

Spis treści

1.	Definicje używane w dokumencie:.....	4
2.	Serwery obliczeniowe.....	5
2.1.	Serwer – parametry wspólne dla każdego typu serwera	5
2.2.	Oprogramowanie do zarządzania serwerami z poziomu konsoli oprogramowania do zarządzania klastrem wirtualizacyjnym.....	10
2.3.	Serwery obliczeniowe typu A, B, C.....	10
2.4.	Serwer obliczeniowy typu „A”	11
2.5.	Serwer obliczeniowy typu „B”	12
2.6.	Dodatkowe wyposażenie serwerów	12
2.6.1.	Dysk SSD	12
2.6.2.	Dysk HDD	13
2.6.3.	Akcelerator graficzny typu „A”	13
2.6.4.	Karta sieciowa 100GbE	14
2.6.5.	Karta FPGAs.....	14
3.	Serwer dyskowy.....	15
3.1.	Serwer dyskowy typu „C”	15
4.	Oprogramowanie do wirtualizacji	19
4.1.	Wymagania wspólne dla wszystkich modułów oprogramowania do wirtualizacji.....	19
4.2.	Oprogramowanie do wirtualizacji zasobów serwerowych i ich mocy obliczeniowej w wersji podstawowej.....	19
4.3.	Oprogramowanie do wirtualizacji zasobów serwerowych i ich mocy obliczeniowej w wersji rozszerzonej.....	22
4.4.	Oprogramowanie do zarządzania klastrem wirtualizacyjnym	23
4.5.	Oprogramowanie do wirtualizacji sieci	24
5.	Infrastruktura sieciowa.....	27
5.1.	Infrastruktura przełączająca i system sterujący	27
5.2.	Moduły optyczne do interfejsów sieciowych	49
5.2.1.	Moduł 1GbE, 1000BASE-T, SFP.....	49
5.2.2.	Moduł 10GbE, BASE-T, SFP+.....	50
5.2.3.	Moduł 10GbE, SR SFP+	50
5.2.4.	Moduł 25 GbE, SR SFP28	50
5.2.5.	Moduł 100GbE, LR4 QSFP28.....	51
5.2.6.	Moduł 100GbE, SR4 QSFP28.....	51

5.2.7.	Moduł 40 GbE, LR QSFP+	52
5.2.8.	Moduł, 40 GbE, SR QSFP+	52
5.3.	Okablowanie sieciowe	52
5.3.1.	Patchcord UTP 3m	52
5.3.2.	Patchcord UTP 5m	52
5.3.3.	Patchcord UTP 10m	53
5.3.4.	Patchcord LC-LC Multimode 3m	53
5.3.5.	Patchcord LC-LC Multimode 5m	53
5.3.6.	Patchcord LC-LC Single Mode 3m	53
5.3.7.	Patchcord LC-LC Single Mode 5m	53
5.3.8.	Patchcord MPO-MPO Multimode 3m – przełącznik -przełącznik	53
5.3.9.	Patchcord MPO-MPO Multimode 5m – przełącznik -przełącznik	53
5.3.10.	Kabel DAC pasywny 100G 3m	54
5.3.11.	Kabel DAC pasywny 100G 5m	54
5.3.12.	Kabel DAC pasywny breakout 100G --> 4 x 25 G 3m	54
5.3.13.	Kabel DAC pasywny breakout 100G --> 4 x 25 G 5m	54
5.3.14.	Kabel DAC pasywny 25G 3m	54
5.3.15.	Kabel DAC pasywny 25G 5m	54
6.	Stacje zarządzania	55
6.1.	Stacja Zarządzania Typ 1	55
6.1.1.	Jednostka główna spełniająca poniższe wymagania:	55
6.1.2.	Monitor	56
6.1.3.	Stacja dokująca	57
6.1.4.	Zestaw klawiatura z myszą	57
6.1.5.	Opis równoważności	58
7.	Dostawa systemu	59
7.1.	Ramowy plan dostaw	59
7.2.	Dostawa urządzeń i oprogramowania	59
7.2.1.	Ogólne wytyczne dotyczące dostawy:	59
7.2.2.	Miejsce dostawy	60
8.	Gwarancja	61
8.1.	Ogólne warunki Gwarancji	61
8.2.	Opis usługi Gwarancji	62

PN 70/09/2023 – dostawa elementów obliczeniowych

8.2.1.	Diagnostyka i rozwiązywanie problemów	62
8.2.2.	Klasyfikacja problemów.....	63
8.2.3.	Poziomy świadczenia usługi	63
8.2.4.	Wymiana informacji pomiędzy Zamawiającym a Wykonawcą	64
8.2.5.	Zgłaszanie problemów.....	64
8.2.6.	Czas reakcji	65
8.2.7.	Rozwiązanie problemu	65
8.2.8.	Czas rozwiązania problemu	66
8.2.9.	Przywrócenie systemu.....	66
8.2.10.	Czas przywrócenia systemu.....	66
8.2.11.	Rozwiązanie zgłoszenia problemu.....	67
8.2.12.	Konsultacje	67
8.2.13.	Dostarczanie i wsparcie w instalacji Oprogramowania.....	68
8.2.14.	Szczegółowe wymagania gwarancji dotyczące elementów Systemu, z wyłączeniem stacji zarządzania.....	68
8.2.15.	Szczegółowe wymagania gwarancji dotyczące Stacji Zarządzania.....	69

IV. SZCZEGÓŁOWE WYMAGANIA DOTYCZĄCE PRZEDMIOTU ZAMÓWIENIA

1. Definicje używane w dokumencie:

Na potrzeby niniejszego dokumentu przyjęto następujące definicje:

- 1) **RU** – jednostka do określenia wysokości obudowy danego urządzenia, wysokości szafy teleinformatycznej (ang. rack unit), 44.45 mm;
- 2) **dzień roboczy** – poniedziałek, wtorek, środa, czwartek i piątek z wyjątkiem dni ustawowo wolnych od pracy w Polsce;
- 3) **czas reakcji na zgłoszenie awarii/wady** – czas, który upłynie od momentu zgłoszenia awarii/wady do podjęcia czynności naprawczych ze strony Wykonawcy; nie dotyczy dostarczanego oprogramowania, dla którego obowiązują warunki gwarancji producenta oraz pozycji dla których przewidziana jest wymiana wadliwego towaru na wolny od wad;
- 4) **czas naprawy/wymiany** – czas liczony od przybycia serwisu po zgłoszeniu awarii/wady liczony do momentu dokonania skutecznej naprawy albo wymiany wadliwego towaru na wolny od wad. Nie dotyczy dostarczanego oprogramowania, dla którego obowiązują warunki gwarancji producenta oraz pozycji dla których przewidziana jest wymiana wadliwego towaru na wolny od wad.
- 5) **Komponent** – element funkcjonalny składające się na System, np. serwer, macierz obiektowa, system wizualizacji.
- 6) **System** – oznacza urządzenia, oprogramowanie i aplikacje spełniające wymagania opisane w SWZ, które mają być dostarczone i wdrożone przez Wykonawcę w celu realizacji przedmiotu niniejszego Zamówienia.

2. Serwery obliczeniowe

2.1. Serwer – parametry wspólne dla każdego typu serwera

Parametr	Charakterystyka (wymagania minimalne)
Obudowa	<ol style="list-style-type: none"> 1) Obudowa zapewniająca poprawny montaż w szafie teleinformatycznej 19" o głębokości 120 cm wraz z akcesoriami opisanym w podpunkcie poniżej (2). 2) Obudowa musi zostać dostarczona wraz z zestawem szyn i ramieniem porządkującym ułożenie przewodów umożliwiającym pełne wysunięcie serwera do celów serwisowych bez potrzeby odłączania przewodów podłączonych do zasilaczy i kart sieciowych oraz umożliwiającym bezprzerwowe serwisowanie serwera, w tym minimum wymianę dysków oraz wentylatorów i zasilaczy. 3) Obudowa umożliwiająca instalację dysków 2,5" SATA/SAS/NVMe.
Płyta główna	<ol style="list-style-type: none"> 1) Płyta główna z możliwością zainstalowania dwóch procesorów. 2) Na płycie głównej muszą znajdować się minimum 32 gniazda przeznaczone do instalacji pamięci. 3) Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym. 4) Płyta główna musi obsługiwać interfejs PCIe 4.0
Wbudowane porty	<ol style="list-style-type: none"> 1) Minimum 1 port USB 2.0 lub wyższy na przednim panelu serwera. 2) Minimum 1 port USB 3.0 lub wyższy na tylnym panelu. 3) Minimum 1 port VGA.
Wentylatory	<ol style="list-style-type: none"> 1) Redundantne typu Hot-Plug.
Bezpieczeństwo	<ol style="list-style-type: none"> 1) Panel przedni zamykany na klucz służący do ochrony przed nieautoryzowanym dostępem do dysków twardej. 2) Funkcja wyłączenia w BIOS funkcji przycisku zasilania. 3) BIOS musi mieć możliwość przejścia do bezpiecznego trybu rozruchowego z funkcją zarządzania blokadą zasilania, zmianą ustawień BIOS, zmianą hasła do BIOS. 4) Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą. 5) Wbudowany moduł TPM minimum 2.0. 6) Funkcjonalność włączania i wyłączania portów USB na obudowie. 7) Możliwość wymazania danych z dysków znajdujących się wewnątrz serwera: <ol style="list-style-type: none"> a) niezależne od zainstalowanego systemu operacyjnego, b) uruchamiane z poziomu systemu zarządzania serwerem. 8) Serwer musi spełniać wymagania normy NIST SP 800-193 ochrony przed cyberatakami.

	<p>9) Serwer musi być wyposażony w rozwiązanie zapewniające ochronę oprogramowania układowego (ang. firmware) przed manipulacją ze strony złośliwego oprogramowania.</p> <p>a) Ochrona taka musi być zgodna z zaleceniami NIST SP 800-147B.</p> <p>b) Zamawiający wymaga, aby dostarczony serwer posiadał zaimplementowane sprzętowo mechanizmy kryptograficzne poświadczające integralność oprogramowania BIOS (Root of Trust).</p> <p>10) Serwer musi umożliwiać utworzenie bezpiecznego profilu w oparciu o konfigurację sprzętową oraz o konfigurację wewnętrznego oprogramowania komponentów serwera. Jakikolwiek odchylenie od profilu musi zostać automatycznie zgłoszone administratorowi.</p> <p>11) Dla zapewnienia odpowiedniego poziomu bezpieczeństwa wszystkie pakiety oprogramowania układowego muszą być podpisane cyfrowo za pomocą kryptograficznej funkcji skrótu (ang. hash) SHA-256 z 2048-bitowym szyfrowaniem lub silniejszym. Serwer musi skanować aktualizacje oprogramowania układowego i porównywać ich sygnatury za pomocą wbudowanego w sprzęt łańcucha zaufania.</p>
Karta Zarządzania	<p>Serwer musi być wyposażony w kartę na potrzeby zdalnego zarządzania. Karta musi być niezależna od zainstalowanego na serwerze systemu operacyjnego, posiadać dedykowany port RJ-45 Gigabit Ethernet oraz musi zapewniać:</p> <ol style="list-style-type: none"> 1) zdalny dostęp do graficznego interfejsu www karty zarządzającej, interfejs www musi być wykonany w standardzie HTML5 2) szyfrowane połączenie (TLS) oraz uwierzytelnienie i autoryzację użytkownika 3) funkcję zdalnego włączenia, wyłączenia, restartu serwera 4) odczyt dzienników zdarzeń (ang. logs) dotyczących serwera 5) podmontowanie zdalnych napędów wirtualnych 6) uruchomienie wirtualnej konsoli z dostępem do myszy i klawiatury 7) wsparcie dla protokołu IPv4 i IPv6 8) wsparcie dla protokołów: SNMP, IPMI2.0, VLAN tagging, SSH 9) funkcję zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer, dane historyczne muszą być dostępne dla min. 7 dni wstecz 10) funkcję zdalnego ustawienia limitu poboru prądu przez serwer 11) integrację z Microsoft Active Directory lub LDAP w zakresie uwierzytelnienia i autoryzacji kont dostępowych 12) obsługę przez minimum trzech administratorów jednocześnie 13) wsparcie dla automatycznej rejestracji w systemie DNS 14) wysyłanie do administratorów wiadomości e-mail z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej 15) zarządzanie bezpośrednio poprzez złącze USB 16) monitorowanie zużycia dysków SSD 17) automatyczne zgłaszanie alertów do centrum serwisowego producenta

	<p>18) aktualizacje oprogramowania układowego (ang. firmware) dla wszystkich komponentów serwera</p> <p>19) przywrócenie poprzednich wersji oprogramowania układowego</p> <p>20) funkcję eksportu/importu konfiguracji (ustawienie karty zarządzającej, BIOSu, kart sieciowych, HBA oraz konfiguracji kontrolera RAID) serwera do/z pliku XML lub JSON</p> <p>21) funkcję automatycznego tworzenia kopii konfiguracji serwera w oparciu o zdefiniowany harmonogram</p> <p>22) wykrywanie odchyłeń konfiguracji na poziomie konfiguracji UEFI oraz wersji oprogramowania układowego serwera</p> <p>23) uruchomienie funkcjonalności umożliwiającej dostęp bezpośrednio poprzez urządzenia mobilne – funkcja konfiguracji oraz monitorowania najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej (Android/Apple iOS) używając jednego z protokołów BLE lub WIFI</p> <p>24) zdalne wyłączenia i włączenia portów USB</p> <p>25) mechanizm bezpiecznego wycofywania z eksploatacji poprzez automatyczne usuwanie poufnych danych w tym minimum:</p> <ul style="list-style-type: none"> a) konfiguracji BIOS b) konfiguracji kontrolera RAID c) dzienników systemowych d) danych konfiguracyjnych e) wszystkich danych z nośników wewnętrznych (dyski twarde, DCPMM, NVDIMM). <p>Jeśli wymagana jest dodatkowa licencja na jakąkolwiek funkcjonalność wskazaną przez zamawiającego to musi ona być dostarczona wraz z serwerem w wersji bez ograniczeń czasowych. Ponadto Zamawiający wymaga, aby żadna z powyższych funkcjonalności nie wymagała okresowego sprawdzania licencji na zewnętrznych systemach (np. producenta).</p>
System do zarządzania	<p>1) System do zarządzania serwerami wraz z niezbędną licencją, który musi spełniać niżej wymienione wymagania:</p> <ul style="list-style-type: none"> a) integracja z Microsoft Active Directory lub LDAP w zakresie uwierzytelnienia i autoryzacji kont dostępowych b) zarządzanie dostarczonymi serwerami bez udziału dedykowanego agenta c) wsparcie dla protokołów SNMP, IPMI, Linux SSH, Redfish d) uruchamianie procesu wykrywania urządzeń w oparciu o harmonogram e) szczegółowy opis wykrytych systemów oraz ich komponentów f) funkcja eksportu raportu do min. CSV, HTML, XLS, PDF g) funkcja tworzenia własnych raportów w oparciu o wszystkie informacje zawarte w inwentarzu h) grupowanie serwerów w oparciu o kryteria użytkownika

	<ul style="list-style-type: none">i) tworzenie automatycznie grup serwerów w oparciu o dowolny element konfiguracji serwera np. nazwa, lokalizacja, system operacyjny, obsadzenie slotów PCIe, pozostały czas gwarancjij) podgląd stanu środowiska zawierający najważniejsze informacje na jego tematk) podsumowanie stanu dla każdego serweral) szczegółowy status serwera i jego elementów/komponentówm) filtry raportów umożliwiające podgląd wybranych zdarzeńn) integracja z systemem do obsługi zgłoszeń producenta dostarczonej platformy sprzętowejo) możliwość uruchomienia/przechwycenia wirtualnej konsoli serwerap) możliwość podmontowania wirtualnego napędu na zarządzanym serwerzeq) kreator umożliwiający dostosowanie akcji dla wybranych alertówr) możliwość importu plików MIBs) możliwość definiowania ról administratorówt) możliwość zdalnej aktualizacji oprogramowania układowego serwerówu) możliwość aktualizacji oprogramowania układowego oparta o wybrane źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania)v) możliwość aktualizacji oprogramowania układowego (ang. firmware) bez potrzeby instalacji agenta na serwerzew) możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerówx) moduł raportujący pozwalający na wygenerowanie raportu zawierającego co najmniej następujące informacje:<ul style="list-style-type: none">i) numery seryjne serwerówii) konfiguracje poszczególnych serwerówiii) wersje oprogramowania wewnętrznegoiv) obsadzenie slotów PCI i gniazd pamięciv) informacje o maszynach wirtualnychvi) aktualne informacje o stanie i poziomie gwarancjivii) adresy IP kart sieciowychviii) występujące alertyix) adresy MAC kart sieciowychx) stan poszczególnych komponentów serwerówy) możliwość tworzenia sprzętowej konfiguracji bazowej i na jej podstawie weryfikacji środowiska w celu wykrycia rozbieżnościz) wdrażanie serwerów w oparciu o profile konfiguracjiaa) możliwość migracji ustawień serwera wraz z wirtualnymi adresami sieciowymi (MAC, WWN, IQN) między serwerami
--	--

	<p>bb) tworzenie gotowych paczek informacji umożliwiających zdiagnozowanie awarii serwera przez serwis producenta</p> <p>cc) zdalne uruchamianie diagnostyki serwera.</p> <p>2) System może być zaoferowany jako prekonfigurowany obraz maszyny wirtualnej (ang. virtual appliance) dla zaoferowanego oprogramowania do wirtualizacji mocy obliczeniowej.</p> <p>3) Musi być dostępna dedykowana aplikacja na urządzenia mobilne (Android/Apple iOS) integrująca się z wyżej opisanym systemem do zarządzania.</p> <p>Jeśli wymagana jest dodatkowa licencja na jakąkolwiek funkcjonalność wskazaną przez zamawiającego to musi ona być dostarczona wraz z serwerem w wersji bez ograniczeń czasowych. Ponadto Zamawiający wymaga, aby żadna z powyższych funkcjonalności nie wymagała okresowego sprawdzania licencji na zewnętrznych systemach (np. producenta).</p>
Diagnostyka	<p>1) Serwer musi być wyposażony w panel LCD dedykowany przez producenta do zaoferowanej obudowy umożliwiający sprawdzenie stanu pracy serwera (umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, zasilania i o temperaturze oraz wyświetlenie tekstu zdefiniowanego przez Zamawiającego (np. nr inwentarzowy, nr serwera)).</p>
Zasilacze	<p>1) Minimum 2 szt., redundantne, typu Hot-Plug, o sprawności Platinum, o mocy zapewniającej poprawną pracę serwera w zaoferowanej konfiguracji przy pracy na połowie zainstalowanych zasilaczy.</p>
Certyfikaty	<p>1) Microsoft Windows Server min. w wersji 2022 – zgodność potwierdzona dla oferowanego modelu serwera na stronie: https://www.windowsservercatalog.com/</p> <p>2) Red Hat Enterprise Linux (RHEL) min. w wersji 8 – zgodność potwierdzona dla oferowanego modelu serwera na stronie: https://access.redhat.com/ecosystem/hardware</p> <p>3) VMware ESXi min. w wersji 7 – zgodność potwierdzona dla oferowanego modelu serwera na stronie: https://www.vmware.com/resources/compatibility/search.php</p>
Dokumentacja użytkownika	<p>1) Zamawiający wymaga dostarczenia dokumentacji w języku polskim lub angielskim w wersji elektronicznej.</p>

2.2. Oprogramowanie do zarządzania serwerami z poziomu konsoli oprogramowania do zarządzania klastrem wirtualizacyjnym

Oprogramowanie do zarządzania serwerami z poziomu konsoli oprogramowania do zarządzania klastrem wirtualizacyjnym (zwanej dalej konsolą wirtualizatora) musi być zintegrowane z zaferowaną konsolą oprogramowania do zarządzania klastrem wirtualizacyjnym (opisaną w niniejszych wymaganiach).

Wymagania, które musi spełniać to oprogramowanie:

- 1) możliwość instalowania poprawek podnoszących wersję oprogramowania układowego (ang. firmware) serwera wprost z konsoli wirtualizatora (wymagana zgodność z zaferowanym oprogramowaniem wirtualizacyjnym)
- 2) instalacja poprawek dla klastra serwerów musi uwzględniać specyfikę pracy tego klastra i brać pod uwagę środowisko wirtualizatora, aby nie wpływać na stan maszyn wirtualnych, tzn. przełączać kolejno aktualizowany serwer w tryb serwisowy, instalować poprawkę, przełączać z powrotem w tryb produkcyjny zanim uruchomi proces na kolejnym serwerze
- 3) konsola wirtualizatora musi prezentować szczegółowe informacje o serwerze takie jak ilość oraz typ komponentu dla co najmniej:
 - a) procesor
 - b) pamięć RAM
 - c) karty I/O
 - d) wentylatory
 - e) dyski pamięci masowej
- 4) konsola wirtualizatora musi prezentować informacje wspierające serwisowanie takie jak:
 - a) numer serwisowy/seryjny serwera
 - b) data obowiązywania gwarancji
- 5) informacje sprzętowe i alerty muszą być prezentowane w konsoli wirtualizatora i mogą być używane tak jak inne alerty wirtualizatora w zakresie ustawień powiadomień, potwierdzania przeczytania alertów oraz używania ich w regułach automatyzujących zarządzanie alertami
- 6) konsola wirtualizatora musi pozwalać na ustawienie bazowej konfiguracji dla serwerów (wersje oprogramowania układowego, wersje sterowników) oraz raportowanie odchylenia wersji na poszczególnych serwerach względem konfiguracji bazowej

2.3. Serwery obliczeniowe typu A, B, C

Wymagania wspólne dla serwerów typu A, B, C

Parametr	Charakterystyka (wymagania minimalne)
Obudowa	1) Wysokość 2 RU
Kontroler RAID	1) Sprzętowy kontroler dyskowy wspierający interfejs PCIe 4.0, z pojemnością cache minimum 4 GB, umożliwiający konfigurację RAID 0, 1, 5, 6, 10, 50, 60 oraz wyposażony w baterię do podtrzymania pamięci cache w przypadku zaniku zasilania. 2) Kontroler musi być zgodny z zaferowanym oprogramowaniem do wirtualizacji.

Interfejsy sieciowe	<ol style="list-style-type: none"> 1) Dwa interfejsy sieciowe o przepustowości 1 Gb/s Ethernet w standardzie Base-T. 2) Dwuportowa karta sieciowa zainstalowana w serwerze jako karta rozszerzeń w slocie PCIe 4.0, z gniazdami o przepustowości 100 Gb/s Ethernet w standardzie QSFP56, posiadająca: <ol style="list-style-type: none"> a) interfejs PCIe 4.0 x16 b) wsparcie dla wirtualizacji SR-IOV oraz VirtIO c) sprzętowe wsparcie dla szyfrowania AES-GCM 128/256 dla protokołów IPsec i TLS, wsparcie dla AES-XTS d) wydajność min. 215 Mpps e) wsparcie dla RoCE Programmable Congestion Control f) wsparcie dla IEEE 1588v2 g) sprzętowe wsparcie enkapsulacji i deenkapsulacji dla protokołów VxLAN, NVGRE, Geneve h) wsparcie dla Jumbo Frames o rozmiarach minimum 9 KB. 3) Dwuportowa karta sieciowa zainstalowana w serwerze jako karta rozszerzeń w slocie PCIe lub w slocie z interfejsem OCP 3.0, z gniazdami o przepustowości 25 Gb/s Ethernet w standardzie SFP28, wspierająca również gniazda 10 Gb/s Ethernet w standardzie SFP+, posiadająca: <ol style="list-style-type: none"> a) wsparcie dla wirtualizacji SR-IOV b) wsparcie dla enkapsulacji i deenkapsulacji dla protokołów VxLAN, NVGRE, Geneve c) wsparcie dla RoCE d) wsparcie dla Jumbo Frames o rozmiarach minimum 9 KB. <p>Karty opisane w pkt. 2) i 3) muszą poprawnie współpracować z modułami optycznymi (zgodnymi z ogólnie przyjętymi normami właściwymi dla danego typu interfejsu) pochodzącymi od różnych producentów. Obsługa modułów optycznych innych producentów nie może wymagać instalacji dodatkowego oprogramowania lub zmian w konfiguracji karty.</p>
---------------------	---

2.4. Serwer obliczeniowy typu „A”

Zaferowany serwer musi spełniać wszystkie wymagania wspólne opisane w punkcie 2.1 oraz wymagania wspólne dla podzbioru typu serwów opisane w punkcie 2.3 oraz poniższe wymagania.

Parametr	Charakterystyka (wymagania minimalne)
Procesor	<ol style="list-style-type: none"> 1) Zainstalowane 2 procesory 64-rdzeniowe, o taktowaniu co najmniej 2.0 GHz, klasy x86-64 do pracy z zaferowanym serwerem umożliwiające osiągnięcie wyniku podstawowego (Base) min. 605 punktów w teście CPU2017 Floating Point Rate. Wynik dla zaferowanego modelu serwera w konfiguracji z zaproponowanymi procesorami musi być dostępny na stronie www.spec.org 2) Procesor musi obsługiwać interfejs PCIe 4.0.

Pamięć RAM	1) Minimum 2 TB DDR4 RDIMM 3200 MT/s w konfiguracji wypełniającej wszystkie gniazda pamięci na płycie głównej. Płyta główna musi zapewniać obsługę do co najmniej 4 TB pamięci RAM.
Dyski twarde	1) Zainstalowane 2 jednakowe dyski twarde hot-swap o pojemności minimum 480 GB każdy, SATA SSD do różnych zastosowań (ang. mixed-use) o współczynniku DWPD minimum 3 i rozmiarze 2,5", podłączone za pomocą zaoferowanego kontrolera RAID.

2.5. Serwer obliczeniowy typu „B”

Zaoferowany serwer musi spełniać wszystkie wymagania wspólne opisane w punkcie 2.1 oraz wymagania wspólne dla podzbioru typu serwów opisane w punkcie 2.3 oraz poniższe wymagania.

Parametr	Charakterystyka (wymagania minimalne)
Procesor	1) Zainstalowane 2 procesory 32-rdzeniowe, o taktowaniu co najmniej 2.2 GHz, klasy x86-64 do pracy z zaoferowanym serwerem umożliwiające osiągnięcie wyniku podstawowego (Base) min. 393 punktów w teście CPU2017 Floating Point Rate. Wynik dla zaoferowanego modelu serwera w konfiguracji z zaproponowanymi procesorami musi być dostępny na stronie www.spec.org 2) Procesor musi obsługiwać interfejs PCIe 4.0.
Pamięć RAM	1) Minimum 1 TB DDR4 RDIMM 3200 MT/s. Płyta główna musi zapewniać obsługę co najmniej 4 TB pamięci RAM.
Dyski twarde	1) Zainstalowane 2 jednakowe dyski twarde hot-swap o pojemności minimum 480 GB każdy, SATA SSD do różnych zastosowań (ang. mixed-use) o współczynniku DWPD minimum 3 i rozmiarze 2,5", podłączone za pomocą zaoferowanego kontrolera RAID.

2.6. Dodatkowe wyposażenie serwerów

Wszystkie poniższe elementy muszą być kompatybilne i możliwe do zainstalowania do zaoferowanych w ramach tego postępowania serwerach. Gwarancja na komponenty musi być na tych samych warunkach co na serwery.

2.6.1. Dysk SSD

Parametr	Charakterystyka (wymagania minimalne)
Typ	Dysk twarde w specyfikacji serwerowej, certyfikowany przez producenta serwera
Rodzaj nośnika	SSD
Interfejs	1 x SATA 6 Gb/s
Pojemność	480GB
Funkcje dodatkowe	1) Funkcja hot-swap 2) Dysk SSD zoptymalizowany pod kątem zapisu i odczytu danych (wykorzystanie mieszane)

2.6.2. Dysk HDD

Parametr	Charakterystyka (wymagania minimalne)
Typ	Dysk twardej w specyfikacji serwerowej, certyfikowany przez producenta serwera
Rodzaj nośnika	HDD
Prędkość obrotowa	10000 obr/min
Interfejs	SAS 12Gb/s
Pojemność	2,4 TB
Funkcje dodatkowe	1) Funkcja hot-swap

2.6.3. Akcelerator graficzny typu „A”

Parametr	Charakterystyka (wymagania minimalne)
Typ	Akcelerator graficzny w specyfikacji serwerowej, certyfikowany przez producenta serwera
Liczba graficznych rdzeni obliczeniowych	Min. 6192 rdzeni CUDA
Liczba rdzeni wspierających uczenie maszynowe	Min. 432 wyspecjalizowanych rdzeni wspierających uczenie maszynowe
Pamięć VRAM	Min. 80GB typu HBM2e o szerokości szyny danych 5120bit
Częstotliwość GPU	1) Bazowa: min. 1060MHz 2) Boost: min. 1400MHz
Częstotliwość pamięci	Min. 1510MHz
Wsparcie wirtualizacji	1) Wsparcie dla wirtualizacji karty graficznej, w szczególności wsparcie dla mechanizmów umożliwiających przekazanie karty graficznej do kontenerów uruchamianych z wykorzystaniem technologii Docker 2) Możliwość partycjonowania karty graficznej na co najmniej 7, niezależnych, zwirtualizowanych kart graficznych
Interfejs	1) Interfejs PCIe co najmniej w wersji 4.0 x16 ze wsparciem dla „Lane and polarity reversal” 2) Karty muszą być połączone ze sobą (każda z każdą) szyną dwukierunkową o przepustowości minimum 600GB/s
Wsparcie dla API obliczeniowych	Wymagane wsparcie dla min. 4 różnych API, np. CUDA, DirectCompute, OpenCL, OpenACC
Wydajność	Min. 19 TFLOPS dla obliczeń FP32 wg. deklaracji producenta

Zasilanie	Zużycie energii nie większe niż 300W, 8pinowe złącze zasilające
-----------	---

2.6.4.Karta sieciowa 100GbE

Parametr	Charakterystyka (wymagania minimalne)
Typ	Karta sieciowa w specyfikacji serwerowej, certyfikowana przez producenta serwera
Maksymalna przepustowość	200Gb/s, 2 porty QSFP56
Interfejsy	1) Wsparcie dla prędkości 10/25/40/50/100/200GbE 2) Urządzenie przeznaczone do działania z interfejsem PCIe Gen4.0 x16,
Liczba portów	2 porty sieciowe
Wirtualizacja	Wsparcie dla SR-IOV oraz VirtIO
Cyberbezpieczeństwo	Sprzętowe wsparcie dla szyfrowania AES-GCM 128/256 dla protokołów IPSec i TLS. Wsparcie dla AES-XTS
Wydajność	DPDK message rate: min. 215Mpps
Wspierane funkcje	RoCE Programmable Congestion Control, IEEE 1588v2 (dokładność do poziomu nanosekund), Sprzętowe wsparcie enkapsulacji i dekapulacji dla VXLAN, NVGRE, Geneve

2.6.5.Karta FPGGA

Parametr	Charakterystyka (wymagania minimalne)
Typ	Akcelerator FPGA w specyfikacji serwerowej, certyfikowany przez producenta serwera
Pamięć	Min. 64GB pamięci DDR o min. przepustowości 75GB/s i wydajności min. 2400MT/s
Interfejsy	1) 2x QSFP28 100Gbps 2) PCI-e Gen3 x16
Liczba portów	2 porty sieciowe
Parametry FPGA	1) Min. 1182000 LUT 2) 2364000 rejestrów 3) 6840 DSP slices
Typ chłodzenia	Pasywne
Zasilanie	Maks. 250W

3. Serwer dyskowy

3.1. Serwer dyskowy typu „C”

Parametr	Charakterystyka (wymagania minimalne)
Zasoby dyskowe	<p>1) Serwer dyskowy / macierz dyskowa musi być dostarczona z minimum:</p> <p>a) 10 jednakowymi dyskami SSD 2,5" o współczynniku DWPD minimum 3 (w przypadku zastosowania dysków o DWPD mniejszym od 3 należy dostarczyć dwukrotnie większą pojemność na dyskach SSD) – pojemność użyteczna dla przestrzeni zbudowanej w oparciu o te dyski musi wynosić minimum 22 TiB</p> <p>b) 9 jednakowymi dyskami SAS (HDD 10k lub SSD) 2,5" – pojemność użyteczna dla przestrzeni zbudowanej w oparciu o te dyski musi wynosić minimum 12 TiB.</p> <p>Pojemność użyteczną macierzy dyskowej należy rozumieć jako pojemność prezentowaną do serwerów i pozwalającą na rzeczywisty zapis danych o tej objętości na macierzy bez uwzględnienia mechanizmów redukcji danych. Pojemność użyteczna to pojemność po odliczeniu wszelkich narzutów związanych z organizacją danych na dyskach takich jak przechowywanie parzystości, sum kontrolnych, danych systemowych, pojemności zapasowej, itp.</p> <p>2) Zastosowane mechanizmy ochrony danych muszą zabezpieczać dane przed ich utratą w przypadku awarii co najmniej 1 (jednego) dowolnego dysku każdej grupy dysków wymienionych w punkcie 1) a) i 1) b).</p> <p>3) Należy dodatkowo uwzględnić dyski zapasowe („Hot Spare”) w ilości zgodnej z zaleceniami producenta dla oferowanej konfiguracji – nie mniej niż 1 (jeden) zapasowy dysk dla każdej grupy dysków wymienionych w punkcie 1) a) i 1) b). Dyski zapasowe nie mogą być wliczone do ilości dysków z punktu 1).</p> <p>4) Podczas awarii dysku kontroler macierzy dyskowej musi automatycznie rozpocząć odtwarzanie danych na fizycznym dysku zapasowym.</p> <p>5) W przypadku stosowania dysku zapasowego proces odtwarzania danych nie może wiązać się z procesem przenoszenia danych po wymianie dysku uszkodzonego (dysk wymieniony musi być automatycznie uznany za zapasowy).</p> <p>6) Kontrolery macierzy dyskowej muszą obsługiwać minimum 500 dysków.</p>
Kontrolery macierzy dyskowej	<p>1) Macierz dyskowa musi być złożona z minimum jednej pary identycznych kontrolerów tworzących klaster wysokiej dostępności (ang. high availability cluster). Kontrolery muszą udostępniać dane poprzez protokoły iSCSI, Fibre Channel, CIFS oraz NFS.</p> <p>2) Obszar pamięci cache przeznaczony do zapisów danych musi posiadać lustrzaną kopię (ang. mirror).</p> <p>3) W przypadku awarii zasilania dane niezapisane na dyskach muszą być zabezpieczone za pomocą podtrzymania baterijnego w celu zachowania ich w pamięci nieulotnej kontrolera do momentu przywrócenia zasilania.</p>

	<ol style="list-style-type: none"> 4) Kontrolery w klastrze wysokiej dostępności muszą oferować funkcjonalność automatycznego przejmowania funkcjonalności i zadań w przypadku awarii drugiego kontrolera w tej samej parze. 5) Macierz musi mieć minimum 128 GB pamięci cache obsługującej zapis i odczyt dostępnej dla wszystkich wolumenów macierzy. Włączenie lub wyłączenie pamięci cache nie może wymagać operacji usunięcia i utworzenia na nowo wolumenów lub grup dyskowych. Nie dopuszcza się stosowania pamięci na wymiennych dyskach jako podstawowego modułu cache. 6) Macierz dyskowa musi realizować replikację (ang. mirroring) pamięci cache między kontrolerami. 7) System operacyjny kontrolerów musi natywnie obsługiwać automatyczny „tiering” bloków danych pomiędzy dyskami SSD, SAS (macierz może alokować bloki dla danego wolumenu spośród wszystkich typów dysków: SSD, SAS równocześnie). 8) Macierz musi mieć możliwość obsługi różnych poziomów RAID równocześnie, minimum RAID 1 (lub 10), 5, 6. 9) Awaria dowolnego pojedynczego aktywnego elementu macierzy dyskowej nie może powodować przerwy w dostępie do danych. 10) Musi być możliwe utworzenie minimum 1000 wolumenów blokowych o rozmiarze minimum 256 TB, plikowych o rozmiarze minimum 256 TB. 11) Macierz musi posiadać wbudowaną funkcjonalność typu „thin provisioning” umożliwiającą alokację wirtualnej przestrzeni dyskowej, do której fizyczne dyski mogą być dostarczone w przyszłości.
Interfejsy	<ol style="list-style-type: none"> 1) Macierz musi być wyposażona w następujące, działające porty: <ol style="list-style-type: none"> a) 8 portów 25 Gb/s Ethernet do podłączania serwerów, każdy port wyposażony w moduł optyczny SFP28 b) 2 porty 1 Gb/s Ethernet Base-T do zdalnego zarządzania kontrolerem c) 4 porty SAS minimum 12 Gb/s do podłączania półek dyskowych d) opcjonalnie 4 porty 10 Gb/s Ethernet do podłączania serwerów, każdy port wyposażony w moduł optyczny SFP+. 2) Interfejsy optyczne opisane w punkcie 1) muszą współpracować z modułami optycznymi (zgodnymi z ogólnie przyjętymi normami właściwymi dla danego typu interfejsu) pochodzącymi od różnych producentów. 3) Porty przeznaczone do podłączenia serwerów nie mogą być wykorzystane do połączeń wewnątrz macierzy (np. pomiędzy kontrolerami). 4) Musi być możliwość rozbudowy on-line macierzy do minimum 16 portów FC 32 Gb/s lub 25 Gb/s Ethernet jedynie poprzez instalację dodatkowych kart rozszerzeń bez konieczności instalacji dodatkowych kontrolerów bądź usuwania zainstalowanych kart.
Kopie migawkowe	<ol style="list-style-type: none"> 1) System operacyjny macierzy dyskowej musi natywnie obsługiwać mechanizm kopii migawkowych, który będzie dostępny dla wszystkich rodzajów danych udostępnianych. Niedopuszczalne są rozwiązania wykonujące kopie

	<p>migawkowe jedynie w trybie „Copy On Write” dla dowolnego rodzaju danych (blokowe lub plikowe).</p> <ol style="list-style-type: none"> 2) Odtwarzanie plików i folderów z kopii migawkowych wykonanych dla wolumenów plikowych udostępnionych dla systemów typu Windows i Unix musi być dostępne za pomocą wydzielonego udziału sieciowego z zachowaniem praw dostępu na poziomie użytkownika. 3) System operacyjny macierzy dyskowej musi umożliwiać wykonywanie kopii migawkowych wolumenów plikowych w trybie „on-line” – bez zatrzymywania operacji odczytu i zapisu. Deklarowana przez producenta liczba kopii migawkowych musi wynosić minimum 256 na wolumen. 4) Musi być możliwe odtwarzanie danych z kopii migawkowych bezpośrednio na wolumen produkcyjny. 5) Musi być możliwe udostępnienie kopii migawkowej w trybie do odczytu i zapisu. 6) Należy dostarczyć oprogramowanie do wykonywania spójnych kopii danych aplikacji: Microsoft SQL Server, Oracle Databases, VMware dla blokowych i plikowych „datastore” oraz zaoferowanego oprogramowania do wirtualizacji zasobów serwerowych i ich mocy obliczeniowej. Spójne kopie rozumiane jako funkcjonalność automatycznego przełączenia aplikacji w tryb wykonania spójnej kopii swoich danych. Oprogramowanie to musi rozpoznać, na których wolumenach logicznych aplikacja składa swoje dane i wykonać kopie tylko tych wolumenów.
<p>Obsługiwane protokoły</p>	<ol style="list-style-type: none"> 1) System operacyjny macierzy dyskowej musi udostępniać dane za pomocą protokołu CIFS i Fibre Channel – jeśli do uruchomienia potrzebna jest licencja, to Zamawiający wymaga jej dostarczenia. System operacyjny macierzy dyskowej musi mieć możliwość uruchomienia udostępniania danych za pomocą protokołów NFS oraz iSCSI - licencje na protokoły CIFS, NFS, Fibre Channel oraz iSCSI są przedmiotem obecnego postępowania. 2) Jednoczesna obsługa różnych protokołów dostępu do danych nie może być zrealizowana za pomocą dodatkowego oprogramowania ani dodatkowych urządzeń pośredniczących typu wirtualizator, gateway, switch, itp. firm trzecich.
<p>Pozostałe wymagania</p>	<ol style="list-style-type: none"> 1) System operacyjny macierzy dyskowej musi umożliwiać dynamiczną zmianę rozmiaru wolumenów danych (zwiększanie) bez przerywania pracy i bez przerywania użytkownikom zewnętrznym dostępu do danych. 2) System operacyjny macierzy, za pomocą interfejsu graficznego, musi mieć możliwość: <ol style="list-style-type: none"> a) konfiguracji macierzy dyskowej b) zbierania i wyświetlania informacji o stanie zasobów macierzy dyskowej c) prezentowania i gromadzenia zdarzeń zachodzących w macierzy dyskowej d) prezentowania bieżących statystyk wydajnościowych macierzy dyskowej e) podglądu parametrów wydajnościowych macierzy dyskowej w czasie rzeczywistym.

	<ol style="list-style-type: none"> 3) Dostęp do CLI systemu operacyjnego kontrolerów musi odbywać się przy użyciu połączenia szyfrowanego. 4) W systemie operacyjnym kontrolera musi być możliwość utworzenia wirtualnych serwerów plików, a każdy wirtualny serwer plików musi obsługiwać użytkowników z innej domeny Microsoft (MS Active Directory). 5) W celu zabezpieczania danych macierz dyskowa musi mieć mechanizm replikacji jej zasobów na zasoby innej macierzy tej samej rodziny. Replikacja musi działać na poziomie systemu operacyjnego macierzy. Macierz musi mieć mechanizm replikacji w trybie synchronicznym i asynchronicznym bez potrzeby użycia urządzeń zewnętrznych typu gateway, serwer pośredniczący, etc. Musi istnieć funkcja odwrócenia kierunku replikacji. Replikacja danych między macierzami nie może być realizowana przy użyciu zewnętrznego oprogramowania. Licencja na replikację jest przedmiotem obecnego postępowania. 6) System operacyjny kontrolerów macierzy musi oferować funkcjonalność QoS (ang. Quality of Service) dla dowolnego wolumenu blokowego, to znaczy musi być możliwość ograniczenia liczby operacji na sekundę lub przepustowości w kB (lub innych jednostkach) na sekundę, jaka jest możliwa do uzyskania ze wskazanego przez administratora wolumenu. 7) Wymagane jest szyfrowanie danych na dyskach. Należy dostarczyć niezbędne licencje na całą pojemność macierzy. 8) Macierz musi posiadać funkcję zarządzania w sposób zautomatyzowany. Zamawiający dopuszcza możliwość zastosowania oprogramowania firm trzecich np. Ansible. 9) Jeśli wymagana jest dodatkowa licencja na jakąkolwiek funkcjonalność wskazaną przez Zamawiającego to musi ona być dostarczona wraz z macierzą. 10) Wszystkie kontrolery muszą posiadać tą samą liczbę portów w identycznej konfiguracji.
Gwarancja	<ol style="list-style-type: none"> 1) 7 lat gwarancji realizowanej w miejscu instalacji sprzętu, z czasem reakcji następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii w trybie 365x7x24 poprzez ogólnopolską linię telefoniczną producenta. Stałe monitorowanie macierzy przez zdalne centrum serwisowe.
Wymiana dysków	<ol style="list-style-type: none"> 1) Wymiana dysków może być dokonywana samodzielnie przez Zamawiającego. 2) Zamawiający zatrzymuje uszkodzone dyski.

4. Oprogramowanie do wirtualizacji

Zaoferowane oprogramowanie do wirtualizacji musi być w pełni kompatybilne ze sobą w ramach wszystkich zaoferowanych modułów, których specyfikację zawarto w poniższych podpunktach. Zaoferowanie oprogramowania do wirtualizacji wraz z wszystkimi wymaganymi modułami od jednego producenta będzie dodatkowo punktowane.

4.1. Wymagania wspólne dla wszystkich modułów oprogramowania do wirtualizacji

- 1) Producent zaoferowanego oprogramowania do wirtualizacji musi wspierać rozwiązania do automatyzacji procesów oraz wirtualizacji sieci (SDN, ang. Software-Defined Networking).
- 2) Licencjonowanie zaoferowanego oprogramowania lub zapewnienie udzielenia licencji na zaoferowane oprogramowanie spełniające wymagania opisane w tym rozdziale musi posiadać możliwość swobodnego przeniesienia praw do użytkowania na dowolny podmiot wymieniony w umowie i dowolny serwer fizyczny będący w posiadaniu Zamawiającego (bez ograniczeń licencji OEM). Licencje dostępne w modelu licencjonowania na procesor fizyczny.

4.2. Oprogramowanie do wirtualizacji zasobów serwerowych i ich mocy obliczeniowej w wersji podstawowej

- 1) Zaoferowane oprogramowanie do wirtualizacji zasobów serwerowych i ich mocy obliczeniowej w wersji podstawowej musi:
 - a) być instalowane bezpośrednio na sprzęcie fizycznym i nie może być ono częścią innego systemu operacyjnego
 - b) alokować dla własnych celów nie więcej niż 600MB pamięci operacyjnej RAM serwera fizycznego
 - c) potrafić obsłużyć i wykorzystać zasoby fizyczne serwera: 2 procesory fizyczne, co najmniej 128 logicznych wątków procesora, 2TB pamięci fizycznej RAM
 - d) zapewniać możliwość skonfigurowania maszyn wirtualnych z możliwością przydzielenia od 1 do minimum 256 procesorów wirtualnych
 - e) zapewniać możliwość skonfigurowania maszyn wirtualnych z możliwością przydzielenia minimum 4 TB pamięci operacyjnej RAM
 - f) zapewniać 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
 - g) zapewniać możliwość skonfigurowania maszyn wirtualnych, z których każda może mieć 32 porty szeregowo, 3 porty równoległe i 20 urządzeń USB
 - h) wspierać następujące systemy operacyjne: Windows Server 2012, Windows Server 2016, Windows Server 2019, Windows 7, Windows 8, Windows 10, SLES 12, SLES 11, SLES 10, RHEL 8, REHL 7, Solaris 11, Debian, CentOS, FreeBSD, Ubuntu, Oracle Linux, CoreOS
 - i) umożliwiać przydzielenie łącznie większej ilości pamięci RAM dla maszyn wirtualnych niż fizyczne zasoby RAM serwera, na którym maszyny te są umieszczone

PN 70/09/2023 – dostawa elementów obliczeniowych

- j) umożliwić udostępnienie maszynie wirtualnej większej ilości zasobów dyskowych niż jest fizycznie dostępne na zasobach dyskowych
- k) zapewniać wsparcie dla wirtualizacji zagnieżdżonej, w szczególności w zakresie możliwości zastosowania wszystkich funkcjonalności co najmniej dla wirtualizatora (ang. hypervisor) Microsoft Hyper-V pakietu Microsoft Windows Server 2016 i nowszego na maszynie wirtualnej
- l) umożliwiać integrację z rozwiązaniami antywirusowymi firm trzecich w zakresie skanowania maszyn wirtualnych z poziomu warstwy wirtualizacji bez ingerencji w systemy operacyjne maszyn wirtualnych
- m) 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 administratora („root“)
- n) zapewniać możliwość powielania maszyn wirtualnych wraz z ich pełną konfiguracją i danymi
- o) zapewniać możliwość wykonywania kopii migawkowych instancji systemów operacyjnych na potrzeby tworzenia kopii zapasowych bez przerywania ich pracy z możliwością zachowania stanu pamięci pracującej maszyny wirtualnej
- p) zapewniać możliwość dodawania zasobów w czasie pracy maszyny wirtualnej, w szczególności w zakresie ilości procesorów, pamięci operacyjnej i przestrzeni dyskowej
- q) posiadać funkcjonalność tworzenia wirtualnego przełącznika (ang. virtual switch) umożliwiającego tworzenie sieci wirtualnej w obszarze serwera wirtualizacyjnego (ang. hypervisor) i pozwalającego połączyć tym przełącznikiem maszyny wirtualne w obszarze jednego serwera, a także na zewnątrz sieci fizycznej. Pojedynczy przełącznik wirtualny powinien mieć możliwość konfiguracji minimum 4000 wirtualnych portów Ethernet
- r) w celu zapewnienia bezpieczeństwa połączenia ethernetowego w razie awarii fizycznej karty sieciowej pojedynczy wirtualny przełącznik, musi posiadać możliwość przyłączania do niego minimum dwóch fizycznych kart sieciowych
- s) posiadać funkcjonalność obsługi wirtualnych sieci lokalnych (VLAN) na wirtualnych przełącznikach w zaoferowanym oprogramowaniu
- t) zapewniać możliwość konfigurowania polityk separacji sieci w warstwie trzeciej, tak aby zapewnić oddzielne grupy wzajemnej komunikacji pomiędzy maszynami wirtualnymi
- u) umożliwiać wykorzystanie technologii przepustowości sieci komputerowych 200 GbE w tym agregację połączeń fizycznych do minimalizacji czasu przenoszenia maszyny wirtualnej pomiędzy serwerami fizycznymi
- v) obsługiwać przełączenie ścieżek LAN (bez utraty komunikacji) w przypadku awarii jednej ze ścieżek
- w) zapewniać możliwość zdefiniowania alertów informujących o przekroczeniu wartości progowych
- x) 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

PN 70/09/2023 – dostawa elementów obliczeniowych

- y) obsługiwać przełączenie ścieżek używanych przy dostępie do pamięci masowej bez utraty komunikacji w przypadku awarii jednej ze ścieżek
- z) 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
- aa) umożliwiać automatyczne, ponowne uruchomienie maszyn wirtualnych w przypadku awarii jednego z serwerów wirtualizacyjnych na kolejnym działającym w tym samym klastrze serwerze (funkcjonalność wysokiej dostępności, ang. High Availability, HA)
- bb) w środowisku z minimum dwoma serwerami wirtualizacyjnymi musi zapewniać pracę bez przestoju dla wybranych maszyn wirtualnych, niezależnie od systemu operacyjnego oraz aplikacji, podczas awarii serwera wirtualizacyjnego, bez utraty danych i dostępności danych na maszynach wirtualnych objętych ochroną
- cc) zapewniać możliwość obsługiwanie dysków wirtualnych maszyn do rozmiaru co najmniej 60 TB
- dd) posiadać funkcjonalność zarządzania poprzez ustandaryzowany interfejs programistyczny (API)
- ee) posiadać wbudowany interfejs programistyczny (API) zapewniający pełną integrację zewnętrznych rozwiązań wykonywania kopii zapasowych z istniejącymi mechanizmami warstwy wirtualizacyjnej
- ff) być kompatybilne z TPM 2.0. Minimalne wymaganie Zamawiającego dla TPM oznacza, że TPM zapewnia mechanizm gwarantujący, że serwer fizyczny, na którym zainstalowane jest zaferowane oprogramowanie, uruchomił się z włączoną opcją Secure Boot. Po potwierdzeniu, że Secure Boot jest włączone, system gwarantuje, poprzez weryfikację podpisu cyfrowego, że serwer wirtualizacyjny (ang. hypervisor) uruchomił się w niezmienionej formie
- gg) posiadać funkcjonalność wirtualnego TPM 2.0 dla maszyn wirtualnych z zainstalowanym Microsoft Windows 10, Microsoft Windows 2016 i nowszych. Zamawiający wymaga aby z punktu widzenia maszyny wirtualnej z systemem operacyjnym Microsoft Windows 10, Microsoft Windows 2016 i nowszym 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
- hh) posiadać funkcjonalność szybkiego uruchamiania oprogramowania wirtualizacyjnego po przeprowadzonym procesie jego aktualizacji. Zamawiający wymaga, aby w procesie aktualizacji oprogramowania, jeśli wymagany jest jego restart, funkcjonalność szybkiego uruchamiania powodowała eliminację czasochłonnej fazy inicjalizacji serwera fizycznego
- ii) wspierać protokół precyzyjnej synchronizacji czasu PTP (ang. Precision Time Protocol) i NTP (ang. Network Time Protocol)
- jj) posiadać mechanizm, który ogranicza dostęp do indywidualnego zarządzania warstwą wirtualizacji na serwerach fizycznych, w ramach klastra serwerów, w celu zwiększenia bezpieczeństwa dostępu warstwy wirtualizacji

- kk) 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
- ll) zapewniać podstawowe funkcje serwera zarządzania kluczami (KMS), które upraszcza włączenie szyfrowania i zaawansowanych funkcji bezpieczeństwa
- mm) mieć możliwość przenoszenia maszyn wirtualnych w czasie ich pracy pomiędzy serwerami fizycznymi, pamięciami masowymi (niezależnie od dostępności współdzielonej przestrzeni dyskowej), różnymi rodzajami wirtualnych przełączników sieciowych
- nn) posiadać co najmniej 2 niezależne mechanizmy wzajemnej komunikacji między serwerami z zainstalowanym oprogramowaniem wirtualizacyjnym oraz z serwerem zarządzającym tym oprogramowaniem, gwarantujące właściwe działanie mechanizmów wysokiej dostępności na wypadek izolacji sieciowej serwerów fizycznych lub partycjonowania sieci.

4.3. Oprogramowanie do wirtualizacji zasobów serwerowych i ich mocy obliczeniowej w wersji rozszerzonej

- 1) Zaoferowane oprogramowanie do wirtualizacji zasobów serwerowych i ich mocy obliczeniowej w wersji rozszerzonej musi spełniać wszystkie wymagania z wersji podstawowej (opisanej w punkcie 4.2).
- 2) Zaoferowane oprogramowanie do wirtualizacji zasobów serwerowych i ich mocy obliczeniowej w wersji rozszerzonej dodatkowo musi:
 - a) umożliwiać automatyczne równoważenie obciążenia procesora i pamięci operacyjnej serwerów fizycznych pracujących jako platforma dla infrastruktury wirtualnej
 - b) zapewniać mechanizm pozwalający tworzyć profil (szablon konfiguracji) wybranego serwera wirtualizacyjnego (ang. hypervisor), a następnie wymuszać ten profil/konfigurację na innych serwerach fizycznych lub sprawdzać zgodność konfiguracji pomiędzy zdefiniowanym wcześniej profilem a wskazanym serwerem fizycznym
 - c) w środowisku z minimalnie dwoma serwerami wirtualizacyjnym, w przypadku potrzeby wgrania aktualizacji do warstwy wirtualizacji, oprogramowanie musi posiadać możliwość automatycznego bezprzerwowego przeniesienia działających maszyn wirtualnych na inny serwer wirtualizacyjny, który nie jest objęty aktualizacją, przed rozpoczęciem samej aktualizacji
 - d) umożliwiać utworzenie w nim jednorodnego, wirtualnego przełącznika sieciowego, rozproszonego na wszystkie serwery fizyczne. Przełącznik taki musi:
 - i) zapewniać możliwość konfiguracji parametrów sieciowych maszyny wirtualnej z granulacją na poziomie portu tego przełącznika. Pojedyncza maszyna wirtualna musi mieć możliwość wykorzystania jednego lub wielu portów przełącznika z niezależną od siebie konfiguracją
 - ii) współpracować z protokołem NetFlow
 - iii) umożliwiać funkcjonalność duplikowania ruchu sieciowego dowolnego jego portu wirtualnego na inny port

PN 70/09/2023 – dostawa elementów obliczeniowych

- iv) mieć wbudowane mechanizmy składowania kopii konfiguracji, przywracania tej kopii a także mechanizmy automatycznie zapobiegające niewłaściwej konfiguracji sieciowej, które w całości lub w części mogą eliminować błędy ludzkie i utratę łączności sieciowej
- e) mieć wbudowany mechanizm kontrolowania i monitorowania ruchu sieciowego oraz ustalania priorytetów w zależności od jego rodzaju na poziomie konkretnych maszyn wirtualnych
- f) w środowisku z minimum dwoma serwerami wirtualizacyjnymi, zapewniać pracę bez przestoju dla wybranych maszyn wirtualnych (o minimalnie czterech procesorach wirtualnych), niezależnie od systemu operacyjnego oraz aplikacji, podczas awarii serwera wirtualizacyjnego, bez utraty danych i dostępności danych na maszynach wirtualnych objętych ochroną
- g) mieć możliwość grupowania pamięci masowych o podobnych parametrach w grupy i przydzielania ich do wirtualnych maszyn zgodnie z ustaloną przez administratora polityką
- h) umożliwiać udostępnianie pojedynczego urządzenia fizycznego (PCIe) jako logicznie separowanego wirtualnego urządzenia dedykowanego dla poszczególnych maszyn wirtualnych
- i) mieć możliwość równoważenia obciążenia i zajętości pamięci masowych wraz z pełną automatyką i przenoszeniem plików wirtualnych maszyn z bardziej zajętych na mniej zajęte przestrzenie dyskowe lub/i z przestrzeni dyskowych bardziej obciążonych operacjami I/O na mniej obciążone
- j) wspierać technologię rozproszonego udostępniania procesora graficznego Nvidia Grid vGPU zainstalowanego w serwerze fizycznym do maszyn wirtualnych
- k) wspierać funkcjonalność trwałej, nieulotnej pamięci (ang. Persistent Memory)
- l) posiadać certyfikację dla pakietu NVIDIA AI Enterprise, natywnego dla chmury zbioru zoptymalizowanych aplikacji sztucznej inteligencji (AI) i systemów (ang. framework) przeznaczonych dla kompleksowego rozwiązania AI
- m) mieć wbudowany mechanizm kontrolowania i monitorowania ruchu do pamięci masowych oraz ustalania priorytetów dostępu do nich na poziomie konkretnych wirtualnych maszyn
- n) umożliwiać uruchamianie kontenerów zbudowanych w topologii Docker Image
- o) wspierać protokół Remote Direct Memory Access (RDMA) poprzez konwergentny Ethernet – RoCE w wersji „v2”, Fiber Channel over Ethernet (FCoE) i iSCSI rozszerzenie dla RDMA (iSER). Wymaga się aby maszyny wirtualne można było konfigurować z wykorzystaniem protokołu RDMA

4.4. Oprogramowanie do zarządzania klastrem wirtualizacyjnym

- 1) Zaoferowane oprogramowanie do zarządzania musi:
 - a) posiadać konsolę graficzną do zarządzania maszynami wirtualnymi i do konfigurowania innych funkcjonalności – zasobów dyskowych oraz zasobów sieci komputerowej. Konsola graficzna powinna działać jako zainstalowana aplikacja na maszynie wirtualnej. Dodatkowo wymaga się aby powyższa maszyna z aplikacją była wstępnie skonfigurowana

PN 70/09/2023 – dostawa elementów obliczeniowych

- i dostępna jako tzw. virtual appliance. Instalacja ww. virtual appliance nie może wiązać się z potrzebą dostawy dodatkowego oprogramowania takiego jak np. system operacyjny lub baza danych. Virtual appliance musi być uruchomiony za pomocą dostarczonego oprogramowania do wirtualizacji zasobów serwerowych i ich mocy obliczeniowej (zwanym dalej „wirtualizatorem”)
- b) posiadać wbudowany serwer zapory sieciowej (ang. firewall) dający możliwość konfiguracji blokady lub akceptacji ruchu pomiędzy konsolą zarządzającą a serwerami oraz maszynami wirtualnymi na nich uruchomionymi, przy założeniu blokowania całego ruchu a nie poszczególnych portów
 - c) mieć możliwość konfiguracji uwierzytelniania użytkowników logujących się do niego w oparciu o minimum: domenę Microsoft Active Directory i Open LDAP
 - d) posiadać konsole graficzną, która musi być dostępna poprzez przeglądarkę internetową (co najmniej przez Google Chrome i Mozilla Firefox) i być wykonana z wykorzystaniem języka HTML5
 - e) posiadać funkcjonalność zcentralizowanego zarządzania hostami opartymi na rozwiązaniu dostarczanego wirtualizatora
 - f) posiadać natywne mechanizmy do wykonywania kopii zapasowej swojej konfiguracji. Dodatkowo wymaga się możliwości ustawienia harmonogramu wykonywania kopii zapasowej. Wymaga się aby mechanizm kopii zapasowych wspierał protokoły: FTPS, HTTPS, SCP, FTP oraz http
 - g) posiadać interfejs graficzny do prowadzenia prac administracyjnych w zakresie swojej konfiguracji oraz monitoringu (możliwość monitorowania obciążenia takich zasobów jak vCPU, vRAM, vHDD, sieci, bazy danych). Interfejs graficzny musi być wykonany w standardzie HTML5
 - h) posiadać możliwość konfiguracji dostarczonego oprogramowania do wirtualizacji zasobów serwerowych i ich mocy obliczeniowej poprzez użycie schematów konfiguracji i umożliwiać załadowanie takiego schematu dla wielu serwerów równocześnie
 - i) umożliwiać jednoczesną aktualizację oprogramowania na wielu dostarczanych wirtualizatorach
 - j) zapewniać natywne mechanizmy wysokiej dostępności (ang. High Availability, HA) w niezawodnej architekturze Active-Passive-Witness dla wszystkich składowych komponentów centralnej konsoli graficznej zarządzającej platformą wirtualną
 - k) w przypadku zarządzania serwerami opartymi o dostarczany wirtualizator zasobów serwerowych i ich mocy obliczeniowej, musi prezentować poziom zbalansowania obciążenia w klastrze opartym o ww. wirtualizatory
 - l) umożliwiać dostęp przez przeglądarkę do konsoli graficznej w sposób skalowalny tj. powinien umożliwiać rozdzielenie komponentów na wiele instancji w przypadku zapotrzebowania na dużą liczbę jednoczesnych dostępuów administracyjnych do środowiska.

4.5. Oprogramowanie do wirtualizacji sieci

- 1) Zaoferowane oprogramowanie do wirtualizacji sieci w wersji podstawowej musi:
 - a) oferować możliwość budowy sieci komunikacyjnych z wykorzystaniem protokołu IP w oparciu o środowiska wirtualne zintegrowane z zaoferowanym oprogramowaniem do wirtualizacji zasobów serwerowych i ich mocy obliczeniowej
 - b) zapewniać funkcjonalność tworzenia wirtualnych sieci w sposób niezależny od topologii sieci fizycznej i używanych w obrębie tej sieci protokołów sieciowych
 - c) posiadać funkcję tworzenia rozproszonego, wirtualnego przełącznika instalowanego bezpośrednio w zaoferowanym oprogramowaniu do wirtualizacji zasobów serwerowych i ich mocy obliczeniowej (ang. hypervisor), umożliwiającego tworzenie logicznych segmentów sieci w warstwie drugiej modelu ISO/OSI
 - d) posiadać funkcję tworzenia rozproszonego, wirtualnego routera instalowanego bezpośrednio w zaoferowanym oprogramowaniu do wirtualizacji zasobów serwerowych i ich mocy obliczeniowej (ang. hypervisor), zapewniającego funkcję bramy domyślnej dla środowiska serwerów wirtualnych. Brama domyślna musi działać w trybie rozproszonym. Przełączanie pakietów w warstwie sieci modelu ISO/OSI musi odbywać się w obrębie fizycznego serwera, bez wynoszenia ruchu do fizycznych przełączników (poza środowisko wirtualizacyjne)
 - e) posiadać możliwość kreowania segmentów sieci wirtualnej przy użyciu technologii VxLAN i/lub GENEVE (ang. Generic Network Virtualization Encapsulation)
 - f) zapewnić funkcjonalność łączenia (ang. bridging) środowiska zwirtualizowanego opartego o technologię VxLAN/GENEVE z środowiskiem niezvirtualizowanym zdefiniowanego za pomocą technologii VLAN
 - g) zapewniać funkcjonalność wirtualnego routera wspierającego protokół routingu BGP. Routing statyczny oraz BGP musi być możliwy do wykonania poprzez tunel GRE
 - h) zapewniać funkcjonalność łączenia segmentów sieci w warstwie drugiej VLAN i GENEVE poprzez zastosowanie wirtualnej bramy
 - i) zapewniać funkcjonalność translowania adresów IP zarówno dla ruchu wychodzącego ze środowiska wirtualnego (SNAT) jak i przychodzącego do środowiska wirtualnego (DNAT)
 - j) posiadać funkcjonalność serwera DHCP w celu dynamicznego nadawania adresów IP dla środowiska zwirtualizowanego
 - k) posiadać interfejs programistyczny (API) umożliwiający automatyzowanie wdrażania lub modyfikacji konfiguracji sieci wirtualnych
 - l) umożliwiać tworzenie planów aktualizacji oraz zapewniać mechanizmy sprawdzenia poprawności działania systemu przed i po aktualizacji
 - m) zapewniać bezpieczeństwo transmisji danych (filtracja pakietów) na poziomie wirtualnego interfejsu sieciowego maszyny wirtualnej jak również dla całości transmisji danych (włączając w to transmisję pomiędzy wirtualnymi maszynami w tym samym wirtualnym segmencie sieci) bez wynoszenia ruchu do fizycznych urządzeń w warstwie L2-L4 modelu ISO/OSI na zewnątrz (poza warstwę wirtualizacji mocy obliczeniowej)
 - n) posiadać funkcjonalność rozproszonej, stanowej zapory sieciowej (ang. firewall), realizowanej bezpośrednio na poziomie wirtualnego interfejsu sieciowego maszyny wirtualnej, umożliwiającej tworzenie polityk bezpieczeństwa w warstwach L2-L4 modelu

PN 70/09/2023 – dostawa elementów obliczeniowych

ISO/OSI. Zapora ta musi umożliwiać definiowanie reguł do warstwy L7 modelu ISO/OSI dla wybranych aplikacji, w celu zapewnienia kontroli przepływu danych oraz planowania mikrosegmentacji

- o) zapewniać możliwość tworzenia reguł firewall w trybie bezstanowym dla różnych grup wirtualnych serwerów
- p) zapewniać możliwość tworzenia reguł polityk bezpieczeństwa z wykorzystaniem parametrów takich jak adres IP, porty i protokoły, dodatkowe parametry obiektów, tj. nazwa maszyny wirtualnej, nazwa przełącznika wirtualnego, nazwa grupy maszyn wirtualnych, system operacyjny wirtualnej maszyny
- q) zabezpieczać środowisko wirtualne przed nieautoryzowaną zmianą adresu IP wirtualnej maszyny, poprzez zablokowanie ruchu z i do tej wirtualnej maszyny po zmianie jej adresu IP w sposób nieautoryzowany
- r) posiadać możliwość zestawienia tuneli „IPsec Site-to-Site” z uwierzytelnieniem za pomocą współdzielonego klucza (ang. pre-shared key) lub certyfikatu.

5. Infrastruktura sieciowa

5.1. Infrastruktura przełączająca i system sterujący

Wszystkie zawarte poniżej wymagania są wymaganiami minimalnymi, należy zaoferować urządzenie zapewniające co najmniej podane parametry i funkcje.

I.p	Wymaganie	100GbE	25GbE	10GbE	1GbE
Typy i minimalne ilości wymaganych portów					
1	Ilość portów 400GbE (QSFP-DD)				
2	Ilość portów 100GbE (QSFP)	32	8	8	
3	Ilość portów 1/10/25GbE (SFP+)		48		4
4	Ilość portów 10GbE (10GBase-T)			48	
5	Ilość portów 1GbE (1000Base-T), wykluczając porty dedykowane do zarządzania				48
6	Interfejsy 400GbE muszą umożliwiać rozdzielanie na cztery interfejsy do pracy z szybkością 100GbE (ang. breakout)				
7	Interfejsy 100GbE muszą umożliwiać rozdzielanie na cztery interfejsy do pracy z szybkością 25GbE (ang. breakout)	Tak	Tak	Tak	
1	Wysokość elementu liczona w jednostkach Rack Units [RU]	1RU	1RU	1RU	1RU
2	Przełącznik musi poprawnie pracować w temperaturze od 0 do 40 °C.	Tak	Tak	Tak	Tak
3	Przełącznik musi poprawnie pracować przy względnej wilgotności powietrza co najmniej w zakresie od 5% do 95% zakładając brak występowania zjawiska kondensacji pary wodnej.	Tak	Tak	Tak	Tak

I.p	Wymaganie	100GbE	25GbE	10GbE	1GbE
4	W celu zachowania redundancji zasilania, każdy przełącznik musi poprawnie działać po podłączeniu do dwóch niezależnych, obwodów napięcia przemiennego (AC). Zanik napięcia na jednym z obwodów zasilających, nie może spowodować przerwy w działaniu przełącznika oraz ograniczenia jego funkcjonalności i wydajności (w zakresie wymaganym przez zamawiającego). Przełącznik musi być wyposażony w co najmniej dwa zasilacze. Dostarczone zasilacze muszą umożliwiać poprawną pracę przełącznika w pełnej (wymaganej przez zamawiającego) konfiguracji z wykorzystaniem połowy zainstalowanych zasilaczy.	Tak	Tak	Tak	Tak
5	Przepływ powietrza (związany z działaniem wentylatorów urządzenia) musi odbywać się w kierunku od frontu (porty we/wy) do tyłu urządzenia. UWAGA: możliwa zmiana kierunku zgodnie z zapisami w punkcie Błąd! Nie można odnaleźć źródła odwołania., które należy uwzględnić przed realizacją.	Tak	Tak	Tak	Tak
7	Przełącznik musi umożliwiać instalację, wymianę lub zamianę poszczególnych modułów (takich jak np. karty z interfejsami sieciowymi,	Tak	Tak	Tak	Tak

I.p	Wymaganie	100GbE	25GbE	10GbE	1GbE
	moduły optyczne) w trakcie pracy urządzenia (hot-swap).				
8	Przełącznik musi umożliwiać instalację lub wymianę zasilaczy w trakcie pracy urządzenia (hot-swap).	Tak	Tak	Tak	
Wymagania licencyjne i status urządzeń					
1	Wszystkie przełączniki oraz elementy współpracujące z nimi (np. moduły optyczne) muszą być fabrycznie nowe (tj. nieużywane z wyjątkiem wykonania testów potrzebnych do sprawdzenia ich poprawnego działania). Na dzień złożenia oferty żadne z oferowanych urządzeń nie może być przeznaczone do wycofania ze sprzedaży przez producenta (ang. end of sale), ani nie może być wiadomym, że urządzenia te nie będą objęte pomocą techniczną producenta (ang. end of life).	Tak	Tak	Tak	Tak
2	Wszystkie Elementy przełączające i system zarządzania (wraz z działającym na nich oprogramowaniem sterującym) muszą pochodzić od jednego producenta. Nie dotyczy to Systemu Monitorowania Przepływów Pakietów, który może pochodzić od innego dostawcy.	Tak	Tak	Tak	Tak
3	Elementy muszą mieć odblokowane wszystkie wymagane funkcjonalności, a jeśli potrzebne są do tego licencje, dostawca musi je	Tak	Tak	Tak	Tak

l.p	Wymaganie	100GbE	25GbE	10GbE	1GbE
	<p>dostarczyć wraz z urządzeniami. Licencje nie mogą być ograniczone czasowo, terytorialnie, ani w żaden inny sposób wpływający na cel ich wykorzystania. Restart elementów nie może powodować konieczności wykonania prac serwisowych, utrzymaniowych lub konfiguracyjnych potrzebnych do odblokowania wszystkich wymaganych funkcjonalności. Licencje powinny być lokalne dla każdego urządzenia - nie dopuszcza się komunikacji z systemami trzecimi w celu utrzymywania/weryfikacji licencji.</p>				
4	<p>Wszystkie interfejsy liniowe przełączników muszą być odblokowane. Oznacza to, że nie mogą posiadać żadnych blokad umożliwiających ich wykorzystanie dopiero po wprowadzeniu jakiegokolwiek licencji, klucza, kodu lub innego mechanizmu odblokowującego. Dotyczy to wszystkich interfejsów znajdujących się fizycznie w oferowanych przełącznikach.</p>	Tak	Tak	Tak	Tak
5	<p>Moduły optyczne (ang. transceiver) muszą pochodzić od producenta elementów sieciowych lub posiadać jego certyfikację do stosowania w elementach sieciowych. Jednakże karty liniowe, moduły</p>	Tak	Tak	Tak	Tak

l.p	Wymaganie	100GbE	25GbE	10GbE	1GbE
	<p>lub porty przełącznika zawierające interfejsy przeznaczone do obsadzenia modułami optycznymi, muszą współpracować z modułami optycznymi (zgodnymi z ogólnie przyjętymi normami właściwymi dla danego typu interfejsu), pochodzącymi od różnych producentów. Restart przełącznika nie może powodować konieczności wykonania prac serwisowych, utrzymaniowych lub konfiguracyjnych, które pozwolą na wykorzystywanie modułów optycznych innych producentów.</p>				
6	<p>Wszystkie Elementy przełączające muszą pracować z tą samą (identyczną) wersją oprogramowania. Oprogramowanie musi być oficjalną wersją oferowaną przez producenta oraz być w komercyjnie dostępnej wersji, tj. wersji oferowanej wszystkim klientom. Wersja ta musi być wersją rekomendowaną przez producenta. Niedopuszczalne jest wykorzystanie oprogramowania prototypowego, wytwarzanie wersji oprogramowania wyłącznie na potrzeby zamawiającego, nieoferowanej innym klientom.</p>	Tak	Tak	Tak	Tak
Minimalne wymagania wydajnościowe i pojemnościowe					

I.p	Wymaganie	100GbE	25GbE	10GbE	1GbE
1	Wydajność przełączania co najmniej	6.4 Tbps	4.0 Tbps	2.5 Tbps	290Gbps
2	Liczba przetwarzanych pakietów na sekundę	2 Bpps	1 Bpps	1 Bpps	200Mpps
3	Czas przełączania ramek nie dłuższy niż	1 μ s	1 μ s	3 μ s	3 μ s
4	Całkowita wielkość buforów	32MB	32MB	32MB	4MB
5	Minimalna liczba obsługiwanych adresów MAC	280 000	280 000	280 000	60 000
6	Minimalna liczba adresów sieci (nie hostów) IP wersji 4, która musi być zaprogramowana do sprzętowego przełączania pakietów w bazie FIB (ang. Forwarding Information Base).	360 000	360 000	360 000	16 000
7	Minimalna liczba adresów sieci IP o prefiksie /64 (nie hostów) wersji 6, która musi być zaprogramowana do sprzętowego przełączania pakietów w bazie FIB (ang. Forwarding Information Base)	190 000	190 000	190 000	4 000
8	Obsługa protokołu MACSEC				
9	Ilość jednocześnie aktywnych VLANów	4096	4096	4096	1024
10	Całkowita maksymalna moc pobierana przez urządzenie	370W	310W	350W	110W
11	Maksymalna typowa moc pobierana przez urządzenie	200W	130W	220W	95W
Wymagania operacyjne					
1	Moduły optyczne dla interfejsów muszą umożliwiać sprawdzenie mocy odbieranego sygnału.	Tak	Tak	Tak	Tak
2	Element Przełączający musi mieć możliwość dostarczania danych o parametrach jakościowych łączy do innych Elementów. Parametry	Tak	Tak	Tak	Tak

I.p	Wymaganie	100GbE	25GbE	10GbE	1GbE
	określone są jako Opóźnienie (ang. Latency), Zmiany Opóźnień (ang. Jitter), Straty pakietów (ang. Packet Loss). Dane te muszą być poprawnie interpretowane i prezentowane w Systemie Zarządzania.				
3	Elementy Przełączające muszą umożliwiać konfigurację z interfejsu tekstowego (ang. CLI) z potwierdzeniem (ang. Commit), gdzie po wprowadzeniu modyfikacji operator potwierdza wszystkie zmiany jednocześnie. Przy wykorzystaniu trybu z potwierdzeniem powinna być możliwość automatycznego wycofania wszystkich wprowadzonych modyfikacji (ang. rollback).	Tak	Tak	Tak	Tak
4	System operacyjny Elementów Przełączających powinien umożliwiać monitorowanie i obrazowanie przetwarzanych pakietów w trybie tekstowym skierowanych do CPU/Modułu zarządzającego – odpowiednik narzędzia Linux TCPDUMP.	Tak	Tak	Tak	Tak
5	Elementy Przełączające muszą umożliwiać konfigurację wykorzystując modele OpenConfig. Musi być zapewniona obsługa następujących protokołów: gRPC, RESTCONF, NETCONF.	Tak	Tak	Tak	Tak
6	Elementy Przełączające muszą zapewniać strumieniowanie danych telemetrycznych	Tak	Tak	Tak	Tak

I.p	Wymaganie	100GbE	25GbE	10GbE	1GbE
	wykorzystując protokół NETCONF/gRPC lub w formacie GPB. Dane te muszą być poprawnie interpretowane i prezentowane w Systemie Zarządzania.				
7	Wszystkie Elementy przełączające muszą umożliwiać kopiowanie ruchu z wybranych interfejsów na inny wskazany interfejs (ang. SPAN, Mirroring). Musi istnieć możliwość skonfigurowania minimalnie 4 aktywnych sesji kopiowania ruchu.	Tak	Tak	Tak	Tak
8	Wszystkie Elementy przełączające muszą obsługiwać protokoły NTP i NTP6	Tak	Tak	Tak	Tak
9	Wszystkie Elementy przełączające muszą obsługiwać protokół LLDP	Tak	Tak	Tak	Tak
10	Wszystkie Elementy przełączające muszą umożliwiać dodanie wydzielonej tablicy routingu dla funkcji zarządzania (ang. Management VRF)	Tak	Tak	Tak	Tak
11	Wszystkie Elementy przełączające muszą umożliwiać wykonywanie skryptów inicjowanych określonymi zdarzeniami (ang. Event driven scripts).	Tak	Tak	Tak	Tak
12	Wszystkie Elementy przełączające muszą zapewniać mechanizm sprzętowej ochrony przeciw atakowi przeciążającemu (ang. DoS) na	Tak	Tak	Tak	Tak

I.p	Wymaganie	100GbE	25GbE	10GbE	1GbE
	jednostkę sterującą CPU (ang. Control Plane Protection)				
Wymagania dla obsługi VXLAN					
1	Elementy przełączające muszą zapewniać sprzętowo obsługę enkapsulacji VXLAN. Jednocześnie przy enkapsulacji musi być możliwa obsługa przełączania w warstwie L2 (ang. bridging).	Tak	Tak	Tak	Tak
2	Elementy przełączające muszą zapewniać sprzętowo obsługę enkapsulacji VXLAN. Jednocześnie, przy enkapsulacji musi być możliwa obsługa routingu IP.	Tak	Tak	Tak	Tak
3	Elementy przełączające muszą obsługiwać MP- BGP EVPN (Ethernet VPN) jako mechanizm sygnalizacyjny (ang. control-plane) dla enkapsulacji VXLAN. Musi być zapewniona obsługa L2 EVPN (Type-2), L3-EVPN (type-5) oraz jednoczesna obsługa routingu i bridging'u IRB.	Tak	Tak	Tak	Tak
4	Elementy przełączające muszą obsługiwać mechanizm protekcji grup linków Ethernet (LAG z LACP) poprzez podłączenie ich do co najmniej dwóch Elementów przełączających. To znaczy, pojedyncza wiązka LAG musi mieć możliwość zakończenia na co najmniej dwóch Elementach przełączających zapewniając w pełni aktywną komunikację na wszystkich linkach grupy.	Tak	Tak	Tak	Tak

I.p	Wymaganie	100GbE	25GbE	10GbE	1GbE
	<p>Protekcja musi zapewniać nieprzerwaną pracę w przypadku awarii dowolnego pojedynczego komponentu. Protekcja musi poprawnie współpracować z VXLAN, EVPN, SpanningTree.</p> <p>Jeśli implementacja protekcji wymaga dodatkowych portów które przenoszą ruch w czasie awarii wykonawca musi dostarczyć odpowiednie okablowanie o długości minimum 2.5m</p>				
Wymagania sieciowe					
1	Wszystkie Elementy przełączające muszą obsługiwać ramki Ethernet o wielkości co najmniej 9216 Bytes. Liczonej łącznie z preambułą (7 oktetów), polem FCS (4 oktety), Frame Delimiter (1 oktet) i Interframe Gap (12 oktetów).	Tak	Tak	Tak	Tak
2	Wszystkie Elementy przełączające muszą obsługiwać funkcję IGMP snooping (dla IGMPv2 oraz IGMPv3).	Tak	Tak	Tak	Tak
3	Wszystkie Elementy przełączające muszą obsługiwać agregację interfejsów z wykorzystaniem protokołu LACP (IEEE 802.3ad)	Tak	Tak	Tak	Tak
4	Wszystkie Elementy przełączające muszą umożliwić stworzenie protekcji terminującej zagregowane interfejsy (LAG) na dwu Elementach przełączających	Tak	Tak	Tak	Tak

I.p	Wymaganie	100GbE	25GbE	10GbE	1GbE
	(ang. Dual Homing). W ramach takiej protekcji wszystkie porty zagregowanego połączenia LAG muszą aktywnie przenosić dane (ang. Active/Active). Awaria jednego Elementu nie może wpływać na status połączenia zagregowanego. Jeśli implementacja protekcji wymaga dodatkowych portów które przenoszą ruch w czasie awarii wykonawca musi dostarczyć odpowiednie okablowanie o długości minimum 2.5m				
5	Wszystkie Elementy przełączające muszą obsługiwać 802.1w RSTP, 802.1s MSTP.	Tak	Tak	Tak	Tak
6	Wszystkie Elementy przełączające muszą umożliwiać tworzenie list bezpieczeństwa (ang. ACLs) na warstwie L2 (MAC ACL), warstwie L3 (IP) i warstwie L4 (porty).	Tak	Tak	Tak	Tak
7	Wszystkie Elementy przełączające muszą obsługiwać protokół 802.1Qbb PFC (Priority-based Flow Control).	Tak	Tak	Tak	Tak
8	Wszystkie Elementy przełączające muszą umożliwiać regulację (ang. Shaping) wielkości ruchu wyjściowego.	Tak	Tak	Tak	Tak
9	Wszystkie Elementy przełączające muszą umożliwiać ograniczanie (ang. Policing) wielkości ruchu wyjściowego.	Tak	Tak	Tak	Tak
10	Wszystkie Elementy przełączające zapewniać	Tak	Tak	Tak	Tak

I.p	Wymaganie	100GbE	25GbE	10GbE	1GbE
	statyczny routing IP oraz dynamiczny routing IP zgodny z OSPFv2, OSPFv3, BGP, ISIS.				
11	Wszystkie Elementy przełączające muszą zapewniać mechanizm dystrybucji pakietów IP poprzez ścieżki z równym kosztem (ang. Equal Cost Multi-Path routing ECMP).	Tak	Tak	Tak	Tak
12	Wszystkie Elementy przełączające muszą zapewniać możliwość tworzenia polityk dla routing IP (ang. Route Maps).	Tak	Tak	Tak	Tak
13	Wszystkie Elementy przełączające muszą zapewniać możliwość dystrybucji informacji routingowych pomiędzy różnymi wirtualnymi tablicami routingowymi (ang. VRF route leaking).	Tak	Tak	Tak	Tak
14	Wszystkie Elementy przełączające muszą obsługiwać protokół BFD.	Tak	Tak	Tak	Tak
System Zarządzania (System sterujący)					
Wymagania ogólne					
1	Licencja dostarczona wraz z systemem zarządzania nie może ograniczać liczby ani użytkowników, ani administratorów korzystających jednocześnie z platformy systemu zarządzania.	Tak	Tak	Tak	Tak
2	System Zarządzania musi być dostarczony jako skonfigurowany obraz maszyny wirtualnej do uruchomienia na platformie KVM lub VMWare. Maksymalne wymagania Systemu Zarządzania nie mogą	Tak	Tak	Tak	Tak

I.p	Wymaganie	100GbE	25GbE	10GbE	1GbE
	przekroczyć 16 cores CPU, 32 GB RAM, 1TB HDD. Jeśli System Zarządzania przekracza te wymagania wykonawca musi dostarczyć platformę sprzętową, która zapewni odpowiednie parametry.				
3	Licencja dostarczona wraz z systemem zarządzania musi umożliwić stworzenie klastra maszyn wirtualnych pracujących w trybie wysokiej dostępności tak, aby awaria wyłączająca jedną z maszyn wirtualnych nie powodowała przerwy w działaniu systemu zarządzania.	Tak	Tak	Tak	Tak
4	Interfejs użytkownika systemu zarządzania musi być dostępny z poziomu przeglądarki WWW z prawidłową obsługą co najmniej następujących przeglądarek: Microsoft Edge, Google Chrome, Firefox	Tak	Tak	Tak	Tak
5	System zarządzania musi obsługiwać jednoczesną pracę wielu użytkowników.	Tak	Tak	Tak	Tak
6	System Zarządzania musi zapewnić możliwość dodawania prywatnych identyfikatorów Elementów oraz interfejsów, które następnie wspomagają proces wyszukiwania.	Tak	Tak	Tak	Tak
7	System Zarządzania musi zapewniać możliwość zdalnego aktualizowania Elementów przełączających, z możliwością wycofania i przywrócenia poprzedniej wersji.	Tak	Tak	Tak	Tak

I.p	Wymaganie	100GbE	25GbE	10GbE	1GbE
8	System Zarządzania musi zapewniać możliwość zapisania i odtworzenia kopii zapasowej Modułów Konfiguracyjnych.	Tak	Tak	Tak	Tak
9	System Zarządzania musi zapewniać możliwość wykorzystania interfejsu programistycznego (REST API) do wykonywania typowych operacji konfigurowania takich jak tworzenie, dodawanie i implementowanie Modułów Konfiguracyjnych	Tak	Tak	Tak	Tak
10	Niedostępność systemu zarządzania nie może mieć jakiegokolwiek wpływu na urządzenia sieciowe zintegrowane z systemem zarządzania. W szczególności nie może uniemożliwiać lub ograniczać możliwość konfiguracji urządzeń sieciowych za pomocą interfejsu CLI.	Tak	Tak	Tak	Tak
11	System zarządzania musi posiadać możliwość realizacji funkcji AAA poprzez integrację z zewnętrznym serwerem Radius oraz z zewnętrznym serwerem TACACS (przy czym nie jest wymagana integracja z dwoma tymi serwerami jednocześnie)	Tak	Tak	Tak	Tak
12	System zarządzania musi posiadać możliwość integracji z zewnętrznymi dostawcami usług uwierzytelnienia i tożsamości z wykorzystaniem standardów OAuth i SAML.	Tak	Tak	Tak	Tak

I.p	Wymaganie	100GbE	25GbE	10GbE	1GbE
13	System musi umożliwiać tworzenie token-ów dostępowych wykorzystywanych jako mechanizm uwierzytelnienia do REST API, które eksponuje system zarządzania. System musi umożliwiać przypisywanie uprawnień do poszczególnych token-ów w oparciu o role dostępowe. Te same role dostępowe powinny być wykorzystywane do zarządzania uprawnieniami użytkowników GUI.	Tak	Tak	Tak	Tak
Wymagania dla funkcji monitorowania					
1	System Zarządzania musi zbierać i prezentować alarmy generowane przez Elementy Przełączające. Alarmy muszą obejmować zdarzenia generowane przez syslog, zmiany stanu interfejsów, przekroczenia progów błędów na interfejsach wejściowych (CRC), przeciążenia ruchowe interfejsów wejściowych i wyjściowych. System Zarządzania musi zapewnić mechanizm potwierdzania alarmów i dodawania komentarzy. System Zarządzania musi zapewnić mechanizm wyróżniania ważności alarmów i zdarzeń oraz możliwość ich modyfikacji. Przy wyświetlaniu alarmów powinna być możliwość	Tak	Tak	Tak	Tak

I.p	Wymaganie	100GbE	25GbE	10GbE	1GbE
	filtrowania alarmów pod kątem ważności.				
2	<p>System zarządzania musi umożliwiać zbieranie i wizualizacja następujących parametrów: Parametry urządzenia: wykorzystanie CPU, pamięci RAM, temperatura pracy.</p> <p>Interfejsy: stan pracy (aktywny, wyłączony, itp.), statystyki ruchowe dla transmisji i odbioru, statystyki błędów, wartość MTU</p> <p>Ethernet: tablica MAC, wpisy ARP</p> <p>IP routing: zbudowana tablica routingu IPv4 i IPv6, (wliczając wirtualne tablice routingu VRF), BGP: numery AS, zestawione sąsiedztwa Parametry muszą być wizualizowane w czasie rzeczywistym oraz historycznie z możliwością wyboru dowolnego przedziału czasowego z ostatniego miesiąca zbieranych danych. System Zarządzania musi umożliwiać budowanie i komponowanie własnych zestawień parametrów do obserwacji.</p>	Tak	Tak	Tak	Tak
3	System zarządzania musi zapewniać wizualizację topologii połączeń. Topologia połączeń musi być automatycznie wykrywana i budowana.	Tak	Tak	Tak	Tak

I.p	Wymaganie	100GbE	25GbE	10GbE	1GbE
4	Na planie topologii system zarządzania musi wizualizować: wydarzenia i alarmy, szybkości interfejsów, wykorzystanie pasma, błędy w postaci utraconych pakietów, przepływy pakietów dla wskazanych par IP i protokołów.	Tak	Tak	Tak	Tak
5	System zarządzania musi zbierać i prezentować parametry jakości transmisji pomiędzy Elementami przełączającymi. Parametry określone są jako Opóźnienie (ang. Latency), Zmiany Opóźnień (ang. Jitter), Straty pakietów (ang. Packet Loss).	Tak	Tak	Tak	Tak
6	System zarządzania musi zbierać i prezentować informację o przepływach pakietów danych w postaci par IP i protokołów.	Tak	Tak	Tak	Tak
7	System zarządzania musi umożliwiać wyszukiwanie adresów IP oraz MAC widocznych z poziomu Elementów przełączających. Możliwość wyszukiwania dotyczy adresów statycznych i dynamicznych tablicach poszczególnych Elementów. Odnalezione adresy muszą być prezentowane wraz z kontekstem opisującym Elementy oraz interfejsy/tablice związane z danym adresem.	Tak	Tak	Tak	Tak
8	System zarządzania musi umożliwiać porównywanie i wizualizację różnic pomiędzy	Tak	Tak	Tak	Tak

l.p	Wymaganie	100GbE	25GbE	10GbE	1GbE
	<p>parametrami dla dwu dowolnych Elementów przełączających we wskazanych momentach czasowych. Parametrami podlegającymi porównaniu muszą być konfiguracje urządzeń, podstawowe tablice danych sieciowych (adresy IP, adresy MAC, wpisy ARP, sąsiedztwa sieciowe na bazie LLDP, tablice VXLAN, tablice NDP, tablice routingu IPv4, tablice routingu IPv6, tablice multicast IPv4). System musi umożliwiać równoczesne porównywanie stanu wymienionych metryk dwóch różnych urządzeń w niezależnych punktach czasu dla każdego z urządzeń. Np. Porównanie tablicy routingu IPv4 urządzenia A z godziny X z tablicą routingu urządzenia B z godziny Y.</p>				
9	<p>System Zarządzania musi na bieżąco (bez wymuszenia) sygnalizować modyfikację konfiguracji wykonaną z poziomu konsoli Elementów przełączający, która wprowadza różnicę pomiędzy konfiguracją budowaną przez System Zarządzania a wprowadzoną na urządzeniu. Administrator Systemu Zarządzania powinien mieć możliwość przywrócenia poprzedniej konfiguracji lub akceptacji zmian dokonanych na poziomie konsoli.</p>	Tak	Tak	Tak	Tak

I.p	Wymaganie	100GbE	25GbE	10GbE	1GbE
Wymagania dla funkcji zestawiania usług (ang. provisioning)					
1	System Zarządzania musi zapewnić automatyczną procedurę budowania konfiguracji początkowej (ang. ZTP „Zero Touch Provisioning”). W szczególności, nowe urządzenie, z konfiguracją fabryczną, po podłączeniu do sieci, powinno za pomocą DHCP odnaleźć system zarządzania a następnie pobrać konfigurację początkową i automatycznie zintegrować się z systemem zarządzania. Proces ten musi uwzględniać automatyczną aktualizację oprogramowania urządzenia sieciowego do wskazanej wersji.	Tak	Tak	Tak	Tak
2	System Zarządzania musi zapewnić automatyczną procedurę ładowania konfiguracji przy wymianie urządzenia (ang. „Zero Touch Replacement”). W szczególności, nowe urządzenie, z konfiguracją fabryczną, po podłączeniu do sieci, powinno za pomocą DHCP odnaleźć system zarządzania a następnie pobrać konfigurację urządzenia zastępowanego. Proces ten musi uwzględniać automatyczną aktualizację oprogramowania urządzenia sieciowego do takiej samej wersji jaka była wykorzystywana na urządzeniu zastępowanym.	Tak	Tak	Tak	Tak

I.p	Wymaganie	100GbE	25GbE	10GbE	1GbE
3	System Zarządzania musi umożliwiać budowanie konfiguracji Elementów. Konfiguracja musi być zgodna z konfiguracją tworzoną z wykorzystaniem interfejsu tekstowego (ang. Command Line Interface / CLI). Za pomocą systemu zarządzania musi istnieć możliwość skonfigurowania wszystkich parametrów Elementów przełączających.	Tak	Tak	Tak	Tak
4	Zintegrowanie Elementów przełączających z systemem zarządzania nie może wykluczać bezpośredniej pracy z interfejsami administracyjnymi Elementów. Rozwiązanie musi umożliwiać wymienną konfigurację Elementów: poprzez System Zarządzania lub bezpośrednio z wykorzystaniem interfejsu tekstowego (ang. CLI).	Tak	Tak	Tak	Tak
5	System Zarządzania musi umożliwiać definiowanie sekcji konfiguracji urządzeń, które są zarządzane poza Systemem Zarządzania i które mają przez System Zarządzania być ignorowane.	Tak	Tak	Tak	Tak
6	System Zarządzania musi wykrywać i wizualizować rozbieżności pomiędzy konfiguracją wynikającą z parametrów zdefiniowanych na Systemie Zarządzania oraz parametrów skonfigurowanych	Tak	Tak	Tak	Tak

I.p	Wymaganie	100GbE	25GbE	10GbE	1GbE
	bezpośrednio na urządzeniach sieciowych.				
7	System Zarządzania musi dostarczyć mechanizm budowania konfiguracji Elementów z wykorzystaniem Modułów Konfiguracyjnych (części konfiguracji CLI). Musi istnieć możliwość wykorzystania Modułów Konfiguracyjnych w trybie hierarchicznym, to znaczy że Moduł Konfiguracji jest dziedziczony przez wszystkie Elementy znajdujące się w danej hierarchii. Modyfikacja Modułu Konfiguracji musi powodować odpowiednią zmianę konfiguracji wszystkich Elementów znajdujących się w danej hierarchii.	Tak	Tak	Tak	Tak
8	Moduły Konfiguracji muszą być dostępne w trybie tekstowym (analogicznie jak pliki konfiguracyjne interfejsu tekstowego CLI). Ponadto, musi istnieć mechanizm automatyzacji tworzenia Modułów Konfiguracyjnych wykorzystując języka skryptów oparty na języku Python lub Perl. Tworzenie, testowanie, uruchamianie i zarządzanie skryptami Python/Perl musi w całości odbywać się poprzez interfejs GUI systemu zarządzania i musi stanowić integralną część tego systemu.	Tak	Tak	Tak	Tak

I.p	Wymaganie	100GbE	25GbE	10GbE	1GbE
9	System Zarządzania musi dostarczyć mechanizm weryfikacji oczekiwanych wyników przed implementacją Modułów Konfiguracyjnych na Elementach Przełączających. Po implementacji zmian konfiguracyjnych opisanych w Modułach Konfiguracyjnych musi istnieć mechanizm wycofania tych zmian.	Tak	Tak	Tak	Tak
10	System Zarządzania musi umożliwiać proces automatyzacji wielu zmian konfiguracyjnych i grupowania ich w pakiety. W ramach pakietów zmian, musi istnieć możliwość konfigurowania kolejności wykonywania poszczególnych zmian. System Zarządzania musi umożliwiać wybranie wykonywania zmian w pakiecie sekwencyjnie lub równoległe. System musi umożliwiać wykonywanie niestandardowych akcji (np. wykonania skryptu) jako jeden z elementów pakietów zmian. System musi umożliwiać zatrzymanie wykonywania kolejnych zmian w sekwencji, jeżeli zamiany je poprzedzające się nie powiodą. System musi umożliwiać zatwierdzanie pakietu zmian przez upoważnionego użytkownika zanim możliwe będzie uruchomienie pakietu.	Tak	Tak	Tak	Tak

I.p	Wymaganie	100GbE	25GbE	10GbE	1GbE
11	System zarządzania musi umożliwiać tworzenie własnej biblioteki pomocniczych skryptów, napisanych w języku Python lub Perl, które mogą być uruchamiane i parametryzowane z poziomu Systemu Zarządzania. Tworzenie, testowanie, uruchamianie i zarządzanie skryptami Python/Perl musi w całości odbywać się poprzez interfejs GUI systemu zarządzania i musi stanowić integralną część tego systemu.	Tak	Tak	Tak	Tak

5.2. Moduły optyczne do interfejsów sieciowych

5.2.1. Moduł 1GbE, 1000BASE-T, SFP

Parametr	Charakterystyka (wymagania minimalne)
Typ	Moduł 1000BASE-T SFP
Kompatybilność	Moduł musi być zgodny ze standardem SFP Multi Source Agreement (MSA) - Small Form Factor Pluggable (SFP) Transceiver Multi-Source Agreement (MSA), September 2000
Interfejs	<ol style="list-style-type: none"> 1) Moduł musi posiadać interfejs Gigabit Ethernet (1000BASE-T) zgodnie ze standardem IEEE Std 802.3 2) Wymaga się funkcji negocjacji szybkości łącza (10Mbit/s, 100Mbit/s, 1Gbit/s) i trybu pracy (full duplex, half duplex). 3) Moduł musi być wyposażony w złącze RJ-45
Zasięg	min. 100m
Przepustowość	Moduł musi umożliwiać pracę z prędkością 10/100/1000 Mb/s
Dodatkowe	<ol style="list-style-type: none"> 1) Moduł musi być kompatybilny z urządzeniami sieciowymi (przełączniki), interfejsami sieciowymi w serwerach i serwerach dyskowych (macierzach dyskowych) dostarczanych w ramach tego postępowania. 2) Wymaga się, by moduł mógł być instalowany w urządzeniu i wyjmowany z urządzenia podczas jego pracy (Hot-Pluggable).

5.2.2. Moduł 10GbE, BASE-T, SFP+

Parametr	Charakterystyka (wymagania minimalne)
Typ	Moduł BASE-T SFP+
Kompatybilność	Moduł musi być zgodny ze standardami: 1) SFF-8431 – “Specifications for Enhanced 8.5 and 10 Gigabit Small Form Factor Pluggable Module ‘SFP+ ’”, SFF Document Number SFF-8431, Revision 3.0.
Interfejs	1) Moduł musi posiadać interfejs 10GBASE-T zgodnie ze standardem IEEE 802.3an. 2) Moduł musi być wyposażony w złącze RJ-45
Zasięg	min. 30m
Przepustowość	Moduł musi umożliwiać pracę z prędkością 10 Gb/s
Dodatkowe	1) Moduł musi być kompatybilny z urządzeniami sieciowymi (przełączniki), interfejsami sieciowymi w serwerach i serwerach dyskowych (macierzach dyskowych) dostarczanych w ramach tego postępowania. 2) Wymaga się by moduł mógł być instalowany w urządzeniu i wyjmowany z urządzenia podczas jego pracy (Hot-Pluggable).

5.2.3. Moduł 10GbE, SR SFP+

Parametr	Charakterystyka (wymagania minimalne)
Typ	Moduł SR SFP+
Kompatybilność	Moduł musi być zgodny ze standardami: 1) SFF-8431 – “Specifications for Enhanced 8.5 and 10 Gigabit Small Form Factor Pluggable Module ‘SFP+ ’”, SFF Document Number SFF-8431, Revision 3.0.
Interfejs	Moduł musi posiadać interfejs 10GBASE-SR zgodnie ze standardem IEEE 802.3ae. Moduł musi być wyposażony w złącze LC Duplex
Zasięg	min. 100m
Przepustowość	Moduł musi umożliwiać pracę z prędkością 10 Gb/s
Dodatkowe	1) Moduł musi być kompatybilny z urządzeniami sieciowymi (przełączniki), interfejsami sieciowymi w serwerach i serwerach dyskowych (macierzach dyskowych) dostarczanych w ramach tego postępowania. 2) Wymaga się by moduł mógł być instalowany w urządzeniu i wyjmowany z urządzenia podczas jego pracy (Hot-Pluggable).

5.2.4. Moduł 25 GbE, SR SFP28

Parametr	Charakterystyka (wymagania minimalne)
Typ	Moduł SR SFP28

Kompatybilność	Moduł musi być zgodny ze standardem IEEE 802.3by dla interfejsu 25GBase-SR4
Interfejs	Moduł musi być wyposażony w interfejs LC Duplex
Zasięg	min. 100m
Przepustowość	Moduł musi umożliwiać pracę z prędkością 25 Gb/s oraz 10 Gb/s
Dodatkowe	1) Moduł musi być kompatybilny z urządzeniami sieciowymi (przełączniki), interfejsami sieciowymi w serwerach i serwerach dyskowych (macierzach dyskowych) dostarczanych w ramach tego postępowania. 2) Wymaga się by moduł mógł być instalowany w urządzeniu i wyjmowany z urządzenia podczas jego pracy (Hot-Pluggable).

5.2.5.Moduł 100GbE, LR4 QSFP28

Parametr	Charakterystyka (wymagania minimalne)
Typ	Moduł LR4 QSFP28
Kompatybilność	Moduł musi być zgodny ze standardem IEEE 802.3ba dla interfejsu 100GBase-LR4
Interfejs	Moduł musi być wyposażony w złącze LC Duplex
Zasięg	min. 10km
Przepustowość	Moduł musi umożliwiać pracę z prędkością 100 Gb/s
Dodatkowe	1) Moduł musi być kompatybilny z urządzeniami sieciowymi (przełączniki), interfejsami sieciowymi w serwerach i serwerach dyskowych (macierzach dyskowych) dostarczanych w ramach tego postępowania. 2) Wymaga się by moduł mógł być instalowany w urządzeniu i wyjmowany z urządzenia podczas jego pracy (Hot-Pluggable).

5.2.6.Moduł 100GbE, SR4 QSFP28

Parametr	Charakterystyka (wymagania minimalne)
Typ	Moduł SR4 QSFP28
Kompatybilność	Moduł musi być zgodny ze standardem IEEE 802.3bm dla interfejsu 100GBase-SR4
Interfejs	Moduł musi być wyposażony w złącze MTP/MPO-12
Zasięg	min. 100m
Przepustowość	Moduł musi umożliwiać pracę z prędkością 100 Gb/s
Dodatkowe	1) Moduł musi być kompatybilny z urządzeniami sieciowymi (przełączniki), interfejsami sieciowymi w serwerach i serwerach dyskowych (macierzach dyskowych) dostarczanych w ramach tego postępowania. 2) Wymaga się by moduł mógł być instalowany w urządzeniu i wyjmowany z urządzenia podczas jego pracy (Hot-Pluggable).

5.2.7. Moduł 40 GbE, LR QSFP+

Parametr	Charakterystyka (wymagania minimalne)
Typ	Moduł LR QSFP+
Kompatybilność	Moduł musi być zgodny ze standardem IEEE 802.3ba dla interfejsu 40GBase-LR4
Interfejs	Moduł musi być wyposażony w złącze LC Duplex
Zasięg	min. 10km
Przepustowość	Moduł musi umożliwiać pracę z prędkością 40 Gb/s
Dodatkowe	<ol style="list-style-type: none"> 1) Moduł musi być kompatybilny z urządzeniami sieciowymi (przełączniki), interfejsami sieciowymi w serwerach i serwerach dyskowych (macierzach dyskowych) dostarczanych w ramach tego postępowania. 2) Wymaga się by moduł mógł być instalowany w urządzeniu i wyjmowany z urządzenia podczas jego pracy (Hot-Pluggable).

5.2.8. Moduł, 40 GbE, SR QSFP+

Parametr	Charakterystyka (wymagania minimalne)
Typ	Moduł SR QSFP+
Kompatybilność	Moduł musi być zgodny ze standardem IEEE 802.3ba dla interfejsu 40GBase-SR4
Interfejs	Moduł musi być wyposażony w złącze MTP/MPO-12
Zasięg	min. 100m
Przepustowość	Moduł musi umożliwiać pracę z prędkością 40 Gb/s
Dodatkowe	<ol style="list-style-type: none"> 1) Moduł musi być kompatybilny z urządzeniami sieciowymi (przełączniki), interfejsami sieciowymi w serwerach i serwerach dyskowych (macierzach dyskowych) dostarczanych w ramach tego postępowania. 2) Wymaga się by moduł mógł być instalowany w urządzeniu i wyjmowany z urządzenia podczas jego pracy (Hot-Pluggable).

5.3. Okablowanie sieciowe

Zaoferowane okablowanie musi być kompatybilne i działać prawidłowo z zaoferowanymi kartami sieciowymi w serwerach, serwerach dyskowych oraz przełącznikami sieciowymi.

5.3.1. Patchcord UTP 3m

Typ i parametry	UTP kat. 6
Długość	3m
Złącza	RJ45

5.3.2. Patchcord UTP 5m

Typ i parametry	UTP kat. 6
Długość	5m
Złącza	RJ45

5.3.3.Patchcord UTP 10m

Typ i parametry	UTP kat. 6
Długość	10m
Złącza	RJ45

5.3.4.Patchcord LC-LC Multimode 3m

Typ i parametry p	LC UPC to LC UPC Duplex OM5 Multimode
Długość	3m
Tłumienność	tłumienność złącza nie większa niż 0,35 dB
Złącza	LC/UPC

5.3.5.Patchcord LC-LC Multimode 5m

Typ i parametry	LC UPC to LC UPC Duplex OM5 Multimode
Długość	5m
Tłumienność	tłumienność złącza nie większa niż 0,35 dB
Złącza	LC/UPC

5.3.6.Patchcord LC-LC Single Mode 3m

Typ i parametry	LC UPC to LC UPC Duplex OS2 Single Mode
Długość	3m
Tłumienność	tłumienność złącza nie większa niż 0,25 dB
Złącza	LC/UPC

5.3.7.Patchcord LC-LC Single Mode 5m

Typ i parametry	LC UPC to LC UPC Duplex OS2 Single Mode
Długość	5m
Tłumienność	tłumienność złącza nie większa niż 0,25 dB
Złącza	LC/UPC

5.3.8.Patchcord MPO-MPO Multimode 3m – przełącznik -przełącznik

Typ i parametry	MPO to MPO OM4 Multimode – 12 włókien
Długość	3m
Tłumienność	tłumienność złącza nie większa niż 0,35 dB
Złącza	MPO/MTP
Kompatybilność	Patchcord musi gwarantować poprawną łączność pomiędzy dwoma dostarczonymi przełącznikami sieciowymi dla portów 100Gb/s

5.3.9.Patchcord MPO-MPO Multimode 5m – przełącznik -przełącznik

Typ i parametry	MPO to MPO OM4 Multimode – 12 włókien
Długość	5m

Tłumienność	tłumienność złącza nie większa niż 0,35 dB
Złącza	MPO/MTP
Kompatybilność	Patchcord musi gwarantować poprawną łączność pomiędzy dwoma dostarczonymi przełącznikami sieciowymi dla portów 100Gb/s

5.3.10. Kabel DAC pasywny 100G 3m

Typ i parametry	DAC pasywny 100G QSFP28
Długość	3m
Złącza	QSFP28

5.3.11. Kabel DAC pasywny 100G 5m

Typ i parametry	DAC pasywny 100G QSFP28
Długość	5m
Złącza	QSFP28

5.3.12. Kabel DAC pasywny breakout 100G --> 4 x 25 G 3m

Typ i parametry	DAC pasywny 100G QSFP28 to 4 x 25G SFP28 Breakout
Długość	5m
Złącza	QSFP28 – 4 x SFP28

5.3.13. Kabel DAC pasywny breakout 100G --> 4 x 25 G 5m

Typ i parametry	DAC pasywny 100G QSFP28 to 4 x 25G SFP28 Breakout
Długość	5m
Złącza	QSFP28 – 4 x SFP28

5.3.14. Kabel DAC pasywny 25G 3m

Typ i parametry	DAC pasywny 25G SFP28
Długość	3m
Złącza	SFP28

5.3.15. Kabel DAC pasywny 25G 5m

Typ i parametry	DAC pasywny 25G SFP28
Długość	5m
Złącza	SFP28

6. Stacje zarządzania

6.1. Stacja Zarządzania Typ 1

Pojedyncza Stacja Zarządzania Typ 1 składa się z następujących części składowych:

6.1.1. Jednostka główna spełniająca poniższe wymagania:

- 1) Wyświetlacz: 14" cala, rozdzielczość min. 2560x1600, jasność min. 500 nit, z technologią niskiej emisji niebieskiego światła (ang. Low Blue Light);
- 2) Procesor: zgodny z x64, posiadający co najmniej 14 fizycznych rdzeni, co najmniej 20 wątków. Zaprojektowany do pracy w mobilnych stacjach roboczych (pobór mocy w podstawowym trybie pracy nie więcej niż 45W), co najmniej 24MB cache, osiągający wydajność minimum: 30000 punktów Passmark CPU Mark w teście wydajności Pass Mark Performance Test (stan na 04.08.2023) pracujący z minimalną częstotliwością w trybie turbo 5,4GHz;
- 3) Pamięć RAM: nie mniej niż 64 GB;
- 4) Dysk twardey: M.2 SSD NVMe: min. 2TB;
- 5) Dodatkowa karta graficzna z min. 4GB RAM;
- 6) Zintegrowane porty (co najmniej):
 - a) min. 4x gniazdo Thunderbolt 4 (USB Type-C) z obsługą PowerDelivery i DisplayPort,
 - b) zintegrowany czytnik kart micro,
 - c) złącze słuchawkowo-mikrofonowe – Jack 3,5 mm,
- 7) Komunikacja:
 - a) Wi-Fi min. 6E,
 - b) Bluetooth.
- 8) Bateria: nie mniej niż 70Wh, przy czym Zamawiający dopuszcza odchylenia od podanej wartości o +/- 5%;
- 9) Waga: nie więcej niż 1,55 kg;
- 10) Dodatkowe wymagania:
 - a) klawiatura: QWERTY, podświetlana,
 - b) Touchpad,
 - c) co najmniej dwa wbudowane głośniki oraz mikrofon,
 - d) wbudowana kamera HD o rozdzielczości min. 720p z funkcją IR,
 - e) zintegrowany czytnik linii papilarnych,
 - f) dedykowany przez producenta zasilacz z wtyczką USB Type-C z obsługą napięcia 100-240VAC wraz z przewodem umożliwiającym zasilanie z gniazdek używanych na terenie PL,
 - g) wbudowany układ zabezpieczający TPM (Trusted Platform Module),
 - h) zestaw funkcji wbudowanych w płytę główną komputera i innych podzespołów zapewniających kombinację technologii zawartych w procesorze, usprawnień sprzętowych, funkcji zarządzających i zabezpieczających. Zapewnia on zdalny dostęp do komputera wliczając monitoring, sterowanie nim, konserwację niezależnie od stanu systemu operacyjnego nawet wtedy, gdy komputer jest wyłączony, w szczególności w zakresie:

- i. inwentaryzacji zasobów systemowych,
 - ii. zdalnego włączenie/wyłączenie/restart komputera poprzez TCP/IP,
 - iii. zdalnego diagnozowania - zdalna konsola tekstowa do BIOSu i konsola graficznej (KVM),
 - iv. obsługi moduł TMP,
 - v. zdalna konfiguracja BIOS, zdalny update BIOS,
 - vi. zdalne monitorowanie stanu komponentów komputera – m.in. CPU, pamięć, dysk itp.,
 - vii. możliwość zdalnej blokady komputera w przypadku kradzieży sprzętowego. Jedynym warunkiem jest podłączenie komputera do sieci komputerowej oraz do zasilania.
- 11) System operacyjny: Licencja na system Windows 11 Professional PL 64-bit lub równoważny;
- 12) Wsparcie producenta dla następujących systemów operacyjnych:
- a) Microsoft Windows 11 Pro 64-bit,
 - b) Ubuntu Linux,
- 13) Bezpłatne oprogramowanie do automatycznej diagnostyki z funkcją przewidywania usterek dysków twardych oraz baterii laptopa, i informowania o nich zanim wystąpią awarie. Musi posiadać co najmniej poniższą funkcjonalność:
- a) monitorowanie komputera i generowanie zgłoszeń o błędach / nieprawidłowym działaniu w zakresie pracy komponentów i wydajności systemów,
 - b) powiadamiania o nowych wersjach sterowników i umożliwienie użytkownikowi wykonania upgrade systemu,
 - c) powiadamianie o problemach wydajnościowych i diagnozowanie / rozwiązywanie takich problemów.

6.1.2. Monitor

Kompatybilny ze stacją zarządzania Typu 1 monitor LCD 27" 4K ze złączem USB-C o następującej parametrach technicznych:

1. przekątna „27” – widoczna matryca min. 26." w formacie 16:9,
2. rozdzielczość 3840 x 2160 (WQHD),
3. matowa matryca IPS,
4. kontrast min. 2000:1,
5. jasność min. 400 cd/m²
6. czas reakcji monitora – 5 ms,
7. kąty widzenia: 178° w pionie i poziomie,
8. paleta kolorów – 100% Rec 709, 100% sRGB, 98% DCI-P3
9. złącza (gniazda) co najmniej: min. 1x HDMI , min. 1x DisplayPort min. 1.4, 1x wyjście DisplayPort (dla monitora z obsługą MST (Multi-Stream Transport), min. 1x USB Type-C do podłączenia z komputerem (z funkcją ładowania laptopa z mocą min. 90W oraz DisplayPort z obsługą min. 3840 x 2160), RJ45 (Ethernet), min 4x USB Type-A w USB w standardzie min. 3.2 Gen 2; min. 1x USB Type-C w USB w standardzie min. 3.2 Gen 2,

PN 70/09/2023 – dostawa elementów obliczeniowych

10. funkcje: funkcja obrotowego ekranu (PIVOT -90° /+90°), regulacja wysokości (min. 150mm), regulacja kąta pochylenia (w zakresie min. -5/+20)
11. dołączone przewody: 1 x kabel z wtyczkami DisplayPort-DisplayPort, 1 x kabel z wtyczkami USB Type-C – USB Type-C, 1 x kabel z wtyczkami USB Type-C – USB Type-A ,
12. zasilanie – napięcie 100-240VAC,
13. z monitorem musi zostać dostarczony przewód umożliwiającym zasilanie z gniazdek używanych na terenie PL,

6.1.3. Stacja dokująca

Stacja dokująca kompatybilny ze stacjami zarządzania Typu 1 podłączana poprzez Thunderbolt 4 Type-C za pomocą złącza USB Type-C. Musi być wyposażona co najmniej w następujące złącza (gniazda):

- 1) 1x USB Type-C w standardzie co najmniej USB 3.2 Gen 2,
- 2) 3x USB Type-A w standardzie co najmniej 3.2 Gen 1 w tym co najmniej 1 z funkcjonalnością PowerShare
- 3) 2x DisplayPort 1.4,
- 4) 1x HDMI min. 2.0,
- 5) 1x USB-C w standardzie co najmniej USB 3.2 Gen 2 z funkcją DisplayPort 1.4
- 6) 1 x LAN 10/100/1000 Ethernet (RJ-45)
- 7) 2 x Thunderbolt 4 w postaci złącza USB Type-C,
- 8) gniazdo do podłączenia zewnętrznego dedykowanego do stacji zasilacza zasilacza

Stacja dokująca musi być wyposażona w 1 wtyczkę Thunderbolt 4 w postaci złącza USB Type-C, do podłączenia komputera, na kablu o długości min. 0,8 m.

Stacja musi zapewnić poprawną pracę z 3 monitorami w rozdzielczość 4K.

Ze stacją musi zostać dostarczony zasilacz, zapewniający zasilanie podłączonego do stacji dokującej komputera o mocy min. 90W (130W w przypadku podłączenie komputera producenta stacji dokującej) z obsługą napięcia 100-240VAC wraz z przewodem umożliwiającym zasilanie z gniazdek używanych na terenie PL. Wymagane jest aby dostarczane poprzez stację zasilanie było wystarczające do poprawnej pracy stacji zarządzania Typu 1 bez potrzeby podłączania ich do dodatkowe zasilania.

Dodatkowa wymagana poprawna obsługa: PXE Boot, Wake-On-LAN, Wake-On-Dock. Stacja dokująca musi poprawnie współpracować z następującymi systemami operacyjnymi: Windows 11, Ubuntu Linux.

6.1.4. Zestaw klawiatura z myszą

- 1) Kompatybilny ze stacjami zarządzania Typu 1 zestaw klawiatury i myszy.
- 2) Musi posiadać następującą funkcjonalność:
 - a) Zasilanie za pomocą baterii lub akumulatorów – poprawność pracy na jednym komplecie baterii 36 miesięcy,
 - b) Możliwość jednoczesnego bezprzewodowe podłączenie do trzech różnych komputerów – jednego za pomocą odbiornika USB Type-A, pozostałych dwóch za pomocą Bluetooth. Przetwarzania pomiędzy poszczególnymi komputerami musi być realizowane przy użyciu klawisza lub przycisku na klawiaturze lub myszy. Aktualne

PN 70/09/2023 – dostawa elementów obliczeniowych

podłączone urządzenie musi być sygnalizowane za pomocą dedykowanej diody zarówno na klawiaturze jak i na myszy,

- c) Układ klawiatury QWERTY US międzynarodowy z oddzielnym blokiem numerycznym oraz klawiszami strzałek i klawiszami funkcyjnymi,
 - d) Mysz z optyczną technologią wykrywania ruchu obsługującą rozdzielczość min. 1000 dpi,
 - e) Mysz musi posiadać co najmniej 7 przycisków ,
 - f) Poprawna współpraca z systemami: Microsoft Windows 10, Android, Apple macOS,
- 3) Do zestawu muszą zostać dołączone baterie w liczbie i modelu umożliwiającym poprawną pracę zestawu.

6.1.5.Opis równoważności

Poniżej opisano kryteria, jakie Zamawiający będzie stosował w celu oceny równoważności rozwiązania zaproponowanego przez Wykonawcę jako równoważne dla systemu operacyjnego Windows 11 Professional PL 64-bit lub równoważny.

Przez równoważność Zamawiający rozumie konieczność:

- 1) zapewnienia przez system pełnej funkcjonalności jaką oferuje system Windows w minimalnej wskazanej przez Zamawiającego wersji,
- 2) dostępność dla systemu równoważnego tych aplikacji oraz oprogramowania, które są dostępne dla wskazanego przez Zamawiającego systemu Windows lub aplikacji i oprogramowań alternatywnych, zapewniających wszystkie te same funkcjonalności.

7. Dostawa systemu

7.1. Ramowy plan dostaw

Plan realizacji przedmiotu zamówienia:

Lp.	Element realizacji przedmiotu zamówienia	Dni kalendarzowe (terminy maksymalne)
1.	Złożenie zapotrzebowania przez Zamawiającego	4 dni robocze od podpisania umowy
2.	Dostawa urządzeń i oprogramowania	30 dni roboczych od złożenia zapotrzebowania
3.	Podpisanie przez Zamawiającego protokołu zdawczo-odbiorczego	Maksymalnie 1 dzień roboczy po pozytywnym zakończeniu dostaw urządzeń i oprogramowania. Możliwe jest podpisanie protokołu zdawczo-odbiorczego w dniu zakończenia dostaw.

7.2. Dostawa urządzeń i oprogramowania

Wykonawca zobowiązany jest dostarczyć wszelkie urządzenia będące przedmiotem realizacji do lokalizacji wskazanej w punkcie **7.2.2.**

7.2.1. Ogólne wytyczne dotyczące dostawy:

- 1) Termin każdej dostawy musi zostać uzgodniony z Zamawiającym.
- 2) Wykonawca zobowiązany jest do zgłoszenia terminu dostawy na co najmniej 5 dni przed planowanym terminem dostawy.
- 3) Wykonawca zobowiązany jest do wskazania osoby nadzorującej realizację przedmiotu zamówienia.
- 4) Wykonawca zobowiązany jest do dostarczenia urządzeń do lokalizacji podanych w punkcie **7.2.2.** Dostawę Wykonawca musi zrealizować własnym sprzętem oraz zobowiązany jest do pokrycia wszelkich kosztów związanych z transportem, montażem i ubezpieczeniem dostawy.
- 5) Wykonawca zobowiązany jest do przestrzegania przepisów porządkowych obowiązujących na terenie budynku Zamawiającego.

PN 70/09/2023 – dostawa elementów obliczeniowych

- 6) Zabronione jest palenie tytoniu oraz używanie innych substancji wonnych (np. papierosy elektroniczne) na terenie wszystkich obiektów Zamawiającego, w których realizowany jest przedmiot zamówienia (również na dachu budynków). Za każdorazowe złamanie tego zakazu zostanie naliczona kara w wysokości 1 000,00 zł, a pracownik łamiący ten zakaz zostanie wykluczony z dalszych prac. Ponadto jeżeli palenie tytoniu lub używanie substancji wonnych spowoduje reakcję systemu detekcji pożaru w budynku Zamawiającego, co może doprowadzić do wyzwolenie systemu gaszenia, to Wykonawca zobowiązany jest do pokrycia wszystkich wynikłych z tego zdarzenia kosztów.
 - 7) Zabronione jest spożywanie posiłków i napojów w salach komputerowych.
- 7.2.2. Miejsce dostawy.

Zamawiający wymaga, aby Wykonawca dostarczył komponenty w następującej lokalizacji:

PCSS – Poznańskie Centrum Superkomputerowo-Sieciowe, Budynek Sal Technologicznych (BST) ul. Jana Pawła II 10 Poznań

8. Gwarancja

8.1. Ogólne warunki Gwarancji

- 1) Wykonawca zobowiązuje się do udzielenia gwarancji na System oraz wykonanie usług gwarancyjnych zgodnie z poniższymi zapisami.
- 2) Okres gwarancji na System wynosi 7 (siedem) lat i rozpoczyna swój bieg od daty podpisania protokołu zdawczo-odbiorczego. Zamawiający dopuszcza, aby okres gwarancji na dostarczone stacje zarządzania był krótszy, jednak w takim przypadku musi być on zgodny z minimalnymi warunkami opisanym w punkcie **8.2.15**.
- 3) Zamawiający może dokonać rozbudowy posiadanej infrastruktury sprzętowej, aplikacyjnej oraz teleinformatycznej wchodzącej w skład Systemu, bez utraty uprawnień wynikających z gwarancji na dostarczony i wdrożony System, z zastrzeżeniem, że rozbudowa została dokonana zgodnie z zaleceniami/wytycznymi producenta/producentów rozbudowywanych elementów Systemu.
- 4) Gwarancja nie wyłącza uprawnień Zamawiającego z tytułu gwarancji udzielonych przez producentów urządzeń i/lub oprogramowania. Warunki gwarancji mają pierwszeństwo przed warunkami gwarancji udzielonymi przez producentów urządzeń i/lub oprogramowania w zakresie, w jakim warunki gwarancji przyznają Zamawiającemu silniejszą ochronę.
- 5) Gwarancja nie wyłącza uprawnień Zamawiającego z tytułu gwarancji udzielonych przez producentów urządzeń i/lub oprogramowania. Warunki gwarancji mają pierwszeństwo przed warunkami gwarancji udzielonymi przez producentów urządzeń i/lub oprogramowania w zakresie, w jakim warunki gwarancji przyznają Zamawiającemu silniejszą ochronę.
- 6) Stosowanie praw wynikających z udzielonej gwarancji nie wyłącza stosowania uprawnień Zamawiającego wynikających z rękojmi za wady urządzeń i/lub oprogramowania. Zamawiający jest uprawniony do realizacji uprawnień wynikających z rękojmi na warunkach analogicznych jak realizacja uprawnień Zamawiającego wynikających z gwarancji.
- 7) W ramach gwarancji Wykonawca zobowiązany jest do:
 - a) diagnostyki i rozwiązywania problemów zgłaszanych przez Zamawiającego,
 - b) dostarczania i wsparcia w instalacji oprogramowania, tj.:
 - i. poprawek (aktualizacji) oprogramowania,
 - ii. najnowszych komercyjnie dostępnych wersji oprogramowania wraz z obowiązkiem udzielenia niezbędnych licencji bez dodatkowych kosztów dla Zamawiającego,
 - c) udzielania konsultacji,
 - d) dostarczenia urządzeń oraz oprogramowania wolnego od wad materiałowych i wykonawczych w trakcie okresu świadczenia usług gwarancji,
 - e) w okresie gwarancji Wykonawca będzie udostępniał Zamawiającemu dostęp do narzędzi konfiguracyjnych i dokumentacji technicznej oprogramowania i urządzeń,
 - f) gwarancja na urządzenia i oprogramowanie będzie świadczona w miejscu używania urządzeń i oprogramowania z możliwością naprawy w serwisie Wykonawcy po uzyskaniu zgody Zamawiającego,

- g) wszelkie koszty rozwiązywania problemów, w tym koszt transportu, instalacji i uruchomienia urządzeń i oprogramowania ponosi Wykonawca,
- h) Wykonawca i Zamawiający będą współpracować przy rozwiązywaniu problemów,
- i) Wykonawca zapewni naprawę lub wymianę Urządzeń lub ich części, na części nowe i oryginalne, zgodnie z metodyką i zaleceniami producenta urządzeń. Zamawiający w uzasadnionych przypadkach ma prawo wnioskować do Wykonawcy o oficjalne potwierdzenie zgodności przeprowadzonych prac z metodyką i zaleceniami producenta, które musi być wystawione przez producenta urządzeń lub podmiot do tego uprawniony, a Wykonawca w ciągu 14 dni dostarczy takie potwierdzenie Zamawiającemu,
- j) dokonania wymiany asortymentu w okresie gwarancji na nowy w przypadku 3 (trzech) istotnych jego awarii; za istotną awarię uznaje się każde uszkodzenie ograniczające funkcjonowanie przedmiotu zamówienia; wymiana przedmiotu zamówienia powinna nastąpić w terminach nie dłuższych niż czas dostawy; w przypadku wymiany uszkodzonego asortymentu (albo jego podzespołu) na nowy obowiązywać będą warunki gwarancji i realizacji świadczeń gwarancyjnych wynikające ze złożonej oferty; okres gwarancji będzie biegł w takim przypadku od początku,
- k) dla dostarczonego sprzętu przez cały okres trwania gwarancji musi być zapewniona możliwość aktualizacji oprogramowania/firmware do najnowszej dostępnej wersji producenta. Koszty aktualizacji ponosi Wykonawca.
- l) dostarczony przedmiot zamówienia musi być fabrycznie nowy, nieeksponowany na wystawach, kompletny i sprawny technicznie. Przez stwierdzenie „fabrycznie nowy” należy rozumieć przedmiot zamówienia oryginalnie zapakowany, nieużywany przed dniem dostarczenia, z wyłączeniem używania niezbędnego dla przeprowadzenia testu jego poprawnej pracy po wyprodukowaniu,
- m) dostarczony przedmiot zamówienia musi pochodzić z oficjalnych kanałów dystrybucyjnych producenta obejmujących rynek Unii Europejskiej, zapewniających w szczególności realizację uprawnień gwarancyjnych,
- n) W przypadku, gdy Wykonawca podczas realizacji usług Gwarancji dostarczy nową fabrycznie część Urządzenia, wymieniając część wadliwą, lub dostarczy fabrycznie nowe Urządzenie, nowa część lub nowe urządzenie staje się własnością Zamawiającego,
- o) Zamawiający może dokonać rozbudowy Systemu bez utraty uprawnień wynikających z gwarancji na urządzenia i oprogramowanie,
- p) Wykonawca zapewni zdalne wsparcie (poprzez platformę do współpracy, telefon lub e-mail) w zakresie rozwiązywania problemów z konfiguracją i użytkowaniem oprogramowania.

8.2. Opis usługi Gwarancji

8.2.1. Diagnostyka i rozwiązywanie problemów

W zakresie gwarancji Wykonawca zapewnia Zamawiającemu usługę diagnostyki i rozwiązywania problemów w ramach Systemu.

8.2.2. Klasyfikacja problemów

Klasyfikację problemów określa Zamawiający. W przypadku, gdy strony zgodzą się, że System pomimo zgłoszenia funkcjonuje prawidłowo, zgłoszenie to nie jest uznawane za awarię.

Awaria Krytyczna – wystąpienie problemu o znaczeniu krytycznym dla Zamawiającego, powodujące poważne i szkodliwe zakłócenie działania Systemu. Możliwe są problemy z bezpieczeństwem, naruszenia zgodności, straty i szkody dla reputacji. Spełniona zostaje jedna z wymienionych niżej przesłanek:

- 1) nie jest możliwe korzystanie przez Zamawiającego z Systemu lub korzystanie z niego jest znacząco utrudnione (degradacja),
- 2) nie działają funkcje Systemu lub występuje ich znacząca degradacja,
- 3) wydajność lub pojemność Systemu uległa obniżeniu, o co najmniej 40% w stosunku do wartości dostarczonej,
- 4) nie jest możliwe stwierdzenie stanu Systemu lub jego elementów.

Awaria Poważna – wystąpienie Problemu, w którym występuje zakłócenie usługi i/lub operacji. Konsekwencje obejmują naruszenia zgodności, szkody dla reputacji i możliwe obawy dotyczące bezpieczeństwa. Możliwe są straty. Spełniona zostaje jedna z wymienionych niżej przesłanek:

- 1) brak możliwości zarządzania elementami Systemu,
- 2) brak możliwości realizacji usług.

Awaria Istotna – wystąpienie Problemu, w wyniku którego powstają utrudnienia w dostępie do komponentu/ów. Obejmuje przerwy w obsłudze użytkownika, głównie o ograniczonym zakresie, czasie trwania lub skutku. Spełniona zostaje jedna z wymienionych niżej przesłanek:

- 1) uszkodzenie komponentu lub jego elementów powodujące ograniczenie możliwości działania Systemu ale nieuniemożliwiające korzystania z Systemu,
- 2) stan Systemu, w którym część Systemu nie funkcjonuje zgodnie z dokumentacją aktualnie eksploatowanej wersji Systemu, co utrudnia pracę co najmniej jednej z jego funkcji.

Usterka – pozostałe Problemy.

8.2.3. Poziomy świadczenia usługi

W zależności od klasyfikacji Problemu, Wykonawca gwarantuje następujący czas realizacji Zgłoszeń Zamawiającego:

Klasa Problemu	Maksymalny czas reakcji na zgłoszenie	Maksymalny czas Rozwiązania Problemu ¹	Maksymalny czas dostarczenia rozwiązania docelowego ²	Tryb Serwisowania (godzin na dobę)

		(przywrócenia normalnego działania)		x liczbę dni w tygodniu)
Awaria Krytyczna	1 godzina	4 godziny	10 dni roboczych	24x7
Awaria Poważna	2 godziny	8 godzin	20 dni roboczych	24x7
Awaria Istotna	8 godzin	16 godzin	80 dni roboczych	8x5 ³
Usterka	24 godziny	40 godzin	100 dni roboczych	8x5 ³

¹ – również zastosowanie obejścia, tj. rozwiązania pozwalającego na prawidłowe korzystanie z Systemu bez usuwania wykrytego błędu

² – w przypadku zastosowania obejścia

³ – należy to rozumieć jako tylko w dni robocze

8.2.4. Wymiana informacji pomiędzy Zamawiającym a Wykonawcą

- 1) Strony dopuszczają następujące kanały komunikacyjne:
 - a) system zgłoszeń problemowych Wykonawcy,
 - b) poczta elektroniczna,
 - c) strona WWW,
 - d) systemy VC,
 - e) telefon.
- 2) Zgłoszenia kierowane przez Zamawiającego za pośrednictwem telefonu, będą również potwierdzane niezwłocznie, poprzez wysłanie e-mail do Wykonawcy, z podaniem czasu zgłoszenia za pośrednictwem telefonu. W takiej sytuacji za czas Zgłoszenia Problemu, uważa się moment zgłoszenia za pośrednictwem telefonu.
- 3) Wykonawca zobowiązany jest przyjmować i rejestrować Zgłoszenia Problemów składane przez Zamawiającego w trybie 24/7/365.
- 4) Wykonawca będzie aktualizował wszelkie dane o Problemie takie jak postępy prac, statusy, priorytet, typ w systemie zgłoszeń problemowych, a cała historia korespondencji oraz statusów będzie dostępna dla Zamawiającego.
- 5) Wszelka korespondencja między stronami będzie odbywała się w języku polskim.
- 6) Szczegóły przekazania dostępu do systemu zgłoszeń problemowych Wykonawcy zostaną przekazane Zamawiającemu w trybie roboczym.
- 7) Strony, w trakcie trwania usługi gwarancji, mogą umówić się na integrację między systemami zgłoszeń problemowych Wykonawcy i Zamawiającego. Szczegóły zostaną uzgodnione w trybie roboczym.

8.2.5. Zgłaszanie problemów

PN 70/09/2023 – dostawa elementów obliczeniowych

- 1) Zamawiający jest odpowiedzialny za przekazanie w zgłoszeniu problemu kompletu informacji, w szczególności:
 - a) osobę lub osoby kontaktowe reprezentujące Zamawiającego,
 - b) identyfikację i lokalizację urządzenia,
 - c) opis problemu,
 - d) klasyfikację problemu.
- 2) Za czas zgłoszenia problemu uznaje się moment skutecznego poinformowania Wykonawcy przez Zamawiającego o zaistniałym problemie.
- 3) Za klasyfikację problemu odpowiedzialny jest Zamawiający.
- 4) Wykonawca w trybie roboczym będzie przedstawiał swoje uwagi, gdy problemy będą zgłaszane w sposób nieprawidłowy po rozwiązaniu problemu.

8.2.6. Czas reakcji

- 1) Oznacza czas, który upłynie od wystąpienia zgłoszenia awarii do podjęcia czynności naprawczych ze strony Wykonawcy.
- 2) Wykonawca informuje Zamawiającego o przyjęciu zgłoszenia problemu za pośrednictwem poczty elektronicznej lub umieszczeniu odpowiedniej informacji w systemie zgłoszeń problemowych udostępnionym Zamawiającemu.

8.2.7. Rozwiązanie problemu

- 1) W ramach rozwiązywania problemu Wykonawca prowadzi diagnostykę, mającą na celu znalezienie przyczyn wystąpienia problemu. Diagnostyka będzie prowadzona w miejscu instalacji lub zdalnie po wyrażeniu zgody przez Zamawiającego i udostępnieniu Wykonawcy dostępu do Systemu.
- 2) Wykonawca informuje Zamawiającego o stanie prac mających na celu rozwiązanie problemu.
- 3) W przypadku uszkodzenia urządzeń, urządzenia lub części urządzenia, Wykonawca zapewnia dostawę i wymianę uszkodzonych urządzeń, urządzenia lub części urządzenia zgodnie z warunkami opisanymi w niniejszym załączniku. W przypadku, gdy wymienione urządzenia, urządzenie lub część urządzenia wymagają konfiguracji, będzie ona wykonana przez Wykonawcę.
- 4) Zamawiający po uzgodnieniu z Wykonawcą, ma prawo wymienić uszkodzoną część we własnym zakresie, którą następnie przekaże Wykonawcy w celu naprawy lub wymiany.
- 5) W przypadku wystąpienia problemu z oprogramowaniem, Wykonawca będzie współpracował z producentem oprogramowania w celu rozwiązania problemu.
- 6) Rozwiązanie problemu zostaje uznane za skuteczne w przypadku, gdy Wykonawca zgłosi Zamawiającemu fakt rozwiązania problemu, a Zamawiający ten fakt potwierdzi. Zamawiający zostanie poinformowany o fakcie rozwiązania problemu.
- 7) Jeżeli Wykonawca pięciokrotnie przekroczy terminy usunięcia problemów, wskazane w punkcie 8.2.3, z przyczyn leżących po jego stronie, Zamawiający będzie miał prawo do usunięcia problemu samodzielnie lub zlecając to innemu podmiotowi. Koszt usunięcia problemu ponosi Wykonawca.

8.2.8. Czas rozwiązania problemu

- 1) Czas rozwiązania problemu liczony jest oddzielnie dla każdego zgłoszenia problemu.
- 2) Czas rozwiązania problemu liczony jest od momentu zgłoszenia problemu do momentu poinformowania Zamawiającego przez Wykonawcę o rozwiązaniu problemu.
- 3) Czas potwierdzenia przez Zamawiającego do Wykonawcy rozwiązania problemu nie liczy się do czasu rozwiązania problemu – na ten czas Wykonawca zawiesza zgłoszenie problemu.
- 4) W przypadku skierowania przez Zamawiającego do Wykonawcy informacji o braku rozwiązania problemu, tj. dalszego występowania problemu, Wykonawca odwołuje zgłoszenie problemu i czas rozwiązania problemu jest kontynuowany o czas oczekiwania na dostęp do urządzeń.

8.2.9. Przywrócenie systemu

- 1) W ramach rozwiązywania Problemu, Wykonawca może zaproponować Zamawiającemu Przywrócenie Systemu poprzez wykorzystanie Obejścia.
- 2) Wykonawca informuje Zamawiającego o stanie prac mających na celu Przywrócenie Systemu.
- 3) Przywrócenie Systemu z wykorzystaniem Obejścia nie zwalnia Wykonawcy z obowiązku Rozwiązania Problemu, zgodnie z czasami określonymi w niniejszym Załączniku.
- 4) W przypadku wystąpienia Problemu z Oprogramowaniem, Wykonawca będzie współpracował z producentem Oprogramowania w celu Rozwiązania Problemu.
- 5) Przywrócenie Systemu zostaje uznane za skuteczne w przypadku, gdy Wykonawca zgłosi Zamawiającemu fakt Przywrócenia Systemu, a Zamawiający ten fakt potwierdzi.

8.2.10. Czas przywrócenia systemu

- 1) Czas przywrócenia systemu mierzony jest oddzielnie dla każdego zgłoszenia problemu.
- 2) Czas przywrócenia systemu liczony jest od momentu zgłoszenia problemu do momentu poinformowania Zamawiającego przez Wykonawcę o przywróceniu systemu.
- 3) Czas potwierdzenia przez Zamawiającego do Wykonawcy przywrócenia systemu nie liczy się do czasu przywrócenia systemu – na ten czas Wykonawca zawiesza zgłoszenie problemu.
- 4) W przypadku skierowania przez Zamawiającego do Wykonawcy informacji o braku przywrócenia Systemu, tj. dalszego występowania problemu, Wykonawca odwołuje zgłoszenie problemu i czas przywrócenia Systemu jest kontynuowany.
- 5) W przypadku, gdy w celu przywrócenia systemu występuje konieczność wymiany lub naprawy urządzeń, na czas wymiany lub naprawy urządzeń, Zamawiający ma obowiązek zapewnić dostęp do Urządzeń upoważnionym pracownikom Wykonawcy. W przypadku braku takiego dostępu, czas przywrócenia systemu odpowiednio wydłuża się o czas oczekiwania na dostęp do urządzeń.
- 6) Zgłoszenie problemu po przywróceniu Systemu zostaje ustawione w odpowiedni stan ze stosowną adnotacją, do momentu ostatecznego rozwiązania problemu, zgodnie z czasami określonymi w punkcie **8.2.3**.

8.2.11. Rozwiązanie zgłoszenia problemu

- 1) Zgłoszenie problemu zostaje uznane za rozwiązane w przypadku, gdy Wykonawca zgłosi Zamawiającemu fakt rozwiązania problemu, a Zamawiający ten fakt potwierdzi.
- 2) Zamawiający zostanie poinformowany o fakcie rozwiązania problemu za pomocą jednego ze środków komunikacji opisanych w punkcie 8.2.4, przy czym Wykonawca jednocześnie dokona stosownej adnotacji w systemie zgłoszeń problemowych.
- 3) Po potwierdzeniu przez Zamawiającego rozwiązania problemu, Wykonawca zamyka zgłoszenie problemu w systemie zgłoszeń problemowych.
- 4) W przypadku analogicznego zgłoszenia problemu, zostanie ono zarejestrowane przez Wykonawcę pod innym numerem zgłoszenia.

8.2.12. Konsultacje

W zakresie gwarancji Wykonawca zapewnia Zamawiającemu usługę konsultacji.

1) Przedmiot konsultacji:

- a) w zakresie usługi konsultacji, Wykonawca zapewnia Zamawiającemu dostęp do pomocy technicznej Wykonawcy, jako wsparcie w rozwiązywaniu problemów związanych z bieżącą eksploatacją Systemu, w szczególności w zakresie
 - i) obsługi, administracji i konfiguracji urządzeń
 - ii) obsługi, administracji i konfiguracji oprogramowania
 - iii) wsparcia w rozwiązywaniu problemów u Zamawiającego, które nie są Problemami
- b) pracownicy pomocy technicznej po stronie Wykonawcy powinni posiadać odpowiednią wiedzę techniczną niezbędną do świadczenia usług konsultacji.

2) Przebieg konsultacji:

- a) Zamawiający kontaktuje się z Wykonawcą drogą mailową lub telefoniczną z opisem sytuacji wymagającej konsultacji,
- b) Wykonawca przekazuje Zamawiającemu potwierdzenie przyjęcia zgłoszenia i rozpoczęcia prac w zakresie danej Konsultacji, zgodnie z czasem podjęcia konsultacji,
- c) strony komunikują się wzajemnie w ramach godzin świadczenia konsultacji,
- d) strony dopuszczają zmianę kanału komunikacji na ustalony wspólnie w trybie roboczym,
- e) Wykonawca rejestruje usługi konsultacji w celach raportowych.

3) Poziom świadczenia usługi

Wykonawca gwarantuje następujący poziom świadczenia usługi:

Godziny świadczenia konsultacji:	Dni robocze w godzinach 8:00 – 17:00
Czas podjęcia Konsultacji:	jeden dzień roboczy

8.2.13. Dostarczanie i wsparcie w instalacji Oprogramowania

W zakresie gwarancji Wykonawca zapewnia Zamawiającemu usługę dostarczania i wsparcia w instalacji oprogramowania dla uaktualnień oraz nowych wersji.

- 1) Dostarczanie oprogramowania:
 - a) w okresie gwarancji Wykonawca będzie udostępniał Zamawiającemu aktualizacje całego dostarczonego oprogramowania, oprogramowania urządzeń do najnowszych wersji oferowanych przez producenta oprogramowania (włączając tzw. firmware). Uaktualnienia są realizowane bez ograniczeń ilościowych,
 - b) aktualizacje będą dostarczane Zamawiającemu wraz ze szczegółową procedurą instalacji po przetestowaniu aktualizacji przez Wykonawcę i potwierdzeniu pozytywnego wyniku testów po stronie Wykonawcy,
 - c) procedura instalacji będzie zawierała również szczegółowe informacje w zakresie wycofania zmian,
 - d) w okresie gwarancji, Wykonawca zapewnia Zamawiającemu dostęp do usług wsparcia technicznego producenta urządzeń i oprogramowania właściwych dla danego produktu.
- 2) Wsparcie w instalacji aktualizacji/poprawek do oprogramowania:
 - a) Wykonawca będzie świadczył Zamawiającemu wsparcie w ramach instalacji aktualizacji/poprawek do dostarczonego oprogramowania,
 - b) Wykonawca może rekomendować, aby instalacja danego oprogramowania była zrealizowana przez Wykonawcę. W takim przypadku Wykonawca zgłasza taką rekomendację do Zamawiającego, podając uzasadnienie. Zamawiający po konsultacjach z Wykonawcą podejmuje decyzję, czy dane oprogramowanie zostanie zainstalowane przez Wykonawcę przy asyście Zamawiającego.
- 3) Poziom świadczenia usług
Wykonawca gwarantuje następujący poziom świadczenia usługi:
Dni robocze w godzinach 8:00 – 17:00

8.2.14. Szczegółowe wymagania gwarancji dotyczące elementów Systemu, z wyłączeniem stacji zarządzania

W ramach usługi gwarancji, Wykonawca zobowiązany jest do:

- 1) dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wsparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego,
- 2) dołączenia do oferty oświadczenia producenta potwierdzające, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z autoryzowanym partnerem serwisowym producenta,
- 3) zapewnienia prawa do pobieranie uaktualnień oprogramowania układowego oraz sterowników, także po wygaśnięciu gwarancji na urządzenie,

PN 70/09/2023 – dostawa elementów obliczeniowych

- 4) zapewnienia możliwości sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji poprzez dedykowaną stronę producenta po podaniu numeru seryjnego urządzenia,
- 5) zapewnienia możliwości telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji poprzez ogólnopolską linię telefoniczną producenta po podaniu numeru seryjnego urządzenia,
- 6) zagwarantowana możliwości zgłaszania awarii w trybie 365x7x24 poprzez ogólnopolską linię telefoniczną producenta,
- 7) zagwarantowana możliwości wymiany uszkodzonych dysków samodzielnie przez Zamawiającego bez utraty gwarancji,
- 8) dostarczenia wszystkich licencji wraz ze wsparciem, świadczonym przez Producenta będącego licencjodawcą oprogramowania na pierwszym, drugim i trzecim poziomie, które musi umożliwiać zgłaszanie problemów 7 dni w tygodniu przez 24h na dobę. Zamawiający wymaga, aby w przypadku wystąpienia problemów, wysyłanie zgłoszeń serwisowych do Producenta było zapewnione z poziomu portalu użytkownika, służącego do kompleksowego zarządzania kluczami licencyjnymi oprogramowania do wirtualizacji.
- 9) Wszystkie oferowane licencje powinny być bezterminowe i dostarczone na wszystkie węzły klastra wraz z 7-letnim wsparciem.
- 10) Producent rozwiązania musi udostępniać aktualizacje, do wszystkich opisanych Komponentów i muszą być one dostępne bezpłatnie podczas całego okresu wsparcia.

8.2.15. Szczegółowe wymagania gwarancji dotyczące Stacji Zarządzania

Wykonawca zobowiązuje się do udzielenia gwarancji zgodnie z poniższymi wymaganiami oraz w poniższych terminach

Przedmiot Zamówienia	Czas reakcji na zgłoszenie awarii (dni)	Czas naprawy/wymiany (dni)	Okres gwarancji (miesiące)
1	2	3	4
Stacja zarządzania Typ 1: – jednostka główna – monitor – zestaw klawiatura mysz – stacja dokująca	1 dzień roboczy od zgłoszenia	Następny dzień roboczy od zgłoszenia jednostka główna, 2 dni robocze od zgłoszenia pozostałe elementy	60 miesięcy

Przez czas „naprawy/wymiany” rozumie się czas liczony od momentu zakończenia czasu reakcji na zgłoszenie do dokonania skutecznej naprawy albo wymiany wadliwego towaru na wolny od wad i dostarczenia sprzętu zastępczego.

Szczegółowe Wymaganie dotyczące stacji zarządzania Typu 1:

PN 70/09/2023 – dostawa elementów obliczeniowych

- 1) Gwarancja musi zapewniać ochronę komputera mobilnego przed uszkodzeniem fizycznym spowodowanymi typowymi zdarzeniami mogącymi powstać z winy użytkownika końcowego, takimi jak: upuszczenie, zalanie, skok napięcia (przebiecie) lub usterka zintegrowanego ekranu. W takim wypadku udzielający gwarancji zobowiązuje się do pokrycia pełnych kosztów naprawy, a w przypadku niemożności lub nieoptymalności naprawy – do dostarczenia nowej stacji. Wymagane jest, aby gwarancja obejmowała taką możliwość co najmniej trzy razy w okresie gwarancyjnym.
- 2) Gwarancja musi zapewniać w przypadku uszkodzenia dysku twardego oraz wymiany na nowy prawo do pozostawienia uszkodzonego dysku twardego u Zamawiającego w celu jego utylizacji przez Zamawiającego.
- 3) Gwarancja na baterię musi wynosić co najmniej 36 miesięcy.
- 4) Zamawiający wymaga zapewnienia możliwości sprawdzenia konfiguracji sprzętowej na dedykowanej do tego celu stronie producenta po podaniu numeru seryjnego urządzenia.
- 5) prawo do pobieranie uaktualnień oprogramowania układowego oraz sterowników także po wygaśnięciu gwarancji na urządzenie,
- 6) Zamawiający wymaga aby warunki gwarancji były widoczne w systemie producenta na dedykowanej do tego celu stronie producenta po podaniu numeru seryjnego urządzenia zarówno w przypadku jednostki głównej jak również monitora oraz stacji dokującej,
- 7) w przypadku dłuższego czasu naprawy lub czasu wymiany aniżeli wskazany w kolumnie 3 w tabeli powyżej Wykonawca musi zapewnić Zamawiającemu w pełni sprawny asortyment o nie gorszych parametrach i funkcjonalności; dopuszcza się za zgodą Zamawiającego dostarczenie asortymentu zastępczego (oraz jego zwrotne odesłanie przez Zamawiającego) za pośrednictwem firmy kurierskiej na koszt i ryzyko Wykonawcy, a jego uruchomienie przez Wykonawcę nie jest wymagane; dostarczenie i uruchomienie takiego sprzętu zastępczego powoduje, że nie jest naliczana kara umowna za przekroczenie czasu naprawy/wymiany, pod warunkiem, że przekroczenie czasu naprawy/wymiany będzie nie dłuższe niż 30 dni; po przekroczeniu tego terminu kara będzie naliczana.