Załącznik Nr 2
do SWZ nr SZPZOZ/TP/03/2026
z dnia 13.08.2026 roku

SPECYFIKACJA TECHNICZNA

I. Serwer – 4 szt.

1. Typu RACK, wysokość nie więcej niż 1U;
2. Szyny umożliwiające wysunięcie serwera z szafy stelażowej;
3. Obudowa musi umożliwiać zainstalowania 10 dysków twardych hot plug 2,5” SATA/SAS;
4. Możliwość rozbudowy o panel diagnostyczny z wyświetlaczem LCD umożliwiającym detekcję usterek umożliwiający wyświetlenie następujących informacji:
   4.1 aktywne ostrzeżenia;
   4.2 status serwera;
   4.3 typ oraz model serwera, numer seryjny;
   4.4 wersje oprogramowania UEFI oraz modułu zarządzania;
   4.5 informacje modułu zarządzania: nazwa hosta, adres MAC, adres IP, adres DNS;
   4.6 dane środowiskowe: temperaturę procesora, poziom napięcia wejściowego, poziom zużycia energii;
   4.7 aktywne sesje połączeniowe do interfejsu zarządzania;
5. Zainstalowane 2 szt. dysków Hot-Swap SSD NVMe 960GB, dyski skonfigurowane w RAID-1 podłączone do sprzętowego kontrolera RAID;
6. Płyta główna
   6.1 Dwuprocesorowa;
   6.2 Płyta główna dedykowana przez producenta serwera do oferowanego modelu urządzenia, dystrybuowana i wspierana bezpośrednio przez niego pod unikalnym numerem katalogowym. Wymaga się, aby kod źródłowy oprogramowania układowego (BIOS/UEFI) oraz wszelkie jego aktualizacje były autoryzowane, rozwijane i udostępniane bezpośrednio przez producenta serwera;

6.3 Możliwość instalacji procesorów 86-rdzeniowych;

6.4 Moduł TPM 2.0;

6.5 2 złącza PCI Express Gen5 x16 w tym minimum 1 złącze Full-Height;

6.6 32 gniazda pamięci RAM;

6.7 Obsługa pamięci CXL 2.0

6.8 Obsługa 8 TB pamięci operacyjnej RAM DDR5;

6.9 Wsparcie dla zaawansowanych technologii ochrony i korekcji pamięci RAM przed błędami wielobitowymi na poziomie pojedynczych układów pamięci, a także technologii lustrzanego odbicia pamięci.

6.10 Wewnętrzny slot na kartę Micro SD

7. Procesory

7.1 Jeden procesor 16-rdzeniowy, taktowanie bazowe 3,2 GHz, architektura x86_64;

7.2 osiągający w teście SPEC CPU2017 Floating Point 5 minimum 535 pkt (wynik osiągnięty dla zainstalowanych dla dwóch procesorów). Wynik musi być opublikowany na stronie http://spec.org dla oferowanego serwera.

8. Pamięć RAM

8.1 128GB pamięci RAM;

8.2 DDR5 Registered 6400MT/s;

9. Kontrolery LAN

9.1 Interfejsy LAN, nie zajmujące slotów PCI Express (OCP):

a) 2x 10/25Gbit SFP28 obsadzone modułami 10/25Gbit LC;

b) 1x 1G Base-T dedykowany do zarządzania serwerem w trybie OOB;

9.2 Interfejsy LAN, w slotach PCI Express:

a) 2x 10/25Gbit SFP28 obsadzone modułami 10/25Gbit LC;

10. Porty

10.1 Zintegrowana karta graficzna posiadająca 16MB pamięci rozdzielczość 1920x1200 przy 60 Hz, ze złączem VGA z tyłu serwera, możliwość zainstalowania portu cyfrowego (DP lub HDMI)

10.2 Dwa porty USB 5Gb/s dostępne z tyłu serwera;

10.3 Dwa opcjonalne porty USB 5Gbp/s na panelu przednim;

10.4 Opcjonalny port USB 5Gbp/s wewnętrzny;

10.5 Jeden z opcjonalnych frontowych portów USB musi posiadać możliwość zarządzania serwerem;

10.6 Dedykowany port do zarządzania i diagnostyki dostępny z przodu serwera;

10.7 Opcjonalny port serial;

10.8 Ilość dostępnych złącz USB nie może być osiągnięta poprzez stosowanie zewnętrznych przejściówek, rozgałęziaczy czy dodatkowych kart rozszerzeń zajmujących jakikolwiek slot PCI Express i/lub USB serwera.

11. Zasilanie, chłodzenie

11.1 Redundantne zasilacze hotplug o sprawności 96% (tzw. klasa Titanium) o mocy 1300W;

11.2 Redundantne wentylatory hotplug dające gwarancję poprawnego działania serwera w temperaturze otoczenia nie przekraczającej 30 stopni celsjusza;

12. Bezpieczeństwo

12.1 Możliwość automatycznego przywrócenia BIOS do wspieranej wersji w przypadku wykrycia nieautoryzowanej modyfikacji;

12.2 Wbudowany w BIOS mechanizm umożliwiający usunięcie konfiguracji kart zarządzających, BIOS oraz danych ze wszystkich wewnętrznych urządzeń pamięci masowej;

12.3 Czujnik otwarcia obudowy zintegrowany z modułem zarządzania serwerem;

12.4 Fizyczne zabezpieczenie (np. na klucz lub elektrozamek) uniemożliwiające fizyczny dostęp do dysków twardych;

12.5 Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z systemu zarządzania serwerem;

12.6 Możliwość wyłączenia w BIOS funkcji przycisku zasilania;

12.7 Możliwość ustawienia hasła włączania serwera;

12.8 Możliwość ustawienia hasła administratora;

12.9 Możliwość przewidywania awarii dla procesorów, regulatorów napięcia, pamięci, dysków wewnętrznych, wentylatorów, zasilaczy, kontrolerów RAID;

13. Zarządzanie

13.1 Wymaga się aby serwer posiadał diody sygnalizujące awarię przy każdej kości pamięci RAM, każdej zatoce dyskowej, każdym zasilaczu.

13.2 Możliwość instalacji serwera oraz serwisowania (instalacji oraz deinstalacji) komponentów takich jak: riser PCIe, backplane dysków twardych, kart rozszerzeń, wentylatorów, bez użycia dodatkowych narzędzi mechanicznych;

13.3 Możliwość użycia aplikacji mobilnej na telefonie (iOS lub Android), do przeglądania awarii, konfigurowania ustawień i włączenia/wyłączenia serwera. Podłączenie telefonu odbywa się poprzez opcjonalny dedykowany port USB na froncie serwera.

13.4 Funkcjonalność kontrolera zdalnego zarządzania:

13.4.1 Monitoring stanu systemu (komponenty objęte monitoringiem to przynajmniej: CPU, pamięć RAM, dyski, karty PCI, zasilacze, wentylatory, płyta główna)

13.4.2 Uzyskanie następujących informacji o serwerze: nazwa, typ i model, numer seryjny, nazwa systemu, wersja UEFI oraz BMC, adres IP karty zarządzającej, utylizacja CPU, utylizacja pamięci oraz komponentów I/O

13.4.3 Logowanie zdarzeń systemowych oraz związanych z działaniami użytkownika- każdy dziennik zdarzeń powinien mieć możliwość zapisu co najmniej 1024 rekordów.

13.4.4 Logowanie zdarzeń związanych z utrzymaniem systemu jak upgrade firmware, zmiana/instalacja sprzętu - system powinien umożliwiać zapisanie minimum 250 zdarzeń.

13.4.5 Wysyłanie określonych zdarzeń poprzez SMTP oraz SNMPv3

13.4.6 Update systemowego firmware

13.4.7 Monitoring i możliwość ograniczenia poboru prądu

13.4.8 Zdalne włączanie/wyłączanie/restart

13.4.9 Zapis video zdalnych sesji

13.4.10 Podmontowanie lokalnych mediów z wykorzystaniem Java client

13.4.11 Przekierowanie konsoli szeregowej przez IPMI

13.4.12 Zrzut ekranu w momencie zawieszenia systemu

13.4.13 Możliwość przejęcia zdalnego ekranu

13.4.14 Możliwość zdalnej instalacji systemu operacyjnego

13.4.15 Alerty Syslog

13.4.16 Przekierowanie konsoli szeregowej przez SSH

13.4.17 Wsparcie dla dynamic DNS

13.4.18 Wyświetlanie danych aktualnych i historycznych dla zużycia energii oraz temperatury serwera

13.4.19 Wirtualna konsola z dostępem do myszy, klawiatury;

13.4.20 Montowanie obrazów ISO bez instalacji dodatkowych komponentów Java czy AciveX (musi działać w oparciu o HTML5)

13.4.21 Możliwość mapowania obrazów ISO przez HTTPS, SFTP, CIFS oraz NFS

13.4.22 Możliwość jednoczesnej pracy do 6 użytkowników przez wirtualną konsolę

13.4.23 wspierane protokoły/interfejsy: IPMI v2.0, SNMP v3, CIM, DCMI v1.5, REST API

13.4.24 Możliwość wykorzystania opcjonalnego frontowego portu USB do celów serwisowych (komunikacja portu z karta zarządzającą) bez możliwości uzyskania jakiejkolwiek funkcjonalności na poziomie zainstalowanego systemu operacyjnego. Funkcjonalność ta musi być realizowana na poziomie sprzętowym i musi być niezależna od zainstalowanego systemu operacyjnego.

13.4.25 Kontroler zarządzania musi posiadać 4GB wewnętrznej pamięci (dopuszcza się zastosowanie karty Micro SD w celu uzyskania tej pojemności). Pamięć kontrolera zarządzania musi pełnić funkcję RDOC (Remote Disc on Card) oraz musi umożliwiać przechowywanie plików firmware.

13.4.26 Monitorowanie zmian sprzętowych w celu wykrycia nieoczekiwanych zmian. Po wykryciu zmiany zapis w logu serwera lub uniemożliwienie boot'u.

13.4.27 Możliwość synchronizacji konfiguracji i poziomów firmware pomiędzy serwerami.

13.4.28 Możliwość monitorowania i zarządzania grupą serwerów z poziomu kontrolera zarządzania pojedynczego serwera. Ilość serwerów możliwych do zarządzania – minimum 20.

13.5 Opcjonalne oprogramowanie producenta serwera do zarządzania, spełniające poniższe wymagania (możliwość zakupienia licencji lub subskrypcji w przyszłości) :

13.5.1 Wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych

13.5.2 Integracja z Active Directory

13.5.3 Możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta w systemie operacyjnym

13.5.4 Automatyczne rozpoznawanie nowych serwerów poprzez protokół SLP oraz SSDP

13.5.5 Szczegółowy opis wykrytych systemów oraz ich komponentów

13.5.6 Możliwość eksportu danych min do formatu CSV

13.5.7 Grupowanie urządzeń w oparciu o kryteria użytkownika

13.5.8 Możliwość wizualizacji rozmieszczenia serwerów i zarządzanych urządzeń w szafach RACK

13.5.9 Tworzenie automatycznie grup urządzeń w oparciu o elementy konfiguracji serwera np. nazwa, lokalizacja, system operacyjny, obsadzenie slotów PCIe, pozostałego czasu gwarancji czy stanu np. firmware czy BIOS

13.5.10 Szybki podgląd stanu środowiska

13.5.11 Podsumowanie stanu dla każdego urządzenia

13.5.12 Szczegółowy status urządzenia/elementu/komponentu

13.5.13 Filtry raportów umożliwiające podgląd najważniejszych zdarzeń

13.5.14 Integracja z service desk producenta dostarczonej platformy sprzętowej, pozwalając min weryfikację statusu i wysyłanie paczek diagnostycznych

13.5.15 Uruchomienie zdalnej konsoli graficznej serwera bezpośrednio z poziomu panelu oprogramowania, niezależnie od stanu systemu operacyjnego serwera.

13.5.16 Możliwość zamontowania wirtualnego napędu

13.5.17 Kreator umożliwiający dostosowanie akcji dla wybranych alertów

13.5.18 Przesyłanie alertów „as-is” do innych konsol firm trzecich

13.5.19 Możliwość definiowania ról administratorów

13.5.20 Możliwość zdalnej aktualizacji oprogramowania wewnętrznego serwerów

13.5.21 Aktualizacja oparta o repozytorium aktualizacji – budowanie repozytorium w sposób automatyczny ze stron producenta

13.5.22 Możliwość definiowania polityk aktualizacji (konkretne wersje firmware)

13.5.23 Automatyczna polityka aktualizacji „Najnowsze dostępne”

13.5.24 Możliwość instalacji oprogramowania wewnętrznego bez potrzeby instalacji agenta na systemie operacyjnym

13.5.25 Możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów

13.5.26 Tworzenie gotowych paczek informacji umożliwiających zdiagnozowanie awarii urządzenia przez serwis producenta

13.5.27 Możliwość tworzenia sprzętowej konfiguracji bazowej i na jej podstawie weryfikacji środowiska w celu wykrycia rozbieżności czy powielania konfiguracji na inne serwery czy backup aktualnej konfiguracji.

13.5.28 Wdrażanie serwerów, rozwiązań modularnych oraz przełączników sieciowych w oparciu o profile

13.5.29 Wykonanie restartu serwera i automatyczne wejście do BIOSu/UEFI

13.5.30 Zdalne bezpieczne usunięcie danych na dyskach SSD/HDD w serwerach

13.5.31 Dedykowana aplikacja na urządzenia mobilne integrująca się z wyżej opisanymi oprogramowaniem zarządzającym.

13.5.32 Monitorowanie i raportowanie historii (min. 24h) poboru mocy oraz temperatur serwera.

13.5.33 Oprogramowanie musi być dostarczone w postaci gotowego obrazu wirtualnego (Appliance) wspieranego przez środowiska: **KVM (w tym natywnie Proxmox VE)**, ESXi lub Hyper-V.

13.5.34 Oprogramowanie musi umożliwiać realizację poniższych funkcji **zarówno poprzez niezależną (samodzielną) konsolę zarządzającą Web HTML5, jak i poprzez dedykowane wtyczki (integracje)** do systemów zarządzania wirtualizacją (jeśli są wykorzystywane w infrastrukturze Zamawiającego, np. VMware vCenter / Windows Admin Center / API Proxmox VE):

14. Gwarancja

14.1 Dostarczony sprzęt serwerowy musi być objęty 36 miesięczną gwarancją producenta w trybie on-site z czasem zakończenia naprawy w 24H od zakończenia diagnostyki. Naprawa realizowana przez producenta serwera lub autoryzowany przez producenta serwis. Dyski twarde nie podlegają zwrotowi organizacji serwisowej.

14.2 Funkcja automatycznego zgłaszania usterek i awarii sprzętowych w helpdesk/servicedesk producenta sprzętu;

14.3 Firma serwisująca musi posiadać ISO 9001 na świadczenie usług serwisowych;

14.4 Możliwość odpłatnego wydłużenia gwarancji producenta do 7 lat w trybie onsite z gwarantowanym skutecznym zakończeniem naprawy serwera w 24h od zgłoszenia usterki (podać koszt na dzień składania oferty).

15. Uwagi

15.1 Elementy, z których zbudowane są serwery muszą być produktami producenta tych serwerów lub być przez niego certyfikowane oraz muszą być objęte gwarancją producenta, o wymaganym w specyfikacji poziomie SLA – wymagane oświadczenie wykonawcy lub producenta;

15.2 Serwer musi być fabrycznie nowy i pochodzić z oficjalnego kanału dystrybucyjnego w UE – wymagane oświadczenie wykonawcy lub producenta;

15.3 Serwis w wymaganym zakresie będzie świadczony przez producenta lub autoryzowany serwis producenta posiadający certyfikat ISO9001, w przypadku nie wywiązywania się z obowiązków gwarancyjnych oferenta lub firmy serwisującej, producent przejmie na siebie wszelkie zobowiązania związane z serwisem - wymagane oświadczenie producenta;

15.4 Ogólnopolska, telefoniczna infolinia/linia techniczna producenta serwera, w ofercie należy podać link do strony producenta na której znajduje się nr telefonu na który można zgłaszać usterki;

15.5 Możliwość aktualizacji i pobrania sterowników do oferowanego modelu serwera w najnowszych certyfikowanych wersjach bezpośrednio z sieci Internet za pośrednictwem strony www producenta serwera;

II. MACIERZ DYSKOWA WRAZ Z PÓŁKĄ DYSKOWĄ – 1 KOMPLET

1. System musi być dostarczony ze wszystkimi komponentami do instalacji w standardowej szafie rack 19” z zajętością maks. 4U w tej szafie. Każdy skonfigurowany moduł/obudowa musi posiadać układ nadmiarowy zasilania i chłodzenia, zapewniający bezprzerwową pracę macierzy bez ograniczeń czasowych w przypadku utraty redundancji w danym układzie (zasilania lub chłodzenia). Każdy moduł/obudowa powinien posiadać widoczne elementy sygnalizacyjne do informowania o stanie poprawnej pracy lub awarii.
2. Oferowana macierz musi obsługiwać rozbudowę do minimum 240 dysków hot-plug oraz umożliwiać zdefiniowanie minimum 1024 woluminów logicznych (LUN).

3. Macierz musi posiadać 4 porty SAS 12 Gb/s do podłączenia dodatkowych półek dyskowych.
4. Pojemność macierzy wraz z półką dyskową:

   4.1 Sześć sztuk dysków 1,9TB SSD-SAS lub NVMe

   4.2 Sześć sztuk dysków 4TB SAS, NL-SAS lub SSD SAS

5. Kontrolery

   5.1 Macierz musi być dostarczona z zainstalowanymi minimum 2 kontrolerami.

   5.2 Każdy z kontrolerów macierzy musi posiadać po minimum 64GB pamięci podręcznej Cache.

   5.3 W przypadku awarii zasilania dane niezapisane na dyski, przechowywane w pamięci kontrolera muszą być zabezpieczone za pomocą podtrzymania bateryjnego przez 72 godziny lub jako zrzut na pamięć flash.

   5.4 Macierz musi obsługiwać rozbudowę pamięci podręcznej cache dla operacji odczytu o minimum 4TB poprzez instalację dodatkowych modułów pamięci w kontrolerach lub wykorzystanie pojemności zainstalowanych dysków SSD.

   5.5 Macierz musi obsługiwać wymianę kontrolera RAID bez utraty danych zapisanych na dyskach.

   5.6 Macierz musi posiadać funkcjonalność automatycznego balansowania obciążenia kontrolerów macierzy przez przełączanie w trybie online volumenów logicznych pomiędzy nimi w zależności od wygenerowanego na nich ruchu. Musi istnieć możliwość wyłączenia tej funkcjonalności z poziomu interfejsu użytkownika.

   5.7 Każdy z kontrolerów RAID powinien posiadać dedykowany interfejs RJ-45 Ethernet obsługujący połączenia z prędkością minimum 1Gb/s dla zdalnej komunikacji z oprogramowaniem zarządzającym i konfiguracyjnym macierzy.

   5.8 Oferowana macierz musi mieć wyprowadzone 2 porty iSCSI 25Gbps (obsadzone modułami 10/25G LC MMF) do dołączenia serwerów bezpośrednio lub do sieci SAN na każdy kontroler RAID.

   5.9 Macierz musi umożliwiać dołożenie dodatkowych portów do transmisji danych:

      5.9.1 SAS 12 Gbps

      5.9.2 iSCSI 10Gbps Base-T

      5.9.3 FC 32Gbps

6. Poziomy RAID

6.1 Macierz musi zapewniać poziom zabezpieczenia danych na dyskach definiowany poziomami RAID: Raid-1, Raid-10, Raid-5, Raid-6

6.2 Obliczanie sum kontrolnych (kodów parzystości) dla grup dyskowych RAID5 i RAID6 musi być realizowane w sposób sprzętowy przez dedykowany układ w macierzy.

6.3 Macierz musi posiadać mechanizm tworzenia wirtualnej przestrzeni na dyskach macierzy wraz z wyliczaniem parzystości oraz podwójnej parzystości w celu zabezpieczenia danych. Mechanizm ten musi być przygotowany do optymalizacji procesów odtwarzania dysków pojemnościowych.

6.4 Macierz musi pozwalać na dynamiczną migrację pomiędzy poziomami RAID, czyli zmianę sposobu zabezpieczenia grupy dyskowej z jednego poziomu RAID na drugi.

7. Dyski

7. 1 Oferowana macierz musi wspierać dyski hot-plug:

7.1.1 Dyski SSD

7.1.2 HDD z interfejsem SAS12Gb/s

7.1.3 HDD o prędkości obrotowej 7,2 krpm, 10 krpm,

7.2 Macierz musi obsługiwać mieszaną konfigurację dysków hot-plug SSD i HDD zainstalowanych w dowolnym module rozwiązania.

7.3 Wszystkie dyski wspierane przez oferowany model macierzy muszą być wykonane w technologii hot-plug.

7.4 Macierz musi obsługiwać 120 dysków SAS SSD w całym rozwiązaniu, bez konieczności dokupowania/wymiany żadnych innych elementów sprzętowych czy licencyjnych innych niż same półki dyskowe wraz z dyskami.

7.5 Macierz musi posiadać oprogramowanie do monitoringu stanu dysków, które pozwala na identyfikowanie potencjalnie zagrożonych awarią dysków oraz z poziomu graficznego interfejsu do zarządzania musi być możliwość sprawdzenia stanu zużycia dysków SSD.

7.6 Macierz musi umożliwiać skonfigurowanie każdego zainstalowanego dysku hot-plug jako dysk hot-spare (dysk zapasowy).

7.7 W przypadku awarii dysku fizycznego i wykorzystania wcześniej skonfigurowanego dysku zapasowego, wymiana uszkodzonego dysku na sprawny

nie może powodować powrotnego kopiowania danych z dysku hot-spare na wymieniony dysk (tzw. CopyBackLess).

7.8 Macierz musi pozwalać na zaszyfrowanie danych na dedykowanych do tego dyskach kluczem AES256-bit zgodnie z wytycznymi Information Technology Laboratory przy National Institute of Standards and Technology (NIST).

7.9 Macierz musi posiadać możliwość skasowania wszystkich danych z dysku FDE celem bezpiecznego ponownego użycia w innym środowisku (Secure Erase).

8. Opcje programowe

8.1 Macierz musi być wyposażona w system kopii migawkowych umożliwiający wykonanie 256 kopii migawkowych z opcją rozbudowy do 512.

8.2 Macierz powinna umożliwiać podłączenie logiczne z minimum 50 serwerami.

8.3 Macierz musi umożliwiać aktualizację oprogramowania wewnętrznego kontrolerów RAID i dysków bez konieczności wyłączania macierzy oraz bez konieczności wyłączania ścieżek logicznych FC/iSCSI dla podłączonych stacji/serwerów.

8.4 Macierz musi umożliwiać dynamiczną zmianę rozmiaru wolumenów logicznych bez przerywania pracy macierzy i bez przerywania dostępu do danych znajdujących się na danym wolumenie.

8.5 Macierz musi posiadać wsparcie dla systemów operacyjnych:

8.5.1 Microsoft Windows Server 2019, 2022, 2025

8.5.2 SuSE Linux Enterprise Server 15, 12

8.5.3 Red Hat Linux Enterprise Server 9, 8

8.5.4 Vmware vSphere 7, 8;

8.6 Macierz musi być dostarczona z licencją na oprogramowanie wspierające technologię typu multipath (obsługa nadmiarowości dla ścieżek transmisji danych pomiędzy macierzą i serwerem) dla połączeń FC i iSCSI.

8.7 Macierz musi posiadać możliwość uruchamiania mechanizmów zdalnej replikacji danych, w trybie asynchronicznym i synchronicznym, bez konieczności stosowania zewnętrznych urządzeń konwersji. Funkcjonalność replikacji danych musi być zapewniona z poziomu oprogramowania wewnętrznego macierzy, jako tzw. storage-based data replication. Replikacja danych musi być obsługiwana w połączeniu macierzą z tej samej rodziny urządzeń wspierającą obsługę zdalnej replikacji danych - funkcjonalność opcjonalna, możliwość wykupienia opcji w przyszłości.

8.8 Macierz musi posiadać możliwość tworzenia lokalnych tj. w obrębie zasobów macierzy, pełnych kopii danych (tzw. klony danych).

8.9 Macierz musi obsługiwać mechanizmy Thin Provisioning, czyli przydziału dla obsługiwanych środowisk woluminów logicznych o sumarycznej pojemności większej od sumy pojemności dysków fizycznych zainstalowanych w macierzy. Macierz musi umożliwiać odzyskiwanie przestrzeni dyskowych po usuniętych danych w ramach wolumenów typu Thin.

9. Zarządzanie

9.1 Oprogramowanie do zarządzania musi być zintegrowane z systemem operacyjnym systemu pamięci masowej.

9.2 Komunikacja z wbudowanym oprogramowaniem zarządzającym macierzą musi być możliwa w trybie graficznym np. poprzez przeglądarkę WWW oraz w trybie tekstowym.

9.3 Musi być możliwe zdalne zarządzanie macierzą z wykorzystaniem standardowej przeglądarki internetowej (minimum Microsoft Edge, Google Chrome, Mozilla Firefox) bez konieczności instalacji dodatkowych aplikacji na stacji administratora.

9.4 Wbudowane oprogramowanie macierzy musi obsługiwać połączenia z modułem zarządzania macierzy poprzez szyfrowanie komunikacji protokołami: SSL dla komunikacji poprzez przeglądarkę WWW i protokołem SSH dla komunikacji poprzez CLI.

9.5 Wraz z system musi zostać dostarczone narzędzie do monitoringu macierzy w kontekście wydajności i opóźnień na wolumenach, wydajności I/Ops, MB/s, trafności w cache

9.6 Macierz musi posiadać możliwość integracji z Active Directory w zakresie definicji i mapowania grup i użytkowników pod kątem autentykacji.

10. Gwarancja i serwis

10.1 Całe rozwiązanie musi być objęte minimum 36 miesięcznym okresem gwarancji producenta macierzy z naprawą miejscu instalacji urządzenia i z gwarantowanym czasem zakończenia naprawy w 24h od zakończenia diagnostyki.

10.2 Uszkodzone dyski twarde nie podlegają zwrotowi organizacji serwisowej.

10.3 Serwis gwarancyjny musi obejmować dostęp do poprawek i nowych wersji oprogramowania wbudowanego, które są elementem zamówienia.

10.4 Macierz musi pochodzić z oficjalnego kanału sprzedaży producenta w UE. Nie dopuszcza się użycia macierzy odnawianych, demonstracyjnych lub powystawowych.

10.5 Urządzenie musi być wykonane zgodnie z europejskimi dyrektywami RoHS i WEEE stanowiącymi o unikaniu i ograniczaniu stosowania substancji szkodliwych dla zdrowia.

10.6 Serwis w wymaganym zakresie będzie świadczony przez producenta lub autoryzowany serwis producenta posiadający certyfikat ISO9001, w przypadku nie wywiązywania się z obowiązków gwarancyjnych oferenta lub firmy serwisującej, producent przejmie na siebie wszelkie zobowiązania związane z serwisem - wymagane oświadczenie producenta;

10.7 Producent oferowanej macierzy musi posiadać dedykowaną, ogólnie dostępną stronę internetową, gdzie po wpisaniu numeru seryjnego macierzy można zweryfikować co najmniej: czas i poziom oferowanego serwisu gwarancyjnego producenta zarówno dla macierzy jak i dowolnej z półek dyskowych, datę zakończenia wsparcia gwarancyjnego, datę zakończenia wsparcia producenta dla oferowanego urządzenia – w formularzu ofertowym należy podać adres internetowy strony producenta macierzy, gdzie można zweryfikować wymagane informacje.

III. PRZEŁĄCZNIKI – szt. 2

1. Stackowalny przełącznik warstwy 3 wspierający dynamiczny routing, wymagana obsługa: RIPv1/v2/ng, OSPFv2/v3,VRRP, ECMP, PIM-DM
2. Urządzenie musi być wyposażone w min. 24 portów SFP+ oraz min. sześć portów SFP28+. Nie są dopuszczane porty współdzielone tzw. „Combo”
3. Porty SFP/SFP+ muszą obsługiwać moduły o prędkości transmisji zarówno 1 jak i 10Gbps. Porty SFP28 muszą obsługiwać moduły o prędkości 1/10/25Gbps
4. Urządzenie musi posiadać port konsolowy RJ45 i/lub USB typu C
5. Urządzenie musi umożliwiać łączenie jednostek w stos za pomocą fizycznych połączeń. Nie dopuszcza się łączenia urządzeń w stos wirtualny (virtual stacking)
6. Do łączenia urządzeń w stos nie dopuszcza się złącz i/lub modułów w standardzie zastrzeżonym prawnie przez konkretnego producenta
7. Urządzenie musi posiadać port Ethernet umożliwiający zarządzanie out of band
8. Dopuszczane są jedynie urządzenia w architekturze nieblokującej, pracujące w trybie store-and-forward

9. Rozmiar tablicy adresów MAC urządzenia min. 128K
10. Przepustowość magistrali dla zadanej minimalnej ilości portów musi wynosić min. 820Gbps
11. Min. szybkość przekierowań pakietów 610 Mpps
12. Przełącznik musi posiadać bufor pakietów o rozmiarze min. 8MB
13. Urządzenie musi posiadać możliwość wymiany wszystkich zasilaczy oraz umożliwiać montaż min. 2 zasilaczy, nie dopuszcza się rozwiązania 1+1 gdzie tylko jeden z zasilaczy jest wymienny
14. Urządzenie musi posiadać wymienne wentylatory umożliwiające ich wymianę bez konieczności wyłączania urządzenia, tzw. „hot swap”
15. Przełącznik musi być w formacie 1U umożliwiającym jego montaż w standardowej szafie 19” oraz posiadać w zestawie odpowiednie uchwyty montażowe
16. Urządzenie musi spełniać następujące standardy: 802.3z, 802.3ab, 802.3ae, 802.3by, 802.3cc, 802.3ad, 802.3ah, 802.3x, 802.1ab, 802.1D, 802.1w, 802.1s, 802.1p, 802.1q
17. Wymaga się, aby urządzenie posiadało następujące funkcjonalności:

    17.1 Zarządzanie za pomocą przeglądarki poprzez interfejs http/https in band jak i out of band

    17.2 Zarządzanie z poziomu CLI (Telnet, SSH, port konsoli) - musi być możliwa konfiguracja wszystkich funkcji urządzenia

    17.3 RSPAN

    17.4 sFlow

    17.5 DDM

    17.6 ERPS

    17.7 Obsługę stosu IPv4 i IPv6

    17.8 Funkcję wykrywania pętli

    17.9 Funkcję izolacji portów

    17.10 Funkcję agregacji portów z wykorzystaniem protokołu LACP (min. 100 grup, do 8 portów w danej grupie agregacji)

    17.11 Obsługę protokołu LLDP/LLDP-MED.

    17.12 Funkcję DHCP Snooping zarówno dla IPv4 jak i IPv6

    17.13 Funkcję umożliwiającą powiązanie adresu IP z adresem MAC (zarówno dla IPv4 jak i IPv6)

17.14 Obsługę protokołu drzewa rozpinającego (STP/RSTP/MSTP)

17.15 Obsługę 4096 identyfikatorów VLAN

17.16 Funkcję umożliwiającą podwójne tagowanie ramek (QinQ VLAN)

17.17 Obsługę dla ramek Jumbo o rozmiarze min. 9K

17.18 Funkcję umożliwiającą automatyczne przypisywanie wyznaczonych urządzeń do konkretnej sieci VLAN (MAC VLAN)

17.19 IGMP Snooping oraz MLD Snooping

17.20 Obsługę min. 4000 grup multicastowych jednocześnie

17.21 MVR

17.22 Możliwość konfiguracji co najmniej 250 interfejsów IP

17.23 Obsługę min. 1000 tras statycznych dla funkcji routingu statycznego

17.24 Obsługę AAA z wykorzystaniem mechanizmów Radius oraz TACACS+

17.25 Uwierzytelnianie użytkowników z wykorzystaniem 802.1X w oparciu o adres MAC urządzenia

17.26 Obsługę list kontroli dostępu (ACL)

17.27 Obsługę SNMP w wersjach v1/v2c/v3

17.28 Obsługę grup RMON 1,2,3,9

18. Pozostałe wymagania:

18.1 Urządzenie musi posiadać certyfikację CE

18.2 Dostarczony sprzęt musi być objęty gwarancją min. 60 miesięcy

18.3 Urządzenie musi pochodzić z polskiego autoryzowanego kanału dystrybucyjnego producenta

18.4 Urządzenie wyposażone w dwa zasilacze redundantne typu hot-swap o mocy adekwatnej do pełnego pokrycia zapotrzebowania energetycznego urządzenia przy maksymalnym obciążeniu wszystkich portów

18.5 Urządzenie obsadzone oryginalnymi modułami SFP+/SFP28+ producenta urządzenia w ilości 12x 10GBase-SR LC, 4x 25GBase-SR LC, wyposażone w 2x 1m kabel SFP28 25G DAC oraz w kable potrzebne do połączenia zamawianego sprzętu serwerowego z przełącznikami i istniejącą siecią LAN.

IV. UPS – szt. 2

1. Topologia: podwójna konwersja on-line z systemem PFC (korekcja współczynnika mocy)
2. Obudowa: do montażu w szafie rack 19”, dołączony zestaw do montażu
3. Wartość znamionowa kVA/kW): min. 5 kVA / min. 4,5 kW
4. Sprawność: min. 94,2% w trybie online
5. Wejście: połączenie poprzez zaciski 3-przewodowe (1fazowy+N+uziemienie)
6. Wyjścia: min. 6x AC IEC320 10A, 4x AC IEC320 16A
7. Bypass: wewnętrzny tor obejściowy (automatyczny lub ręczny)
8. Porty komunikacyjne: LAN RJ45, COM SubD-9 (USV/V24)
9. Slot komunikacyjny: 1 slot z kartą sieciową Network w standardzie
10. Wyświetlacz: graficzny wyświetlacz LCD
11. Czas pracy: min. 3,9 min. przy pełnym obciążeniu
12. Gwarancja: min. 36 m-cy

V. Wymagania dotyczące oprogramowania wirtualizacyjnego, backupowego, instalacji i niezbędnych usług.

Wszystkie dostarczane urządzenia muszą zostać zainstalowanie w wyznaczonej przez Zamawiającego serwerowni wyposażonej w szafę serwerową. Podłączone zgodnie z najlepszymi praktykami zapewniającymi bezpieczeństwo i wydajność całego systemu.

1. Rodzaj wirtualizacji: system musi obsługiwać wirtualizację maszynową (sprzętową) oraz kontenerową (systemową, np. LXC, Docker lub równoważną) zarządzaną z poziomu graficznego interfejsu administracyjnego.
2. Maszyny wirtualne (sprzętowe)

3.1 Uruchamianie VM z systemami Linux, Windows, BSD.

3.2 Możliwość przydziału CPU i RAM z dokładnością do rdzeni/MB.

3.3 Obsługa wirtualnych dysków i interfejsów sieciowych, snapshotów, migracji „na żywo” i offline.

3. Kontenery:

   4.1 Uruchamianie kontenerów Linux z wydzielonymi zasobami CPU, RAM, dysk, I/O.

4. Tworzenie snapshotów, wsparcie dla sieci bridge/NAT/VLAN, kontenery nieuprzywilejowane.

5. Zarządzanie:

   6.1 Interfejs webowy umożliwiający pełną administrację hostami, VM, kontenerami, pamięcią masową i siecią.

6. Dostęp CLI i API do automatyzacji.

7. Klastrowanie i HA

   7.1 Możliwość tworzenia klastra z synchronizacją konfiguracji.

   7.2 Mechanizmy wysokiej dostępności VM i kontenerów, automatyczne przenoszenie w przypadku awarii węzła.

8. Pamięć masowa

   8.1 Obsługa lokalnych i sieciowych magazynów danych (NFS, iSCSI, Fibre Channel, SMB, RBD/Ceph).

   8.2 Thin provisioning, snapshoty i klonowanie obrazów dysków.

9. Sieć

   9.1 Mosty, agregacja interfejsów (bonding), VLAN.

   9.2 Wirtualne interfejsy dla VM i kontenerów, wbudowany firewall na poziomie hosta i VM.

10. Backup i replikacja

    10.1 Tworzenie kopii zapasowych VM i kontenerów „na żywo”.

    10.2 Harmonogramowanie backupów i replikacja między węzłami klastra.

11. Bezpieczeństwo

    11.1 Role i uprawnienia (RBAC), uwierzytelnianie lokalne i zewnętrzne (LDAP/AD).

    11.2 Szyfrowanie transmisji TLS i mechanizmy aktualizacji bezpieczeństwa.

12. Pozostałe

    12.1 System musi być oparty na oprogramowaniu, którego kod źródłowy jest publicznie dostępny online, co umożliwia weryfikację bezpieczeństwa, audyt oraz

dostosowanie funkcjonalności w ramach zgodnych z licencją mechanizmów lub dostarczone oprogramowanie musi posiadać udokumentowane, niezależne audyty bezpieczeństwa kodu oraz gwarantować brak ukrytych funkcjonalności (backdoorów) poprzez oficjalne deklaracje bezpieczeństwa producenta..

12.2 Zamawiający dopuszcza zaoferowanie systemu wirtualizacji opartego na architekturze innej niż KVM oraz systemie kontenerów innych niż LXC, pod warunkiem, że zaoferowane rozwiązanie umożliwia jednoczesne uruchamianie maszyn wirtualnych i kontenerów z poziomu jednej konsoli zarządzającej (Web GUI) bez potrzeby instalacji osobnych systemów zarządzania

12.3 Zaoferowany system backupu musi wspierać natywną integrację z oferowanym wirtualizatorem, umożliwiając wykonywanie kopii zapasowych bezagentowo (na poziomie hiperwizora) zarówno dla maszyn wirtualnych, jak i kontenerów, a także zapewniać mechanizmy deduplikacji danych u źródła (client-side deduplication).

13. Licencja

13.1 Model licencjonowania zgodny z polityką producenta (np. per Socket CPU).

Oferta musi obejmować odpowiednią liczbę subskrypcji pokrywającą wszystkie procesory (gniazda) w dostarczanym sprzęcie (serwery, macierze, przełączniki).

14. Instalacja, konfiguracja i uruchomienie:

14.1 Instalacja Systemu (Hypervisor)

14.1.1 Instalacja oprogramowania wirtualizacyjnego w najnowszej stabilnej wersji na wszystkich dostarczonych serwerach fizycznych, konfiguracja macierzy i pamięci masowej dla wirtualizacji.

14.1.2 Aktualizacja systemów do najnowszych wersji pakietów z repozytorium stabilnego przy użyciu dostarczonych subskrypcji.

14.1.3 Konfiguracja parametrów BIOS/UEFI serwerów pod kątem wirtualizacji (włączenie VT-x/AMD-V, wyłączenie stanów oszczędzania energii C-States dla maksymalnej wydajności, włączenie IOMMU).

14.1.4 Migracja maszyn wirtualnych ze środowiska VMWARE na nowe środowisko wirtualne

14.2 Instalacja oprogramowania backupu

14.2.1 Instalacja oprogramowania backupu na wyznaczonych urządzeniach. Konfiguracja podstawowego magazynu danych (Datastore) z wykorzystaniem natywnych mechanizmów blokowych macierzy rozproszonej (RBD). Rozwiązanie musi zapewniać wysoką wydajność operacji wejścia/wyjścia (I/O) oraz minimalizację parametru RTO (Restore Time Objective) poprzez bezpośrednią integrację warstwy backupu z klastrem obliczeniowym.

14.3 Konfiguracja Sieci

14.3.1 Konfiguracja przełączników sieciowych w celu zapewnienia redundancji i zwiększenia przepustowości.

14.3.2 Separacja ruchu: Logiczne wydzielenie ruchu sieciowego (np. poprzez VLAN lub dedykowane interfejsy) dla: - Zarządzania (Management), - Komunikacji klastrowej (mechanizmów synchronizacji stanu klastra i mechanizmów heart-beat), - Ruchu maszyn wirtualnych (VM Traffic), - Dostępu do pamięci masowej/replikacji.

14.4 Szkolenie dla administratora w zakresie obsługi dostarczonych urządzeń oraz oprogramowania wirtualizacyjnego i backupowego.

14.4.1 Celem usługi jest przekazanie wiedzy niezbędnej do zapewnienia bezpieczeństwa danych oraz ciągłości działania infrastruktury informatycznej. Z uwagi na ścisłą integrację systemu backupu z warstwą wirtualizacji, szkolenie obejmuje kompleksową obsługę systemu backupu oraz środowiska źródłowego (wirtualizatora), niezbędnego do przeprowadzenia skutecznych procedur odtwarzania po awarii (Disaster Recovery).

14.4.2 w zakresie szkolenia musi się znaleźć również obsługa dostarczanych urządzeń, konfiguracja i zarządzanie.

14.4.3 czas trwania min. 1 dzień/8h