Deduplikator ilość: 1 szt

Lp.	Parametr wymagany
1.	Urządzenie musi być przeznaczone do deduplikacji i przechowywania kopii zapasowych. Urządzenie musi spełniać wymagania wyspecyfikowane w niniejszej tabeli.
2.	Dostarczone urządzenie musi oferować minimalną przestrzeń 12 TB netto (powierzchni użytkowej dostępnej po założeniu systemu plików) i musi być skalowalne do minimum 170 TB netto, z możliwością dalszej rozbudowy, jeżeli wymagana przez Zamawiającego przestrzeń dyskowa wzrośnie.
3.	Dostarczone urządzenie musi umożliwiać rozbudowę o warstwę typu cloud, dedykowaną do długotrwałego przechowywania danych (tzw. Long Term Retention), zgodnie z polityką retencyjną Zamawiającego. Dane o określonej retencji powinny być migrowane (w postaci zdeduplikowanej) bezpośrednio na dodatkową warstwę typu cloud, bez pośrednictwa dodatkowych urządzeń fizycznych typu gateway, co zapewnia wysoką wydajność, bezpieczeństwo oraz minimalizuje ryzyko awarii lub opóźnień w procesie migracji. Wymagane jest wsparcie dla dowolnej platformy chmurowej (publicznej, prywatnej lub hybrydowej), spełniającej wymogi bezpieczeństwa, dostępności oraz skalowalności, z zapewnieniem szyfrowania danych na warstwie cloud. Przykładowymi platformami mogą być AWS, Microsoft Azure, Google Cloud Platform (GCP), przy czym dopuszczalne są inne rozwiązania o podobnych funkcjonalnościach. Należy dostarczyć licencję na przestrzeń minimum 60 TB netto dla warstwy cloud. Wymagana funkcjonalność musi być w pełni kompatybilna z oprogramowaniem Veeam Backup and Replication.
4.	Oferowane urządzenie musi posiadać co najmniej: 4 porty 10Gb/s Ethernet (wraz z dostawą 4 kabli 10GbE AOC o długości 3m), Możliwość obsługi protokołów CIFS, NFS oraz deduplikacji na źródle za pośrednictwem każdego z tych portów. Możliwość rozszerzenia konfiguracji o 2 porty Fibre Channel 16Gb/s, Wymagana obsługa protokołów VTL oraz deduplikacji na źródle za pośrednictwem portów Fibre Channel.
5.	Oferowane urządzenie musi umożliwiać jednoczesny dostęp za pomocą następujących protokołów: CIFS oraz NFS, oraz zapewniać deduplikację na źródle, z wymaganym wsparciem dla Veeam Backup and Replication.
7.	Oferowane pojedyncze urządzenie musi osiągać zagregowaną wydajność (dla maksymalnej konfiguracji) przy użyciu protokołu NFS na poziomie co najmniej 10 TB/h oraz co najmniej 20 TB/h z wykorzystaniem deduplikacji na źródle.
8.	Urządzenie musi umożliwiać jednoczesną obsługę co najmniej 250 strumieni danych, w tym: co najmniej 150 strumieni dla zapisu, co najmniej 50 strumieni dla odczytu, co najmniej 50 strumieni dla replikacji. Strumienie muszą pochodzić z różnych aplikacji oraz obsługiwać różne protokoły (np. CIFS, NFS, deduplikacja na źródle) oraz różne interfejsy (takie jak Fibre Channel, Ethernet), zapewniając jednoczesną obsługę w różnych protokołach i interfejsach. Urządzenie musi obsługiwać deduplikację in-line, tj. przed zapisem na dysk, zgodnie z opisem zawartym w niniejszej specyfikacji.
9.	Oferowane urządzenie musi deduplikować dane in-line przed zapisem na nośnik dyskowy. Na wewnętrznych dyskach urządzenia nie mogą być zapisywane dane w oryginalnej postaci (niezdeduplikowanej) z jakiegokolwiek fragmentu strumienia danych przychodzącego do urządzenia.

10.	Oferowane urządzenie deduplikacyjne musi wykorzystywać algorytm deduplikacji oparty na zmiennym, dynamicznym bloku o maksymalnej wielkości nie większej niż 12 kB. Algorytm ten musi samoczynnie dostosowywać się do strumienia danych, dzieląc dane na bloki o różnej wielkości w zależności od zawartości. Wielkość każdego bloku musi być dynamicznie ustalana przez algorytm deduplikacji, bez konieczności predefiniowania długości bloków dla poszczególnych typów danych.
11.	Oferowane urządzenie musi zapewniać deduplikację in-line, która odbywa się przed zapisem danych na nośnik dyskowy. Zapisowi muszą podlegać wyłącznie unikalne bloki danych, bez zapisywania oryginalnych danych w niezdeduplikowanej formie. Urządzenie musi obsługiwać globalną deduplikację dla danych przesyłanych za pomocą różnych protokołów (CIFS, NFS, VTL), co oznacza, że dane zapisane w jednej lokalizacji lub protokole nie mogą zostać ponownie zapisane w innej lokalizacji lub protokole, jeśli już istnieją w systemie. Deduplication in-line musi działać automatycznie i niezależnie od zewnętrznych aplikacji backupowych.
13.	Proponowane rozwiązanie nie może w żadnej fazie procesu korzystać (w całości lub częściowo) z bufora na składowanie danych w postaci oryginalnej (niezdeduplikowanej). Deduplikacja musi być realizowana w trybie in-line, co oznacza, że żadne dane nie mogą być zapisywane w niezdeduplikowanej formie w celu ich późniejszej deduplikacji.
14.	Wszystkie unikalne bloki przed zapisaniem na dysk muszą być dodatkowo kompresowane.
15.	Tryb zapisu zabezpieczanych danych nie może umożliwiać nadpisywania danych, dane mogą być zapisywane jedynie w trybie append-only, dane dla których wygasła retencja powinny zostać usunięte podczas procesu czyszczenia tzw. Cleaning, wymaganie dotyczy wszystkich danych zapisanych na urządzeniu a nie wybranych grup danych objętych działaniem blokad zabezpieczających przed usunięciem/modyfikacją danych.
16.	Urządzenie musi wspierać deduplikację na źródle przy backupach realizowanych za pomocą Veeam Backup & Replication, NetWorker oraz Microsoft SQL Server (przy wykorzystaniu SQL Server Management Studio). Deduplication na źródle musi odbywać się na poziomie następujących komponentów: Veeam B&R: na poziomie proxy Data Mover, NetWorker: na poziomie Client, Microsoft SQL: na poziomie serwera SQL. Wszystkie nowe, unikalne bloki danych, które nie znajdują się jeszcze na urządzeniu, muszą być przesyłane przez sieć Fibre Channel (FC). Deduplication musi zapewniać, że przez sieć LAN będą transmitowane jedynie te fragmenty danych, które nie znajdują się jeszcze na urządzeniu
18.	Oferowane urządzenie musi umożliwiać uruchamianie maszyn wirtualnych VMware bezpośrednio z danych backupowych, bez konieczności ich uprzedniego odtwarzania. Funkcjonalność ta musi być wspierana zarówno przez oprogramowanie Veeam Backup & Replication, jak i NetWorker.
19.	Oferowane urządzenie musi posiadać funkcjonalność Load Balancing oraz Link Failover dla portów sieciowych wykorzystywanych przez aplikację backupową. Funkcjonalność ta musi być wspierana przez oprogramowanie Veeam Backup & Replication oraz NetWorker, zapewniając wysoką dostępność i optymalizację przesyłu danych podczas operacji backupu.
20.	Oferowane urządzenie musi wspierać backupy typu Virtual Synthetics w przypadku oprogramowania Veeam Backup & Replication oraz NetWorker. Funkcjonalność ta musi umożliwiać tworzenie syntetycznych pełnych kopii zapasowych bez konieczności ponownego odczytu pełnych danych z serwerów źródłowych, przy jednoczesnym wykorzystaniu istniejących bloków danych na urządzeniu backupowym.
21.	W przypadku deduplikacji na źródle realizowanej poprzez sieć IP (LAN oraz WAN), urządzenie musi umożliwiać szyfrowanie komunikacji z użyciem klucza o długości minimum 256 bitów, zapewniając ochronę przesyłanych danych podczas ich transferu.
22.	Urządzenie musi umożliwiać zaszyfrowanie przechowywanych danych. Wymagane są licencje umożliwiające zaszyfrowanie oraz przechowywanie zaszyfrowanych danych w obrębie maksymalnej pojemności oferowanego urządzenia.
23.	Urządzenie musi wspierać deduplikację na źródle poprzez sieć FC (SAN) minimum dla następujących systemów operacyjnych: Windows, Linux (RedHat, SuSE).

24.	Oferowane urządzenie musi umożliwiać bezpośrednią replikację danych do drugiego urządzenia tego samego typu. Konfiguracja replikacji musi być możliwa w każdym z następujących trybów: jeden do jednego, wiele do jednego, jeden do wielu, kaskadowej (urządzenie A replikuje dane do urządzenia B, a urządzenie B replikuje te same dane do urządzenia C). Replikacja musi odbywać się w trybie asynchronicznym, przy czym transmitowane mogą być jedynie te fragmenty danych (bloki), które nie znajdują się jeszcze na docelowym urządzeniu. Ewentualne licencje na replikacje są przedmiotem postępowania.
25.	Urządzenie musi umożliwiać wydzielenie określonych portów Ethernet dedykowanych wyłącznie do realizacji operacji replikacji danych.
26.	W przypadku wykorzystania portów Ethernet do replikacji, urządzenie musi umożliwiać realizację następujących operacji za pomocą tych samych portów: przyjmowanie backupów, odtwarzanie danych, przyjmowanie strumienia replikacji oraz wysyłanie strumienia replikacji.
27.	W przypadku replikacji danych między dwoma urządzeniami oferowanego typu, wymagana jest możliwość kontroli przez NetWorker oraz Microsoft SQL Server Management Studio. Muszą być jednocześnie spełnione następujące funkcjonalności: Replikacja odbywa się bezpośrednio między dwoma urządzeniami bez udziału serwerów pośredniczących. Replikacji podlegają tylko te fragmenty danych (na poziomie bloków używanych do deduplikacji), które nie znajdują się na docelowym urządzeniu. Replikacja zarządzana jest z poziomu wymaganego oprogramowania. Aplikacja posiada informację o obydwu kopiach zapasowych znajdujących się w obu urządzeniach bez konieczności przeprowadzania procesu inwentaryzacji.
28.	Oferowane urządzenie musi działać poprawnie przy zapełnieniu danymi na poziomie co najmniej 90%.
29.	Oferowane urządzenie musi posiadać mechanizm umożliwiający ograniczenie pasma używanego do replikacji między dwoma urządzeniami oferowanego typu. Urządzenie powinno umożliwiać zarządzanie stopniem wykorzystania dostępnego pasma na potrzeby replikacji, pozwalając na dostosowanie przepustowości w celu optymalizacji przesyłu danych.
30.	Zdeduplikowane i skompresowane dane przechowywane w obrębie podsystemu dyskowego urządzenia muszą być chronione za pomocą technologii RAID 6 lub równoważnej, zapewniającej ochronę danych w przypadku awarii dysków.
31.	Oferowane urządzenie musi umożliwiać realizację oraz przechowywanie SnapShot'ów, czyli umożliwiać zamrożenie obrazu danych (stanu backupów) w urządzeniu na określoną chwilę. Ponadto, urządzenie musi również umożliwiać odtworzenie danych ze SnapShot'u, zapewniając dostęp do zamrożonego obrazu danych w dowolnym momencie. Odtworzenie danych ze SnapShot'u nie może wymagać nadpisania danych produkcyjnych, ani powodować przerw w normalnej pracy urządzenia, w tym przyjmowania lub odtwarzania backupów.
32.	Urządzenie musi umożliwiać przechowywanie minimum 500 Snapshotów jednocześnie w obrębie oferowanej przestrzeni, przy zachowaniu globalnej deduplikacji oraz standardowego trybu pracy urządzenia, co oznacza możliwość korzystania ze wszystkich dostępnych funkcjonalności bez obniżenia wydajności systemu.
33.	Urządzenie musi umożliwiać podział na logiczne części, przy czym dane znajdujące się w każdej logicznej części muszą być deduplikowane globalnie między sobą. Oznacza to, że deduplikacja musi obejmować wszystkie logiczne części urządzenia, zapewniając, że żaden fragment danych nie zostanie zapisany więcej niż raz, niezależnie od tego, w której logicznej części urządzenia znajduje się dana informacja.

34.	Urządzenie musi mieć możliwość podziału na minimum 10 logicznych części pracujących równolegle. Producent musi oficjalnie wspierać pracę co najmniej 10 logicznych części pracujących równolegle z pełną wydajnością urządzenia, zapewniając brak spadków wydajności podczas równoczesnego działania wszystkich logicznych jednostek.
35.	Dla każdej z wymienionych logicznych części oferowanego urządzenia musi istnieć możliwość zdefiniowania oddzielnego użytkownika zarządzającego daną logiczną częścią deduplikatora. Użytkownicy przypisani do zarządzania logiczną częścią A muszą mieć dostęp wyłącznie do zasobów tej części (A) i nie mogą widzieć ani mieć dostępu do zasobów innych logicznych części oferowanego urządzenia.
36.	Oferowane urządzenie musi umożliwiać zaprezentowanie każdej z logicznych części urządzenia jako niezależnego urządzenia, dostępnego za pośrednictwem następujących protokołów i mechanizmów: CIFS, NFS, VTL, deduplikacja na źródle.
37.	Urządzenie musi umożliwiać zdefiniowanie blokady skasowania danych (funkcjonalność WORM), która chroni pliki przed ich usunięciem lub modyfikacją przez określony czas. Blokada musi działać w dwóch trybach, wybieranych przez administratora: Możliwość zdjęcia blokady przed upływem okresu ważności danych. Brak możliwości zdjęcia blokady przed upływem okresu ważności danych (COMPLIANCE), zgodnie z normami SEC 17a-4(f), ISO 15489-1 lub równoważnymi normami dotyczącymi ochrony danych. Licencje na blokadę usunięcia lub zmiany przechowywanych plików muszą być dostarczone wraz z urządzeniem. Urządzenie musi również automatycznie aktywować blokadę WORM podczas zapisu danych na obszary objęte tą blokadą oraz umożliwiać stosowanie WORM dla danych uzyskanych przez funkcjonalność SnapShot.
38.	Urządzenie musi umożliwiać przechowywanie danych niezmienialnych, takich jak: Video, Grafika, Nagrania dźwiękowe, Pliki PDF na udziałach CIFS/NFS.
39.	Urządzenie musi weryfikować dane po zapisie (nie dotyczy to weryfikacji danych indeksowych generowanych przez urządzenie, ale weryfikacji wszystkich zabezpieczanych danych backupowych). Każda zapisana porcja danych musi być odczytana i porównana z danymi otrzymanymi przez urządzenie. Weryfikacja musi być realizowana w locie, czyli przed usunięciem z pamięci oryginalnych danych otrzymanych z aplikacji backupowej, i musi być wykonywana w trybie ciągłym. Wydajność urządzenia musi uwzględniać tę funkcjonalność.
40.	Urządzenie musi automatycznie usuwać przeterminowane dane (bloki danych, które nie należą już do backupów o aktualnej retencji) w procesie czyszczenia, zapewniając efektywne zarządzanie przestrzenią dyskową oraz optymalizację zasobów przechowywania.
41.	Proces usuwania przeterminowanych danych (czyszczenia) nie może uniemożliwiać ani zakłócać pracy procesów backupu oraz odtwarzania danych (zapisu/odczytu danych z zewnątrz do systemu). Proces czyszczenia musi być realizowany w tle, zapewniając ciągłość operacji backupowych oraz pełną dostępność systemu dla operacji związanych z zapisem i odczytem danych.
42.	Urządzenie musi umożliwiać zdefiniowanie maksymalnego poziomu obciążenia procesora przez proces usuwania przeterminowanych danych (czyszczenia). Konfiguracja ta musi pozwalać na ograniczenie wpływu procesu czyszczenia na ogólną wydajność urządzenia.

43.	Urządzenie musi umożliwiać zdefiniowanie harmonogramu, według którego wykonywany jest proces usuwania przeterminowanych danych (czyszczenia). Proces ten musi być realizowany równolegle z operacjami backupu, odtwarzania danych oraz replikacji, zapewniając ciągłość działania wszystkich operacji systemu.
44.	Zamawiający wymaga, aby operacja usuwania przeterminowanych danych (czyli danych, które przekroczyły okres retencji) była przeprowadzana regularnie, co najmniej raz na tydzień lub zgodnie z harmonogramem dostosowanym do obciążenia systemu i optymalizacji przestrzeni dyskowej. Proces usuwania danych powinien minimalizować wpływ na bieżące operacje, takie jak tworzenie kopii zapasowych oraz odtwarzanie danych, zgodnie z możliwościami technicznymi systemu.
45.	Urządzenie musi umożliwiać realizację procesu pierwszego czyszczenia dopiero po przekroczeniu 75% zajętości oferowanej przestrzeni dyskowej. Funkcjonalność ta musi być zintegrowana systemowo, bez konieczności korzystania z zewnętrznych narzędzi lub oprogramowania.
46.	Urządzenie musi umożliwiać zarządzanie za pomocą: Interfejsu graficznego dostępnego z poziomu przeglądarki internetowej, Linii komend (CLI) dostępnej z poziomu ssh (Secure Shell).
47.	Oprogramowanie do zarządzania musi rezydować na oferowanym urządzeniu deduplikacyjnym. Wszystkie operacje zarządzania urządzeniem, w tym obsługa interfejsu graficznego oraz CLI, muszą być wykonywane lokalnie, bez konieczności instalowania zewnętrznego oprogramowania zarządzającego na dodatkowych serwerach lub komputerach.
48.	Oferowane urządzenie musi posiadać możliwość sprawdzenia pakietu upgrade'ującego firmware za pomocą interfejsu GUI lub CLI. Funkcjonalność ta powinna umożliwiać weryfikację, czy instalacja nowej wersji systemu nie spowoduje problemów z działaniem urządzenia, zanim aktualizacja zostanie wdrożona.
49.	Oferowane urządzenie musi być rozwiązaniem kompletnym, typu appliance, pochodzącym od jednego producenta. Zamawiający nie dopuszcza stosowania rozwiązań typu gateway, ze względu na możliwość wystąpienia problemów z wydajnością, kompatybilnością, zarządzaniem oraz wsparciem technicznym, co może prowadzić do zwiększonych kosztów eksploatacji oraz ryzyka utraty integralności systemu. Oferowane urządzenie musi być oficjalnie dostępne w ofercie producenta przed datą ukazania się niniejszego postępowania.
50.	Oferowane urządzenie musi być objęte minimum 60-miesięczną gwarancją producenta, działającym w trybie zgłaszania awarii 24x7, z reakcją na zgłoszenie NBD (Next Business Day).

Serwer backupu ilość: 1 szt

Parametr	Charakterystyka (wymagania minimalne)
Obudowa	Obudowa Rack o wysokości max 1U z możliwością instalacji min. 8 dysków 2.5" wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych. Obudowa z możliwością wyposażenia w panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS'u, zasilaniu oraz temperaturze.
Płyta główna	Płyta główna z możliwością zainstalowania do dwóch procesorów. Obsługa procesorów 32 rdzeniowych. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym. Na płycie głównej powinno znajdować się minimum 16 slotów przeznaczonych do instalacji pamięci. Płyta główna powinna obsługiwać do 1TB pamięci RAM.
Chipset	Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych.
Procesor	Jeden procesor 8-rdzeniowy, min. 2.6GHz, umożliwiający osiągnięcie wyniku min. 169 w teście SPECrate2017_int_base, dla oferowanego serwera, dostępnym na stronie www.spec.org w konfiguracji dwuprocesorowej
RAM	Minimum 64GB DDR5 RDIMM 4800MT/s,

Funkcjonalność pamięci RAM	Demand Scrubing, Patrol Scrubing, Permanent Fault Detection
Interfejsy sieciowe/FC/SAS	Wbudowane minimum 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT oraz minimum 2 interfejsy sieciowe 10Gb Ethernet w standardzie BaseT
Dyski twarde	Zainstalowane minimum 4x dysk SAS o pojemności min. 1.2TB, 12Gb, 2,5“ Hot-Plug. Zainstalowane minimum 2 x dysk M.2 NVMe SSDs o pojemności min. 480GB Hot-Plug z możliwością konfiguracji RAID 1.
Kontroler RAID	Sprzętowy kontroler dyskowy, posiadający Minimum 8GB nieulotnej pamięci cache, Możliwość konfiguracji poziomów RAID: 0, 1, 5, 6, 10, 50, 60. Wsparcie dla dysków samoszyfrujących
Wbudowane porty	minimum 4 x USB z czego nie mniej niż 1x USB 3.0, minimum 2x VGA
Video	Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości minimum 1920x1200
Zasilacze	Redundantne, Hot-Plug minimum 1100W klasy Redundantne, Hot-Plug minimum 1100W klasy Titanium
System operacyjny	Zamawiający wymaga, aby dostarczony serwer był wyposażony w system operacyjny i środowisko wspierające instalację oraz pełną integrację z oprogramowaniem Veeam Backup & Replication, z zachowaniem kompatybilności z platformą wirtualizacji VMware lub równoważną. Środowisko to musi umożliwiać zarządzanie kopiami zapasowymi oraz odtwarzanie maszyn wirtualnych bez potrzeby używania emulatorów. Wymagane jest również wsparcie dla zaawansowanych funkcji zarządzania zdalnego, failover clustering oraz funkcji bezpieczeństwa, takich jak ochrona tożsamości i szyfrowanie danych na poziomie systemu operacyjnego.
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 Serwer musi być wyposażony w rozwiązanie zapewniające ochronę oprogramowania układowego przed manipulacją złośliwego oprogramowania. Ochrona ta musi spełniać wymagania bezpieczeństwa zgodne z wytycznymi NIST SP 800-147B i NIST SP 800-155 lub równoważnymi, zapewniającymi porównywalny poziom bezpieczeństwa. Zamawiający wymaga, aby dostarczony serwer posiadał mechanizmy kryptograficzne, które poświadczają integralność oprogramowania BIOS (Root of Trust) lub równoważne rozwiązania, które gwarantują wysoki poziom ochrony integralności BIOS-u.
	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;

Karta Zarządzania	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) SSL/TSL
Oprogramowanie do zarządzania	Możliwość zainstalowania oprogramowania producenta do zarządzania, spełniającego poniższe wymagania: Oprogramowanie musi wspierać zarządzanie serwerami, urządzeniami sieciowymi oraz pamięciami masowymi różnych producentów, zgodnie z wymaganiami standardów komunikacyjnych Oprogramowanie musi umożliwiać integrację z systemami katalogowymi opartymi na protokole LDAP, takimi jak Active Directory, w celu autoryzacji i zarządzania uprawnieniami użytkowników lub równoważnymi rozwiązaniami, które umożliwiają zbliżony poziom zarządzania tożsamością i dostępem. Oprogramowanie do zarządzania musi oferować możliwość zarządzania serwerami bez konieczności instalacji dedykowanego agenta na serwerach, z wykorzystaniem standardowych protokołów komunikacyjnych (np. IPMI, Redfish) Oprogramowanie do zarządzania musi wspierać standardowe protokoły do zarządzania sprzętem, takie jak SNMP, IPMI, SSH (dla systemów Linux), Redfish lub równoważne Oprogramowanie musi umożliwiać automatyczne wykrywanie zarządzanych urządzeń w oparciu o harmonogram, z możliwością dostosowania częstotliwości skanowania Oprogramowanie do zarządzania musi zapewniać szczegółowe raporty na temat wykrytych urządzeń, w tym informacje o komponentach sprzętowych, wersjach oprogramowania i stanie urządzeń Oprogramowanie do zarządzania musi umożliwiać eksportowanie raportów w formatach otwartych (CSV, HTML, PDF) oraz kompatybilnych z oprogramowaniem biurowym (XLS). 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. 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. Oprogramowanie dostarczane jako wirtualny appliance dla KVM, ESXi i Hyper-V.
Certyfikaty	Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015, ISO-50001 oraz ISO-14001 Serwer musi posiadać deklaracja CE. Serwer musi spełniać wymagania normy NIST SP 800-193 ochrony przed cyberatakami lub równoważnej normy dotyczącej bezpieczeństwa oprogramowania układowego 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.
Dokumentacja użytkownika	Zamawiający wymaga dokumentacji w języku polskim lub angi*e* lskim.
Warunki gwarancji	Oferowane urządzenie musi być objęte minimum 60-miesięczną gwarancją producenta, działającym w trybie zgłaszania awarii 24x7, z reakcją na zgłoszenie NBD (Next Business Day).