**OPIS PRZEDMIOTU ZAMÓWIENIA**

1. **PRZEDMIOT ZAMÓWIENIA**

Przedmiotem zamówienia jest dostawa i instalację urządzeń/elementów wchodzących w skład platformy wirtualizacji wraz z 36 miesięczną gwarancją i przeprowadzeniem instruktażu.

Zadania realizowane w ramach zamówienia:

* 1. dostawa fabrycznie nowych urządzeń/elementów wraz z 36 miesięczną gwarancją oraz niezbędnymi do prawidłowego działania licencjami stanowiącymi platformę wirtualizacji do wskazanej przez Zamawiającego lokalizacji:
  2. instalacja, konfiguracja, testowanie i uruchomienie urządzeń/elementów wchodzących w skład platformy wirtualizacji oraz wykonanie dokumentacji i przeprowadzenie instruktażu dla administratorów platformy.
  3. Asysta techniczna w zakresie administracji zaoferowanym sprzętem oraz dostarczonym oprogramowaniem

1. **TERMIN REALIZACJI ZAMÓWIENIA**

Zadania w ramach zamówienia, będą realizowane w etapach zgodnie z poniższymi terminami

* 1. Etap I – realizacja zadań, o których mowa w pkt I. ppkt 1) termin realizacji zadań w ramach Etapu I - do 60 dni od daty zawarcia umowy

* 1. Etap II - realizacja zadań, o których mowa w pkt I ppkt 2), do 75 dni od daty od daty zawarcia umowy

1. **Minimalne wymagania platformy wirtualizacji będącej przedmiotem zamówienia**

Dostarczenie i instalacja platformy wirtualizującej będzie realizowana we wskazanej lokalizacji m. st. Warszawy. Sprzęt będący przedmiotem niniejszego zamówienia zostanie dostarczony do lokalizacji wskazanej przez Zamawiającego.

Zaoferowany sprzęt musi być fabrycznie nowy, przeznaczony do sprzedaży na rynku europejskim (zgodnie z ustawą z dnia 30.08.2002 r. o systemie oceny zgodności i z wydanymi na jej podstawie rozporządzeniami, wyprodukowany nie wcześniej niż w 2022 r. oraz objęty wymaganą przez Zamawiającego gwarancją w Polsce. Zamawiający nie dopuszcza produktów „odnawianych" (ang. Refurbished).

Zaoferowany sprzęt oraz oprogramowanie nie może być przeznaczone przez producenta do wycofania z produkcji lub sprzedaży.

Wszystkie podzespoły dostarczone z urządzeniami (serwery, macierz, przełączniki FC, przełączniki LAN), będą pochodziły od jednego producenta. Stosowane podzespoły muszą być wspierane przez producenta urządzeń i być objęte możliwością analizy potencjalnych błędów w trakcie potencjalnych zgłoszeń serwisowych. Muszą pochodzić z autoryzowanego kanału sprzedaży producentów Urządzeń na rynek polski lub Unii Europejskiej

Dostarczenie platformy obejmuje dostawę wszelkich wymaganych do działania platformy oprogramowania oraz licencji/subskrypcji.

W przypadku czasowego modelu licencjonowania – subskrypcji, minimalny okres objęcia taką licencją musi wynosić co najmniej 12 miesięcy.

Dostarczone urządzenia muszą być objęte minimum 36 miesięczną gwarancją opartą na serwisie producenta świadczonym w reżimie 8x5xNBD, zaś macierz w reżimie 24x7 z naprawą w 6 godz.

**Instalacja platformy obejmuje:**

1. **Konfigurację i uruchomienie urządzeń/elementów platformy wirtualizującej w środowisku Zamawiającego w terminie do 75 dni od podpisania umowy.**

Wykonawca przeprowadzi instalację i konfigurację wszystkich elementów dostarczonego systemu wymaganą przez Zamawiającego.

Wszelkie prace konfiguracyjne muszą uwzględniać dobre praktyki i rekomendacje eksploatacyjne publikowane przez producenta dostarczonej infrastruktury sprzętowej oraz programowej.

Wdrożony klaster wirtualizacyjny musi być skonfigurowany tak, aby był w pełni funkcjonalny we wszystkich czterech aspektach: serwerowym, dyskowym, sieciowym i zarządzania.

Przed rozpoczęciem prac należy ustalić plan adresacji sieci IP. Ustalenia te będą prowadzone z wyznaczonym do tego celu pracownikiem/pracownikami Zamawiającego.

Zamawiający zapewni przestrzeń min. 15U w szafie RACK 19”, zasilanie gwarantowane wraz z niezbędną ilością gniazd w listwach zasilających.

Zamawiający zapewni niezbędną ilość portów w standardzie 1000BASE-T na potrzeby zarządzania dostarczonym środowiskiem.

Prace wdrożeniowe klastra wirtualizacyjnego będą polegały w szczególności na:

* + montażu i podłączeniu fizycznym sprzętu w serwerowni (szafa RACK wskazana przez zamawiającego),
  + podłączeniu zasilania oraz sieci management,
  + aktualizacji oprogramowania układowego i jego komponentów wszystkich serwerów, macierzy, przełączników sieciowych oraz FC do wersji rekomendowanych przez producenta,
  + konfiguracji przełączników FC, macierzy dyskowej, przełączników sieciowych,
  + instalacji oraz konfiguracji NAS,
  + konfiguracji systemu backupu Zamawiającego
  + hardeningu urządzeń oraz wdrażanego oprogramowania według najlepszych praktyk producenta,
  + niezbędnej rekonfiguracji istniejącej infrastruktury informatycznej (VLANY, routing, polityki firewalla, wpisy DNS),
  + aktywacji zakupionego oprogramowania oraz wszelkich subskrypcji i serwisów producenta,
  + konfiguracji oraz uruchomieniu klastra wirtualizacyjnego, opartego o dostarczane oprogramowanie witrualizacyjne.

1. Wykonaniu testów akceptacyjnych (niezawodnościowe oraz funkcjonalne) oraz opracowaniu i przedstawieniu Raport z testów Wykonanie dokumentacji powykonawczej platformy wirtualizującej.
2. Dokumentacja powykonawcza platformy, musi w szczególności zawierać następujące elementy:
   * architektury logicznej,
   * architektury fizycznej,
   * architektury sieciowej,
   * konfiguracji klastra wirtualizacyjnego, zasobów dyskowych i sieci,
   * zestawienie wersji firmware zainstalowanych na dostarczonych urządzeniach,
   * zestawienie zakupionego i aktywowanego oprogramowania,
   * specyfikacja techniczna dostarczonego sprzętu,
   * schemat rozmieszczenia zainstalowanych urządzeń w szafach RACK i fizycznymi połączeniami między nimi,
   * tabele wykorzystanych adresów IP
   * zebrane informacje na temat obsługi wsparcia dostarczonych urządzeń, adresy url, nazwy kont do logowania, numery telefonów, adresy e-mail
3. Przeprowadzenie instruktażu
4. Wykonawca przeprowadzi instruktaż dla administratorów wskazanych przez

Zamawiającego:

* Instruktaż zostanie przeprowadzony w terminie uzgodnionym z Zamawiającym (jednak nie później niż 10 dni od daty wdrożenia), w jego siedzibie, tj. Plac Trzech Krzyży 3/5, 00-507 Warszawa.

Instruktaż powinien obejmować:

* omówienie dostarczonego sprzętu i oprogramowania (parametry, funkcjonalności),
* omówienie przeprowadzonych prac instalacyjno-konfiguracyjnych,
* omówienie i weryfikację przygotowanych i dostarczonych procedur,
* omówienie scenariuszy w przypadku wystąpienia błędów/awarii.

Przed ustalonym terminem instruktażu Wykonawca prześle Zamawiającemu zakres tematyczny/programu instruktażu. Zamawiający będzie miał prawo do weryfikacji zakresu tematycznego/programu instruktażu i zgłoszenia ew. dodatkowego zakresu tematycznego.

1. Asysta techniczna

Wykonawca zobowiązany jest zapewnić 300 roboczogodzin asysty technicznej w zakresie administracji zaoferowanym sprzętem oraz dostarczonym oprogramowaniem z osobami wskazanymi przez Wykonawcę w okresie 36 miesięcy od podpisania protokołu odbioru.

Asysta techniczna będzie polegała w szczególności na:

* + Zapewnieniu Zamawiającemu pomocy w rozwiązaniu problemów i incydentów wynikłych w trakcie obsługi dostarczonego sprzętu oraz oprogramowania tj.:
  + analiza problemów zgłaszanych przez Zamawiającego,
  + asysta przy określaniu i usuwaniu przyczyn oraz skutków zgłaszanych incydentów,
  + dostarczanie, instalacja (po uzyskaniu zgody Zamawiającego) i konfiguracja uaktualnień i nowych wersji oprogramowania lub jego komponentów, oraz związana z tym aktualizacja dostarczonej dokumentacji,
  + przeprowadzanie analiz oraz udzielanie konsultacji Zamawiającemu,
  + dokonywanie zmian konfiguracji oprogramowania,
  + opracowywanie i dostarczanie dokumentacji, w tym aktualizacji dokumentacji oraz dostarczanie dokumentacji wprowadzanych zmian.

1. Dokonywanie okresowych (nie rzadziej niż co 6 m-cy) przeglądów gwarancyjnych dostarczonego oprogramowania. W ramach przeprowadzanych okresowych przeglądów gwarancyjnych muszą być wykonane co najmniej następujące czynności:
   * weryfikacja poprawności działania oraz optymalizacja konfiguracji wszystkich komponentów wchodzących w skład dostarczonego rozwiązania,
   * analiza logów i podjęcie działań naprawczych w razie potrzeby,
   * aktualizacja (w razie potrzeby i po uzyskaniu uprzedniej zgody Zamawiającego) wersji poszczególnych komponentów wchodzących w skład dostarczonego rozwiązania.

Proces realizacji asysty technicznej będzie przebiegał następująco:

1. Zamawiający przekaże Wykonawcy drogą mailową zlecenie wykonania asysty technicznej. Zgłoszenie zawierać będzie co najmniej:
   * zakres prac do wykonania lub opis problemu do rozwiązania,
   * określenie proponowanego terminu realizacji (opcjonalnie).
2. W terminie nie dłuższym niż 3 dni robocze od dnia otrzymania zgłoszenia o asystę techniczną Wykonawca skontaktuje się z Zamawiającym w celu ustalenia szczegółowego zakresu prac, terminu realizacji i szacowanego wymiaru godzin realizacji asysty technicznej.
3. Po kontakcie z Zamawiającym, w terminie nie dłuższym niż 1 dzień roboczy (o ile Strony nie ustalą późniejszego terminu) Wykonawca rozpocznie realizację usługi.
4. Po wykonaniu każdorazowych prac związanych z asystą techniczną i uzyskaniem przez Wykonawcę potwierdzenia ich wykonania od Zamawiającego, Wykonawca przedstawi dokument – Raport z asysty technicznej, zawierający co najmniej:
   * opis wykonanych prac,
   * liczbę godzin poświęconą na wykonanie prac,
   * całkowitą liczbę godzin asysty technicznej zrealizowanych od początku trwania usługi, których realizacji została potwierdzona przez Zamawiającego.
5. Wykonawca ma prawo odmówić wykonania asysty technicznej o ile:
   * zamawiający wyczerpał przysługujący limit roboczogodzin lub zakończył się okres realizacji asysty technicznej,
   * realizacja asysty technicznej w zaproponowanym zakresie spowodowałaby przekroczenie przysługującego Zamawiającego limitu roboczogodzin asysty technicznej.
6. Zamawiający umożliwi Wykonawcy realizację usługi asysty technicznej poprzez udostępnienie wymaganych zasobów technicznych oraz niezbędnych pracowników Zamawiającego.
7. Prace będą świadczone w dni robocze w godzinach od 8 do 16 w języku polskim, zdalnie lub w siedzibie Zamawiającego. Dzień Roboczy należy rozumieć każdy dzień od poniedziałku do piątku z wyłączeniem dni ustawowo wolnych od pracy.
8. Konsultacje i porady będą udzielane na bieżąco podczas rozmowy telefonicznej lub w postaci elektronicznej, jednak nie później niż w ciągu 3 dni roboczych od skierowania zapytania. Jeżeli nie jest możliwe wykonanie zadania w ciągu 3 dni roboczych, Wykonawca uzgodni z Zamawiającym inny termin konsultacji lub porady, jeżeli Zamawiający wyrazi na to zgodę.

**Postanowienia końcowe:**

1. Po zakończonym wdrożeniu Wykonawca przekaże Zamawiającemu wszystkie hasła dostępowe do kont „super użytkowników” oraz dokumentację wraz z dokumentami potwierdzającymi nabycie dla Zamawiającego licencji oraz nośnikami danych zawierającymi zainstalowane oprogramowanie.

**Szczegółowy opis przedmiotu zamówienia**

Wszystkie ewentualne nazwy własne i marki handlowe urządzeń i elementów zawarte w opisie przedmiotu zamówienia, zostały użyte w celu sprecyzowania oczekiwań jakościowych i technologicznych Zamawiającego. Zamieszczone w specyfikacji nazwy technologicznych lub producentów kluczowych komponentów użyto jedynie w celu przykładowym. Zamawiający informuje, że dopuszcza składanie ofert, w których poszczególne urządzenia bądź materiały wymienione w opisie przedmiotu zamówienia mogą być zastąpione urządzeniami bądź materiałami/elementami równoważnymi. Poprzez pojęcie materiałów/elementów i urządzeń równoważnych należy rozumieć materiały zapewniające uzyskanie parametrów technicznych nie gorszych od założonych w opisie przedmiotu zamówienia. Zastosowanie rozwiązań równoważnych nie może prowadzić do pogorszenia właściwości przedmiotu zamówienia w stosunku do opisywanych.

**Serwer do obsługi wirtualizacji 5 szt.**

|  |  |
| --- | --- |
| **Element konfiguracji** | **Wymagania minimalne** |
| Obudowa | Maksymalnie 1U RACK 19 cali wraz z szynami montażowymi i prowadnicą kabli umożliwiającymi serwisowanie serwera w szafie rack bez wyłączania urządzenia.  Serwer wyposażony w zdejmowany panel przedni z możliwością instalacji zamka chroniącym przed nieuprawionym dostępem do dysków oraz z zainstalowanym czujnikiem otwarcia obudowy współpracujący z BIOS/UEFI. |
| Procesor | Procesor szesnastordzeniowy, x86 - 64 bity, pracujący z częstotliwością bazową min. 2.8GHz i osiągające w testach SPECrate2017\_int\_base wynik nie gorszy niż 339 punktów, dla testu oferowanego modelu serwera z 2 procesorami.  W przypadku zaoferowania procesora równoważnego, wynik testu musi być opublikowany na stronie [www.spec.org](about:blank)  Płyta główna wspierająca zastosowanie procesorów od 8 do 64 rdzeni, mocy do min. 385W i taktowaniu CPU do min. 3.7GHz. |
| Liczba procesorów | Min. 2 procesory |
| Pamięć operacyjna | Min. 512 GB RDIMM DDR5 5600 MT/s w modułach pamięci o pojemności min. 32GB każdy  Płyta główna z minimum 32 slotami na pamięć i umożliwiająca instalację do minimum 8TB. |
| Sloty rozszerzeń | Min. 3 aktywne gniazda PCI-Express generacji 5, x16 (szybkość slotu – bus width) w tym dwa nieobsadzone.  Dwa sloty OCP 3.0 możliwe do obsadzenia poprzez kontrolery sprzętowe dla dysków lub karty sieciowe w dowolnej konfiguracji. |
| Dysk twardy | Serwer bezklatkowy z możliwością rozbudowy/rekonfiguracji w przyszłości serwera do 10 dysków typu Hot Swap, SAS/SATA/SSD/NVMe, 2,5” montowane z przodu obudowy.  W przypadku braku opcji rozbudowy/rekonfiguracji o dodatkowe zatoki dyskowe, serwer standardowo wyposażony w minimum 10 zatok dyskowych SFF gotowe do instalacji dysków SAS/SATA/SSD/NVMe 2,5”typu Hot Swap.  Zainstalowane min. 2 szt. dysków SSD NVMe 480GB nie zajmujących wnęk na dyski twarde, pracujące w konfiguracji ze sprzętowym RAID 1. |
| Kontroler | Serwer wyposażony w kontroler software dla dysków SATA, obsługujący poziomy: RAID 0, 1, 5, 10.  Możliwość zastosowania/wymiany kontrolera na kontroler sprzętowy wyposażony w min. 8GB cache z mechanizmem podtrzymywania zawartości pamięci cache w razie braku zasilania, obsługujący poziomy: RAID 0/1/10/5/50/6/60. Kontroler wraz z niezbędnymi elementami zapewniający obsługę napędów dyskowych SSD/SATA/SAS/NVMe.  Kontroler umożliwiający pracę z dyskami w trybach RAID i JBOD jednocześnie. |
| Interfejsy sieciowe | Dwie dwuportowe karty 10/25GbE nie zajmujące gniazd opisanych w sekcji „sloty rozszerzeń”.  Jedna karta dwuportowa 32Gb FC z wkładkami SR.  Jedna karta dwuportowa 1GbE z interfejsem RJ45 |
| Karta graficzna | Zintegrowana karta graficzna |
| Porty | 5 x USB, z czego min. 4szt. w wersji USB 3.2 oraz jeden port USB 2.0,  1x VGA  Możliwość rozbudowy/rekonfiguracji o:  - port szeregowy typu DB9/DE-9 (9 pinowy), wyprowadzony na zewnątrz obudowy bez pośrednictwa portu USB/RJ45 oraz bez konieczności instalowania kart w slotach PCI-Express  - cyfrowy port video ( Display Port lub HDMI), bez użycia przejściówek z portu VGA lub USB |
| Zasilacz | 2 szt., typu Hot-plug, redundantny, każdy o mocy minimum 900W. |
| Chłodzenie | Zestaw wentylatorów redundantnych typu hot-plug |
| Diagnostyka | Możliwość zainstalowania elektronicznego panelu diagnostycznego dostępnego z przodu serwera pozwalającego uzyskać informacje o stanie: procesora, pamięci, wentylatorów, zasilaczy, temperaturze. |
| Bezpieczeństwo | Serwer wyposażony w moduł TPM 2.0. |
| Karta/moduł zarządzający | Niezależna od system operacyjnego, zintegrowana z płytą główną serwera lub jako dodatkowa karta w slocie PCI Express, jednak nie może ona powodować zmniejszenia minimalnej liczby gniazd PCIe w serwerze, posiadająca minimalną funkcjonalność:   * monitorowanie podzespołów serwera: temperatura, zasilacze, wentylatory, procesory, pamięć RAM, kontrolery macierzowe i dyski (fizyczne i logiczne), karty sieciowe * praca w trybie bezagentowym – bez agentów zarządzania instalowanych w systemie operacyjnym z generowaniem alertów SNMP * dostęp do karty zarządzającej poprzez   + dedykowany port RJ45 z tyłu serwera lub   + przez współdzielony port karty sieciowej serwera * dostęp do karty możliwy   + z poziomu przeglądarki webowej (GUI)   + z poziomu linii komend zgodnie z DMTF System Management Architecture for Server Hardware, Server Management Command Line Protocol (SM CLP)   + z poziomu skryptu (XML/Perl)   + poprzez interfejs IPMI 2.0 (Intelligent Platform Management Interface) * wbudowane narzędzia diagnostyczne * zdalna konfiguracji serwera (BIOS) i instalacji systemu operacyjnego * obsługa mechanizmu remote support - automatyczne połączenie karty z serwisem producenta sprzętu, automatyczne przesyłanie alertów, zgłoszeń serwisowych i zdalne monitorowanie * wbudowany mechanizm logowania zdarzeń serwera i karty zarządzającej w tym włączanie/wyłączanie serwera, restart, zmiany w konfiguracji, logowanie użytkowników * przesyłanie alertów poprzez e-mail oraz przekierowanie SNMP (SNMP passthrough) * uwierzytelnianie oprogramowania sprzętowego PCIe z protokołem bezpieczeństwa i modelem danych (SPDM) zapewnia integralność komponentu * obsługa zdalnego serwera logowania (remote syslog) * wirtualna zdalna konsola, tekstowa i graficzna, z dostępem do myszy i klawiatury i możliwością podłączenia wirtualnych napędów FDD, CD/DVD i USB i wirtualnych folderów * mechanizm przechwytywania, nagrywania i odtwarzania sekwencji video dla ostatniej awarii i ostatniego startu serwera a także nagrywanie na żądanie * funkcja zdalnej konsoli szeregowej - Textcons przez SSH (wirtualny port szeregowy) z funkcją nagrywania i odtwarzania sekwencji zdarzeń i aktywności * monitorowanie zasilania oraz zużycia energii przez serwer w czasie rzeczywistym z możliwością graficznej prezentacji * konfiguracja maksymalnego poziomu pobieranej mocy przez serwer (capping) * zdalna aktualizacja oprogramowania (firmware) * zarządzanie grupami serwerów, w tym:   + tworzenie i konfiguracja grup serwerów   + sterowanie zasilaniem (wł/wył)   + ograniczenie poboru mocy dla grupy (power capping)   + aktualizacja oprogramowania (firmware)   + wspólne wirtualne media dla grupy * możliwość równoczesnej obsługi przez 6 administratorów * autentykacja dwuskładnikowa (Kerberos) * wsparcie dla Microsoft Active Directory * obsługa SSL i SSH * enkrypcja AES/3DES oraz RC4 dla zdalnej konsoli * wsparcie dla IPv4 oraz iPv6, obsługa SNMP v3 oraz RESTful API * wsparcie dla Integrated Remote Console for Windows clients * możliwość autokonfiguracji sieci karty zarządzającej (DNS/DHCP) |
| Wsparcie dla systemów operacyjnych i systemów wirtualizacyjnych | Microsoft Windows Server 2019, 2022  Ubuntu 20.04 LTS, 22.04 LTS  Red Hat Enterprise Linux (RHEL) 8.6, 9.0  VMware ESXi 7.0 U3, 8.0, 8.0 U1/U2 |
| Wsparcie techniczne | Minimum 3-letnia gwarancja producenta w miejscu instalacji.  Czas reakcji 2h w standardowe dni robocze w godzinach od 9:00 do 17:00. Przybycie serwisu do miejsca instalacji w ciągu następnego dnia roboczego od zgłoszenia usterki.  Wsparcie techniczne realizowane jest przez serwis producenta oferowanego serwera. |
| Inne | Urządzenia muszą być zakupione w oficjalnym kanale dystrybucyjnym producenta. Na żądanie Zamawiającego, Wykonawca musi przedstawić oświadczenie producenta oferowanego serwera, potwierdzające pochodzenie urządzenia z oficjalnego kanału dystrybucyjnego producenta oraz, że sprzęt produkowany jest zgodnie z normami ISO 9001 oraz ISO 14001.  Deklaracja zgodności CE. |

**Przełączniki Fiber Channel – 2 szt.**

|  |  |
| --- | --- |
| **Lp.** | **Charakterystyka (wymagania minimalne)** |
| 1. | Przełącznik Fibre Channel musi mieć wysokość maksymalnie 1U (jednostka wysokości szafy montażowej) i zapewniać techniczną możliwość montażu w szafie 19” |
| 2. | Przełącznik FC musi być wykonany w technologii Brocade FC 16 Gb/s oraz 32 Gb/s i zapewniać możliwość pracy portów FC z prędkościami 32, 16, 8, 4 Gb/s w zależności od rodzaju zastosowanych wkładek SFP.   * 1. W przypadku obsadzenia portu FC za pomocą wkładki SFP 16Gb/s przełącznik musi umożliwiać pracę tego portu z prędkością 16, 8 lub 4 Gb/s, przy czym wybór prędkości musi być możliwy w trybie autonegocjacji   2. W przypadku obsadzenia portu FC za pomocą wkładki SFP 8Gb/s przełącznik musi umożliwiać pracę tego portu z prędkością 8 lub 4 Gb/s, przy czym wybór prędkości musi być możliwy w trybie autonegocjacji   3. Wszystkie zaoferowane porty przełącznika FC muszą umożliwiać działanie bez tzw. Oversubscrypcji, gdzie wszystkie porty w maksymalnie rozbudowanej konfiguracji przełącznika wyposażonej we wkładki 32Gbs mogą pracować równocześnie z pełną prędkością 32Gb/s.   4. Całkowita przepustowość przełącznika FC dostępna dla maksymalnie rozbudowanej konfiguracji (24 porty) wyposażonej we wkładki 32Gbs musi wynosić minimum 768 Gb/s end-to-end. |
| 3. | Ilość i rodzaj portów Fibre Channel:   * 1. Przełącznik Fibre Channel musi być wyposażony, w co najmniej 8 aktywnych portów FC obsadzone 8 wkładkami SFP+, wielomodowymi, krótkodystansowymi, ze złączem LC o prędkości 32 Gbit każda.   2. Wszystkie dostarczone wkładki muszą być oryginalne, tj. dostarczane przez producenta oferowanego przełącznika, lub certyfikowane przez producenta oferowanego przełącznika do pracy z oferowanym modelem przełącznika, co oznacza że dostarczony model wkładki musi znajdować się w ofercie sprzedaży producenta przełącznika lub na oficjalnej opublikowanej przez producenta przełącznika liście kompatybilności.   3. Niedopuszczalne jest dostarczenie zamiennych wkładek niecertyfikowanych, których montaż mógłby spowodować utratę gwarancji producenta przełącznika lub jakiekolwiek problemy konfiguracyjne |
| 4. | Typ portów  Możliwość konfiguracji portów typu : D\_Port, E\_Port, ,F\_Port, M\_Port; Przełącznik musi mieć obsługę trybu NPIV na portach  Oczekiwana wartość opóźnienia przy przesyłaniu ramek FC między dowolnymi portami przełącznika nie może być większa niż 900ns. |
| 5. | Funkcje niezawodnościowe  Przełącznik Fibre Channel musi mieć możliwość wymiany i aktywacji wersji firmware’u (zarówno na wersję wyższą jak i na niższą) w czasie pracy urządzenia i bez zakłócenia przesyłanego ruchu FC |
| 6. | Mechanizmy bezpieczeństwa:  Przełącznik Fibre Channel musi wspierać następujące mechanizmy zwiększające poziom bezpieczeństwa:   * 1. mechanizm tzw. Switch Binding, który umożliwia zdefiniowanie listy kontroli dostępu regulującej prawa urządzeń FC do podłączenia do przełącznika fabric   2. mechanizm tzw. Port Binding, który umożliwia zdefiniowanie listy kontroli dostępu regulującej prawa hostów i urządzeń storage FC do podłączenia do portu przełącznika   3. uwierzytelnianie (autentykacja) przełączników w sieci Fabric za pomocą protokołów FCAP   4. uwierzytelnianie (autentykacja) urządzeń końcowych w sieci Fabric za pomocą protokołu DH-CHAP   5. szyfrowanie połączenia z konsolą administracyjną. Wsparcie dla SSHv2.   6. definiowanie wielu kont administratorów z możliwością ograniczenia ich uprawnień za pomocą mechanizmu tzw. RBAC (Role Based Access Control)   7. definiowane kont administratorów w środowisku RADIUS, LDAP w MS Active Directory, Open LDAP, TACACS+   8. szyfrowanie komunikacji narzędzi administracyjnych za pomocą SSL/HTTPS   9. obsługa SNMP v1 oraz v3   10. wgrywanie nowych wersji firmware przełącznika FC z wykorzystaniem bezpiecznych protokołów SCP oraz SFTP   11. wykonywanie kopii bezpieczeństwa konfiguracji przełącznika FC z wykorzystaniem bezpiecznych protokołów SCP oraz SFTP |
| 7. | Funkcjonalności   * 1. Przełącznik Fibre Channel musi umożliwiać rozbudowę o agregację połączeń ISL między dwoma przełącznikami i tworzenia w ten sposób logicznych połączeń typu trunk o przepustowości minimum 128 Gb/s half duplex dla każdego logicznego połączenia. Load balancing ruchu między fizycznymi połączeniami ISL w ramach połączenia logicznego typu trunk musi być realizowany na poziomie pojedynczych ramek FC a połączenie logiczne musi zachowywać kolejność przesyłanych ramek.   2. Przełącznik Fibre Channel musi realizować sprzętową obsługę zoningu (przez tzw. układ ASIC) na podstawie portów i adresów WWN.   3. Przełącznik Fibre Channel musi umożliwiać rozbudowę instalacji wkładek SFP umożliwiających bezpośrednie połączenie (bez dodatkowych urządzeń pośredniczących) z innymi przełącznikami na odległość minimum 25km z prędkością 16Gb/s.   4. Wsparcie dla N\_Port ID Virtualization (NPIV). Obsługa, co najmniej 255 wirtualnych urządzeń na pojedynczym porcie przełącznika |
| 8. | Zarządzanie  Przełącznik Fibre Channel musi mieć możliwość konfiguracji przez:   * + - HTTP/HTTPS, poprzez SSH, obsługa SNMP v1/v3,     - możliwość wysyłania logów na zewnętrzny serwer syslog,     - Osobny interfejs sieciowy 10/100/1000 Mbps Ethernet RJ-45 pozwalający na zarządzanie przełącznikiem     - Port szeregowy (RJ-45) pozwalający na bezpośrednie podłączenie się do przełącznika |
| 9. | Możliwość rozbudowy w przyszłości o poniższe licencje (dla każdego przełącznika)   * + - Fabric Vision     - ISL Trunking     - Extended Fabric |
| 10. | Diagnostyka  Możliwość diagnozowania z poziomu przełącznika połączeń światłowodowych, Możliwość pomiaru połączenia (prędkość, opóźnienia, dystans), wbudowany generator przepływu danych, możliwość wykonywania poleceń FC ping, Pathinfo (FCtraceroute), możliwość podglądu ramek, monitorowanie stanu łącz, monitorowanie stanu urządzenia |
| 11. | Preferowany sposób montażu i kierunek przepływu chłodnego powietrza   * + - Montaż w tylnej części szafy rack     - Przepływ powietrza chłodzącego przez przełącznik od tyłu urządzenia w kierunku interfejsów.     - Wraz z przełącznikiem wymagane jest dostarczenie wszelkich elementów i akcesoriów niezbędnych do prawidłowego zamontowania przełącznika w szafie RACK oraz prawidłowej cyrkulacji powietrza (np. szyny montażowe, śruby itp.) |
| 12. | Zasilanie  urządzenie musi współpracować z krajową siecią energetyczną o parametrach znamionowych: 230 V, 50 Hz.  Maksymalny dopuszczalny pobór mocy przełącznika FC wyposażonego w 24 aktywne porty 32Gbps to 77W. Zainstalowany dodatkowo zasilacz redundantny AC 230V. Zasilacze wymienne (możliwość instalacji/wymiany „na gorąco” – ang. hot swap)  Chłodzenie - Redundantne i wymienne moduły wentylatorów |
| 13. | Oferowane produkty (urządzenia, sprzęt) muszą spełniać wymagania norm CE, tj. muszą spełniać wymogi niezbędne do oznaczenia produktów znakiem CE |
| 14. | Urządzenia i ich komponenty muszą być oznakowane przez producenta w taki sposób, aby możliwa była identyfikacja zarówno produktu jak i producenta. |
| 15. | Przełączniki sieci SAN muszą być nowe, nigdy wcześniej nie używane i pochodzić z autoryzowanego kanału dystrybucji producenta na terenie Polski a także być objęta serwisem producenta. |
| 16. | Wymagana jest gwarancja na wszystkie elementy przełącznika sieci SAN (sprzęt oraz oprogramowanie) na okres min. 3 lat, klasy NBD (onsite), czas reakcji na zgłoszenie 2h |
| 17. | Wraz z każdym przełącznikiem należy dostarczyć 8 szt. okablowania OM4 o długości minimum 2 metrów |

**Macierz – 1 szt.**

|  |  |  |
| --- | --- | --- |
| **L.p.** | **Cecha** | **Wymagania minimalne** |
|  | Typ obudowy | Macierz musi być przystosowana do montażu w szafie rack 19”. |
|  | Przestrzeń dyskowa | Macierz musi być wyposażona w minimum 12 dysków SSD NVMe o pojemności nie mniejszej niż 1,92 TB zapewniającej minimum 14,90 TB przestrzeni użytkowej dla hostów bez stosowani mechanizmów deduplikacji i kompresji i przy zapewnieniu odporności na awarię co najmniej 2 dowolnych dysków.  Nie dopuszcza się stosowania protokołu innego niż NVMe do obsługi dysków w macierzy. Nie dopuszcza się stosowania dysków QLC. Wymagane są dyski MLC lub TLC.  Macierz musi mieć możliwość obsługi co najmniej 1PB pojemności surowej (raw) na dyskach SSD NVMe. Nie dopuszcza się stosowania dysków SSD SAS ani żadnych innych nośników poza SSD NVMe. Nie dopuszcza się wirtualizacji zewnętrznych pamięci masowych.  Macierz musi umożliwić rozbudowę do minimum 72 ysków SSD NVMe. |
|  | Sposób zabezpieczenia danych | Macierz musi posiadać mechanizm RAID zabezpieczający przed utratą spójności danych w przypadku jednoczesnej awarii dwóch dowolnych dysków. Mechanizm realizowany sprzętowo za pomocą dedykowanego układu z wykorzystaniem puli wszystkich dysków twardych (tzw. wide-striping).  Rozłożenie dysków w macierzy musi zapewniać redundancję pozwalającą na nieprzerwaną pracę i dostęp do wszystkich danych w sytuacji awarii pojedynczego komponentu sprzętowego typu: dysk, port, kontroler, zasilacz, kabel.  Macierz musi umożliwiać definiowanie dysków „spare” lub odpowiadającej im przestrzeni dyskowej „spare”.  Wymagane zabezpieczenie minimum RAID-6. |
|  | Kontrolery macierzowe | Macierz All-NVMe wyposażona w minimum 2 kontrolery macierzowe obsługujące protokoły blokowe i pracujące w trybie ALUA (Asymmetric Logical Unit Access). Oba kontrolery muszą jednocześnie aktywnie obsługiwać wolumeny. Oprogramowanie macierzy musi rozkładać obsługę wolumenów pomiędzy kontrolery  i dążyć do ich równomiernego obciążenia.  Każdy z kontrolerów musi być wyposażony w wielordzeniowe procesory x86 (każdy w minimum 16 fizycznych rdzeni). Z uwagi na kompatybilność z systemami operacyjnymi oraz aplikacjami występującymi w środowisku Zamawiającego, a listą rozkazów obsługiwanych przez procesory zainstalowane w oferowanym rozwiązaniu, Zamawiający zaakceptuje jedynie rozwiązania wyposażone w procesory firm Intel lub AMD. Zastosowany procesor musi wspierać standard PCIe Gen4.  Każdy kontroler musi posiadać co najmniej 192GB pamięci RAM o szybkości 3200MT/s.  Kontrolery muszą obsługiwać protokół FC, NVMeoF-FC na portach wystawionych do hostów (front-end). |
|  | Interfejsy | Macierz musi być wyposażona, w co najmniej:   * 2 karty 4 portowe (po 1 karcie na kontroler) min. 32Gb FC wyposażone w min. 4 wkładki 32Gb SW( po 2 szt. na kontroler). * 2 porty (po 1 na kontroler) Ethernet min. 1Gb BaseT do zarządzania macierzą * Możliwość instalacji dodatkowo 2 kart 4 portowych (po 1 karcie na kontroler) 10/25 Gb iSCSI |
|  | Sposób zarządzania | Zarządzanie macierzą dyskową musi być możliwe z poziomu interfejsu graficznego oraz linii poleceń.  Oprogramowanie do zarządzania musi pozwalać na stałe monitorowanie stanu macierzy oraz umożliwiać konfigurowanie jej zasobów dyskowych. Narzędzie musi pozwalać na obserwację danych wydajnościowych oraz prezentację ich w postaci wykresów oraz czytelnych raportów. Wymagane jest monitorowanie bieżących parametrów pracy macierzy. |
|  | Zarządzanie grupami dyskowymi oraz dyskami logicznymi | Macierz musi zapewniać możliwość dynamicznego zwiększania pojemności wolumenów logicznych oraz wielkości grup dyskowych (przez dodanie dysków) z poziomu kontrolera macierzowego bez przerywania dostępu do danych. Musi istnieć możliwość rozłożenia pojedynczego wolumenu logicznego na wszystkie dyski fizyczne macierzy (tzw. wide-striping) bez konieczności łączenia wielu różnych dysków logicznych w jeden większy. |
|  | Thin Provisioning | Macierz musi umożliwiać udostępnianie zasobów dyskowych do serwerów w trybie typu Thin Provisioning.  Macierz musi umożliwiać odzyskiwanie przestrzeni dyskowych po usuniętych danych w ramach wolumenów typu Thin. Proces odzyskiwania danych musi być automatyczny bez konieczności uruchamiania dodatkowych procesów na kontrolerach macierzowych (wymagana obsługa standardu T10 SCSI UNMAP). |
|  | Wewnętrzne kopie migawkowe | Macierz musi umożliwiać dokonywanie na żądanie tzw. migawkowej kopii danych (snapshot, point-in-time) w ramach macierzy za pomocą wewnętrznych kontrolerów macierzowych. Kopia migawkowa wykonuje się bez konieczności wcześniejszego alokowania dodatkowej przestrzeni dyskowej na potrzeby kopii. Wymagany jest mechanizm Redirect-on-wite (ROW) lub równoważny, który nie wymaga kopiowania oryginalnych danych przy ich zmianie po wykonaniu migawki. Macierz musi posiadać mechanizm uniemożliwiający jakiemukolwiek użytkownikowi (w tym administratorom) usunięcie migawkowej kopii danych przez zdefiniowany okres. Okres ten nie może zostać skrócony. |
|  | Zdalna replikacja danych | Macierz musi umożliwiać zdalną replikację danych typu online do innej macierzy z tej samej rodziny z wykorzystaniem protokołu FC i IP. Replikacja musi być wykonywana na poziomie kontrolerów, bez użycia dodatkowych serwerów lub innych urządzeń i bez obciążania serwerów podłączonych do macierzy. Musi istnieć możliwość jednoczesnej natywnej replikacji w trybach: synchronicznym i asynchronicznym za pośrednictwem różnych infrastruktur (FC i IP).  Oprogramowanie musi zapewniać funkcjonalność zawieszania i ponownej przyrostowej resynchronizacji kopii z oryginałem oraz zamiany ról oryginału i kopii (dla określonej pary wolumenów logicznych) z poziomu interfejsu administratora. |
|  | Ciągła dostępność do danych | Macierz musi umożliwiać replikowanie danych synchronicznie z drugą taką macierzą i zapewniać – w przypadku awarii i całkowitej niedostępności jednej z macierzy – ciągłą pracę systemów działających na platformie przetwarzania danych i korzystających z zasobów pamięci masowych. Opisane powyżej przełączenie między macierzami musi odbywać się w sposób automatyczny i transparentny dla korzystających z dysków logicznych macierzy serwerów i aplikacji. Opisana funkcjonalność musi zapewniać integrację z co najmniej Microsoft Cluster Service oraz platformą wirtualizacyjną VMware (VMware vSphere Metro Storage Cluster).  Rozwiązanie musi umożliwiać hostom jednoczesny zapis do obu macierzy dla tego samego wolumenu. |
|  | Zarządzanie wydajnością | Macierz musi umożliwiać konfigurację gwarancji wydajności typu QoS w postaci ustawień kilku poziomów priorytetów obsługi. |
|  | Kompresja i deduplikacja danych | Macierz musi zapewniać kompresję i deduplikację danych na poziomie blokowym. Musi istnieć możliwość uruchomienia deduplikacji na poziomie pojedynczych wolumenów logicznych. Kompresja i deduplikacja nie mogą być realizowane za pomocą zewnętrznego urządzenia lub oprogramowania. |
|  | Podłączanie zewnętrznych systemów operacyjnych | Macierz musi umożliwiać jednoczesne podłączenie wielu serwerów w trybie wysokiej dostępności (co najmniej dwoma ścieżkami).  Macierz musi wspierać podłączenie następujących systemów operacyjnych dla protokołu FC: Windows Server 2022, Red Hat 9.x, VMware 8.x, SLES 15.  Macierz musi wspierać podłączenie następujących systemów operacyjnych dla protokołu NVMeoF-FC: Red Hat 9.x, VMware 8.x. |
|  | Wysoka dostępność | Macierz nie może posiadać pojedynczego punktu awarii, który powodowałby brak dostępu do danych. Musi być zapewniona pełna redundancja komponentów, w szczególności zdublowanie kontrolerów, zasilaczy i wentylatorów.  Macierz musi umożliwiać wymianę elementów systemu w trybie „hot-swap”, a w szczególności takich, jak: dyski, kontrolery, zasilacze, wentylatory.  Macierz musi mieć możliwość zasilania z dwóch niezależnych źródeł zasilania – odporność na zanik zasilania jednej fazy lub awarię jednego z zasilaczy macierzy.  Macierz musi umożliwiać wykonywanie aktualizacji mikrokodu macierzy w trybie online bez wyłączania żadnego z interfejsów macierzy.  Macierz musi umożliwiać zdalne zarządzanie macierzą oraz automatyczne informowanie centrum serwisowego o awarii.  Producent macierzy musi gwarantować 100% dostępność do danych dla pojedynczej macierzy. Wymagane potwierdzenie na publicznej stronie producenta na żądanie Zamawiającego. |
|  | Dodatkowe wymagania | Oferowana macierz dyskowa musi być fabrycznie nowa, wyprodukowana nie wcześniej niż 6 miesięcy przed datą dostarczenia do Zamawiającego i pochodzić z oficjalnego kanału dystrybucyjnego producenta na rynek polski. Zamawiający zastrzega sobie, aby Wykonawca na żądanie Zamawiającego przedłożył oświadczenie Producenta oferowanego sprzętu, w języku polskim, potwierdzające pochodzenie sprzętu z autoryzowanego kanału sprzedaży z Polski. |
|  | Gwarancja | Minimum 3-letnia gwarancja producenta w miejscu instalacji. Możliwość zgłoszenia awarii przez siedem dni w tygodniu, 24 godziny na dobę. Czas reakcji serwisu do 1 godz. usunięcie usterki do 6-ciu godzin.  Uszkodzone dyski pozostają u Zamawiającego.  W okresie gwarancji Zamawiający ma prawo do otrzymywania poprawek oraz aktualizacji wersji oprogramowania dostarczonego wraz z macierzą oraz oprogramowania wewnętrznego macierzy.  Gwarancja na sprzęt musi być dostarczona i realizowana przez organizację serwisową producenta sprzętu. |

**Przełącznik LAN – 2 szt.**

Obecnie Zamawiający posiada infrastrukturę sieciową opartą o cztery rodzaje przełączników: Cisco Catalyst 3650, 9200, 9500. Sprzęt będący przedmiotem niniejszego zamówienia musi być kompatybilny z posiadaną przez Zamawiającego infrastrukturą. Zaoferowany sprzęt nie może powodować zmniejszenia funkcjonalności posiadanych przełączników sieciowych.

Zaoferowane przełączniki sieciowe oraz oprogramowanie muszą pochodzić od tego samego producenta.

1. Typ i liczba portów - 24-porty 1/10/25G SFP/SFP+/SFP28 i 4 porty 40G/100G QSFP+
2. Porty SFP/SFP+/SFP28 możliwe do obsadzenia szerokim wachlarzem wkładek zależnie od potrzeb:
   1. Porty SFP+/ SFP28 - wkładki Gigabit Ethernet – w tym 1000Base-T, 1000Base-SX, 1000Base-LX/LH, 1000Base-EX, 1000Base-ZX, 1000Base-BX-D/U oraz 10Gigabit Ethernet – w tym 10GBase-SR, 10GBase-LR, 10GBase-LRM, 10GBase-ER, 10GBase-ZR, 10GBase-BX-D/U, twinax 10/25G-CSR, 10/25G-LR
   2. Porty QSFP+ - wkładki 40Gigabit Ethernet w tym 40G-SR4, 40G-LR4, 40G-ER4, 40G-SR-BD, twinax, wkładki 100Gigabit Ethernet w tym 100G-SR4, 100G-LR4, 100G-SM-SR, 100G-ER4L
   3. Z każdym przełącznikiem dostarczone zestaw kabli i modułów optycznych pochodzących od Producenta przełącznika:
      1. Kabel typu 25Gb AOC SFP28, min. 3m – min. 10 szt.
      2. Kabel typu 100 Gb AOC QSFP28 min. 1m – min. 1 szt.
      3. Moduł optyczny typu 25Gb SFP-25G-SR – min. 2 szt.
      4. Kabel typu 100Gb AOC QSFP28 min. 10m – min. 1 szt.
3. Zasilanie i chłodzenie
   1. Redundantne i wymienne moduły wentylatorów
   2. Zainstalowany dodatkowo zasilacz redundantny AC 230V. Zasilacze wymienne (możliwość instalacji/wymiany „na gorąco” – ang. hot swap)
4. Parametry wydajnościowe:
   1. Szybkość przełączania zapewniająca pracę z pełną wydajnością wszystkich interfejsów – również dla pakietów 64-bajtowych (przełącznik line-rate)
   2. Bufor pakietów – 32MB
   3. Pamięć DRAM – 16GB
   4. Pamięć flash – 16GB
   5. Obsługa
      1. 4.000 sieci VLAN
      2. 82.000 adresów MAC
      3. 200.000 tras IPv4
      4. 200.000 tras IPv6
5. Obsługa protokołu NTP
6. Obsługa IGMPv1/2/3 i MLDv1/2 Snooping
7. Przełącznik wspiera następujące mechanizmy związane z zapewnieniem ciągłości pracy sieci:
   1. IEEE 802.1w Rapid Spanning Tree
   2. Per-VLAN Rapid Spanning Tree (PVRST+)
   3. IEEE 802.1s Multi-Instance Spanning Tree
   4. Obsługa 128 instancji protokołu STP
8. Obsługa protokołu LLDP i LLDP-MED.
9. Funkcjonalność Layer 2 traceroute umożliwiająca śledzenie fizycznej trasy pakietu o zadanym źródłowym i docelowym adresie MAC
10. Obsługa funkcji Voice VLAN umożliwiającej odseparowanie ruchu danych i ruchu głosowego
11. Możliwość uruchomienia funkcji serwera DHCP
12. Mechanizmy związane z bezpieczeństwem sieci:
    1. Wiele poziomów dostępu administracyjnego poprzez konsolę. Przełącznik umożliwia zalogowanie się administratora z konkretnym poziomem dostępu zgodnie z odpowiedzą serwera autoryzacji (privilege-level)
    2. Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania użytkownika do określonej sieci VLAN
    3. Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania listy ACL
    4. Obsługa funkcji Guest VLAN umożliwiająca uzyskanie gościnnego dostępu do sieci dla użytkowników bez suplikanta 802.1X
    5. Możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC
    6. Możliwość uwierzytelniania użytkowników w oparciu o portal www dla klientów bez suplikanta 802.1X
    7. Możliwość uwierzytelniania wielu użytkowników na jednym porcie oraz możliwość jednoczesnego uwierzytelniania na porcie telefonu IP i komputera PC podłączonego za telefonem
    8. Możliwość obsługi żądań Change of Authorization (CoA) zgodnie z RFC 5176
    9. 27.000 wpisów dla list kontroli dostępu (Security ACE)
    10. Funkcjonalność flexible authentication (możliwość wyboru kolejności uwierzytelniania – 802.1X/uwierzytelnianie w oparciu o MAC adres/uwierzytelnianie w oparciu o portal www)
    11. Obsługa funkcji Port Security, DHCP Snooping, Dynamic ARP Inspection i IP Source Guard
    12. Zapewnienie podstawowych mechanizmów bezpieczeństwa IPv6 na brzegu sieci (IPv6 FHS) – w tym minimum ochronę przed rozgłaszaniem fałszywych komunikatów Router Advertisement (RA Guard) i ochronę przed dołączeniem nieuprawnionych serwerów DHCPv6 do sieci (DHCPv6 Guard)
    13. Możliwość autoryzacji prób logowania do urządzenia (dostęp administracyjny) do serwerów RADIUS i TACACS+
    14. Obsługa list kontroli dostępu (ACL), możliwość konfiguracji tzw. czasowych list ACL (aktywnych w określonych godzinach i dniach tygodnia)
    15. Możliwość szyfrowania ruchu zgodnie z IEEE 802.1AE (MACSec) dla wszystkich portów przełącznika (dla połączeń switch-switch i switch-host) kluczami o długości 128-bitów (gcm-aes-128)
    16. Wbudowane mechanizmy ochrony warstwy kontrolnej przełącznika (CoPP – Control Plane Policing)
    17. Funkcja Private VLAN
13. Technologie umożliwiające zapewnienie autentyczności sprzętu i oprogramowania
    1. Trust Anchor Module - odporne na manipulacje, zabezpieczone kryptograficzne rozwiązanie zapewniające autentyczność sprzętu w celu jednoznacznej identyfikacji produktu – daje pewność, że produkt jest oryginalny
    2. Secure Boot – zabezpiecza proces sekwencji startowej zapewniając, że mamy niezmieniony sprzęt oraz zapewniając warstwową ochronę przed próbą załadowania nielegalnego/zmodyfikowanego oprogramowania systemowego
    3. Image signing - obrazy podpisane kryptograficznie zapewniają, że oprogramowanie systemowe (firmware), BIOS i inne oprogramowanie są autentyczne i niezmodyfikowane. Podczas uruchamiania systemu sygnatury oprogramowania są sprawdzane pod kątem integralności.
14. Mechanizmy związane z zapewnieniem jakości usług w sieci:
    1. Implementacja 8 kolejek dla ruchu wyjściowego na każdym porcie dla obsługi ruchu o różnej klasie obsługi
    2. Implementacja algorytmu Shaped Round Robin dla obsługi kolejek
    3. Możliwość obsługi jednej z powyżej wspomnianych kolejek z bezwzględnym priorytetem w stosunku do innych (Strict Priority)
    4. Klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy/docelowy adres MAC, źródłowy/docelowy adres IP, źródłowy/docelowy port TCP
    5. Możliwość ograniczania pasma dostępnego na danym porcie dla ruchu o danej klasie obsługi z dokładnością do 8 Kbps (policing, rate limiting)
    6. Kontrola sztormów dla ruchu broadcast/multicast/unicast
    7. Możliwość zmiany przez urządzenie kodu wartości QoS zawartego w ramce Ethernet lub pakiecie IP – poprzez zmianę pola 802.1p (CoS) oraz IP ToS/DSCP
15. Obsługa protokołów routingu:
    1. Routing statyczny dla IPv4 i IPv6
    2. Routing dynamiczny – RIP, OSPF, EIGRP (Zamawiający wykorzystuje dynamiczny protokół routingu EIGRP w infrastrukturze sieciowej)
    3. Policy-based routing (PBR)
    4. Obsługa protokołu redundancji bramy (VRRP)
16. Przełącznik umożliwia lokalną i zdalną obserwację ruchu na określonym porcie, polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego – mechanizmy SPAN, RSPAN
17. Przełącznik posiada wzorce konfiguracji portów zawierające prekonfigurowane ustawienia rekomendowane zależnie od typu urządzenia dołączonego do portu (np. telefon IP, kamera itp.)
18. Zarządzanie
    1. Port konsoli
    2. Dedykowany port Ethernet do zarządzania out-of-band
    3. Plik konfiguracyjny urządzenia możliwy do edycji w trybie off-line (możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC). Po zapisaniu konfiguracji w pamięci nieulotnej możliwość uruchomienia urządzenia z nową konfiguracją
    4. Obsługa protokołów SNMPv3, SSHv2, SCP, https, syslog – z wykorzystaniem protokołów IPv4 i IPv6
    5. Możliwość konfiguracji za pomocą protokołu NETCONF (RFC 6241) i modelowania YANGa (RFC 6020) oraz eksportowania zdefiniowanych według potrzeb danych do zewnętrznych systemów
    6. Przełącznik posiada diodę umożliwiającą identyfikację konkretnego urządzenia podczas akcji serwisowych
    7. Przełącznik posiada wbudowany tag RFID w celu łatwiejszego zarządzania infrastrukturą
    8. Port USB umożliwiający podłączenie zewnętrznego nośnika danych. Urządzenie ma możliwość uruchomienia z nośnika danych umieszczonego w porcie USB
19. Możliwość montażu w szafie rack 19”. Wysokość urządzenia 1 RU

**Oprogramowanie do zarządzania przełącznikami**

1. Przełącznik musi posiadać funkcjonalność połączenia dwóch przełączników w stos (z wykorzystaniem standardowych modułów optycznych/twinax) celem stworzenia pojedynczego logicznego przełącznika z zapewnieniem następujących funkcjonalności:
   1. Zarządzanie poprzez jeden adres IP
   2. Możliwość tworzenia połączeń cross-stack Link Aggregation (czyli dla portów należących do różnych jednostek w stosie) zgodnie z IEEE 802.3ad
   3. Możliwość aktualizacji oprogramowania w trakcie pracy stosu (ISSU – In Service Software Upgrade)
2. Wsparcie dla protokołu LISP zgodnie z RFC 6830
3. Obsługa MPLS – w tym L3 VPN i Multicast VPN (mVPN)
4. Obsługa zaawansowanych protokołów routingu
   1. IS-IS i BGP dla IPv4 i IPv6
   2. Routing multicastów - PIM-SM, PIM-SSM
   3. Multicast Source Discovery Protocol (MSDP)
   4. VRF-Lite
5. Możliwość szyfrowania ruchu zgodnie z IEEE 802.1AE kluczami o długości 256-bitów (gcm-aes-256)
6. Możliwość enkapsulacji ruchu w pakiety VXLAN
7. Wsparcie dla IEEE 1588v2 (PTP – Precision Time Protocol)
8. Wsparcie dla IEEE 802.1BA (AVB – Audio Video Bridging)
9. Możliwość próbkowania i eksportu statystyk ruchu do zewnętrznych kolektorów danych (bez samplowania) ze wsparciem sprzętowym - NetFlow – obsługa 98.000 strumieni
10. Możliwość tworzenia skryptów celem obsługi zdarzeń, które mogą pojawić się w systemie
11. Możliwość tworzenia i uruchamiania skryptów Python bezpośrednio na przełączniku
12. Funkcjonalność bramy dla usług mDNS
13. Wbudowany analizator pakietów
14. Możliwość zdalnej obserwacji ruchu z określonych portów lub sieci VLAN polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego poprzez sieć IP (ERSPAN)

**Certyfikaty i gwarancja:**

1. Przełącznik musi posiadać deklaracja CE lub równoważną.
2. Przełącznik musi być wyprodukowany zgodnie z normą ISO-9001:2008 oraz ISO-14001 lub równoważną.
3. Zamawiający wymaga dla dostarczanych przełączników zapewnienia serwisu gwarancyjnego dla na okres minimum 36 miesięcy na poziomie 8x5xNBD.
4. Wraz z przełącznikami zostanie dostarczone niezbędne do zapewnienia wymaganych funkcjonalności i prawidłowego działania do którego są przeznaczone, oprogramowanie w ilości umożliwiającej spełnienie wymagań funkcjonalnych. Oprogramowanie zostanie dostarczone, w postaci stałej licencji lub minimum 36 miesięcznej subskrypcji, o ile producent nie oferuje oprogramowania w innej formie niż subskrypcja.

**Licencje na oprogramowanie do wirtualizacji**

Wszystkie licencje zaoferowanego oprogramowania do wirtualizacji muszą być licencjami subskrypcyjnymi, tj. licencja na określony czas - 1 rok wraz ze wsparciem technicznym do tych licencji świadczonym przez producenta zaoferowanego oprogramowania. Ilość licencji musi uwzględniać parametry serwerów do wirtualizacji (5 serwerów dwuprocesorowych z procesorami szesnastordzeniowymi).

Wszystkie wymagane poniżej komponenty/moduły muszą pochodzić od jednego producenta oprogramowania.

Licencje

1. W zakresie wirtualizacji mocy obliczeniowej Zamawiający wymaga:
   1. Licencje zaoferowanego oprogramowania muszą być zaoferowane w formie „per core” fizyczny procesora fizycznego.
   2. Zaoferowane oprogramowanie musi być instalowane bezpośrednio na sprzęcie fizycznym i nie może być ono częścią innego systemu operacyjnego.
   3. Zaoferowane oprogramowanie musi być instalowane bezpośrednio na sprzęcie fizycznym i nie może być ono częścią innego systemu operacyjnego.
   4. W zaoferowanym oprogramowaniu warstwa wirtualizacji nie może dla własnych celów alokować więcej niż 700MB pamięci operacyjnej RAM serwera fizycznego
   5. Zaoferowane oprogramowanie do wirtualizacji zainstalowane na serwerze fizycznym musi potrafić obsłużyć i wykorzystać procesory fizyczne tego serwera wyposażone w 768 logicznych wątków, 24TB pamięci fizycznej RAM tego serwera oraz 16 procesorów fizycznych tego serwera.
   6. Zaoferowane oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych z ilością od 1 do 768 procesorów wirtualnych
   7. Zaoferowane oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych z możliwością przydzielenia do 24 TB pamięci operacyjnej RAM.
   8. Zaoferowane oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych z możliwością przydzielenia od 1 do 10 wirtualnych kart sieciowych dla każdej z nich. Dodatkowo, oprogramowanie musi posiadać możliwość utworzenia maszyny wirtualnej bez przydzielonej wirtualnej karty sieciowej.
   9. Zaoferowane oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych, z których każda może mieć 32 porty szeregowe, 3 porty równoległe i 20 urządzeń USB.
   10. Zaoferowane oprogramowanie musi wspierać minimum następujące systemy operacyjne: Windows Server 2012/2016/2019/2022, Windows 8/10/11, RHEL 6/7/8/9, SLES 12/15, Debian 10/11, CentOS 7/8, Ubuntu 16/18/20/22, Photon OS 2/3/4, Oracle Linux 6/7/8/9, FreeBSD 12/13.
   11. W celu osiągnięcia maksymalnego współczynnika konsolidacji, zaoferowane oprogramowanie musi umożliwiać przydzielenie łącznie większej ilości pamięci RAM dla maszyn wirtualnych niż fizyczne zasoby RAM serwera, na którym maszyny te są posadowione.
   12. Rozwiązanie musi umożliwiać udostępnienie maszynie wirtualnej większej ilości zasobów dyskowych niż jest fizycznie dostępne na zasobach dyskowych
   13. Zaoferowane oprogramowanie musi umożliwiać integrację z rozwiązaniami antywirusowymi firm trzecich w zakresie skanowania maszyn wirtualnych z poziomu warstwy wirtualizacji bez ingerencji w systemy operacyjne maszyn wirtualnych (bezagentowość).
   14. Zaoferowane oprogramowanie musi zapewniać zdalny i lokalny dostęp administracyjny do wszystkich serwerów fizycznych poprzez protokół SSH, z możliwością nadawania uprawnień do takiego dostępu nazwanym użytkownikom bez konieczności wykorzystania konta „root”
   15. Zaoferowane oprogramowanie do wirtualizacji musi zapewnić możliwość powielania maszyn wirtualnych wraz z ich pełną konfiguracją i danymi
   16. Zaoferowane oprogramowanie do wirtualizacji musi zapewnić możliwość wykonywania kopii migawkowych instancji systemów operacyjnych na potrzeby tworzenia kopii zapasowych bez przerywania ich pracy z możliwością konieczności zachowania stanu pamięci pracującej maszyny wirtualnej.
   17. Konsola zarządzająca zaoferowanego oprogramowania musi posiadać możliwość przydzielania i konfiguracji uprawnień z możliwością integracji z usługami katalogowymi, minimalnie z: Microsoft Active Directory i Open LDAP oraz umożliwiać federacyjne zarządzanie tożsamością w oparciu o Microsoft Active Directory Federation Services (ADFS).
   18. Zaoferowane oprogramowanie musi zapewniać możliwość dodawania zasobów w czasie pracy maszyny wirtualnej, w szczególności w zakresie ilości procesorów, pamięci operacyjnej i przestrzeni dyskowej
   19. Zaoferowane oprogramowanie musi posiadać funkcjonalność tworzenia wirtualnego przełącznika (virtual switch) umożliwiającego tworzenie sieci wirtualnej w obszarze hosta (hypervisora wirtualizacyjnego) i pozwalającego połączyć tym przełącznikiem maszyny wirtualne w obszarze jednego hosta, a także na zewnątrz sieci fizycznej. Pojedynczy przełącznik wirtualny powinien mieć możliwość konfiguracji aż do 4096 portów
   20. Pojedynczy wirtualny przełącznik w zaoferowanym oprogramowaniu, w celu zapewnienia bezpieczeństwa połączenia ethernetowego w razie awarii fizycznej karty sieciowej, musi posiadać możliwość przyłączania do niego minimum dwóch fizycznych kart sieciowych
   21. Wirtualne przełączniki w zaoferowane oprogramowaniu muszą posiadać funkcjonalność obsługi wirtualnych sieci lokalnych (VLAN)
   22. Zaoferowane oprogramowanie musi umożliwiać wykorzystanie technologii przepustowości sieci komputerowych do 200GbE poprzez agregację połączeń fizycznych do minimalizacji czasu przenoszenia maszyny wirtualnej pomiędzy serwerami fizycznymi
   23. Zaoferowane oprogramowanie do wirtualizacji musi obsługiwać przełączenie ścieżek LAN (bez utraty komunikacji) w przypadku awarii jednej ze ścieżek
   24. Zaoferowane oprogramowanie musi zapewnić możliwość zdefiniowania alertów informujących o przekroczeniu wartości progowych
   25. Zaoferowane oprogramowanie, w przypadku działania pod zarządcą klastra VMware vCenter, musi zapewniać możliwość replikacji maszyn wirtualnych z dowolnej pamięci masowej w tym z dysków wewnętrznych serwerów fizycznych na dowolną pamięć masową w tym samym lub oddalonym ośrodku przetwarzania. Replikacja musi gwarantować współczynnik RPO (ang. Recovery Point Objective) na poziomie minimum 5 minut
   26. Zaoferowane oprogramowanie do wirtualizacji musi obsługiwać przełączenie ścieżek SAN (bez utraty komunikacji) w przypadku awarii jednej ze ścieżek
   27. Zaoferowane oprogramowanie, w przypadku działania pod zarządcą klastra VMware vCenter, musi mieć możliwość przenoszenia maszyn wirtualnych pomiędzy serwerami fizycznymi bez przerywania pracy usług na przenoszonych maszynach wirtualnych. Wymaga się wsparcia natywnego szyfrowania ruchu sieciowego dla maszyn wirtualnych podczas ich przenoszenia między serwerami fizycznymi
   28. Zaoferowane oprogramowanie, w przypadku działania pod zarządcą klastra VMware vCenter oraz w środowisku z więcej niż pojedynczym wirtualizatorem, musi umożliwiać automatyczne, ponowne uruchomienie maszyn wirtualnych w przypadku awarii jednego z wirtualizatorów na kolejnym, działającym w tym samym klastrze wirtualizatorze (funkcjonalność HA) (ang. High Availability)
   29. Zaoferowane oprogramowanie, w przypadku działania pod zarządcą klastra VMware vCenter w środowisku z minimalnie dwoma wirtualizatorami oraz w przypadku potrzeby wgrania aktualizacji do warstwy wirtualizacji, musi posiadać możliwość w przypadku wywołania startu aktualizacji, automatycznego przeniesienia bezprzerwowego działających maszyn wirtualnych do innego wirtualizatora nie objętego aktualizacją, przed rozpoczęciem samej aktualizacji
   30. Zaoferowane oprogramowanie musi posiadać co najmniej 2 niezależne mechanizmy wzajemnej komunikacji między serwerami z zainstalowanym wirtualizatorem oraz z serwerem zarządzającym, gwarantujące właściwe działanie mechanizmów wysokiej dostępności na wypadek izolacji sieciowej serwerów fizycznych lub partycjonowania sieci
   31. Zaoferowane oprogramowanie, w przypadku działania pod zarządcą klastra VMware vCenter, w środowisku z minimum dwoma wirtualizatorami, musi zapewniać pracę bez przestojów dla wybranych maszyn wirtualnych (o maksymalnie dwóch procesorach wirtualnych), niezależnie od systemu operacyjnego oraz aplikacji, podczas awarii wirtualizatora, bez utraty danych i dostępności danych na maszynach wirtualnych objętych ochroną
   32. Zaoferowane oprogramowanie do wirtualizacji musi zapewniać możliwość stworzenia dysku maszyny wirtualnej o wielkości 62 TB
   33. Zaoferowane oprogramowanie musi posiadać wbudowany interfejs programistyczny (API) zapewniający pełną integrację zewnętrznych rozwiązań wykonywania kopii zapasowych z istniejącymi mechanizmami warstwy wirtualizacyjnej
   34. Producent zaoferowanego oprogramowania do wirtualizacji musi wspierać rozwiązania do automatyzacji procesów oraz wirtualizacji sieci (SDN, ang. Software Defined Network).
   35. Zaoferowane oprogramowanie musi wspierać mechanizmy zaawansowanego uwierzytelniania do systemu operacyjnego wirtualnej maszyny za pomocą technologii Smart Card Reader
   36. Zaoferowane oprogramowanie musi wspierać TPM 2.0. Minimalne wymaganie Zamawiającego dla TPM oznacza, że TPM zapewnia mechanizm gwarantujący, że serwer fizyczny, na którym zainstalowane jest zaoferowane oprogramowanie, uruchomił się z włączoną opcją Secure Boot. Po potwierdzeniu, że Secure Boot jest włączone, system gwarantuje, poprzez weryfikację podpisu cyfrowego, że hypervisor uruchomił się w niezmienionej formie
   37. Wirtualizator w zaoferowanym oprogramowaniu musi mieć możliwość włączenia funkcji “Microsoft virtualization-based security”, tzw. Microsoft VBS dla systemów operacyjnych maszyn wirtualnych opartych o system operacyjny Microsoft Windows 10, Microsoft Windows Server 2016 oraz Microsoft Windows Server 2019
   38. Zaoferowane oprogramowanie musi posiadać certyfikację FIPS-140-2 min. dla modułu jądra wirtualizatora odpowiedzialnego za szyfrowanie danych
   39. Zaoferowane oprogramowanie musi posiadać funkcjonalność wirtualnego TPM 2.0 dla maszyn wirtualnych z zainstalowanym Microsoft Windows 10 oraz Microsoft Windows 2016. Zamawiający wymaga, aby z punktu widzenia maszyny wirtualnej z systemem operacyjnym Microsoft Windows 10 lub Microsoft Windows 2016 wirtualny TPM widziany był jako standardowy TPM, gdzie można przechowywać bezpiecznie wrażliwe dane np. certyfikaty. Zawartość wirtualnego TPM musi być przechowywana w pliku przynależnym do maszyny wirtualnej oraz musi być szyfrowana.
   40. Zaoferowane oprogramowanie musi posiadać funkcjonalność szybkiego uruchamiania wirtualizatora po przeprowadzonym procesie jego aktualizacji. Zamawiający wymaga, aby w procesie aktualizacji wirtualizatora, jeśli wymagany jest jego restart, funkcjonalność szybkiego uruchamiania powodowała eliminację czasochłonnej fazy inicjalizacji serwera fizycznego
   41. Zaoferowane oprogramowanie, w przypadku działania pod zarządcą klastra, musi posiadać możliwość aktualizacji i kontroli wersji oprogramowania do wirtualizacji w ramach klastra serwerów z poziomu centralnej konsoli zarządzającej. Dodatkowo centralna konsola zarządzająca musi posiadać funkcjonalność aktualizacji firmware komponentów serwera fizycznego (dyski, kontrolery, karty sieciowe) z poziomu konsoli zarządzającej wirtualizatora. Konsola zarządzająca musi mieć możliwość automatycznej weryfikacji, czy zainstalowane komponenty serwera posiadają rekomendowaną wersję sterowników i firmware, eliminując ryzyko pracy na nieaktualnych wersjach. Taka funkcjonalność powinna być dostępna dla minimum dwóch producentów serwerów obecnych na rynku
   42. Zaoferowane oprogramowanie musi posiadać wsparcie dla natywnych dysków 4K
   43. Zaoferowane oprogramowanie musi wspierać protokół precyzyjnej synchronizacji czasu PTP (ang. Precision Time Protocol)
   44. Zaoferowane oprogramowanie, w przypadku działania pod zarządcą klastra, musi posiadać mechanizm, który ogranicza dostęp do indywidualnego zarządzania warstwą wirtualizacji na serwerach fizycznych w ramach klastra serwerów w celu utwardzenia/hardening (maksymalnego zwiększenia bezpieczeństwa dostępu) systemu wirtualizacji.
   45. Zaoferowane oprogramowanie musi mieć funkcjonalność migracji w trybie rzeczywistym dysków działających maszyn wirtualnych z jednego podsystemu dyskowego do innego bez konieczności przerywania pracy maszyny wirtualnej, której dysk jest migrowany
   46. Zaoferowane oprogramowanie obejmuje walidację FIPS, a także zaktualizowane przewodniki audytów.
   47. Zaoferowane oprogramowanie musi mieć możliwość utworzenia, poprzez API, maszyny wirtualnej jako tzw. Instant Clone poprzez klonowanie działającej maszyny wirtualnej w wyniku którego powstanie nowa działająca maszyna wirtualna identyczna z klonowaną. Nowa maszyna wirtualna musi powstawać w pamięci operacyjnej wirtualizatora
   48. Zaoferowane oprogramowanie, w przypadku działania pod zarządcą klastra, musi mieć możliwość monitorowania i wyświetlania za pomocą grafu w konsoli bieżącego poboru energii elektrycznej dla hosta wirtualizacyjnego oraz dla maszyn wirtualnych na nim posadowionych
2. W zakresie zarządzania klastrem wirtualizacyjnym Zamawiający wymaga:
   1. Ilość instancji zaoferowanego oprogramowania do zarządzania klastrem wirtualizacyjnym musi być równa liczbie fizycznych core zaoferowanych w oprogramowaniu do wirtulizacji mocy obliczeniowej
   2. Zaoferowane oprogramowanie musi posiadać konsolę graficzną do zarządzania maszynami wirtualnymi i do konfigurowania innych funkcjonalności. min: zasobów dyskowych oraz zasobów sieci komputerowej. Konsola graficzna powinna działać jako zainstalowana aplikacja na maszynie wirtualnej. Dodatkowo wymaga się aby maszyna z aplikacją była wstępnie skonfigurowana i dostępna jako tzw. virtual appliance. Instalacja w/w virtaul appliance nie może wiązać się z potrzebą dostawy dodatkowego oprogramowania takiego jak np. system operacyjny lub baza danych.
   3. Zaoferowane oprogramowanie musi posiadać wbudowany serwer ściany ogniowej (ang. firewall) dający możliwość konfiguracji blokady lub akceptacji ruchu pomiędzy konsolą zarządzającą a serwerami oraz serwerami wirtualnymi na nich posadowionymi, przy założeniu blokowania całego ruchu a nie poszczególnych portów
   4. Zaoferowane oprogramowanie musi mieć możliwość konfiguracji uwierzytelniania użytkowników logujących się do niego w oparciu o minimum: domenę Microsoft Active Directory, Microsoft Active Directory over LDAP oraz Open LDAP.
   5. Zaoferowane oprogramowanie musi posiadać konsole graficzną, która musi być dostępna poprzez dedykowanego klienta (za pomocą przeglądarek minimum Mozilla Firefox oraz Chrome) lub poprzez konsolę graficzną, która zbudowana jest z wykorzystaniem języka HTML5
   6. Zaoferowane oprogramowanie musi posiadać funkcjonalność zcentralizowanego zarządzania hostami VMware vSphere.
   7. Zaoferowane oprogramowanie musi posiadać natywne mechanizmy do wykonywania kopii zapasowej swojej konfiguracji. Dodatkowo wymaga się możliwości ustawienia harmonogramu wykonywania kopii zapasowej. Wymaga się aby kopie zapasowe wspierały protokoły: FTPS, HTTPS, SCP, FTP oraz http.
   8. Zaoferowane oprogramowanie, poprzez rozszerzenie o dodatkową licencję oferowaną przez tego samego producenta musi posiadać wbudowaną funkcjonalność zarządzania wirtualną przestrzenią dyskową SDS (ang. Software Defined Storage).
   9. Zaoferowane oprogramowanie musi posiadać interfejs graficzny do prowadzenia prac administracyjnych w zakresie swojej konfiguracji oraz monitoringu (możliwość monitorowania obciążenia min. vCPU, vRAM, vHDD, sieci, bazy danych). Interfejs graficzny powinien być wykonany w standardzie HTML5
   10. Zaoferowane oprogramowanie zawiera możliwość automatyzacji instalacji wielu konsoli zarządzania poprzez użycie schematów konfiguracji.
   11. Zaoferowane oprogramowanie umożliwia aktualizowanie wielu wirtualizatorów równocześnie.
   12. Rozwiązanie musi pozwalać na wykorzystanie łącz o szybkości do 100 GbE do bezawaryjnego przenoszenia maszyn wirtualnych między wirtualizatorami.
   13. Rozwiązanie musi zapewniać natywne mechanizmy wysokiej dostępności HA (ang. High Availability) w niezawodnej architekturze Active-Passive-Witness dla wszystkich składowych komponentów centralnej konsoli graficznej zarządzającej platformą wirtualną.
   14. Zaoferowane oprogramowanie zapewnia podstawowe funkcje serwera zarządzania kluczami (KMS), które upraszcza włączenie szyfrowania i zaawansowanych funkcji bezpieczeństwa.
   15. Zaoferowane oprogramowanie, w przypadku zarządzania serwerami opartymi o VMware vSphere, musi prezentować poziom zbalansowania mocy obliczeniowej w klastrze opartym o w/w wirtualizatory.
   16. Dostęp przez przeglądarkę do konsoli graficznej w zaoferowanym oprogramowaniu musi być skalowalny tj. powinien umożliwiać rozdzielenie komponentów na wiele instancji w przypadku zapotrzebowania na dużą liczbę jednoczesnych dostępów administracyjnych do środowiska.

**Serwer NAS – 1 szt.**

|  |  |
| --- | --- |
| Procesor | 6-rdzeniowy/12-wątkowy procesor o taktowaniu 3,8 GHz (zwiększanym do min. 5,0 GHz) , procesor musi osiągać wynik co najmniej 26000 punktów w teście porównawczym znajdującym się na stronie <https://www.cpubenchmark.net/> |
| Obudowa | Rack 2U o wymiarach maksymalnych 89 × 440 × 520 mm  (wys. x szer. x gł.) wraz z szynami do montażu w szafie rack |
| Pamięć RAM | 16 GB UDIMM DDR5  Możliwość rozbudowy poprzez dołożenie kolejnych pamięci do min. 192 GB (4 x 48GB) |
| Ilość obsługiwanych dysków | 12 dysków 3,5-calowych SATA 6 Gb/s, 3 Gb/s o maksymalnej pojemności 24TB każdy |
| Gniazda m.2 | 2 gniazda M.2 2280 PCIe Gen 5 |
| Interfejsy sieciowe | 2 porty 2,5 Gigabit sieci Ethernet (RJ45)  2 porty SFP+ 10GbE z modułami optycznymi 10GBase SR  2 porty 10GbE (10GBase-T)  możliwość zamontowania (jako płatna opcja):  - dodatkowej karty sieciowej 100GbE,  - dodatkowej karty sieciowej 25GbE,  - dodatkowej karty sieciowej FC 16GbE,  - dodatkowej karty sieciowej FC 32GbE.  obsługa VLAN i Jumbo Frame. |
| Porty USB | Minimum 2, gniazdo typu A USB 3.2 Gen 2 10 Gb/s |
| Gniazda PCIe | Minimum 3 gniazda PCIe  2 x Gen 4 x4, 1 x Gen 4x8 (lub Gen 4x4) |
| Wskaźniki LED | HDD 1–12, stan, LAN, stan gniazda rozszerzenia pamięci masowej |
| Obsługa RAID | RAID 0, 1, 5, 6, 10, 50, 60, Tripple Mirror, Tripple Parity, RAID 5, 6, 10 + dysk zapasowy. |
| Funkcje RAID | Dodanie grupy RAID do puli magazynu, wymiana wszystkich dysków w danej grupie RAID na większe, podłączanie jednostek rozszerzających JBOD. |
| Szyfrowanie | 256-bitowe szyfrowanie AES folderów |
| System Operacyjny | Apple Mac OS 10.10 lub nowszy  Ubuntu 14.04, CentOS 7, RHEL 6.6, SUSE 12 lub nowszy Linux  IBM AIX 7, Solaris 10 lub nowszy UNIX  Microsoft Windows 7, 8, 10, 11  Microsoft Windows Server 2008 R2, 2012, 2012 R2 oraz 2016, 2019, 2022 |
| Stacja monitoringu | W standardzie 8 licencji na podłączenie kamer. |
| Protokoły | CIFS, AFP, NFS, FTP, WebDAV, iSCSI, Telnet, SSH, SNMP |
| Usługi | Stacja monitoringu, Windows ACL, Integracja w Windows ADS, Serwer wydruku, Serwer WWW, Serwer plików, Manager plików przez WWW, Replikacja w czasie rzeczywistym, Serwer RADIUS, Klient LDAP, Serwer Syslog |
| Zarządzanie dyskami | SMART, sprawdzanie złych sektorów. |
| Język GUI | Polski |
| Waga | Maksymalnie 14 kg (netto) |
| System plików | Dyski wewnętrzne ZFS lub EXT4. Dyski zewnętrzne EXT3, EXT4, NTFS, FAT32, HFS+ |
| Funkcje ZFS | Liniowa deduplikacja, kompresja i kompakcja, Cache odczytu & ZIL |
| iSCSI | Obsługa MPIO, MC/S i SPC-3 Persistent Reservation |
| Liczba kont użytkowników | 4096 |
| Liczba grup | 512 |
| Liczba udziałów | 512 |
| Max ilość połączeń (CIFS) | 5000 |
| Zasilanie | Redundantne min. 550W (x2), 100–240 V |
| Wentylatory | 3 x 60mm, 12VDC |
| UPS | Obsługa sieciowych awaryjnych zasilaczy UPS. |
| Zamontowane dyski | 12 dysków zgodnych z listą kompatybilości podaną przez producenta NAS o pojemności minimum 10TB każdy, 256MB cache, 7200RPM, 2 mln MTBF, gwarancja dysków 5 lat, o parametrach minimalny transfer wewnętrzny 271MB/sek |
| Gwarancja producenta | Min. 3 lata gwarancji Producenta sprzętu w tym 3 lata gwarancji Producenta sprzętu w miejscu instalacji typu NBD On-site |