**Załącznik nr 2**

Znak sprawy: **DZA 381.1.2024**

**Wykonawca:**

……………………………………………………

……………………………………………………

*(pełna nazwa/firma, adres, w zależności od podmiotu: NIP/PESEL, KRS/CEiDG)*

reprezentowany przez:

……………………………………………………

……………………………………………………

*(imię, nazwisko, stanowisko/podstawa do reprezentacji)*

**OPIS WYMAGANYCH PARAMETRÓW TECHNICZNYCH**

przystępując do udziału w postępowaniu o udzielenie zamówienia publicznego pn:

**DOSTAWA SERWERÓW, MACIERZY DYSKOWYCH, SYSTEMU BACKUP WRAZ   
Z MONTAŻEM, URUCHOMIENIEM URZĄDZEŃ, WIRTUALIZACJĄ.**

Oświadczam, że przedmiot zamówienia – spełnia minimalne wymagania i parametry opisane poniżej:

1. **Serwer – 3 szt. działające w klastrze:**

Producent serwerów: …………………………...............................

Model serwerów: ………………………….....................................

Rok produkcji serwerów: ………………………….........................

***Minimalne parametry określone w tabeli dotyczą 1 szt. Serwera. Zamawiający wymaga dostarczenia trzech jednakowych serwerów.***

|  |  |  |  |
| --- | --- | --- | --- |
| **Lp.** | **Nazwa komponentu** | **Opis wymaganych parametrów** | **Parametry oferowane** |
| **1.** | **2.** | **3.** | **4.** |
| **1.** | **Typ:** | Serwer Typu RACK (fabrycznie nowy) rok produkcji nie starszy niż 2022 r., |  |
| **2.** | **Obudowa** | Obudowa Rack o wysokości max 2U z możliwością instalacji min. 8 dysków 2,5” wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych oraz organizatorem do kabli.  Wyposażona w panel LCD  Obudowa z możliwością wyposażenia w kartę umożliwiającą dostęp bezpośredni poprzez urządzenia mobilne - serwer musi posiadać możliwość konfiguracji oraz monitoringu najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej min. (Android/ Apple iOS) przy użyciu jednego z protokołów BLE/ WIFI. |  |
| **3.** | **Płyta główna** | Płyta główna z możliwością zainstalowania do dwóch procesorów.  Obsługa procesorów 56 rdzeniowych.  Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym.  Płyta główna powinna obsługiwać do 8TB pamięci RAM. |  |
| **4.** | **Chipset** | Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych |  |
| **5.** | **Procesor** | Zainstalowane dwa procesory min. 8-rdzeniowe klasy x86, dedykowane do pracy z zaoferowanym serwerem umożliwiające osiągnięcie wyniku min. 177 w teście SPECrate2017\_int\_base, dostępnym na stronie www.spec.org dla konfiguracji dwuprocesorowej. |  |
| **6.** | **Pamięć RAM** | Minimum 256GB DDR5 RDIMM 4800MT/s,  Na płycie głównej powinno znajdować się minimum 32 sloty przeznaczone do instalacji pamięci. |  |
| **7.** | **Funkcjonalności pamięci RAM** | Demand Scrubbing,  Patrol Scrubbing,  Permanent Fault Detection (PFD) |  |
| **8.** | **Gniazda PCI** | Min. 8 slotów PCIe w tym minimum 4 sloty Gen5 |  |
| **9.** | **Interfejsy sieciowe/FC/SAS** | Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT oraz  6 interfejsów sieciowych 25Gb Ethernet w standardzie SFP28, wyposażonych we wkładki SFP+ SR 10Gbe. Wkładki muszą być przetestowane przez producenta oferowanego serwera i znajdować się na liście wkładek rekomendowanych do użycia z oferowanym typem serwera - Wykonawca złoży dokument potwierdzający spełnianie wymogu.  4 zewnętrzne porty SAS 12Gb/s do podłączenia zewnętrznej macierzy dyskowej. |  |
| **10.** | **Dyski twarde** | Zainstalowane 2 dyski SSD SATA o pojemności min. 480GB Read Intensive, 2,5“ Hot-Plug.  Możliwość zainstalowania dwóch dysków M.2 NVMe SSDs o pojemności min. 960GB Hot-Plug z możliwością konfiguracji RAID 1. |  |
| **11.** | **Kontroler RAID** | Sprzętowy kontroler dyskowy, posiadający:  Min. 8GB nieulotnej pamięci cache,  Możliwość konfiguracji poziomów RAID: 0, 1, 5, 6, 10, 50, 60. |  |
| **12.** | **Wbudowane porty** | 4x USB, w tym min. 1 porty USB 3.0  Min. 1x VGA z czego jeden na panelu przednim, możliwość instalacji drugiego portu z tyłu obudowy.  Możliwość rozbudowy o Serial Port |  |
| **13.** | **Video** | Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1280x1024 |  |
| **14.** | **Wentylatory** | Redundantne, Hot-Plug |  |
| **15.** | **Zasilacze** | Redundantne, Hot-Plug min. 1100W każdy.  Dołączone dwa kable zasilające z końcówkami odpowiednimi do posiadanych przez urządzenie gniazd zasilania oraz z końcówkami do listwy PDU, umożlwiające zasilanie z sieci 230V. |  |
| **16.** | **Bezpieczeństwo** | Zatrzask górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych.  Możliwość wyłączenia w BIOS funkcji przycisku zasilania.  BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła  Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą.  Moduł TPM 2.0  Możliwość dynamicznego włączania I wyłączania portów USB na obudowie – bez potrzeby restartu serwera  Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem |  |
| **17.** | **Karta Zarządzania** | * Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca:   + zdalny dostęp do graficznego interfejsu Web karty zarządzającej;   + zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera);   + szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika;   + możliwość podmontowania zdalnych wirtualnych napędów;   + wirtualną konsolę z dostępem do myszy, klawiatury;   + wsparcie dla IPv6;   + wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish;   + możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer;   + możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer;   + integracja z Active Directory;   + możliwość obsługi przez dwóch administratorów jednocześnie;   + wsparcie dla dynamic DNS;   + wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej.   + możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera   + możliwość zarządzania do 100 serwerów bezpośrednio z konsoli karty zarządzającej pojedynczego serwera   oraz z możliwością rozszerzenia funkcjonalności o:   * + Wirtualny schowek ułatwiający korzystanie z konsoli zdalnej   + Przesyłanie danych telemetrycznych w czasie rzeczywistym   + Dostosowanie zarządzania temperaturą i przepływem powietrza w serwerze   + Automatyczna rejestracja certyfikatów (ACE) |  |
| **18.** | **Oprogramowanie do zarządzania** | * Zainstalowane oprogramowanie producenta do zarządzania, spełniającego poniższe wymagania:   + Wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych   + integracja z Active Directory   + Możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta   + Wsparcie dla protokołów SNMP, IPMI, Linux SSH, Redfish   + Możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram   + Szczegółowy opis wykrytych systemów oraz ich komponentów   + Możliwość eksportu raportu do CSV, HTML, XLS, PDF   + Możliwość tworzenia własnych raportów w oparciu o wszystkie informacje zawarte w inwentarzu.   + Grupowanie urządzeń w oparciu o kryteria użytkownika   + Tworzenie automatycznie grup urządzeń w oparciu o dowolny element konfiguracji serwera np. Nazwa, lokalizacja, system operacyjny, obsadzenie slotów PCIe, pozostałego czasu gwarancji   + Możliwość uruchamiania narzędzi zarządzających w poszczególnych urządzeniach   + Szybki podgląd stanu środowiska   + Podsumowanie stanu dla każdego urządzenia   + Szczegółowy status urządzenia / elementu / komponentu   + Generowanie alertów przy zmianie stanu urządzenia.   + Filtry raportów umożliwiające podgląd najważniejszych zdarzeń   + Integracja z service desk producenta dostarczonej platformy sprzętowej   + Możliwość przejęcia zdalnego pulpitu   + Możliwość podmontowania wirtualnego napędu   + Kreator umożliwiający dostosowanie akcji dla wybranych alertów   + Możliwość importu plików MIB   + Przesyłanie alertów „as-is” do innych konsol firm trzecich   + Możliwość definiowania ról administratorów   + Możliwość zdalnej aktualizacji oprogramowania wewnętrznego serwerów   + Aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania)   + Możliwość instalacji oprogramowania wewnętrznego bez potrzeby instalacji agenta   + Możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów   + Moduł raportujący pozwalający na wygenerowanie następujących informacji: nr seryjne sprzętu, konfiguracja poszczególnych urządzeń, wersje oprogramowania wewnętrznego, obsadzenie slotów PCI i gniazd pamięci, informację o maszynach wirtualnych, aktualne informacje o stanie i poziomie gwarancji, adresy IP kart sieciowych, występujących alertów, MAC adresów kart sieciowych, stanie poszczególnych komponentów serwera.   + Możliwość tworzenia sprzętowej konfiguracji bazowej i na jej podstawie weryfikacji środowiska w celu wykrycia rozbieżności.   + Wdrażanie serwerów, rozwiązań modularnych oraz przełączników sieciowych w oparciu o profile   + Możliwość migracji ustawień serwera wraz z wirtualnymi adresami sieciowymi (MAC, WWN, IQN) między urządzeniami.   + Tworzenie gotowych paczek informacji umożliwiających zdiagnozowanie awarii urządzenia przez serwis producenta.   + Zdalne uruchamianie diagnostyki serwera.   + Dedykowana aplikacja na urządzenia mobilne integrująca się z wyżej opisanymi oprogramowaniem zarządzającym.   + Oprogramowanie dostarczane jako wirtualny appliance dla KVM, ESXi i Hyper-V. |  |
| **19.** | **Certyfikaty** | * Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015, ISO-50001 oraz ISO-14001 * Serwer musi posiadać deklaracja CE. * Oferowane produkty muszą zawierać informacje dotyczące ponownego użycia i recyklingu, nie mogą zawierać farb i powłok na dużych plastikowych częściach, których nie da się poddać recyklingowi lub ponownie użyć. Wszystkie produkty zawierające podzespoły elektroniczne oraz niebezpieczne składniki powinny być bezpiecznie i łatwo identyfikowalne oraz usuwalne. Usunięcie materiałów i komponentów powinno odbywać się zgodnie z wymogami Dyrektywy WEEE 2002/96/EC. Produkty muszą składać się z co najmniej w 65% ze składników wielokrotnego użytku/zdatnych do recyklingu. We wszystkich produktach części tworzyw sztucznych większe niż 25-gramowe powinny zawierać nie więcej niż śladowe ilości środków zmniejszających palność sklasyfikowanych w dyrektywie RE 67/548/EEC. Potwierdzeniem spełnienia powyższego wymogu jest wydruk ze strony internetowej [www.epeat.net](http://www.epeat.net) potwierdzający spełnienie normy co najmniej Epeat Silver według normy wprowadzonej w 2019 roku. * Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Microsoft Windows Server 2019, Microsoft Windows Server 2022. |  |
| **20.** | **Dokumentacja użytkownika** | * Zamawiający wymaga dokumentacji w języku polskim lub angielskim. * Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela. |  |
| **21.** | **Gwarancja** | * 5 lat gwarancji producenta serwera w trybie on-site z gwarantowaną skuteczną naprawą miejscu użytkowania sprzętu w ciągu 24 godzin od skutecznego zgłoszenia. Naprawa realizowana przez producenta serwera lub autoryzowany przez producenta serwis. * Funkcja zgłaszania usterek i awarii sprzętowych poprzez automatyczne założenie zgłoszenia w systemie helpdesk/servicedesk producenta sprzętu; * Firma serwisująca musi posiadać ISO 9001:2000 na świadczenie usług serwisowych; * Bezpłatna dostępność poprawek i aktualizacji BIOS/Firmware/sterowników dożywotnio dla oferowanego serwera – jeżeli funkcjonalność ta wymaga dodatkowego serwisu lub licencji producenta serwera, takowy element musi być uwzględniona w ofercie; * Możliwość odpłatnego wydłużenia gwarancji producenta do 7 lat w trybie onsite z gwarantowanym skutecznym zakończeniem naprawy serwera najpóźniej w następnym dniu roboczym od zgłoszenia usterki (podać koszt na dzień składania oferty); * Gwarancja o której mowa nie wyłącza ani nie ogranicza gwarancji udzielanej na Przedmiot Umowy przez Wykonawcę |  |
| **22.** | **Warunki wsparcia technicznego** | * Wykonawca gwarantuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 lub 366 w latach przestępnych następującymi kanałami: telefonicznie, przez Internet oraz z wykorzystaniem aplikacji. * Wykonawca gwarantuje rozpoczęcie diagnostyki telefonicznej / internetowej już w momencie dokonania zgłoszenia. Certyfikowany Technik wykonawcy / producenta z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) ma rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym (NBD) od otrzymania zgłoszenia / zakończenia diagnostyki. Naprawa ma się odbywać w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę. * Wykonawca gwarantuje bezpośredni dostęp do wykwalifikowanej kadry inżynierów technicznych a w przypadku konieczności eskalacji zgłoszenia serwisowego wyznaczonego Kierownika Eskalacji po stronie wykonawcy. * Wykonawca gwarantuje pojedynczy punkt kontaktu dla całego rozwiązania producenta, w tym także sprzedanego oprogramowania. * Zgłoszenie przyjęte jest potwierdzane przez zespół pomocy technicznej (mail/telefon / aplikacja / portal) przez nadanie unikalnego numeru zgłoszenia pozwalającego na identyfikację zgłoszenia w trakcie realizacji naprawy i po jej zakończeniu. * Wykonawca gwarantuje możliwość samodzielnego kwalifikowania poziomu ważności naprawy. * Wykonawca gwarantuje możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji serwera. * Wykonawca gwarantuje nieodpłatne udostępnienie narzędzi serwisowych i procesów wsparcia umożliwiających: Wykrywanie usterek sprzętowych z predykcją awarii. * Automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych. * Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego. * Firma serwisująca musi posiadać ISO 9001:2015 oraz ISO-27001 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta * Wykonawca gwarantuje że serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta.   Możliwość rozszerzenia wsparcia technicznego o:   * Wyznaczonego przez wykonawcę Opiekuna Technicznego Klienta, do którego obowiązków będzie należało:   + Monitorowanie zdarzeń w obrębie infrastruktury   + Zarządzanie eskalacjami i współpraca z kierownikiem eskalacji * Przygotowywanie kwartalnych zaleceń dotyczące konserwacji infrastruktury sprzętowej (BIOS, firmware, patche) * Zdalne lub na miejscu wdrażanie poprawek - 2x w roku * Raportowanie realizacji kontraktów serwisowych i wykorzystania zasobów sprzętowych (na żądanie) |  |
| **23.** | **System operacyjny** | Wraz z dostarczanym urządzeniami należy dostarczyć licencje do Serwerowego Systemu Operacyjnego – SSO. Licencja musi uprawniać do uruchamiania SSO w środowisku fizycznym i nielimitowanej ilości wirtualnych środowisk SSO za pomocą wbudowanych  mechanizmów wirtualizacji. SSO musi posiadać następujące, wbudowane cechy:   1. możliwość wykorzystania, co najmniej 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym, 2. możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności min. 64TB przez każdy wirtualny serwerowy system operacyjny, 3. możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania do 8000 maszyn wirtualnych, 4. możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci, 5. wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy, 6. wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy, 7. automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego, możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy (mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading), 8. wbudowane wsparcie instalacji i pracy na wolumenach, które: 9. pozwalają na zmianę rozmiaru w czasie pracy systemu, 10. umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów, 11. umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów, 12. umożliwiają zdefiniowanie list kontroli dostępu (ACL), 13. wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość, 14. wbudowane szyfrowanie dysków 15. możliwość uruchamiania aplikacji internetowych wykorzystujących technologię ASP.NET, 16. możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów, 17. wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych, 18. graficzny interfejs użytkownika, 19. zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe, 20. wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play), 21. możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu, 22. dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa, 23. możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji: 24. podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC, 25. usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji: 26. podłączenie SSO do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną, 27. ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania, 28. odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza, 29. zdalna dystrybucja oprogramowania na stacje robocze, 30. praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej, 31. centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające: 32. dystrybucję certyfikatów poprzez http, 33. konsolidację CA dla wielu lasów domeny, 34. automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen, 35. szyfrowanie plików i folderów, 36. szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec), 37. możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów, 38. serwis udostępniania stron WWW, 39. wsparcie dla protokołu IP w wersji 6 (IPv6), 40. wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie min. 1000 aktywnych środowisk wirtualnych systemów operacyjnych. Wirtualne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności. Mechanizmy wirtualizacji mają zapewnić wsparcie dla: 41. dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych, 42. obsługi ramek typu jumbo frames dla maszyn wirtualnych, 43. obsługi 4-KB sektorów dysków, 44. nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra, 45. możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API, 46. możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk model), 47. możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta SSO umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet,  w) wsparcie dostępu do zasobu dyskowego SSO poprzez wiele ścieżek (Multipath), 48. możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego, 49. mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty, 50. możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF. |  |

**Pozostałe wymagania Zamawiającego.**

1. Serwerowy system operacyjny musi być dostarczony z licencjami dostępowymi dla użytkowników i urządzeń autoryzowanych w sieci w ilości: 300 sztuk licencji na użytkowników końcowych.
2. Zamawiający wymaga, aby Wykonawca zainstalował w dostarczone urządzenia w serwerowni Zamawiającego i wykonał poniższą konfigurację startową:
3. zainstalowanie, połączenie i uruchomienie dostarczonych urządzeń wraz z dostarczana macierzą
4. w ramach dostawy należy dostarczyć patchcordy pozwalające na redundatne połączenie serwerów z przełącznikiem szkieletowym Zamawiającego – 10Gb SFP+, Zamawiający posiada niezbędne wkładki do przełącznika.
5. konfiguracja klastra HA w ramach dostarczonego środowiska Wirtualnego
6. utworzenie czystych 10 maszyn wirtualnych zgodnie z parametrami wskazanymi przez Zamawiającego na etapie konfiguracji (8 maszyn w ramach dostarczanego środowiska SSO, oraz 2 Linux)
7. **Macierz – 1szt.**

Producent macierzy: …………………………...............................

Model macierzy: ………………………….....................................

Rok produkcji macierzy: ………………………….........................

|  |  |  |  |
| --- | --- | --- | --- |
| **Lp.** | **Nazwa komponentu** | **Opis wymaganych parametrów** | **Parametry oferowane** |
| **1.** | **2.** | **3.** | **4.** |
| **1.** | **Typ:** | Macierz dyskowa Typu RACK (fabrycznie nowy) rok produkcji nie starszy niż 2022 r., |  |
| **2.** | **Obudowa** | Do instalacji w standardowej szafie RACK 19”, macierz musi zajmować maksymalnie 2U i pozwalać na instalacje min. 24 dysków 2.5”. |  |
| **3.** | **Kontrolery** | Dwa kontrolery RAID pracujące w układzie active-active posiadające łącznie minimum osiem portów z przepustowością minimum 12 Gbps SAS  Komunikacja kontrolerów z podłączanymi półkami dyskowymi musi być realizowana przez połączenia SAS o przepustowości minimum 12 Gb/s  Możliwość konfiguracji RAID 1, 5, 6, 10. |  |
| **4.** | **Cache** | Minimum 16GB na kontroler, pamięć cache zapisu mirrorowana między kontrolerami, podtrzymywana bateryjnie przez min. 72h w razie awarii. |  |
| **5.** | **Dyski** | Zainstalowane 13 dysków SSD SAS Mixed Use o pojemności min. 3.2TB.  Zaproponowane rozwiązanie musi wspierać instalację minimum 220 dysków w ramach jednego rozwiązania.  Rozwiązanie musi mieć możliwość rozbudowy do minimum 2.3PB przestrzeni surowej. |  |
| **6.** | **Oprogramowanie/Funkcjonalności** | - Zarządzanie macierzą poprzez minimum przeglądarkę internetową, GUI oparte o HTML5.  - Wbudowany system powiadamiania drogą mailową o awarii.  - Macierz musi umożliwiać utworzenie minimum 512 LUN’ów oraz 1024 kopii migawkowych na całą macierz.  - Wbudowana funkcjonalność automatycznego (bez interwencji człowieka) rozkładania danych między dyskami poszczególnych typów (tzw. auto-tiering). Dane muszą być automatycznie przemieszczane miedzy rożnymi typami dysków.  - Możliwość wykorzystania dysków SSD jako cache macierzy, możliwość rozbudowy pamięci cache do min. 8TB poprzez dyski SSD.  - Rozwiązanie musi wspierać obsługę samoszyfrujących się dysków  Jeżeli którakolwiek z powyższych funkcjonalności wymaga dostarczenia dodatkowej licencji to należy ją zapewnić na całe oferowane rozwiązanie rozumiane w szczególności w zakresie przestrzeni dyskowej |  |
| **7.** | **Wsparcie dla systemów operacyjnych** | Windows Server 2019, Windows Server 2022, Red Hat Enterprise Linux (RHEL), SLES, Vmware ESXi. |  |
| **8.** | **Bezpieczeństwo** | Ciągła praca obu kontrolerów nawet w przypadku zaniku jednej z faz zasilania. Zasilacze, wentylatory, kontrolery RAID redundantne. |  |
| **9.** | **Komponenty dodatkowe** | 6 x kabel Mini-SAS do HD Mini-SAS 12Gb/s o długości min. 2 metry |  |
| **10.** | **Gwarancja** | • 5 lat gwarancji producenta macierzy w trybie on-site z gwarantowaną skuteczną naprawą miejscu użytkowania sprzętu w ciągu 24 godzin od skutecznego zgłoszenia. Naprawa realizowana przez producenta serwera lub autoryzowany przez producenta serwis.  • Funkcja zgłaszania usterek i awarii sprzętowych poprzez automatyczne założenie zgłoszenia w systemie helpdesk/servicedesk producenta sprzętu;  • Firma serwisująca musi posiadać ISO 9001:2000 na świadczenie usług serwisowych;  • Możliwość odpłatnego wydłużenia gwarancji producenta do 7 lat w trybie onsite z gwarantowanym skutecznym zakończeniem naprawy serwera najpóźniej w następnym dniu roboczym od zgłoszenia usterki (podać koszt na dzień składania oferty);  • Gwarancja o której mowa nie wyłącza ani nie ogranicza gwarancji udzielanej na Przedmiot Umowy przez Wykonawcę |  |
| **11.** | **Warunki wsparcia technicznego** | Wykonawca gwarantuje wsparcie realizowane w miejscu instalacji sprzętu, z 4 godzinnym czasem reakcji od przyjęcia zgłoszenia,  Wykonawca gwarantuje możliwość zgłaszania awarii w trybie 24/7/365 lub 366 w latach przestępnych poprzez ogólnopolską linię telefoniczną producenta.  Wykonawca gwarantuje że serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta.  Wykonawca gwarantuje możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia, oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji macierzy.   * Wszystkie naprawy gwarancyjne powinny być możliwe na miejscu. * Dostawca ponosi koszty napraw gwarancyjnych, włączając w to koszt części I transportu. * W czasie obowiązywania gwarancji dostawca zobowiązany jest do udostępnienia Zamawiającemu nowych wersji BIOS, firmware i sterowników (na płytach CD lub stronach internetowych).   Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego. |  |
| **12.** | **Dokumentacja użytkownika** | Zamawiający wymaga dokumentacji w języku polskim lub angielskim |  |
| **13.** | **Certyfikaty** | Macierz musi być wyprodukowany zgodnie z normą ISO 9001:2015. |  |

1. **Serwer Backup – 1szt.**

Producent macierzy: …………………………...............................

Model macierzy: ………………………….....................................

Rok produkcji macierzy: ………………………….........................

|  |  |  |  |
| --- | --- | --- | --- |
| **Lp.** | **Nazwa komponentu** | **Opis wymaganych parametrów** | **Parametry oferowane** |
| **1.** | **2.** | **3.** | **4.** |
| **1.** | **Typ:** | Serwer Backup Typu RACK (fabrycznie nowy) rok produkcji nie starszy niż 2022 r., |  |
| **2.** | **Obudowa** | Obudowa Rack o wysokości max 2U z możliwością instalacji min. 12 dysków 3,5” wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych oraz organizatorem do kabli.  Wyposażona w panel LCD  Obudowa z możliwością wyposażenia w kartę umożliwiającą dostęp bezpośredni poprzez urządzenia mobilne - serwer musi posiadać możliwość konfiguracji oraz monitoringu najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej min. (Android/ Apple iOS) przy użyciu jednego z protokołów BLE/ WIFI. |  |
| **3.** | **Płyta główna** | Płyta główna z możliwością zainstalowania do dwóch procesorów.  Obsługa procesorów 56 rdzeniowych.  Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym.  Płyta główna powinna obsługiwać do 8TB pamięci RAM. |  |
| **4.** | **Chipset** | Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych |  |
| **5.** | **Procesor** | Zainstalowane dwa procesory 8-rdzeniowe klasy x86, o bazowej częstotliwości pracy minimum 2.60 GHz, wyposażone w pamięć podręczną 22,5 MB oraz dedykowane do pracy z zaoferowanym serwerem. |  |
| **6.** | **RAM** | Minimum 64GB DDR5 RDIMM 4800MT/s,  Na płycie głównej powinno znajdować się minimum 32 sloty przeznaczone do instalacji pamięci. |  |
| **7.** | **Funkcjonalność pamięci RAM** | Demand Scrubbing,  Patrol Scrubbing,  Permanent Fault Detection (PFD) |  |
| **8.** | **Gniazda PCI** | Min. 8 slotów PCIe w tym minimum 4 sloty Gen5 |  |
| **9.** | **Interfejsy sieciowe/FC/SAS** | Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT oraz  4 interfejsy sieciowe 25Gb Ethernet w standardzie SFP28, wyposażone we wkładki SFP+ SR 10Gbe. Wkładki muszą być przetestowane przez producenta oferowanego serwera i znajdować się na liście wkładek rekomendowanych do użycia z oferowanym typem serwera - Wykonawca złoży dokument potwierdzający spełnianie wymogu. |  |
| **10.** | **Dyski twarde** | Zainstalowane min. 7 dysków 12TB 7.2K RPM NLSAS 12Gbps 512e 3.5“ Hot-Plug.  Zainstalowana karta wyposażona w dwa dyski M.2 SSD 480GB skonfigurowane w RAID1  Możliwość zainstalowania dwóch dysków M.2 NVMe SSDs o pojemności min. 960GB Hot-Plug z możliwością konfiguracji RAID 1. |  |
| **11.** | **Kontroler RAID** | Sprzętowy kontroler dyskowy, posiadający  Min. 8GB nieulotnej pamięci cache,  Możliwość konfiguracji poziomów RAID: 0, 1, 5, 6, 10, 50, 60. |  |
| **12.** | **Wbudowane porty** | 4x USB, w tym min. 1 porty USB 3.0  Min. 1x VGA z czego jeden na panelu przednim, możliwość instalacji drugiego portu z tyłu obudowy.  Możliwość rozbudowy o Serial Port |  |
| **13.** | **Video** | Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1280x1024 |  |
| **14.** | **Wentylatory** | Redundantne, Hot-Plug |  |
| **15.** | **Zasilacze** | Redundantne, Hot-Plug min. 1100W każdy.  Dołączone dwa kable zasilające z końcówkami odpowiednimi do posiadanych przez urządzenie gniazd zasilania oraz z końcówkami do listwy PDU, umożlwiające zasilanie z sieci 230V. |  |
| **16.** | **Bezpieczeństwo** | * Zatrzask górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych. * Możliwość wyłączenia w BIOS funkcji przycisku zasilania. * BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła * Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą. * Moduł TPM 2.0 * Możliwość dynamicznego włączania I wyłączania portów USB na obudowie – bez potrzeby restartu serwera   Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem |  |
| **17.** | **Karta Zarządzania** | Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca:   * + zdalny dostęp do graficznego interfejsu Web karty zarządzającej;   + zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera);   + szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika;   + możliwość podmontowania zdalnych wirtualnych napędów;   + wirtualną konsolę z dostępem do myszy, klawiatury;   + wsparcie dla IPv6;   + wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish;   + możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer;   + możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer;   + integracja z Active Directory;   + możliwość obsługi przez dwóch administratorów jednocześnie;   + wsparcie dla dynamic DNS;   + wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej.   + możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera   + możliwość zarządzania do 100 serwerów bezpośrednio z konsoli karty zarządzającej pojedynczego serwera   + oraz z możliwością rozszerzenia funkcjonalności o:   + Wirtualny schowek ułatwiający korzystanie z konsoli zdalnej   + Przesyłanie danych telemetrycznych w czasie rzeczywistym   + Dostosowanie zarządzania temperaturą i przepływem powietrza w serwerze   + Automatyczna rejestracja certyfikatów (ACE) |  |
| **18.** | **Oprogramowanie do zarządzania** | Zainstalowane oprogramowanie producenta do zarządzania, spełniającego poniższe wymagania:   * + Wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych   + integracja z Active Directory   + Możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta   + Wsparcie dla protokołów SNMP, IPMI, Linux SSH, Redfish   + Możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram   + Szczegółowy opis wykrytych systemów oraz ich komponentów   + Możliwość eksportu raportu do CSV, HTML, XLS, PDF   + Możliwość tworzenia własnych raportów w oparciu o wszystkie informacje zawarte w inwentarzu.   + Grupowanie urządzeń w oparciu o kryteria użytkownika   + Tworzenie automatycznie grup urządzeń w oparciu o dowolny element konfiguracji serwera np. Nazwa, lokalizacja, system operacyjny, obsadzenie slotów PCIe, pozostałego czasu gwarancji   + Możliwość uruchamiania narzędzi zarządzających w poszczególnych urządzeniach   + Szybki podgląd stanu środowiska   + Podsumowanie stanu dla każdego urządzenia   + Szczegółowy status urządzenia/elementu/komponentu   + Generowanie alertów przy zmianie stanu urządzenia.   + Filtry raportów umożliwiające podgląd najważniejszych zdarzeń   + Integracja z service desk producenta dostarczonej platformy sprzętowej   + Możliwość przejęcia zdalnego pulpitu   + Możliwość podmontowania wirtualnego napędu   + Kreator umożliwiający dostosowanie akcji dla wybranych alertów   + Możliwość importu plików MIB   + Przesyłanie alertów „as-is” do innych konsol firm trzecich   + Możliwość definiowania ról administratorów   + Możliwość zdalnej aktualizacji oprogramowania wewnętrznego serwerów   + Aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania)   + Możliwość instalacji oprogramowania wewnętrznego bez potrzeby instalacji agenta   + Możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów   + Moduł raportujący pozwalający na wygenerowanie następujących informacji: nr seryjne sprzętu, konfiguracja poszczególnych urządzeń, wersje oprogramowania wewnętrznego, obsadzenie slotów PCI i gniazd pamięci, informację o maszynach wirtualnych, aktualne informacje o stanie i poziomie gwarancji, adresy IP kart sieciowych, występujących alertów, MAC adresów kart sieciowych, stanie poszczególnych komponentów serwera.   + Możliwość tworzenia sprzętowej konfiguracji bazowej i na jej podstawie weryfikacji środowiska w celu wykrycia rozbieżności.   + Wdrażanie serwerów, rozwiązań modularnych oraz przełączników sieciowych w oparciu o profile   + Możliwość migracji ustawień serwera wraz z wirtualnymi adresami sieciowymi (MAC, WWN, IQN) między urządzeniami.   + Tworzenie gotowych paczek informacji umożliwiających zdiagnozowanie awarii urządzenia przez serwis producenta.   + Zdalne uruchamianie diagnostyki serwera.   + Dedykowana aplikacja na urządzenia mobilne integrująca się z wyżej opisanymi oprogramowaniem zarządzającym.   + Oprogramowanie dostarczane jako wirtualny appliance dla KVM, ESXi i Hyper-V. |  |
| **19.** | **Certyfikaty** | * Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015, ISO-50001 oraz ISO-14001 * Serwer musi posiadać deklaracja CE. * Oferowane produkty muszą zawierać informacje dotyczące ponownego użycia i recyklingu, nie mogą zawierać farb i powłok na dużych plastikowych częściach, których nie da się poddać recyklingowi lub ponownie użyć. Wszystkie produkty zawierające podzespoły elektroniczne oraz niebezpieczne składniki powinny być bezpiecznie i łatwo identyfikowalne oraz usuwalne. Usunięcie materiałów i komponentów powinno odbywać się zgodnie z wymogami Dyrektywy WEEE 2002/96/EC. Produkty muszą składać się z co najmniej w 65% ze składników wielokrotnego użytku/zdatnych do recyklingu. We wszystkich produktach części tworzyw sztucznych większe niż 25-gramowe powinny zawierać nie więcej niż śladowe ilości środków zmniejszających palność sklasyfikowanych w dyrektywie RE 67/548/EEC. Potwierdzeniem spełnienia powyższego wymogu jest wydruk ze strony internetowej [www.epeat.net](http://www.epeat.net) potwierdzający spełnienie normy co najmniej Epeat Silver według normy wprowadzonej w 2019 roku * Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Microsoft Windows Server 2019, Microsoft Windows Server 2022. |  |
| **20.** | **Dokumentacja użytkownika** | * Zamawiający wymaga dokumentacji w języku polskim lub angi*e*lskim. * Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela. |  |
| **21.** | **Gwarancja** | * 5 lat gwarancji producenta serwera w trybie on-site z gwarantowaną skuteczną naprawą miejscu użytkowania sprzętu w ciągu 24 godzin od skutecznego zgłoszenia. Naprawa realizowana przez producenta serwera lub autoryzowany przez producenta serwis. * Funkcja zgłaszania usterek i awarii sprzętowych poprzez automatyczne założenie zgłoszenia w systemie helpdesk/servicedesk producenta sprzętu; * Firma serwisująca musi posiadać ISO 9001:2000 na świadczenie usług serwisowych; * Bezpłatna dostępność poprawek i aktualizacji BIOS/Firmware/sterowników dożywotnio dla oferowanego serwera – jeżeli funkcjonalność ta wymaga dodatkowego serwisu lub licencji producenta serwera, takowy element musi być uwzględniona w ofercie; * Możliwość odpłatnego wydłużenia gwarancji producenta do 7 lat w trybie onsite z gwarantowanym skutecznym zakończeniem naprawy serwera najpóźniej w następnym dniu roboczym od zgłoszenia usterki (podać koszt na dzień składania oferty); * Gwarancja o której mowa nie wyłącza ani nie ogranicza gwarancji udzielanej na Przedmiot Umowy przez Wykonawcę |  |
| **22.** | **Warunki wsparcia technicznego** | * Wykonawca gwarantuje możliwość zgłaszania zdarzeń serwisowych w trybie 24/7/365 lub 366 w latach przestępnych następującymi kanałami: telefonicznie, przez Internet oraz z wykorzystaniem aplikacji. * Wykonawca gwarantuje rozpoczęcie diagnostyki telefonicznej / internetowej już w momencie dokonania zgłoszenia. Certyfikowany Technik wykonawcy / producenta z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) ma rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym (NBD) od otrzymania zgłoszenia / zakończenia diagnostyki. Naprawa ma się odbywać w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę. * Wykonawca gwarantuje bezpośredni dostęp do wykwalifikowanej kadry inżynierów technicznych a w przypadku konieczności eskalacji zgłoszenia serwisowego wyznaczonego Kierownika Eskalacji po stronie wykonawcy. * Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania producenta, w tym także sprzedanego oprogramowania. * Zgłoszenie przyjęte jest potwierdzane przez zespół pomocy technicznej (mail/telefon / aplikacja / portal) przez nadanie unikalnego numeru zgłoszenia pozwalającego na identyfikację zgłoszenia w trakcie realizacji naprawy i po jej zakończeniu. * Wykonawca gwarantuje możliwość samodzielnego kwalifikowania poziomu ważności naprawy. * Wykonawca gwarantuje możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji serwera. * Wykonawca gwarantuje nieodpłatne udostępnienia narzędzi serwisowych i procesów wsparcia umożliwiających: Wykrywanie usterek sprzętowych z predykcją awarii. * Automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych. * Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego. * Firma serwisująca musi posiadać ISO 9001:2015 oraz ISO-27001 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń. * Wykonawca gwarantuje że serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta.   Możliwość rozszerzenia gwarancji o:   * Wyznaczonego przez wykonawcę Opiekuna Technicznego Klienta, do którego obowiązków będzie należało:   + Monitorowanie zdarzeń w obrębie infrastruktury   + Zarządzanie eskalacjami i współpraca z kierownikiem eskalacji * Przygotowywanie kwartalnych zaleceń dotyczące konserwacji infrastruktury sprzętowej (BIOS, firmware, patche) * Zdalne lub na miejscu wdrażanie poprawek - 2x w roku * Raportowanie realizacji kontraktów serwisowych i wykorzystania zasobów sprzętowych (na żądanie) |  |
| **23.** | **System operacyjny** | Wraz z dostarczanym urządzeniami należy dostarczyć licencje do Serwerowego Systemu Operacyjnego – SSO. Licencja musi uprawniać do uruchamiania SSO w środowisku fizycznym i dwóch wirtualnych środowisk SSO za pomocą wbudowanych mechanizmów wirtualizacji. SSO musi posiadać następujące, wbudowane cechy:   1. możliwość wykorzystania, co najmniej 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym, 2. możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności min. 64TB przez każdy wirtualny serwerowy system operacyjny, 3. możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania do 8000 maszyn wirtualnych, 4. możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci, 5. wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy, 6. wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy, 7. automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego, możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy (mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading), 8. wbudowane wsparcie instalacji i pracy na wolumenach, które: 9. pozwalają na zmianę rozmiaru w czasie pracy systemu, 10. umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów, 11. umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów, 12. umożliwiają zdefiniowanie list kontroli dostępu (ACL), 13. wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość, 14. wbudowane szyfrowanie dysków 15. możliwość uruchamiania aplikacji internetowych wykorzystujących technologię ASP.NET, 16. możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów, 17. wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych, 18. graficzny interfejs użytkownika, 19. zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe, 20. wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play), 21. możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu, 22. dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa, 23. możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji: 24. podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC, 25. usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji: 26. podłączenie SSO do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną, 27. ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania, 28. odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza, 29. zdalna dystrybucja oprogramowania na stacje robocze, 30. praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej, 31. centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające: 32. dystrybucję certyfikatów poprzez http, 33. konsolidację CA dla wielu lasów domeny, 34. automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen, 35. szyfrowanie plików i folderów, 36. szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec), 37. możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów, 38. serwis udostępniania stron WWW, 39. wsparcie dla protokołu IP w wersji 6 (IPv6), 40. wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie min. 1000 aktywnych środowisk wirtualnych systemów operacyjnych. Wirtualne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności. Mechanizmy wirtualizacji mają zapewnić wsparcie dla: 41. dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych, 42. obsługi ramek typu jumbo frames dla maszyn wirtualnych, 43. obsługi 4-KB sektorów dysków, 44. nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra, 45. możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API, 46. możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk model), 47. możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta SSO umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet, 48. wsparcie dostępu do zasobu dyskowego SSO poprzez wiele ścieżek (Multipath), 49. możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego, 50. mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty, 51. możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF. |  |

**Pozostałe wymagania Zamawiającego.**

1. Zamawiający wymaga, aby Wykonawca zainstalował w dostarczone urządzenie w serwerowni Zamawiającego i wykonał poniższą konfigurację startową:
2. zainstalowanie, połączenie i uruchomienie dostarczonego urządzenia do współpracy z dostarczanym klastrem serwerów i macierzą
3. w ramach dostawy należy dostarczyć patchcordy pozwalające na redundatne połączenie serwera z przełącznikiem szkieletowym Zamawiającego – 10Gb SFP+, Zamawiający posiada niezbędne wkładki do przełącznika.
4. **Oprogramowanie wirtualizacyjne:**

Producent oprogramowania: …………………………...............................

Wersja oprogramowania: ………………………….....................................

1. Zaoferowane oprogramowanie do wirtualizacji musi być instalowane bezpośrednio na sprzęcie fizycznym i nie może być ono częścią innego systemu operacyjnego
2. W zaoferowanym oprogramowaniu warstwa wirtualizacji nie może dla własnych celów alokować więcej niż 200MB pamięci operacyjnej RAM serwera fizycznego
3. Zaoferowane oprogramowanie do wirtualizacji zainstalowane na serwerze fizycznym musi potrafić obsłużyć i wykorzystać procesory fizyczne tego serwera wyposażone w 768 logicznych wątków, 24TB pamięci fizycznej RAM tego serwera oraz 16 procesorów fizycznych tego serwera
4. Zaoferowane oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych z ilością od 1 do 768 procesorów wirtualnych
5. Zaoferowane oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych z możliwością przydzielenia do 24 TB pamięci operacyjnej RAM
6. Zaoferowane oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych z możliwością przydzielenia od 1 do 10 wirtualnych kart sieciowych dla każdej z nich. Dodatkowo, oprogramowanie musi posiadać możliwość utworzenia maszyny wirtualnej bez przydzielonej wirtualnej karty sieciowej.
7. Zaoferowane oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych, z których każda może mieć 32 porty szeregowe, 3 porty równoległe i 20 urządzeń USB
8. Zaoferowane oprogramowanie musi wspierać następujące systemy operacyjne: Windows XP, Windows Vista, Windows 2000, Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows Server 2016, Windows Server 2019, Windows 2022, Windows 7, Windows 8, SLES 12, SLES 11, SLES 10, SLES 9, RHEL 8, REHL 7, RHEL 6, RHEL 5, RHEL 4, RHEL 3, RHEL Atomic 7, Solaris 11, Solaris 10, Debian, CentOS, FreeBSD, Asianux, Ubuntu, SCO OpenServer, SCO Unixware, Mac OS X, Photon OS, eCommStation 1/2/2.1, Oracle Linux , CoreOS, NeoKylin, Amazon Linux 2,
9. W celu osiągnięcia maksymalnego współczynnika konsolidacji, zaoferowane oprogramowanie musi umożliwiać przydzielenie łącznie większej ilości pamięci RAM dla maszyn wirtualnych niż fizyczne zasoby RAM serwera, na którym maszyny te są posadowione
10. Rozwiązanie musi umożliwiać udostępnienie maszynie wirtualnej większej ilości zasobów dyskowych niż jest fizycznie dostępne na zasobach dyskowych
11. Zaoferowane oprogramowanie musi zapewniać sprzętowe wsparcie dla wirtualizacji zagnieżdżonej, w szczególności w zakresie możliwości zastosowania trybu XP mode w Microsoft Windows 7 a także instalacji wszystkich funkcjonalności w tym Microsoft Hyper-V pakietu Microsoft Windows Server 2012 na maszynie wirtualnej
12. Zaoferowane oprogramowanie musi umożliwiać integrację z rozwiązaniami antywirusowymi firm trzecich w zakresie skanowania maszyn wirtualnych z poziomu warstwy wirtualizacji bez ingerencji w systemy operacyjne maszyn wirtualnych (bezagentowość)
13. Zaoferowane oprogramowanie 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”
14. Zaoferowane oprogramowanie do wirtualizacji musi zapewnić możliwość powielania maszyn wirtualnych wraz z ich pełną konfiguracją i danymi
15. Zaoferowane oprogramowanie do wirtualizacji musi zapewnić możliwość wykonywania kopii migawkowych instancji systemów operacyjnych na potrzeby tworzenia kopii zapasowych bez przerywania ich pracy z możliwością konieczności zachowania stanu pamięci pracującej maszyny wirtualnej.
16. Konsola zarządzająca zaoferowanego oprogramowania musi posiadać możliwość przydzielania i konfiguracji uprawnień z możliwością integracji z usługami katalogowymi, minimalnie z: Microsoft Active Directory i Open LDAP oraz umożliwiać federacyjne zarządzanie tożsamością w oparciu o Microsoft Active Directory Federation Services (ADFS).
17. Zaoferowane oprogramowanie musi zapewniać możliwość dodawania zasobów w czasie pracy maszyny wirtualnej, w szczególności w zakresie ilości procesorów, pamięci operacyjnej i przestrzeni dyskowej
18. Zaoferowane oprogramowanie musi posiadać funkcjonalność tworzenia wirtualnego przełącznika (virtual switch) umożliwiającego tworzenie sieci wirtualnej w obszarze hosta (hypervisora wirtualizacyjnego) i pozwalającego połączyć tym przełącznikiem maszyny wirtualne w obszarze jednego hosta, a także na zewnątrz sieci fizycznej. Pojedynczy przełącznik wirtualny powinien mieć możliwość konfiguracji minimum 4000 portów
19. Pojedynczy wirtualny przełącznik w zaoferowanym oprogramowaniu, w celu zapewnienia bezpieczeństwa połączenia ethernetowego w razie awarii fizycznej karty sieciowej, musi posiadać możliwość przyłączania do niego minimum dwóch fizycznych kart sieciowych
20. Wirtualne przełączniki w zaoferowane oprogramowaniu muszą posiadać funkcjonalność obsługi wirtualnych sieci lokalnych (VLAN)
21. Zaoferowane oprogramowanie musi zapewniać możliwość konfigurowania polityk separacji sieci w warstwie trzeciej, tak aby zapewnić oddzielne grupy wzajemnej komunikacji pomiędzy maszynami wirtualnymi
22. Zaoferowane oprogramowanie musi umożliwiać wykorzystanie technologii przepustowości sieci komputerowych do 200GbE w tym agregację połączeń fizycznych do minimalizacji czasu przenoszenia maszyny wirtualnej pomiędzy serwerami fizycznymi
23. Zaoferowane oprogramowanie do wirtualizacji musi obsługiwać przełączenie ścieżek LAN (bez utraty komunikacji) w przypadku awarii jednej ze ścieżek
24. Zaoferowane oprogramowanie musi zapewnić możliwość zdefiniowania alertów informujących o przekroczeniu wartości progowych
25. Zaoferowane oprogramowanie, w przypadku działania pod zarządcą klastra VMware vCenter, musi zapewniać możliwość replikacji maszyn wirtualnych z dowolnej pamięci masowej w tym z dysków wewnętrznych serwerów fizycznych na dowolną pamięć masową w tym samym lub oddalonym ośrodku przetwarzania. Replikacja musi gwarantować współczynnik RPO (ang Recovery Point Objective) na poziomie minimum 5 minut
26. Zaoferowane oprogramowanie do wirtualizacji musi obsługiwać przełączenie ścieżek SAN (bez utraty komunikacji) w przypadku awarii jednej ze ścieżek
27. Zaoferowane oprogramowanie, w przypadku działania pod zarządcą klastra VMware vCenter, musi mieć możliwość przenoszenia maszyn wirtualnych pomiędzy serwerami fizycznymi bez przerywania pracy usług na przenoszonych maszynach wirtualnych. Wymaga się wsparcia natywnego szyfrowania ruchu sieciowego dla maszyn wirtualnych podczas ich przenoszenia między serwerami fizycznymi
28. Zaoferowane oprogramowanie, w przypadku działania pod zarządcą klastra VMware vCenter, oraz w środowisku z więcej niż pojedynczym wirtualizatorem, musi umożliwiać automatyczne, ponowne uruchomienie maszyn wirtualnych w przypadku awarii jednego z wirtualizatorów na kolejnym, działającym w tym samym klastrze wirtualizatorze (funkcjonalność HA) (ang. high availability)
29. Zaoferowane oprogramowanie musi posiadać co najmniej 2 niezależne mechanizmy wzajemnej komunikacji między serwerami z zainstalowanym wirtualizatorem oraz z serwerem zarządzającym, gwarantujące właściwe działanie mechanizmów wysokiej dostępności na wypadek izolacji sieciowej serwerów fizycznych lub partycjonowania sieci
30. Zaoferowane oprogramowanie do wirtualizacji musi zapewniać możliwość stworzenia dysku maszyny wirtualnej o wielkości 62 TB
31. Zaoferowane oprogramowanie musi posiadać wbudowany interfejs programistyczny (API) zapewniający pełną integrację zewnętrznych rozwiązań wykonywania kopii zapasowych z istniejącymi mechanizmami warstwy wirtualizacyjnej
32. Zaoferowane oprogramowanie musi wspierać TPM 2.0. Minimalne wymaganie Zamawiającego dla TPM oznacza, że TPM zapewnia mechanizm gwarantujący, że serwer fizyczny, na którym zainstalowane jest zaoferowane oprogramowanie, uruchomił się z włączoną opcją Secure Boot. Po potwierdzeniu, że Secure Boot jest włączone, system gwarantuje, poprzez weryfikację podpisu cyfrowego, że hypervisor uruchomił się w niezmienionej formie
33. Wirtualizator w zaoferowanym oprogramowaniu musi mieć możliwość włączenia funkcji “Microsoft virtualization-based security”, tzw. Microsoft VBS dla systemów operacyjnych maszyn wirtualnych opartych o system operacyjny Microsoft Windows 10 oraz Microsoft Windows Server 2016.
34. Zaoferowane oprogramowanie musi posiadać certyfikację FIPS-140-2 min. dla modułu jądra wirtualizatora odpowiedzialnego za szyfrowanie danych
35. Zaoferowane oprogramowanie musi posiadać funkcjonalność wirtualnego TPM 2.0 dla maszyn wirtualnych z zainstalowanym Microsoft Windows 10 oraz Microsoft Windows 2016. Zamawiający wymaga, aby z punktu widzenia maszyny wirtualnej z systemem operacyjnym Microsoft Windows 10 lub Microsoft Windows 2016 wirtualny TPM widziany był jako standardowy TPM, gdzie można przechowywać bezpiecznie wrażliwe dane np. certyfikaty. Zawartość wirtualnego TPM musi być przechowywana w pliku przynależnym do maszyny wirtualnej oraz musi być szyfrowana.
36. Zaoferowane oprogramowanie musi posiadać funkcjonalność szybkiego uruchamiania wirtualizatora po przeprowadzonym procesie jego aktualizacji. Zamawiający wymaga aby w procesie aktualizacji wirtualizatora, jeśli wymagany jest jego restart, funkcjonalność szybkiego uruchamiania powodowała eliminację czasochłonnej fazy inicjalizacji serwera fizycznego
37. Zaoferowane oprogramowanie musi posiadać możliwość aktualizacji i kontroli wersji oprogramowania do wirtualizacji w ramach klastra serwerów z poziomu centralnej konsoli zarządzającej. Dodatkowo centralna konsola zarządzająca musi posiadać funkcjonalność aktualizacji firmware komponentów serwera fizycznego (dyski, kontrolery, karty sieciowe) z poziomu konsoli zarządzającej wirtualizatora. Konsola zarządzająca musi mieć możliwość automatycznej weryfikacji, czy zainstalowane komponenty serwera posiadają rekomendowaną wersję sterowników i firmware, eliminując ryzyko pracy na nieaktualnych wersjach. Taka funkcjonalność powinna być dostępna dla minimum dwóch producentów serwerów obecnych na rynku
38. Zaoferowane oprogramowanie musi wspierać protokół precyzyjnej synchronizacji czasu PTP (ang. Precision Time Protocol)
39. Zaoferowane oprogramowanie, w przypadku działania pod zarządcą klastra VMware vCenter, musi posiadać mechanizm, który ogranicza dostęp do indywidualnego zarządzania warstwą wirtualizacji na serwerach fizycznych w ramach klastra serwerów w celu utwardzenia/hardening (maksymalnego zwiększenia bezpieczeństwa dostępu) systemu wirtualizacji.
40. Zaoferowane oprogramowanie zapewnia podstawowe funkcje serwera zarządzania kluczami (KMS), które upraszcza włączenie szyfrowania i zaawansowanych funkcji bezpieczeństwa.

Wszystkie licencje powinny być dostarczone wraz z 5 letnim wsparciem. Wsparcie powinno umożliwiać zgłaszanie problemów 7 dni w tygodniu przez 24 godziny.

W ramach usługi wsparcia technicznego dla Oprogramowania, w ramach uiszczonego przez Zamawiającego na rzecz Wykonawcy wynagrodzenia, Zamawiającemu przysługiwać będzie przez okres co najmniej 5 lat:

* prawo do korzystania, bez jakichkolwiek dodatkowych opłat do wydawanych przez producenta Oprogramowania najnowszych jego wersji, poprawek do Oprogramowania oraz aktualizacji Oprogramowania,
* dostęp elektroniczny (np. przez stronę Web) do aktualizacji Oprogramowania, oraz poprawek do Oprogramowania,

1. **Oprogramowanie do backupu:**

Producent oprogramowania: …………………………...............................

Wersja oprogramowania: ………………………….....................................

1. **Wymagania ogólne**
2. Oprogramowanie musi być produktem przeznaczonym do obsługi środowisk DataCenter. Oferowany produkt musi znajdować się w kwadracie liderów Gartner Magic Quadrant for Data Center Backup and Recovery Solutions oraz na ogólnie dostępnej liście referencyjnej Gartner: https://www.gartner.com/reviews/market/data-center-backup-and-recovery-solutions i spełniać minimalne wymaganie : - minimalna liczba referencji 150, - minimalna ocena z referencji 4,5,
3. Oprogramowanie musi współpracować z infrastrukturą VMware w wersji 6.x, 7.x i 8.0 oraz Microsoft Hyper-V 2012, 2012R2, 2016, 2019 i 2022. Wszystkie funkcjonalności w specyfikacji muszą być dostępne na wszystkich wspieranych platformach wirtualizacyjnych, chyba, że wyszczególniono inaczej
4. Oprogramowanie musi zapewniać tworzenie kopii zapasowych z sieciowych urządzeń plikowych NAS opartych o SMB, CIFS i/lub NFS oraz bezpośrednio z serwerów plikowych opartych o Windows i Linux.
5. **Całkowite koszty posiadania**
6. Oprogramowanie musi być niezależne sprzętowo i umożliwiać wykorzystanie dowolnej platformy serwerowej i dyskowej
7. Oprogramowanie musi tworzyć “samowystarczalne” archiwa do odzyskania których nie wymagana jest osobna baza danych z metadanymi deduplikowanych bloków
8. Oprogramowanie musi mieć mechanizmy deduplikacji i kompresji w celu zmniejszenia wielkości archiwów. Włączenie tych mechanizmów nie może skutkować utratą jakichkolwiek funkcjonalności wymienionych w tej specyfikacji
9. Oprogramowanie nie może przechowywać danych o deduplikacji w centralnej bazie. Utrata bazy danych używanej przez oprogramowanie nie może prowadzić do utraty możliwości odtworzenia backupu. Metadane deduplikacji muszą być przechowywane w plikach backupu.
10. Oprogramowanie musi zapewniać warstwę abstrakcji nad poszczególnymi urządzeniami pamięci masowej, pozwalając utworzyć jedną wirtualną pulę pamięci na kopie zapasowe. Wymagane jest wsparcie dla nieograniczonej liczby pamięci masowych to takiej puli.
11. Oprogramowanie musi pozwalać na tworzenie repozytorium kopii zapasowych bezpośrednio na zasobach Microsoft Azure Blob, Google Cloud Storage, Amazon S3, Wasabi Cloud Storage oraz na innych kompatybilnych z S3 przestrzeniach obiektowych. Dodatkowo, oprogramowanie musi wspierać archiwizowanie tych danych do Microsoft Azure Archive Blob Storage oraz Amazon S3 Glacier.
12. Oprogramowanie musi wspierać niezmienność kopii zapasowych na potrzeby ochrony przed ransomware poprzez niedopuszczenie do usunięcia lub modyfikacji kopii zapasowej w zadanym okresie czasu.
13. Oprogramowanie nie może instalować żadnych stałych agentów wymagających wdrożenia czy upgradowania wewnątrz maszyny wirtualnej dla jakichkolwiek funkcjonalności backupu lub odtwarzania
14. Oprogramowanie musi oferować portal samoobsługowy, umożliwiający odtwarzanie użytkownikom wirtualnych maszyn, obiektów MS Exchange i baz danych MS SQL, Oracle oraz PostgreSQL (w tym odtwarzanie point-in-time)
15. Oprogramowanie musi zapewniać możliwość delegacji uprawnień do odtwarzania na portalu
16. Oprogramowanie musi mieć możliwość integracji z innymi systemami poprzez wbudowane RESTful API
17. Oprogramowanie musi mieć wbudowane mechanizmy backupu konfiguracji w celu prostego odtworzenia systemu po całkowitej reinstalacji
18. Oprogramowanie musi mieć wbudowane mechanizmy szyfrowania zarówno plików z backupami jak i transmisji sieciowej. Włączenie szyfrowania nie może skutkować utratą jakiejkolwiek funkcjonalności wymienionej w tej specyfikacji
19. Oprogramowanie musi posiadać mechanizmy chroniące przed utratą hasła szyfrowania
20. Oprogramowanie musi posiadać architekturę klient/serwer z możliwością instalacji wielu instancji konsoli administracyjnych.
21. Oprogramowanie musi posiadać natywne mechanizmy uwierzytelniania wieloskładnikowego (MFA) w celu dostępu do konsoli administracyjnej
22. **Wymagania RPO**
23. Oprogramowanie musi wykorzystywać mechanizmy Change Block Tracking na wszystkich wspieranych platformach wirtualizacyjnych. Mechanizmy muszą być certyfikowane przez dostawcę platformy wirtualizacyjnej
24. Oprogramowanie musi wykorzystywać mechanizmy śledzenia zmienionych plików przy zabezpieczaniu udziałów plikowych.
25. Oprogramowanie musi oferować możliwość sterowania obciążeniem storage'u produkcyjnego tak aby nie przekraczane były skonfigurowane przez administratora backupu poziomy latencji. Funkcjonalność ta musi być dostępna na wszystkich wspieranych platformach wirtualizacyjnych z dokładnością do pojedynczego datastoru
26. Oprogramowanie musi zapewniać tworzenie kopii zapasowych z bezpośrednim wykorzystaniem snapshotów macierzowych. Musi też zapewniać odtwarzanie maszyn wirtualnych z takich snapshotów. Proces wykonania kopii zapasowej nie może wymagać użycia jakichkolwiek hostów tymczasowych. Opisana funkcjonalność powinna działać w środowisku VMware.
27. Oprogramowanie musi posiadać wsparcie dla VMware vSAN potwierdzone odpowiednią certyfikacją VMware.
28. Oprogramowanie musi wspierać kopiowanie backupów oraz zasobów plikowych na taśmy.
29. Oprogramowanie musi mieć możliwość tworzenia retencji GFS (Grandfather-Father-Son)
30. Oprogramowanie musi wspierać bezpośrednią integrację z urządzeniami deduplikacyjnymi. Minimalnie wsparcie wymagane dla Dell DataDomain, HPE StoreOnce, ExaGrid, Fujitsu CS800, Quantum DXi oraz Infinidat InfiniGuard.
31. Oprogramowanie musi wspierać BlockClone API w przypadku użycia Windows Server 2016, 2019 lub 2022 z systemem pliku ReFS jako repozytorium backupu. Podobna funkcjonalność musi być zapewniona dla repozytoriów opartych o linuxowy system plików XFS.
32. Oprogramowanie musi mieć możliwość kopiowania backupów oraz replikacji wirtualnych maszyn z wykorzystaniem wbudowanej akceleracji WAN.
33. Oprogramowanie musi mieć możliwość replikacji asynchronicznej włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere pomiędzy hostami ESXi oraz pomiędzy hostami Hyper-V. Dodatkowo oprogramowanie musi mieć możliwość użycia plików kopii zapasowych jako źródła replikacji.
34. Oprogramowanie musi mieć możliwość replikacji ciągłej, opartej o VMware VAIO, włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere. Dla replikacji ciągłej musi być możliwość zdefiniowania dziennika pozwalającego na odzyskanie danych z dowolnego punku w ramach ustalonego parametru RPO.
35. Oprogramowanie musi umożliwiać przechowywanie punktów przywracania dla replik
36. Oprogramowanie musi umożliwiać wykorzystanie istniejących w infrastrukturze wirtualnych maszyn jako źródła do dalszej replikacji (replica seeding)
37. Oprogramowanie musi wykorzystywać wszystkie oferowane przez hypervisor tryby transportu (sieć, hot-add, LAN Free-SAN)
38. **Wymagania RTO**
39. Oprogramowanie musi umożliwiać jednoczesne uruchomienie wielu maszyn wirtualnych bezpośrednio ze zdeduplikowanego i skompresowanego pliku backupu, z dowolnego punktu przywracania, bez potrzeby kopiowania jej na storage produkcyjny. Funkcjonalność musi być oferowana dla środowisk VMware, Hyper-V oraz Nutanix AHV niezależnie od rodzaju storage’u użytego do przechowywania kopii zapasowych.
40. Dodatkowo dla środowiska vSphere, Hyper-V i Nutanix AHV powyższa funkcjonalność powinna umożliwiać uruchomianie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna)
41. Oprogramowanie musi pozwalać na migrację on-line tak uruchomionych maszyn na storage produkcyjny. Migracja powinna odbywać się mechanizmami wbudowanymi w hypervisor. Jeżeli licencja na hypervisor nie posiada takich funkcjonalności - oprogramowanie musi realizować taką migrację swoimi mechanizmami
42. Oprogramowanie musi pozwalać na zaprezentowanie pojedynczego dysku bezpośrednio z kopii zapasowej do wybranej działającej maszyny wirtualnej vSpehre
43. Oprogramowanie musi pozwalać na uruchomienie zasobów plikowych SMB oraz baz danych MS SQL i Oracle bezpośrednio ze skompresowanego i skompresowanego pliku backupu. Dodatkowo wspierana musi być migracja on-line tak uruchomionych zasobów na środowisko produkcyjne.
44. Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny, plików konfiguracji i dysków
45. Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny bezpośrednio do Microsoft Azure, Microsoft Azure Stack, Amazon EC2 oraz Google Cloud Platform.
46. Oprogramowanie musi umożliwić odtworzenie plików/folderów lub ich uprawnień na maszynę operatora, lub na serwer produkcyjny bez potrzeby użycia agenta instalowanego wewnątrz wirtualnej maszyny. Funkcjonalność ta nie powinna być ograniczona wielkością i liczbą przywracanych plików
47. Oprogramowanie musi mieć możliwość odtworzenia plików bezpośrednio do maszyny wirtualnej poprzez sieć, przy pomocy natywnego API dla platformy VMware i PowerShell Direct dla platformy Hyper-V.
48. Oprogramowanie musi wspierać odtwarzanie pojedynczych plików z systemów Windows, Linux, BSD, Solaris, Mac, Novell
49. Oprogramowanie musi wspierać przywracanie plików z partycji Linux LVM
50. Oprogramowanie musi umożliwiać szybkie granularne odtwarzanie obiektów aplikacji bez użycia jakiegokolwiek agenta zainstalowanego wewnątrz maszyny wirtualnej.
51. Oprogramowanie musi wspierać granularne odtwarzanie obiektów Active Directory takich jak konta komputerów, konta użytkowników, dowolnych atrybutów, rekordów DNS zintegrowanych z AD, Microsoft System Objects, certyfikatów CA, elementów AD Sites oraz pozwalać na odtworzenie haseł.
52. Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Exchange 2013SP1 i nowszych (dowolny obiekt w tym obiekty w folderze "Permanently Deleted Objects"). Odtwarzanie musi być możliwe bezpośrednio do środowiska produkcyjnego.
53. Oprogramowanie musi wspierać granularne odtwarzanie Microsoft SQL 2008 i nowszych. Odtwarzanie musi być możliwe bezpośrednio do środowiska produkcyjnego dla odzysku point-in-time, całych baz lub pojedynczych tabeli, widoków oraz procedur.
54. Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Sharepoint 2013 i nowszych. Odtwarzanie musi być możliwe bezpośrednio do środowiska produkcyjnego dla odzysku całych witryn, bibliotek oraz pojedynczych dokumentów wraz z historią ich wersji.
55. Oprogramowanie musi wspierać granularne odtwarzanie baz danych Oracle z opcją odtwarzanie point-in-time wraz z włączonym Oracle DataGuard. Funkcjonalność ta musi być dostępna dla baz uruchomionych w środowiskach Windows oraz Linux.
56. Oprogramowanie musi wspierać granularne odtwarzanie baz danych PostgreSQL z opcją odtwarzanie point-in-time. Funkcjonalność ta musi być dostępna dla baz uruchomionych w środowiskach Linux.
57. Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez Oracle RMAN
58. Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez SAP HANA, SAP Oracle
59. Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez MS SQL VDI
60. Oprogramowanie musi wspierać także specyficzne metody odtwarzania w tym "reverse CBT" oraz odtwarzanie z wykorzystaniem sieci SAN
61. **Ograniczenie ryzyka**
62. Oprogramowanie musi dawać możliwość stworzenia laboratorium (izolowane środowisko) dla vSphere i Hyper-V używając wirtualnych maszyn uruchamianych bezpośrednio z plików backupu. Powyższa funkcjonalność powinna umożliwiać uruchomianie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna)
63. Dla VMware’a oprogramowanie musi pozwalać na uruchomienie takiego środowiska dla replik maszyn wirtualnych oraz bezpośrednio ze snapshotów macierzowych stworzonych na wspieranych urządzeniach.
64. Oprogramowanie musi umożliwiać weryfikację odtwarzalności wielu wirtualnych maszyn jednocześnie z dowolnego backupu według własnego harmonogramu w izolowanym środowisku. Testy powinny uwzględniać możliwość uruchomienia dowolnego skryptu testującego również aplikację uruchomioną na wirtualnej maszynie. Testy muszą być przeprowadzone bez interakcji z administratorem
65. Oprogramowanie musi umożliwiać integrację z oprogramowaniem antywirusowym w celu wykonania skanu zawartości pliku backupowego przed odtworzeniem jakichkolwiek danych. Integracja musi być zapewniona minimalnie dla Windows Defender, Symantec Protection Engine oraz ESET NOD32.
66. Oprogramowanie musi umożliwiać dwuetapowe, automatyczne, odtwarzanie maszyn wirtualnych z możliwością wstrzyknięcia dowolnego skryptu przed odtworzeniem danych do środowiska produkcyjnego.
67. **Środowiska fizyczne**
68. Rozwiązanie musi wykonywać kopię zapasową systemu Windows oraz Linux wykorzystując agenta znajdującego się wewnątrz systemu operacyjnego
69. Rozwiązanie musi wspierać systemy operacyjne Windows w wersjach klienckich oraz serwerowych
70. Rozwiązanie musi wspierać co najmniej następujące dystrybucje systemów Linux: Debian, Ubuntu, RHEL, CentOS, Oracle Linux, SLES, Fedora, openSUSE
71. Rozwiązanie musi wspierać system operacyjny macOS
72. Oprogramowanie musi wspierać odtwarzanie pojedynczych plików z systemów Windows, Linux, MacOS, Unix
73. Rozwiązanie musi mieć możliwość instalacji oraz zarządzania wykorzystując tryb niezależny (per agent) jak również zcentralizowany (poprzez centralną konsolę zarządzającą)
74. Rozwiązanie musi wspierać systemy oparte o Microsoft Failover Cluster
75. Rozwiązanie musi wspierać zabezpieczanie do oraz odzyskiwanie z urządzeń blokowych pozwalając na odzysk całej maszyny (tzw. bare metal recovery) wybranych wolumenów, oraz wybranych plików i folderów
76. Rozwiązanie musi wspierać backup podłączonych dysków USB
77. Kopia zapasowa całej maszyny oraz pojedynczych wolumenów musi być wykonywana na poziomie blokowym
78. Rozwiązanie musi pozwalać na przechowywanie kopii zapasowych na zasobach lokalnych (wewnętrznych) dyskach zabezpieczanej maszyny, Direct Attached Storage (DAS), takich jak zewnętrzne dyski USB, eSATA lub Firewire, Network Attached Storage (NAS) pozwalającym na wystawienie swoich zasobów poprzez SMB (CIFS) lub NFS, bezpośrednio na zasobach obiektowych (w tym chmury)
79. Rozwiązanie musi wspierać deduplikacje oraz kompresję na źródle. Dane wysyłane na repozytorium muszą być już odpowiednio przetworzone
80. Rozwiązanie musi wspierać kontrolę pasma sieciowego
81. Rozwiązanie musi wspierać ograniczenie wykonywania backupów dla konkretnych sieci bezprzewodowych
82. Rozwiązanie musi wspierać ograniczenia wykonywania backupów dla połączeń VPN
83. Rozwiązanie musi wspierać śledzenie zmienionych bloków podczas wykonywania kopii zapasowych. Dla systemów Windows technologia śledzenia bloków dla systemów serwerowych musi być certyfikowana przez Microsoft
84. Rozwiązanie musi wspierać technologię BitLocker
85. Rozwiązanie musi wspierać uruchamianie z nośnika odtwarzania
86. Rozwiązanie musi wspierać odzysk pojedynczych elementów aplikacji z jednoprzebiegowej kopii zapasowej dla Microsoft Exchange 2013SP1 i nowszych, Microsoft Active Directory 2008 i nowszych, Microsoft Sharepoint 2013 i nowszych, Microsoft SQL 2008 i nowszych, Oracle 11g i nowszych oraz PostgreSQL 12 i nowszych
87. Rozwiązanie musi wspierać odzysk do konkretnego punktu w czasie (point-in-time) dla wspieranych systemów bazodanowych
88. Rozwiązanie musi umożliwiać natychmiastowe publikowanie baz MS SQL i Oracle poprzez bezpośrednie uruchomienie ich z pliku backupu.
89. Rozwiązanie musi wspierać odzysk obrazów kopii zapasowych bezpośrednio do vSphere, Hyper-V, Nutanix AHV, Microsoft Azure, Microsoft Azure Stack, Amazon EC2 oraz Google Cloud Platform
90. Rozwiązanie musi wspierać szyfrowanie
91. Rozwiązanie musi wspierać możliwość wykonywania kopii zapasowych stacji klienckich, lokalnie do repozytorium tymczasowego (cache) gdy połączenie sieciowe do głównego repozytorium kopii zapasowych jest niedostępne
92. Rozwiązanie musi posiadać funkcjonalność automatycznego zmniejszenia szybkości przetwarzania danych, aby nie dopuścić do obniżenia wydajności systemu zabezpieczanego
93. Rozwiązanie musi posiadać ochronę przed ransomware poprzez automatyczne odmontowanie nośnika po wykonanym backupie stacji klienckiej
94. Rozwiązanie musi wspierać tworzenie wielu zadań backupowych
95. **Monitoring**
96. System musi zapewnić możliwość monitorowania środowiska wirtualizacyjnego opartego na VMware vSphere i Microsoft Hyper-V bez potrzeby korzystania z narzędzi firm trzecich
97. System musi umożliwiać monitorowanie środowiska wirtualizacyjnego VMware w wersji 6.x, 7.x oraz 8.0 – zarówno w bezpłatnej wersji ESXi jak i w pełnej wersji ESX/ESXi zarządzane przez konsole vCenter Server lub pracujące samodzielnie
98. System musi umożliwiać monitorowanie środowiska wirtualizacyjnego Microsoft Hyper-V 2012, 2012R2, 2016, 2019 oraz 2022 zarówno w wersji darmowej jak i zawartej w płatnej licencji Microsoft Windows Server zarządzane poprzez System Center Virtual Machine Manager lub pracujące samodzielnie.
99. System musi umożliwiać kategoryzacje obiektów infrastruktury wirtualnej niezależnie od hierarchii stworzonej w vCenter
100. System musi umożliwiać tworzenie alarmów dla całych grup wirtualnych maszyn jak i pojedynczych wirtualnych maszyn
101. System musi dawać możliwość układania terminarza raportów i wysyłania tych raportów przy pomocy poczty elektronicznej w formacie HTML oraz Excel
102. System musi dawać możliwość podłączenia się do kilku instancji vCenter Server i serwerów Hyper-V jednocześnie, w celu centralnego monitorowania wielu środowisk
103. System musi mieć wbudowane predefiniowane zestawy alarmów wraz z możliwością tworzenia własnych alarmów i zdarzeń przez administratora
104. System musi mieć wbudowane połączenie z bazą wiedzy opisującą problemy z predefiniowanych alarmów
105. System musi mieć centralną konsolę z sumarycznym podglądem wszystkich obiektów infrastruktury wirtualnej (ang. Dashboard)
106. System musi mieć możliwość monitorowania platformy sprzętowej, na której jest zainstalowana infrastruktura wirtualna
107. System musi zapewnić możliwość podłączenia się do wirtualnej maszyny (tryb konsoli) bezpośrednio z narzędzia monitorującego
108. System musi mieć możliwość integracji z oprogramowaniem do tworzenia kopii zapasowych tego samego producenta
109. System musi mieć możliwość monitorowania obciążenia serwerów backupowych, ilości zabezpieczanych danych oraz statusu zadań kopii zapasowych, replikacji oraz weryfikacji odzyskiwalności maszyn wirtualnych.
110. System musi oferować inteligentną diagnostykę rozwiązania backupowego poprzez monitorowanie logów celem wykrycia znanych problemów oraz błędów konfiguracyjnych w celu wskazania rozwiązania bez potrzeby otwierania zgłoszenia suportowego oraz bez potrzeby wysyłania jakichkolwiek danych diagnostycznych do producenta oprogramowania backupu.
111. System musi mieć możliwość granularnego monitorowania infrastruktury, zależnego od uprawnień nadanym użytkownikom dla platformy VMware
112. System musi mieć możliwość monitorowania instancji VMware vCloud Director w wersji od 10.x do 10.4
113. **Raportowanie**
114. System musi umożliwiać raportowanie środowiska wirtualizacyjnego VMware w wersji 6.x, 7.x oraz 8.0 – zarówno w bezpłatnej wersji ESXi jak i w pełnej wersji ESX/ESXi zarządzane przez konsole vCenter Server lub pracujące samodzielnie
115. System musi umożliwiać raportowanie środowiska wirtualizacyjnego Microsoft Hyper-V 2012, 2012R2, 2016, 2019 oraz 2022 zarówno w wersji darmowej jak i zawartej w płatnej licencji Microsoft Windows Server zarządzane poprzez System Center Virtual Machine Manager lub pracujące samodzielnie.
116. System musi wspierać wiele instancji vCenter Server i Microsoft Hyper-V jednocześnie bez konieczności instalowania dodatkowych modułów.
117. System musi być systemem bezagentowym. Nie dopuszcza się możliwości instalowania przez system agentów na monitorowanych hostach ESXi i Hyper-V
118. System musi mieć możliwość eksportowania raportów do formatów Microsoft Word, Microsoft Excel, Microsoft Visio, Adobe PDF
119. System musi mieć możliwość ustawienia harmonogramu kolekcji danych z monitorowanych systemów jak również możliwość tworzenia zadań kolekcjonowania danych ad-hoc
120. System musi mieć możliwość ustawienia harmonogramu generowania raportów i dostarczania ich do odbiorców w określonych przez administratora interwałach
121. System w raportach musi mieć możliwość uwzględniania informacji o zmianach konfiguracji monitorowanych systemów
122. System musi mieć możliwość generowania raportów z dowolnego punktu w czasie zakładając, że informacje z tego czasu nie zostały usunięte z bazy danych
123. System musi posiadać predefiniowane szablony z możliwością tworzenia nowych jak i modyfikacji wbudowanych
124. System musi mieć możliwość analizowania „przeszacowanych” wirtualnych maszyn wraz z sugestią zmian w celu optymalnego wykorzystania fizycznej infrastruktury
125. System musi mieć możliwość generowania raportów na podstawie danych uzyskanych z oprogramowania do tworzenia kopii zapasowych tego samego producenta
126. System musi mieć możliwość generowania raportu dotyczącego zabezpieczanych maszyn, zdefiniowanych zadań tworzenia kopii zapasowych oraz replikacji jak również wykorzystania zasobów serwerów backupowych.
127. System musi mieć możliwość generowania raportu planowania pojemności (capacity planning) bazującego na scenariuszach ‘what-if’.
128. System musi mieć możliwość granularnego raportowania infrastruktury, zależnego od uprawnień nadanym użytkownikom dla platformy VMware
129. System musi mieć możliwość generowania raportów dotyczących tzw. migawek-sierot (orphaned snapshots)
130. System musi mieć możliwość generowania personalizowanych raportów zawierających informacje z dowolnych predefiniowanych raportów w pojedynczym dokumencie