

OPIS PRZEDMIOTU ZAMÓWIENIA – Część nr 7

Przedmiotem zamówienia jest dostawa klastra do wirtualizacji składającego się z 3 serwerów do wirtualizacji, macierzy dyskowej, oprogramowania i licencji Microsoft, biblioteki taśmowej, serwera kopii zapasowej, serwera repozytorium, oprogramowania do wirtualizacji, oprogramowania kopii zapasowej oraz usługa wdrożenia i dokumentacji.

Wszystkie podane parametry opisujące przedmiot zamówienia są parametrami jakościowymi określającymi właściwości (cechy) nie gorsze niż wymagane i odnoszą się do co najmniej głównych elementów składających się na przedmiot zamówienia. Oznacza to, że parametry mogą być odpowiednio wyższe, jeżeli dzięki temu polepszają właściwości przedmiotu zamówienia.

Jeżeli do opisanego przedmiotu zamówienia użyto oznaczenia lub parametry wskazujące konkretnego producenta, produkt, znaki towarowe, patenty lub pochodzenie urządzeń, Zamawiający dopuszcza zastosowanie produktów równoważnych, przez które należy rozumieć produkty o parametrach nie gorszych od przedstawionych w OPZ.

PRZEDMIOT		Liczba
Klaster do wirtualizacji z instalacją, wdrożeniem i dokumentacją składający się z:		1
1	<i>Serwer do wirtualizacji</i>	<i>3</i>
2	<i>Macierz dyskowa</i>	<i>1</i>
3	<i>Oprogramowanie serwerów</i>	<i>1</i>
4	<i>Biblioteka taśmowa</i>	<i>1</i>
5	<i>Serwer kopii zapasowej</i>	<i>1</i>
6	<i>Serwer repozytorium</i>	<i>1</i>
7	<i>Oprogramowanie do wirtualizacji</i>	<i>1</i>
8	<i>Oprogramowanie do kopii zapasowej</i>	<i>1</i>

1. Serwer do wirtualizacji

Parametr	Charakterystyka (wymagania minimalne)
Obudowa	Obudowa Rack o wysokości max 2U. Komplet wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych oraz organizatorem do kabli. Obudowa musi mieć możliwość wyposażenia w kartę umożliwiającą dostęp bezpośredni poprzez urządzenia mobilne - serwer musi posiadać możliwość konfiguracji oraz monitoringu najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej min. (Android/ Apple iOS) przy użyciu jednego z protokołów BLE/ WIFI.
Płyta główna	Płyta główna z możliwością zainstalowania do dwóch procesorów. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym.
Chipset	Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych
Procesor	Zainstalowane dwa procesory min. 16-rdzeniowe klasy x86, min. 2.8GHz, dedykowane do pracy z zaoferowanym serwerem umożliwiające osiągnięcie wyniku min. 339 w teście SPECrate2017_int_base, dostępnym na stronie www.spec.org dla konfiguracji dwuprocesorowej dla oferowanego modelu serwera.
RAM	Minimum 512 DDR5 RDIMM 5600MT/s, w oparciu o kości pamięci 32GB. Na płycie głównej powinno znajdować się minimum 32 sloty przeznaczone do instalacji pamięci. Płyta główna powinna obsługiwać do 8TB pamięci RAM.
Funkcjonalność pamięci RAM	<ul style="list-style-type: none">• Demand Scrubbing,• Patrol Scrubbing,• Permanent Fault Detection
Gniazda PCI	Min. 6 slotów PCIe w tym min. 3 sloty x16 i min. 2 sloty Gen5
Interfejsy sieciowe/FC/SAS	Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT oraz 4 interfejsy sieciowe 10/25Gb w standardzie SFP28 obsadzone wkładkami jednomodowymi SFP+ 10Gb LR / SFP28 25Gb LR (porty nie mogą być osiągnięte poprzez karty w slotach PCIe) Dodatkowa, dwuportowa karta 64Gb FC wraz z wkładkami SW o natywnej prędkości portów.
Dyski twarde	Zainstalowane dwa dyski M.2 NVMe SSDs o pojemności min. 960GB Hot-Plug z możliwością konfiguracji RAID 1 Możliwość zainstalowania dedykowanego modułu dla hypervisora wirtualizacyjnego, wyposażony w 2 nośniki typu flash o pojemności min. 64GB, z możliwością konfiguracji zabezpieczenia synchronizacji pomiędzy nośnikami z poziomu BIOS serwera, rozwiązanie nie może powodować zmniejszenia ilości wnek na dyski twarde.
Wbudowane porty	4x USB, w tym min. 1 port USB 3.0 2 porty VGA, Możliwość rozbudowy o Serial Port
Video	Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1920 x 1200
Wentylatory	Redundantne
Zasilacze	Redundantne, Hot-Plug min. 1100W każdy wraz z kablami zasilającymi o długości min. 2m.
Bezpieczeństwo	<ul style="list-style-type: none">• Zatrask 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

	<p>możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła</p> <ul style="list-style-type: none"> • 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
Diagnostyka	Panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS'u, zasilaniu oraz temperaturze.
Karta Zarządzania	<ul style="list-style-type: none"> • Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca: <ul style="list-style-type: none"> ○ 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; ○ 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 ○ Wirtualny schowek ułatwiający korzystanie z konsoli zdalnej oraz z możliwością rozszerzenia funkcjonalności o: <ul style="list-style-type: none"> ○ Przesyłanie danych telemetrycznych w czasie rzeczywistym ○ Dostosowanie zarządzania temperaturą i przepływem powietrza w serwerze ○ Automatyczna rejestracja certyfikatów (ACE)
Oprogramowanie do zarządzania	<ul style="list-style-type: none"> • 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

	<p>informacje zawarte w inwentarzu.</p> <ul style="list-style-type: none"> • Grupowanie urządzeń w oparciu o kryteria użytkownika • Tworzenie automatycznie grup urządzeń w oparciu o dowolny element konfiguracji serwera np. Nazwa, lokalizacja, system operacyjny, obsadzenie slotów PCIe, pozostałego czasu gwarancji • Możliwość uruchamiania narzędzi zarządzających w poszczególnych urządzeniach • Szybki podgląd stanu środowiska • Podsumowanie stanu dla każdego urządzenia • Szczegółowy status urządzenia/elementu/komponentu • Generowanie alertów przy zmianie stanu urządzenia. • Filtry raportów umożliwiające podgląd najważniejszych zdarzeń • Integracja z service desk producenta dostarczonej platformy sprzętowej • Możliwość przejęcia zdalnego pulpitu • Możliwość podmontowania wirtualnego napędu • Kreator umożliwiający dostosowanie akcji dla wybranych alertów • Możliwość importu plików MIB • Przesyłanie alertów „as-is” do innych konsol firm trzecich • Możliwość definiowania ról administratorów • Możliwość zdalnej aktualizacji oprogramowania wewnętrznego serwerów • Aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania) • Możliwość instalacji oprogramowania wewnętrznego bez potrzeby instalacji agenta • Możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów • Moduł raportujący pozwalający na wygenerowanie następujących informacji: nr seryjne sprzętu, konfiguracja poszczególnych urządzeń, wersje oprogramowania wewnętrznego, obsadzenie slotów PCI i gniazd pamięci, informację o maszynach wirtualnych, aktualne informacje o stanie i poziomie gwarancji, adresy IP kart sieciowych, występujących alertów, MAC adresów kart sieciowych, stanie poszczególnych komponentów serwera. • Możliwość tworzenia sprzętowej konfiguracji bazowej i na jej podstawie weryfikacji środowiska w celu wykrycia rozbieżności. • Wdrażanie serwerów, rozwiązań modularnych oraz przełączników sieciowych w oparciu o profile • Możliwość migracji ustawień serwera wraz z wirtualnymi adresami sieciowymi (MAC, WWN, IQN) między urządzeniami. • Tworzenie gotowych paczek informacji umożliwiających zdiagnozowanie awarii urządzenia przez serwis producenta. • Zdalne uruchamianie diagnostyki serwera. • Dedykowana aplikacja na urządzenia mobilne integrująca się z wyżej opisanymi oprogramowaniem zarządzającym. • Oprogramowanie dostarczane jako wirtualny appliance dla KVM, ESXi i Hyper-V.
Certyfikaty	<ul style="list-style-type: none"> • Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015, ISO-50001 oraz ISO-14001 • Serwer musi posiadać deklarację CE. • Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Microsoft

	<p>Windows Server 2019, Microsoft Windows Server 2022, Microsoft Windows Server 2025</p> <ul style="list-style-type: none"> • Wsparcie dla ESXi 8.
Warunki gwarancji	<ul style="list-style-type: none"> • Gwarancji producenta: 5 lat • Możliwość rozszerzenia gwarancji przez producenta do 7 lat. • Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie oraz przez Internet • Zamawiający oczekuje rozpoczęcia diagnostyki telefonicznej / internetowej już w momencie dokonania zgłoszenia. Certyfikowany Technik wykonawcy / producenta z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) 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. • Zamawiający oczekuje bezpośredniego dostępu 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/portal) przez nadanie unikalnego numeru zgłoszenia pozwalającego na identyfikację zgłoszenia w trakcie realizacji naprawy i po jej zakończeniu. • Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy. • Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji serwera. • Zamawiający oczekuje nieodpłatnego udostępnienia narzędzi serwisowych i procesów wsparcia umożliwiających: Wykrywanie usterek sprzętowych z predykcją awarii. • Możliwość automatycznej diagnostyki i zdalne otwieranie zgłoszeń serwisowych. • Firma serwisująca musi posiadać ISO 9001:2015 oraz ISO-27001 na świadczenie usług serwisowych oraz posiadać autoryzację producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty. • Wymagane dołączenie do oferty oświadczenia Producenta potwierdzając, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta. • Wymagane dołączenie do oferty oświadczenia Producenta potwierdzające, że serwer pochodzi z autoryzowanego kanału dystrybucji producenta. <p>Możliwość rozszerzenia gwarancji o:</p> <ul style="list-style-type: none"> • Wyznaczonego przez wykonawcę Opiekuna Technicznego Klienta, do którego obowiązków będzie należało: <ul style="list-style-type: none"> ○ Monitorowanie zdarzeń w obrębie infrastruktury ○ Zarządzanie eskalacjami i współpraca z kierownikiem eskalacji • Przygotowywanie kwartalnych zaleceń dotyczące konserwacji infrastruktury sprzętowej (BIOS, firmware, patche)

	Raportowanie realizacji kontraktów serwisowych i wykorzystania zasobów sprzętowych (na żądanie)
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.

2. Macierz dyskowa

Lp.	Szczegółowy opis wymagań
1	Macierz musi umożliwiać instalację w standardowej szafie RACK 19”.
2	Macierz mieć możliwość instalacji kombinacji poniższych nośników dyskowych w ramach jednej obudowy podstawowej (zawierającej kontrolery): - Flash NVMe lub NVMe SSD, gdzie Flash NVMe oznacza dyski autorskie dostawców macierzy wykorzystujące protokół NVMe - SCM (Storage Class Memory) Możliwość podłączenia półek dyskowych dla dysków SSD/SAS/NL-SAS.
3	Możliwość zainstalowania co najmniej 12 dysków NVMe o rozmiarze 2,5”.
4	Kontrolery macierzowe muszą komunikować się z nośnikami dyskowymi umieszczonymi w obudowie podstawowej (zawierającej kontrolery) wyłącznie z użyciem protokołu NVMe.
5	Macierz musi być zbudowana z minimum dwóch kontrolerów pracujących w trybie active-active lub dual-active.
6	Architektura macierzy ma być oparta o sprawdzone i powszechnie dostępne procesory technologii x86/x64. Nie dopuszcza się procesorów typu ARM.
7	Wszystkie krytyczne komponenty macierzy takie jak: kontrolery dyskowe, pamięć cache, zasilacze i wentylatory muszą być zdublowane tak, aby awaria pojedynczego elementu nie wpływała na funkcjonowanie całego systemu. Komponenty te muszą być wymienne w trakcie pracy macierzy.
8	Macierz musi cechować brak pojedynczego punktu awarii.
9	Wsparcie dla zasilania z dwóch niezależnych źródeł prądu poprzez nadmiarowe zasilacze typu Hot-Swap. Wentylatory typu Hot-Swap.
10	Macierz musi być odporna na zaniki napięcia, tzn. chwilowy zanik napięcia nie powinien przerywać pracy macierzy.
11	Macierz musi umożliwiać zarządzanie za pomocą interfejsu Ethernet. Możliwość zarządzania całością dostępnych zasobów dyskowych z jednej konsoli administracyjnej.
12	Funkcjonalność bezpośredniego monitoringu stanu w jakim w danym momencie macierz się znajduje.
13	Urządzenie musi składać się z pojedynczej macierzy dyskowej zarządzanej z jednego wbudowanego w macierz interfejsu GUI (interfejs graficzny), CLI (interfejs tekstowy) oraz zapewniać możliwość tworzenia skryptów użytkownika. Interfejs ten musi być natywnie dostępny na macierzy, bez zastosowania zewnętrznych urządzeń.
14	Wymagane jest nie mniej niż 4 x FC 32Gb/s per kontroler
15	Całkowita pojemność użytkowa NVMe min. 51.5 Tib (użyteczne przy założeniu konfiguracji odpornej na awarię minimum 2 dysków (typu RAID-6 lub równoważnego) , z uwzględnieniem przestrzeni spare o wielkości 1 dysku oraz bez uwzględnienia technik redukcji danych takich jak kompresja, deduplikacja czy thin-provisioning). Przestrzeń musi być zbudowana wyłącznie w oparciu o nośniki NVMe Flash lub NVMe SSD. Przestrzeń musi być zbudowana w oparciu o nośniki o pojemności max. 10TB. Całkowita pojemność użytkowa NL-SAS min. 535 Tib (użyteczne przy założeniu konfiguracji

	odpornej na awarię minimum 2 dysków (typu RAID-6 lub równoważnego) , z uwzględnieniem przestrzeni spare o wielkości 1 dysku oraz bez uwzględnienia technik redukcji danych takich jak kompresja, deduplikacja czy thin-provisioning). Przestrzeń musi być zbudowana wyłącznie w oparciu o nośniki NL-SAS 12Gb. Przestrzeń musi być zbudowana w oparciu o nośniki o pojemności max. 20TB.
16	Macierz musi pozwalać na alokację 99% pojemności użytecznej bez spadku wydajności macierzy (brak zwiększonego czasu odpowiedzi, brak spadku przepustowości macierzy). Wydajność macierzy musi być niezależna od poziomu alokacji przestrzeni macierzy w zakresie od 0% alokacji do wartości wymaganej pojemności użytecznej. Opisana funkcjonalność musi być realizowana minimum dla dysków NVMe. Jeżeli oferowane rozwiązanie nie spełnia opisanego wymagania należy dostarczyć co najmniej 20% pojemności użytecznej więcej na nośnikach NVMe.
17	Macierz musi obsługiwać poziomy: RAID6 (dystrybuowane) i zapewniać zabezpieczenie przed awarią dwóch dysków jednocześnie w ramach jednej grupy raid.
18	Dyski/przestrzeń "spare" muszą zostać skonfigurowane/dostarczone w ilości/pojemności zgodnej z udokumentowanymi rekomendacjami producenta oferowanej macierzy.
19	Kontrolery macierzowe muszą posiadać możliwość szyfrowania danych, uniemożliwiając odczyt danych z usuniętych z macierzy nośników dyskowych. Ta funkcjonalność nie jest wymagana na etapie tego postępowania.
20	Macierz musi mieć możliwość obsługi min. 200 dysków poprzez dodanie półek rozszerzeń. Macierz musi mieć możliwość rozbudowy poprzez dodanie pojedynczego dysku, dodanie kontrolerów oraz półek dyskowych.
21	Niezależnie od zastosowanych nośników danych, macierz musi umożliwiać granularną rozbudowę grupy RAID w zakresie od co najmniej od 1 do 12 nośników dyskowych, proces rozbudowy nie może powodować niedostępności do danych.
22	Macierz musi być wyposażona w minimum 2 kontrolery dyskowe z możliwością rozbudowy do 4 kontrolerów. Każdy z kontrolerów musi udostępniać co najmniej 256GB pamięci Cache.
23	Macierz musi umożliwiać rozbudowę pamięci cache do 1TB w ramach klastra macierzy składającego się z identycznych kontrolerów i zarządzanego z jednego interfejsu GUI, CLI. Zamawiający nie dopuszcza zastosowania dysków SSD/ SSD NVMe lub kart pamięci/modułów FLASH jako rozszerzenia pamięci cache.
24	Funkcjonalność partycjonowania pamięci cache.
25	Funkcjonalność separacji przestrzeni dyskowych pomiędzy różnymi podłączonymi hostami.
26	Funkcjonalność dynamicznego zwiększania rozmiaru wolumenów.
27	Funkcjonalność zarządzania maksymalną ilością operacji wejścia / wyjścia wykonywanych na danym wolumenie - zarządzanie musi być możliwe zarówno poprzez określenie ilości operacji I/O na sekundę jak również przepustowości określonej w MB/s.
28	Macierz musi mieć możliwość kompresji i deduplikacji dla wszystkich rodzajów dysków. Licencja na tą funkcjonalność musi być zawarta w cenie i musi obejmować zaoferowaną w ramach macierzy przestrzeń dyskową Wsparcie dla kompresji danych w trybie inline („na bieżąco” bez potrzeby zapisywania danych na nośnikach danych w formie nie skompresowanej) dla dostępu blokowego.
29	Macierz musi wspierać kompresję i deduplikację w trybie "inline".
30	Zaoferowane rozwiązanie musi posiadać możliwość implementacji klastra wysokiej dostępności. W ramach architektury klastra wysokiej dostępności musi być wspierane bezprzerwowe migrowanie maszyn wirtualnych pomiędzy ośrodkami. W przypadku awarii jednej z macierzy nastąpi bezprzerwowe przełączenie do lokalizacji zapasowej. Powyższa funkcjonalność musi być realizowana niezależnie od systemu operacyjnego na poziomie przełączania ścieżek do urządzenia logicznego. Licencja na tą funkcjonalność musi być zawarta w cenie i musi obejmować zaoferowaną w ramach macierzy przestrzeń dyskową.

31	Macierz musi optymalizować wykorzystanie dysków SSD/ modułów Flash/ HDD, tak aby w ramach tego samego rodzaju dysków (pojemności/prędkości) wszystkie grupy dysków były uitylizowane w równym stopniu. Licencja na tą funkcjonalność musi być zawarta w cenie i musi obejmować całą oferowaną pojemność macierzy.
32	Macierz musi mieć możliwość rozłożenia wolumenu logicznego pomiędzy co najmniej dwoma różnymi typami macierzy dyskowych
33	Macierz musi umożliwiać stworzenie mirrorowanych LUN pomiędzy różnymi macierzami, dla których awaria jednej kopii lustra musi być niezauważalna dla systemu hosta.
34	Macierz musi obsługiwać funkcjonalność thin provisioning dla wszystkich wolumenów. Należy dostarczyć licencję umożliwiającą korzystanie z funkcji thin provisioning na całą oferowaną pojemność macierzy.
35	Kopie danych typu snapshot muszą być tworzone w trybach incremental, multitarget, oraz kopii pełnej oraz kopii wskaźników. Licencja na tą funkcjonalność musi być zawarta w cenie i musi obejmować całą oferowaną pojemność macierzy.
36	Macierz musi posiadać możliwość tworzenia kopii migawkowych w trybie WORM (Write Once Read Many). Kopie powinny być tworzone za pomocą harmonogramu i mieć możliwość ustawienia retencji kopii, po upływie której kopia automatycznie zostanie usunięta z macierzy.
37	Macierz musi mieć możliwość wykonywania replikacji synchronicznej i asynchronicznej wolumenów logicznych pomiędzy różnymi typami macierzy dyskowych. Zasoby źródłowe kopii zdalnej oraz docelowe kopii zdalnej mogą być zabezpieczone różnymi poziomami RAID i egzystować na różnych technologicznie dyskach stałych (SAS, SSD, SATA). Licencja na tą funkcjonalność musi być zawarta w cenie i musi obejmować zaoferowaną w ramach macierzy przestrzeń dyskową.
38	Macierz musi być nowa, nigdy wcześniej nie używana i pochodzić z autoryzowanego kanału dystrybucji producenta a także być objęta serwisem producenta na terenie RP.
39	Wsparcie systemów operacyjnych Macierz musi być wspierana przez systemy operacyjne i wirtualizatory: MS Windows Server 2019, 2022, 2025 Vmware vSphere 8 i nowsze, RedHat Enterprise Server 7.6 i nowsze
40	Macierz musi zapewniać integrację z oferowanym oprogramowaniem kopii zapasowej na poziomie umożliwiającym na pełną współpracę w zakresie: - backupu z migawek pamięci masowych - eksplorator migawek pamięci masowych - tworzenie wyizolowanego środowiska z użyciem migawek pamięci masowych Współpraca z zaoferowanym oprogramowaniem ma się odbywać bez konieczności instalacji dodatkowych modułów (pluginów).
41	Wymagana jest gwarancja świadczona w trybie 24 godziny przez 7 dni w tygodniu na wszystkie elementy macierzy (sprzęt oraz oprogramowanie) na okres 60 miesięcy z gwarantowanym czasem naprawy w ciągu 24 godzin. Uszkodzony dysk po wymianie zostaje własnością Zamawiającego. Usługi serwisowe będą świadczone przez producenta oferowanego sprzętu.
42.	Wraz z macierzą należy dostarczyć oprogramowanie do monitorowania macierzy blokowych, plikowych, obiektowych oraz hostów i przełączników SAN. Oprogramowanie musi zapewniać przechowywanie trendów historycznych środowiska przez okres co najmniej 365 dni. Rozwiązanie posiada możliwość odpytywania danych telemetrycznych w celu uzyskania szczegółowych informacji w sekwencjach co najmniej 5-minutowych. "Rozwiązanie musi pozwalać na monitorowanie następujących metryk dla macierzy dyskowych różnych producentów (co najmniej Dell EMC, Hitachi, IBM, NetApp, Pure): <ul style="list-style-type: none"> ogólną aktywność i wydajność systemu pojemność macierzy

	<ul style="list-style-type: none"> • najbardziej aktywne kontrolery • najbardziej aktywne wolumeny • najbardziej aktywne pule • szybkość operacji I/O (op/s) per macierz, kontroler, pula, wolumen. • przepustowość (MiB/s) per macierz, kontroler, pula, wolumen. • czas odpowiedzi (ms/op) per macierz, kontroler, pula, wolumen • przepustowość i użycie portów/interfejsów macierzy • użycie CPU macierzy (ogólna oraz per rdzeń) <p>Rozwiązanie musi pozwalać na tworzenie raportów na podstawie informacji zawartych w tabelach interfejsu użytkownika rozwiązania.</p> <p>Możliwość tworzenia użytkowników oraz grup i przypisywanie im określonych ról i poziomów dostępu.</p> <p>Wysyłanie alertów z rozwiązania do wewnętrznego systemu powiadamiania.</p>
--	--

3. Oprogramowanie serwerów

Zamawiający dysponuje infrastrukturą opartą o systemy Microsoft Windows i serwery Active Directory i w związku z tym wymaga rozbudowy licencji o następujące:

1. Licencje Windows Server 2025 Datacenter na 96 rdzeni dla oferowanych serwerów do wirtualizacji. Dopuszcza się dostarczenie licencji OEM wraz z serwerem.
2. 95 licencji Windows Server 2025 CAL na użytkownika. Dopuszcza się dostarczenie licencji OEM wraz z serwerem.
3. 10 licencji Windows Server 2025 RDS CAL na użytkownika. Dopuszcza się dostarczenie licencji OEM wraz z serwerem.

4. Biblioteka taśmowa

Parametr	Charakterystyka (wymagania minimalne)
Obudowa	Do zamontowania w szafie rack, maksymalnie 3U, wbudowany czytnik kodów kreskowych, redundantne zasilanie wraz z kablami zasilającymi, szyny RACK.
Napęd	1x LTO9 z możliwością rozbudowy biblioteki taśmowej do min. 48 napędów LTO.
Interfejs	FC
Liczba slotów	40 w tym minimum pięć slotów we/wy, jeżeli licencjonowana jest liczba slotów - wymagane aktywowanie wszystkich slotów W komplecie min.: <ul style="list-style-type: none"> • 1 taśma czyszcząca • 40 taśm LTO8 • Etykiety do taśm LTO9 o numerach 1-200
Dodatkowe	<ul style="list-style-type: none"> • interfejs do zarządzania poprzez przeglądarkę WWW oraz możliwość zarządzania bezpośrednio z użyciem wbudowanych klawiszy i wyświetlacza LCD • wyjmowane magazynki kieszeni na taśmy w celu łatwego zarządzania większą ilością taśm • wsparcie dla nośników LTO WORM (Write Once, Read Many), umożliwiających spełnienie norm prawnych dotyczących odpowiednio długiego przechowywania nienaruszonych danych (archiwizacja) • Obsługa SNMP, TLS1.2 oraz IP6 • Wsparcie dla technologii szyfrowania backupowanych danych.
Warunki gwarancji dla autoloadera	5 lat gwarancji producenta realizowanej w miejscu instalacji sprzętu, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii 24x7x365 poprzez ogólnopolską linię telefoniczną producenta. <ul style="list-style-type: none"> • Dostawca ponosi koszty napraw gwarancyjnych, włączając w to koszt części i transportu.

	<ul style="list-style-type: none"> • W czasie obowiązywania gwarancji dostawca zobowiązany jest do udostępnienia Zamawiającemu nowych wersji BIOS, firmware i sterowników (na płytach CD lub stronach internetowych). • Firma serwisująca musi posiadać ISO 9001:2008 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta serwera – dokumenty potwierdzające załączyć do oferty. • Oświadczenie producenta biblioteki, że w przypadku niewywiązywania się z obowiązków gwarancyjnych oferenta lub firmy serwisującej, przejmie na siebie wszelkie zobowiązania związane z serwisem.
--	--

5. Serwer kopii zapasowej

Parametr	Charakterystyka (wymagania minimalne)
Obudowa	<p>Obudowa Rack o wysokości max 2U z możliwością instalacji min. 12 dysków 3,5" Hot-Plug oraz 2 dysków 2,5" Hot-Plug wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych oraz organizatorem do kabli.</p> <p>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.</p>
Płyta główna	Płyta główna z możliwością zainstalowania minimum jednego procesora. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym.
Chipset	Dedykowany przez producenta procesora do pracy w serwerach jednoprocessorowych
Procesor	Zainstalowany jeden procesor, min. 16-rdzeniowy, min. 3.0GHz, klasy x86 dedykowany do pracy z zaoferowanym serwerem umożliwiający osiągnięcie wyniku min. 177 w teście SPECrate2017_int_base w konfiguracji jedno procesorowej dla oferowanego serwera, dostępnym na stronie www.spec.org . Możliwość obsługi procesorów 128 rdzeniowych
RAM	Minimum 64GB DDR5 RDIMM 5600MT/s, na płycie głównej powinno znajdować się minimum 12 slotów przeznaczonych do instalacji pamięci. Płyta główna powinna obsługiwać do min. 3TB pamięci RAM.
Zabezpieczenia pamięci RAM	Patrol Scrubbing
Gniazda PCI	Minimum 6 slotów PCIe, z czego przynajmniej 2 x16
Interfejsy sieciowe/FC/SAS	<p>Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT oraz 4 interfejsy sieciowe 10/25Gb Ethernet w standardzie SFP28 (porty nie mogą być osiągnięte poprzez karty w slotach PCIe)</p> <p>Interfejsy SFP28 muszą być wyposażone we wkładki jednomodowe 10Gb SFP+</p> <p>Dodatkowa, dwuportowa karta 32GB FC wraz z wkładkami SW o natywnej prędkości portów.</p> <p>Dodatkowa, dwuportowa karta 64GB FC wraz z wkładkami SW o natywnej prędkości portów.</p>
Dyski twarde	<p>Zainstalowane:</p> <ul style="list-style-type: none"> • 12 dysków SAS o pojemności min. 12TB, 12Gbps, Hot-Plug. • 2 dyski SSD SATA RI o pojemności min. 960GB, Hot-Plug. <p>Możliwość zainstalowania dwóch dysków M.2 NVMe SSDs o pojemności min. 960GB Hot-Plug z możliwością konfiguracji RAID 1.</p>
Kontroler RAID	Sprzętowy kontroler dyskowy, posiadający min. 8GB nieulotnej pamięci cache, możliwe konfiguracje poziomów RAID: 0, 1, 5, 6, 10, 50, 60

Wbudowane porty	3x USB w tym przynajmniej 1x USB 3.0 1x port VGA na przednim panelu obudowy Możliwość rozbudowy o port RS232
Diagnostyka	Panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS'u, zasilaniu oraz temperaturze.
Video	Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1920x1080
System operacyjny / dodatkowe oprogramowanie	Windows Server 2025 Standard na 16 rdzeni.
Wentylatory	Redundantne
Zasilacze	Redundantne, Hot-Plug min. 1100W każdy wraz z kablami zasilającymi o długości min. 2m.
Bezpieczeństwo	<ul style="list-style-type: none"> • Zatrzaszk górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardech. • 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
Karta Zarządzania	<p>Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca:</p> <ul style="list-style-type: none"> • zdalny dostęp do graficznego interfejsu Web karty zarządzającej; • zdalne monitorowanie i informowanie o statusie serwera (np. 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; • 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

<p>Oprogramowanie do zarządzania</p>	<ul style="list-style-type: none"> • Możliwość zainstalowania oprogramowania producenta do zarządzania, spełniającego poniższe wymagania: <ul style="list-style-type: none"> ○ 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.
---	---

	<ul style="list-style-type: none"> o Możliwość tworzenia sprzętowej konfiguracji bazowej i na jej podstawie weryfikacji środowiska w celu wykrycia rozbieżności. o Wdrażanie serwerów, rozwiązań modularnych oraz przełączników sieciowych w oparciu o profile o Możliwość migracji ustawień serwera wraz z wirtualnymi adresami sieciowymi (MAC, WWN, IQN) między urządzeniami. o Tworzenie gotowych paczek informacji umożliwiających zdiagnozowanie awarii urządzenia przez serwis producenta. o Zdalne uruchamianie diagnostyki serwera. o Dedykowana aplikacja na urządzenia mobilne integrująca się z wyżej opisanymi oprogramowaniem zarządzającym. o Oprogramowanie dostarczane jako wirtualny appliance dla KVM, ESXi i Hyper-V.
Certyfikaty	<p>Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015, ISO-50001 oraz ISO-14001</p> <p>Serwer musi posiadać deklarację CE.</p> <p>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, Microsoft Windows Server 2025.</p> <p>Wsparcie dla ESXi 8.</p>
Dokumentacja użytkownika	<p>Zamawiający wymaga dokumentacji w języku polskim lub angielskim.</p> <p>Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.</p>
Warunki gwarancji	<p>5 lat gwarancji producenta, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia.</p> <p>Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie, przez Internet oraz z wykorzystaniem aplikacji.</p> <p>Zgłoszenie przyjęte jest potwierdzane przez zespół pomocy technicznej (mail/telefon/portal) przez nadanie unikalnego numeru zgłoszenia pozwalającego na identyfikację zgłoszenia w trakcie realizacji naprawy i po jej zakończeniu.</p> <p>Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji serwera.</p> <p>Zamawiający oczekuje nieodpłatnego udostępnienia narzędzi serwisowych i procesów wsparcia umożliwiających: Wykrywanie usterek sprzętowych z predykcją awarii.</p> <p>Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wsparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego.</p> <p>Firma serwisująca musi posiadać ISO 9001:2015 oraz ISO-27001 na świadczenie usług serwisowych oraz posiadać autoryzację producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty.</p>

6. Serwer repozytorium

Parametr	Charakterystyka (wymagania minimalne)
Obudowa	Obudowa Rack o wysokości max 2U z możliwością instalacji min. 12 dysków

	3,5" Hot-Plug oraz 2 dysków 2,5" Hot-Plug wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych oraz organizatorem do kabli. Obudowa z możliwością wyposażenia w kartę umożliwiającą dostęp bezpośredni poprzez urządzenia mobilne - serwer musi posiadać możliwość konfiguracji oraz monitoringu najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej min. (Android/ Apple iOS) przy użyciu jednego z protokołów BLE/ WIFI.
Płyta główna	Płyta główna z możliwością zainstalowania minimum jednego procesora. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym.
Chipset	Dedykowany przez producenta procesora do pracy w serwerach jednoprocessorowych
Procesor	Zainstalowany jeden procesor, min. 16-rdzeniowy, min. 3.0GHz, klasy x86 dedykowany do pracy z zaoferowanym serwerem umożliwiający osiągnięcie wyniku min. 177 w teście SPECrate2017_int_base w konfiguracji jedno procesorowej dla oferowanego serwera, dostępnym na stronie www.spec.org . Możliwość obsługi procesorów 128 rdzeniowych
RAM	Minimum 32GB DDR5 RDIMM 5600MT/s, na płycie głównej powinno znajdować się minimum 12 slotów przeznaczonych do instalacji pamięci. Płyta główna powinna obsługiwać do min. 3TB pamięci RAM.
Zabezpieczenia pamięci RAM	Patrol Scrubbing
Gniazda PCI	Minimum 6 slotów PCIe, z czego przynajmniej 2 x16
Interfejsy sieciowe/FC/SAS	Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT oraz 4 interfejsy sieciowe 10/25Gb Ethernet w standardzie SFP28 (porty nie mogą być osiągnięte poprzez karty w slotach PCIe) Interfejsy SFP28 muszą być wyposażone we wkładki jednomodowe 10Gb SFP+
Dyski twarde	Zainstalowane: <ul style="list-style-type: none"> • 12 dysków SAS o pojemności min. 12TB, 12Gbps, Hot-Plug. • 2 dyski SSD SATA RI o pojemności min. 480GB, Hot-Plug. Możliwość zainstalowania dwóch dysków M.2 NVMe SSDs o pojemności min. 960GB Hot-Plug z możliwością konfiguracji RAID 1.
Kontroler RAID	Sprzętowy kontroler dyskowy, posiadający min. 8GB nieulotnej pamięci cache, możliwe konfiguracje poziomów RAID: 0, 1, 5, 6, 10, 50, 60
Wbudowane porty	3x USB w tym przynajmniej 1x USB 3.0 1x port VGA na przednim panelu obudowy Możliwość rozbudowy o port RS232
Diagnostyka	Panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS'u, zasilaniu oraz temperaturze.
Video	Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1920x1080
Wentylatory	Redundantne
Zasilacze	Redundantne, Hot-Plug min. 1100W każdy wraz z kablami zasilającymi o długości min. 2m.
Bezpieczeństwo	<ul style="list-style-type: none"> • Zatrzaśki górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardej. • 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. <ul style="list-style-type: none"> • 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
Karta Zarządzania	Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiającą: <ul style="list-style-type: none"> • zdalny dostęp do graficznego interfejsu Web karty zarządzającej; • zdalne monitorowanie i informowanie o statusie serwera (np. prędkości obrotowej wentylatorów, konfiguracji serwera); • szyfrowane połączenie (TLS) oraz autentykację 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; • 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
Oprogramowanie do zarządzania	<ul style="list-style-type: none"> • Możliwość zainstalowania oprogramowania producenta do zarządzania, spełniającego poniższe wymagania: <ul style="list-style-type: none"> ○ 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

	<ul style="list-style-type: none"> ○ Szybki podgląd stanu środowiska ○ Podsumowanie stanu dla każdego urządzenia ○ Szczegółowy status urządzenia/elementu/komponentu ○ Generowanie alertów przy zmianie stanu urządzenia. ○ Filtry raportów umożliwiające podgląd najważniejszych zdarzeń ○ Integracja z service desk producenta dostarczonej platformy sprzętowej ○ Możliwość przejęcia zdalnego pulpitu ○ Możliwość podmontowania wirtualnego napędu ○ Kreator umożliwiający dostosowanie akcji dla wybranych alertów ○ Możliwość importu plików MIB ○ Przesyłanie alertów „as-is” do innych konsol firm trzecich ○ Możliwość definiowania ról administratorów ○ Możliwość zdalnej aktualizacji oprogramowania wewnętrznego serwerów ○ Aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania) ○ Możliwość instalacji oprogramowania wewnętrznego bez potrzeby instalacji agenta ○ Możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów ○ Moduł raportujący pozwalający na wygenerowanie następujących informacji: nr seryjne sprzętu, konfiguracja poszczególnych urządzeń, wersje oprogramowania wewnętrznego, obsadzenie slotów PCI i gniazd pamięci, informację o maszynach wirtualnych, aktualne informacje o stanie i poziomie gwarancji, adresy IP kart sieciowych, występujących alertów, MAC adresów kart sieciowych, stanie poszczególnych komponentów serwera. ○ Możliwość tworzenia sprzętowej konfiguracji bazowej i na jej podstawie weryfikacji środowiska w celu wykrycia rozbieżności. ○ Wdrażanie serwerów, rozwiązań modularnych oraz przełączników sieciowych w oparciu o profile ○ Możliwość migracji ustawień serwera wraz z wirtualnymi adresami sieciowymi (MAC, WWN, IQN) między urządzeniami. ○ Tworzenie gotowych paczek informacji umożliwiających zdiagnozowanie awarii urządzenia przez serwis producenta. ○ Zdalne uruchamianie diagnostyki serwera. ○ Dedykowana aplikacja na urządzenia mobilne integrująca się z wyżej opisanymi oprogramowaniem zarządzającym. ○ Oprogramowanie dostarczane jako wirtualny appliance dla KVM, ESXi i Hyper-V.
Certyfikaty	<p>Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015, ISO-50001 oraz ISO-14001</p> <p>Serwer musi posiadać deklaracja CE.</p> <p>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, Microsoft Windows Server</p>

	2025. Wsparcie dla ESXi 8.
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.
Warunki gwarancji	<p>5 lat gwarancji producenta, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia.</p> <p>Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie, przez Internet oraz z wykorzystaniem aplikacji.</p> <p>Zgłoszenie przyjęte jest potwierdzane przez zespół pomocy technicznej (mail/telefon/portal) przez nadanie unikalnego numeru zgłoszenia pozwalającego na identyfikację zgłoszenia w trakcie realizacji naprawy i po jej zakończeniu.</p> <p>Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia oraz pobieranie uaktualnień mikro kodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji serwera.</p> <p>Zamawiający oczekuje nieodpłatnego udostępnienia narzędzi serwisowych i procesów wsparcia umożliwiających: Wykrywanie usterek sprzętowych z predykcją awarii.</p> <p>Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wsparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego.</p> <p>Firma serwisująca musi posiadać ISO 9001:2015 oraz ISO-27001 na świadczenie usług serwisowych oraz posiadać autoryzację producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty.</p>

7. Oprogramowanie do wirtualizacji

1. Licencja na 96 rdzeni, oprogramowanie dostarczone w formie subskrypcji ze wsparciem technicznym producenta na 5 lat 24/7 NBD.
2. Warstwa wirtualizacji musi być zainstalowana bezpośrednio na sprzęcie fizycznym bez dodatkowych pośredniczących systemów operacyjnych.
3. Rozwiązanie musi zapewnić możliwość obsługi wielu instancji systemów operacyjnych na jednym serwerze fizycznym i powinno się charakteryzować maksymalnym możliwym stopniem konsolidacji sprzętowej.
4. Oprogramowanie do wirtualizacji musi zapewniać możliwość stworzenia dysku maszyny wirtualnej o wielkości 62 TB.
5. Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych z możliwością przydzielenia 24 TB pamięci operacyjnej RAM.
6. Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych, z których każda może mieć 1-10 wirtualnych kart sieciowych.
7. Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych, z których każda może mieć 32 porty szeregowy.
8. Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych, z których każda może mieć 20 portów USB.
9. Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych, z których każda może mieć 4 GB pamięci graficznej.
10. Rozwiązanie musi umożliwiać łatwą i szybką rozbudowę infrastruktury o nowe usługi bez spadku wydajności i dostępności pozostałych wybranych usług.
11. Rozwiązanie powinno w możliwie największym stopniu być niezależne od producenta platformy sprzętowej.

12. Rozwiązanie musi wspierać następujące systemy operacyjne: Windows 7/8/10/11, Windows Server, Amazon Linux 2, macOS, OS X, Asianux, Ubuntu, CentOS, NeoKylin, Debian, FreeBSD, Oracle Linux, RHEL, SUSE, Photon OS.
13. Rozwiązanie musi umożliwiać przydzielenie większej ilości pamięci RAM dla maszyn wirtualnych niż fizyczne zasoby RAM serwera w celu osiągnięcia maksymalnego współczynnika konsolidacji.
14. Oprogramowanie do wirtualizacji powinno zapewnić możliwość wykonywania kopii migawkowych instancji systemów operacyjnych (tzw. snapshot) na potrzeby tworzenia kopii zapasowych bez przerywania ich pracy.
15. Rozwiązanie musi umożliwiać udostępnienie maszynie wirtualnej większej ilości zasobów dyskowych niż jest fizycznie zarezerwowane na dyskach lokalnych serwera lub na macierzy.
16. System musi posiadać funkcjonalność wirtualnego przełącznika sieciowego 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.
17. Pojedynczy wirtualny przełącznik musi posiadać możliwość przyłączania do niego dwóch i więcej fizycznych kart sieciowych, aby zapewnić bezpieczeństwo połączenia ethernetowego w razie awarii karty sieciowej.
18. Wirtualne przełączniki muszą obsługiwać wirtualne sieci lokalne (VLAN).
19. Polityka licencjonowania musi umożliwiać przenoszenie licencji na oprogramowanie do wirtualizacji pomiędzy serwerami różnych producentów z zachowaniem wsparcia technicznego i zmianą wersji oprogramowania na niższą (downgrade). Wsparcie techniczne musi być świadczone bezpośrednio przez producenta oprogramowania. Licencjonowanie nie może odbywać się w trybie OEM.
20. Oprogramowanie zarządzające musi posiadać możliwość przydzielania i konfiguracji uprawnień z możliwością integracji z usługami katalogowymi, w szczególności Microsoft Active Directory, Open LDAP.
21. Rozwiązanie musi posiadać wbudowany interfejs programistyczny (API) zapewniający pełną integrację zewnętrznych rozwiązań wykonywania kopii zapasowych z istniejącymi mechanizmami warstwy wirtualizacyjnej.
22. Rozwiązanie musi zapewniać mechanizm replikacji wskazanych maszyn wirtualnych pomiędzy różnymi systemami pamięci masowych.
23. Rozwiązanie musi zawierać funkcjonalność pozwalającą na ominięcie testów inicjalizacyjnych sprzętu fizycznego w celu szybkiego startu wirtualizatora.
24. Rozwiązanie musi zawierać możliwość zabezpieczania maszyn wirtualnych przez rozwiązania antywirusowe firm trzecich bez konieczności instalacji agenta wewnątrz maszyny wirtualnej.
25. Rozwiązanie musi mieć możliwość przenoszenia maszyn wirtualnych w czasie ich pracy, bez jakiegokolwiek przestoju i bez utraty danych, pomiędzy serwerami fizycznymi, niezależnie od dostępności współdzielonej przestrzeni dyskowej,
26. Rozwiązanie musi mieć możliwość przenoszenia maszyn wirtualnych w czasie ich pracy, bez jakiegokolwiek przestoju i bez utraty danych, pomiędzy zasobami dyskowymi, niezależnie od dostępności współdzielonej przestrzeni dyskowej,
27. Rozwiązanie musi mieć możliwość przenoszenia maszyn wirtualnych w czasie ich pracy, bez jakiegokolwiek przestoju i bez utraty danych, jednocześnie między serwerami fizycznymi oraz zasobami dyskowymi, niezależnie od dostępności współdzielonej przestrzeni dyskowej.
28. Musi zostać zapewniona odpowiednia redundancja i taki mechanizm (wysokiej dostępności HA), aby w przypadku awarii lub niedostępności serwera fizycznego wybrane przez administratora i uruchomione nim wirtualne maszyny zostały uruchomione na innych serwerach z zainstalowanym oprogramowaniem wirtualizacyjnym. 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.

29. Rozwiązanie musi zapewniać wsparcie dla wirtualizacji zagnieżdżonej, w szczególności w zakresie możliwości zastosowania wszystkich funkcjonalności w tym Hyper-V systemu Windows Server na maszynie wirtualnej.
30. Rozwiązanie musi zapewniać możliwość dodawania zasobów w czasie pracy maszyny wirtualnej, w szczególności w zakresie ilości procesorów, pamięci operacyjnej i przestrzeni dyskowej.
31. Oprogramowanie do wirtualizacji musi zapewniać mechanizm takiego zabezpieczenia wybranych przez administratora wirtualnych maszyn, aby w przypadku awarii lub niedostępności serwera fizycznego maszyny, które na nim pracowały, były bezprzerwowo dostępne na innym serwerze z zainstalowanym oprogramowaniem wirtualizacyjnym. Mechanizm ten umożliwia zabezpieczenie maszyn wirtualnych wyposażonych w minimum 2 wirtualne procesory.

8. Oprogramowanie do kopii zapasowej

1. Licencja na 15 maszyn wirtualnych, permanentna, na 5 lat ze wsparciem 24/7 NBD.
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 Peer Insights: 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, 2022 i 2025. Wszystkie funkcjonalności w specyfikacji muszą być dostępne na wszystkich wspieranych platformach wirtualizacyjnych, chyba, że wyszczególniono inaczej
4. Oprogramowanie musi współpracować z infrastrukturą Nutanix w wersji 6.5.x - 7.0, Red Hat Virtualization 4.4 SP1, Oracle Linux Virtualization 4.5.4 lub nowszy oraz Proxmox VE 8.2 lub nowszy.
5. Oprogramowanie musi zapewniać tworzenie kopii zapasowych z sieciowych urządzeń plikowych NAS opartych o SMB, CIFS i/lub NFS, obiektowych pamięci masowych kompatybilnych z Microsoft Azure, Microsoft Azure Data Lake, AWS S3 i urządzeń kompatybilnych z protokołem S3 oraz bezpośrednio z serwerów plikowych opartych o Windows i Linux.
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 co najmniej trzech pamięci masowych to takiej puli.
11. Oprogramowanie musi pozwalać na przechowywanie kopii bezpieczeństwa w chmurze producenta.
12. 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.

13. Oprogramowanie musi wspierać niezmiennosc kopii zapasowych na potrzeby ochrony przed ransomware poprzez niedopuszczenie do usunięcia lub modyfikacji kopii zapasowej w zadanym okresie czasu.
14. Oprogramowanie nie może instalować żadnych stałych agentów wymagających wdrożenia czy upgradowania wewnątrz maszyny wirtualnej dla jakichkolwiek funkcjonalności backupu lub odtwarzania
15. 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)
16. Oprogramowanie musi zapewniać możliwość delegacji uprawnień do odtwarzania na portalu
17. Oprogramowanie musi mieć możliwość integracji z innymi systemami poprzez wbudowane RESTful API
18. Oprogramowanie musi mieć wbudowane mechanizmy backupu konfiguracji w celu prostego odtworzenia systemu po całkowitej reinstalacji
19. 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
20. Oprogramowanie musi posiadać mechanizmy chroniące przed utratą hasła szyfrowania
21. Oprogramowanie musi posiadać architekturę klient/serwer z możliwością instalacji wielu instancji konsoli administracyjnych.
22. Oprogramowanie musi posiadać natywne mechanizmy uwierzytelniania wieloskładnikowego (MFA) w celu dostępu do konsoli administracyjnej
23. Oprogramowanie musi wymagać autoryzacji dwóch administratorów backupu do wykonania krytycznych operacji (np skasowanie backupu, dodanie kolejnego administratora)
24. Oprogramowanie musi posiadać integracje z systemami zarządzania kluczami szyfrującymi (KMS)
25. Oprogramowanie musi posiadać integracje z systemami typu SIEM
26. Oprogramowanie musi posiadać asystenta produktu opartego o AI, pozwalającego na przeszukiwanie dokumentacji technicznej. Powinna istnieć możliwość wyłączenia tej opcji.
27. Oprogramowanie musi wykorzystywać mechanizmy Change Block Tracking na wszystkich wspieranych platformach wirtualizacyjnych. Mechanizmy muszą być certyfikowane przez dostawcę platformy wirtualizacyjnej
28. Oprogramowanie musi wykorzystywać mechanizmy śledzenia zmienionych plików przy zabezpieczaniu udziałów plikowych.
29. 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 conajmniej dla platformy VMware i Hyper-V
30. 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.
31. Oprogramowanie musi posiadać wsparcie dla VMware vSAN potwierdzone odpowiednią certyfikacją VMware.
32. Oprogramowanie musi wspierać kopiowanie backupów oraz zasobów plikowych na taśmy (LTO oraz IBM 3592).
33. Oprogramowanie musi mieć możliwość tworzenia retencji GFS (Grandfather-Father-Son)
34. Oprogramowanie musi wspierać bezpośrednią integrację z urządzeniami deduplikacyjnymi. Minimalnie wsparcie wymagane dla Dell DataDomain, HPE StoreOnce, ExaGrid, Fujitsu CS800, Quantum DXi oraz Infinidat InfiniGuard.

35. 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.
36. Oprogramowanie musi mieć możliwość kopiowania backupów oraz replikacji wirtualnych maszyn z wykorzystaniem wbudowanej akceleracji WAN.
37. 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.
38. Oprogramowanie musi mieć możliwość replikacji ciągłej, opartej o VMware VAAI, włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere. Dla replikacji ciągłej musi być możliwość zdefiniowania dziennika pozwalającego na odzyskanie danych z dowolnego punktu w ramach ustalonego parametru RPO.
39. Oprogramowanie musi umożliwiać przechowywanie punktów przywracania dla replik
40. Oprogramowanie musi umożliwiać wykorzystanie istniejących w infrastrukturze wirtualnych maszyn jako źródła do dalszej replikacji (replica seeding)
41. Oprogramowanie musi wykorzystywać wszystkie oferowane przez hypervisor tryby transportu (sieć, hot-add, LAN Free-SAN)
42. 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.
43. Dodatkowo dla środowiska vSphere, Hyper-V i Nutanix AHV powyższa funkcjonalność powinna umożliwiać uruchamianie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna)
44. 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
45. Oprogramowanie musi pozwalać na zaprezentowanie pojedynczego dysku bezpośrednio z kopii zapasowej do wybranej działającej maszyny wirtualnej vSphere
46. Oprogramowanie musi pozwalać na uruchomienie zasobów plikowych SMB oraz baz danych MS SQL, Oracle i PostgreSQL bezpośrednio ze skompresowanego i skompresowanego pliku backupu. Dodatkowo wspierana musi być migracja on-line tak uruchomionych zasobów na środowisko produkcyjne.
47. Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny, plików konfiguracji i dysków
48. Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny bezpośrednio do Microsoft Azure, Microsoft Azure Stack, Amazon EC2 oraz Google Cloud Platform.
49. 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
50. 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.
51. Oprogramowanie musi wspierać odtwarzanie pojedynczych plików z systemów Windows, Linux, BSD, Solaris, Mac, Novell
52. Oprogramowanie musi wspierać przywracanie plików z partycji Linux LVM

53. Oprogramowanie musi umożliwiać szybkie granularne odtwarzanie obiektów aplikacji bez użycia jakiegokolwiek agenta zainstalowanego wewnątrz maszyny wirtualnej.
54. 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.
55. Oprogramowanie musi pozwalać na backup i odtwarzanie usługi Entra ID. W szczególności użytkowników, grupy, role, jednostki administracyjne, enterprise applications oraz logi audytowe i sign-in.
56. 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.
57. 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.
58. 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.
59. 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.
60. 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.
61. Oprogramowanie musi wspierać granularne odtwarzanie baz danych MongoDB. Funkcjonalność ta musi być dostępna dla baz uruchomionych w środowiskach Linux.
62. Oprogramowanie musi wspierać granularne odtwarzanie baz danych SAP HANA do oryginalnej lub innej lokalizacji
63. Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez Oracle RMAN
64. Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez SAP HANA, SAP Oracle
65. Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez MS SQL VDI
66. Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez IBM Db2
67. Oprogramowanie musi wspierać także specyficzne metody odtwarzania w tym "reverse CBT" oraz odtwarzanie z wykorzystaniem sieci SAN
68. 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 uruchomienie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna)
69. Dla VMware'a oprogramowanie musi pozwalać na uruchomienie takiego środowiska dla replik maszyn wirtualnych
70. 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

71. 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.
72. Oprogramowanie musi posiadać swój wbudowany program antywirusowy zoptymalizowany do przeszukiwania kopii backupowych
73. Oprogramowanie musi analizować indeksy systemów plików zabezpieczanych maszyn w poszukiwaniu rozszerzeń, notatek żądania okupu oraz innych oznak obecności ransomware/malware
74. Oprogramowanie musi mieć możliwość skanowania plików backupu przy pomocy znanych sygnatur złośliwego oprogramowania
75. Oprogramowanie, bazując na wyuczonym modelu maszynowym (machine learning) musi w locie wykrywać oznaki złośliwego oprogramowania (malware, ransomware) oraz cyberataków
76. Oprogramowanie musi posiadać mechanizm wykrywania oznak ataku hakerskiego tzw Indicators of Compromise
77. Oprogramowanie musi umożliwiać dwuetapowe, automatyczne, odtwarzanie maszyn wirtualnych z możliwością wstrzyknięcia dowolnego skryptu przed odtworzeniem danych do środowiska produkcyjnego.
78. Oprogramowanie musi mieć możliwość integracji z innymi systemami bezpieczeństwa - minimum Splunk, Palo Alto Networks XSOAR
79. System musi zapewnić możliwość monitorowania środowiska wirtualizacyjnego opartego na VMware vSphere i Microsoft Hyper-V bez potrzeby korzystania z narzędzi firm trzecich
80. 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 konsolę vCenter Server lub pracujące samodzielnie
81. System musi umożliwiać monitorowanie środowiska wirtualizacyjnego Microsoft Hyper-V 2012, 2012R2, 2016, 2019, 2022 oraz 2025 zarówno w wersji darmowej jak i zawartej w płatnej licencji Microsoft Windows Server zarządzane poprzez System Center Virtual Machine Manager lub pracujące samodzielnie.
82. System musi umożliwiać kategoryzację obiektów infrastruktury wirtualnej niezależnie od hierarchii stworzonej w vCenter
83. System musi umożliwiać tworzenie alarmów dla całych grup wirtualnych maszyn jak i pojedynczych wirtualnych maszyn
84. System musi dawać możliwość układania terminarza raportów i wysyłania tych raportów przy pomocy poczty elektronicznej w formacie HTML oraz Excel
85. System musi dawać możliwość podłączenia się do kilku instancji vCenter Server i serwerów Hyper-V jednocześnie, w celu centralnego monitorowania wielu środowisk
86. System musi mieć wbudowane predefiniowane zestawy alarmów wraz z możliwością tworzenia własnych alarmów i zdarzeń przez administratora
87. System musi mieć wbudowane połączenie z bazą wiedzy opisującą problemy z predefiniowanych alarmów
88. System musi mieć centralną konsolę z sumarycznym podglądem wszystkich obiektów infrastruktury wirtualnej (ang. Dashboard)
89. System musi mieć możliwość monitorowania platformy sprzętowej, na której jest zainstalowana infrastruktura wirtualna
90. System musi zapewnić możliwość podłączenia się do wirtualnej maszyny (tryb konsoli) bezpośrednio z narzędzia monitorującego
91. System musi mieć możliwość integracji z oprogramowaniem do tworzenia kopii zapasowych tego samego producenta

92. System musi mieć możliwość monitorowania obciążenia serwerów backupowych, ilości zabezpieczanych danych oraz statusu zadań kopii zapasowych, replikacji oraz weryfikacji odzyskiwalności maszyn wirtualnych.
93. 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.
94. System musi mieć możliwość granularnego monitorowania infrastruktury, zależnego od uprawnień nadanym użytkownikom dla platformy VMware
95. 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
96. System musi umożliwiać raportowanie środowiska wirtualizacyjnego Microsoft Hyper-V 2012, 2012R2, 2016, 2019, 2022 oraz 2025 zarówno w wersji darmowej jak i zawartej w płatnej licencji Microsoft Windows Server zarządzane poprzez System Center Virtual Machine Manager lub pracujące samodzielnie.
97. System musi wspierać wiele instancji vCenter Server i Microsoft Hyper-V jednocześnie bez konieczności instalowania dodatkowych modułów.
98. System musi być systemem bezagentowym. Nie dopuszcza się możliwości instalowania przez system agentów na monitorowanych hostach ESXi i Hyper-V
99. System musi mieć możliwość eksportowania raportów do formatów Microsoft Word, Microsoft Excel, Microsoft Visio, Adobe PDF
100. System musi mieć możliwość ustawienia harmonogramu kolekcji danych z monitorowanych systemów jak również możliwość tworzenia zadań kolekcjonowania danych ad-hoc
101. System musi mieć możliwość ustawienia harmonogramu generowania raportów i dostarczania ich do odbiorców w określonych przez administratora interwałach
102. System w raportach musi mieć możliwość uwzględniania informacji o zmianach konfiguracji monitorowanych systemów
103. System musi mieć możliwość generowania raportów z dowolnego punktu w czasie zakładając, że informacje z tego czasu nie zostały usunięte z bazy danych
104. System musi posiadać predefiniowane szablony z możliwością tworzenia nowych jak i modyfikacji wbudowanych
105. System musi mieć możliwość analizowania „przeszacowanych” wirtualnych maszyn wraz z sugestią zmian w celu optymalnego wykorzystania fizycznej infrastruktury
106. System musi mieć możliwość generowania raportów na podstawie danych uzyskanych z oprogramowania do tworzenia kopii zapasowych tego samego producenta
107. System musi mieć możliwość generowania raportu dotyczącego zabezpieczanych maszyn, zdefiniowanych zadań tworzenia kopii zapasowych oraz replikacji jak również wykorzystania zasobów serwerów backupowych.
108. System musi mieć możliwość generowania raportu planowania pojemności (capacity planning) bazującego na scenariuszach ‘what-if’.
109. System musi mieć możliwość granularnego raportowania infrastruktury, zależnego od uprawnień nadanym użytkownikom dla platformy VMware
110. System musi mieć możliwość generowania raportów dotyczących tzw. migawek-sierot (orphaned snapshots)
111. System musi mieć możliwość generowania personalizowanych raportów zawierających informacje z dowolnych predefiniowanych raportów w pojedynczym dokumencie

9. Wdrożenie i dokumentacja

1. Fizyczna instalacja urządzeń w miejscu wskazanym przez Zamawiającego. Zamawiający dysponuje szafami RACK oraz ma przygotowane wyprowadzenie zasilania dla urządzeń.
2. Okablowanie urządzeń dla ruchu LAN, SAN i zarządzanie:
 - a. Podłączenie LAN ma być wykonane do istniejącej infrastruktury sieciowej Zamawiającego. Zamawiający dysponuje przełącznikami sieciowymi z portami o przepustowości 10Gb SFP+ / 25Gb SFP28 i wkładkami optycznymi w ilości odpowiedniej dla oferowanej infrastruktury.
 - b. Podłączenie SAN serwerów do macierzy ma być wykonane bezpośrednio bez urządzeń pośredniczących.
 - c. Podłączenie dla zarządzania portami miedzianymi do przełączników będących w posiadaniu Zamawiającego.
 - d. W ramach dostarczonych urządzeń należy dostarczyć wszelkie okablowanie miedziane i optyczne oraz wkładki optyczne potrzebne do podłączenia urządzeń w sposób redundanty dla ruchu LAN i SAN oraz dla ruchu systemów zarządzania.
3. Instalacja i inicjalizacja macierzy dyskowej w sposób zalecany i udokumentowany przez producenta macierzy. W procesie instalacji zasoby dyskowe macierzy mają być zostać udostępnione do serwerów do wirtualizacji jako współdzielone zasoby do przechowywania maszyn wirtualnych. Ilości oraz wielkości zostaną ustalone z Zamawiającym podczas wdrożenia.
4. Instalacja i konfiguracja oprogramowanie do wirtualizacji w sposób zalecany i udokumentowany przez producenta:
 - a. Utworzenie klastra HA przy pomocy dostarczonych serwerów.
 - b. Konfiguracja oprogramowania w taki sposób aby awaria pojedynczego połączenia LAN, SAN nie powodowała utraty komunikacji do zasobów macierzy i sieci.
5. Instalacja i konfiguracja oprogramowanie kopii zapasowych w sposób zalecany i udokumentowany przez producenta:
 - a. Instalacja i konfiguracja serwera kopii zapasowej.
 - b. Instalacja i konfiguracja serwera repozytorium z funkcjonalnością IMMUTABLE/WORM.
 - c. Instalacja i konfiguracja biblioteki taśmowej oraz jej podłączenie do serwera kopii zapasowej.
6. Dokumentacja konfiguracji, topologii połączeń i poświadczeń dla wdrożonych systemów.

Pozostałe wymagania dotyczące przedmiotu zamówienia:

1. Dostarczony sprzęt będący przedmiotem umowy musi być fabrycznie nowy (nieużywany).
2. Dostarczony sprzęt będący przedmiotem umowy musi posiadać wszystkie niezbędne kable, zasilacze oraz inne akcesoria niezbędne do jego prawidłowej pracy.
3. Sterowniki/oprogramowanie do urządzeń będą dostarczone na osobnych nośnikach.
4. Wszystkie urządzenia dostarczone przez Wykonawcę muszą pochodzić z autoryzowanego kanału sprzedaży producenta na rynek polski lub Unii Europejskiej.
5. Dostarczony sprzęt musi posiadać oznakowanie CE.
6. Całość przedmiotu zamówienia musi być objęta gwarancją Wykonawcy na okres **60 miesięcy**.
7. W przypadku pojawienia się wątpliwości co do pochodzenia oferowanego sprzętu, jego właściwości, parametrów technicznych, oznaczeń czy też funkcjonalności, Zamawiający zastrzega sobie prawo do wezwania Wykonawców do składania wyjaśnień, w tym do

przedstawiania dokumentów uwiarygadniających powyższe, a także prawo do żądania próbek testowych tego sprzętu.

8. Niedozwolone jest oferowanie sprzętu polegające na działaniu de-brandingu, ponieważ działanie to stanowi czyn nieuczciwej konkurencji. Oferty w których sprzęt został poddany działaniu usunięcia, zastąpienia lub w jakikolwiek inny sposób przerobienia oznaczeń mających na celu ukrycie lub wprowadzenie w błąd co do pochodzenia, jakości, czy właściwości sprzętu będą odrzucane.