jeżeli pełna redundancja nie jest możliwa na poziomie samej aplikacji należy zaimplementować tą funkcjonalność na poziomie VMware. * Koszty takiego rozwiązania muszą być uwzględnione w ofercie (licencje i usługi). * Rozwiązanie musi posiadać mechanizm synchronicznej replikacji między lokalizacjami dla krytycznych maszyn VM. * Jeżeli replikacja synchroniczna nie jest możliwa za pomocą tej samej aplikacji Wykonawca musi dostarczyć dodatkowe rozwiązanie do replikacji synchronicznej wybranych maszyn VM * Rozwiązanie musi zapewnić następującą retencję przechowywanych kopi bezpieczeństwa:   + RPO=30s z ostatnich 24h,   + RPO=24h z ostatniego tygodnia,   + RPO=1tydzień z ostatniego miesiąca * Dopuszcza się zastosowanie uzupełniającego oprogramowanie backupowego do składowania danych z dłuższą retencją. * Oba systemy muszą działać jednocześnie i być kompatybilne. * Wymagana jest możliwość zarządzania oprogramowaniem z poziomu vCenter. * Wymagane jest wsparcie dla wykonywania kopii maszyn wirtualnych z systemów VMware w najnowszej dostępnej wersji * Możliwość instalacji nowej wersji oprogramowania bez konieczności wstrzymania operacji wykonywania kopii zapasowych. * Automatyczne włączenie do procesu wykonywania kopii bezpieczeństwa nowo dodanych dysków do zabezpieczanych maszyn wirtualnych. * Wsparcie dla więcej niż 1 ośrodka zdalnego, gdzie wykonywane są kopie bezpieczeństwa. * Możliwość replikacji synchronicznej maszyn wirtualnych do zdalnej lokalizacji. * Architektura odporna na awarię (Fault Tolerant). * Możliwość tworzenia kilku kopii maszyny wirtualnej w ramach tej jednej grupy konsystencji. * Możliwość wykonywania kopii bezpieczeństwa w trybie CDP (Continuous Data Protection). * Możliwość odtwarzania danych z dowolnego punktu w czasie z okresu powyżej tygodnia. * Wsparcie dla równoległej replikacji zabezpieczanego środowiska do więcej niż jednego ośrodka docelowego, wsparcie dla replikacji równoległej musi być zapewnione również na poziomie grup konsystencji (CONSISTENCY GROUP). |  |
| **Oprogramowanie do wirtualizacji serwerów** | * Warstwa wirtualizacji musi być zainstalowana bezpośrednio na sprzęcie fizycznym i nie może być częścią innego systemu operacyjnego. * Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych 1-256 procesorowych. * Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych, z których każda może mieć 1-10 wirtualnych kart sieciowych. * Rozwiązanie musi umożliwiać łatwą i szybką rozbudowę infrastruktury o nowe usługi bez spadku wydajności i dostępności pozostałych wybranych usług. * Rozwiązanie musi w możliwie największym stopniu być niezależne od producenta platformy sprzętowej. Rozwiązanie musi współpracować z więcej niż jednym producentem sprzętu i musi być dostępne na rynku jako niezależne oprogramowanie z możliwością zakupu licencji. * Rozwiązanie musi umożliwiać przydzielenie większej ilości pamięci RAM dla maszyn wirtualnych niż fizyczne zasoby RAM serwera w celu osiągnięcia maksymalnego współczynnika konsolidacji. * Rozwiązanie musi umożliwiać udostępnienie maszynie wirtualnej większej ilości zasobów dyskowych niż jest fizycznie zarezerwowane na zasobach dyskowych. * Konsola graficzna musi być dostępna poprzez dedykowanego klienta (za pomocą przeglądarek, minimum Edge i Firefox). * Dostęp przez przeglądarkę do konsoli graficznej musi być skalowalny tj. powinien umożliwiać rozdzielenie komponentów na wiele instancji w przypadku zapotrzebowania na dużą liczbę jednoczesnych dostępów administracyjnych do środowiska. * Rozwiązanie musi umożliwiać integrację z rozwiązaniami antywirusowymi firm trzecich w zakresie skanowania maszyn wirtualnych z poziomu warstwy wirtualizacji. * Rozwiązanie musi zapewniać zdalny i lokalny dostęp administracyjny do wszystkich serwerów fizycznych poprzez protokół SSH, z możliwością nadawania uprawnień do takiego dostępu nazwanym użytkownikom bez konieczności wykorzystania konta root. * Oprogramowanie do wirtualizacji musi zapewnić możliwość klonowania systemów operacyjnych wraz z ich pełną konfiguracją i danymi. * Oprogramowanie do wirtualizacji musi zapewnić możliwość wykonywania kopii migawkowych instancji systemów operacyjnych na potrzeby tworzenia kopii zapasowych bez przerywania ich pracy. * Oprogramowanie zarządzające musi posiadać możliwość przydzielania i konfiguracji uprawnień z możliwością integracji z usługami katalogowymi. * Rozwiązanie musi zapewniać możliwość dodawania zasobów w czasie pracy maszyny wirtualnej, w szczególności w zakresie ilości procesorów, pamięci operacyjnej i przestrzeni dyskowej. * System musi mieć możliwość uruchamiania fizycznych serwerów z centralnie przygotowanego obrazu poprzez protokół PXE. * System musi posiadać funkcjonalność wirtualnego przełącznika (virtual switch) umożliwiającego tworzenie sieci wirtualnej w obszarze hosta i pozwalającego połączyć maszyny wirtualne w obszarze jednego hosta, a także na zewnątrz sieci fizycznej. * Pojedynczy przełącznik wirtualny powinien mieć możliwość konfiguracji do 4000 portów. * Pojedynczy wirtualny przełącznik musi posiadać możliwość przyłączania do niego dwóch i więcej fizycznych kart sieciowych, aby zapewnić bezpieczeństwo połączenia w razie awarii karty sieciowej. * Wirtualne przełączniki muszą obsługiwać wirtualne sieci lokalne (VLAN). * Rozwiązanie musi zapewniać możliwość konfigurowania polityk separacji sieci w warstwie trzeciej, tak aby zapewnić oddzielne grupy wzajemnej komunikacji pomiędzy maszynami wirtualnymi. * Rozwiązanie musi umożliwiać wykorzystanie technologii 10GbE w tym agregację połączeń fizycznych do minimalizacji czasu przenoszenia maszyny wirtualnej pomiędzy serwerami fizycznymi. * Oprogramowanie do wirtualizacji musi obsługiwać przełączenie ścieżek LAN (bez utraty komunikacji) w przypadku awarii jednej ze ścieżek. * Rozwiązanie musi zapewnić możliwość bieżącego monitorowania wykorzystania zasobów fizycznych infrastruktury wirtualnej (np. wykorzystanie procesorów, pamięci RAM, wykorzystanie przestrzeni na dyskach/wolumenach). * Rozwiązanie musi zapewnić możliwość zdefiniowania alertów informujących o przekroczeniu wartości progowych. * Rozwiązanie musi mieć możliwość przenoszenia maszyn wirtualnych w czasie ich pracy pomiędzy serwerami fizycznymi, pamięciami masowymi niezależnie od dostępności współdzielonej przestrzeni dyskowej, różnymi rodzajami wirtualnych przełączników sieciowych. * Musi zostać zapewniona odpowiednia redundancja i nadmiarowość zasobów tak by w przypadku awarii np. serwera fizycznego usługi na nim świadczone zostały automatycznie przełączone na inne serwery infrastruktury. * Rozwiązanie musi umożliwiać łatwe i szybkie ponowne uruchomienie systemów/usług w przypadku awarii poszczególnych elementów infrastruktury bez utraty danych. * Rozwiązanie musi zapewniać mechanizm bezpiecznego, bezprzerwowego i automatycznego uaktualniania warstwy wirtualizacyjnej wliczając w to zarówno poprawki bezpieczeństwa jak i zmianę jej wersji bez potrzeby wyłączania wirtualnych maszyn. * Rozwiązanie musi posiadać co najmniej 2 niezależne mechanizmy wzajemnej komunikacji między serwerami oraz z serwerem zarządzającym, gwarantujące właściwe działanie mechanizmów wysokiej dostępności na wypadek izolacji sieciowej serwerów fizycznych lub partycjonowania sieci. * Decyzja o próbie przywrócenia funkcjonalności maszyny wirtualnej w przypadku awarii lub niedostępności serwera fizycznego powinna być podejmowana automatycznie, jednak musi istnieć możliwość określenia przez administratora czasu po jakim taka decyzja jest wykonywana. * Oprogramowanie do wirtualizacji musi zapewniać możliwość stworzenia dysku maszyny wirtualnej o wielkości do 62 TB. * Rozwiązanie musi posiadać wbudowany interfejs programistyczny (API) zapewniający pełną integrację zewnętrznych rozwiązań wykonywania kopii zapasowych z istniejącymi mechanizmami warstwy wirtualizacyjnej. * Zamawiający dopuszcza, aby wymagana funkcjonalność rozwiązania była realizowana przez kilka osobnych komponentów/zbiorów oprogramowania, ale wymaga się pomiędzy nimi ścisłej integracji. * Dostarczone oprogramowanie musi zapewniać możliwość wirtualizacji dla wszystkich dostarczonych w ramach postępowania serwerów. |  |
| **Oprogramowanie do wirtualizacji przestrzeni dyskowej** | * Rozwiązanie musi być zbudowane zgodnie z koncepcją Software-Defined Storage które polega na uniezależnieniu storage’u od hardware’u poprzez wirtualizację pamięci masowej, przy czym w swojej budowie musi gwarantować użytkownikowi dowolność doboru producenta składowych komponentów sprzętowych. * Rozwiązanie musi umożliwiać zbudowanie wspólnej przestrzeni dyskowej w oparciu o dyski wewnętrzne serwerów fizycznych (tj. w modelu hybrydowym zbudowanym z dysków SSD i HDD lub modelu All-Flash składającym się tylko z dysków SSD). * Rozwiązanie musi zapewniać możliwość „cache’owania” operacji Read/Write po stronie serwerów fizycznych tak, aby maksymalnie zredukować opóźnienia operacji dyskowych. * Rozwiązanie musi umożliwiać dowolność w konfiguracji dyskowej przestrzeni akcelerującej operacje Read/Write (cache) oraz przestrzeni budującej pojemność, zarówno pod kątem wydajności jak i pojemności. * Rozwiązanie musi być zintegrowane z warstwą wirtualizacji w sposób bezpośredni, niewymagający instalacji/konfiguracji żadnych dodatkowych komponentów sprzętowych ani dodatkowego oprogramowania. * Rozwiązanie musi współdzielić zasób dyskowy dla platformy wirtualizacyjnej oraz musi umożliwiać wykorzystanie ww. przestrzeni dyskowej przez serwery fizyczne nie posiadające dysków wewnętrznych. * Konfiguracja, zarządzanie i monitoring ww. przestrzeni dyskowej muszą być zintegrowane z konsolą zarządzającą platformą wirtualizacyjną. * Narzut na zasoby fizyczne procesora i pamięci RAM podczas działania rozwiązania nie może być większy niż 10%. * Rozwiązanie musi zapewniać możliwość budowy wspólnej wysokowydajnej i wysokodostępnej przestrzeni dyskowej z wykorzystaniem dysków wewnętrznych udostępnianych przez minimalnie 2 serwery fizyczne, oraz umożliwiać rozbudowę w ramach jednej logicznej puli do minimum 64 serwerów fizycznych. * Rozwiązanie musi zapewniać obsługiwanie dysków wirtualnych maszyn do rozmiaru do min. 60TB. * Rozwiązanie musi zapewniać wysoką dostępność oraz odporność na awarie usług uruchomionych na ww. przestrzeni dyskowej realizowaną w oparciu o wbudowane mechanizmy, w przypadku awarii komponentów takich jak: serwer fizyczny, dysk cache’ujący, dysk pojemnościowy oraz składnika sieć komunikującej ze sobą serwery fizyczne. * Rozwiązanie musi zapewnić wsparcie dla funkcjonalności platformy wirtualizacyjnej dla usług uruchamianych na tak zbudowanej przestrzeni dyskowej, a w szczególności możliwość korzystania z technologii VMware takich jak: VMware HA, VMware vMotion, VMware DRS, VMware Snapshot and Clones, vSphere Replication oraz vSphere Fault Tolerance. * Rozwiązanie nie może w żaden sposób ograniczać funkcjonalności platformy wirtualizacyjnej. * Rozwiązanie musi zapewniać możliwość tworzenia i konfigurowania polityk niezawodnościowych, wydajnościowych i pojemnościowych przypisanych do maszyn wirtualnych tak, aby można było określić np. liczbę serwerów fizycznych które mogą ulec awarii jednocześnie, liczbę operacji I/O, użycie funkcji thin-provisioning, użycie deduplikacji czy kompresji danych, itp. * Rozwiązanie powinno wspierać mechanizmy poprawienia wykorzystywania przestrzeni dyskowych a w szczególności technologię deduplikacji oraz implementacja RAID5 i RAID6 za pomocą oprogramowania. * Rozwiązanie musi gwarantować konfigurowalną funkcję zabezpieczania danych na wypadek ich niedostępności lub/i utraty w taki sposób, aby zabezpieczane dane można było rozlokować np.: między różnymi lokalizacjami, różnymi centami przetwarzania danych, różnymi szafami rack/chassis, itp. * Rozwiązanie musi być maksymalnie niezależne od warstwy sprzętowej, musi istnieć możliwość budowania ww. przestrzeni dyskowej na serwerach fizycznych różnych producentów. * Rozwiązanie musi zapewniać łatwość liniowego skalowania zarówno mocy obliczeniowej jak i pojemności przestrzeni dyskowej. * Rozwiązanie musi zapewniać możliwość rozbudowy ww. przestrzeni dyskowej (dodanie pojedynczego dysku, dodanie serwera/serwerów fizycznych) w sposób niewymagający przestoju i przerwy w dostępie do działających usług wirtualnych. * Rozwiązanie musi zapewniać możliwość konfiguracji i określania QoS dla poszczególnych usług wirtualnych. * Rozwiązanie musi zapewniać możliwość ochrony danych przed utratą ich integralności (sfałszowaniem) za pomocą weryfikacji sum kontrolnych. * Rozwiązanie musi umożliwiać utworzenie jednej przestrzeni dyskowej jako „rozciągniętego klastra geograficznego” realizującego scenariusze Disaster Recovery/Disaster Avoidance, zbudowanego w oparciu o dyski wewnętrzne serwerów fizycznych umieszczonych w dwóch różnych lokalizacjach fizycznych. * Rozwiązanie musi umożliwiać utworzenie wysokodostępnego klastra przestrzeni dyskowej w scenariuszu dla tzw. „oddziału zdalnego” firmy, zbudowanego w oparciu o min. 2 serwery fizyczne i min. dwie lokalizacje i zarówno musi mieć możliwość dołączania nieograniczonej liczby kolejnych lokalizacji „oddziałów zdalnych”. |  |
| **Oprogramowanie do zarządzania klastrem** | Zintegrowana konsola do obsługi sprzętu, działająca jako wtyczka (plug-in) do oprogramowania do wirtualizacji pozwalająca na:   * Zapewnienie platformy oprogramowania (software stack) dla modułów centrum danych definiowanych programowo (SDDC), w tym obliczeń, sieci, pamięci masowej i zarządzania. * Monitorowanie statusu sprzętu oraz prezentacji graficznej statusów. * Zautomatyzowane dodawanie nowych serwerów do klastra. * Aktualizację oprogramowania i elementów klastra. * Dostęp do platformy analitycznej, centralnego mechanizmu przechowującego dane zebrane z sond monitorujących klaster, która ułatwia podejmowanie decyzji administracyjnych w sprawie zmiany wydajności oraz pojemności klastra. |  |
| **Oprogramowanie wymagania** | Wszystkie licencje dla rozwiązania są zapewnione dla jego maksymalnej możliwej pojemności w ramach oferowanego klastra. Wszystkie licencje dla rozwiązania są zapewnione tak aby obejmować całkowitą wymaganą dla danego ukompletowania funkcjonalność rozwiązania.  Wszystkie licencje oprogramowania powinny być niewyłączne, nieograniczone czasowo, dostarczone wraz ze wsparciem świadczonym przez producenta będącego licencjodawcą oprogramowania.  Serwer, oprogramowanie do wirtualizacji, oprogramowanie do wirtualizacji przestrzeni dyskowej, zintegrowana konsola do obsługi sprzętu muszą być oferowane jako jeden produkt dostarczany przez jego producenta, objęty jednolitą gwarancją i wsparciem techniczny. Zamawiający nie dopuszcza oferowania serwera oraz jakiegokolwiek elementu oprogramowania jako produkty niezależne, które będą integrowane dopiero na etapie wdrożenia. |  |
| **Funkcjonalność** | Opis dotyczy funkcjonalności klastra zbudowanego z czterech oferowanych serwerów hyperkonwergentnych.  Klaster systemu wirtualizacji typu HCI (Hyperconverged Infrastructure) pod rozwiązanie do wirtualizacji maszyn wirtualnych. Wymaga się dostarczenia pojedynczego klastra, implementującego na potrzeby środowiska zwirtualizowanego jedną współdzieloną pamięć masową (datastore) wyłącznie w oparciu o urządzenia Flash (tzw All Flash).  Wymaga się dostarczenia co najmniej czterech węzłów dla zaimplementowania klastra.  Oferowane urządzenia muszą być urządzeniami typu appliance, czyli zintegrowanymi przez producenta elementami sprzętu i oprogramowania, zwane dalej „rozwiązaniem”.  Rozwiązanie zapewnia architekturę klastrową z możliwością obsługi minimum 64 węzłów pamięci masowej w pojedynczym klastrze lub federacji.  Rozwiązanie oparte jest o węzły serwerowe integrujące procesory, pamięć operacyjną i pamięć masową opartą o dyski SSD, przy czym każdy z serwerów wyprowadza co najmniej cztery interfejsy 10 Gigabit Ethernet dla łączności w klastrze.  Każdy serwer fizyczny powinien dostarczać zarówno moc obliczeniową do klastra (CPU i RAM) jak również przestrzeń dyskową, na podstawie których oferowane rozwiązanie zbuduje pamięć masową typu Software Defined Storage (SDS) oraz moc obliczeniową dla potrzeb wirtualizatora. Zamawiający wymaga, aby rozwiązanie SDS było konfigurowalne z poziomu posiadanej konsoli systemu wirtualizacji. Rozwiązanie zapewnia implementację wspólnego zasobu pamięci masowej (datastore) w oparciu o cały klaster, dostępnego w taki sam sposób dla każdego węzła wchodzącego w skład klastra.  Rozwiązanie jest skalowalne (scale-out) czyli rozbudowa jest zapewniona poprzez bezprzerwowe dołożenie kolejnego węzła do klastra a w przypadku, gdy w węźle klastra nie ma maksymalnej ilości dysków rozwiązanie jest skalowalne (scale-up), czyli rozbudowa jest zapewniona poprzez bezprzerwowe dołożenie kolejnego dysku do węzła klastra.  Rozwiązanie zapewnia pełną ciągłość i funkcjonalność działania w wypadku awarii lub całkowitej niedostępności pojedynczego węzła.  Rozwiązanie zapewnia pełną ciągłość i funkcjonalność działania w wypadku jednoczesnej awarii pojedynczego dysku w dwóch węzłach.  Rozwiązanie musi zapewniać wysoką dostępność oraz odporność na awarie usług uruchomionych na serwerach z zainstalowanym oprogramowaniem do udostępniana przestrzeni dyskowej. Wysoka dostępność musi być realizowana w oparciu o wbudowane mechanizmy i nie dopuszcza się stosowania produktów firm trzecich lub dedykowanych komponentów sprzętowych, aby zapewnić ciągłość działania w przypadku awarii komponentów takich jak: serwer fizyczny i jego komponenty takie jak: cache, dysk pojemnościowy.  Rozwiązanie po ewentualnej rozbudowie posiada możliwość kontrolowanego wyłączania pojedynczego węzła z klastra poprzez przełączanie go w tryb utrzymaniowy (maintenance) w sposób niewymagający przestoju i przerwy w dostępie do działających usług wirtualnych.  Rozwiązanie integruje się z infrastrukturą wirtualizacyjną posiadaną przez Użytkownika, tj. VMware vCenter oraz VMware vSphere.  Rozwiązanie posiada wbudowany portal do zarządzania i monitorowania lub musi być zintegrowane z centralną konsolą zarządzającą platformą wirtualizacyjną posiadana przez użytkownika opartą o VMware vCenter i VMware vSphere i umożliwia:  a. Raportowanie i monitorowanie węzłów pamięci masowej oraz ich zasobów dyskowych.  b. Zarządzanie pamięcią masową rozwiązania.  c. Monitorowanie i wizualizowanie wydajności rozwiązania, w tym parametrów: ilość operacji / sekundę, opóźnienie pamięci masowej, przepustowość.  d. Uruchamianie i zatrzymywanie maszyn wirtualnych VM oraz tworzenie ich klonów oraz kopii migawkowych.  e. Konfigurowanie replikacji danych między różnymi ośrodkami.  f. Dziennik czynności, zdarzeń i alarmów.  g. Aktualizację oprogramowania pamięci masowej oraz innych komponentów.  Rozwiązanie posiada możliwość weryfikacji i diagnozowania działania poprzez dedykowany interfejs linii komend (CLI).  Rozwiązanie zapewnia zwiększenie wydajności operacji wejścia/wyjścia za pomocą architektury cache implementowanej na pojedynczych węzłach klastra.  Rozwiązanie posiada możliwość rozszerzenia funkcjonalności o szyfrowanie zapisywanych na dyskach danych bez konieczności rozbudowy sprzętowej.  Rozwiązanie posiada możliwość rozszerzenia funkcjonalności o deduplikację i kompresję danych maszyn wirtualnych.  Rozwiązanie nie może wymagać instalacji dodatkowych komponentów i maszyn wirtualnych na serwerach wykorzystywanych do udostępniania przestrzeni dyskowych i musi posiadać integrację z oprogramowaniem systemu wirtualizacji VMware vSphere posiadanym przez użytkownika na poziomie jądra. W przypadku braku tej funkcjonalności, należy zwiększyć ukompletowanie klastra systemu wirtualizacji typu HCI. Dla każdego węzła klastra, pamięć RAM i wydajność SPECspeed2017\_fp\_base muszą być większe o minimum 40%.  Architektura rozwiązania umożliwia maszynom wirtualnym na korzystanie również z innych, znajdujących się poza klasterem zasobów pamięci masowej udostępnianych poprzez FC, iSCSCI, NFS.  Rozwiązanie posiada wbudowany mechanizm dedykowanej asynchronicznej replikacji danych między dwoma ośrodkami przetwarzania danych (OPD) dla wybranych maszyn wirtualnych (VM) z możliwością ich odtwarzania po awarii (disaster recovery)  Rozwiązanie posiada możliwość rozbudowy do obsługi funkcjonalności rozciągnięcia pojedynczego klastra na 2 odległe o 100km ośrodki przetwarzania danych (OPD) z synchroniczną replikacją danych i obsługą środowiska w trybie aktywne-aktywne między OPD (maszyny wirtualne VM aktywne w obu lokalizacjach) przy czym musi być zachowania spójność systemu w przypadku zerwania połączenia między OPD (split-brain) oraz możliwość automatycznego przełączenia do ośrodka zapasowego w przypadku awarii.  Możliwość aktualizacji firmware i oprogramowania systemowego dla wszystkich warstw, tj. infrastruktury sprzętowej, infrastruktury wirtualizacyjnej oraz oprogramowania pamięci masowej z poziomu systemu zarządzania rozwiązaniem  Możliwość uruchomienia automatycznego informowania centrum wsparcia technicznego producenta rozwiązania o błędach i usterkach  Możliwość monitorowania klastra poprzez interfejs REST API. |  |
| **Warunki gwarancji** | Min. 3 lata gwarancji producenta, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii 24x7x365 poprzez ogólnopolską linię telefoniczną producenta.  Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.  Wymagane jest regularne (przez cały czas trwania wykupionego wsparcia serwisowego) dostarczanie przez producenta rozwiązania pełnego zestawu aktualizacji jako kompletu poprawek do wszystkich jego komponentów: oprogramowania wirtualizacyjnego serwerów, oprogramowania do zarządzania pamięcią masową Software Defined Storage, oprogramowania do zarządzania systemem wirtualizacji, jak i serwerów stanowiących węzły klastra (BIOS, procesor serwisowy, firmware kart storage, firmware kart sieciowych, firmware dysków, sterowniki do dysków). Poprawki te muszą być każdorazowo przetestowane przez producenta rozwiązania dla środowiska zgodnego z oferowanym rozwiązaniem. |  |
| **Dokumentacja użytkownika** | Zamawiający wymaga dokumentacji w języku polskim lub angi*e*lskim. |  |

1. **Przełącznik (typ 1)**

|  |  |  |
| --- | --- | --- |
| **Parametr** | **Charakterystyka (wymagania minimalne lub równoważne)** | **Parametry oferowane** |
| **Porty** | Przełącznik 1U wyposażony w porty:  - 48 x 10 Gigabit Ethernet SFP+  - 4 x 100 Gigabit Ethernet QSFP28  - 2 x 40 Gigabit Ethernet QSFP+  - 1 port konsolowy RJ45  - 1 port zarządzający typu out-of-band management  - 1 port typu USB |  |
| **System operacyjny** | Modularny system operacyjny.  Musi być zgodny ze standardem ONIE i umożliwiać instalacje systemów operacyjnych innych producentów, w celu uzyskania dodatkowych funkcjonalności. |  |
| **Zasilanie** | Dwa redundantne zasilacze AC. |  |
| **Rack** | Musi zapewniać instalację w szafach 19”. |  |
| **Pamięć** | Pamięć: 4GB  Pojemność bufora pakietów: 12MB |  |
| **Wydajność** | Musi posiadać matrycę przełączającą o wydajności min. 1.76Tbps (full-duplex), min. 1320Mpps. |  |
| **Chłodzenie** | Musi posiadać możliwość chłodzenia urządzenia w trybie przód-do-tyłu lub tył-do-przodu (ustawienia fabryczne).  Musi być wyposażone w redundantne i wymienne w trakcie pracy (hot-swappable) wiatraki  Temperatura pracy w przedziale 0-40 stopni Celsjusza |  |
| **Funkcjonalności warstwy II** | Musi obsługiwać ramki „Jumbo” o długości min. 9200B.  Musi obsługiwać, co najmniej 4000 VLANów.  Pamięć dla co najmniej 270 000 adresów MAC.  Musi obsługiwać, co najmniej protokoły: STP, RSTP, RPVST+, MSTP  Musi wspierać funkcjonalność wirtualnej agregacji portów umożliwiającą:  - terminowanie pojedynczej wiązki EtherChannel/LACP wyprowadzonej z urządzenia zewnętrznego (serwera, przełącznika) na 2 niezależnych opisywanych urządzeniach  - budowę topologii sieci bez pętli z pełnym wykorzystaniem agregowanych łączy  - umożliwiać wysokodostępny mechanizm kontroli dla 2 niezależnych opisywanych urządzeń  Urządzenie musi posiadać możliwość definiowana łączy w grupy LAG (802.3ad). Obsługa min. 16 łączy w grupie LAG. |  |
| **Funkcjonalności warstwy III** | Musi obsługiwać protokoły dynamicznego routingu dla IPv4 i dla IPv6: OSPF, BGP.  Musi obsługiwać protokół BFD, przynajmniej dla protokołu OSPF i OSFP v3 i tras statycznych.  Musi przechowywać sprzętowo minimum 200 000 wpisów rotingu IPv4 lb minimum 130 000 wpisów routigu IPv6.  Musi wspierać mechanizm L3 ECMP Load Balancing.  Musi wspierać protokół redundancji VRRP.  Wsparcie dla DHCP Server i DHCP Relay.  Obsługa Policy Based Routing.  Musi obsługiwać funkcjonalność VxLAN, Static VxLAN.  Musi obsługiwać funkcjonalność VxLAN BGP EVPN (Ethernet VPN) z MP-BGP.  Obsługa routingu między VxLAN-ami (VxLAN Routing) z wykorzystaniem BGP EVPN oraz funkcjonalności Anycast Gateway.  Obsługa Multi-AS dla EVPN oraz trybów Asymmetric IRB (Integrated routing and bridging) oraz Symmetric IRB.  Obsługa mechanizmu BGP unnumbered dla EVPN. |  |
| **Mechanizmy bezpieczeństwa i QoS** | Klasyfikacja ruchu dla klas różnej, jakości obsługi QoS poprzez wykorzystanie, co najmniej następujących paramentów: źródłowy/docelowy adres MAC, źródłowy/docelowy adres IP, VLAN, wartość DSCP.  Implementacja co najmniej 8 kolejek sprzętowych na każdym porcie wyjściowym dla obsługi ruchu o różnej klasie obsługi.  Możliwość obsługi jednej z powyższych kolejek z bezwzględnym priorytetem w stosunku do innych (Strict Priority).  Implementacja mechanizmu Weighted Random Early Detection (WRED).  Obsługa IP Precedence i DSCP.  Obsługa Control-Plane-Policing (ochrona systemu operacyjnego przed atakami DoS).  Musi obsługiwać DCB (Data Center Bridging), 802.1Qbb Priority-Based Flow Control oraz Priority Flow Control oraz Enhanced Transmission Selection.  Co najmniej 3 poziomy dostępu administracyjnego przez konsolę:  - autoryzacja użytkowników/portów w oparciu o 802.1x.  - obsługa List dostępu ACL dla adresów MAC i adresów IPv4 i IPv6. |  |
| **Mechanizmy zarządzania** | Musi wspierać następujące mechanizmy zarządzania:  Możliwość uzyskania dostępu do urządzenia przez SNMPv1/2/3 i SSHv2.  Obsługa monitorowania ruchu na porcie (Port Monitoring), ACL-Based Monitoring oraz RSPAN.  Urządzenie musi posiadać dedykowany port konsolowy do zarządzania typu RJ45 (konsola) oraz drugi wydzielony typu Ethernet 100/1000BaseT.  Plik konfiguracyjny urządzenia musi być możliwy do edycji ‘offline’. Tzn. konieczna jest możliwość przeglądania zmian konfiguracji w pliku tekstowym na dowolnym PC. Po zapisaniu konfiguracji w pamięci nieulotnej musi być możliwe uruchomienie urządzenia z nową konfiguracją. Zmiany aktywnej konfiguracji muszą być widoczne bez częściowych restartów urządzania po dokonaniu zmian.  Wsparcie dla mechanizmu Beacon LED control – włączenie diody danego interfejsu celem identyfikacji.  Urządzenie musi posiadać funkcjonalność automatycznej instalacji oprogramowania poprzez ściągnięcie z serwera TFTP pliku z oprogramowaniem (firmware), w trakcie pierwszego podłączenia do sieci Ethernet.  Urządzenie musi mieć możliwość utworzenia skryptów systemu linux oraz uruchomienia skryptów utworzonych w języku Python oraz umożliwiać jego konfigurację przez narzędzia Ansible, Chef i Puppet.  Możliwość użycia RESTconf API oraz wsparcie dla mechanizmu tłumaczenia dowolnej komendy CLI na wywołanie RESTconf. |  |
| **Inne** | Przełącznik musi obsługiwać protokół Precision Time Protocol (PTP) do synchronizacji czasu zegara między urządzeniami sieciowymi.  Możliwość instalacji zewnętrznych pakietów Docker-CE I uruchamiania ich w ramach systemu operacyjnego. |  |
| **Kable** | Wymagane jest dostarczenie do każdego z przełączników:  - kabla QSFP28 do QSFP28 pasywnego podłączanego bezpośrednio o długości 0,5 metra  - 4 kabli SFP+ do SFP+ pasywnego podłączanego bezpośrednio o długości 3 metrów |  |
| **Gwarancja** | Min. 3 lata gwarancji producenta, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii 24x7x365 poprzez ogólnopolską linię telefoniczną producenta. |  |

1. **Przełącznik (typ 2)**

|  |  |  |
| --- | --- | --- |
| **Parametr** | **Charakterystyka (wymagania minimalne lub równoważne)\*** | **Parametry oferowane** |
| **Porty** | Przełącznik 1U wyposażony w porty:  - 24 x 1000Base-T RJ-45  - 2 x LAN 10 Gb SFP+  - 1 x port konsolowy RJ-45  - 1 x USB Type A  - 2 x GbE combo media port |  |
| **System operacyjny** | Modularny system operacyjny,  Musi być zgodny ze standardem ONIE i umożliwiać instalacje systemów operacyjnych innych producentów, w celu uzyskania dodatkowych funkcjonalności. |  |
| **Zasilanie** | Dwa redundantne zasilacze AC. |  |
| **Rack** | Musi zapewniać instalację w szafach 19”. |  |
| **Rodzaj obudowy** | Musi posiadać możliwość chłodzenia urządzenia w trybie przód-do-tyłu.  Musi być wyposażone w redundantne wiatraki.  Temperatura pracy w przedziale 0-45 stopni Celsjusza |  |
| **Parametry wydajnościowe** | MAC addresses: 56K (80K in L2 scaled mode)  Static routes: 16K (IPv4)/8K (IPv6)  Dynamic routes: 16K (IPv4)/8K (IPv6)  Switch fabric capacity: 212Gbps  Forwarding rate: 158Mpps  Link aggregation: 16 links per group, 128 groups  Priority queues per port: 8  Line-rate Layer 2 switching: All (non-blocking)  Line-rate Layer 3 routing: All (non-blocking)  Flash memory: 1G  Packet buffer memory: 4MB  CPU memory: 2GB DDR3  Layer 2 VLANs: 4K  MSTP: 64 instances  VRF-lite: 511 instances  Line-rate Layer 2 switching: All protocols, including IPv4 and IPv6  Line-rate Layer 3 routing: IPv4 and IPv6  IPv4 host table size: 22K (42K in L3 scaled hosts mode)  IPv6 host table size: 16K (both global + Link Local) (32K in L3 scaled hosts mode)  IPv4 Multicast table size: 8K  LAG load balancing: Based on Layer 2, IPv4 or IPv6 headers  **Musi być zgodny z następującymi standardami IEEE:**  802.1AB LLDP  802.1D Bridging, STP  802.1p L2 Prioritization  802.1Q VLAN Tagging  802.1Qbb PFC  802.1Qaz ETS  802.1s MSTP  802.1w RSTP  802.1x Network Access Control  802.1x-2010 Port Based Network Access Control  802.3ab Gigabit Ethernet (1000BASE-T)  802.3ac Frame Extensions for VLAN Tagging  802.3ad Link Aggregation with LACP  802.1ax Link Aggregation Revision - 2008 and 2011  802.3ae 10 Gigabit Ethernet (10GBase-X)  802.3az Energy Efficient Ethernet (EEE)  802.3u Fast Ethernet (100Base-TX) on mgmt ports  802.3x Flow Control  802.3z Gigabit Ethernet (1000Base-X)  ANSI/TIA-1057 LLDP-MED  Force10 PVST+  MTU 12,000 bytes  **Musi wspierać następujące protokoły i standardy:**  768 UDP  793 TCP  854 Telnet  959 FTP  791 IPv4  792 ICMP  826 ARP  1027 Proxy ARP  1035 DNS (client)  1042 Ethernet Transmission  1305 NTPv3  1519 CIDR  1542 BOOTP (relay)  1812 Requirements for IPv4 Routers  1918 Address Allocation for Private Internets  2474 Diffserv Field in IPv4 and Ipv6 Headers  2596 Assured Forwarding PHB Group  3164 BSD Syslog  3195 Reliable Delivery for Syslog  3246 Expedited Assured Forwarding  4364 VRF-lite (IPv4 VRF with OSPF and BGP)  5798 VRRP  1981 Path MTU Discovery Features  2460 Internet Protocol, Version 6 (IPv6) Specification  2464 Transmission of IPv6 Packets over Ethernet Networks  2711 IPv6 Router Alert Option  4007 IPv6 Scoped Address Architecture  4213 Basic Transition Mechanisms for IPv6 Hosts and Routers  4291 IPv6 Addressing Architecture  4443 ICMP for IPv6  4861 Neighbour Discovery for IPv6  4862 IPv6 Stateless Address Autoconfiguration  5095 Deprecation of Type 0 Routing Headers in IPv6  IPv6 Management support (telnet, FTP, TACACS, RADIUS, SSH, NTP)  1058 RIPv1 2453 RIPv2  1587 NSSA 4552 Authentication/  2154 OSPF Digital Signatures  2328 OSPFv2 OSPFv3  2370 Opaque LSA 5340 OSPF for IPv6  5301 Dynamic hostname exchange mechanism for IS-IS  5302 Domain-wide prefix distribution with two-level IS-IS  5303 Three-way handshake for IS-IS point-to-point adjacencies  5308 IS-IS for IPv6  1997 Communities  2385 MD5  2545 BGP-4 Multiprotocol Extensions for IPv6 Inter-Domain Routing  2439 Route Flap Damping  2796 Route Reflection  2842 Capabilities  2858 Multiprotocol Extensions  2918 Route Refresh  3065 Confederations  4360 Extended Communities  4893 4-byte ASN  5396 4-byte ASN representations  1112 IGMPv1  2236 IGMPv2  3376 IGMPv3  MSDP  PIM-SMw |  |
| **Mechanizmy zarządzania** | Musi wspierać następujące mechanizmy zarządzania:  1155 SMIv1  1157 SNMPv1  1212 Concise MIB Definitions  1215 SNMP Traps  1493 Bridges MIB  1850 OSPFv2 MIB  1901 Community-Based SNMPv2  2011 IP MIB  2096 IP Forwarding Table MIB  2578 SMIv2  2579 Textual Conventions for SMIv2  2580 Conformance Statements for SMIv2  2618 RADIUS Authentication MIB  2665 Ethernet-Like Interfaces MIB  2674 Extended Bridge MIB  2787 VRRP MIB  2819 RMON MIB (groups 1, 2, 3, 9)  2863 Interfaces MIB  3273 RMON High Capacity MIB  3410 SNMPv3  3411 SNMPv3 Management Framework  3412 Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)  3413 SNMP Applications  3414 User-based Security Model (USM) for NMPv3  3415 VACM for SNMP  3416 SNMPv2  3417 Transport mappings for SNMP  3418 SNMP MIB  3434 RMON High Capacity Alarm MIB  3584 Coexistence between SNMP v1, v2 and v3  4022 IP MIB  4087 IP Tunnel MIB  4113 UDP MIB  4133 Entity MIB  4292 MIB for IP  4293 MIB for IPv6 Textual Conventions  4502 RMONv2 (groups 1,2,3,9)  5060 PIM MIB |  |
| **Gwarancja** | Minimum 3 lata gwarancji producenta z czasem reakcji na następny dzień roboczy od przyjęcia zgłoszenia, możliwość zgłaszania awarii w trybie 24x7x365 poprzez ogólnopolską linię telefoniczną producenta. |  |

1. **Serwer (Backup)**

|  |  |  |
| --- | --- | --- |
| **Parametr** | **Charakterystyka (wymagania minimalne lub równoważne)\*** | **Parametry oferowane** |
| **Parametry rozwiązania** | • Serwer musi być przeznaczony do deduplikacji i przechowywania kopii zapasowych. Urządzenie musi spełniać wymagania wyspecyfikowane w niniejszej tabeli.  • Dostarczony serwer musi oferować przestrzeń min. 60TB netto (powierzchni użytkowej) bez uwzględniania mechanizmów protekcji, wymagana skalowalność do min. 100TB netto. (parametr stanowi kryterium oceny – Tabela: **Opis właściwości technicznych serwera (backup), stanowiących kryterium oceny punktowej oferty**)  • Dostarczone urządzenie powinno umożliwiać 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 oraz Microsoft Azure. Wymagana enkrypcja danych przechowywanych na warstwie typu Cloud. Wymagane dostarczenie licencji na przestrzeń 200TB netto dla warstwy Cloud, skalowanie w przypadku wykorzystywanej przestrzeni warstwy typu Cloud powinno stanowić równoważność co najmniej dwukrotnej wymaganej maksymalnej pojemności netto oferowanego urządzenia (bez uwzględnienia warstwy CLOUD), czyli 170TB x 2 = 340TB.  • Oferowane urządzenie musi posiadać minimum 4 porty Eth 10Gb/s SFP+  Wymagana możliwość obsługi każdym z w/w portów protokołów CIFS, NFS, deduplikacja na źródle.  Wymagana możliwość rozbudowy urządzenia o co najmniej 2 porty FC 16Gb/s.  Wymagana możliwość obsługi poprzez porty FC protokołów VTL oraz deduplikacja na źródle.  • Oferowane urządzenie musi umożliwiać jednoczesny dostęp wszystkimi poniższymi protokołami:  - CIFS, NFS  - zapewniającymi deduplikację na źródle – alternatywnie: OST/BOOST/CATALYST  - VTL (min. 10 jednocześnie)  • Wymagane jest dostarczenie licencji, pozwalającej na jednoczesną obsługę protokołów CIFS, NFS, OST/BOOST/CATALYST, VTL dla maksymalnej pojemności urządzenia.  • 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).  • Urządzenie musi pozwalać na jednoczesną obsługę minimum 250 strumieni w tym jednocześnie:  - zapis danych minimum 150 strumieniami  - odczyt danych minimum 50 strumieniami  - replikacja minimum 50 strumieniami  pochodzących z różnych aplikacji oraz dowolnych protokołów (CIFS, NFS, VTL, OST/BOOST/CTALYST) 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.  • Oferowane urządzenie musi mieć możliwość emulacji następujących bibliotek taśmowych:  - StorageTek L180  - IBM TS 3500  • Oferowane urządzenie musi mieć możliwość emulacji napędów taśmowych min. LTO5 oraz LTO7.  • Serwer 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.  • Oferowany serwer musi deduplikować dane in-line przed zapisem na nośnik dyskowy. Na wewnętrznych dyskach urządzenia nie mogą być zapisywane dane w oryginalnej postaci (niezdeduplikowanej) z jakiegokolwiek fragmentu strumienia danych przychodzącego do urządzenia.  • 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.  • Oferowany serwer musi posiadać obsługę mechanizmów globalnej deduplikacji dla danych otrzymywanych jednocześnie wszystkimi protokołami (CIFS, NFS, VTL, OST/BOOST/CATALYST) przechowywanych w obrębie całego 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 powinny 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.  W przypadku niespełnienia opisanego powyżej wymogu globalnej deduplikacji, przy spełnieniu pozostałych wymaganych funkcjonalności, oferowane urządzenie powinno oferować przestrzeń min. 150TB netto (powierzchni użytkowej) bez uwzględniania mechanizmów protekcji, wymagana skalowalność urządzenia w takim wypadku do min. 1050TB netto.  • 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.  • 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).  • Wszystkie unikalne bloki przed zapisaniem na dysk muszą być dodatkowo kompresowane.  • Oferowany serwer musi wspierać (wymagane formalne wsparcie producenta urządzenia), co najmniej następujące aplikacje: oferowana aplikacja backup’owa, RMAN, Microsoft SQL Server Management Studio.  W przypadku współpracy z każdą z poniższych aplikacji:  - oferowana aplikacja backup’owa  - RMAN (dla ORACLE)  - Microsoft SQL Server Management Studio (dla Microsoft SQL)  urządzenie musi umożliwiać deduplikację na źródle i przesłanie nowych, nie znajdujących się jeszcze na urządzeniu bloków poprzez sieć LAN.  Deduplikacja danych odbywa się na dowolnym serwerze posiadającym funkcjonalność: Media Agenta / klienta /serwera RMAN / serwera SQL.  Deduplikacja w wyżej wymienionych przypadkach musi zapewniać, aby z zabezpieczanych serwerów do urządzenia były transmitowane poprzez sieć LAN jedynie fragmenty danych nie znajdujące się dotychczas na urządzeniu.  • W przypadku przyjmowania backupów z Oracle RMAN oraz Microsoft MSSQL (przy wykorzystaniu Microsoft SQL Server Management Studio) , urządzenie musi umożliwiać deduplikację na źródle i przesłanie nowych, nieznajdujących się jeszcze na urządzeniu bloków poprzez sieć FC.  Deduplikacja w wyżej wymienionych przypadkach musi zapewniać, aby z serwerów do urządzenia były transmitowane poprzez sieć FC tylko fragmenty danych nie znajdujące się dotychczas na urządzeniu.  • W przypadku systemów Linux (min.: RedHat oraz SuSE) oraz Windows urządzenie powinno umożliwiać deduplikację na źródle na poziomie systemu plików. Dane kopiowane na wydzielony system plików (bez pośrednictwa aplikacji backupowej) powinny podlegać deduplikacji ew. licencje nie są przedmiotem tego postępowania.  • Oferowane urządzenie powinno umożliwiać uruchamianie maszyn wirtualnych VMware bezpośrednio z danych backupowych bez konieczności odtwarzania danych.  • W przypadku deduplikacji na źródle poprzez sieć IP (LAN oraz WAN), wymagana możliwość szyfrowania komunikacji kluczem minimum 256 bitów.  • Urządzenie powinno umożliwiać zaszyfrowanie przechowywanych danych, wymagane licencje umożliwiające zaszyfrowanie i przechowywanie zaszyfrowanych danych w obrębie maksymalnej pojemności oferowanego urządzenia.  • Serwer musi wspierać deduplikację na źródle poprzez sieć FC (SAN) minimum dla następujących systemów operacyjnych:  - Windows  - Linux (RedHat, SuSE)  • Oferowane urządzenie musi umożliwiać bezpośrednią replikację danych do drugiego urządzenia takiego samego typu. Konfiguracja replikacji musi być możliwa w każdym z trybów:  - jeden do jednego  - wiele do jednego  - jeden do wielu  - kaskadowej (urządzenie A replikuje dane do urządzenia B, które te same dane replikuje do urządzenia C)  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 nie jest przedmiotem postępowania. • Wymagana możliwość zaprezentowania każdej z logicznych części oferowanego urządzenia jako niezależnego urządzenia dostępnego za pośrednictwem CIFS, NFS, VTL, BOOST.  • Urządzenie musi umożliwiać wydzielenie określonych portów Ethernet dedykowanych do replikacji.  • W przypadku wykorzystania portów Ethernet do replikacji urządzenie musi umożliwiać przyjmowanie backupów, odtwarzanie danych, przyjmowanie strumienia replikacji, wysyłanie strumienia replikacji tymi samymi portami.  • W przypadku replikacji danych między dwoma urządzeniami oferowanego typu, wymagana możliwość kontroli przez: oferowaną aplikację backup’ową/RMAN/Microsoft SQL Server Management Studio muszą być możliwe do uzyskania jednocześnie wszystkie następujące funkcjonalności:  - replikacja odbywa się bezpośrednio między dwoma urządzeniami bez udziału serwerów pośredniczących  - replikacji podlegają tylko te fragmenty danych, które nie znajdują się na docelowym urządzeniu  - replikacja zarządzana jest z poziomu wymaganej aplikacji  - aplikacja posiada informację o obydwu kopiach zapasowych znajdujących się w obydwu urządzeniach bez konieczności przeprowadzania procesu inwentaryzacji  • 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%.  • Wymagana możliwość ograniczenia pasma używanego do replikacji między dwoma urządzeniami – oferowane urządzenie powinno być wyposażone w mechanizm umożliwiający zarządzaniem stopnia wykorzystania pasma na potrzeby replikacji.  • Zdeduplikowane i skompresowane dane przechowywane w obrębie podsystemu dyskowego urządzenia muszą być chronione za pomocą technologii RAID 6 bądź równoważnej.  • 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.  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).  • Urządzenie musi pozwalać na przechowywanie minimum 700 snapshotów jednocześnie w obrębie oferowanej przestrzeni, przy zachowaniu globalnej deduplikacji oraz standardowego trybu pracy urządzenia – umożliwiającego wykorzystanie wszystkich dostępnych funkcjonalności.  • 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).  • Urządzenie musi mieć możliwość podziału na minimum 30 logicznych części pracujących równolegle. Producent musi oficjalnie wspierać pracę minimum 30 logicznych części pracujących równolegle z pełną wydajnością urządzenia.  • Dla każdej z w/w 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.  • Wymagana możliwość zaprezentowania każdej z logicznych części oferowanego urządzenia jako niezależnego urządzenia dostępnego za pośrednictwem:  - CIFS  - NFS  - VTL  - OST/BOOST/CATALYST  • Urządzenie powinno umożliwiać zdefiniowanie blokady skasowania danych (funkcjonalność WORM). Blokada skasowania danych musi chronić plik w zdefiniowanym czasie przed usunięciem pliku, modyfikacją pliku.  Blokada skasowania danych musi działać w dwóch trybach (do wyboru przez administratora):  - możliwość zdjęcia blokady przed upływem ważności danych  - brak możliwości zdjęcia blokady przed upływem ważności danych (compliance), w tym wypadku wymagane wsparcie norm SEC 17a-4(f) lub ISO Standard 15489-1 w zakresie ochrony danych  Licencje na blokadę usunięcia/zmiany przechowywanych plików muszą być dostarczone wraz z urządzeniem.  W przypadku braku wymaganej funkcjonalności typu WORM, wymagana dostawa dodatkowej macierzy typu NAS (NFS/CIFS) o pojemności netto dwukrotnie większej od wymaganej pojemności netto deduplikatora (60TB x 2 = 120TB netto), wyposażonej w wymaganą funkcjonalność WORM. Wymagana funkcjonalność WORM niezależnie od tego czy jest dostępna na oferowanym deduplikatorze czy dodatkowej macierzy NAS musi być zintegrowana z oferowaną aplikacją backup’ową co oznacza:  - możliwość uruchomienia blokady typu WORM dla określonych danych z poziomu oferowanej aplikacji backup’owej  - możliwość określenia/wymuszenia czasu blokady z poziomu oferowanej aplikacji backup’owej  - możliwość raportowania od strony oferowanej aplikacji backup’owej danych zabezpieczonych przed usunięciem wymaganą blokadą typu WORM  • Urządzenie musi mieć możliwość przechowywania danych niezmienialnych:  - video  - grafika  - nagrania dźwiękowe  - pliki pdf  na udziałach CIFS/NFS.  • Serwer 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 powinna 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 urzadzenia muszą uwzględniać tę funkcjonalność.  Wymagane potwierdzenie opisanej funkcjonalności w oficjalnej dokumentacji producenta oferowanego urządzenia.  • 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).  • Wymagana możliwość zdefiniowania maksymalnego obciążenia urządzenia procesem usuwania przeterminowanych danych (poziomu obciążenia procesora).  • Wymagana możliwość zdefiniowania harmonogramu wg. którego wykonywany jest proces usuwania przeterminowanych danych (czyszczenia), realizowany równolegle z procesami backup/restore/replication.  • 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).  • Urządzenie musi mieć możliwość zarządzania poprzez:  - interfejs graficzny dostępny z przeglądarki internetowej  - poprzez linię komend (CLI) dostępną z poziomu ssh (secure shell)  • Oprogramowanie do zarządzania musi rezydować na oferowanym na urządzeniu deduplikacyjnym.  • Oferowane urządzenie musi mieć możliwość sprawdzenia pakietu upgrade’ującego firmware urządzenia (GUI lub CLI), to znaczy sprawdzenia czy nowa wersja systemu nie spowoduje problemów z urządzeniem.  • Urządzenie musi być rozwiązaniem kompletnym, appliancem sprzętowym pochodzącym od jednego producenta. Zamawiający nie dopuszcza stosowania rozwiązań typu gateway. Oferowany typ urządzenia musi być oficjalnie dostępne w ofercie producenta przed ukazaniem się niniejszego postępowania. |  |
| **Wsparcie techniczne i gwarancja** | Minimum 3 lata gwarancji producenta, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii 24x7x365 poprzez ogólnopolską linię telefoniczną producenta. |  |

**Opis właściwości technicznych serwera (backup), stanowiących kryterium oceny punktowej oferty.**

|  |  |  |
| --- | --- | --- |
| **Lp.** | **Charakterystyka (wymagania minimalne lub równoważne\*)** | **Spełnia (TAK/NIE)\*\*** |
| 1 | Dostarczony serwer musi oferować przestrzeń min. 60TB netto (powierzchni użytkowej) bez uwzględniania mechanizmów protekcji, wymagana skalowalność do min. 100TB netto. |  |
| Gdzie:  Deklaracja spełnienia na „NIE” – 0 pkt.  Deklaracja spełnienia na „TAK”:  100 TB - 0 pkt.  101-119 TB - 10 pkt.  120-149 TB – 15 pkt.  150-159 TB – 20 pkt.  160-170 TB – 25 pkt.  Od 171 TB – 30 pkt. | **Oferujemy**  **…………….. TB** |

1. **Oprogramowanie do wykonywania kopii zapasowych**

|  |  |  |
| --- | --- | --- |
| **Parametr** | **Charakterystyka (wymagania minimalne lub równoważne)\*** | **Parametry oferowane** |
| **Parametry rozwiązania** | • Zamawiający wymaga dostarczenia, uruchomienia i wdrożenia oprogramowania do backupu środowiska datacenter (baz danych, maszyn wirtualnych, serwerów plików, serwerów wolnostojących).  • Wymagane jest dostarczenie wszystkich modułów oprogramowania backupowego tak, aby zapewnić backup całości wyspecyfikowanego środowiska oraz spełnić wszystkie wymienione w niniejszej tabeli funkcjonalności.  • Dostarczone licencje muszą umożliwiać backup/odtwarzanie:  - dowolnej liczby maszyn wirtualnych jako obrazów („image level”)  - agentowo, dowolnej liczby baz danych, plików ze środka maszyn wirtualnych  - dowolnej liczby TB w zabezpieczanym środowisku  • Serwer backupu musi być zainstalowany jako maszyną wirtualna systemu wirtualnego oferowanego z serwerami hyperkonwergentnymi.  • Serwer backupu musi być dostarczony w postaci gotowej maszyny wirtualnej.  • Wymagana jest pełna integracja oferowanego rozwiązania z zaoferowanym serwerem archiwizacyjnym.  • Wymaga się, aby dla wszystkich rodzajów wspieranych środowisk, oferowane rozwiązanie wykonywało backup z deduplikacją na źródle na oferowany serwer archiwizacyjny.  • Oprogramowanie backupowe musi zapewniać bezpośredni backup z każdej zabezpieczanej maszyny znajdującej się w sieci LAN bezpośrednio na oferowany serwer archiwizacyjny bez pośrednictwa jakichkolwiek innych serwerów. Powyższa funkcjonalność nie może wymagać dodatkowej licencji.  • Backup z dededuplikacją na źródle musi być dostępny dla wszystkich typów danych w ramach oferowanego rozwiązania: pliki, bazy danych, obrazy maszyn wirtualnych, Kubernetes.  • Wymaga się, aby oprogramowanie backupowe zapewniało szybki backup blokowy wielomilionowych systemów plików na maszynach Windows / Linux.  W trakcie backupu oprogramowanie backupowe musi wykonywać kopie zapasowe fizycznych bloków a nie plików, jednocześnie wymagana jest możliwość odtworzenia:  - całego wolumenu  - pojedynczego pliku  Celem minimalizacji czasu backupu oprogramowanie backupowe nie może indeksować plików znajdujących się na zabezpieczanym wolumenie (zaindeksowanie wielu milionów plików powoduje duże wydłużenie czasu backupu).  • Wymaga się, aby oprogramowanie backupowe zapewniało pełen backup (full backup) blokowy wielomilionowych systemów plików na maszynach Windows / Linux poprzez odczyt tylko zmienionych bloków, odczyt całości zabezpieczanego dysku może być wykonany jedynie podczas pierwszego backupu bądź po restarcie serwera. Wszystkie kolejne backupy mają odczytywać z dysku jedynie zmienione bloki w stosunku do ostatniego backupu (w efekcie na serwerze archiwizacyjnym muszą pojawić się kopie typu full backup). Oprogramowanie backupowe musi odczytywać, jedynie zmienione na dysku bloki (a nie całe pliki).  • Ze względów bezpieczeństwa rozwiązanie backupowe musi mieć możliwość wykonania kopii wewnętrznej bazy danych w trakcie pracy systemu bez konieczności ograniczania jego funkcjonalności.  • Oprogramowanie backupowe musi umożliwiać zarządzanie replikacją backupów między serwerami archiwizacyjnymi oferowanego typu, bezpośrednio z poziomu interfejsu oprogramowania backupowego przy spełnieniu wszystkich poniższych wymagań:  - replikacji podlegają tylko te bloki które nie znajdują się na docelowym serwerze archiwizacyjnym  - replikacja między serwerami archiwizacyjnymi następuje w zdefiniowanych interwałach czasowych  - oferowane oprogramowanie backupowe przechowuje informacje o wszystkich kopiach danych znajdujących się na serwerach archiwizacyjnych (czyli kopii oryginalnej oraz zreplikowanej)  - oferowane oprogramowanie backupowe pozwala na wybór serwera archiwizacyjnego z którego zostanie wykonane odtwarzanie bez konieczności przeprowadzania inwentaryzacji  • Oprogramowanie backupowe musi umożliwiać określenie różnych retencji dla danych na podstawowym nośniku i nośniku zawierającym kopię (replika backupu). Określenie czasu retencji przechowywania dla kopii (repliki) musi być możliwe w momencie definiowania zadania backupowego.  • Oferowane rozwiązanie backupowe musi pozwalać na użycie blokady WORM dostępnej na oferowanym serwerze archiwizacyjnym (wymagane wsparcie potwierdzone w dokumentacji serwera archiwizacyjnego i oprogramowania), zabezpieczającej przed skasowaniem/zmianą backupów w określonym czasie.  • Oprogramowanie musi umożliwiać natychmiastową aktywację blokady WORM natychmiast po zakończeniu wykonywania backupu.  • Wymagana możliwość aktywacji blokady WORM - per zadanie backupowe, dla każdego zadania backupowego wymagana możliwość ustawienia innego czasu blokady backupu.  • Wymaga się, aby użycie blokady WORM było możliwe dla wszystkich systemów wspieranych przez oferowane oprogramowanie.  • Wymaga się, aby z poziomu konsoli oprogramowania backupowego dostępna była możliwość definiowania wymaganej retencji danych (backupów) w oparciu o kryteria czasowe (dni, miesiące, lata). Po przekroczeniu okresu retencji, określone kopie backupowe muszą być automatycznie usunięte.  • Dla baz danych MSSQL wymagana możliwość inicjowania backupów przez administratora MSSQL przy spełnieniu wszystkich poniższych wymagań:  - backup jest wykonywany przez oferowane oprogramowanie backupowe  - inicjowanie backupu z graficznego interfejsu będącego częścią MSSQL Management Studio  - możliwość wyboru backupu pełnego, różnicowego, logów  - backup inicjowany przez administratora MSSQL nie może wymagać kontaktu z administratorem oferowanego rozwiązania backupowego  • W przypadku zabezpieczania baz MSSQL wymagana możliwość inicjowania i wykonywania backupów przez administratora MSSQL także w przypadku, gdy serwer backupu jest niedostępny.  • Dla baz danych MSSQL wymagana możliwość odtworzenia backupów przez administratora MSSQL przy spełnieniu wszystkich poniższych wymagań:  - odtworzenie dowolnego backupu wykonanego przez oferowane rozwiązanie backupowe  - zarządzanie odtwarzaniem z graficznego interfejsu będącego częścią MSSQL Management Studio  - możliwość odtworzenia do dowolnego punktu w czasie wybranego przez administratora MSSQL w ramach przechowywanych przez oferowane oprogramowanie backupowe logów MSSQL  - odtworzenie bazy danych przez administratora MSSQL nie może wymagać kontaktu z administratorem oferowanego rozwiązania backupowego  • Dla baz danych MSSQL wymagana możliwość realizowania samobackupującego się środowiska MS-SQL umożliwiającego automatyczny wybór backupowych baz danych w momencie startu backupu. Administrator definiuje reguły – jakie bazy danych mają być backupowane w ramach polityki – oprogramowanie backupowe backupuje wszystkie bazy danych spełniające określone reguły.  • Wymaga się, aby reguły (o których mowa w poprzednim punkcie), umożliwiające określenie, które bazy będą backupowane uwzględniały:  - nazwy backupowanych baz danych  - nazwy serwerów bazy danych  - nazwy klastrów  - typy hostów  - nazwy aplikacji  Reguły muszą pozwalać na wybór nazw:  - zaczynających się od określonego tekstu  - zawierających określony tekst  - niezawierających określonego tekstu  - kończących się określonym tekstem  • Rozwiązanie backupowe musi wspierać backup i odtwarzanie środowisk VMware. Oprogramowanie backupowe musi umożliwiać w przypadku środowisk VMware następujące typy backupu:  - backup pojedynczych plików i baz danych ze środka maszyny wirtualnej VMware.  - backup całych maszyn wirtualnych (obrazów, plików vmdk reprezentujących wirtualną maszynę, realizacja backupu nie może wymagać bufora dyskowego na kopię obrazów maszyn wirtualnych)  - backup tylko wybranych dysków maszyny wirtualnej (wybranych plików vmdk systemu VMware, realizacja backupu nie może wymagać bufora dyskowego na kopię obrazów maszyn wirtualnych)  - wszystkie backupy obrazów maszyn wirtualnych muszą być wykonywane przy pomocy technologii CBT systemu VMware to znaczy do medium backupowego z systemu VMware muszą być transferowane tylko zmienione bloki, z punktu widzenia systemu backupowego musza to być backupy pełne (full backup).  Powyższe metody backupu maszyn wirtualnych muszą podlegać deduplikacji ze zmiennym blokiem przed wysłaniem danych do oferowanego serwera archiwizacyjnego, metody te muszą być wbudowane w system backupu i w pełni automatyczne bez wykorzystania skryptów/dodatkowych komend.  • Oferowane rozwiązanie backupowe musi umożliwiać odtwarzanie obrazów maszyn wirtualnych VMware przy zachowaniu następujących funkcjonalności:  - odtworzenie całych maszyn wirtualnych musi wykorzystywać mechanizm CBT systemu VMware (odtwarzane są tylko te bloki wirtualnej maszyny/dysku które uległy zmianie od ostatniego backupu)  - odtworzenie pojedynczych dysków maszyn wirtualnych musi wykorzystywać mechanizm CBT systemu VMware (odtwarzane są tylko te bloki wirtualnej maszyny/dysku które uległy zmianie od ostatniego backupu)  - odtworzenie pojedynczych plików z backupu obrazu maszyny wirtualnej bez konieczności odtworzenia całej maszyny wirtualnej. Funkcjonalność musi być dostępna dla obrazów maszyn wirtualnych z zainstalowanym systemem operacyjnym Windows oraz Linux  Powyższe metody odtworzenia muszą być wbudowane w system backupu i w pełni automatyczne bez wykorzystania skryptów/dodatkowych komend.  • Oferowane rozwiązanie backupowe musi umożliwiać uruchomianie maszyn wirtualnych bezpośrednio z oferowanego serwera archiwizacyjnrgo bez konieczności odtwarzania danych (Instant Access).  • Skalowalność oferowanego rozwiązania dla środowisk VMware musi pozwalać na:  - backup minimum 1000 maszyn wirtualnych w ramach pojedynczej instancji systemu backupu  - równoległy backup dysków w ramach backupu pojedynczej maszyny wirtualnej VMware  • Oferowane rozwiązanie backupowe musi umożliwiać backup minimum 25 maszyn wirtualnych z pojedynczego serwera proxy (z pojedynczego serwera odczytującego obrazy maszyn wirtualnych) VMware.  • Wymaga się, aby Administrator aplikacji backupowej za pośrednictwem GUI (graficzna konsola) miał dostępne następujące możliwości odtwarzania maszyn VMware:  - odtworzenie całej maszyny wirtualnej VMware  - odtworzenie pojedynczego dysku uprzednio zarchiwizowanej całej maszyny wirtualnej  - odtworzenie plików / katalogów z backupu obrazu maszyny wirtualnej  - uruchomienie maszyny wirtualnej bezpośrednio z backupu dostępnego na oferowanym serwerze archiwizacyjnym bez wcześniejszego odtwarzania danych  - naprawienie aktualnej instancji maszyny wirtualnej– odtworzenie tylko zmienionych bloków od ostatniego backupu  Wszystkie w/w możliwości muszą być dostępne w postaci graficznych wizardów.  • Oferowane 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, przy czym całość informacji dot. backupów środowisk VMware musi być przechowywana na serwerze backupu.  • Wymaga się, aby maszyna wirtualna VMware zbackupowana poprzez serwer pośredniczący: A, mogła być odtworzona przez dowolny inny system pośredniczący np: B, C, itd.  • Oferowane oprogramowanie backupowe musi samo dystrybuować zadania backupu/odtwarzania obrazów maszyn wirtualnych VMware między dostępne serwery pośredniczące zapewniając równomierne obciążenie.  • Wymaga się, aby w przypadku środowisk VMware oferowane rozwiązanie backupowe automatycznie rozpoznawało nowo utworzone maszyny wirtualne oraz przypisywało je do odpowiednich polityk backupowych, wymagana możliwość konfiguracji/realizacji następującego scenariusza:  - wszystkie nowo utworzone maszyny wirtualne zawierające w nazwie frazę „krytyczna” muszą być backupowana automatycznie co godzinę  - wszystkie nowo utworzone maszyny wirtualne zawierające w nazwie frazę „produkcja” muszą być backupowana automatycznie raz na dzień  - pozostałe maszyny wirtualne są backupowane raz na tydzień  Oferowane rozwiązanie backupowe musi umożliwiać realizację backupów wg. w/w scenariusza, bez jakichkolwiek akcji ze strony administratora backupu/VMware czy też jakiekolwiek innej osoby.  • Wymaga się, aby w przypadku środowisk VMware oferowane oprogramowanie backupowe pozwalało na:  - automatyczne dodanie do odpowiednich polityk backupowych wszystkich maszyn wirtualnych zawierających w nazwie maszyny wirtualnej podany tekst  - automatyczne dodanie do odpowiednich polityk backupowych wszystkich maszyn wirtualnych znajdujących się we wszystkich folderach zawierających w nazwie podany tekst  - automatyczne dodanie do odpowiednich polityk backupowych wszystkich maszyn wirtualnych których Tag zawiera podany tekst  - automatyczne dodanie do odpowiednich polityk backupowych wszystkich maszyn wirtualnych znajdujących się na wszystkich datastore’ach które w nazwie zawierają podany tekst.  • Wymaga się, aby w środowisku VMware oferowane oprogramowanie backupowe pozwalało na automatyczne usuwanie maszyn wirtualnych z polityk backupowych w tym samym momencie, w którym maszyna jest usunięta z vCenter, dotychczas wykonane kopie zapasowe muszą być przechowywane zgodnie z określoną wcześniej retencją, umożliwiając odtworzenie tej maszyny.  • Oferowane rozwiązanie backupowe musi wspierać środowiska Kubernetes  • Wymaga się, aby podpięcie środowiska Kubernetes do oferowanego rozwiązania backupowego było maksymalnie proste, ograniczało się do podania jedynie nazwy FQDN/IP środowiska i uprawnień.  • Wymaga się, aby oprogramowanie backupowe automatycznie instalowało wymagane moduły w zabezpieczanym środowisku Kubernetes, wprost z repozytorium sieciowego producenta (np. GitHub).  Jeśli sieciowe repozytorium producenta jest niedostępne z poziomu środowiska Kubernetes, wymagana możliwość automatycznego pobierania modułów ze wskazanego repozytorium.  • Oferowane rozwiązanie musi zapewniać backup dowolnych namespace znajdujących się w środowisku Kubernetes.  • Wymagana możliwość wykluczenia dowolnych dysków PVC z backupu dowolnego namespace.  • Wymagana możliwość skonfigurowania samobackupującego się środowiska Kubernetes - w momencie startu backupu następuje automatyczny wybór backupowanych namespace zgodnie z regułami określonymi przez Administratora.  • Wymagana możliwość tworzenia w/w reguł używanych przy backupie określonych namespace w oparciu o:  - nazwy backupowanych namespace  - etykiety backupowanych namespace  Reguły muszą pozwalać na wybór nazw:  - zaczynających się od określonego tekstu  - zawierających określony tekst  - niezawierających określonego tekst  - kończących się określonym tekstem  • Wymaga się, aby backup realizowany był zgodnie ze zdefiniowana polityką lub inicjowany ad hoc, uruchomiony ręcznie przez administratora.  • W ramach dostarczonych licencji wymagana możliwość spójnego backupu baz danych i aplikacji Cassandra, MySQL, PostreSQL, MongoDB działających w obrębie zabezpieczanych środowisk Kubernetes.  • Wymagana możliwość realizacji backupów syntetycznych.  W przypadku środowisk Kubernetes działających w infrastrukturze VMware: odczyt jedynie zmienionych bloków, finalnie na serwerze archiwizacyjnym uzyskiwany jest pełen backup (full).  Oferowane oprogramowanie musi umożliwiać automatyczną realizację powyższego scenariusza, nie może wymagać dodatkowych działań ze strony administratora backupu.  • W przypadku środowisk Kubernetes wymagana możliwość odtworzenia całych namespace lub wybranych dysków PVC.  • W przypadku środowisk Kubernetes wymagana możliwość odtworzenia danych zarówno na oryginalne środowisko Kubernetes jak również inne środowisko Kubernetes.  • Wymagana możliwość bezpośredniego odtwarzania danych zarówno przez administratora backupu jak również przez administratora Kubernetes.  • Wymaga się, aby zarządzanie zarówno w przypadku backupu, odtwarzania oraz wszystkich dostępnych funkcjonalności dla środowisk Kubernetes było dostępne za pośrednictwem jednej centralnej konsoli graficznej GUI HTML 5.  • Wymaga się, aby konsola oprogramowania backupowego umożliwiała definiowanie polityk backupowych obejmujących całość cyklu życia kopii zapasowej.  W szczególności wymagana możliwość zdefiniowania polityki backupowej która dla dowolnej liczby zabezpieczanych systemów (zadań backupowych) zapewnia:  - lokalny backup na oferowany serwer archiwizacyjny z retencją 30-dniową  - replikację (na poziomie bloków) do drugiego serwera archiwizacyjnego oferowanego typu (retencja 60 dni)  Całość wymaganych operacji powinna być skonfigurowana poprzez pojedynczą politykę backupową stworzoną poprzez GUI oprogramowania backupowego w oparciu o dostępny „wizard”.  Wymaga się, aby administrator backupu za pośrednictwem konsoli (GUI) oferowanego oprogramowania backupowego mógł odtwarzać dane VMware/Kubernetes z dowolnych w/w kopii (1-2). |  |
| **Wymagana ilość i**  **rodzaj licencji** | Wymagane licencjonowanie oprogramowania backupowego powinno uwzględniać sumaryczną ilość CPU zabezpieczanego środowiska bez ograniczeń dotyczących ilości zabezpieczanych danych (FET), ilości zabezpieczanych serwerów wirtualnych jak i fizycznych czy ilości używanych mediów dedykowanych do przechowywania danych.  Wymagane jest dostarczenie licencji oprogramowania backupowego dla 4 procesorów fizycznych (zajętych socketów) w zabezpieczanych maszynach.  Wymaga się, aby wszystkie dostępne funkcjonalności oferowanego rozwiązania były odblokowane w ramach oferowanej licencji procesorowej. |  |
| **Gwarancja i serwis** | Oprogramowanie musi posiadać co najmniej 36 miesięczną opiekę serwisową. Musi istnieć możliwość zgłaszania problemów z oprogramowaniem bezpośrednio do producenta z reakcją następnego dnia roboczego. |  |

1. **Zasilacz awaryjny**

|  |  |  |
| --- | --- | --- |
| **Parametr** | **Charakterystyka (wymagania minimalne lub równoważne)\*** | **Parametry oferowane** |
| Moc wyjściowa | 5.0 kVA |  |
| Moc rzeczywista | 4.5 kW |  |
| Napięcie wyjściowe | 230 V |  |
| Zniekształcenia napięcia wyjściowego | Poniżej 2% |  |
| Częstotliwość na wyjściu (zsynchronizowana z siecią zasilającą) | 50/60 Hz +/- 3 Hz synchronicznie z siecią |  |
| Współczynnik szczytu | 3:1 |  |
| Topologia | Technologia Double Conversion Online |  |
| Typ przebiegu | Sinusoida |  |
| Złącza wyjściowe | (6) IEC 320 C13  (4) IEC 320 C19 |  |
| Układ obejściowy (bypass) | Wewnętrzny bypass (automatyczny i ręczny) |  |
| Nominalne napięcie wejściowe | 230 V |  |
| Częstotliwość wejściowa | 40 - 70 Hz |  |
| Typ gniazda wejściowego | kablowe (1PH + N + G) |  |
| Zakres napięcia wejściowego w trybie podstawowym | 100 - 275 |  |
| Typ akumulatora | Akumulator kwasowo-ołowiowy |  |
| Typowy czas ładowania | 1,5h |  |
| Znamionowe napięcie akumulatora | 192 V |  |
| Oczekiwana żywotność akumulatora | Min. 3 lata |  |
| Pojemność akumulatora (Volt-Amp-hour) | Min. 800 |  |
| Typowy czas podtrzymania przy pełnym obciążeniu | Min. 4 minuty |  |
| Typowa sprawność przy pełnym obciążeniu | Min. 90% |  |
| Zarządzanie (porty) | RJ-45 Ethernet, RJ-45 Szeregowe, gniazdo modułów komunikacyjnych, USB |  |
| Panel sterowania | LCD |  |
| Alarm dźwiękowy | Alarmy dżwiękowe i wizualne według priorytetu ważności zdarzenia |  |
| Awaryjny wyłącznik zasilania | Tak |  |
| Ochrona przed przepięciami i filtracja | Klasa energetyczna sprzętu przeciwprzepięciowego: 480 J |  |
| Maksymalna wysokość | 3U |  |
| Maksymalna głębokość | 720 mm |  |
| Hałas słyszalny w odległości 1 m od powierzchni urządzenia | Poniżej 57 dBA |  |
| Certyfikaty i zgodność z normami | CE, Znak CE, EAC, EN/IEC 62040-1, EN/IEC 62040-2, IRAM, RCM, VDE |  |
| Gwarancja | Minimum 3 lata gwarancji naprawy lub wymiany (bez akumulatora) i 2 lata na akumulator |  |

**Formularz cenowy**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Lp. | Opis | Oferowany model, rodzaj, typ, nazwa producenta | Spełnienie minimalnych parametrów technicznych (TAK/NIE\*\*) | Ilość | Cena netto | Cena brutto | Wartość netto | Podatek VAT | Wartość brutto |
| [szt.] | [PLN] | [PLN] | [PLN] | [%] | [PLN] |
| 1 | Sewer (HCI) |  | TAK | 4 |  |  |  | 23 |  |
| 2 | Przełącznik (typ 1) |  | TAK | 2 |  |  |  | 23 |  |
| 3 | Przełącznik (typ 2) |  | TAK | 1 |  |  |  | 23 |  |
| 4 | Serwer (Backup) |  | TAK | 1 |  |  |  | 23 |  |
| 5 | Oprogramowanie do wykonywania kopii zapasowych |  | TAK | 1 |  |  |  | 23 |  |
| 6 | Zasilacz awaryjny |  | TAK | 2 |  |  |  | 23 |  |
| **SUMA** | | | | | |  |  | **X** |  |

**UWAGI:**

\*) Wykorzystanie w opisie przedmiotu zamówienia nazw własnych oraz znaków towarowych ma na celu wyłącznie zapewnienie kompatybilności zamawianego sprzętu i oprogramowania ze sprzętem i oprogramowaniem już posiadanym przez Zamawiającego oraz zapewnienie właściwości i parametrów zamawianego sprzętu i oprogramowania niezbędnych ze względu na specyfikę prowadzonej działalności naukowo-badawczej. Dopuszcza się zastosowanie parametrów równoważnych

\*\*) Wpisać właściwe.

1. Wykonawca zobowiązany jest przy realizacji zamówienia do:
2. Wykonawca odpowiedzialny jest za podłączenie wszystkich komponentów i ich konfigurację. Za dostarczenie i ew. konfigurację modułów optycznych zarówno do serwerów jak i przełączników Zamawiającego odpowiada Wykonawca.
3. W ramach dostawy Wykonawca dostarczy niezbędne Urządzenia oraz Oprogramowanie.
4. W ramach wdrożenia Wykonawca wykona: instalację, podłączenie, uruchomienie oraz skonfigurowanie urządzeń oraz oprogramowania. W zakres prac będzie wchodziło co najmniej:
   1. montaż serwerów w szafach Zamawiającego;
   2. podłączenie urządzeń do zasilania elektrycznego w szafach;
   3. podłączenie serwerów do przełączników, które zostaną zainstalowane w szafach;
   4. instalacja Oprogramowania na serwerach we współpracy z inżynierami Zamawiającego, w tym wirtualizatorów, systemu zarządzającego platformą wirtualizacyjną, Oprogramowania HCI i każdego innego dostarczonego w ramach rozwiązania Oprogramowania;
   5. konfiguracja całego rozwiązania (w tym konfiguracja sieciowa) we współpracy z Zamawiającym w sposób umożliwiający uzyskanie system HCI pełni wymaganych funkcjonalności.
   6. migrację serwerów wirtualnych utrzymywanych w obecnym środowisku wirtualnym Zamawiającego (minimum 8 szt.)
   7. wdrożenie systemu archiwizacji danych w oparciu o dostarczone urządzenia oraz oprogramowanie
   8. wykonanie dokumentacji powykonawczej
5. Wykonawca wraz z Urządzeniami dokona dostawy wszystkich niezbędnych elementów koniecznych do montażu i uruchomiania Urządzeń w Lokalizacjach tj. pasywnego sprzętu sieciowego i okablowania.
6. Wykonawca zainstaluje Urządzenia oraz dokona konfiguracji w uzgodnieniu z Zamawiającym.
7. Zapewnienie wsparcia technicznego w liczbie 100h, do wykorzystania w okresie do 3 miesięcy od daty podpisania protokołu odbioru. Obszary objęte wsparciem technicznym systemów informatycznych:
   1. Administracja serwerów wirtualnych MS Windows, Unix/Linux w środowisku HCI
   2. Administracja warstwą sprzętową infrastruktury kluczowej HCI
      * Administracja Vmware vSphere / Vmware vSAN
      * Monitoring systemów HCI
   3. Wsparcie dla technologii klastra HCI
   4. Administracja systemami backupu i archiwizacji danych
   5. Wsparcie administratorów Zamawiającego – Help Desk w godzinach 8:00-16:00 w dni robocze z czasem reakcji na zgłoszenie do 1 godziny.

**Dotyczy pozycji od 1 do 4 formularza cenowego:**

Uniwersytet Medyczny w Białymstoku jest uprawniony do stosowania 0% stawki podatku VAT przy zakupie sprzętu komputerowego. Zastosowanie stawki podatku VAT w wysokości 0% przy zakupie przez Uniwersytet Medyczny w Białymstoku sprzętu komputerowego jest możliwe pod warunkiem otrzymania z Ministerstwa Zdrowia zaświadczenia uprawniającego do zastosowania takiej stawki podatkowej.

Zgodnie z ustawą z dnia 11 marca 2004 r. o podatku od towarów i usług, stawką podatku VAT w wysokości 0% objęty jest zakup następującego sprzętu komputerowego:

* jednostki centralne komputerów, serwery, monitory, zestawy komputerów stacjonarnych;
* drukarki; skanery;
* urządzenia komputerowe do pism Braille'a (dla osób niewidomych i niedowidzących);
* urządzenia do transmisji danych cyfrowych (w tym koncentratory i switche sieciowe, routery i modemy).

W związku z powyższym Wykonawca zobowiązany jest na podstawie wymienionych wyżej warunków do wystawienia faktury VAT w kwocie netto (w przypadku wcześniejszego uzyskania zaświadczenia przez UMB) lub do wystawienia faktury korygującej z 0% stawką VAT.