Spis treści

1. Definicje używane w dokumencie: 5
2. Serwery obliczeniowe 6
   - 2.1. Serwer – parametry wspólne dla każdego typu serwera 6
   - 2.2. Wymagania wspólne dla serwerów typu A, B, C, D, E 12
   - 2.3. Serwer obliczeniowy typu „A” 12
   - 2.4. Serwer obliczeniowy typu „B” 13
   - 2.5. Serwer obliczeniowy typu „C” 14
   - 2.6. Serwer obliczeniowy typu „D” 14
   - 2.7. Serwer obliczeniowy typu „E” 15
   - 2.8. Interfejsy Fibre Channel do serwera typu „A” 16
3. Macierz blokowa typu „A” 18
4. Macierz blokowa typu „B” 23
5. System szybkiej pamięci masowej o dostępie plikowym typu „A” 27
6. System szybkiej pamięci masowej o dostępie plikowym typu „B” 34
7. System archiwalnej pamięci masowej o dostępie plikowym typu „A” 40
8. System archiwalnej pamięci masowej o dostępie plikowym typu „B” 47
9. System pamięci masowej o dostępie obiektowym 53
10. Urządzenie do przechowywania kopii zapasowych 58
    - 10.1. Opis równoważności 64
11. Oprogramowanie do wykonywania kopii zapasowych 65
12. Oprogramowanie do wirtualizacji 74
    - 12.1. Wymagania wspólne dla wszystkich modułów oprogramowania do wirtualizacji 74
    - 12.2. Oprogramowanie do wirtualizacji zasobów serwerowych i ich mocy obliczeniowej w wersji podstawowej 74
    - 12.3. Oprogramowanie do wirtualizacji zasobów serwerowych i ich mocy obliczeniowej w wersji rozszerzonej 77
    - 12.4. Oprogramowanie do zarządzania klastrem wirtualizacyjnym 78
    - 12.5. Oprogramowanie do wirtualizacji sieci w wersji podstawowej 79
    - 12.6. Oprogramowanie do wirtualizacji sieci w wersji rozszerzonej 80
    - 12.7. Oprogramowanie do wirtualizacji przestrzeni dyskowej w wersji podstawowej 81
    - 12.8. Oprogramowanie do wirtualizacji przestrzeni dyskowej w wersji rozszerzonej 84
    - 12.9. Oprogramowanie do automatyzacji zadań w ramach środowiska zwirtualizowanego 85
    - 12.10. Oprogramowanie do monitorowania i zarządzania platformą wirtualizacyjną 87
    - 12.11. Oprogramowanie do centralnego zbierania logów 90
    - 12.12. Oprogramowanie do wirtualizacji mocy obliczeniowej akceleratorów graficznych 91

12.13. Oprogramowanie dostarczające zintegrowaną platformę Kubernetes 92
12.14. Oprogramowanie do wirtualizacji stacji roboczych 94
13. Przełączniki sieciowe 97
14. Przełączniki Fibre Channel 104
15. System zdalnego dostępu 107
15.1. Terminal zdalnego dostępu 107
15.2. Urządzenie dostępowe typ D1 107
15.3. Urządzenie dostępowe typ D2 110
15.4. System dostępowy typ D3 113
15.4.1. Urządzenie dostępowe typ D3 113
15.4.2. Systemem zarządzający typ D3 117
15.5. Mobilne urządzenie monitorujące 120
15.6. Opis równoważności 122
16. Stacje zarządzania 124
16.1. Stacja Zarządzania Typ 1 124
16.1.1. Jednostka główna spełniająca poniższe wymagania: 124
16.1.2. Monitor 125
16.1.3. Stacja dokująca 125
16.1.4. Zestaw klawiatura z myszą 125
16.2. Stacja Zarządzania Typ 2 125
16.2.1. Jednostka główna spełniająca poniższe wymagania: 125
16.2.2. Monitor 126
16.2.3. Stacja dokująca 127
16.2.4. Zestaw klawiatura z myszą 127
16.3. Monitor 127
16.4. Stacja dokująca 127
16.5. Zestaw klawiatura z myszą Typ A 128
16.6. Zestaw klawiatura z myszą Typ B 128
16.7. Opis równoważności 129
17. Przełączniki warstwy trzeciej 131
18. Wdrożenie systemu 148
18.1. Ramowy plan wdrożenia 148
18.1.1. Ogólne wytyczne dotyczące dostawy i instalacji 153
18.1.2. Warunki instalacji zapewnione przez Zamawiającego dla Zadania nr 1 154
18.1.3. Szczegółowe wymagania dotyczące dostawy i instalacji, które musi spełnić Wykonawca dla Zadania nr 1 154

18.1.4. Warunki instalacji zapewnione przez Zamawiającego dla Zadania nr 2 161
18.1.5. Szczegółowe wymagania dotyczące dostawy i instalacji, które musi spełnić Wykonawca dla Zadania nr 2 161
18.2. Dokumentacja 167
18.3. Dokumentacja Techniczna 167
18.4. Dokumentacja Powykonawcza 168
18.5. Wytyczne do testów 170
18.5.1. Testy weryfikacyjne 170
18.5.2. Testy akceptacyjne (podstawowe i niezawodnościowe) 171
18.5.3. Testy wydajnościowe 172
18.5.4. Testy odbiorcze 173
18.6. Odbiory 174
19. Instruktaż dla Zadania nr 1 175
19.1. Wstęp 175
19.2. Zbiór wymagań dla instruktaży 175
19.3. Czas trwania 186
20. Instruktaż dla Zadania nr 2 187
20.1. Wstęp 187
20.2. Zbiór wymagań dla instruktaży 187
20.3. Czas trwania 196
21. Gwarancja 197
21.1. Ogólne warunki Gwarancji 197
21.2. Opis usługi Gwarancji 198
21.2.1. Diagnostyka i rozwiązywanie problemów 198
21.2.2. Klasyfikacja problemów 198
21.2.3. Poziomy świadczenia usługi 199
21.2.4. Wymiana informacji pomiędzy Zamawiającym a Wykonawcą 200
21.2.5. Zgłaszanie problemów 201
21.2.6. Czas reakcji 201
21.2.7. Rozwiązanie problemu 201
21.2.8. Czas rozwiązania problemu 201
21.2.9. Przywrócenie systemu 202
21.2.10. Czas przywrócenia systemu 202
21.2.11. Rozwiązanie zgłoszenia problemu 203
21.2.12. Konsultacje 203
21.2.13. Dostarczanie i wsparcie w instalacji Oprogramowania 204

21.2.14. Szczegółowe wymagania gwarancji dotyczące elementów Systemu, z wyłączeniem stacji zarządzania, mobilnego urządzenia monitorującego oraz systemu dostępowego typu D.204

21.2.15. Szczegółowe wymagania gwarancji dotyczące stacji zarządzania oraz mobilnego urządzenia monitorującego oraz systemu dostępowego typu D. 205

22. Szczegółowy wykaz zamówienia 208

22.1. Zadanie nr 1 – PCSS 208

22.2. Zadanie nr 2 – NENCKI 210

1. Definicje używane w dokumencie:

Na potrzeby niniejszego dokumentu przyjęto następujące definicje:

1) **RU** – jednostka wysokości obudowy danego urządzenia i wysokości szafy teleinformatycznej (ang. rack unit), równa 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** – czas, który upłynie od momentu zgłoszenia awarii 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 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 składający się na System, np. serwer, macierz obiektowa, system wizualizacji.
6) **Licencja** – jeżeli Zamawiający wymaga dostarczenia licencji na korzystanie z oprogramowania, to w braku innych wyraźnych zastrzeżeń, uważa się, że wymagana licencja musi być dostarczona w ramach ceny ofertowej i nie może być ograniczona czasowo i terytorialnie (dotyczy terytorium UE).
7) **System** – oznacza całościowe rozwiązanie obejmujące m.in. urządzenia, oprogramowanie i aplikacje spełniające wymagania opisane w SWZ, które ma być dostarczone i wdrożone przez Wykonawcę w celu realizacji przedmiotu niniejszego Zamówienia objętego danym Zadaniem.
8) **Zadanie** – pojedyncze zapotrzebowanie złożone przez Zamawiającego albo inny podmiot odbierający, realizowane niezależnie od innych zapotrzebowań.

2. Serwery obliczeniowe

2.1. Serwer – parametry wspólne dla każdego typu serwera

Parametr	Charakterystyka (wymagania minimalne)
Obudowa	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. 4) Obudowa musi umożliwiać instalację co najmniej 8 dysków w rozmiarze 2,5”.
Płyta główna	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	1) Minimum 1 port USB Type-A w standardzie USB 2.0 lub wyższy na przednim panelu serwera. 2) Minimum 1 port USB Type-A w standardzie USB 3.0 lub wyższy na tylnym panelu. 3) Minimum 1 port VGA.
Wentylatory	1) Redundantne typu Hot-Plug.
Bezpieczeństwo	1) Panel przedni zamykany na klucz służący do ochrony przed nieautoryzowanym dostępem do dysków twardych. 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: 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. 9) Serwer musi być wyposażony w rozwiązanie zapewniające ochronę oprogramowania układowego (ang. firmware) przed manipulacją ze strony złośliwego oprogramowania. a) Ochrona taka musi być zgodna z zaleceniami NIST SP 800-147B. b) Zamawiający wymaga, aby dostarczony serwer posiadał zaimplementowane sprzętowo mechanizmy kryptograficzne poświadczające integralność oprogramowania BIOS (Root of Trust). 10) Serwer musi umożliwiać utworzenie bezpiecznego profilu w oparciu o konfigurację sprzętową oraz o konfigurację wewnętrznego oprogramowania komponentów serwera. Jakiekolwiek odchylenie od profilu musi zostać automatycznie zgłoszone administratorowi. 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.
Karta Zarządzania	Serwer musi być wyposażony w dedykowaną 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: 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, RedFish 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 posiadanym przez Zamawiajacego LDAP lub Microsoft Active Directory 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 bezpośrednie poprzez złącze USB 16) monitorowanie zużycia dysków SSD

	17) automatyczne zgłaszanie alertów do centrum serwisowego producenta 18) aktualizacje oprogramowania układowego (ang. firmware) dla wszystkich komponentów serwera 19) przywrócenie poprzednich wersji oprogramowania układowego 20) funkcję eksportu/importu konfiguracji (ustawienie karty zarządzającej, BIOSu, kart sieciowych, HBA oraz konfiguracji kontrolera RAID) serwera do/z pliku XML lub JSON 21) funkcję automatycznego tworzenia kopii konfiguracji serwera w oparciu o zdefiniowany harmonogram 22) wykrywanie odchyleń konfiguracji na poziomie konfiguracji UEFI oraz wersji oprogramowania układowego serwera 23) uruchomienie funkcjonalności umożliwiającej dostęp bezpośrednio poprzez urządzenia mobilne – funkcja konfiguracji oraz monitorowania najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej (dostępnej dla systemów operacyjnych co najmniej Android i Apple iOS) używając jednego z protokołów BLE lub WIFI (dotyczy serwerów typu „A", „B", „C") 24) zdalne wyłączenia i włączenia portów USB 25) mechanizm bezpiecznego wycofywania z eksploatacji poprzez automatyczne usuwanie poufnych danych w tym minimum: a) konfiguracji BIOS b) konfiguracji kontrolera RAID c) dzienników systemowych d) danych konfiguracyjnych e) wszystkich danych z nośników wewnętrznych (dyski twarde, DCPMM, NVDIMM). Jeśli wymagana jest dodatkowa licencja na jakąkolwiek funkcjonalność wskazaną przez zmawiającego, to musi ona być dostarczona wraz z serwerem w wersji bez ograniczeń czasowych i terytorialnych(dotyczy terytorium UE). Ponadto Zamawiający wymaga, aby żadna z powyższych funkcjonalności nie wymagała okresowego sprawdzania licencji na zewnętrznych systemach (np. producenta).
System do zarządzania	1) System do zarządzania serwerami wraz z niezbędną licencją, który musi spełniać niżej wymienione wymagania: a) Integrację z posiadanym i wykorzystywanym przez Zamawiajacego lub planowanym do wykorzystania w projekcie przez Zamawiającego oprogramowaniem LDAP lub Microsoft Active Directory w zakresie uwierzytelnienia i autoryzacji kont dostępowych b) zarządzanie dostarczonymi serwerami bez udziału dedykowanego agenta c) wsparcie dla protokołów SNMP, IPMI, 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 i) tworzenie automatycznie grup serwerów w oparciu o dowolny element konfiguracji serwera np. nazwa, lokalizacja, system operacyjny, obsadzenie slotów PCIe, pozostały czas gwarancji j) podgląd stanu środowiska zawierający najważniejsze informacje na jego temat k) podsumowanie stanu dla każdego serwera l) szczegółowy status serwera i jego elementów/komponentów m) filtry raportów umożliwiające podgląd wybranych zdarzeń n) integracja z systemem do obsługi zgłoszeń producenta dostarczonej platformy sprzętowej o) możliwość uruchomienia/przechwycenia wirtualnej konsoli serwera p) możliwość podmontowania wirtualnego napędu na zarządzanym serwerze q) kreator umożliwiający dostosowanie akcji dla wybranych alertów r) możliwość importu plików MIB s) możliwość definiowania ról administratorów t) możliwość zdalnej aktualizacji oprogramowania układowego serwerów u) 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 serwerze w) możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów x) moduł raportujący pozwalający na wygenerowanie raportu zawierającego co najmniej następujące informacje: i) numery seryjne serwerów ii) konfiguracje poszczególnych serwerów iii) wersje oprogramowania wewnętrznego iv) obsadzenie slotów PCI i gniazd pamięci v) informacje o maszynach wirtualnych vi) aktualne informacje o stanie i poziomie gwarancji vii) adresy IP kart sieciowych viii) występujące alerty ix) adresy MAC kart sieciowych x) stan poszczególnych komponentów serwerów y) możliwość tworzenia sprzętowej konfiguracji bazowej i na jej podstawie weryfikacji środowiska w celu wykrycia rozbieżności z) wdrażanie serwerów w oparciu o profile konfiguracji

	aa) możliwość migracji ustawień serwera wraz z wirtualnymi adresami sieciowymi (MAC, WWN, IQN) między serwerami bb) tworzenie gotowych paczek informacji umożliwiających zdiagnozowanie awarii serwera przez serwis producenta cc) zdalne uruchamianie diagnostyki serwera. 2) System może być zaoferowany jako prekonfigurowany obraz maszyny wirtualnej (ang. virtual appliance) dla zaoferowanego oprogramowania do wirtualizacji mocy obliczeniowej. 3) Musi być dostępna dedykowana aplikacja na urządzenia mobilne (wyposażone w system operacyjny co najmniej Android/ iOS) integrująca się z wyżej opisanym systemem do zarządzania (dotyczy serwerów typu „A", „B", „C"). 4) System do zarządzania serwerem musi być zintegrowany z zaoferowanym oprogramowaniem do zarządzania klastrem wirtualizacyjnym (zwanym dalej konsolą wirtualizatora i opisanym w niniejszym dokumencie w punkcie 12.4) i spełniać następujące wymagania: a) możliwość instalowania poprawek podnoszących wersję oprogramowania układowego (ang. firmware) serwera wprost z konsoli wirtualizatora (wymagana zgodność z zaoferowanym oprogramowaniem wirtualizacyjnym) b) 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 c) 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 d) konsola wirtualizatora musi prezentować informacje wspierające serwisowanie takie jak: a. numer serwisowy/seryjny serwera b. data obowiązywania gwarancji e) 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 f) 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.

	Jeśli wymagana jest dodatkowa licencja na jakąkolwiek funkcjonalność wskazaną przez zmawiającego, to musi ona być dostarczona wraz z serwerem w wersji bez ograniczeń czasowych i terytorialnych(dotyczy terytorium UE). Ponadto Zamawiający wymaga, aby żadna z powyższych funkcjonalności nie wymagała okresowego sprawdzania licencji na zewnętrznych systemach (np. producenta).
Diagnostyka	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)).
Zasilacze	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.
Certyfikaty	Certyfikaty potwierdzające zgodność oferowanego modelu serwera z wykorzystywanym lub planowany do wykorzystania w projekcie przez Zamawiającego oprogramowaniem: 1) Microsoft Windows Server min. w wersji 2022 na stronie: https://www.windowsservercatalog.com/ 2) Red Hat Enterprise Linux (RHEL) min. w wersji 9 na stronie: https://access.redhat.com/ecosystem/hardware 3) VMware ESXi min. w wersji 7 na stronie: https://www.vmware.com/resources/compatibility/search.php
Dokumentacja użytkownika	1) Zamawiający wymaga dostarczenia dokumentacji technicznej w języku polskim lub angielskim w wersji elektronicznej.

Kod pola został zmieniony

2.2. Wymagania wspólne dla serwerów typu A, B, C, D, E

Parametr	Charakterystyka (wymagania minimalne)
Pamięć RAM (dotyczy serwerów typu A,B,C,D)	1) Minimum 2 TB DDR4 RDIMM 3200 MT/s w konfiguracji wypełniającej wszystkie gniazda pamięci na płycie głównej. Płyta główna musi zapewniać obsługę co najmniej 4 TB pamięci RAM.
Pamięć RAM (dotyczy serwerów typu E)	1) Minimum 2 TB DDR5 RDIMM min. 4400 MT/s w konfiguracji wypełniającej wszystkie gniazda pamięci na płycie głównej. Płyta główna musi zapewniać obsługę co najmniej 4 TB pamięci RAM.
Interfejsy sieciowe	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 posiadająca: 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 dekapsulacji 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: a) wsparcie dla wirtualizacji SR-IOV b) wsparcie dla enkapsulacji i dekapsulacji dla protokołów VxLAN, NVGRE, Geneve c) wsparcie dla RoCE d) wsparcie dla Jumbo Frames o rozmiarach minimum 9 KB. 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.

2.3. Serwer obliczeniowy typu „A”

Zaoferowany serwer musi spełniać wszystkie wymagania wspólne opisane w punkcie 2.1 oraz wymagania wspólne dla podzbioru typu serwów opisane w punkcie 2.2 oraz poniższe wymagania.

Parametr	Charakterystyka (wymagania minimalne)
Obudowa	1) Wysokość 1 lub 2 RU.
Procesor	1) Zainstalowane 2 procesory 32-rdzeniowe, o taktowaniu co najmniej 2.1 GHz, klasy x86-64 do pracy z zaoferowanym serwerem umożliwiające osiągnięcie wyniku podstawowego (Base) min. 615 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 5.0.
Dyski twarde	1) Zainstalowane 2 jednakowe dyski M.2 SSD o pojemności minimum 480 GB każdy, skonfigurowane w RAID 1, podłączone za pośrednictwem kontrolera zoptymalizowanego pod kątem rozruchu.
Kontroler RAID	1) Sprzętowy kontroler dyskowy HBA PCIe 4 zgodny z zaoferowanym oprogramowaniem do wirtualizacji.

2.4. 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 2.2 oraz poniższe wymagania.

Parametr	Charakterystyka (wymagania minimalne)
Obudowa	1) Wysokość 1 lub 2 RU.
Procesor	1) Zainstalowane 2 procesory 32-rdzeniowe, o taktowaniu co najmniej 2.1 GHz, klasy x86-64 do pracy z zaoferowanym serwerem umożliwiające osiągnięcie wyniku podstawowego (Base) min. 615 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 5.0.
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 zaoferowanym oprogramowaniem do wirtualizacji.
Dyski twarde	1) Zainstalowane 2 jednakowe dyski M.2 SSD o pojemności minimum 480 GB każdy, skonfigurowane w RAID 1, podłączone za pośrednictwem kontrolera zoptymalizowanego pod kątem rozruchu. 2) Zainstalowane 2 jednakowe dyski NVME SSD Hot-Swap do intensywnego odczytu (ang. read intensive) o współczynniku DWPD minimum 1 i pojemności minimum 960 GB każdy podłączone za pomocą zaoferowanego kontrolera RAID.

2.5. Serwer obliczeniowy typu „C”

Zaoferowany serwer musi spełniać wszystkie wymagania wspólne opisane w punkcie 2.1 oraz wymagania wspólne dla podzbioru typu serwów opisane w punkcie 2.2 oraz poniższe wymagania.

Parametr	Charakterystyka (wymagania minimalne)
Obudowa	1) Wysokość 1 lub 2 RU.
Procesor	1) Zainstalowane dwa procesory 32-rdzeniowe, o taktowaniu co najmniej 2.1 GHz, klasy x86-64 do pracy z zaoferowanym serwerem umożliwiające osiągnięcie wyniku podstawowego (Base) min. 615 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 5.0.
Dyski twarde	1) Zainstalowane 2 jednakowe dyski M.2 SSD o pojemności minimum 480 GB każdy, skonfigurowane w RAID 1, podłączone za pośrednictwem kontrolera zoptymalizowanego pod kątem rozruchu. 2) Zainstalowane 2 jednakowe dyski NVME SSD Hot-Swap do różnych zastosowań (ang. mixed-use) o współczynniku DWPD minimum 3 i pojemności minimum 1.6 TB każdy. 3) Zainstalowane 10 jednakowych dysków SSD Hot-Swap do intensywnego odczytu (ang. read intensive) o współczynniku DWPD minimum 1 i pojemności minimum 3.84 TB każdy, podłączone za pomocą zaoferowanego kontrolera RAID.
Kontroler	1) Sprzętowy kontroler dyskowy zgodny z zaoferowanym oprogramowaniem do wirtualizacji oraz znajdujący się na liście zgodności zaoferowanego oprogramowania do wirtualizacji przestrzeni dyskowej opisanego w punkcie **12.7** i **12.8**.

Usunięte: HBA, wspierający interfejs PCIe 4.0,

2.6. Serwer obliczeniowy typu „D”

Zaoferowany serwer musi spełniać wszystkie wymagania wspólne opisane w punkcie 2.1 oraz wymagania wspólne dla podzbioru typu serwów opisane w punkcie 2.2 oraz poniższe wymagania.

Parametr	Charakterystyka (wymagania minimalne)
Obudowa	1) Nie więcej niż 4 RU.
Procesor	1) Zainstalowane 2 procesory 32-rdzeniowe, o taktowaniu co najmniej 2.95GHz, klasy x86-64 do pracy z zaoferowanym serwerem umożliwiające osiągnięcie wyniku min. 87 tysięcy punktów w teście PassMark – CPU Mark (stan na 07.06.2023r), w konfiguracji dwuprocesorowej, potwierdzony na stronie cpubenchmark.net 2) Procesor musi obsługiwać interfejs PCIe 4.0.

Dyski twarde	1) Zainstalowane 2 jednakowe dyski M.2 SSD o pojemności minimum 480 GB każdy, skonfigurowane w RAID 1, podłączone za pośrednictwem kontrolera zoptymalizowanego pod kątem rozruchu.
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 zaoferowanym oprogramowaniem do wirtualizacji.
Akcelerator Graficzny	1) Zainstalowane min. 4 karty GPU przeznaczone do wspomagania obliczeń naukowo inżynierskich pojedynczej i podwójnej precyzji spełniające co najmniej wymagania: a) chłodzenie pasywne b) bazowe taktowanie rdzenia minimum 1060 MHz c) taktowanie rdzenia w trybie turbo minimum 1400 MHz d) pamięcią minimum 80 GB typu HBM2e o taktowaniu minimum 1500 MHz e) szerokością szyny pamięci minimum 5120 bitów f) przepustowością maksymalną pamięci minimum 2000 GB/s g) wspierające PCIe 4.0 x16 wraz z lane and polarity reversal h) karty muszą być połączone ze sobą (każda z każdą) szyną dwukierunkową o przepustowości minimum 600 GB/s i) karty muszą gwarantować natywne wspieranie wykorzystywanego przez Zamawiającego modelu programistycznego CUDA j) karty muszą gwarantować natywne wsparcie dla używanego przez zamawiającego pakietu OpenACC k) karty GPU muszą być komponentem oferowanym w oficjalnym kanale producenta serwera i być objęte tą samą gwarancją co cały serwer.
Interfejsy Fibre Channel	1) Zainstalowana 1 karta w serwerze jako karta rozszerzeń w slocie PCIe, która musi posiadać co najmniej 2 porty FibreChannel 32 Gb/s wyposażonych we wkładki optyczne SR. Karta FibreChannel musi poprawnie działać z zaoferowanym oprogramowaniem do wirtualizacji zasobów serwerowych i ich mocy obliczeniowej.

2.7. Serwer obliczeniowy typu „E”

Zaoferowany serwer musi spełniać wszystkie wymagania wspólne opisane w punkcie 2.1 oraz wymagania wspólne dla podzbioru typu serwów opisane w punkcie 2.2 oraz poniższe wymagania.

Parametr	**Charakterystyka (wymagania minimalne)**
Obudowa	1) Nie więcej niż 6 RU.
Procesor	1) Zainstalowane dwa procesory 32-rdzeniowe, o taktowaniu co najmniej 2.8 GHz, klasy x86-64 do pracy z zaoferowanym serwerem umożliwiające

	osiągnięcie wyniku podstawowego (Base) min. 15.3 punktów w teście CPU2017 Integer Speed. Wynik dla dowolnego serwera w konfiguracji z zaproponowanymi procesorami musi być dostępny na stronie www.spec.org. 2) Procesor musi obsługiwać interfejs PCIe 5.0.
Dyski twarde	1) Zainstalowane 2 jednakowe dyski M.2 SSD o pojemności minimum 480 GB każdy, skonfigurowane w RAID 1, podłączone za pośrednictwem kontrolera zoptymalizowanego pod kątem rozruchu. 2) Zainstalowane 2 jednakowe dyski NVME SSD Hot-Swap do intensywnego odczytu (ang. read intensive) o współczynniku DWPD minimum 1 i pojemności minimum 960 GB każdy podłączone za pomocą zaoferowanego kontrolera RAID.
Kontroler RAID	1) Kontroler zgodny z zaoferowanym oprogramowaniem do wirtualizacji.
Akcelerator Graficzny	1) Zainstalowane 8 kart GPU w standardzie SXM5 przeznaczone do wspomagania obliczeń naukowo inżynierskich pojedynczej i podwójnej precyzji spełniające co najmniej wymagania: a) chłodzenie pasywne b) bazowe taktowanie rdzenia minimum 1600 MHz c) taktowanie rdzenia w trybie turbo minimum 1900 MHz dla FP64 d) pamięcią minimum 80 GB typu HBM3 o taktowaniu minimum 2600 MHz e) szerokością szyny pamięci minimum 5120 bitów f) przepustowością maksymalną pamięci minimum 3300 GB/s g) karty muszą być połączone ze sobą (każda z każdą) szyną dwukierunkową o przepustowości minimum 900 GB/s h) karty muszą gwarantować natywne wspieranie wykorzystywanego przez Zamawiajacego modelu programistycznego CUDA i) karty muszą gwarantować natywne wsparcie dla używanego przez zamawiającego pakietu OpenACC j) karty GPU muszą być komponentem oferowanym w oficjalnym kanale producenta serwera i być objęte tą samą gwarancją co cały serwer.
Sloty PCI	1) Serwer wyposażony w min. 8 slotów PCI Express x16 Gen. 5

2.8. Interfejsy Fibre Channel do serwera typu „A”

Opis dodatkowych interfejsów Fibre Channel do konfiguracji serwera typy „A”

Parametr	**Charakterystyka (wymagania minimalne)**
Interfejsy Fibre Channel	1) Zainstalowana 1 karta w serwerze jako karta rozszerzeń w slocie PCIe, która musi posiadać co najmniej 2 porty FibreChannel 32 Gb/s wyposażonych we wkładki optyczne SR.

	2) Karta FibreChannel musi poprawnie działać z zaoferowanym oprogramowaniem do wirtualizacji zasobów serwerowych i ich mocy obliczeniowej.

3. Macierz blokowa typu „A”

Zaoferowana macierz blokowa musi spełniać wszystkie wymagania przedstawione w poniższej tabeli.

Parametr	Charakterystyka (wymagania minimalne)
Obudowa	1) Obudowa przystosowana do zainstalowania w szafie teleinformatycznej 19” o wysokości 2 RU, musi być dostarczona wraz z zestawem szyn montażowych.
Zasoby dyskowe	1) Macierz musi zostać dostarczona w konfiguracji z minimum 19 jednakowymi dyskami 2.5" SSD NVMe Hot-Swap. 2) Dostarczona macierz musi zapewnić pojemność użyteczną minimum 100 TiB. Pojemność użyteczną macierzy 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. 3) Dostarczona macierz musi zapewnić przestrzeń efektywną (po zastosowaniu mechanizmów kompresji i deduplikacji) minimum 400 TiB. 4) Osiągnięta przestrzeń min. 400 TiB musi być zapewniona i gwarantowana przez producenta macierzy. Macierz musi posiadać możliwość zapełnienia całej dostarczonej przestrzeni. Jeśli macierz pozwala na zapełnienie tylko części przestrzeni (np. 80%) to pozostająca „pusta - niewykorzystana" przestrzeń nie będzie wliczona w dostarczoną przestrzeń. 5) Macierz w dostarczonej konfiguracji (z włączoną deduplikacją i kompresją) musi umożliwiać osiągnięcie wydajności minimum 500 tysięcy IOPS z przestrzeni dyskowej (przy założeniach: dla bloku danych o wielkości 4k odczyt 80%, zapis 20% oraz wszystkie operacje losowe). 6) Macierz w dostarczonej konfiguracji (z włączoną deduplikacją i kompresją) musi umożliwiać osiągnięcie minimum 1900 MiB/s odczytu z przestrzeni dyskowej (nie z cache macierzy). 7) Zastosowane mechanizmy ochrony danych w zaoferowanej konfiguracji muszą zabezpieczać dane przed ich utratą w przypadku awarii co najmniej 1 (jednego) dysku. 8) W zaoferowanej konfiguracji macierzy należy uwzględnić przestrzeń zapasową lub dyski zapasowe („Hot Spare”) według zaleceń producenta macierzy. Minimalnie pojemność jednego dysku lub jeden dysk. 9) Dostarczona macierz musi być rozwiązaniem zaprojektowanym tylko i wyłącznie do dysków SSD lub modułów flash. Dostarczona macierz w żadnej konfiguracji nie może oferować obsługi dysków obrotowych, a co za tym idzie nie może oferować rozbudowy o dyski obrotowe. 10) Macierz musi umożliwiać budowę jednego obszaru danych na wszystkich dyskach zainstalowanych wewnątrz macierzy. Dyski muszą być skonfigurowane w taki sposób aby utrata dowolnego z nich zapewniła ciągłość dostępu do danych.

	11) Macierz dyskowa musi umożliwiać stosowanie w niej na potrzeby składowania danych dysków SSD NVMe lub SCM. 12) Wymagane jest szyfrowanie danych na dyskach. 13) Należy dostarczyć niezbędne licencje na całą pojemność macierzy. Do oferty należy dołączyć wydruk z narzędzia producenta oferowanej macierzy – konfiguratora / estymatora potwierdzony przez producenta, potwierdzający spełnienie powyższych wymagań, zawierający zarówno proponowaną konfigurację sprzętową z dokładnym wskazaniem numerów producenta („part number") dla wszystkich elementów jak i ich ilości, w tym typów i okresów wsparcia licencji i gwarancji, jak i wynikające z niej parametry pojemnościowe i wydajnościowe.
Kontrolery macierzy dyskowej	1) Macierz musi być wyposażona w minimum 2 kontrolery. 2) Każdy kontroler macierzy musi być wyposażony w co najmniej 576 GB przestrzeni cache służącej do buforowania operacji odczytu oraz zapisu. 3) Kontrolery muszą wspierać jednocześnie ruch - blokowy i plikowy (wymagane co najmniej protokoły: iSCSI, FC oraz plikowy CIFS - minimum SMB w wersjach 1,2,3,3.1.1, FTP, SFTP oraz NFS). Nie dopuszcza się realizacji funkcjonalności ruchu plikowego za pomocą dodatkowych/zewnętrznych urządzeń. 4) Kontrolery muszą działać w sposób redundantny - tj. przy uszkodzeniu dowolnego kontrolera, macierz musi nadal działać i utrzymywać dostęp do odczytu i zapisu danych - praca w trybie Active/Active. 5) W przypadku awarii zasilania dane nie zapisane na dyskach muszą być zabezpieczone za pomocą podtrzymania bateryjnego w celu zachowania ich w pamięci nieulotnej kontrolera do momentu przywrócenia zasilania. 6) Obszar pamięci cache przeznaczony do zapisów danych (ang. write cache) musi posiadać lustrzaną kopię (ang. mirror) i poprawnie funkcjonować nawet w razie awarii jednego z kontrolerów macierzy. 7) Każdy kontroler macierzy musi być wyposażony w wielordzeniowe procesory (minimum 48 rdzeni łącznie). 8) Macierz musi umożliwiać obsługę różnych poziomów RAID, co najmniej RAID5, RAID6.
Interfejsy	1) Minimalnie macierz musi być wyposażona w następujące działające porty: a) 4 porty 100 Gb/s Ethernet do podłączania serwerów, każdy port wyposażony w moduł optyczny QSFP28 b) 8 portów 25Gb/s Ethernet do podłączania serwerów, każdy port wyposażony w moduł optyczny SFP28 c) 2 porty 1 Gb/s Ethernet Base-T do zdalnego zarządzania kontrolerem d) 4 porty minimum 100 Gb/s do podłączania półek dyskowych po protokole NVMe. 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) Musi być zapewniona możliwość rozbudowy macierzy o minimum 4 dodatkowe porty 100 Gb/s Ethernet jedynie poprzez instalację dodatkowych kart rozszerzeń bez konieczności instalacji dodatkowych kontrolerów.

Redukcja danych	1) Macierz musi zapewniać mechanizm kompresji i deduplikacji danych w trybie „in-line". Kompresja i deduplikacja muszą być integralną częścią systemu macierzowego bez możliwości zatrzymania bądź wyłączenia przez administratora. 2) Dla każdego wolumenu macierzy musi zachodzić jednocześnie kompresja i deduplikacja danych, która nie wymaga konfiguracji ani żadnej innej interwencji ze strony administratora macierzy. Operacje kompresji i deduplikacji muszą działać na wszystkich rodzajach dostarczanych i opcjonalnych nośników SSD i być dostępne dla wszystkich rodzajów przechowywanych danych (nie jest dozwolone oferowanie rozwiązań, które nie zapewniłyby kompresji i deduplikacji na całej wymaganej pojemności). 3) Wymagane jest zagwarantowane przez producenta oferowanej macierzy osiągnięcie współczynnika redukcji danych dla całej macierzy na poziomie min. 4:1 przy spełnieniu wymagań pojemnościowych określonych w punkcie *Zasoby dyskowe*. Zamawiający dopuszcza możliwość dostarczenia macierzy o gwarantowanym przez producenta współczynnika redukcji danych dla całej macierzy w niższym stopniu, jednak w takim przypadku należy dostarczyć macierz w takiej konfiguracji aby przestrzeń efektywna wynosiła min. 400 TiB. W powyższej kalkulacji nie będzie wymagane uwzględnienie danych wcześniej zaszyfrowanych (z pominięciem mechanizmu szyfrowania przez macierz) i wcześniej skompresowanych. 4) Obowiązkowe jest dodanie do oferty odpowiedniego dokumentu zawierającego najlepsze praktyki dotyczące konfiguracji i zarządzania macierzą dostępne online na stronach producenta. 5) Wymagane jest dostarczenie przez Zamawiającego wraz z ofertą potwierdzenia/oświadczenie producenta, że zaoferowana macierz w zaoferowanej konfiguracji sprzętowej będzie oferowała efektywną przestrzeń o pojemności min. 400 TiB. W sytuacji gdy do uzyskania efektywnej przestrzeni będzie wykorzystywany współczynnik redukcji danych, informacja taka musi znajdować się na dostarczonym oświadczeniu. Jeżeli takie potwierdzenie/oświadczenie Producenta oferowanej macierzy nie zostanie przedstawione Zamawiającemu do dnia odbioru przedmiotu zamówienia zostanie to zinterpretowane jako brak wymaganego współczynnika redukcji danych. W takim przypadku oferent zobowiązuje się dostarczyć powierzchnię 400 TiB przestrzeni użytecznej zbudowaną z tych samych elementów.
Funkcjonalności	1) Macierz musi umożliwiać wykonywanie procesu aktualizacji oprogramowania układowego (ang. firmware) macierzy w trybie online bez przerywania dostępu do zasobów dyskowych macierzy i przerywania pracy aplikacji. 2) Macierz musi umożliwiać skalowalną rozbudowę on-line do co najmniej 8 kontrolerów zarządzanych z jednej konsoli oraz poprzez dodawanie półek dyskowych do par kontrolerów. Po takiej rozbudowie musi być możliwość zaprezentowania każdego wolumenu logicznego LUN przez dowolny z kontrolerów bez przerywania dostępu do danych.

	3) System musi obsługiwać natywną integrację ze środowiskiem wirtualizacyjnym, dostarczanym w ramach tego postępowania, umożliwiając przypisanie do podsystemu pamięci masowej operacji wirtualizatora, takich jak: a) tworzenie dysków wirtualnych b) klonowanie dysków wirtualnych c) wykonanie kopii migawkowych d) przenoszenie dysków wirtualnych. 4) Macierz musi obsługiwać funkcję „Local Protection" (Snapshot z technologią Redirect-On-Write dla danych blokowych i plikowych i Thin Clones), rozwiązania, które nie obsługują funkcji „redirect on write" nie są dozwolone. Rozwiązanie powinno obsługiwać ciągłą ochronę danych dla dostarczanego wirtualizatora. 5) Macierz musi obsługiwać kopie spójności aplikacji z replikacjami lokalnymi. 6) Zamawiający wymaga dostarczenia licencji dla replikacji zdalnych na etapie postępowania. 7) Macierz musi zapewniać: a) monitorowanie wydajności (opóźnienie, IOPS, odczyt/zapis, szerokość pasma, rozmiar IO, długość kolejki), b) monitorowanie pojemności (łącznie, oszczędność - redukcja danych, snapshoty) c) konfigurację umożliwiającą przekierowanie powiadomienia na adres e-mail d) dostęp poprzez dedykowaną do tego celu aplikacje producenta macierzy dla urządzeń mobilnych co najmniej Android i iOS. Rozwiązanie musi być hostowane w środowisku producenta macierzy i być udostępnione bez dodatkowych kosztów przez cały okres użytkowania dostarczonego rozwiązania i zapewniać co najmniej 1 rok danych historycznych. 8) Należy dostarczyć oprogramowanie do wykonywania spójnych kopii danych dla aplikacji wykorzystywanych lub planowanych do wykorzystania w projekcie przez Zamawiającego: a) Microsoft Exchange 2019 b) SQL Server 2019 c) Oracle Databases 19 d) blokowych i plikowych zasobów dla dostarczonego oprogramowania do wirtualizacji mocy obliczeniowej. Spójność kopii rozumieć należy jako funkcjonalność automatycznego przełączenia aplikacji w tryb wykonania spójnej kopii swoich danych. Oprogramowanie to musi rozpoznać, na których wolumenach logicznych aplikacja składuje swoje dane i wykonać kopie tylko tych wolumenów. 9) Macierz zarówno na poziomie jednej macierzy, jak i klastra, musi być zarządzana z poziomu jednej aplikacji, dostarczonej przez jej producenta. Nie dopuszcza się dzielenia zarządzania pomiędzy różne aplikacje. 10) Macierz musi obsługiwać co najmniej dwukierunkową asynchroniczną zdalną replikację przez IP z opcją ustawienia relacji do: "1:1", "1:n", i "n:1".

	11) Macierz musi zapewniać mechanizm „thin provisioning”, który polega na udostępnianiu większej przestrzeni logicznej niż jest to fizycznie alokowane w momencie tworzenia zasobu lub w momencie, gdy aplikacja nie wykorzystała pojemności. Wymagane jest dostarczenie niezbędnych licencji na całą oferowaną pojemność macierzy w wersji bez ograniczeń czasowych. Jeśli wymagana jest dodatkowa licencja na jakąkolwiek funkcjonalność wskazaną przez Zmawiającego to musi ona być dostarczona wraz z macierzą w wersji bez ograniczeń czasowych
Zasilanie	1) Macierz musi być wyposażona w podwójny, redundantny system zasilania i chłodzenia, gwarantujący nieprzerwany dostęp do wolumenów dyskowych (LUN) oraz działania pamięci cache w przypadku awarii jednego ze źródeł zasilania.
Dodatkowe wymagania	1) Rozwiązanie musi mieć możliwość rozbudowy do 432 rdzeni procesora oraz minimum 8TB pamięci RAM. Rozbudowa nie może powodować wymiany zastosowanych dysków twardych. 2) Pamięć Write Cache musi być zabezpieczona dwoma bateriami, tak aby w razie awarii jednej baterii, pamięć cały czas miała bateryjną ochronę podtrzymania zasilania. 3) W przypadku instalacji z dwoma macierzami, macierz oferuje możliwość replikacji wolumenu w trybie synchronicznym w taki sposób, aby możliwy był jednoczesny zapis i odczyt z obu replikowanych wolumenów na obu macierzach w tym samym momencie co najmniej dla oferowanego oprogramowania do wirtualizacji zasobów serwerowych. Dodatkowo w razie całkowitej utraty jednej z macierzy, powinny zadziałać mechanizmy wysokiej dostępności w taki sposób, aby dostęp do wolumenu był nieprzerwany z punktu widzenia serwerów korzystających z zasobów macierzy. Funkcjonalność musi być integralną cechą macierzy lub może być realizowana za pomocą dodatkowych urządzeń. Replikacja synchroniczna między macierzami musi odbywać się za pomocą protokołu IP. 4) Macierz posiada natywne wsparcie dla technologii NVMe-over-TCP.
Wymiana dysków	1) Wymiana dysków może być dokonywana samodzielnie przez zamawiającego. 2) Zamawiający zatrzymuje uszkodzone dyski.

4. Macierz blokowa typu „B”

Zaoferowana macierz blokowa musi spełniać wszystkie wymagania przedstawione w poniższej tabeli.

Parametr	Charakterystyka (wymagania minimalne)
Zasoby dyskowe	1) Serwer dyskowy / macierz dyskowa musi być dostarczona z minimum: a) 35 jednakowymi dyskami SSD 2,5" o współczynniku DWPD minimum 1 – pojemność użyteczna dla przestrzeni zbudowanej w oparciu o te dyski musi wynosić minimum 99 TiB 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. 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). 3) W zaoferowanej konfiguracji dyskowej muszą być uwzględnione dyski zapasowe („Hot Spare”) lub pojemność zapasową w ilości zgodnej z zaleceniami producenta dla oferowanej konfiguracji. 4) Podczas awarii dysku kontroler macierzy dyskowej musi automatycznie rozpocząć odtwarzanie danych na fizycznym dysku zapasowym. 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). 6) Kontrolery macierzy dyskowej muszą obsługiwać minimum 1000 dysków.
Kontrolery macierzy dyskowej	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. 2) Obszar pamięci cache przeznaczony do zapisów danych musi posiadać lustrzaną kopię (ang. mirror). 3) W przypadku awarii zasilania dane niezapisane na dyskach muszą być zabezpieczone za pomocą podtrzymania bateryjnego w celu zachowania ich w pamięci nieulotnej kontrolera do momentu przywrócenia zasilania.

	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 384 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) Macierz musi mieć możliwość obsługi różnych poziomów RAID równocześnie, minimum RAID 1 (lub 10), 5, 6. 8) Awaria dowolnego pojedynczego aktywnego elementu macierzy dyskowej nie może powodować przerwy w dostępie do danych. 9) Musi być możliwe utworzenie minimum 1000 wolumenów blokowych o rozmiarze minimum 256 TB, plikowych o rozmiarze minimum 256 TB. 10) Macierz musi posiadać wbudowaną funkcjonalność typu „thin provisioning" umożliwiającą alokację wirtualnej przestrzeni dyskowej, do której fizyczne dyski mogą być dostarczone w przyszłości.
Interfejsy	1) Macierz musi być wyposażona w następujące, działające porty: 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) 8 portów 32Gb FC do podłączania serwerów. 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	1) System operacyjny macierzy dyskowej musi natywnie obsługiwać mechanizm kopii migawkowych, który będzie dostępny dla wszystkich rodzajów danych udostępnianych. Niedopuszczalne są rozwiązania wykonujące kopie

	migawkowe jedynie w trybie „Copy On Write” dla dowolnego rodzaju danych (blokowe lub plikowe). 2) Odtwarzanie plików i folderów z kopii migawkowych wykonanych dla wolumenów plikowych udostępnionych dla posiadanych i wykorzystywanych lub planowaną do wykorzystania w projekcie przez Zamawiającego 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 do posiadanych i wykorzystywanych przez Zamawiającego lub planowanych do wykorzystania w projekcie przez Zamawiającego 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 składuje swoje dane i wykonać kopie tylko tych wolumenów.
Obsługiwane protokoły	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.
Pozostałe wymagania	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: 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. 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 wykorzystywanej przez Zamawiającego lub planowanej do wykorzystania w projekcie przez Zamawiającego 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 Zmawiającego to musi ona być dostarczona wraz z macierzą. 10) Wszystkie kontrolery muszą posiadać tą samą liczbę portów w identycznej konfiguracji.
Gwarancja	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	1) Wymiana dysków może być dokonywana samodzielnie przez Zamawiającego. 2) Zamawiający zatrzymuje uszkodzone dyski u siebie, bez konieczności ponoszenia dodatkowych opłat.

5. System szybkiej pamięci masowej o dostępie plikowym typu „A”

Zaoferowany system szybkiej pamięci masowej o dostępie plikowym musi spełniać wszystkie wymagania przedstawione w poniższej tabeli.

Parametr	**Charakterystyka (wymagania minimalne)**
Pojemność, wydajność i bezpieczeństwo systemu	1) Zaoferowany system pamięci masowej o dostępie plikowym (zwanym dalej systemem) musi być zbudowany w architekturze „scale-out” (skalowalnej horyzontalnie). 2) System musi być zbudowany w oparciu jednakowe węzły serwerowe (kontrolerowo-dyskowe) zwane dalej węzłami. 3) Rozwiązanie musi być zbudowane na dyskach SSD NVMe nie większych niż 3,84 TB. 4) Architektura systemu oraz zastosowane mechanizmy ochrony danych muszą zabezpieczać dane przed ich utratą w przypadku awarii co najmniej 2 (dwóch) dowolnych dysków jednocześnie lub 2 (dwóch) dowolnych węzłów. 5) Wymagane mechanizmy ochrony przed awarią dysku to RAID lub kodowanie nadmiarowe (ECC). W przypadku mechanizmu RAID, ze względu na dłuższy czas odbudowy, macierz powinna być odporna na jednoczesną awarię co najmniej 3 (trzech) dowolnych dysków (należy uwzględnić w konfiguracji pojemności przestrzeni użytecznej). 6) Rozwiązanie musi umożliwiać ochronę danych przy pomocy wielokrotnego zapisu (ang. mirroring). 7) Musi istnieć możliwość zmiany protekcji danych przy zachowaniu nieprzerwanej dostępności zasobów, również pomiędzy trybem ECC i mirroring, w tym również dla plików w obrębie tego samego folderu, bez konieczności ich przenoszenia na inny zasób. 8) W przypadku awarii dysku czas odbudowy nie może być dłuższy niż 60 godzin (w sytuacji braku obciążenia przez urządzenia klienckie). 9) System musi udostępniać całą dostępną przestrzeń w ramach jednego ciągłego systemu plików, który musi być skalowalny do co najmniej 4000 TiB powierzchni użytkowej. 10) System musi umożliwiać rozbudowę do co najmniej 200 węzłów w ramach tego samego systemu dyskowego, prezentujących do klientów jeden system plików.

	11) System nie może posiadać pojedynczego punktu awarii, tzn. wszystkie jego elementy muszą być redundantne, a jego architektura musi zapewniać odporność na awarię w obrębie poszczególnych grup elementów, przynajmniej w zakresie: a) dysków b) interfejsów sieciowych c) kontrolerów (węzłów) d) zasilaczy e) wentylatorów. 12) Dostarczony system musi zapewnić pojemność użyteczną minimum 610 TiB. Pojemność użyteczną 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. 13) System musi zapewniać wydajność: a) wydajność nie mniejsza niż 9000 MB/s (megabajtów na sekundę) w przypadku losowych odczytów protokołem NFS v.3 (RFC 1813) dla bloku o wielkości 8KB i nie więcej niż 60 jednoczesnych wątków (ang. threads) na węzeł, b) wydajność nie mniejszą niż 750tys. file OPS (operacji plikowych na sekundę) w teście SPEC SFS 2014 dla obciążenia zdefiniowanego jako SWBUILD przy zachowaniu średnich opóźnień nie większych niż 9ms. Oferent musi przedstawić wyniki testu potwierdzające spełnienie tego warunku, potwierdzone przez producenta sprzętu. 14) System musi być zbudowany z co najmniej 25 jednakowych węzłów (kontrolerów), gdzie każdy realizuje dostęp plikowy do danych i zapewnia wysoką wydajność dostępu do zgromadzonych plików w systemie.
Sprzęt	1) W celu maksymalizacji gęstości, tj. minimalizacji wykorzystania obszaru serwerowni do przechowywania danych, pojedynczy węzeł nie może zajmować więcej niż 1 RU w szafie. 2) System musi być dostarczony wraz z kompletem wszystkich niezbędnych elementów potrzebnych do połączenia poszczególnych węzłów w jeden system, zarządzany z jednego interfejsu administracyjnego. 3) Każdy węzeł musi być wyposażony w 2 procesory klasy x86-64, z których każdy posiada minimum 10 rdzeni. 4) Ze względu na przewidywane obciążenie i wymaganą wydajność nie dopuszcza się realizacji pamięci podręcznej (ang. cache) w oparciu o dyski SSD.

	5) Każdy z elementów systemu musi być wyposażony w redundantne zasilacze zapewniające odporność na awarię pojedynczego źródła zasilania. 6) Każdy węzeł musi być wyposażony w 2 karty sieciowe Ethernet, każda z nich musi posiadać 2 porty 100 Gb/s Ethernet QSFP28. Interfejsy z jednej karty muszą być przeznaczone na potrzeby wewnętrznej komunikacji węzłów (interfejsy typu „back-end"). Interfejsy drugiej karty muszą być przeznaczone do zapewniania dostęp do danych (interfejsy typu „front-end"). 7) System musi zapewniać dostęp do danych przy jednoczesnym wykorzystaniu wszystkich interfejsów typu „front-end". 8) Komunikacja pomiędzy węzłami („back-end") musi: a) odbywać się za pośrednictwem osobnych i dedykowanych tylko do tego celu interfejsów (niewspółdzielonych z portami dostępowymi – „front-end"), b) odbywać się za pośrednictwem dedykowanych i przeznaczonych tylko do tego celu przełączników sieciowych (niewspółdzielonych z przełącznikami obsługującymi dostęp do danych – „front-end"), c) być zrealizowana w sposób redundantny, zapewniający prawidłową pracę systemu w przypadku awarii dowolnego przełącznika sieciowego obsługującego komunikację pomiędzy węzłami („back-end"). Wszystkie niezbędne elementy zapewniające tą komunikację (tj. przełączniki sieciowe, okablowanie, inne) muszą być dostarczone wraz z systemem i nie podlegają szczegółowej specyfikacji przez Zamawiającego. Zmawiający dopuszcza możliwość realizacji tych połączeń przy użyciu kabli typy „DAC" (ang. Direct Attach Cable). 9) Dostarczony system musi umożliwiać rozbudowę do min. 60 węzłów bez konieczności rozbudowy o dodatkowe przełączniki sieciowe dla połączeń wewnętrznych („back-end") pomiędzy węzłami. 10) System musi zapewnić gwarantowaną ochronę przed tzw. „cichym uszkodzeniem danych" (ang. silent data corruption) dla wszystkich technologii dyskowych. 11) System musi umożliwiać wymianę uszkodzonego dysku przy zachowaniu nieprzerwanej dostępności wszystkich zasobów, tj. bez czasowego wyłączania z użycia dowolnego z elementów urządzenia. Musi posiadać zaimplementowany system jednoznacznego określenia lokalizacji uszkodzonego dysku, np. za pomocą lampki kontrolnej przy uszkodzonym dysku. 12) System musi zapewniać pracę jednocześnie wszystkich węzłów w trybie aktywny/aktywny w celu zapewnienia niezawodności i dostępności danych (tzn. każdy kontroler powinien umożliwiać dostęp do wszystkich danych oraz prezentować spójny widok systemu plików).

Pamięć RAM	1) System musi zapewniać dostępną, łączną pojemność pamięci RAM nie mniejszą niż 9600 GB (tzn. min. 384 GB dla pojedynczego węzła).
Funkcjonalność	1) System musi umożliwiać dynamiczne rozszerzanie i zmniejszanie udostępnianych systemów plików bez konieczności: a) modyfikacji już zainstalowanych węzłów, b) ręcznej migracji/dystrybucji danych na nowe dyski systemu. 2) System musi zapewniać dostęp z rożnych systemów operacyjnych (posiadanych i wykorzystywanych lub planowanych do wykorzystania w projekcie przez Zamawiającego: UNIX, macOS, Linux, Windows) z wykorzystaniem standardowych protokołów. Wymagana jest poprawna obsługa co najmniej: NFS v3 i v4, SMB (CIFS) v2 i v3, FTP, HTTP i S3 API. 3) System musi wspierać natywnie Hadoop Distributed File System (HDFS). 4) Jednoczesny dostęp do tych samych danych musi być możliwy przy wykorzystaniu wszystkich protokołów wymienionych powyżej. System musi również umożliwiać zarządzanie uprawnieniami użytkowników w dostępie wieloprotokołowym. 5) System musi zapewnić obsługę alertów i umożliwiać monitorowanie za pomocą protokołu SNMP (w wersji min. 2c). 6) System musi zapewnić zdalny monitoring w celu diagnozy i usuwania usterek oraz w zakresie konserwacji – musi mieć możliwość automatycznej diagnozy i samodzielnego zgłaszania usterek w centrum serwisowym producenta. 7) System musi posiadać funkcjonalność asynchronicznej replikacji danych z wykorzystaniem protokołu TCP/IP celem dystrybucji treści i zapewnienia kopii danych w zdalnej lokalizacji. 8) System musi posiadać funkcjonalność wykonywania kopii migawkowych (ang. snapshot) oraz pozwalać stworzenie co najmniej 1000 kopii migawkowych dla danego katalogu w celu zapewnienia lokalnej ochrony danych. 9) System musi obsługiwać funkcjonalność realizacji kopii zapasowej (ang. backup) za pomocą protokołu NDMP. 10) System musi posiadać wbudowaną funkcjonalność definiowania limitów ilości danych (tzw. quoty) dla wybranych katalogów, użytkowników oraz grup użytkowników. 11) System musi posiadać mechanizm dystrybucji połączeń pomiędzy węzłami (ang. load-balancing) bez potrzeby stosowania dodatkowej aplikacji na stacji klienckiej lub zewnętrznych urządzeń równoważących obciążenie. Load-balancing musi być dostępny i być wspierany zarówno dla protokołów plikowych, jak i dla obiektowych (S3 API). 12) Administracja systemem musi odbywać się poprzez interfejs graficzny dostępny przez przeglądarkę internetową (poprawna obsługa przez przeglądarki co najmniej Google Chrome i Mozilla

	Firefox) oraz wiersz poleceń (ang. Command Line Interface, CLI). Musi również istnieć możliwość zarządzania przy pomocy interfejsu programistycznego REST API. 13) Rozwiązanie musi udostępniać statystyki historyczne z wykorzystania systemu i zapewniać statystyki wykorzystania zasobów przez użytkowników oraz generowanie raportów graficznych, w tym raportów porównujących dostępne parametry systemu. 14) System musi posiadać funkcjonalność automatycznego „tiering-u", tzn. przesuwania danych w zależności od ich utylizacji pomiędzy warstwami dyskowymi (ang. tiers), w ramach jednego systemu plików i według polityk ustawionych przez administratora. Dostęp w trybie odczyt/zapis do danych musi być zachowany cały czas, również w trakcie operacji przenoszenia danych (ang. tiering), czy zmiany poziomu protekcji danych (np. z n+1 na n+2) (ang. re-striping). 15) System musi posiadać funkcjonalność monitorowania wydajności (obciążenie CPU lub interfejsów sieciowych, opóźnienia, ilość operacji na sekundę, wydajność per protokół itp.) oraz analityki systemu plików („capacity planning", zmiany na systemie plików). 16) System musi posiadać wbudowaną funkcjonalność audytu, która daje co najmniej możliwość precyzyjnego określenia użytkownika odpowiedzialnego za utworzenie, usunięcie czy nadpisanie danych oraz czas tej operacji. 17) Ze względu na wymóg niskiego czasu dostępu do danych obszaru szybkiego system musi implementować protokół NFS over RDMA. 18) System musi mieć mechanizm deduplikacji danych celem optymalizacji wykorzystania przestrzeni dyskowych. 19) Jeżeli do spełnienia któregokolwiek z wymagań zdefiniowanych powyżej wymagane jest dodatkowe oprogramowanie lub licencja - należy je dostarczyć wraz z zamawianym systemem w wersji bez ograniczeń czasowych na całą pojemność systemu.
Pozostałe wymagane funkcjonalności	1) Możliwość tworzenia lokalnych kopii migawkowych ręcznie lub automatycznie przy pomocy harmonogramu w którym definiuje się czas lub częstotliwość tworzenia kopii migawkowych oraz czas ich wygaśnięcia. Kopie migawkowe, których czas wygaśnięcia upłynął, powinny być automatycznie kasowane. Urządzenie powinno umożliwiać tworzenie kopii migawkowych z dokładnością do pojedynczego folderu. Mechanizm kopii migawkowych powinien się integrować z wykorzystywaną lub planowaną do wykorzystania w projekcie przez Zamawiającego usługą Microsoft Volume Shadowcopy, umożliwiając użytkownikowi końcowemu samodzielne odzyskanie danych (bez angażowania administratora systemu). 2) Rozwiązanie powinno umożliwiać tworzenie kopii migawkowych (ang. snapshot) również w trybie odczyt/zapis.

	3) System powinien posiadać funkcjonalność WORM i powinien pozwalać na tworzenie zasobów (folderów/udziałów plikowych) zarówno objętych politykami WORM, jak i zasobów nie objętych taką polityką. Na jednym urządzeniu powinna być możliwość zdefiniowania zasobów objętych różnymi politykami WORM jednocześnie (np. różnym czasem retencji). Dla zasobów objętych funkcjonalnością WORM powinna istnieć możliwość obejścia polityki WORM poprzez uprzywilejowane kasowanie danych przez uprawnionego do tego użytkownika (np. root, czy tzw. Security Officer). Dla zasobów objętych polityką WORM powinna istnieć możliwość przedłużenia czasu retencji na potrzeby np. dochodzenia (tzw. Litigation Hold). System powinna pozwalać na ręczne ustawianie flagi WORM, jak i na automatyczne nakładanie retencji (np. po określonym czasie od utworzenia pliku) bez dodatkowej akcji ze strony aplikacji. 4) Razem z rozwiązaniem należy dostarczyć platformę umożliwiającą zarządzanie danymi (indeksowanie, przeszukiwanie, czy opisywanie danych – dodawanie tzw. „tag-ów") i raportowanie bazujące m. in na ww. „tag-ach". 5) Polityki warstwowego składowania danych (ang. tiering) muszą umożliwiać elastyczne definiowanie kryteriów przenoszenia plików pomiędzy poszczególnymi tier-ami bazując m. in. na czasie utworzenia pliku (ctime), ostatnim czasie dostępu do pliku (atime), ostatnim czasie modyfikacji pliku (mtime), wielkości pliku, lokalizacji pliku (ścieżce), rozszerzeniu pliku i nazwie pliku. 6) Replikacja zdalna również musi być definiowalna na poziomie wybranego katalogu/udziału. System musi wspierać replikację dwukierunkową, jeden-do-wiele i wiele-do-jeden (na poziomie całego systemu). W celu zapewnienia dodatkowych punktów odzyskiwania danych (ang. Point-in-Time) musi istnieć możliwość automatycznego tworzenie kopii migawkowych na zdalnej macierzy po zakończeniu procesu replikacji. 7) Rozwiązanie musi mieć możliwość rozbudowy o funkcjonalność tworzenia kopii zapasowych danych na nim składowanych przy pomocy protokołu NDMP w trybie „2-way-NDMP" (bezpośrednio po sieci SAN). Zamawiający nie wymagana dostarczenia tej funkcjonalność w ramach tego postępowania. 8) Jeżeli system wymaga zewnętrznych komponentów zapewniających komunikację pomiędzy węzłami (np. w postaci przełączników), muszą one pochodzić od tego samego producenta co system i muszą być uwzględnione w ofercie. 9) Możliwość zabezpieczenia wybranych danych (np. poprzez ustawianie takiego parametru dla poszczególnych folderów) przed nieuprawnioną edycją lub skasowaniem za pomocą mechanizmu

	WORM. Polityki WORM powinny być replikowane do zdalnego systemu.

6. System szybkiej pamięci masowej o dostępie plikowym typu „B”

Zaoferowany system szybkiej pamięci masowej o dostępie plikowym musi spełniać wszystkie wymagania przedstawione w poniższej tabeli.

Parametr	Charakterystyka (wymagania minimalne)
Pojemność, wydajność i bezpieczeństwo systemu	1) Zaoferowany system pamięci masowej o dostępie plikowym (zwanym dalej systemem) musi być zbudowany w architekturze „scale-out” (skalowalnej horyzontalnie). 2) System musi być zbudowany w oparciu jednakowe węzły serwerowe (kontrolerowo-dyskowe) zwane dalej węzłami. 3) Rozwiązanie musi być zbudowane na dyskach SSD NVMe nie większych niż 3,84 TB. 4) Architektura systemu oraz zastosowane mechanizmy ochrony danych muszą zabezpieczać dane przed ich utratą w przypadku awarii co najmniej 2 (dwóch) dowolnych dysków jednocześnie lub jednego węzła (kontrolera). 5) Wymagane mechanizmy ochrony przed awarią dysku to RAID lub kodowanie nadmiarowe (ECC). W przypadku mechanizmu RAID, ze względu na dłuższy czas odbudowy, macierz powinna być odporna na jednoczesną awarię co najmniej 3 (trzech) dowolnych dysków (należy uwzględnić w konfiguracji pojemności przestrzeni użytecznej). 6) Rozwiązanie musi umożliwiać ochronę danych przy pomocy wielokrotnego zapisu (ang. mirroring). 7) Musi istnieć możliwość zmiany protekcji danych przy zachowaniu nieprzerwanej dostępności zasobów, również pomiędzy trybem ECC i mirroring, w tym również dla plików w obrębie tego samego folderu, bez konieczności ich przenoszenia na inny zasób. 8) W przypadku awarii dysku czas odbudowy nie może być dłuższy niż 60 godzin (w sytuacji braku obciążenia przez urządzenia klienckie). 9) System musi udostępniać całą dostępną przestrzeń w ramach jednego ciągłego systemu plików, który musi być skalowalny do co najmniej 800 TiB powierzchni użytkowej. 10) System musi umożliwiać rozbudowę do co najmniej 200 węzłów w ramach tego samego systemu dyskowego, prezentujących do klientów jeden system plików. 11) System nie może posiadać pojedynczego punktu awarii, tzn. wszystkie jego elementy muszą być redundantne, a jego architektura musi zapewniać odporność na awarię w obrębie poszczególnych grup elementów, przynajmniej w zakresie: f) dysków g) interfejsów sieciowych h) kontrolerów (węzłów) i) zasilaczy

	j) wentylatorów. 12) Dostarczony system musi zapewnić pojemność użyteczną minimum 55 TiB. Pojemność użyteczną 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. 13) System musi zapewniać wydajność: a) wydajność nie mniejsza niż 1200 MB/s (megabajtów na sekundę) w przypadku losowych odczytów protokołem NFS v.3 (RFC 1813) dla bloku o wielkości 8KB i nie więcej niż 60 jednoczesnych wątków (ang. threads) na węzeł, b) wydajność nie mniejszą niż 103 tys. file OPS (operacji plikowych na sekundę) w teście SPEC SFS 2014 dla obciążenia zdefiniowanego jako SWBUILD przy zachowaniu średnich opóźnień nie większych niż 9ms. Oferent musi przedstawić wyniki testu potwierdzające spełnienie tego warunku, potwierdzone przez producenta sprzętu. 14) System musi być zbudowany z co najmniej 3 jednakowych węzłów (kontrolerów), gdzie każdy realizuje dostęp plikowy do danych i zapewnia wysoką wydajność dostępu do zgromadzonych plików w systemie.
Sprzęt	1) W celu maksymalizacji gęstości, tj. minimalizacji wykorzystania obszaru serwerowni do przechowywania danych, pojedynczy węzeł nie może zajmować więcej niż 1 RU w szafie. 2) System musi być dostarczony wraz z kompletem wszystkich niezbędnych elementów potrzebnych do połączenia poszczególnych węzłów w jeden system, zarządzany z jednego interfejsu administracyjnego. 3) Każdy węzeł musi być wyposażony w 2 procesory klasy x86-64, z których każdy posiada minimum 10 rdzeni. 4) Ze względu na przewidywane obciążenie i wymaganą wydajność nie dopuszcza się realizacji pamięci podręcznej (ang. cache) w oparciu o dyski SSD. 5) Każdy z elementów systemu musi być wyposażony w redundantne zasilacze zapewniające odporność na awarię pojedynczego źródła zasilania. 6) Każdy węzeł musi być wyposażony w 2 karty sieciowe Ethernet, każda z nich musi posiadać 2 porty 100 Gb/s Ethernet QSFP28. Interfejsy z jednej karty muszą być przeznaczone na potrzeby wewnętrznej komunikacji węzłów (interfejsy typu „back-end"). Interfejsy drugiej karty muszą być przeznaczone do zapewniania dostęp do danych (interfejsy typu „front-end").

	7) System musi zapewniać dostęp do danych przy jednoczesnym wykorzystaniu wszystkich interfejsów typu „front-end”. 8) Komunikacja pomiędzy węzłami („back-end”) musi: a) odbywać się za pośrednictwem osobnych i dedykowanych tylko do tego celu interfejsów (niewspółdzielonych z portami dostępowymi – „front-end”), b) odbywać się za pośrednictwem dedykowanych i przeznaczonych tylko do tego celu przełączników sieciowych (niewspółdzielonych z przełącznikami obsługującymi dostęp do danych – „front-end”), c) być zrealizowana w sposób redundantny, zapewniający prawidłową pracę systemu w przypadku awarii dowolnego przełącznika sieciowego obsługującego komunikację pomiędzy węzłami („back-end”). Wszystkie niezbędne elementy zapewniające tą komunikację (tj. przełączniki sieciowe, okablowanie, inne) muszą być dostarczone wraz z systemem i nie podlegają szczegółowej specyfikacji przez Zamawiającego. Zmawiający dopuszcza możliwość realizacji tych połączeń przy użyciu kabli typy „DAC” (ang. Direct Attach Cable). 9) Dostarczony system musi umożliwiać rozbudowę do min. 30 węzłów bez konieczności rozbudowy o dodatkowe przełączniki sieciowe dla połączeń wewnętrznych („back-end”) pomiędzy węzłami. 10) System musi zapewnić gwarantowaną ochronę przed tzw. „cichym uszkodzeniem danych" (ang. silent data corruption) dla wszystkich technologii dyskowych. 11) System musi umożliwiać wymianę uszkodzonego dysku przy zachowaniu nieprzerwanej dostępności wszystkich zasobów, tj. bez czasowego wyłączania z użycia dowolnego z elementów urządzenia. Musi posiadać zaimplementowany system jednoznacznego określenia lokalizacji uszkodzonego dysku, np. za pomocą lampki kontrolnej przy uszkodzonym dysku. 12) System musi zapewniać pracę jednocześnie wszystkich węzłów w trybie aktywny/aktywny w celu zapewnienia niezawodności i dostępności danych (tzn. każdy kontroler powinien umożliwiać dostęp do wszystkich danych oraz prezentować spójny widok systemu plików).
Pamięć RAM	1) System musi zapewniać dostępną, łączną pojemność pamięci RAM nie mniejszą niż 1536 GB (tzn. min. 384 GB dla pojedynczego węzła).
Funkcjonalność	1) System musi umożliwiać dynamiczne rozszerzanie i zmniejszanie udostępnianych systemów plików bez konieczności: c) modyfikacji już zainstalowanych węzłów, d) ręcznej migracji/dystrybucji danych na nowe dyski systemu. 2) System musi zapewniać dostęp z rożnych systemów operacyjnych (posiadanych i wykorzystywanych lub planowanych do wykorzystania w projekcie przez Zamawiającego: UNIX, macOS,

	Linux, Windows) z wykorzystaniem standardowych protokołów. Wymagana jest poprawna obsługa co najmniej: NFS v3 i v4, SMB (CIFS) v2 i v3, FTP, HTTP i S3 API. 3) System musi wspierać natywnie Hadoop Distributed File System (HDFS). 4) Jednoczesny dostęp do tych samych danych musi być możliwy przy wykorzystaniu wszystkich protokołów wymienionych powyżej. System musi również umożliwiać zarządzanie uprawnieniami użytkowników w dostępie wieloprotokołowym. 5) System musi zapewnić obsługę alertów i umożliwiać monitorowanie za pomocą protokołu SNMP (w wersji min. 2c). 6) System musi zapewnić zdalny monitoring w celu diagnozy i usuwania usterek oraz w zakresie konserwacji – musi mieć możliwość automatycznej diagnozy i samodzielnego zgłaszania usterek w centrum serwisowym producenta. 7) System musi posiadać funkcjonalność asynchronicznej replikacji danych z wykorzystaniem protokołu TCP/IP celem dystrybucji treści i zapewnienia kopii danych w zdalnej lokalizacji. 8) System musi posiadać funkcjonalność wykonywania kopii migawkowych (ang. snapshot) oraz pozwalać stworzenie co najmniej 1000 kopii migawkowych dla danego katalogu w celu zapewnienia lokalnej ochrony danych. 9) System musi obsługiwać funkcjonalność realizacji kopii zapasowej (ang. backup) za pomocą protokołu NDMP. 10) System musi posiadać wbudowaną funkcjonalność definiowania limitów ilości danych (tzw. quoty) dla wybranych katalogów, użytkowników oraz grup użytkowników. 11) System musi posiadać mechanizm dystrybucji połączeń pomiędzy węzłami (ang. load-balancing) bez potrzeby stosowania dodatkowej aplikacji na stacji klienckiej lub zewnętrznych urządzeń równoważących obciążenie. Load-balancing musi być dostępny i być wspierany zarówno dla protokołów plikowych, jak i dla obiektowych (S3 API). 12) Administracja systemem musi odbywać się poprzez interfejs graficzny dostępny przez przeglądarkę internetową (poprawna obsługa przez przeglądarki co najmniej Google Chrome i Mozilla Firefox) oraz wiersz poleceń (ang. Command Line Interface, CLI). Musi również istnieć możliwość zarządzania przy pomocy interfejsu programistycznego REST API. 13) Rozwiązanie musi udostępniać statystyki historyczne z wykorzystania systemu i zapewniać statystyki wykorzystania zasobów przez użytkowników oraz generowanie raportów graficznych, w tym raportów porównujących dostępne parametry systemu.

	14) System musi posiadać funkcjonalność automatycznego „tiering-u", tzn. przesuwania danych w zależności od ich utylizacji pomiędzy warstwami dyskowymi (ang. tiers), w ramach jednego systemu plików i według polityk ustawionych przez administratora. Dostęp w trybie odczyt/zapis do danych musi być zachowany cały czas, również w trakcie operacji przenoszenia danych (ang. tiering), czy zmiany poziomu protekcji danych (np. z n+1 na n+2) (ang. re-striping). 15) System musi posiadać funkcjonalność monitorowania wydajności (obciążenie CPU lub interfejsów sieciowych, opóźnienia, ilość operacji na sekundę, wydajność per protokół itp.) oraz analityki systemu plików („capacity planning", zmiany na systemie plików). 16) System musi posiadać wbudowaną funkcjonalność audytu, która daje co najmniej możliwość precyzyjnego określenia użytkownika odpowiedzialnego za utworzenie, usunięcie czy nadpisanie danych oraz czas tej operacji. 17) Ze względu na wymóg niskiego czasu dostępu do danych obszaru szybkiego system musi implementować protokół NFS over RDMA. 18) System musi mieć mechanizm deduplikacji danych celem optymalizacji wykorzystania przestrzeni dyskowych. 19) Jeżeli do spełnienia któregokolwiek z wymagań zdefiniowanych powyżej wymagane jest dodatkowe oprogramowanie lub licencja - należy je dostarczyć wraz z zamawianym systemem w wersji bez ograniczeń czasowych na całą pojemność systemu.
Pozostałe wymagane funkcjonalności	1) Możliwość tworzenia lokalnych kopii migawkowych ręcznie lub automatycznie przy pomocy harmonogramu w którym definiuje się czas lub częstotliwość tworzenia kopii migawkowych oraz czas ich wygaśnięcia. Kopie migawkowe, których czas wygaśnięcia upłynął, powinny być automatycznie kasowane. Urządzenie powinno umożliwiać tworzenie kopii migawkowych z dokładnością do pojedynczego folderu. Mechanizm kopii migawkowych powinien się integrować z wykorzystywaną lub planowaną do wykorzystania w projekcie przez Zamawiającego usługą Microsoft Volume Shadowcopy, umożliwiając użytkownikowi końcowemu samodzielne odzyskanie danych (bez angażowania administratora systemu). 2) Rozwiązanie powinno umożliwiać tworzenie kopii migawkowych (ang. snapshot) również w trybie odczyt/zapis. 3) System powinien posiadać funkcjonalność WORM i powinien pozwalać na tworzenie zasobów (folderów/udziałów plikowych) zarówno objętych politykami WORM, jak i zasobów nie objętych taką polityką. Na jednym urządzeniu powinna być możliwość zdefiniowania zasobów objętych różnymi politykami WORM jednocześnie (np. różnym czasem retencji). Dla zasobów objętych funkcjonalnością WORM powinna istnieć możliwość obejścia polityki WORM poprzez uprzywilejowane kasowanie danych przez

	uprawnionego do tego użytkownika (np. root, czy tzw. Security Officer). Dla zasobów objętych polityką WORM powinna istnieć możliwość przedłużenia czasu retencji na potrzeby np. dochodzenia (tzw. Litigation Hold). System powinna pozwalać na ręczne ustawianie flagi WORM, jak i na automatyczne nakładanie retencji (np. po określonym czasie od utworzenia pliku) bez dodatkowej akcji ze strony aplikacji. 4) Razem z rozwiązaniem należy dostarczyć platformę umożliwiającą zarządzanie danymi (indeksowanie, przeszukiwanie, czy opisywanie danych – dodawanie tzw. „tag-ów") i raportowanie bazujące m. in na ww. „tag-ach". 5) Polityki warstwowego składowania danych (ang. tiering) muszą umożliwiać elastyczne definiowanie kryteriów przenoszenia plików pomiędzy poszczególnymi tier-ami bazując m. in. na czasie utworzenia pliku (ctime), ostatnim czasie dostępu do pliku (atime), ostatnim czasie modyfikacji pliku (mtime), wielkości pliku, lokalizacji pliku (ścieżce), rozszerzeniu pliku i nazwie pliku. 6) Replikacja zdalna również musi być definiowalna na poziomie wybranego katalogu/udziału. System musi wspierać replikację dwukierunkową, jeden-do-wiele i wiele-do-jeden (na poziomie całego systemu). W celu zapewnienia dodatkowych punktów odzyskiwania danych (ang. Point-in-Time) musi istnieć możliwość automatycznego tworzenie kopii migawkowych na zdalnej macierzy po zakończeniu procesu replikacji. 7) Rozwiązanie musi mieć możliwość rozbudowy o funkcjonalność tworzenia kopii zapasowych danych na nim składowanych przy pomocy protokołu NDMP w trybie „2-way-NDMP" (bezpośrednio po sieci SAN). Zamawiający nie wymaga dostarczenia tej funkcjonalność w ramach tego postępowania. 8) Jeżeli system wymaga zewnętrznych komponentów zapewniających komunikację pomiędzy węzłami (np. w postaci przełączników), muszą one pochodzić od tego samego producenta co system i muszą być uwzględnione w ofercie. 9) Możliwość zabezpieczenia wybranych danych (np. poprzez ustawianie takiego parametru dla poszczególnych folderów) przed nieuprawnioną edycją lub skasowaniem za pomocą mechanizmu WORM. Polityki WORM powinny być replikowane do zdalnego systemu.

7. System archiwalnej pamięci masowej o dostępie plikowym typu „A”

Zaoferowany system archiwalnej pamięci masowej o dostępie plikowym musi spełniać wszystkie wymagania przedstawione w poniższej tabeli.

Parametr	Charakterystyka (wymagania minimalne)
Pojemność, wydajność i bezpieczeństwo systemu	1) Zaoferowany system pamięci masowej o dostępie plikowym (zwanym dalej systemem) musi być zbudowany w architekturze „scale-out” (skalowalnej horyzontalnie). 2) System musi być zbudowany w oparciu jednakowe węzły serwerowe (kontrolerowo-dyskowe) zwane dalej węzłami. 3) Dostarczony system musi zapewnić pojemność użyteczną minimum 3000 TiB. Pojemność użyteczną 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. 4) Architektura systemu oraz zastosowane mechanizmy ochrony danych muszą zabezpieczać dane przed ich utratą w przypadku awarii co najmniej 3 (trzech) dowolnych dysków jednocześnie lub jednego węzła (kontrolera). 5) Wymagane mechanizmy ochrony przed awarią dysku to RAID lub kodowanie nadmiarowe (ECC). 6) Rozwiązanie musi umożliwiać ochronę danych przy pomocy wielokrotnego zapisu (ang. mirroring). 7) Musi istnieć możliwość zmiany protekcji danych przy zachowaniu nieprzerwanej dostępności zasobów, również pomiędzy trybem ECC i mirroring, w tym również dla plików w obrębie tego samego folderu, bez konieczności ich przenoszenia na inny zasób. 8) System musi udostępniać całą dostępną przestrzeń w ramach jednego ciągłego systemu plików, który musi być skalowalny do co najmniej 20 PiB powierzchni użytecznej. 9) System musi zapewniać wydajność: a) wydajność nie mniejsza niż 120 MB/s (megabajtów na sekundę) w przypadku losowych odczytów protokołem NFS v.3 (RFC 1813) dla bloku o wielkości 8KB i nie więcej niż 30 jednoczesnych wątków (ang. threads) na węzeł, b) wydajność nie mniejszą niż 350 tys. file OPS (operacji plikowych na sekundę) w teście SPEC SFS 2014 dla obciążenia zdefiniowanego jako SWBUILD przy zachowaniu średnich opóźnień nie większych niż 9ms. Oferent musi przedstawić wyniki testu potwierdzające spełnienie tego warunku, potwierdzone przez producenta sprzętu.

	10) System musi być zbudowany z 10 jednakowych węzłów (kontrolerów), gdzie każdy realizuje dostęp plikowy do danych i zapewnia wysoką wydajność dostępu do zgromadzonych plików w systemie. Dopuszcza się rozwiązanie, gdzie węzeł (kontroler) pełni jednocześnie rolę półki dyskowej. 11) System musi umożliwiać rozbudowę do co najmniej 200 węzłów w ramach tego samego systemu dyskowego, prezentujących do klientów jeden system plików. 12) System nie może posiadać pojedynczego punktu awarii, tzn. wszystkie jego elementy muszą być redundantne, a jego architektura musi zapewniać odporność na awarię w obrębie poszczególnych grup elementów, przynajmniej w zakresie: a) dysków b) interfejsów sieciowych c) kontrolerów (węzłów) d) zasilaczy e) wentylatorów.
Sprzęt	1) W celu maksymalizacji gęstości, tj. minimalizacji wykorzystania obszaru serwerowni do przechowywania danych, pojedynczy węzeł nie może zajmować więcej niż 1 RU w szafie. 2) System musi być dostarczony wraz z kompletem wszystkich niezbędnych elementów potrzebnych do połączenia poszczególnych węzłów w jeden system, zarządzany z jednego interfejsu administracyjnego. 3) Każdy węzeł musi być wyposażony w co najmniej 1 procesor klasy x86-64, z których każdy posiada minimum 16 rdzeni. 4) System musi zapewniać dostępną, łączną pojemność pamięci RAM nie mniejszą niż 3840 GB (tzn. min. 384 GB dla pojedynczego węzła). 5) Ze względu na przewidywane obciążenie i wymaganą wydajność nie dopuszcza się realizacji pamięci podręcznej (ang. cache) w oparciu o dyski SSD. 6) Każdy z elementów systemu musi być wyposażony w redundantne zasilacze zapewniające odporność na awarię pojedynczego źródła zasilania. 7) Każdy węzeł musi być wyposażony w 2 karty sieciowe Ethernet: a) jedna dwu-portowa karta 100 Gb/s Ethernet QSFP28 na potrzeby wewnętrznej komunikacji węzłów (interfejsy typu „back-end”) b) jedna dwu-portowa karta 100 Gb/s Ethernet QSFP28 przeznaczone do zapewniania dostęp do danych (interfejsy typu „front-end”). 8) Każdy węzeł musi być wyposażony w: a) co najmniej 20 jednakowych dysków typu NLSAS lub SATA o pojemności co najmniej 20 TB każdy przeznaczonych do przechowywania danych

	b) co najmniej 2 jednakowe dyski SSD o pojemności minimum 7.68 TB każdy do buforowania metadanych i samych danych (ang. cache). 9) System musi zapewniać dostęp do danych przy jednoczesnym wykorzystaniu wszystkich interfejsów typu „front-end". 10) Komunikacja pomiędzy węzłami („back-end") musi: a) odbywać się za pośrednictwem osobnych i dedykowanych tylko do tego celu interfejsów (niewspółdzielonych z portami dostępowymi – „front-end"), b) odbywać się za pośrednictwem dedykowanych i przeznaczonych tylko do tego celu przełączników sieciowych (niewspółdzielonych z przełącznikami obsługującymi dostęp do danych – „front-end"), c) być zrealizowana w sposób redundantny, zapewniający prawidłową pracę systemu w przypadku awarii dowolnego przełącznika sieciowego obsługującego komunikację pomiędzy węzłami („back-end"). Wszystkie niezbędne elementy zapewniające tą komunikację (tj. przełączniki sieciowe, okablowanie, inne) muszą być dostarczone wraz z systemem i nie podlegają szczegółowej specyfikacji przez Zamawiającego. Zmawiający dopuszcza możliwość realizacji tych połączeń przy użyciu kabli typy „DAC" (ang. Direct Attach Cable). 11) System musi zapewnić gwarantowaną ochronę przed tzw. „cichym uszkodzeniem danych" (ang. silent data corruption) dla wszystkich technologii dyskowych. 12) System musi umożliwiać wymianę uszkodzonego dysku przy zachowaniu nieprzerwanej dostępności wszystkich zasobów, tj. bez czasowego wyłączania z użycia dowolnego z elementów urządzenia. Musi posiadać zaimplementowany system jednoznacznego określenia lokalizacji uszkodzonego dysku, np. za pomocą lampki kontrolnej przy uszkodzonym dysku. 13) System musi zapewniać pracę jednocześnie wszystkich węzłów w trybie aktywny/aktywny w celu zapewnienia niezawodności i dostępności danych (tzn. każdy kontroler powinien umożliwiać dostęp do wszystkich danych oraz prezentować spójny widok systemu plików).
Funkcjonalność	1) System musi umożliwiać dynamiczne rozszerzanie i zmniejszanie udostępnianych systemów plików bez konieczności: a) modyfikacji już zainstalowanych węzłów, b) ręcznej migracji/dystrybucji danych na nowe dyski systemu. 2) System musi zapewniać dostęp z rożnych systemów operacyjnych (posiadanych i wykorzystywanych lub planowanych do wykorzystania w projekcie przez Zamawiającego: UNIX, macOS, Linux, Windows) z wykorzystaniem standardowych protokołów. Wymagana jest poprawna obsługa co najmniej: NFS v3 i v4, SMB (CIFS) v2 i v3, FTP, HTTP i S3 API.

	3) System musi wspierać natywnie Hadoop Distributed File System (HDFS). 4) Jednoczesny dostęp do tych samych danych musi być możliwy przy wykorzystaniu wszystkich protokołów wymienionych powyżej. System musi również umożliwiać zarządzanie uprawnieniami użytkowników w dostępie wieloprotokołowym. 5) System musi zapewnić obsługę alertów i umożliwiać monitorowanie za pomocą protokołu SNMP (w wersji min. 2c). 6) System musi zapewnić zdalny monitoring w celu diagnozy i usuwania usterek oraz w zakresie konserwacji – musi mieć możliwość automatycznej diagnozy i samodzielnego zgłaszania usterek w centrum serwisowym producenta. 7) System musi posiadać funkcjonalność asynchronicznej replikacji danych z wykorzystaniem protokołu TCP/IP celem dystrybucji treści i zapewnienia kopii danych w zdalnej lokalizacji. 8) System musi posiadać funkcjonalność wykonywania kopii migawkowych (ang. snapshot) oraz pozwalać stworzenie co najmniej 1000 kopii migawkowych dla danego katalogu w celu zapewnienia lokalnej ochrony danych. 9) System musi obsługiwać funkcjonalność realizacji kopii zapasowej (ang. backup) za pomocą protokołu NDMP. 10) System musi posiadać wbudowaną funkcjonalność definiowania limitów ilości danych (tzw. quoty) dla wybranych katalogów, użytkowników oraz grup użytkowników. 11) System musi posiadać mechanizm dystrybucji połączeń pomiędzy węzłami (ang. load-balancing) bez potrzeby stosowania dodatkowej aplikacji na stacji klienckiej lub zewnętrznych urządzeń równoważących obciążenie. Load-balancing musi być dostępny i być wspierany zarówno dla protokołów plikowych, jak i dla obiektowych (S3 API). 12) Administracja systemem musi odbywać się poprzez interfejs graficzny dostępny przez przeglądarkę internetową (poprawna obsługa przez przeglądarki co najmniej Google Chrome i Mozilla Firefox) oraz wiersz poleceń (ang. Command Line Interface, CLI). Musi również istnieć możliwość zarządzania przy pomocy interfejsu programistycznego REST API. 13) Rozwiązanie musi udostępniać statystyki historyczne z wykorzystania systemu i zapewniać statystyki wykorzystania zasobów przez użytkowników oraz generowanie raportów graficznych, w tym raportów porównujących dostępne parametry systemu. 14) System musi posiadać funkcjonalność automatycznego „tiering-u”, tzn. przesuwania danych w zależności od ich utylizacji pomiędzy warstwami dyskowymi (ang. tiers), w ramach jednego systemu plików i według polityk ustawionych przez administratora. Dostęp w

	trybie odczyt/zapis do danych musi być zachowany cały czas, również w trakcie operacji przenoszenia danych (ang. tiering), czy zmiany poziomu protekcji danych (np. z n+1 na n+2) (ang. re-striping). 15) System musi posiadać funkcjonalność monitorowania wydajności (obciążenie CPU lub interfejsów sieciowych, opóźnienia, ilość operacji na sekundę, wydajność per protokół itp.) oraz analityki systemu plików („capacity planning", zmiany na systemie plików). 16) System musi posiadać wbudowaną funkcjonalność audytu, która daje co najmniej możliwość precyzyjnego określenia użytkownika odpowiedzialnego za utworzenie, usunięcie czy nadpisanie danych oraz czas tej operacji. 17) Ze względu na wymóg niskiego czasu dostępu do danych obszaru szybkiego system musi implementować protokół NFS over RDMA. 18) System musi mieć mechanizm deduplikacji danych celem optymalizacji wykorzystania przestrzeni dyskowych. 19) Jeżeli do spełnienia któregokolwiek z wymagań zdefiniowanych powyżej wymagane jest dodatkowe oprogramowanie lub licencja - należy je dostarczyć wraz z zamawianym systemem w wersji bez ograniczeń czasowych na całą pojemność systemu.
Dodatkowe funkcjonalności	1) Możliwość tworzenia lokalnych kopii migawkowych ręcznie lub automatycznie przy pomocy harmonogramu w którym definiuje się czas lub częstotliwość tworzenia kopii migawkowych oraz czas ich wygaśnięcia. Kopie migawkowe, których czas wygaśnięcia upłynął, powinny być automatycznie kasowane. Urządzenie powinno umożliwiać tworzenie kopii migawkowych z dokładnością do pojedynczego folderu. Mechanizm kopii migawkowych powinien się integrować z wykorzystywaną lub planowaną do wykorzystania w projekcie przez Zamawiającego usługą Microsoft Volume Shadowcopy, umożliwiając użytkownikowi końcowemu samodzielne odzyskanie danych (bez angażowania administratora systemu). 2) Rozwiązanie powinno umożliwiać tworzenie kopii migawkowych (ang. snapshot) również w trybie odczyt/zapis. 3) System powinien posiadać funkcjonalność WORM i powinien pozwalać na tworzenie zasobów (folderów/udziałów plikowych) zarówno objętych politykami WORM, jak i zasobów nie objętych taką polityką. Na jednym urządzeniu powinna być możliwość zdefiniowania zasobów objętych różnymi politykami WORM jednocześnie (np. różnym czasem retencji). Dla zasobów objętych funkcjonalnością WORM powinna istnieć możliwość obejścia polityki WORM poprzez uprzywilejowane kasowanie danych przez uprawnionego do tego użytkownika (np. root, czy tzw. Security Officer). Dla zasobów objętych polityką WORM powinna istnieć możliwość przedłużenia czasu retencji na potrzeby np. dochodzenia (tzw. Litigation Hold). System powinna pozwalać na ręczne

	ustawianie flagi WORM, jak i na automatyczne nakładanie retencji (np. po określonym czasie od utworzenia pliku) bez dodatkowej akcji ze strony aplikacji. 4) Razem z rozwiązaniem należy dostarczyć platformę umożliwiającą zarządzanie danymi (indeksowanie, przeszukiwanie, czy opisywanie danych – dodawanie tzw. „tag-ów") i raportowanie bazujące m. in na ww. „tag-ach". 5) Polityki warstwowego składowania danych (ang. tiering) muszą umożliwiać elastyczne definiowanie kryteriów przenoszenia plików pomiędzy poszczególnymi tier-ami bazując m. in. na czasie utworzenia pliku (ctime), ostatnim czasie dostępu do pliku (atime), ostatnim czasie modyfikacji pliku (mtime), wielkości pliku, lokalizacji pliku (ścieżce), rozszerzeniu pliku i nazwie pliku. 6) Replikacja zdalna również musi być definiowalna na poziomie wybranego katalogu/udziału. System musi wspierać replikację dwukierunkową, jeden-do-wiele i wiele-do-jeden (na poziomie całego systemu). W celu zapewnienia dodatkowych punktów odzyskiwania danych (ang. Point-in-Time) musi istnieć możliwość automatycznego tworzenie kopii migawkowych na zdalnej macierzy po zakończeniu procesu replikacji. 7) Rozwiązanie musi mieć możliwość rozbudowy o funkcjonalność tworzenia kopii zapasowych danych na nim składowanych przy pomocy protokołu NDMP w trybie „2-way-NDMP" (bezpośrednio po sieci SAN). Zamawiający nie wymagana dostarczenia tej funkcjonalność w ramach tego postępowania. 8) Jeżeli system wymaga zewnętrznych komponentów zapewniających komunikację pomiędzy węzłami (np. w postaci przełączników), muszą one pochodzić od tego samego producenta co system i muszą być uwzględnione w ofercie. 9) Możliwość zabezpieczenia wybranych danych (np. poprzez ustawianie takiego parametru dla poszczególnych folderów) przed nieuprawnioną edycją lub skasowaniem za pomocą mechanizmu WORM. Polityki WORM powinny być replikowane do zdalnego systemu.
Dodatkowe wyposażenie „cold spare"	System musi zostać dostarczony z dodatkową przestrzenią typu „cold spare" składającą się z co najmniej 20 dysków o poniższych parametrach każdy: 1) pojemność co najmniej 20TB; 2) format dysku 3,5"; 3) pojemność pamięci podręcznej (cache) co najmniej 256 MB; 4) musi być przystosowane do pracy ciągłej przez cały rok (24x7x365); 5) prędkość obrotowa (RPM) min. 7200 obr./min; 6) interfejs SATA III (6 Gb/s); 7) prędkość odczytu/zapisu: a) maks. ciągła szybkość transmisji min. 285 MB/sec,

	b) Random Read Speed (4KB, QD16) min. 168 IOPS, c) Random Write Speed (4KB, QD16) min. 550 IOPS; 8) obsługa trybu Hot-Plug; 9) obsługa technologii S.M.A.R.T.; 10) wbudowane funkcje optymalizujące poziom zużycia energii podczas pracy u w trybie spoczynku; 11) wykonanie w technologii CMR (ang. Conventional Magnetic Recording); 12) posiadanie MTFB (niezawodność) – co najmniej 2500000 godzin; 13) posiadanie średniego opóźnienia (ang. latency) – nie więcej niż 4.16 ms; 14) pobór mocy maksymalny podczas pracy – nie więcej niż 10W; 15) poprawna praca w zakresie temperatur 5-60 st. C.

8. System archiwalnej pamięci masowej o dostępie plikowym typu „B”

Zaoferowany system archiwalnej pamięci masowej o dostępie plikowym musi spełniać wszystkie wymagania przedstawione w poniższej tabeli.

Parametr	Charakterystyka (wymagania minimalne)
Pojemność, wydajność i bezpieczeństwo systemu	1) Zaoferowany system pamięci masowej o dostępie plikowym (zwanym dalej systemem) musi być zbudowany w architekturze „scale-out” (skalowalnej horyzontalnie). 2) System musi być zbudowany w oparciu jednakowe węzły serwerowe (kontrolerowo-dyskowe) zwane dalej węzłami. 3) Dostarczony system musi zapewnić pojemność użyteczną minimum 640 TiB. Pojemność użyteczną 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. 4) Architektura systemu oraz zastosowane mechanizmy ochrony danych muszą zabezpieczać dane przed ich utratą w przypadku awarii co najmniej 2 (dwóch) dowolnych dysków jednocześnie lub jednego węzła (kontrolera). 5) Wymagane mechanizmy ochrony przed awarią dysku to RAID lub kodowanie nadmiarowe (ECC). W przypadku mechanizmu RAID, ze względu na dłuższy czas odbudowy, macierz powinna być odporna na jednoczesną awarię co najmniej 3 (trzech) dowolnych dysków (należy uwzględnić w konfiguracji pojemności przestrzeni użytecznej). 6) Rozwiązanie musi umożliwiać ochronę danych przy pomocy wielokrotnego zapisu (ang. mirroring). 7) Musi istnieć możliwość zmiany protekcji danych przy zachowaniu nieprzerwanej dostępności zasobów, również pomiędzy trybem ECC i mirroring, w tym również dla plików w obrębie tego samego folderu, bez konieczności ich przenoszenia na inny zasób. 8) System musi udostępniać całą dostępną przestrzeń w ramach jednego ciągłego systemu plików, który musi być skalowalny do co najmniej 20 PiB powierzchni użytecznej. 9) System musi zapewniać wydajność: a) wydajność nie mniejsza niż 58 MB/s (megabajtów na sekundę) w przypadku losowych odczytów protokołem NFS v.3 (RFC 1813) dla bloku o wielkości 8KB i nie więcej niż 30 jednoczesnych wątków (ang. threads) na węzeł, b) wydajność nie mniejszą niż 180 tys. file OPS (operacji plikowych na sekundę) w teście SPEC SFS 2014 dla obciążenia

	zdefiniowanego jako SWBUILD przy zachowaniu średnich opóźnień nie większych niż 9ms. Oferent musi przedstawić wyniki testu potwierdzające spełnienie tego warunku, potwierdzone przez producenta sprzętu. 10) System musi być zbudowany z 4 jednakowych węzłów (kontrolerów), gdzie każdy realizuje dostęp plikowy do danych i zapewnia wysoką wydajność dostępu do zgromadzonych plików w systemie. Dopuszcza się rozwiązanie, gdzie węzeł (kontroler) pełni jednocześnie rolę półki dyskowej. 11) System musi umożliwiać rozbudowę do co najmniej 200 węzłów w ramach tego samego systemu dyskowego, prezentujących do klientów jeden system plików. 12) System nie może posiadać pojedynczego punktu awarii, tzn. wszystkie jego elementy muszą być redundantne, a jego architektura musi zapewniać odporność na awarię w obrębie poszczególnych grup elementów, przynajmniej w zakresie: a) dysków b) interfejsów sieciowych c) kontrolerów (węzłów) d) zasilaczy e) wentylatorów.
Sprzęt	1) W celu maksymalizacji gęstości, tj. minimalizacji wykorzystania obszaru serwerowni do przechowywania danych, pojedynczy węzeł nie może zajmować więcej niż 1 RU w szafie. 2) System musi być dostarczony wraz z kompletem wszystkich niezbędnych elementów potrzebnych do połączenia poszczególnych węzłów w jeden system, zarządzany z jednego interfejsu administracyjnego. 3) Każdy węzeł musi być wyposażony w co najmniej 1 procesor klasy x86-64, z których każdy posiada minimum 16 rdzeni. 4) System musi zapewniać dostępną, łączną pojemność pamięci RAM nie mniejszą niż 1536 GB (tzn. min. 384 GB dla pojedynczego węzła). 5) Ze względu na przewidywane obciążenie i wymaganą wydajność nie dopuszcza się realizacji pamięci podręcznej (ang. cache) w oparciu o dyski SSD. 6) Każdy z elementów systemu musi być wyposażony w redundantne zasilacze zapewniające odporność na awarię pojedynczego źródła zasilania. 7) Każdy węzeł musi być wyposażony w 2 karty sieciowe Ethernet: a) jedna dwu-portowa karta 100 Gb/s Ethernet QSFP28 na potrzeby wewnętrznej komunikacji węzłów (interfejsy typu „back-end") b) jedna dwu-portowa karta 100 Gb/s Ethernet QSFP28 przeznaczone do zapewniania dostęp do danych (interfejsy typu „front-end").

	8) Każdy węzeł musi być wyposażony w: a) co najmniej 20 jednakowych dysków typu NLSAS lub SATA o pojemności co najmniej 12 TB każdy przeznaczonych do przechowywania danych b) co najmniej 2 jednakowe dyski SSD o pojemności minimum 3.2 TB każdy do buforowania metadanych i samych danych (ang. cache). 9) System musi zapewniać dostęp do danych przy jednoczesnym wykorzystaniu wszystkich interfejsów typu „front-end". 10) Komunikacja pomiędzy węzłami („back-end") musi: a) odbywać się za pośrednictwem osobnych i dedykowanych tylko do tego celu interfejsów (niewspółdzielonych z portami dostępowymi – „front-end"), b) odbywać się za pośrednictwem dedykowanych i przeznaczonych tylko do tego celu przełączników sieciowych (niewspółdzielonych z przełącznikami obsługującymi dostęp do danych – „front-end"), c) być zrealizowana w sposób redundantny, zapewniający prawidłową pracę systemu w przypadku awarii dowolnego przełącznika sieciowego obsługującego komunikację pomiędzy węzłami („back-end"). Wszystkie niezbędne elementy zapewniające tą komunikację (tj. przełączniki sieciowe, okablowanie, inne) muszą być dostarczone wraz z systemem i nie podlegają szczegółowej specyfikacji przez Zamawiającego. Zmawiający dopuszcza możliwość realizacji tych połączeń przy użyciu kabli typy „DAC" (ang. Direct Attach Cable). 11) System musi zapewnić gwarantowaną ochronę przed tzw. „cichym uszkodzeniem danych" (ang. silent data corruption) dla wszystkich technologii dyskowych. 12) System musi umożliwiać wymianę uszkodzonego dysku przy zachowaniu nieprzerwanej dostępności wszystkich zasobów, tj. bez czasowego wyłączania z użycia dowolnego z elementów urządzenia. Musi posiadać zaimplementowany system jednoznacznego określenia lokalizacji uszkodzonego dysku, np. za pomocą lampki kontrolnej przy uszkodzonym dysku. 13) System musi zapewniać pracę jednocześnie wszystkich węzłów w trybie aktywny/aktywny w celu zapewnienia niezawodności i dostępności danych (tzn. każdy kontroler powinien umożliwiać dostęp do wszystkich danych oraz prezentować spójny widok systemu plików).
Funkcjonalność	1) System musi umożliwiać dynamiczne rozszerzanie i zmniejszanie udostępnianych systemów plików bez konieczności: a) modyfikacji już zainstalowanych węzłów, b) ręcznej migracji/dystrybucji danych na nowe dyski systemu. 2) System musi zapewniać dostęp z rożnych systemów operacyjnych posiadanych i wykorzystywanych lub planowanych do wykorzystania

	w projekcie przez Zamawiającego: UNIX, macOS, Linux, Windows) z wykorzystaniem standardowych protokołów. Wymagana jest poprawna obsługa co najmniej: NFS v3 i v4, SMB (CIFS) v2 i v3, FTP, HTTP i S3 API. 3) System musi wspierać natywnie Hadoop Distributed File System (HDFS). 4) Jednoczesny dostęp do tych samych danych musi być możliwy przy wykorzystaniu wszystkich protokołów wymienionych powyżej. System musi również umożliwiać zarządzanie uprawnieniami użytkowników w dostępie wieloprotokołowym. 5) System musi zapewnić obsługę alertów i umożliwiać monitorowanie za pomocą protokołu SNMP (w wersji min. 2c). 6) System musi zapewnić zdalny monitoring w celu diagnozy i usuwania usterek oraz w zakresie konserwacji – musi mieć możliwość automatycznej diagnozy i samodzielnego zgłaszania usterek w centrum serwisowym producenta. 7) System musi posiadać funkcjonalność asynchronicznej replikacji danych z wykorzystaniem protokołu TCP/IP celem dystrybucji treści i zapewnienia kopii danych w zdalnej lokalizacji. 8) System musi posiadać funkcjonalność wykonywania kopii migawkowych (ang. snapshot) oraz pozwalać stworzenie co najmniej 1000 kopii migawkowych dla danego katalogu w celu zapewnienia lokalnej ochrony danych. 9) System musi obsługiwać funkcjonalność realizacji kopii zapasowej (ang. backup) za pomocą protokołu NDMP. 10) System musi posiadać wbudowaną funkcjonalność definiowania limitów ilości danych (tzw. quoty) dla wybranych katalogów, użytkowników oraz grup użytkowników. 11) System musi posiadać mechanizm dystrybucji połączeń pomiędzy węzłami (ang. load-balancing) bez potrzeby stosowania dodatkowej aplikacji na stacji klienckiej lub zewnętrznych urządzeń równoważących obciążenie. Load-balancing musi być dostępny i być wspierany zarówno dla protokołów plikowych, jak i dla obiektowych (S3 API). 12) Administracja systemem musi odbywać się poprzez interfejs graficzny dostępny przez przeglądarkę internetową (poprawna obsługa przez przeglądarki co najmniej Google Chrome i Mozilla Firefox) oraz wiersz poleceń (ang. Command Line Interface, CLI). Musi również istnieć możliwość zarządzania przy pomocy interfejsu programistycznego REST API. 13) Rozwiązanie musi udostępniać statystyki historyczne z wykorzystania systemu i zapewniać statystyki wykorzystania zasobów przez użytkowników oraz generowanie raportów graficznych, w tym raportów porównujących dostępne parametry systemu.

	14) System musi posiadać funkcjonalność automatycznego „tiering-u", tzn. przesuwania danych w zależności od ich utylizacji pomiędzy warstwami dyskowymi (ang. tiers), w ramach jednego systemu plików i według polityk ustawionych przez administratora. Dostęp w trybie odczyt/zapis do danych musi być zachowany cały czas, również w trakcie operacji przenoszenia danych (ang. tiering), czy zmiany poziomu protekcji danych (np. z n+1 na n+2) (ang. re-striping). 15) System musi posiadać funkcjonalność monitorowania wydajności (obciążenie CPU lub interfejsów sieciowych, opóźnienia, ilość operacji na sekundę, wydajność per protokół itp.) oraz analityki systemu plików („capacity planning", zmiany na systemie plików). 16) System musi posiadać wbudowaną funkcjonalność audytu, która daje co najmniej możliwość precyzyjnego określenia użytkownika odpowiedzialnego za utworzenie, usunięcie czy nadpisanie danych oraz czas tej operacji. 17) Ze względu na wymóg niskiego czasu dostępu do danych obszaru szybkiego system musi implementować protokół NFS over RDMA. 18) System musi mieć mechanizm deduplikacji danych celem optymalizacji wykorzystania przestrzeni dyskowych. 19) Jeżeli do spełnienia któregokolwiek z wymagań zdefiniowanych powyżej wymagane jest dodatkowe oprogramowanie lub licencja - należy je dostarczyć wraz z zamawianym systemem w wersji bez ograniczeń czasowych na całą pojemność systemu.
Dodatkowe funkcjonalności	1) Możliwość tworzenia lokalnych kopii migawkowych ręcznie lub automatycznie przy pomocy harmonogramu w którym definiuje się czas lub częstotliwość tworzenia kopii migawkowych oraz czas ich wygaśnięcia. Kopie migawkowe, których czas wygaśnięcia upłynął, powinny być automatycznie kasowane. Urządzenie powinno umożliwiać tworzenie kopii migawkowych z dokładnością do pojedynczego folderu. Mechanizm kopii migawkowych powinien się integrować z z posiadaną i wykorzystywaną lub planowaną do wykorzystania w projekcie przez Zamawiającego usługą Microsoft Volume Shadowcopy, umożliwiając użytkownikowi końcowemu samodzielne odzyskanie danych (bez angażowania administratora systemu). 2) Rozwiązanie powinno umożliwiać tworzenie kopii migawkowych (ang. snapshot) również w trybie odczyt/zapis. 3) System powinien posiadać funkcjonalność WORM i powinien pozwalać na tworzenie zasobów (folderów/udziałów plikowych) zarówno objętych politykami WORM, jak i zasobów nie objętych taką polityką. Na jednym urządzeniu powinna być możliwość zdefiniowania zasobów objętych różnymi politykami WORM jednocześnie (np. różnym czasem retencji). Dla zasobów objętych funkcjonalnością WORM powinna istnieć możliwość obejścia polityki

	WORM poprzez uprzywilejowane kasowanie danych przez uprawnionego do tego użytkownika (np. root, czy tzw. Security Officer). Dla zasobów objętych polityką WORM powinna istnieć możliwość przedłużenia czasu retencji na potrzeby np. dochodzenia (tzw. Litigation Hold). System powinna pozwalać na ręczne ustawianie flagi WORM, jak i na automatyczne nakładanie retencji (np. po określonym czasie od utworzenia pliku) bez dodatkowej akcji ze strony aplikacji. 4) Razem z rozwiązaniem należy dostarczyć platformę umożliwiającą zarządzanie danymi (indeksowanie, przeszukiwanie, czy opisywanie danych – dodawanie tzw. „tag-ów") i raportowanie bazujące m. in na ww. „tag-ach". 5) Polityki warstwowego składowania danych (ang. tiering) muszą umożliwiać elastyczne definiowanie kryteriów przenoszenia plików pomiędzy poszczególnymi tier-ami bazując m. in. na czasie utworzenia pliku (ctime), ostatnim czasie dostępu do pliku (atime), ostatnim czasie modyfikacji pliku (mtime), wielkości pliku, lokalizacji pliku (ścieżce), rozszerzeniu pliku i nazwie pliku. 6) Replikacja zdalna również musi być definiowalna na poziomie wybranego katalogu/udziału. System musi wspierać replikację dwukierunkową, jeden-do-wiele i wiele-do-jeden (na poziomie całego systemu). W celu zapewnienia dodatkowych punktów odzyskiwania danych (ang. Point-in-Time) musi istnieć możliwość automatycznego tworzenie kopii migawkowych na zdalnej macierzy po zakończeniu procesu replikacji. 7) Rozwiązanie musi mieć możliwość rozbudowy o funkcjonalność tworzenia kopii zapasowych danych na nim składowanych przy pomocy protokołu NDMP w trybie „2-way-NDMP" (bezpośrednio po sieci SAN). Zamawiający nie wymagana dostarczenia tej funkcjonalność w ramach tego postępowania. 8) Jeżeli system wymaga zewnętrznych komponentów zapewniających komunikację pomiędzy węzłami (np. w postaci przełączników), muszą one pochodzić od tego samego producenta co system i muszą być uwzględnione w ofercie. 9) Możliwość zabezpieczenia wybranych danych (np. poprzez ustawianie takiego parametru dla poszczególnych folderów) przed nieuprawnioną edycją lub skasowaniem za pomocą mechanizmu WORM. Polityki WORM powinny być replikowane do zdalnego systemu.

9. System pamięci masowej o dostępie obiektowym

Minimalne wymagania na sprzęt do budowy przestrzeni obiektowej:

Parametr	Szczegółowy opis wymagania
Pojemność, wydajność i bezpieczeństwo systemu	1) Zaoferowany system pamięci masowej o dostępie obiektowym (zwanym dalej systemem) musi być zbudowany w architekturze „scale-out" (skalowalnej horyzontalnie). 2) System musi być zbudowany w oparciu jednakowe węzły serwerowe (kontrolerowo-dyskowe) zwane dalej węzłami. 3) Dostarczony system musi zapewnić pojemność użyteczną minimum 3 PiB przy zabezpieczaniu danych przed ich utratą w przypadku awarii co najmniej 2 (dwóch) dowolnych dysków twardych jednocześnie lub 2 (dwóch) dowolnych węzłów (kontrolerów) jednocześnie. Pojemność użyteczną 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. 4) Wymagana pojemność musi być dostarczona na dyskach twardych znajdujących się wewnątrz poszczególnych węzłów zaoferowanego systemu. Nie są dopuszczalne rozwiązania oparte o taśmy czy platformy chmurowe. 5) System musi umożliwiać skalowanie poprzez dokładanie kolejnych węzłów i/lub dysków. Wymagana jest skalowalność do pojemności minimum 100 PiB. Rozbudowa rozwiązania musi być bezprzerwowa. 6) Dostarczony system po zainstalowaniu oprogramowania musi zapewniać wydajność nie mniejszą niż: a) dostęp losowy, rozmiar obiektu mniejszy niż 10 KiB: i. 90 tys. TPS w operacjach odczytu ii. 28 tys. TPS w operacjach zapisu b) dostęp sekwencyjny, rozmiar obiektu większy niż 128 MiB: i. 30 GB/s w operacjach odczytu ii. 6 GB/s w operacjach zapisu. Oferent musi przedstawić wyniki testu lub raport z konfiguratora producenta potwierdzające spełnienie tego warunku. 7) System musi być zbudowany z 18 węzłów (kontrolerów), gdzie każdy realizuje dostęp do danych i zapewnia wysoką wydajność dostępu do zgromadzonych danych w systemie. 8) System nie może posiadać pojedynczego punktu awarii, tzn. wszystkie jego elementy muszą być redundantne, a jego architektura musi zapewniać odporność na awarię w obrębie poszczególnych grup elementów, przynajmniej w zakresie: a) dysków twardych b) interfejsów sieciowych c) kontrolerów (węzłów)

	d) zasilaczy e) wentylatorów. 9) System musi mieć możliwość podłączenia go do centrum serwisowego producenta w celu zdalnego monitorowania poprawności funkcjonowania komponentów rozwiązania.
Sprzęt	1) W celu maksymalizacji gęstości, tj. minimalizacji wykorzystania obszaru serwerowni do przechowywania danych, pojedynczy węzeł nie może zajmować więcej niż 2 RU w szafie. 2) System musi być dostarczony wraz z kompletem wszystkich niezbędnych elementów potrzebnych do połączenia poszczególnych węzłów w jeden system, zarządzany z jednego interfejsu administracyjnego. 3) Każdy węzeł musi być wyposażony w 2 procesory klasy x86-64, z których każdy posiada minimum 10 rdzeni. 4) Każdy węzeł musi być wyposażony w a) 24 jednakowe dyski typu NLSAS lub SATA o pojemności 12 TB każdy przeznaczone do przechowywania danych b) 1 dysk SSD o pojemności 960 GB do buforowania metadanych i samych danych (ang. read cache) c) 1 dysk M.2 o pojemności minimum 480 GB do startu systemu operacyjnego. 5) System musi zapewniać dostępną, łączną pojemność pamięci RAM nie mniejszą niż 3456 GB (tzn. min. 192 GB dla pojedynczego węzła). 6) Każdy węzeł musi być wyposażony w 2 karty sieciowe Ethernet, każda z nich musi posiadać minimum 2 porty 25 Gb/s Ethernet SFP28. Interfejsy z jednej karty muszą być przeznaczone na potrzeby wewnętrznej komunikacji węzłów (interfejsy typu „back-end"). Interfejsy drugiej karty muszą być przeznaczone do zapewniania dostępu do danych (interfejsy typu „front-end"). 7) System musi zapewniać dostęp do danych przy jednoczesnym wykorzystaniu wszystkich interfejsów typu „front-end". 8) Komunikacja pomiędzy węzłami („back-end") musi: a) odbywać się za pośrednictwem osobnych i dedykowanych tylko do tego celu interfejsów (niewspółdzielonych z portami dostępowymi – „front-end"), b) odbywać się za pośrednictwem dedykowanych i przeznaczonych tylko do tego celu przełączników sieciowych (niewspółdzielonych z przełącznikami obsługującymi dostęp do danych – „front-end"), c) być zrealizowana w sposób redundantny, zapewniający prawidłową pracę systemu w przypadku awarii dowolnego przełącznika sieciowego obsługującego komunikację pomiędzy węzłami („back-end"). Wszystkie niezbędne elementy zapewniające tą komunikację (tj. przełączniki sieciowe, okablowanie, inne) muszą być dostarczone wraz z systemem i nie podlegają szczegółowej specyfikacji przez Zamawiającego.

	Zmawiający dopuszcza możliwość realizacji tych połączeń przy użyciu kabli typy „DAC" (ang. Direct Attach Cable).
Składowanie danych i protokoły	1) System musi realizować dostęp do danych za pomocą co najmniej następujących interfejsów i protokołów**:** Amazon S3, OpenStack Swift, HDFS (Hadoop Distributed File System) oraz NFS. Jeżeli wykorzystanie któregokolwiek z wymienionych protokołów wymaga zastosowania dodatkowej licencji, to należy je dostarczyć wraz z systemem. 2) Dane w systemie pamięci masowej o dostępie obiektowym będącym przedmiotem zamówienia muszą być składowane jako obiekty składające się z danych oraz opisujących je metadanych**.** Metadane nie mogą być składowane w wydzielonej bazie danych. 3) Replikacja danych (obiektów) musi być realizowana spójnie z metadanymi. 4) Dla protokołu S3 system musi posiadać wbudowany mechanizm indeksowania i przeszukiwania metadanych. Musi istnieć możliwość wyszukiwania w oparciu o wewnętrzną wyszukiwarkę i interfejs programistyczny (API) pozwalający na integrację silnika wyszukiwania z własną aplikacją. 5) System musi posiadać możliwość zdefiniowania i indeksowania co najmniej 10 atrybutów metadanych dla obiektu. 6) System musi posiadać wbudowany mechanizm wersjonowania obiektów w przypadku wykorzystania protokołu S3. 7) System musi umożliwiać zarządzanie listami kontroli dostępu (ACL) oraz politykami dostępu do „bucket-ów" (Bucket Policy), przy pomocy których można definiować uprawnienia przyznawane użytkownikom.
Funkcjonalność	1) System musi zapewniać i gwarantować niezmienność składowanych w nim obiektów poprzez wykorzystanie wbudowanej funkcjonalności WORM (Write Once Read Many) przynajmniej dla protokołu S3. 2) Funkcjonalność WORM musi być realizowana wewnątrz dostarczonego gotowego rozwiązania sprzętowego w jego oprogramowaniu systemowym. 3) System musi posiadać możliwość definiowania różnych poziomów retencji przechowywania danych, gwarantujących brak możliwości skasowania danych przed upływem zdefiniowanego czasu. 4) System musi pozwalać na zdefiniowanie partycji, w których istnieje możliwość usuwania danych przed upływem retencji oraz partycji w których usuwanie danych przed upływem retencji jest niemożliwe – również przez operatora/administratora systemu (tzw. tryb Compliance). System musi pozwalać na definiowanie i uruchamianie jednocześnie obydwu typów partycji. 5) System musi posiadać możliwość tworzenia logicznie odseparowanych obszarów tzw. „multi-tenancy". Wymagana jest możliwość rozdzielnego administrowania (np.: przypisywanie użytkowników, tworzenie praw dostępu, polityki składowania

	danych, monitorowanie wykorzystania) tak tworzonymi obszarami (tzn. „tenants”). 6) Każdy „tenant” może mieć zdefiniowanych wiele przestrzeni nazw („namespace”), które mogą być dedykowane dla określonych aplikacji i w ramach, których operator może definiować niezależnie różne polityki i kryteria w zależności od wymagań każdej z tych aplikacji (polityki typu: wersjonowanie, retencja, replikacja, kompresja, ilość kopii wewnętrznych, tiering itp.). 7) System musi pozwalać na podział logiczny na wiele logicznych partycji (tzw. „tenants”), dedykowanych dla określonych odbiorców usług, np. określonych rozwiązań i projektów lub podmiotów zewnętrznych. 8) Zamawiający wymaga, aby dostarczony system posiadał możliwość zdefiniowania co najmniej 1000 logicznych partycji ("tenant-ów"). 9) System musi posiadać integrację z Microsoft Active Directory oraz Open LDAP w zakresie uwierzytelnienia i autoryzacji kont dostępowych. 10) System musi posiadać swoje własne wbudowane mechanizmy weryfikacji integralności danych np. przy pomocy sum kontrolnych składowanych obiektów. 11) System musi posiadać wbudowane mechanizmy redukcji danych, w tym co najmniej kompresję danych. W przypadku braku tej funkcjonalności, należy dostarczyć 100% więcej wymaganej pojemności. 12) System musi posiadać funkcjonalność szyfrowania danych przechowywanych na dyskach obiektowego magazynu składowania danych. Wymagane jest użycie algorytmu min. AES-256 lub równoważnego. Jeżeli wymagana jest licencja, należy ją dostarczyć. 13) System musi umożliwiać zarządzanie co najmniej poprzez graficzny interfejs użytkownika oraz interfejs programistyczny (AP)I. 14) System musi umożliwiać automatyczny monitoring obejmujący minimalnie takie parametry jak: a) utylizację zasobów on-line (w tym CPU, pamięć RAM, sieć) b) zajętość miejsca c) transfery d) ilość operacji. 15) System musi umożliwiać tworzenie alertów i powiadomień dotyczących stanu systemu z możliwością automatycznego ich przesyłania na adres e-mail. 16) Jeżeli do spełnienia któregokolwiek z wymagań zdefiniowanych powyżej wymagane jest dodatkowe oprogramowanie lub licencja - należy je dostarczyć wraz z zamawianym systemem w wersji bez ograniczeń czasowych na całą pojemność systemu.
Gwarancja	1) Dostarczony sprzęt musi być nowy. 2) Wszystkie urządzenia wchodzące w skład oferowanego systemu muszą być objęte co najmniej 7-letnim pełnym wsparciem technicznym producenta w zakresie sprzętu i oprogramowania.

	3) Gwarancja musi umożliwiać dostęp do najnowszych wersji oprogramowania (firmware) oraz poprawek i łatek dla oprogramowania. 4) Możliwość zgłaszania awarii przez 24 godziny na dobę z czasem reakcji w następnym dniu roboczym. 5) Gwarancja będzie realizowana w miejscu instalacji sprzętu. 6) Wykonawca zapewni możliwość zgłaszania awarii w trybie 365x7x24 poprzez ogólnopolską linię telefoniczną producenta. 7) Zamawiający wymaga, aby uszkodzone dyski pozostawały u Zamawiającego. 8) Oświadczenie producenta serwera, potwierdzające, że sprzęt pochodzi z oficjalnego kanału dystrybucyjnego producenta. 9) Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia.

10. Urządzenie do przechowywania kopii zapasowych

Zaoferowane urządzenie do przechowywania kopii zapasowych musi spełniać wszystkie wymagania przedstawione w poniższej tabeli.

Parametr	Charakterystyka (wymagania minimalne)
Obudowa	1) Obudowa przystosowana do zainstalowania w szafie teleinformatycznej 19”, musi być dostarczona wraz z zestawem szyn do jej montażu.
Zasoby dyskowe	1) Dostarczone urządzenie musi posiadać co najmniej 94 TiB pojemności użytecznej. Pojemność użyteczną należy rozumieć jako pojemność pozwalającą na rzeczywisty zapis danych o tej objętości na urządzeniu 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. 2) Urządzenie musi posiadać minimum dwa identyczne dyski SDD przeznaczone na pamięć podręczną (ang. cache). Pojedynczy dysk o rozmiarze nie mniejszym niż 1,9 TB. 3) Oferowane rozwiązanie musi mieć możliwość rozbudowy pojemności użytecznej przeznaczonej na przechowywanie unikalnych segmentów danych do minimum 150 TB. 4) Rozbudowa przestrzeni musi być możliwa w kwantach nie większych niż 8TB. 5) Zdeduplikowane i skompresowane dane przechowywane w obrębie podsystemu dyskowego urządzenia muszą być chronione za pomocą technologii RAID 6 bądź równoważnej. 6) Oferowane urządzenie musi posiadać zapasowe dyski lub zapasową pojemność zgodnie z najlepszymi praktykami producenta rozwiązania.
Interfejsy Sieciowe	1) Oferowane urządzenie musi posiadać minimum a) 4 porty Ethernet 10 Gb/s SFP+ b) 4 porty Ethernet 25 Gb/s SFP28 2) Oferowane urządzenie musi mieć możliwość rozszerzenia o dodatkowe porty. Zamawiający musi mieć możliwość rozszerzenia o 2 porty Ethernet 25 Gb/s lub 2 porty FC 16 Gb/s. 3) Interfejsy muszą być podłączone przy użyciu medium światłowodowego.
Zasilanie	1) Urządzenie musi posiadać redundantne zasilacze. W przypadku awarii jednego toru zasilania urządzenie musi poprawnie pracować na jednym zasilaczu.
Wydajność	1) Oferowane pojedyncze urządzenie musi osiągać zagregowaną wydajność protokołami CIFS, NFS, VTL co najmniej 8 TB/h (dane podawane przez producenta) oraz co najmniej 20 TB/h z wykorzystaniem de-duplikacji na źródle (dane podawane przez producenta). 2) Urządzenie musi pozwalać na jednoczesną obsługę minimum 250 strumieni, w tym jednocześnie: • zapis danych minimum 200 strumieni • odczyt danych minimum 30 strumieni • replikacja minimum 20 strumieni pochodzących z różnych aplikacji, dowolnych protokołów: CIFS, NFS, VTL oraz dowolnych interfejsów (FC, LAN) w tym samym czasie wraz z de-

	duplikacja na źródle. Wymienione wartości jednoczesnych strumieni dla wszystkich protokołów muszą mieścić się w przedziale oficjalnie rekomendowanym i wspieranym przez producenta urządzenia. 3) Urządzenie musi zapewniać jednoczesny dostęp wraz z de-duplikacją wszystkimi protokołami: CIFS, NFS de-duplikacja na źródle oraz VTL 4) Wymagane jest by urządzenie pozwalało na uruchomienie kopii zapasowych co najmniej 10 maszyn wirtualnych.
Funkcjonalność	1) Urządzenie musi pozwalać na uruchomienie kopii zapasowych maszyn wirtualnych bezpośrednio z urządzenia bez odtwarzania na jakikolwiek zewnętrzny magazyn danych. 2) Urządzenie musi posiadać możliwość obsługi każdym portem Ethernet protokołów CIFS, NFS, de-duplikacja na źródle. 3) Oprócz de-duplikacji urządzenie musi wykonywać sprzętową kompresję nowych bloków – musi posiadać dedykowana kartę sprzętową kompresującą nowe, unikalne bloki, minimum przy użyciu algorytmu gzfast. 4) Oferowane urządzenie musi mieć możliwość emulacji napędów taśmowych LTO-1, LTO-2, LTO-3, LTO-4, LTO-5. 5) Urządzenie musi umożliwiać przyporządkowanie minimum 120 napędów do pojedynczej emulowanej biblioteki taśmowej. 6) Oferowane urządzenie musi de-duplikować dane „in-line" przed zapisem na nośnik dyskowy. Na wewnętrznych dyskach urządzenia nie mogą być zapisywane dane w oryginalnej postaci (niezdeduplikowanej) z jakiegokolwiek fragmentu strumienia danych przychodzącego do urządzenia. 7) Technologia de-duplikacji musi wykorzystywać algorytm bazujący na zmiennym, dynamicznym bloku. Algorytm ten musi samoczynnie i automatycznie dopasowywać się do otrzymywanego strumienia danych. Oznacza to, że urządzenie musi dzielić otrzymany pojedynczy strumień danych na bloki o różnej długości. 8) De-duplikacja zmiennym, dynamicznym blokiem musi oznaczać, że wielkość każdego bloku (na jaki są dzielone dane pojedynczego strumienia backupowego) może być inna niż poprzedniego i jest indywidualnie ustalana przez algorytm urządzenia. 9) Urządzenie nie może przechowywać danych o de-duplikacji w centralnej bazie. Utrata bazy danych używanej przez oprogramowanie nie może prowadzić do utraty możliwości odtworzenia backupu. Metadane de-duplikacji muszą być trzymane razem z kopiami zapasowymi danych. 10) Oferowany produkt musi posiadać obsługę mechanizmów globalnej de-duplikacji dla danych otrzymywanych jednocześnie wszystkimi protokołami (CIFS, NFS, VTL, de-duplikacja na źródle) przechowywanych w obrębie całego urządzenia. W obrębie całego urządzenia, raz otrzymany i zapisany w urządzeniu fragment danych nie może nigdy więcej zostać zapisany bez względu na to, jakim protokołem zostanie ponownie otrzymany. 11) Powyższe oznacza również, że oferowany produkt musi również posiadać obsługę mechanizmów globalnej de-duplikacji pomiędzy różnymi udziałami CIFS jakie można wystawić z urządzenia. 12) Powyższe oznacza również, że oferowany produkt musi również posiadać obsługę mechanizmów globalnej de-duplikacji pomiędzy dowolnymi wirtualnymi bibliotekami. Blok danych otrzymany i zapisany w wirtualnej

	bibliotece A, nie może zostać ponownie zapisany jeśli trafi do innej wirtualnej biblioteki (wirtualnej biblioteki B). 13) Przestrzeń składowania zde-duplikowanych danych musi być jedna dla wszystkich protokołów dostępowych (CIFS, NFS, VTL, de-duplikacja na źródle). 14) Proces de-duplikacji musi odbywać się „in-line" – w pamięci urządzenia, przed zapisem danych na nośnik dyskowy. Zapisowi na system dyskowy muszą podlegać tylko unikalne bloki danych nie znajdujące się jeszcze w systemie dyskowym urządzenia. Dotyczy to każdego fragmentu przychodzących do urządzenia danych. 15) Proponowane rozwiązanie nie może w żadnej fazie korzystać (w całości lub częściowo) z dodatkowego bufora na składowanie danych w postaci oryginalnej (niezdeduplikowanej). 16) Wszystkie unikalne bloki przed zapisaniem na dysk muszą być kompresowane minimum metodą gz. 17) Oferowane urządzenie musi pozwalać na de-duplikację na źródle na poziomie systemu plików. Oznacza to, że musi być możliwość wskazania dowolnego katalogu na maszynie wirtualnej dla którego będzie wykonywana de-duplikacja na źródle. Każdy plik zapisany do wskazanego katalogu podlega zapisowi na oferowanym urządzeniu przy wykorzystaniu globalnej de-duplikacji na źródle. Dane są zapisywane na oferowanym urządzeniu przy transferze tylko tych fragmentów danych, których jeszcze nie ma na urządzeniu (globalna de-duplikacja na źródle). 18) W przypadku de-duplikacji na źródle poprzez sieć IP (LAN oraz WAN), musi być możliwość szyfrowania komunikacji kluczem minimum 256 bitów. 19) Urządzenie nie może zmniejszać swojej wydajności w czasie przybywania kolejnych danych. 20) Urządzenie musi mieć możliwość: a) wydzielenia dedykowanego portu Ethernet do replikacji b) replikacji dowolnym portem Ethernet. 21) W przypadku wykorzystania portów Ethernet do replikacji urządzenie musi umożliwiać przyjmowanie backupów, odtwarzanie danych, przyjmowanie strumienia replikacji, wysyłanie strumienia replikacji tymi samymi portami. 22) Oferowane urządzenie musi umożliwiać replikację danych do drugiego urządzenia fizycznego lub wirtualnego. Konfiguracja replikacji musi być możliwa w każdym z trybów: a) jeden do jednego b) wiele do jednego c) jeden do wielu d) kaskadowej (urządzenie A replikuje dane do urządzania B, które te same dane replikuje do urządzenia C). Replikacja musi się odbywać w trybie asynchronicznym. Transmitowane mogą być tylko te fragmenty danych (bloki), które nie znajdują się na docelowym urządzeniu. Licencja na replikację musi być dostarczona w ramach postępowania. 23) W przypadku backupów z wykorzystywanych lub planowanych do wykorzystania w projekcie przez Zamawiającego systemów VMware lub baz danych Oracle, urządzenie musi umożliwiać uruchomienie maszyn wirtualnych lub baz danych Oracle bezpośrednio z urządzenia, bez konieczności odtwarzania na zewnętrzny magazyn danych.

	24) Oferowane urządzenie musi działać poprawnie dla zapełnienia minimum 85%. Dokumentacja urządzenia nie może wskazywać na jakiekolwiek problemy, obostrzenia, które mogą pojawić się przy jakimkolwiek zapełnieniu urządzenia do 85% włącznie. 25) Narzut na wydajność związany z replikacją nie może zmniejszyć wydajności urządzenia o więcej niż 10%. 26) Musi istnieć możliwość ograniczenia pasma używanego do replikacji między dwoma urządzeniami. 27) Oferowane urządzenie musi umożliwiać wykonywanie migawek (ang. snapshot) czyli możliwość zamrożenia obrazu danych (stanu backupów) w urządzeniu na określoną chwilę. Oferowane urządzenie musi również umożliwiać odtworzenie danych z takiej migawki. Odtworzenie danych z migawki nie może wymagać konieczności nadpisania danych produkcyjnych jak również nie może oznaczać przerwy w normalnej pracy urządzenia (przyjmowania backupów / odtwarzania). 28) Urządzenie musi pozwalać na przechowywanie minimum 500 migawek jednocześnie dla każdej logicznej części oddzielnie. 29) Urządzenie musi pozwalać na podział na logiczne części. Dane znajdujące się w każdej logicznej części muszą być między sobą de-duplikowane (globalna de-duplikacja między logicznymi częściami urządzenia). 30) Urządzenie musi mieć możliwość podziału na minimum 100 logicznych części pracujących równolegle. Producent musi oficjalnie wspierać pracę minimum 100 logicznych częściach pracujących równolegle z pełną wydajnością urządzenia. 31) Oferowane urządzenie powinno umożliwiać zdefiniowanie limitów tzw. „quota” na pojemność używaną przez każdą z w/w logicznych części urządzenia. 32) Dla każdej z logicznych części oferowanego urządzenia musi być możliwość zdefiniowania oddzielnego użytkownika zarządzającego daną logiczną częścią de-duplikatora. Użytkownicy zarządzający logiczną częścią A muszą widzieć tylko i wyłącznie zasoby logicznej części i nie mogą widzieć żadnych innych zasobów oferowanego urządzenia. 33) Musi być możliwość zaprezentowania każdej z logicznych części oferowanego urządzenia jako niezależnego urządzenia: a) CIFS b) NFS c) VTL d) De-duplikacja na źródle 34) Urządzenie musi mieć możliwość zdefiniowania serwerów (adresów IP) które mają prawo zapisywać/odczytywać dane dla każdej logicznej części. 35) Urządzenie musi mieć możliwość monitorowania jakie serwery (adresy IP) zapisują/odczytują dane ze wszystkich logicznych części 36) Dla każdej z logicznych części oferowanego urządzenia musi być możliwe zdefiniowanie blokady skasowania danych. Blokada skasowania danych musi chronić plik w zdefiniowanym czasie przed usunięciem pliku, modyfikacją pliku. Blokada skasowania danych musi działać w dwóch trybach (do wyboru przez administratora): a) możliwość zdjęcia blokady przed upływem ważności danych, b) brak możliwości zdjęcia blokady przed upływem ważności danych (ang. compliance) przez kogokolwiek – w tym przez administratora backupu.

	37) Funkcjonalność bezwzględnej blokady musi spełniać minimum najmniejsze standardy: a) SEC 17a-4(f) b) CFTC Rule 1.31b c) FDA 21 CFR Part 11 d) Sarbanes-Oxley Act e) IRS 98025 and 97-22 f) ISO Standard 15489-1 g) MoREQ2010 38) Licencje na blokadę usunięcia/zmiany przechowywanych plików (WORM) muszą być dostarczone wraz z urządzeniem. W przypadku braku wymaganej funkcjonalności WORM, wymagana jest dostawa dodatkowej macierzy typu NAS (NFS/CIFS) spełniającej wymagania wydajnościowe stawiane przed opisanym w niniejszym punkcie urządzeniem o pojemności netto dwukrotnie większej od wymaganej pojemności netto tego urządzenia. W każdym z w/w przypadków blokada WORM musi być zintegrowana z zaoferowanym oprogramowaniem do wykonywania kopii zapasowych opisanym w punkcie **0** co oznacza: a) możliwość uruchomienia blokady WORM dla określonych danych z poziomu zaoferowanego oprogramowania, b) możliwość określenia/wymuszenia czasu blokady z poziomu zaoferowanego oprogramowania, c) możliwość raportowania od strony zaoferowanego oprogramowania danych zabezpieczonych przed usunięciem wymaganą blokadą WORM. W każdym z w/w przypadków wymagana również możliwość automatycznego uruchamiania blokady (podczas zapisu) WORM dla danych zapisywanych na obszar objęty działaniem wspomnianej blokady 39) W przypadku założenia bezwzględnej blokady danych na przechowywanych backupach (ang. compliance): a) urządzenie nie może pozwalać na zmianę czasu b) urządzenie nie może pozwalać na obejście blokady c) urządzenie musi wymagać by kluczowe z punktów widzenia bezpieczeństwa operacje były potwierdzane hasłem dwóch niezależnych administratorów – administratora urządzenia i administratora bezpieczeństwa. 40) Urządzenie musi pozwalać na: a) przechowywanie minimum 500 milionów plików b) dzienne zasilenie na poziomie minimum 500 tysięcy plików 41) Urządzenie musi pozwalać na raportowanie ile fizycznie zajmują dane znajdujące się: a) w ramach wskazanej logicznej części b) we wskazanym katalogu c) we wskazanym pliku. 42) Urządzenie musi mieć dedykowany, oddzielny system plików dla przechowywanych danych (backupy, archiwa). System operacyjny urządzenia oraz logi urządzenia nie mogą być przechowywane na systemie plików dedykowanym dla przechowywanych danych.

	43) Po niespodziewanym wyłączeniu prądu i ponownym uruchomieniu, urządzenie musi być gotowe do przyjmowania danych (backupy, archiwa) w czasie nie dłuższym niż 60 minut od włączenia. 44) Urządzenie musi weryfikować ewentualne przekłamanie (zmianę danych) dla: a) systemu plików b) RAID zaimplementowanych w urządzeniu. Wymaga się by urządzenie sprawdzało sumy kontrolne zapisywanych fragmentów danych dla system plików / RAID podczas skanowania. 45) Urządzenie musi weryfikować dane po zapisie. Każda zapisana na dyskach porcja danych musi być odczytana i porównana z danymi otrzymanymi przez urządzenie w momencie zapisu. Wymagane potwierdzenie faktu weryfikacji zapisanych danych w dokumencie producenta. 46) Urządzenie musi automatycznie (samoczynnie) wykonywać sprawdzanie spójności danych po zapisaniu danych na dysk oraz rozpoznawać i naprawiać błędy w locie. Każde zapisane na fizycznych dyskach dane muszą być odczytane i porównane z danymi otrzymanymi. Proces ten musi odbywać się w locie – musi być elementem procesu zapisu danych przez urządzenie. Dopiero sprawdzenie spójności danych musi pozwalać na usunięcie z bufora danych otrzymanych od aplikacji. 47) Urządzenie musi automatycznie usuwać przeterminowane dane (bloki danych nie należące do backupów o aktualnej retencji) w procesie czyszczenia. 48) Proces usuwania przeterminowanych danych (czyszczenia) nie może przerywać pracy procesów backupu / odtwarzania danych oraz zapisu / odczytu danych z zewnątrz do systemu. 49) Musi istnieć możliwość zdefiniowania maksymalnego obciążenia urządzenia procesem usuwania przeterminowanych danych (poziomu obciążenia procesora) 50) Musi istnieć możliwość zdefiniowania czasu kiedy wykonywany jest proces usuwania przeterminowanych danych (czyszczenia). 51) Musi być możliwość by usuwanie przeterminowanych danych (czyszczenie) odbywało się raz na tydzień minimalizując czas, w którym backupy / odtworzenia narażone są na spowolnienie. 52) Urządzenie musi zapewniać w dni robocze (poniedziałek – piątek) minimum 20 godzin pełnej wydajności. W czasie pełnej wydajności (poniedziałek-piątek, minimum 20 godzin dziennie) urządzenie nie może wykonywać jakichkolwiek wewnętrznych procesów w tym nie może wykonywać usuwania przeterminowanych danych. 53) Proces usuwania przeterminowanych danych nie może zajmować więcej niż 4 godziny dziennie w dni robocze (poniedziałek – piątek). 54) Urządzenie musi mieć możliwość zarządzania poprzez a) interfejs graficzny dostępny z przeglądarki internetowej b) linię komend (CLI) dostępną np. z poziomu ssh (secure shell) 55) Oprogramowanie do zarządzania musi znajdować się na oferowanym urządzeniu de-duplikacyjnym. 56) Oferowany produkt musi mieć zaimplementowaną funkcjonalność wewnętrznego mechanizmu szyfrowania danych przed zapisaniem na dysk realizowany na poziomie urządzenia – długość klucza minimum 256-bit.

Inne	1) Dostarczone urządzenie musi być fabrycznie nowe i nieużywane, oraz wolne od wad fizycznych i prawnych. 2) Oferowane urządzenie nie może być prototypem co oznacza, że identyczne modele urządzeń znajdują się w sprzedaży, co najmniej od 60 dni poprzedzających termin złożenia oferty. 3) Wymagane jest dostarczenie licencji, pozwalającej na jednoczesną obsługę wszystkich protokołów CIFS, NFS, VTL, de-duplikacja na źródle na pełną pojemności urządzenia. 4) Urządzenie musi być rozwiązaniem kompletnym, „appliancem" sprzętowym. Zamawiający nie dopuszcza stosowania rozwiązań typu „gateway" z uwagi na brak miarodajnych danych dotyczących ich wydajności oraz dostępności. 5) Dostarczone urządzenie musi być „appliancem" stanowiącym całość pochodzącą od jednego producenta (oprogramowanie oraz sprzęt) 6) Wszystkie zapisywane strumienie muszą podlegać globalnej de-duplikacji przed zapisem na dysk (in-line) jak opisano w niniejszej specyfikacji.
Wymiana dysków	1) Wymiana dysków może być dokonywana samodzielnie przez zamawiającego. 2) Zamawiający zatrzymuje uszkodzone dyski.

10.1. Opis równoważności

Poniżej opisano kryteria, jakie Zamawiający będzie stosował w celu oceny równoważności rozwiązania zaproponowanego przez Wykonawcę jako równoważne dla technologii RAID 6 lub równoważny.

Przez równoważność Zamawiający rozumie konieczność:

1. zapewnienia przez technologię pełnej funkcjonalności jaką oferuje technologia RAID 6 w zakresie wydajności oraz ochrony składowanych danych przy zastosowaniu takiej samej liczby fizycznych dysków.

11. Oprogramowanie do wykonywania kopii zapasowych

Zaoferowane oprogramowanie do wykonywania kopii zapasowych musi spełniać wszystkie wymagania przedstawione poniżej.

1) Zamawiający wymaga dostarczenia, uruchomienia i wdrożenia oprogramowania do wykonywania kopii zapasowych (ang. backup) całego środowiska „data center" składającego się z maszyn wirtualnych.
2) Wymagane jest dostarczenie wszystkich modułów oprogramowania do wykonywania kopii zapasowych tak, aby zapewnić backup całości dostarczanego środowiska oraz spełnić wszystkie wymienione w poniżej funkcjonalności.
3) Wymagane jest by wszystkie dostępne funkcjonalności oferowanego oprogramowania do wykonywania kopii zapasowych były odblokowane w ramach oferowanej licencji procesorowej.
4) W szczególności wymagane jest by w ramach dostarczonej licencji była możliwość tworzenia kopii oraz odtwarzania:
   a) dowolnej liczby maszyn wirtualnych jako obrazów (ang. „image level")
   b) agentowo:
      i) dowolnej liczby baz danych,
      ii) dowolnej liczby plików – zarówno z serwerów niezwirtualizowanych jak również ze środka maszyn wirtualnych
   c) użycia dowolnej liczby mediów backupowych o dowolnej pojemności
5) Serwer kopii zapasowych musi być uruchomiony jako prekonfigurowany obraz maszyny wirtualnej (ang. virtual appliance) dla zaoferowanego oprogramowania do wirtualizacji mocy obliczeniowej.
6) Wymagane jest by serwer backupu działał jako maszyna wirtualna co najmniej na systemach operacyjnych Windows / Linux.
7) Wymagane jest by serwer backupu, jako maszyna wirtualna, wspierał przenoszenie maszyny wirtualnej serwera backupu do innej lokalizacji mechanizmami wirtualizatora.
8) Serwer backupu nie może zużywać więcej zasobów niż:
   a) 2 procesory wirtualne 8 wątków każdy procesor
   b) 32 GB pamięci RAM
   c) 200 GB dysku
9) Oprogramowanie backupowe musi umożliwiać backup zabezpieczanych maszyn na oferowane medium de-duplikacyjne zarówno poprzez sieć LAN jak również SAN.
10) Wymagane jest by istniała możliwość wyboru miejsca de-duplikacji
    a) na źródle
    b) na medium backupowym
    zarówno dla backupu po LAN jak i SAN
11) Backup z de-deduplikacją na źródle musi być dostępny dla wszystkich typów danych w ramach oferowanego rozwiązania: pliki, bazy danych, obrazy maszyn wirtualnych w każdym z przypadków:
    a) backup po LAN
    b) backup po SAN.
12) Oprogramowanie backupowe musi zapewniać backup z każdej zabezpieczanej maszyny bezpośrednio na zaoferowanym urządzeniu do przechowywania kopii zapasowych (medium de-duplikacyjne) bez pośrednictwa jakichkolwiek innych serwerów. Funkcjonalność musi być dostępna dla co najmniej następujących systemów: Windows, RedHat, SuSE, Solaris.

13) Oprogramowanie backupowe musi zapewniać bezpośredni backup z de-duplikacją na źródle z każdej zabezpieczanej maszyny znajdującej się w sieci LAN bezpośrednio na oferowane medium de-duplikacyjne bez pośrednictwa jakichkolwiek innych serwerów. Funkcjonalność musi być dostępna dla co najmniej następujących systemów: Windows, RedHat, SuSE, Solaris.
14) W przypadku awarii połączenia LAN, oprogramowanie backupu musi mieć możliwość automatycznego przełączenia się na inną dostępną ścieżkę LAN i kontynuowania procesu backupu bez konieczności jakiejkolwiek interwencji administratora oraz bez wznawiania procesu backupu.
15) Wymagane jest by oprogramowanie backupowe zapewniało szybki backup blokowy wielomilionowych systemów plików na maszynach z systemami operacyjnymi co najmniej Windows / Linux.
    W trakcie backupu oprogramowanie backupowe musi wykonywać kopie zapasowe fizycznych bloków a nie plików. Jednocześnie musi być możliwość odtworzenia:
    a) całego wolumenu
    b) pojedynczego pliku.
    Celem minimalizacji czasu backupu oprogramowanie backupowe nie może indeksować plików znajdujących się na zabezpieczanym wolumenie (zaindeksowanie wielu milionów plików powoduje istotne wydłużenie czasu backupu).
16) Wymagane jest by oprogramowanie backupowe zapewniało pełny backup blokowy wielomilionowych systemów plików na maszynach systemami operacyjnymi co najmniej Windows / Linux poprzez odczyt tylko zmienionych bloków.
    Wymagane jest by odczyt całości zabezpieczanego dysku był wykonywany tylko raz, podczas pierwszego backupu. Wszystkie kolejne backupy mają odczytywać z dysku tylko zmienione bloki od ostatniego backupu (przy czym na medium backupowym powinien być pełen backup).
    Dopuszcza się odczyt całości danych na dysku po restarcie serwera.
    Oprogramowanie backupowe nie może odczytywać zmienionych plików, jedynie zmienione bloki na dysku.
17) Oferowane rozwiązanie backupowe musi przechowywać całość własnych informacji (informacje o backupach, napędach taśmowych, mediach) w centralnym pojedynczym katalogu. Skopiowanie centralnego katalogu systemu backupu na inną maszynę musi pozwolić na uruchomienie serwera backupu identycznego z oryginalnym na drugiej maszynie. Proces klonowania centralnego katalogu może odbywać się przy wyłączonych procesach backupowych (zapewnienie spójności wewnętrznej bazy danych systemu backupowego).
18) Ze względów bezpieczeństwa rozwiązanie backupowe musi mieć możliwość wykonania kopii wewnętrznej bazy danych w trakcie pracy systemu bez konieczności ograniczania jego funkcjonalności.
19) Oprogramowanie backupowe musi mieć możliwość backupu własnej bazy danych na następujące nośniki:
    a) urządzenia dyskowe
    b) zaoferowane urządzenie de-duplikacyjne
    c) taśmy.
20) W przypadku backupu na nośniki taśmowe musi być możliwość zdefiniowania puli taśm (zawierającej jedną lub więcej taśm) na którą będą zapisywane tylko i wyłącznie backupy wewnętrznej bazy danych systemu backupowego.
21) Oprogramowanie backupowe musi mieć możliwość automatycznego wykonywania backupu własnej bazy danych.

22) Oprogramowanie backupowe po każdorazowym backupie wewnętrznej bazy danych musi mailowo raportować miejsce, w którym znajduje się ostatni backup wewnętrznej bazy danych oprogramowania backupowego.
23) Backup własnej bazy danych musi pozwalać na odtworzenie wszystkich ustawień systemu backupowego na zupełnie nowej, świeżo zainstalowanej instancji oprogramowania backupowego.
24) W przypadku użycia biblioteki taśmowej (backup, replikacja z oferowanego de-duplikatora sprzętowego na taśmę), oferowany system musi generować dla każdego backupu samopsujące się taśmy dla całości zapisywanych taśm. Oznacza to, że wyjęcie jakiejkolwiek taśmy z biblioteki i włożenie jej do zupełnie innej biblioteki zarządzanej przez zupełnie inną instancję oferowanego oprogramowania backupowego (w tym również działająca na innym systemie operacyjnym) musi pozwolić na odtworzenie danych znajdującej się na taśmie.
25) Oferowane rozwiązanie musi generować somo-opisujące się zbiory danych zarówno na oferowanym de-duplikatorze sprzętowym jak i na taśmach. Utraty wszystkich wewnętrznych danych oprogramowania backupowego nie może powodować braku możliwości odtworzenia jakichkolwiek zbiorów z oferowanego de-duplikatora sprzętowego bądź taśm.
26) Oprogramowanie backupowe musi umożliwiać łączenie strumieni backupowych z wielu zabezpieczanych serwerów w sieci LAN i bezpośredni zapis na napędzie taśmowym (multiplexing). Proces multiplexingu nie może wymagać zapisu danych na dysk: czasowego czy tez trwałego.
27) Oprogramowanie backupowe musi umożliwiać zarządzanie replikacją backupów między kilkoma urządzeniami de-duplikacyjnymi (zaoferowanych w tym postępowaniu) bezpośrednio z poziomu interfejsu oprogramowania backupowego przy spełnieniu wszystkich poniższych wymagań
    a) replikacji podlegają tylko te bloki które nie znajdują się na docelowym oferowanym urządzeniu de-duplikacyjnym
    b) replikacja między oferowanymi urządzeniami de-duplikacyjnymi może nastąpić zarówno bezpośrednio po zakończeniu backupu jak również zgodnie z harmonogramem
    c) oferowane oprogramowanie backupowe przechowuje informacje o wszystkich kopiach danych znajdujących się na urządzeniach de-duplikacyjnych.

    W trakcie odtwarzania, z graficznego GUI, oferowane oprogramowanie backupowe misi pozwalać na wybór urządzenia de-duplikacyjnego z którego zostanie wykonane odtwarzanie.
28) Rozwiązanie backupowe musi wspierać bezpośredni backup (bez użycia serwerów pośredniczących) z zabezpieczanych maszyn na macierz obiektową przy użyciu S3 API.
29) Wymagane jest by oferowane oprogramowanie backupowe wspierało backup na fizyczne macierze obiektowe przy użyciu S3 API.
30) Wymagane jest by backup na macierze obiektowe odbywał się:
    a) z de-duplikacją zmiennym blokiem
    b) z de-duplikacja na źródle
    c) poprzez transfer danych bezpośrednio z zabezpieczanych maszyn do macierzy obiektowej bez jakichkolwiek serwerów/elementów pośredniczących.

    Oznacza to, że agent oprogramowania backupowego musi dzielić zabezpieczane dane na kawałki zmiennej długości. Z zabezpieczanej maszyny bezpośrednio do macierzy obiektowej musza być przesłane tylko te kawałki danych, które się tam jeszcze nie znajdują. Funkcjonalność ta musi być dostępna dla systemamów operacyjnymi co najmniej Windows / Linux.
31) Wymagana jest funkcjonalność replikacji backupów wykonanych na macierz obiektową do:
    a) innej, dowolnie wspieranej macierzy obiektowej
    b) biblioteki taśmowej (w postaci backupu bez deduplikacji, czyli w postaci takiej jak wykonanie oryginalnego backupu na bibliotekę taśmową)

c) zasobu dyskowego (w postaci backupu bez deduplikacji, czyli w postaci takiej jak wykonanie oryginalnego backupu na dysk).

32) Oprogramowanie backupowe musi mieć możliwość klonowania zadań backupowych między dowolnym mediami, minimum:
    a) de-duplikacyjnymi
    b) dyskowymi (CIFS, NFS)
    c) taśmowymi
    d) obiektowymi (S3).
33) Oprogramowanie backupowe musi zapewniać różny czas ważności danych na podstawowym nośniku i nośniku zawierającym kopię (replika backupu). Definicja czasu przechowywania kopii (repliki) musi być możliwa w momencie definiowania zadania duplikacji / klonowania zarówno z interfejsu graficznego jak i z wiersza poleceń (ang. Command Line Interface, CLI).
34) Oprogramowanie backupowe musi wspierać multiplexing w procesie klonowania / duplikacja danych na nośniki taśmowe.
    Oznacza to, że w przypadku jednoczesnego klonowania/duplikacji 20 zadań backupowych z de-duplikatora na pojedynczy napęd taśmowy, wszystkie 20 klonowane/duplikowane zadania musi być jednocześnie w tym samym czasie zapisywane na pojedynczy napęd taśmowy.
35) Oprogramowanie backupowe musi pozwalać na backup systemu plików:
    a) pełny
    b) różnicowy
    c) inkrementalny.
36) Oprogramowanie backupowe musi pozwalać na łączenie backupów pełnych i inkrementalnych w jeden pełny backup. Proces ten musi być niewidoczny dla systemu plików którego dotyczą backupy pełne i inkrementalne. Proces odtworzenia danych z połączonego backupu pełnego i inkrementalnego musi identyczny z odtworzeniem danych z normalnie wykonanego backupu pełnego w kontekście zarówno:
    a) zarządzania
    b) wydajności.
37) Łączenie backupów pełnych i inkrementalnych musi odbywać się przez oferowane urządzenie de-duplikacyjne. Jedynie zarządzenie (start, kalendarz łączenia) procesem łączenia backupów pełnych i inkrementalnych musi odbywać się przez aplikację backupową.
38) Oferowane rozwiązanie backupowe musi pozwalać na wymuszenie blokady skasowania backupów na oferowanym urządzenie de-duplikacyjnym. Na przykład blokada skasowania backupu przez 15 dni oznacza, że:
    a) Przez 15 dni nikt (również żaden z administratorów) nie może usunąć backupu
    b) Przez 15 dni nikt (również żaden z administratorów) nie może zmienić backupu
    c) Przez 15 dni nikt (również żaden z administratorów) nie może zmienić czasu blokady backupu
39) Blokada przed skasowaniem backupu musi być bezwzględna (ang. compliance). Nie może być możliwości cofnięcia blokady jakimikolwiek metodami.
40) Blokada backupu musi rozpocząć się bezpośrednio po zakończeniu wykonywania tego backupu.
41) Blokada backupu musi być możliwa do ustawienia dla każdego zadania backupowego, musi być możliwość ustawienia innego czasu blokady dla różnych zadań backupu.
42) Blokada backupu musi być możliwa dla minimum wszystkich następujących backupów:
    a) backup plikowy z systemów operacyjnych co najmniej: Linux / Windows / Unix
    b) backup obrazów maszyn wirtualnych z zaoferowanego oprogramowania do wirtualizacji zasobów serwerowych i ich mocy obliczeniowej
    c) backup wspieranych baz danych.

43) Oprogramowanie backupowe musi pozwalać na zatrzymanie procesu backupu oraz jego wznowienie od momentu zatrzymania.
44) W przypadku nieudanego backupu dla systemu plików (na przykład zerwanie łącza), oprogramowanie backupowe musi pozwalać na wznowienie backupu od ostatnio poprawnie zbackupowanego:
    a) katalogu
    b) pliku.
45) W przypadku awarii fragmentu taśmy, oprogramowanie backupowe musi odtworzyć całość plików, które znajdują się na nieuszkodzonej części nośnika.
46) W konsoli oprogramowania backupowego musi być możliwość definiowania ważności danych (backupów) na podstawie kryteriów czasowych (dni, miesiące, lata). Po okresie ważności backupy musza być automatycznie usuwane.
47) Oprogramowanie musi umożliwiać kopię zapasową:
    a) pojedynczych plików
    b) całych systemów plików
    c) baz danych w trakcie ich normalnej pracy
    d) ustawień wykorzystywanego lub planowanego do wykorzystania w projekcie przez Zamawiającego systemu operacyjnego Windows
    e) całych obrazów maszyn wirtualnych systemu z zaoferowanego oprogramowania do wirtualizacji zasobów serwerowych i ich mocy obliczeniowej.
48) Oprogramowanie backupowe musi wspierać (wymagane wsparcie producenta) posiadane i wykorzystywane przez Zamawiającego lub planowane do wykorzystania w projekcie przez Zamawiającego następujące systemy operacyjne: Windows (także Microsoft Cluster), Linux (Red Hat, SUSE, Oracle Linux, CentOS), Solaris.
49) Oprogramowanie backupowe musi wspierać (wymagane wsparcie producenta) backup online następujących posiadanych i wykorzystywanych przez Zamawiającego lub planowanych do wykorzystania w projekcie przez Zamawiającego aplikacji i baz danych: MS Exchange, MSSQL, Oracle, Oracle MySQL, PostgreSQL, MongoDB.
50) W przypadku baz danych system musi mieć wbudowaną możliwość inicjalizacji backupu określonym zdarzeniem: np. ilością logów, czasem który upłynął od ostatniego zdarzenia lub innym zdarzeniem zdefiniowanym przez użytkownika.
51) Dla posiadanych i wykorzystywanych przez Zamawiajacego lub planowanych do wykorzystania w projekcie przez Zamawiającego baz danych MSSQL musi być możliwość inicjowania backupów przez administratora MSSQL przy spełnieniu wszystkich poniższych wymagań:
    a) backup jest wykonywany przez oferowane oprogramowanie backupowe
    b) inicjowanie backupu z graficznego interfejsu będącego częścią MSSQL Management Studio
    c) możliwość wyboru backupu pełnego, różnicowego
    d) backup inicjowany przez administratora MSSQL nie może wymagać kontaktu z administratorem oferowanego rozwiązania backupowego.
52) Dla posiadanych i wykorzystywanych przez Zamawiajacego lub planowanych do wykorzystania w projekcie przez Zamawiającego baz danych MSSQL musi być możliwość odtworzenia backupów przez administratora MSSQL przy spełnieniu wszystkich poniższych wymagań:
    a) odtworzenie dowolnego backupu wykonanego przez oferowane rozwiązanie backupowe
    b) zarządzanie odtwarzaniem z graficznego interfejsu będącego częścią MSSQL Management Studio
    c) możliwość odtworzenia do dowolnego punktu w czasie wybranego przez administratora MSSQL w ramach przechowywanych przez oferowane oprogramowanie backupowe logów MSSQL

d) odtworzenie bazy danych przez administratora MSSQL nie może wymagać kontaktu z administratorem oferowanego rozwiązania backupowego.

53) Oferowane rozwiązanie backupowe musi integrować się funkcjonalnością FRA (Fast Recovery Area) posiadanych i wykorzystywanych przez Zamawiajacego lub planowanych do wykorzystania w projekcie przez Zamawiającego baz danych Oracle. Musza być spełnione wszystkie poniższe funkcjonalności:
    a) administrator Oracle wykonuje backupy narzędziami RMAN do przestrzeni FRA
    b) oferowane rozwiązanie backupowe automatycznie kopiuje backupy z przestrzeni Oracle FRA na media zarządzane przez oferowane rozwiązanie backupowe.
    c) definiowanie parametrów zadania kopiowania backupów przestrzeni FRA na media zarządzane przez oferowane rozwiązanie backupowe z poziomu interfejsu graficznego
    d) odtworzenie danych możliwe przez administratora Oracle bez kontaktu z administratorem oprogramowania backupowego
    e) w procesie odtwarzania, administrator Oracle nie musi wskazywać miejsca, gdzie znajdują się odtwarzane dane (przestrzeń FRA, media oferowanego rozwiązania backupowego).
54) Oprogramowanie backupowe musi być zarządzane z jednego miejsca poprzez jedną centralną konsolę zarządzającą
55) Konsola oprogramowania backupowego musi umożliwiać definiowanie polityk backupowych obejmujących całość cyklu życia kopii zapasowej.
    W szczególności musi być możliwość zdefiniowania polityki backupowej, która dla dowolnej liczby zabezpieczanych systemów (zadań backupowych) wymusza:
    a) lokalny backup na oferowane medium de-duplikacyjne z retencją miesięczną
    b) replikę zmian do medium de-duplikacyjnego w zdalnej lokalizacji (retencja 60 dni) replikacja odbywa się między urządzeniami de-duplikacyjnymi
    c) replikacja backupu z lokalnego medium de-duplikacyjnego na medium taśmowe (retencja 5 lat)
    d) replikacja backupu ze zdalnego medium de-duplikacyjnego na medium obiektowe (S3).
    Całość powyższych operacji musi być możliwa do zdefiniowania jako pojedyncza polityka backupowa definiowana z poziomu interfejsu graficznego oprogramowania backupowego przy pomocy kreatora (ang. wizard).
    Polityka musi mieć możliwość uruchomienia dla dowolnej liczby serwerów / zadań backupowych.
    Operacje opisane w a) do c) (duplikaty / klony) muszą mieć możliwość zdefiniowania opóźnienia rozpoczęcia wykonywania celem wykonania ich po oknie backupowym (duplikaty / klony nie obciążają wówczas mediów backupowych w trackie okna backupowego).
    Administrator backupu musi mieć możliwość z poziomu interfejsu graficznego głównej konsoli oprogramowania backupowego odtworzenia dowolnej danych z dowolnych z powyższych kopii (1-4).
56) Rozwiązanie backupowe musi mieć możliwość odtworzenia plików na docelową maszynę z poziomu centralnej konsoli systemu backupowego. Nie może być wymagane logowanie się na odtwarzaną maszynę celem odtworzenia danych z systemu backupowego.
57) Musi istnieć możliwość odtworzenia danych z:
    a) zabezpieczanego serwera / komputera
    b) konsoli systemu backupowego.
58) Dla zaoferowanego środowiska wirtualizacji mocy obliczeniowej oprogramowanie backupowe musi umożliwiać następujące typy backupu:
        a) backup pojedynczych plików i baz danych z maszyny wirtualnej ze środka maszyny wirtualnej

b) backup całych maszyn wirtualnych (obrazów, plików reprezentujących wirtualną maszynę). W trakcie backupu odczytowi z systemu dyskowego mają podlegać tylko zmienione bloki wirtualnych maszyn
c) backup tylko wybranych dysków maszyny wirtualnej (wybranych plików systemu do wirtualizacji)
d) w trakcie backupu odczytowi z systemu dyskowego mają podlegać tylko zmienione bloki wirtualnych maszyn
e) Wszystkie backupy obrazów maszyn wirtualnych muszą być wykonywane do medium backupowego przy pomocy technologii transferującej tylko zmienione bloki. Jednocześnie z punktu widzenia systemu backupowego musza to być backupy pełne. To znaczy z punktu widzenia systemu backupu muszą to być backupy identyczne z wykonywanym od zera pełnym backupem.
f) Wykonywanie backupu jak w punkcie b. i c. nie może wymagać bufora dyskowego na kopię obrazów maszyn wirtualnych.

Powyższe metody backupu maszyn wirtualnych muszą podlegać de-duplikacji ze zmiennym blokiem przed wysłaniem danych do medium de-dupikacyjnego zgodnie z wymaganiami dla de-duplikacji powyżej.
Powyższe metody backupu muszą być wbudowane w system backupu i być w pełni automatyczne bez wykorzystania skryptów/dodatkowych komend.

59) Rozwiązanie backupowe musi umożliwiać odtworzenie obrazów maszyn wirtualnych dostarczając następujące funkcjonalności:
a) odtworzenie całych maszyn wirtualnych musi wykorzystywać mechanizm w którym odtwarzane są tylko te bloki wirtualnej maszyny/dysku które uległy zmianie od ostatniego backupu
b) odtworzenie pojedynczych dysków maszyn wirtualnych musi wykorzystywać mechanizm w którym odtwarzane są tylko te bloki wirtualnej maszyny/dysku które uległy zmianie od ostatniego backupu
c) odtworzenie pojedynczych plików z backupu obrazu maszyny wirtualnej bez konieczności odtworzenia całej maszyny wirtualnej. Funkcjonalność musi być dostępna dla obrazów maszyn wirtualnych z zainstalowanym systemem operacyjnym co najmniej Windows oraz Linux.

Powyższe metody odtworzenia muszą być wbudowane w system backupu i być w pełni automatyczne bez wykorzystania skryptów/dodatkowych komend.

60) Rozwiązanie backupowe musi umożliwiać uruchomienie maszyny wirtualnej bezpośrednio z medium backupowego bez konieczności odtwarzania (ang. Instant Access).
61) Z pojedynczego backupu maszyny wirtualnej musi być możliwość jednoczesnej realizacji wszystkich poniższych funkcjonalności:
a) odtworzenie całej maszyny wirtualnej
b) odtworzenie pojedynczego dysku maszyny wirtualnej
c) odtworzenie pojedynczego pliku maszyny wirtualnej
d) uruchomienie maszyny wirtualnej bez odtwarzania (ang. Instant Access).
62) Skalowalność rozwiązania dla środowiska wirtualizacyjnego musi pozwalać na:
a) backup minimum 5000 maszyn wirtualnych w ramach pojedynczej instancji systemu backupu
b) pełny backup minimum 1000 maszyn wirtualnych backupowanych w ciągu godziny w ramach pojedynczej instancji systemu backupu.
63) Rozwiązanie backupowe musi umożliwiać backup i odtwarzanie równolegle, w tym samym czasie minimum 100 maszyn wirtualnych. Wykonywane równoległe backupy maszyn wirtualnych musza być backupami pełnymi przy odczycie tylko zmienionych bloków.

64) Rozwiązanie backupowe musi umożliwiać backup minimum 25 maszyn wirtualnych z pojedynczego serwera proxy (z pojedynczego serwera odczytującego obrazy maszyn wirtualnych). Wszystkie 25 sesji backupujących wirtualne maszyny musi odczytywać tylko zmienione bloki wykonując przy tym pełny backup.
65) Rozwiązanie backupowe musi pozwalać na podłączenie do wielu instancji oprogramowania do zarządzania klastrem wirtualizacyjnym.
66) Rozwiązanie backupowe musi pozwalać na odtworzenie maszyny wirtualnej pomiędzy różnymi instancjami oprogramowania do zarządzania klastrem wirtualizacyjnym zdefiniowanymi w oprogramowaniu backupowym. Z poziomu interfejsu graficznego oprogramowania backupowego, w kreatorze odtwarzania, musi być możliwość wyboru maszyny wirtualnej znajdującej się w jednej instancji i możliwość wyboru innej instancji do którego maszyna wirtualna jest odtwarzana.
67) Administrator aplikacji backupowej musi mieć możliwość odtworzenia maszyny wirtualnej z GUI (graficzna konsola) dla każdego z poniższych sposobów:
    a) odtworzenie całej maszyny wirtualnej
    b) odtworzenie pojedynczego dysku z wcześniej zrobionej kopii całej maszyny wirtualnej
    c) odtworzenie plików / katalogów z backupu obrazów maszyny wirtualnej
    d) uruchomienie maszyny wirtualnej z medium backupowego bez odtwarzania
    e) naprawienie maszyny wirtualnej na obecnej instancji – odtworzenie tylko zmienionych bloków od ostatniego backupu.

    Wszystkie powyższe możliwości muszą być dostępne w postaci graficznych kreatorów.
68) Administrator (właściciel) danej maszyny wirtualnej musi mieć możliwość samodzielnego (bez konieczności kontaktu z administratorem backupu czy tez administratorem środowiska wirtualizacyjnego) odtworzenia pojedynczych plików z dowolnego backupu obrazu jego maszyny wirtualnej z poziomu interfejsu graficznego dostępnego ze środka maszyny wirtualnej – dostarczanego przez oprogramowanie backupowe.
69) Oprogramowanie backupowe musi zawsze przechowywać pełne backupy obrazów maszyn wirtualnych dla każdej wykonanej w przeszłości kopii zapasowej.
    Każdy backup obrazu maszyny wirtualnej musi być backupem pełnym.
70) Rozwiązanie backupowe musi pozwalać na automatyczne polityki backupowe dla np. folderu. Oznacza to, że dodanie maszyny wirtualnej do folderu spowoduje automatyczne backupowanie dodanej maszyny wirtualnej zgodnie z polityka zdefiniowana dla folderu.
71) Wymagane jest by w środowisku wirtualizacyjnym oprogramowanie backupowe pozwalało na automatyczne dodawanie maszyn wirtualnych do odpowiednich polityk na podstawie każdej z poniższych możliwości:
    a) automatyczne dodanie do odpowiednich polityk backupowych wszystkich maszyn wirtualnych zawierających w nazwie maszyny wirtualnej podany tekst
    b) automatyczne dodanie do odpowiednich polityk backupowych wszystkich maszyn wirtualnych znajdujących się we wszystkich folderach zawierających w nazwie podany tekst
    c) automatyczne dodanie do odpowiednich polityk backupowych wszystkich maszyn wirtualnych których tag zawiera podany tekst.

    Automatyczne dodanie do odpowiednich polityk backupowych wszystkich maszyn wirtualnych znajdujących się na wszystkich magazynach danych które w nazwie zawierają podany tekst.
72) Oprogramowanie backupowe musi automatycznie rozpoznawać nowe, utworzone maszyny wirtualne i umieszczać je w odpowiednich politykach backupowych. Wymagana jest możliwość konfiguracji poniższego scenariusza:
    a) wszystkie nowo utworzone maszyny wirtualne zawierające w nazwie frazę „krytyczna” muszą być backupowane automatycznie co godzinę

b) wszystkie nowo utworzone maszyny wirtualne zawierające w nazwie frazę „produkcja” muszą być backupowane automatycznie raz na dzień
c) pozostałe maszyny wirtualne mają być backupowane raz na tydzień

Powyższe rozwiązanie backupowe musi wykonywać się samoczynnie, bez jakichkolwiek akcji ze strony administratora backupu, administratora środowiska wirtualizacyjnego czy też jakiekolwiek innej osoby.

73) Wymagane jest by oprogramowanie backupowe pozwalało na automatyczne usuwanie maszyn wirtualnych z polityk backupowych w tym samym momencie, w którym maszyna jest usunięta z środowiska wirtualizacyjnego.
Jednocześnie dotychczasowo wykonane kopie zapasowe muszą być przechowywane zgodnie z retencją celem możliwości odtworzenia uśniętej wcześniej maszyny wirtualnej.
74) Rozwiązanie backupowe musi umożliwiać zdefiniowanie polityk backupowych dostępnych dla administratora systemu wirtualizacyjnego z poziomu instancji oprogramowania do zarządzania klastrem wirtualizacyjnym. Administrator ten musi mieć możliwość przyporządkowania nowo tworzonych maszyn wirtualnych do polityk backupowych.
75) Całość informacji o backupach środowiska wirtualizowanego musi być przechowywana centralnie, na serwerze backupu.
76) Maszyna wirtualna zbackupowana przez serwer pośredniczący, musi mieć możliwość odtworzenia przez dowolny inny serwer pośredniczący.
77) Oprogramowanie backupowe musi samo dystrybuować zadania backupu/odtwarzania obrazów maszyn wirtualnych pomiędzy dostępne serwery pośredniczące.

12. 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.

12.1. 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.

12.2. 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 szeregowe, 3 porty równoległe i 20 urządzeń USB
   h) wspierać następujące posiadane i wykorzystywane przez Zamawiajacego lub planowane do wykorzystania w projekcie przez Zamawiającego systemy operacyjne Windows Server 2016, Windows Server 2019, , Windows 10, SLES 12, SLES 11, RHEL 8, REHL 7, Solaris 11, Debian, CentOS, FreeBSD, Ubuntu, Oracle Linux
   i) umożliwiać przydzielenie łącznie większej ilości pamięci RAM dla maszyn wirtualnych niż fizyczne zasoby RAM serwera, na którym maszyny te są umieszczone
   j) umożliwiać 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 posiadanego i wykorzystywanego lub planowanego do wykorzystania w projekcie przez Zamawiającego 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
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 przestojów 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 obsługiwania 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 zaoferowane 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 posiadanym i wykorzystywanym przez Zamawiajacego lub planowanym do wykorzystania w projekcie przez Zamawiającego 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.

12.3. 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 **12.2**).
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
      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 przestojów 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 wykorzystywanego lub planowanego do wykorzystania w projekcie przez Zamawiającego 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 wykorzystywanego lub planowanego do wykorzystania w projekcie przez Zamawiającego 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

12.4. 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 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 posiadane i wykorzystywane przez Zamawiajacego lub planowane do wykorzystania w projekcie przez Zamawiającego: 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) być zgodne z oferowanym w ramach tego samego postępowania oprogramowaniem do wirtualizacji przestrzeni dyskowej (opisanego w punkcie **12.7** i **12.8**) i umożliwiać zarządzanie wirtualną przestrzenią dyskową SDS (ang. Software Defined Storage)
h) 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
i) 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
j) umożliwiać jednoczesną aktualizację oprogramowania na wielu dostarczanych wirtualizatorach
k) 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
l) 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
m) 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 dostępów administracyjnych do środowiska.

12.5. Oprogramowanie do wirtualizacji sieci w wersji podstawowej

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 niezwirtualizowanym zdefiniowanego za pomocą technologii VLAN
g) zapewniać funkcjonalność wirtualnego routera wspierającego protokół routingu BGP.
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 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.

Usunięte: Routing statyczny oraz BGP musi być możliwy do wykonania poprzez tunel GRE

12.6. Oprogramowanie do wirtualizacji sieci w wersji rozszerzonej

1) Zaoferowane oprogramowanie do wirtualizacji sieci w wersji rozszerzonej musi spełniać wszystkie wymagania z wersji podstawowej (opisanej w punkcie **12.5**).
2) Zaoferowane oprogramowanie do wirtualizacji sieci w wersji rozszerzonej dodatkowo musi:
   a) zapewniać funkcjonalności rozkładania i równoważenia ruchu (ang. Load-Balancing) pracującej w warstwach 4 do 7 modelu ISO/OSI. Funkcjonalność musi zapewniać

następujące mechanizmy utrzymywania sesji (ang. SessionPersistent), minimum : adres źródłowy, cookie,

Usunięte: , SSL ID oraz SessionID

b) umożliwiać natywną integrację z minimum dwoma produktami firm trzecich oferującymi rozwiązania typu Next Generation Firewall w warstwie siódmej modelu ISO/OSI, w celu dodatkowej filtracji i inspekcji ruchu
c) umożliwiać natywną integrację z produktami firm trzecich oferującymi rozwiązania klasy antywirus / antymalware w postaci bezagentowej. Poprzez bezagentowość zamawiający rozumie instalacje na poziomie wirtualizatora (hypervisora) serwerów, bez ingerencji w maszynę wirtualną
d) posiadać funkcję łączenia segmentów sieci w warstwie drugiej modelu ISO/OSI (ang. bridge) dla VLAN i VXLAN poprzez zastosowanie fizycznego przełącznika
e) posiadać możliwość tworzenia reguł bezpieczeństwa uwzględniających nazwy użytkowników, poprzez integrację z posiadaną i wykorzystywaną przez Zamawiajacego lub planowaną do wykorzystania w projekcie przez Zamawiającego Microsoft Active Directory z obsługą selektywnej synchronizacji
f) posiadać funkcjonalność identyfikacji posiadanych i wykorzystywanych lub planowanych do wykorzystania w projekcie przez Zamawiającego typu aplikacji co najmniej MySQL, MS Active Directory, HTTP, DNS, DHCP, TLS na poziomie sieciowym modelu ISO/OSI w warstwach 5 - 7, a następnie móc wykorzystać wynik identyfikacji w rozproszonym, wewnętrznym firewall w celu kontroli dostępu nie tylko na poziomie adresów IP oraz portów, ale również w połączeniu adresów IP, portów oraz zidentyfikowanej aplikacji
g) w ramach inspekcji warstwy 7 modelu ISO/OSI, mieć funkcjonalność równoważenia ruchu (ang. Load Balancer) oraz oferować funkcję blokowania i modyfikacji URL
h) w przypadku rozwiązania równoważenia ruchu (ang. Load Balancer) musi:
    i) posiadać możliwość dodawania do nagłówka znacznika XFF (X-Fowarder-For)
    ii) być zarządzana oraz instalowana w ramach jednego interfejsu graficznego (pojedynczej konsoli) w ramach zaoferowanego oprogramowania
i) pozwalać na realizację równoważenia obciążenia (ang. Load balancing) w formie scentralizowanej, to znaczy poprzez instalację i procesowanie ruchu na dedykowanym komponencie - na serwerze fizycznym (bare metal) lub maszynie wirtualnej
j) posiadać funkcjonalność typu Identity Firewall umożliwiające obsługę sesji użytkowników na pulpitach wirtualnych (VDI) oraz serwerach aplikacji (RDSH) współdzielących pojedynczy adres IP
k) umożliwiać włączenie funkcjonalności rozproszonego Systemu Wykrywania Włamań (ang. Intrusion Detection System) za pomocą licencji instalowanych na serwerach wirtualizacyjnych i umożliwiającego realizację wykrywania włamań za pomocą dedykowanych sygnatur ataków
l) musi posiadać funkcjonalność wsparcia mechanizmu VRF w obrębie wirtualizacji sieci.

12.7. Oprogramowanie do wirtualizacji przestrzeni dyskowej w wersji podstawowej

1) Zaoferowane oprogramowanie do wirtualizacji przestrzeni dyskowej w wersji podstawowej musi:
    a) umożliwiać zbudowanie współdzielonej przestrzeni dyskowej w oparciu o dyski wewnętrzne serwerów fizycznych. System powinien wspierać następujące konfiguracje:
        i) hybrydowa w oparciu o dyski SSD i HDD
        ii) „allflash" w oparciu o dyski SSD (SAS/SATA/NVMe)

b) w przypadku posiadania wyłącznie dysków SSD, zaoferowane oprogramowanie musi zapewniać możliwość optymalizacji wydajności poprzez wbudowaną funkcjonalność „cache-owania” operacji zapisu
c) w przypadku posiadania dysków mieszanych (tj. SSD i HDD) musi zapewniać możliwość optymalizacji wydajności poprzez wbudowaną funkcjonalność „cache-owania" operacji zapisu i odczytu
d) wspierać technologie NVMe i "cache-owanie" operacji zapisu z wykorzystaniem dysków NVMe
e) umożliwiać konfigurację serwerów fizycznych klasy all-NVMe
f) w przypadku zastosowania dysków NVMe, musi wspierać ich wymianę w trybie hot-plug dla dodawania i wyjmowania dysków w trybie "na gorąco". Taka funkcjonalność musi być dostępna dla minimum dwóch producentów serwerów obecnych na rynku
g) wspierać "cache'owanie" operacji zapisu z wykorzystaniem dysków Intel Optane
h) posiadać możliwość aktualizacji i kontroli wersji oprogramowania do wirtualizacji pamięci masowej w ramach klastra serwerów z poziomu centralnej konsoli zarządzającej. Dodatkowo centralna konsola zarządzająca musi posiadać funkcjonalność aktualizacji firmware komponentów serwera fizycznego (dyski, kontrolery, karty sieciowe) z poziomu konsoli zarządzającej wirtualizatora. Konsola zarządzająca musi mieć możliwość automatycznej weryfikacji, czy zainstalowane komponenty serwera posiadają rekomendowaną wersję sterowników i firmware, eliminując ryzyko pracy na nieaktualnych wersjach. Taka funkcjonalność powinna być dostępna dla minimum dwóch producentów serwerów na rynku
i) zapewniać możliwość zmniejszania lub zwiększenia przestrzeni dyskowej (odjęcie lub dodanie pojedynczego dysku, odjęcie lub dodanie serwera fizycznego) w sposób niewymagający przestoju i przerwy w dostępie do działających na zmienianym środowisku maszyn wirtualnych
j) posiadać integracje funkcji takich jak konfiguracja, zarządzanie i monitoring przestrzeni dyskowej z centralną konsolą zarządzającą platformą wirtualizacyjną zaoferowaną w ramach tego postępowania, dodatkowo nie może w żaden sposób ograniczać lub niwelować żadnej funkcjonalności platformy wizualizacyjnej między innymi w warstwie mechanizmów niezawodnościowych, wydajnościowo-optymalizacyjnych jak i zarządzania.
k) zapewniać możliwość obsługiwania dysków wirtualnych maszyn do rozmiaru co najmniej 60 TB
l) zapewniać funkcjonalność konfigurowalnych mechanizmów zabezpieczania danych na wypadek awarii sprzętowej w ramach lokalizacji lub szafy rack w taki sposób, aby poszczególne kopie dysków maszyny wirtualnej nie były umieszczane na hostach w ramach tej samej szafy rackowej lub w ramach tej samej lokalizacji
m) posiadać, na oficjalnej stronie zaoferowanego oprogramowania, listę wspieranych i certyfikowanych konfiguracji serwerowych
n) nie wprowadzać ograniczenia rozbudowy przestrzeni dyskowej w oparciu jedynie o serwery fizyczne producenta wykorzystane na etapie inicjalizacji oprogramowania. W przypadku rozbudowy o kolejne serwery fizyczne rozwiązanie nie może wprowadzać wymogu, aby w dostarczanych do rozbudowy serwerach fizycznych, wymagana była instalacja komponentów sprzętowych oferowanych tylko przez jednego producenta/dostawcę (np. dyski, adaptery, specjalizowane karty i kontrolery)
o) zapewniać funkcjonalność rozbudowy i skalowania zarówno mocy obliczeniowej, pojemności przestrzeni cache, jak i pojemności przestrzeni dyskowej (w ramach

istniejącej infrastruktury serwerów fizycznych) bez konieczności dodawania kolejnych serwerów fizycznych

p) zapewniać możliwość rozbudowy oferowanej przestrzeni dyskowej poprzez dodanie pojedynczego dysku lub dodanie jednego lub więcej serwera fizycznego w sposób niewymagający przestoju i przerwy w dostępie do działających usług wirtualnych
q) zapewniać możliwość ochrony danych przed utratą ich integralności za pomocą weryfikacji sum kontrolnych. Suma kontrolna musi być liczona w momencie wykonania przez maszynę wirtualną operacji zapisu już na poziomie wirtualizatora
r) umożliwiać zarządzanie warstwą wirtualizacji mocy obliczeniowej i pamięci masowej bez potrzeby otwierania dostępu poprzez protokół SSH
s) umożliwiać utworzenie wysokodostępnego klastra przestrzeni dyskowej w scenariuszu dla tzw. „oddziału zdalnego", zbudowanego w oparciu o min. 2 serwery fizyczne i min. dwie lokalizacje. Architektura systemu musi mieć możliwość dołączania kolejnych lokalizacji „oddziałów zdalnych" w ilości min. 64
t) zapewniać natywną integrację (bez skryptów i/lub wtyczek programowych (ang. plugin)) z dostarczonym w ramach tego postępowania oprogramowaniem do zarządzania klastrem wirtualizacyjnym opisanym w punkcie **12.4** pracującym w oparciu o HTML5.
u) zapewniać możliwość tworzenia i konfigurowania polityk niezawodnościowych, wydajnościowych i pojemnościowych przypisanych z granulacją na poziomie dysków maszyn wirtualnych tak aby można było określić:
   i) liczbę serwerów fizycznych, które mogą ulec awarii jednocześnie
   ii) liczbę operacji wejścia/wyjścia (I/O)
   iii) użycie funkcji „thin-provisioning”
   iv) użycie funkcji „stripe”
v) posiadać możliwość udostępniania przestrzeni dyskowej również dla fizycznych systemów operacyjnych w oparciu o technologię iSCSI i umożliwiać zarządzanie dostępnością, pojemnością i wydajnością bez konieczności wyłączana tych systemów
w) posiadać interfejs programistyczny (API) umożliwiający automatyzowanie wdrażania lub modyfikacji konfiguracji systemu
x) umożliwiać funkcjonalność automatycznego odzyskiwania pojemności dyskowej (przestrzeni dyskowej) zwolnionej na poziomie systemu operacyjnego tj. TRIM/UNMAP (ang. storage space reclamation)
y) pozwalać na wykorzystanie protokołu RDMA
z) posiadać opcję wykorzystania natywnego dostawcy kluczy szyfrujących, jak również wykorzystania zewnętrznych dostawców
aa) umożliwiać konsoli zarządzającej na wykrywanie ostrzeżeń dotyczących komponentów sprzętowych serwera (poprzez wtyczkę – plugin) i w zależności od stopnia ich ważności musi podejmować akcje zapobiegające nieplanowanym awariom
bb) mieć możliwość włączania na żądanie i wyłączania na żądanie dostępnej w ramach funkcjonalności zaoferowanego oprogramowania dedupikacji i kompresji
cc) zapewniać mechanizmy optymalizacji wykorzystania przestrzeni dyskowych (ang. ereasure coding) dla RAID 5 i RAID 6 konfigurowane z dokładnością do dysku maszyny wirtualnej.

2) Każdy serwer fizyczny, na którym zostanie zainstalowane zaoferowane oprogramowane, musi dostarczać zarówno moc obliczeniową do klastra (CPU i RAM) jak również przestrzeń dyskową definiowaną programowo (ang. Software Defined Storage). Powyższa funkcjonalność musi dać możliwość utworzenia przestrzeni dyskowej złożonej z minimum 30 hostów.

3) Wymagane jest wsparcie dla min. 4 niezależnych producentów sprzętu serwerowego dostępnego na terenie Unii Europejskiej.
4) Platforma zarządzania cyklem życia produktu musi wspierać co najmniej 4 różnych producentów serwerów.

12.8. Oprogramowanie do wirtualizacji przestrzeni dyskowej w wersji rozszerzonej

1) Zaoferowane oprogramowanie do wirtualizacji przestrzeni dyskowej w wersji rozszerzonej musi spełniać wszystkie wymagania z wersji podstawowej (opisanej w punkcie **12.7**).
2) Zaoferowane oprogramowanie do wirtualizacji przestrzeni dyskowej w wersji rozszerzonej musi:
   a) umożliwiać rozciągnięcie zdefiniowanej przestrzeni dyskowej pomiędzy dwiema fizycznymi lokalizacjami oddalonymi z czasem RTT (ang. Round Trip Time) wynoszącym nie więcej niż 5ms dla warstw sieci L2 lub L3 w ten sposób, by zapis danych następował synchronicznie do obu lokalizacji
   b) zapewniać możliwość tworzenia i konfigurowania polityk niezawodnościowych, wydajnościowych i pojemnościowych przypisanych z granulacją na poziomie dysków maszyn wirtualnych tak, aby można było określić:
      i) liczbę serwerów fizycznych, które mogą ulec awarii jednocześnie
      ii) liczbę operacji I/O,
      iii) użycie funkcji „thin-provisioning”
      iv) użycie funkcji „stripe”
      v) replikację lub jej brak w ramach rozciągniętego klastra
   c) posiadać konfigurowalne mechanizmy zabezpieczania danych na wypadek awarii jednego z dwóch centrów danych (klaster rozciągnięty) w taki sposób, aby poszczególne kopie maszyn wirtualnych były umieszczane zarówno na hostach w ramach tej samej lokalizacji (lokalna protekcja) oraz w ramach dwóch lokalizacji (protekcja na poziomie lokalizacji)
   d) umożliwiać szyfrowanie przestrzeni dyskowej przydzielonej do serwerów wirtualnych, szyfrowanie nie może być realizowane poprzez dyski samo szyfrujące (ang. Self Encrypting Drives)
   e) posiadać możliwość uruchomienia usługi NFS w wersji 3.1 oraz 4, usługa ta musi być zintegrowana z warstwą wirtualizacji oraz uruchamiania i zarządzana wyłącznie z poziomu centralnej konsoli zarządzającej klastrem wizualizacyjnym bez potrzeby manualnej instalacji dodatkowych komponentów zewnętrznych
   f) zapewniać możliwość tworzenia i konfigurowania polityk niezawodnościowych, wydajnościowych i mechanizmy optymalizacji wykorzystania przestrzeni dyskowych (ang. ereasure coding) dla RAID 5 I RAID 6 konfigurowane granularnie z dokładnością do zasobów NFS/NFS share
   g) funkcjonalność usługi NFS w zaoferowanym oprogramowaniu musi współpracować z Kubernetes CSI driver (Container Storage Interface) w ten sposób, że zasoby NFS tworzone są i usuwane automatyczne z poziomu kontenerów
   h) umożliwiać montowanie zdalnych magazynów danych utworzonych w infrastrukturze SDS (and. Software-defined storage) do istniejącego wirtualizatora, bez potrzeby licencjonowania tegoż wirtualizatora.

12.9. Oprogramowanie do automatyzacji zadań w ramach środowiska zwirtualizowanego

1) Zaoferowane oprogramowanie do automatyzacji zadań w ramach środowiska zwirtualizowanego musi:

a) posiadać portal typu „Self-Service" do automatycznego tworzenia i uruchamiania:
   i. wirtualnych systemów operacyjnych
   ii. platform aplikacyjnych
   iii. całych zestawów/systemów maszyn wirtualnych
b) posiadać interfejs graficzny Ul (ang. user interface), który:
   i. musi być dostępny poprzez przeglądarkę internetową
   ii. musi być wykonany w technologii opartej o HTML5
   iii. mieć możliwość katalogowania widoku poszczególnych typów usług według własnego wzorca
c) posiadać możliwość modyfikacji właściwości obiektów w katalogu (w tym co najmniej konfiguracji wirtualnego zasobu: ilość CPU, pamięć RAM, przestrzeń dyskowa, sieć), zarówno przed „provisioningiem" usługi jak i po „provisioningu"
d) za pomocą dodatkowej integracji, oferować w ramach katalogu usług informacje o kosztach danej usługi – modyfikowana na bieżąco w zależności od konfiguracji wirtualnego sprzętu (np. ilość instancji, ilość pamięci RAM, ilość CPU)
e) prezentować informacje w postaci wykresów o kluczowych metrykach maszyny wirtualnej, wytworzonej w ramach ustalonego procesu co najmniej takich jak CPU, pamięć RAM, liczbę operacji wejścia/wyjścia (IOPS), sieć
f) umożliwiać modyfikację wirtualnego sprzętu przypisanego do obiektu po "provisioningu" danego obiektu z katalogu
g) posiadać zestaw wbudowanych procesów/czynności automatyzacji dostarczania usług wraz z możliwością ich edycji oraz możliwość zmiany konfiguracji i tworzenia nowych kroków w procesie cyklu życia konkretnej usługi
h) informować o statusie usługi w czasie rzeczywistym, wymagane statusy to co najmniej: usługa zaakceptowana, zakolejkowana, odrzucona, w trakcie akceptacji. Dodatkowo zaoferowane oprogramowanie musi mieć możliwość wysłania informacji poprzez pocztę elektroniczną o zmianie statusu usługi
i) posiadać możliwość definiowania sieci wirtualnych, które łączą maszyny wirtualne w ramach zarządzanej platformy – rozwiązanie musi wspierać natywnie nie mniej niż dwa rozwiązania typu SDN
j) posiadać możliwość definiowania sieci wewnętrznych jak i sieci zewnętrznych połączonych do sieci fizycznej pozwalającej na komunikację np. do Internetu za pomocą NAT – rozwiązanie musi wspierać natywnie nie mniej niż dwa rozwiązania typu SDN, posiadać możliwość definiowania fizycznych zasobów (mocy obliczeniowej) oraz zmiany ich wielkości poprzez powiększenie lub pomniejszenie obiektu) bez wpływu na działanie usług – tj. obiekt musi być dostępny przez cały czas, podczas dokonywanych operacji
k) posiadać możliwość definiowania logicznych obiektów zawierających wiele wirtualnych elementów w tym wiele maszyn wirtualnych powiązanych ze sobą zależnościami, tak aby w rezultacie administrator systemu mógł stworzyć wielowarstwowy serwis (np. aplikacja CRM , loadbalance web front-end, middleware oraz sklastrowany back-end baz danych)

l) posiadać możliwość wyboru, które obiekty z katalogu mogą ulegać modyfikacji przez użytkownika końcowego, wymaga się aby lista obiektów była nie mniejsza niż:
   i. liczba wirtualnych procesorów
   ii. wielkość pamięci operacyjnej
   iii. ilość i wielkość dysków oraz typ wolumenu
   iv. ilość kart sieciowych i typy sieci
   v. czas dzierżawy
   vi. polityka archiwizacji
   vii. hasło administracyjne systemu operacyjnego,

   przy czym zmiana parametrów przez użytkownika musi umożliwiać włączenie mechanizmu dodatkowych akceptacji administracyjnych przy procesie uruchomienia serwisu

m) posiadać wsparcie dla dostarczanej platformy wizualizacyjnej
n) posiadać wsparcie dla realizacji modelu: "Projektuj usługę raz, wdrażaj gdziekolwiek"
o) możliwość rezerwacji zasobów fizycznych dla wybranych grup użytkowników oraz pełną kontrolę tych zasobów w obrębie wskazanej grupy użytkowników
p) mieć możliwość tworzenia wielu logicznych, izolowanych od siebie grup maszyn wirtualnych, określania dla nich zasobów fizycznych, grup użytkowników, wzorców usług, a także procesów tworzenia oraz zarządzania cyklem życia usług
q) integrować się z innymi systemami zewnętrznymi typu: CMDB, DNS, IPAM, Load Balancer, Servcie Desk, Monitoring, Web Services, Puppet, Chef, SaltStack jako gotowe lub napisane od początku w języku programowania wtyczki (plug-in). Efektem powyższej integracji musi być w pełni automatyczny proces tworzenia i zarządzania usługą niewymagający czynności ręcznych
r) umożliwiać tworzenie nowych usług wraz z określeniem ilości i rodzaju zasobów dostępnych dla danej usługi zarówno na etapie tworzenia jak i późniejszej rekonfiguracji danej usługi
s) posiadać jedno narzędzie do projektowania usługi opartej na systemie operacyjnym, aplikacjach, usługach sieciowych (tj. Load Balancing, Routing, Switching oraz tworzenia reguł bezpieczeństwa podczas provisioningu). W sieciowym aspekcie rozwiązanie musi mieć wsparcie dla mikrosegmentacji tj. filtrowania ruchu pomiędzy dowolnymi maszynami wirtualnymi również w obrębie tej samej sieci
t) wspierać natywnie nie mniej niż dwa rozwiązania typu SDN oraz:
   i. umożliwiać zbudowanie zunifikowanego Katalogu Usług dla aplikacji, infrastruktury i danych
   ii. posiadać interfejs typu „drag-drop" przeznaczony do tworzenia dowolnego wielowarstwowego serwisu na podstawie utworzonych wcześniej komponentów, aplikacji, systemów, sieci i polityk bezpieczeństwa oraz innych skryptów pomocnych w automatyzacji
u) umożliwiać graficzną edycję przebiegu procesu realizacji usług, definiowanie poszczególnych kroków oraz ich danych wejściowych i wyjściowych. Przebiegi procesów mogą być sekwencyjne lub składać się z wielu sekwencji zadań realizowanych równocześnie
v) mieć możliwość testowania zdefiniowanych procesów realizacji usług przy użyciu „debugger-a", który pozwala analizować postęp procesu krok po kroku ze śledzeniem przekazywanych danych
w) umożliwiać eksport/import zdefiniowanych procesów realizacji usług do/z pliku w celu przeniesienia definicji pomiędzy różnymi środowiskami

x) umożliwiać integrację z wykorzystywanym lub planowanym do wykorzystania w projekcie przez Zamawiającego MS Active Directory oraz Open LDAP i wieloma ich domenami w tym samym czasie
y) dawać możliwość użytkownikowi na wykonywania wszystkich operacji na swojej usłudze z jednej konsoli tj. Self-Service portalu bez konieczności posługiwania się innymi narzędziami administracyjnymi
z) posiadać możliwość granularnego zarządzania uprawnieniami dla poszczególnych użytkowników w zależności od pełnionej roli – przykładowe role: administrator, architekt usługi, architekt sieci, architekt aplikacji
aa) dostarczać mechanizmy monitorowania statusów zdarzeń, notyfikacji o tych zdarzeniach, umożliwiać śledzenie i kontrolę zmian w konfiguracji wszystkich usług za pomocą min. portalu Self-Service i powiadomień e-mail na zdefiniowany adres przez użytkownika/administratora systemu
bb) mieć możliwość zgłaszania przez administratora potrzeby odzyskania poszczególnych zasobów od użytkowników w przypadku ich niewłaściwego wykorzystywania
cc) udostępniać funkcjonalność zarządzania poprzez ustandaryzowany interfejs programistyczny (API).

12.10. Oprogramowanie do monitorowania i zarządzania platformą wirtualizacyjną

1) Zaoferowane oprogramowanie do monitorowania i zarządzania platformą wizualizacyjną musi:

a) uzyskiwać informacje na temat wydajności środowiska wirtualnego pod kątem zarządzania pojemnością
b) za pomocą wbudowanych inteligentnych algorytmów przewidywać trendy związane z pojemnością środowiska wirtualnego opartego na dostarczanej platformie wirtualizacyjnej
c) posiadać funkcjonalność dającą możliwość analizy środowiska wirtualnego pod kątem optymalizacji wykorzystania zasobów (CPU, pamięć RAM, zasoby dyskowe)
d) mieć możliwość tworzenia unikalnego zbioru obiektów korespondujących funkcjami z obiektami centrum danych (ang. Data Center), tzn. musi być możliwe grupowanie obiektów w logiczne zbiory, dla których będzie istniała możliwość informowania o alertach, pojemności, ryzykach zgromadzonych w zbiorze obiektów. Obiekty mogą pochodzić z różnych centrów danych objętych tym rozwiązaniem
e) mieć możliwość tworzenia unikalnego/dedykowanego profilu pojemności, tzn. będzie możliwe grupowanie obiektów z centrów danych w logiczne zbiory dla których będzie istniała możliwość informowania o alertach, pojemności, ryzykach zgromadzonych w zbiorze obiektów
f) posiadać funkcjonalność tworzenia scenariuszy prognozowanego obliczania pojemności na zasadzie "co jeśli" dla minimum „co jeśli dodamy kolejne maszyn wirtualne”. Rozwiązanie musi umożliwiać definiowanie poziomów buforów potrzebnych do zachowania wysokiej dostępności. Analiza pojemności musi odnosić się zarówno do średniego obciążenia środowiska, jak również do tzw. skoków obciążenia

g) posiadać rozwiązanie do generowania alertów na podstawie korelacji (wykrytych podczas monitorowania) anomalii i symptomów, a nie tylko pojedynczych monitorowanych metryk
h) posiadać funkcjonalność dostarczania informacji na temat rekomendowanych, przez wbudowany mechanizm w dostarczanym oprogramowaniu, działań mających na celu prawidłowe działanie dostarczanego środowiska
i) posiadać funkcjonalność obsługi zewnętrznych kolektorów logów i zdarzeń
j) posiadać funkcjonalność monitorowania i zgłaszania alertów na temat zgodności serwerów opartych na dostarczanym rozwiązaniu wirtualizacyjnym mocy obliczeniowej, z najlepszymi praktykami bezpieczeństwa organizacji takich jak ISO (International Organization for Standardization), CIS (Center of Internet Security)
k) posiadać bazę wiedzy eksperckiej, która będzie używana przez administratorów, jako źródło dobrych praktyk, sugestii, opisu typowych problemów i błędów związanych ze środowiskiem zwirtualizowanym
l) wizualizować w trybie online obciążenie środowiska wirtualnego
m) posiadać funkcjonalność graficznej prezentacji monitorowanych parametrów
n) posiadać funkcjonalność aktywnych map graficznych ukazujących elementy lub całe środowisko wirtualne bez konieczności korzystania z usługi wsparcia technicznego producenta do ich dodatkowego wytwarzania podczas używania oprogramowania
o) dokonywać automatycznej prognozy wykorzystania zasobów maszyn fizycznych na podstawie analiz zebranych danych, informacji pochodzących z modułu zarządzania cyklem życia maszyn wirtualnych (wbudowanego w zaoferowane oprogramowanie) oraz planów uruchomienia kolejnych serwerów wirtualnych
p) umożliwiać przeglądanie linii trendu monitorowanych parametrów
q) umożliwiać tworzenie raportów pojemnościowych dla monitorowanego środowiska, zarówno dla urządzeń wirtualnych jak i fizycznych, związanych z dostarczanym oprogramowaniem do wirtualizacji zasobów serwerowych i ich mocy obliczeniowej oraz fizycznymi zasobami dyskowymi poza środowiskiem wirtualnym
r) umożliwiać monitorowanie środowisk w czasie rzeczywistym (przeglądane informacje powinny ukazywać się w trybie rzeczywistym – dopuszczane jest maksymalne opóźnienie nie większe niż 5 minut)
s) prezentować w formie wykresów/tabel aktualne i historyczne dane dotyczące utylizacji zasobów takich jak CPU, pamięć RAM, zasoby dyskowe oraz interfejsy sieciowe dla każdego systemu operacyjnego
t) umożliwiać przeglądanie wszystkich zbieranych statystyk w postaci wykresów
u) umożliwiać szczegółowe monitorowanie komponentów serwerów fizycznych (CPU, sieć Ethernet, pamięć RAM, zasoby dyskowe)
v) umożliwiać definiowanie progów wydajności i pojemności w celu identyfikacji przypadków tzw. wąskich gardeł
w) posiadać funkcjonalność zmiany parametrów maszyn wirtualnych, minimum CPU i pamięci RAM, za pomocą wygenerowanego w tym oprogramowaniu zadania. Dodatkowo, wymagana jest funkcjonalność odkładania w czasie w/w zadania – po wygenerowaniu zadanie może być uruchamiane w momencie utworzenia lub w dowolnie skonfigurowanym przez użytkownika czasie
x) posiadać możliwość kasowania, wykonywania kopii migawkowych (ang. snapshot), włączania oraz wyłączania maszyn wirtualnych uruchomionych na monitorowanym środowisku wirtualnym

y) automatycznie przeszukiwać i analizować zebrane dane w celu wynajdywania nadmiarowości oraz niedoborów przyznanych zasobów (CPU, pamięć RAM, zasoby dyskowe) w monitorowanym środowisku
z) posiadać funkcjonalność automatycznego alarmowania o sytuacjach nietypowych – system monitoringu obserwuje i analizuje zachowanie platformy wirtualnej, na tej podstawie podnosi alarmy o zwiększonym obciążeniu elementu platformy wirtualnej w bieżącym dniu
aa) posiadać możliwość dowolnego przypisywania powiadomień dla różnych grup odbiorców (także z użyciem alertów stworzonych we własnym zakresie przez użytkownika)
bb) pozwalać na odczyt wyświetlanych alarmów dotyczących monitorowanego środowiska wirtualnego wraz z powiązanymi z nimi poradami eksperckimi
cc) umożliwiać definiowanie alertów dla monitorowanego środowiska związanych z:
    i. zarządzaniem pojemnością
    ii. zarządzaniem wydajnością
    iii. anomaliami w środowisku
    iv. zarządzaniu dostępnością
dd) posiadać funkcjonalność przypisania alertu do administratora/operatora rozwiązującego problem
ee) mieć możliwość realizacji funkcji półautomatycznego równoważenia obciążenia serwerów fizycznych w obrębie klastra opartego o dostarczone oprogramowanie do wirtualizacji zasobów serwerowych i ich mocy obliczeniowej, jak również pomiędzy logicznymi klastrami
ff) integrować się z zaoferowanym oprogramowaniem do centralnego zbierania logów (poprzez integracje zamawiający rozumie możliwość przesyłania danych z oprogramowania do centralnego zbierania logów do zaoferowanego oprogramowania). Zamawiający dodatkowo wymaga, aby konfiguracja dostępu/integracji do/z oprogramowaniem do centralnego zbierania logów odbywała się z konsoli zaoferowanego oprogramowania poprzez podanie danych dostępowych i adresowych do systemu zbierania logów
gg) posiadać funkcjonalność generowania gotowych, predefiniowanych raportów o stanie monitorowanego środowiska
hh) posiadać funkcjonalność pulpitu (ang. dashboard) za pomocą którego administrator będzie posiadał gotowe trzy kolumny z następującymi informacjami:
    i. zdarzenia jakie wystąpiły w zadanym okresie czasu, min. dla: wirtualnych maszyn, sieci wirtualnej, wirtualnej przestrzeni dyskowej
    ii. anomalie jakie wystąpiły w zadanym okresie czasu
    iii. zmiany w konfiguracji monitorowanej infrastruktury jakie wystąpiły w zadanym okresie czasu.

    Analiza danych ukazująca powyższe wyniki prezentowane na pulpicie musi odbywać się automatycznie poprzez mechanizmy analityczne zaoferowanego oprogramowania do monitorowania na podstawie zakresu czasowego definiowanego przez użytkownika tego pulpitu. Dodatkowo użytkownik musi mieć możliwość definiowania dla którego obiektu, np. wybranej maszyny wirtualnej, należy przeprowadzić analizę, a następnie wyświetlić jej wyniki.
ii) umożliwiać integrację z systemami firm trzecich monitorującymi infrastrukturę
jj) umożliwiać rozbudowę monitorowania dla rozwiązań firm trzecich
kk) umożliwiać konfigurację trybu wysokiej dostępności (ang. HA) dla każdego swojego komponentu w celu uniknięcia awarii pojedynczego elementu

ll) posiadać możliwość zastosowania dodatkowych wtyczek (ang. plugin) odpowiadających za monitorowanie systemów zewnętrznych takich jak m.in: macierze dyskowe, infrastruktury chmurowe, serwery fizyczne, przełączniki LAN umożliwiając tym samym wykorzystanie dedykowanych dodatkowych mechanizmów monitorujących określone komponenty

mm) posiadać funkcję tzw. konfiguratora własnych widoków zgromadzonych danych, który musi umożliwiać tworzenie zaawansowanych widoków dotyczących wszystkich monitorowanych metryk

nn) posiadać funkcjonalność monitorowania systemów operacyjnych (m.in. Windows, Linux) za pomocą zainstalowanego agenta w monitorowanym systemie operacyjnym

oo) posiadać gotowe paczki do monitorowania (ang. management packs) dla komponentów odpowiedzialnych za wirtualizacje sieci, automatyzacje i orkiestrację.

pp) mieć funkcjonalność tworzenia scenariuszy pojemnościowych na zasadzie: "co jeśli" dla minimum: CPU, pamięci RAM oraz przestrzeni dyskowej dla następujących elementów:

i. dodawania nowych serwerów fizycznych
ii. dodawania dodatkowych elementów wirtualizatora pamięci masowej

qq) wykrywać usługi uruchomione na monitorowanych maszynach wirtualnych, a następnie budować relacje lub zależności między usługami z różnych maszyn wirtualnych na podstawie komunikacji sieciowej

rr) umożliwiać wykonywanie automatycznych działań naprawczych w reakcji na wykryty alarm

ss) posiadać funkcjonalność monitorowania urządzeń firm trzecich typu macierze dyskowe, urządzenia sieciowe, a także innych rozwiązań do wirtualizacji niż dostarczane oprogramowanie do wirtualizacji zasobów serwerowych i ich mocy obliczeniowej.

12.11. Oprogramowanie do centralnego zbierania logów

Przez logi zamawiający rozumie wszelkie zdarzenia w systemie, które są zapisane do specjalnie przygotowanych plików (dzienników zdarzeń, plików logu) gdzie z każdym pojedynczym wpisem skojarzone są m. in. takie atrybuty jak data wystąpienia zdarzenia, poziom istotności, komunikat zdarzenia.

1) Zaoferowane oprogramowanie do centralnego zbierania logów musi:

a) zapewniać możliwość centralnego gromadzenia i analizy wszystkich logów z urządzeń wykorzystujących rozwiązania typu „syslog"

b) integrować się z oprogramowaniem do monitorowania i zarządzania platformą wirtualizacyjną, opisanym w punkcie **12.10**, w ten sposób, że z poziomu konsoli użytkownika oprogramowania do monitorowania i zarządzania platformą wirtualizacyjną musi istnieć możliwość uzyskania natychmiastowego dostępu do logów konkretnego urządzenia fizycznego

c) umożliwiać personalizację i wizualizację logów w postaci wykresów co najmniej liniowych, kołowych oraz słupkowych

d) w pełni integrować się z zaoferowanym w tym postępowaniu oprogramowaniem do wirtualizacji zasobów serwerowych i ich mocy obliczeniowej oraz oprogramowaniem do zarządzania klastrem wirtualizacyjnym

e) zapewnić monitorowanie urządzeń w czasie rzeczywistym

f) posiadać wbudowaną bazę wiedzy dotyczącą logów oraz zdarzeń dla zaoferowanego w tym postępowaniu oprogramowania do wirtualizacji mocy obliczeniowej

g) umożliwiać korelację wybranych zdarzeń w infrastrukturze fizycznej/wirtualnej oraz ich graficzną prezentację
h) posiadać możliwość personalizacji interfejsu graficznego w zależności od użytkownika/operatora
i) umożliwiać przeszukiwanie logów w oparciu o zdefiniowane przez użytkownika kryteria
j) posiadać funkcjonalność implementacji dedykowanych modułów do analizy logów innych urządzeń fizycznych np. macierzy dyskowych, przełączników LAN itp., tak aby analiza i korelacja wszystkich wiadomości systemowych mogła odbywać się z jednej konsoli zarządzającej
k) posiadać mechanizmy efektywnej analizy wszystkich rodzajów logów takich jak np.:
    i. logi aplikacji
    ii. logi sieciowe
    iii. pliki konfiguracyjne
    iv. informacje
    v. dane wydajnościowe
    vi. zrzuty awaryjne itp.
    vii. logów „niestrukturalnych”
l) umożliwiać definiowanie struktury dla logów „niestrukturalnych”
m) musi dopuszczać rozłączność uprawnień do interfejsu prezentacji i analizy logów od uprawnień do infrastruktury z której zbierane są logi
n) umożliwiać generowanie i eksportowanie dowolnych raportów związanych z zarejestrowanymi zdarzeniami i logami
o) posiadać możliwość logowania zdarzeń z zaoferowanego oprogramowania dostarczającego zintegrowaną platformę Kubernetes
p) mieć możliwość określania czasu retencji danych, tzn. administrator w konsoli graficznej do zarządzania platformą do zbierania i korelacji logów musi mieć możliwość określenia czasu po jakim zebrane logi będą archiwizowane (eksportowane) na zewnętrzną macierz dyskową. Dodatkowo wymaga się aby retencja mogła być ustawiana granularnie, tj. np. inny czas retencji dla logów z urządzeń klasy firewall, a inny czas retencji dla logów z wirtualizatorów (ang. hypervisor).

12.12. Oprogramowanie do wirtualizacji mocy obliczeniowej akceleratorów graficznych

1) Zamawiający dopuszcza aby zaoferowane oprogramowanie do wirtualizacji mocy obliczeniowej akceleratorów graficznych było dostarczone z wsparciem na okres co najmniej 18 miesięcy od daty podpisania protokołu zdawczo-odbiorczego**.**
2) Zaoferowane oprogramowanie do wirtualizacji mocy obliczeniowej akceleratorów graficznych musi:
    a) w pełni integrować się z dostarczonym oprogramowaniem do wirtualizacji zasobów serwerowych i ich mocy obliczeniowej dostarczonym w ramach tego postępowania
    b) mieć możliwość wirtualizacji zasobów akceleratorów graficznych GPU (ang. graphics processing unit) w ten sposób, aby tworzyć pule dostępnych zasobów GPU dla aplikacji pracujących na maszynach wirtualnych z granulacją do 1 MB pamięci GPU

c) działać w architekturze klient-serwer, maszyny wirtualne jako klienci z zainstalowanym agentem zaoferowanego oprogramowania współdzielą moc obliczeniową GPU, która jest udostępniana przez serwer posiadający zwirtualizowane zasoby GPU
d) umożliwiać przydzielanie/pobieranie zasobów GPU w sposób dynamiczny np. w celu czasowego wykorzystania przez klienta
e) posiadać mechanizm udostępniania/zapotrzebowywania mocy obliczeniowej GPU oparty o sieć LAN
f) mieć dostępną wtyczkę (ang. plugin) do zaoferowanego oprogramowania do zarządzania klastrem wirtualizacyjnym umożliwiającą:
    i. monitorowanie przydzielonych zasobów GPU
    ii. monitorowanie i zarządzanie serwerami i klientami w ramach architektury opisanej w podpunkcie c)
g) udostępniać interfejs linii komend do pełnego zarządzania tym oprogramowaniem
h) dawać możliwość alokacji całej pamięci GPU na serwerze udostępniającym lub tylko wybranej jej części przez wnioskującą aplikację
i) w przypadku ustawienia przez administratora więcej niż jednego serwera udostępniającego zasoby GPU opartego o zaoferowane oprogramowanie, być możliwość wyboru konkretnego serwera z którego udostępniane będą zasoby.

12.13. Oprogramowanie dostarczające zintegrowaną platformę Kubernetes

1) Zaoferowane oprogramowanie dostarczające zintegrowaną platformę Kubernetes musi być natywnie uruchamiane na dostarczonym oprogramowaniu do wirtualizacji zasobów serwerowych i ich mocy obliczeniowej.
2) Zamawiający dopuszcza aby zaoferowane oprogramowanie dostarczające zintegrowaną platformę Kubernetes było dostarczone z licencją ograniczoną czasowo. Przy czym licencja ta nie może wygasać wcześniej niż na koniec okresu gwarancji dla Systemu.
3) Zaoferowane oprogramowanie dostarczające zintegrowaną platformę Kubernetes musi:
    a) być certyfikowane przez Cloud Native Computing Foundation (CNCF) w ramach programu certyfikacji zgodności z oprogramowaniem Kubernetes (https://www.cncf.io/certification/software-conformance/)
    b) umożliwiać definiowanie limitów zasobów systemowych takich jak pamięć RAM i moc procesora, które będą dostępne dla całej aplikacji jak i dla poszczególnych kontenerów aplikacji
    c) posiadać LoadBalancer warstwy L4 dostarczany wraz z zamawianym oprogramowaniem, ściśle zintegrowany z platformą oraz wpierany przez producenta oprogramowania
    d) posiadać LoadBalancer realizujący serwisy warstwy L7 takie jak Ingress dostarczany wraz z zamawianym oprogramowaniem, ściśle zintegrowany z platformą oraz wpierany przez producenta oprogramowania
    e) umożliwiać uruchamianie wielu aplikacji równocześnie na współdzielonych zasobach sprzętowych umożliwiając budowanie aplikacji pracujących w oparciu o maszyny wirtualne oraz mikroserwisy
    f) posiadać narzędzia do zarządzania infrastrukturą poprzez interfejs programistyczny platformy Kubernetes – Cluster API
    g) zapewniać środowisko wykonawcze kontenera, które umożliwia interakcję z wtyczkami sieciowymi (w standardzie CNI) i pamięcią masową (w standardzie CSI)

h) posiadać możliwość wyboru wtyczki sieciowej CNI – co najmniej dwie wtyczki muszą być wspierane, z czego przynajmniej jedna musi umożliwiać integrację z zaoferowanym oprogramowaniem do wirtualizacji sieci, tak aby była możliwość tworzenia polityk bezpieczeństwa z poziomu tego oprogramowania
i) poprzez zintegrowaną wtyczkę CSI, umożliwiać dostarczanie trwałych zasobów dyskowych, realizowanych bezpośrednio na kompatybilnej z platformą pamięci masowej, co najmniej w trybie pojedynczego odczytu
j) umożliwiać pracę w środowiskach zamkniętych (ang. air-gapped enviroments)
k) zawierać wbudowany mechanizm skalowania, który pozwala określić ile instancji danej aplikacji ma być uruchomionych jednocześnie i pozwala na dynamiczne jej modyfikowanie
l) zawierać wbudowany rejestr obrazów Docker i OCI
m) umożliwiać integrację z rozwiązaniami CI/CD firm trzecich
n) umożliwiać przesyłanie logów do zewnętrznych systemów
o) realizować komunikację pomiędzy aplikacjami i usługami uruchomionymi na platformie poprzez wewnętrzną wirtualną sieć utworzoną w ramach platformy
p) umożliwiać budowanie i uruchamianie aplikacji stanowych i bezstanowych na bazie orkiestratora Kubernetes
q) oferować integrację z wykorzystywanymi lub planowanymi do wykorzystania w projekcie przez Zamawiającego systemami takimi jak Microsoft Active Directory lub Open LDAP w zakresie dostępu (autoryzacja i uwierzytelnienie) do klastrów Kubernetes
r) umożliwiać izolację aplikacji przy użyciu technologii kontenerów w taki sposób, że na jednej instancji systemu operacyjnego równocześnie może być uruchomionych wiele odizolowanych aplikacji mających dostęp do ograniczonych zasobów systemowych takich jak pamięć RAM, moc procesora i system plików
s) umożliwiać konfigurację sieci w taki sposób, żeby poszczególne aplikacje mogły być od siebie sieciowo odizolowane i jakakolwiek komunikacja pomiędzy nimi była zablokowana
t) zapewniać definiowanie uprawnień do poszczególnych obrazów lub grup obrazów dla poszczególnych użytkowników lub grup użytkowników
u) zapewniać możliwość separacji ruchu sieciowego, zasobów sprzętowych, przestrzeni dyskowej pomiędzy różnymi aplikacjami oraz różnymi klastrami Kubernetes
v) umożliwiać definiowanie różnych projektów oraz klastrów Kubernetes dla poszczególnych aplikacji i przypisywania uprawnień do nich dla określonych grup użytkowników
w) mieć możliwość uruchomienia i zarządzania w chmurze prywatnej opartej o dostarczone oprogramowanie do wirtualizacji zasobów serwerowych i ich mocy obliczeniowej
x) mieć możliwość zarządzania wersjami i aktualizacjami klastrów Kubernetes, w sposób automatyczny tj. nie powodujący dodatkowych nakładów pracy po stronie administratorów
y) posiadać oprogramowanie do wykonywania kopii zapasowych klastrów Kubernetes – musi istnieć możliwość ograniczania wykonywania kopii danych dla wewnętrznych komponentów klastra Kubernetes tj. wszystkich aplikacji uruchomionych w ramach klastra lub poszczególnych przestrzeni nazw (ang. namespace)

z) zawierać wbudowane mechanizmy automatycznego skalowania aplikacji (uruchamiania lub wyłączania kolejnych instancji aplikacji) w oparciu o metryki zużycia zasobów systemowych przez aplikację

aa) musi zawierać wbudowaną konsolę administracyjną umożliwiającą wykonywanie zadań administracyjnych przez przeglądarkę internetową lub interfejs CLI.

bb) musi zawierać wbudowane narzędzia umożliwiające administrację i konfigurację platformy z poziomu linii poleceń, działające na wykorzystywanych lub planowanych do wykorzystania w projekcie przez Zamawiającego systemach operacyjnych: Linux, Windows oraz macOS

cc) musi umożliwiać wybór systemu operacyjnego, który jest częścią rozwiązania Kubernetes, wymaga się, aby były wspierane co najmniej dwie dystrybucje systemu typu Linux.

12.14. Oprogramowanie do wirtualizacji stacji roboczych

1) Zaoferowane oprogramowanie do wirtualizacji stacji roboczych musi integrować się z dostarczonym oprogramowaniu do wirtualizacji zasobów serwerowych i ich mocy obliczeniowej.
2) Zamawiający dopuszcza aby zaoferowane oprogramowanie do wirtualizacji stacji roboczych było dostarczone z licencją ograniczoną czasowo i wsparciem na okres co najmniej 5 lat.
3) Zaoferowane oprogramowanie do wirtualizacji stacji roboczych musi:
   a) być licencjonowane na zasadach: ilość licencji zapewnia jednoczesną pracę dowolnych użytkowników
   b) umożliwiać instalację i użytkowanie niezbędnej ilości hostów wirtualizacyjnych (ang. hypervisor) wymaganych do uruchomienia wirtualnych maszyn (stacji roboczych użytkowników)
   c) wspierać posiadane i wykorzystywane przez Zamawiajacego lub planowane do wykorzystania w projekcie przez Zamawiającego systemy: Microsoft Windows 10, Microsoft Windows Server 2019 lub nowszy, Ubuntu, RHEL jako systemy operacyjne zainstalowane na wirtualnych stacjach roboczych
   d) wspierać posiadane i wykorzystywane przez Zamawiajacego lub planowane do wykorzystania w projekcie przez Zamawiającego dostęp do wirtualnych stacji roboczych przez aplikację kliencką, która można zainstalować co najmniej na: Microsoft Windows 10, MacOS X, Android, iOS, ChromeOS oraz Linux. Dostęp do stacji roboczych musi być zapewniony przez urządzenia klasy terminal typu Zero Client lub Thin Client. Dla pozostałych systemów operacyjnych, do maszyny wirtualnej, musi być możliwy dostęp bezpośrednio przez przeglądarkę internetową obsługującą HTML5
   e) zapewniać aby konfiguracja i zarządzanie dostępem do sesji i aplikacji terminalowych była realizowana z poziomu tej samej pojedynczej konsoli zarządzającej dostępnej w przeglądarce w technologii HTML5
   f) posiadać możliwość instalacji więcej niż jednej instancji serwera zarządzającego połączeniami, tak aby w przypadku awarii takiego serwera zapewnić możliwość nawiązania nowej sesji przez inny serwer zarządzający
   g) zapewniać dostęp do centralnej konsoli zarządzającej przy wykorzystaniu przeglądarek internetowych, co najmniej: Chrome lub Firefox
   h) posiadać funkcjonalność integracji centralnej konsoli do zarządzania z posiadanymi i wykorzystywanymi przez Zamawiajacego lub planowanymi do wykorzystania w projekcie przez Zamawiającego usługami katalogowymi Microsoft Active Directory

i) zapewniać aby centralna konsola do zarządzania posiadała możliwość przydzielania i konfiguracji uprawnień do poszczególnych wirtualnych stacji roboczych lub grup wirtualnych stacji roboczych
j) zapewniać aby centralna konsola do zarządzania posiadała możliwość integracji z tokenami RSA (Remote Secure Access) celem zapewnienia możliwości uwierzytelniania dwuskładnikowego dla logowania do wirtualnych stacji roboczych
k) zapewniać możliwość szybkiego dynamicznego tworzenia grup wielu nowych wirtualnych stacji roboczych oraz tworzenia grup wirtualnych stacji
l) zapewniać możliwość tworzenia grup wirtualnych stacji roboczych, w których:
   i. przypisanie użytkownika do wirtualnej stacji roboczej następuje automatycznie, na stałe, po pierwszym zalogowaniu i wówczas wszystkie dane użytkownika pozostają zapisane na dysku maszyny wirtualnej pomimo jego wylogowania
   ii. przypisanie użytkownika do wirtualnej stacji roboczej następuje przy każdym kolejnym logowaniu i wówczas użytkownik za każdym razem otrzymuje nowo wykreowaną wirtualną stację roboczą
m) zapewniać mechanizm pozwalający na podłączenie do wirtualnej stacji roboczej urządzeń typu dysk usb, pendrive poprzez włączenie w/w urządzeń do portu USB urządzenia fizycznego (np. zero client) na którym dostępna jest i działająca poprawnie aplikacja klienta do podłączenia do maszyny wirtualnej
n) zapewniać możliwość wirtualizacji wybranych aplikacji (zwirtualizowana aplikacja musi mieć postać pojedynczego pliku wykonywalnego z rozszerzeniem „exe" lub „msi") z możliwością uzależnienia uruchomienia tej aplikacji na wirtualnych maszynach od członkostwa użytkownika w posiadanej i wykorzystywanej lub planowanej do wykorzystania w projekcie przez Zamawiającego domenie Microsoft Active Directory
o) zapewniać możliwość uruchamiania aplikacji niezgodnych z daną wersją systemu operacyjnego – np. możliwość uruchomienia aplikacji działającej natywnie tylko w posiadanych i wykorzystywanych lub planowanych do wykorzystania w projekcie przez Zamawiającego systemie Microsoft Windows 7 – na systemie Microsoft Windows 10
p) zapewniać mechanizm umożliwiający wydruk danych wytworzonych w wirtualnej stacji roboczej na drukarkach lokalnych lub sieciowych podłączonych do urządzenia fizycznego na którym zainstalowana jest aplikacja klienta dostępowego do wirtualnej stacji roboczej
q) zapewniać aby warstwa wirtualizacji posadowionej bezpośrednio na sprzęcie serwerowym (ang. hypervisor) posiadała możliwość alokacji dla wirtualnych stacji roboczych większej ilości pamięci RAM niż fizycznie zainstalowanej w serwerze w celu osiągnięcia maksymalnego możliwego stopnia konsolidacji. Wspomniana powyżej warstwa wirtualizacji musi być dostarczona jako oprogramowanie wraz z przedmiotowym oprogramowaniem do wirtualizacji stacji roboczych.
r) zapewnić obsługę aplikacji 3D wewnątrz wirtualnych stacji roboczych wykorzystujących API OpenGL lub DirectX bez obciążania procesorów fizycznych w serwerach fizycznych, na których posadowione są maszyny wirtualne
s) zapewnić możliwość skonfigurowania wirtualnych stacji roboczych posiadających 255 lub więcej GB pamięci RAM
t) zapewniać funkcję znaku wodnego widocznego na ekranie połączenia do pulpitu zdalnego. Znak wodny musi zawierać informacje o adresie IP urządzenia klienckiego, nazwie użytkownika, domenie oraz znacznik czasu połączenia
u) umożliwiać przechowywanie buforu najczęściej odczytywanych bloków pamięci masowej w pamięci fizycznej serwerów utrzymujących środowisko VDI. Wielkość buforu powinna

wynosić do 32GB pozwalając na zminimalizowanie operacji odczytu z plików dysków wirtualnych obrazów wzorcowych stacji wirtualnych

v) zapewniać możliwość uruchomienia środowiska na fizycznej platformie HCI (Infrastruktura Hiperkonwergentna). Musi również posiadać certyfikację dla minimum trzech takich platform różnych producentów

w) mieć możliwość uruchomienia w środowisku publicznej chmury obliczeniowej. Musi również posiadać certyfikację dla minimum trzech dostawców chmury publicznej

x) być dostarczone wraz z opisanymi oznaczeniami producenta umożliwiającymi ich identyfikację na stronie przedmiotowego producenta lub w narzędziu udostępnianym przez producenta zaoferowanego oprogramowania

y) zapewniać mechanizm blokady połączeń od użytkowników posiadających zainstalowaną nieaktualną wersję oprogramowania służącego do nawiązywania połączeń z środowiskiem VDI

z) zapewniać możliwość połączenia z wirtualnym desktopem tylko i wyłącznie ze wskazanych przez administratora komputerów fizycznych z posiadanym i wykorzystywanym lub planowanym do wykorzystania w projekcie przez Zamawiającego systemem Windows 10 lub nowszym. Mechanizm ten musi bazować na grupach bezpieczeństwa w posiadanym i wykorzystywanym lub planowanym do wykorzystania w projekcie przez Zamawiającego Active Directory.

aa) integrować się z usługami posiadanymi i wykorzystywanymi lub planowanymi do wykorzystania w projekcie przez Zamawiającego terminalowymi Microsoft RDSH (Microsoft Remote Desktop Session Host) na wykorzystywanych lub planowanych do wykorzystania w projekcie przez Zamawiającego systemach Microsoft Windows Server 2012R2 lub nowszych udostępniając użytkownikom możliwość połączenia się z pełną sesją terminalową lub pojedynczą aplikacją za pomocą dostępnych klientów opisanych w punkcie **d)**.

bb) posiadać komponenty pełniący funkcję Identity Provider i realizujący funkcje portalu web z katalogiem desktopów i aplikacji wraz zapewnieniem pojedynczego logowania (SSO) do tych zasobów.

   i. komponent Identity Provider musi posiadać funkcje MFA (Multi Factor Authentication) opartą o aplikację mobilną z czasowymi kodami dostępu.

   ii. komponent Identity Provider musi zapewnić obsługę kluczy sprzętowych opartych o standard uwierzytelniania FIDO2, np. wykorzystywanych lub planowanych do wykorzystania w projekcie przez Zamawiającego Yubikey.

cc) posiadać funkcje wirtualizacji lokalnych zasobów dyskowych w serwerach fizycznych oraz ich agregację i współdzielenie pomiędzy wszystkimi serwerami fizycznymi będącymi członkiem klastra w celu wyeliminowania konieczności używania zewnętrznych zasobów dyskowych (sieci SAN, NAS).

4) W zaoferowanym oprogramowaniu serwer/serwery zarządzające infrastrukturą wirtualnych stacji roboczych muszą być instalowane na maszynach fizycznych lub wirtualnych z posiadanymi i wykorzystywanymi lub planowanymi do wykorzystania w projekcie przez Zamawiającego systemami operacyjnymi: Microsoft Windows Server 2012 R2 lub nowsze. W/w systemy dopuszczalne są w wersji Standard lub Enterprise

13. Przełączniki sieciowe

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

l.p	Wymaganie	100GbE	25GbE	10GbE	1GbE
Typy i minimalne ilości wymaganych portów					
1	Ilość portów 100GbE (QSFP)	32	8	4	
2	Ilość portów 1/10GbE (SFP+)				4
3	Ilość portów 1/10/25GbE (SFP28)		48		
4	Ilość portów 10GbE (10GBase-T)			48	
5	Ilość portów 1GbE (1000Base-T), wykluczając porty dedykowane do zarządzania.				48
6	Interfejsy 100GbE muszą umożliwiać rozdzielenie na cztery interfejsy do pracy z szybkością 25GbE (ang. breakout).	Tak	Tak		Nie
7	Możliwość instalacji modułu optycznego o przepustowości 40 GbE i 25 GbE w interfejsie 100GbE bez zastosowania rozdzielenia interfejsu (ang. breakout).	Tak	Nie	Tak	Nie
Parametry fizyczne i zasilanie					
1	Wysokość przełącznika 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 90% zakładając brak występowania zjawiska kondensacji pary wodnej.	Tak	Tak	Tak	Tak
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	Tak	Tak	Tak	Tak

l.p	Wymaganie	100GbE	25GbE	10GbE	1GbE
	przełącznika w pełnej (wymaganej przez Zamawiającego) konfiguracji z wykorzystaniem połowy zainstalowanych zasilaczy.				
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 **18.1.3** dla Zadania nr 1 oraz w punkcie **18.1.5** dla Zadania nr 2, które należy uwzględnić.	Tak	Tak	Tak	Tak
6	Przełącznik musi umożliwiać instalację, wymianę lub zamianę poszczególnych modułów (takich jak np. karty z interfejsami sieciowymi, moduły optyczne) w trakcie pracy urządzenia (hot-swap).	Tak	Tak	Tak	Tak
7	Przełącznik musi umożliwiać instalację lub wymianę zasilaczy w trakcie pracy urządzenia (hot-swap).	Tak	Tak	Tak	Nie
	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 przełączniki wraz z działającym na nich oprogramowaniem sterującym muszą pochodzić od jednego producenta.	Tak	Tak	Tak	Tak
3	Przełączniki muszą mieć odblokowane wszystkie wymagane funkcjonalności, a jeśli potrzebne są do tego licencje, dostawca musi je dostarczyć wraz z urządzeniami. Licencje nie mogą być ograniczone czasowo, terytorialnie (dotyczy terytorium UE), ani w żaden inny sposób wpływający na cel ich wykorzystania. Restart elementów nie	Tak	Tak	Tak	Tak

l.p	Wymaganie	100GbE	25GbE	10GbE	1GbE
	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.				
4	Wszystkie interfejsy liniowe przełączników muszą być odblokowane. Oznacza to, że nie mogą posiadać żadnych blokad umożliwiających ich wykorzystanie dopiero po wprowadzeniu jakiejkolwiek licencji, klucza, kodu lub innego mechanizmu odblokowującego. Dotyczy to wszystkich interfejsów znajdujących się fizycznie w oferowanych przełącznikach.	Tak	Tak	Tak	Nie
5	Karty, moduły 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. Zastosowanie modułów optycznych innych producentów nie może skutkować utratą, ograniczaniem gwarancji lub wsparcia producenta przełącznika.	Tak	Tak		Tak
6	Wszystkie przełączniki 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.	Tak	Tak	Tak	Tak

l.p	Wymaganie	100GbE	25GbE	10GbE	1GbE
	Niedopuszczalne jest wykorzystanie oprogramowania prototypowego, wytwarzanie wersji oprogramowania wyłącznie na potrzeby zamawiającego, nieoferowanej innym klientom.				
	Wymagania wydajnościowe i pojemnościowe				
1	Wydajność przełączania co najmniej	6.4 Tbps	4.0 Tbps	1.7 Tbps	290 Gbps
2	Liczba przetwarzanych pakietów na sekundę	2 Bpps	1 Bpps	1 Bpps	200 Mpps
3	Czas przełączania ramek nie dłuższy niż	1 µs	1 µs	3 µs	---
4	Całkowita wielkość buforów	32MB	32MB	12MB	4MB
5	Minimalna liczba obsługiwanych adresów MAC	280 000	280 000	270 000	30 000
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).	128 000	128 000	200 000	8 000
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).	64 000	64 000	64 000	4 000
8	Ilość jednocześnie aktywnych VLANów	4000	4000	4000	1024
9	Całkowita maksymalna moc pobierana przez urządzenie, nie większa niż	650W	650W	450W	250W
10	Typowa moc pobierana przez urządzenie, nie większa niż	400W	400W	350W	250W
	Wymagania operacyjne				
1	Moduły optyczne dla interfejsów muszą umożliwiać sprawdzenie mocy odbieranego sygnału.	Tak	Tak	Tak	Tak
2	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	Nie
3	Przełączniki muszą umożliwiać konfigurację wykorzystując modele OpenConfig. Musi być zapewniona obsługa następujących protokołów: gRPC, RESTCONF, NETCONF.	Tak	Tak	Tak	Nie
4	Przełączniki muszą zapewniać strumieniowanie danych	Tak	Tak	Tak	Nie

l.p	Wymaganie	100GbE	25GbE	10GbE	1GbE
	telemetrycznych wykorzystując protokół NETCONF/gRPC lub w formacie GPB.				
5	Wszystkie przełączniki 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	Nie
6	Wszystkie przełączniki muszą obsługiwać protokoły NTP i NTP6.	Tak	Tak	Tak	Tak
7	Wszystkie Elementy przełączające muszą wspierać Precision Time Protocol (PTP, IEEE 1588v2).	Tak	Tak	Tak	Nie
8	Wszystkie przełączniki muszą obsługiwać protokół LLDP.	Tak	Tak	Tak	Tak
9	Wszystkie przełączniki muszą umożliwiać dodanie wydzielonej tablicy routingu dla funkcji zarządzania (ang. Management VRF).	Tak	Tak	Tak	Nie
10	Wszystkie przełączniki muszą zapewniać mechanizm sprzętowej ochrony przeciw atakowi przeciążającemu (ang. DoS) na jednostkę sterującą CPU (ang. Control Plane Protection).	Tak	Tak	Tak	Nie
	Wymagania dla obsługi VXLAN				
1	Przełączniki muszą zapewniać sprzętową obsługę enkapsulacji VXLAN. Jednocześnie przy enkapsulacji musi być możliwa obsługa przełączania w warstwie L2 (ang. bridging).	Tak	Tak	Tak	Nie
2	Przełączniki muszą zapewniać sprzętową obsługę enkapsulacji VXLAN. Jednocześnie, przy enkapsulacji musi być możliwa obsługa routingu IP.	Tak	Tak	Tak	Nie
3	Przełączniki 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	Nie
4	Przełączniki muszą obsługiwać mechanizm protekcji grup linków Ethernet (LAG z LACP) poprzez podłączenie ich do co najmniej dwóch	Tak	Tak	Tak	Nie

l.p	Wymaganie	100GbE	25GbE	10GbE	1GbE
	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. Protekcja musi zapewniać nieprzerwaną pracę w przypadku awarii dowolnego pojedynczego komponentu. Protekcja musi poprawnie współpracować z VXLAN, EVPN, SpanningTree. Jeśli implementacja protekcji wymaga dodatkowych portów które przenoszą ruch w czasie awarii wykonawca musi dostarczyć odpowiednie okablowanie o długości minimum 2.5m				
	Wymagania sieciowe				
1	Wszystkie przełączniki 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 przełączniki muszą obsługiwać funkcję IGMP snooping (dla IGMPv2 oraz IGMPv3).	Tak	Tak	Tak	Tak
3	Wszystkie przełączniki muszą obsługiwać agregację interfejsów z wykorzystaniem protokołu LACP (IEEE 802.3ad).	Tak	Tak	Tak	Tak
4	Wszystkie przełączniki muszą umożliwiać stworzenie protekcji terminującej zagregowane interfejsy (LAG) na dwu Elementach przełączających (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.	Tak	Tak	Tak	Tak

l.p	Wymaganie	100GbE	25GbE	10GbE	1GbE
5	Wszystkie przełączniki muszą obsługiwać 802.1w RSTP, 802.1s MSTP.	Tak	Tak	Tak	Tak
6	Wszystkie przełączniki 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 przełączniki muszą obsługiwać protokół 802.1Qbb PFC (Priority-based Flow Control).	Tak	Tak	Tak	Nie
8	Wszystkie przełączniki muszą umożliwiać regulację (ang. Shaping) wielkości ruchu wyjściowego.	Tak	Tak	Tak	Nie
9	Wszystkie przełączniki zapewniać statyczny routing IP oraz dynamiczny routing IP zgodny z OSFPv2, OSFPv3, BGP.	Tak	Tak	Tak	Tak
10	Wszystkie przełączniki muszą zapewniać mechanizm dystrybucji pakietów IP poprzez ścieżki z równym kosztem (ang. Equal Cost Multi-Path routing ECMP).	Tak	Tak	Tak	Tak
11	Wszystkie przełączniki muszą zapewniać możliwość tworzenia polityk dla routing IP (ang. Route Maps).	Tak	Tak	Tak	Nie
12	Wszystkie przełączniki muszą zapewniać możliwość dystrybucji informacji routingowych pomiędzy różnymi wirtualnymi tablicami routingowymi (ang. VRF route leaking).	Tak	Tak	Tak	Nie
13	Wszystkie przełączniki muszą obsługiwać protokół BFD.	Tak	Tak	Tak	Nie

14. Przełączniki Fibre Channel

Wszystkie zawarte poniżej wymagania dla przełączników Fibre Channel (zwanego dalej przełącznikiem FC) są wymaganiami minimalnymi, należy zaoferować urządzenia zapewniające co najmniej podane parametry i funkcje.

Parametr	Charakterystyka (wymagania minimalne)
Obudowa	1) Przełącznik FC przystosowany do zainstalowania w szafie teleinformatycznej 19” o wysokości 1 RU wraz z zestawem montażowym przeznaczonym do zainstalowania go w wyżej wymienionej szafie 2) Przełącznik FC musi mieć wysokość maksymalnie 1 U (jednostka wysokości szafy montażowej) i szerokość 19” oraz zapewniać techniczną możliwość montażu w szafie 19”. Wraz z przełącznikiem należy dostarczyć odpowiedni zestaw montażowy do szafy 19”
Interfejsy	1) Przełącznik FC musi być wykonany w technologii FC minimum 32 Gbs i zapewniać możliwość pracy portów FC z prędkościami 32, 16, 8, 4 Gbs w zależności od rodzaju zastosowanych wkładek SFP. 2) Dostarczony przełącznik FC musi być wyposażony w 16 aktywnych portów FC obsadzonych 16 wkładkami SFP+ 16Gbs SWL. 3) Przełącznik musi umożliwiać w przyszłości rozbudowę do co najmniej 24 aktywnych portów w ramach tej samej obudowy. Przyszła rozbudowa musi odbywać się za pomocą aktywacji portów za pomocą odpowiedniej licencji i instalacji dodatkowych wkładek SFP+. 4) Wszystkie zaoferowane porty przełącznika FC muszą umożliwiać działanie bez tzw. oversubscrypcji gdzie wszystkie porty w maksymalnie rozbudowanej konfiguracji przełącznika wyposażonej we wkładki 32 Gbs mogą pracować równocześnie z pełną prędkością 32 Gb/s 5) Rodzaj obsługiwanych portów, co najmniej: E, D oraz F
Połączenia	1) Całkowita przepustowość przełącznika FC dostępna dla maksymalnie rozbudowanej konfiguracji (24 porty) wyposażonej we wkładki 32Gbs musi wynosić minimum 768 Gb/s end-to-end. 2) Oczekiwana wartość opóźnienia przy przesyłaniu ramek FC między dowolnymi portami przełącznika nie może być większa niż 900ns.
Zasilanie	1) Maksymalny dopuszczalny pobór mocy przełącznika FC wyposażonego w 24 aktywne porty 32 Gb/s to 77W. 2) Maksymalna ilość ciepła wydzielanego przez przełącznik FC wyposażony w 24 aktywne porty 32 Gb/s to 215 BTU na godzinę.
Funkcjonalność	1) Przełącznik FC musi obsługiwać mechanizm balansowania ruchu, pomiędzy co najmniej 16 różnymi połączeniami o tym samym koszcie wewnątrz wielodomenowych sieci fabric, przy czym balansowanie ruchu musi odbywać się w oparciu o 3 parametry nagłówka ramki FC: DID, SID i OXID. 2) Przełącznik FC musi realizować sprzętową obsługę zoningu (przez tzw. układ ASIC) na podstawie portów i adresów WWN. 3) Przełącznik FC musi mieć możliwość wymiany i aktywacji wersji oprogramowania układowego (ang. firmware) (zarówno na wersję wyższą

	jak i na niższą) w czasie pracy urządzenia i bez zakłócenia przesyłanego ruchu FC. 4) Przełącznik FC musi wspierać następujące mechanizmy zwiększające poziom bezpieczeństwa: a) mechanizm tzw. Fabric Binding, który umożliwia zdefiniowanie listy kontroli dostępu regulującej prawa przełączników FC do uczestnictwa w sieci fabric b) uwierzytelnianie (autentykacja) przełączników w sieci Fabric za pomocą protokołów DH-CHAP i FCAP c) uwierzytelnianie (autentykacja) urządzeń końcowych w sieci Fabric za pomocą protokołu DH-CHAP d) szyfrowanie połączenia z konsolą administracyjną. Wsparcie dla minimum SSHv2 e) definiowanie wielu kont administratorów z możliwością ograniczenia ich uprawnień za pomocą mechanizmu tzw. RBAC (Role Based Access Control) f) definiowane kont administratorów w środowisku RADIUS, LDAP w MS Active Directory, Open LDAP, TACACS+ g) szyfrowanie komunikacji narzędzi administracyjnych za pomocą SSL/HTTPS h) obsługa protokołu SNMP v3 i) IP Filter dla portu administracyjnego przełącznika j) wgrywanie nowych wersji oprogramowania układowego (ang. firmware) przełącznika FC z wykorzystaniem bezpiecznych protokołów np. SCP, SFTP k) wykonywanie kopii bezpieczeństwa konfiguracji przełącznika FC z wykorzystaniem bezpiecznych protokołów np. SCP, SFTP. 5) Przełącznik FC musi mieć możliwość konfiguracji przez: a) polecenia tekstowe w interfejsie znakowym konsoli terminala b) przeglądarkę internetową z interfejsem graficznym lub dedykowane oprogramowanie. 6) Przełącznik FC musi zapewnić możliwość jego zarządzania przez zintegrowany port Ethernet, RS232 oraz inband IP-over-FC. 7) Przełącznik FC musi zapewniać obsługę protokołu NVMe over FC. 8) Przełącznik FC musi zapewniać obsługę interfejsu zarządzającego REST API. 9) Przełącznik FC musi realizować kategoryzację ruchu między parami urządzeń (initiator - target) oraz przydzielenie takich par urządzeń do kategorii o wysokim, średnim lub niskim priorytecie. Konfiguracja przydziału do różnych klas priorytetów musi się odbywać za pomocą standardowych narzędzi do konfiguracji zoningu. 10) Przełącznik FC musi realizować kategoryzację ruchu na podstawie wartości parametru CS_CTL w nagłówku ramki FC oraz odpowiednie przydzielenie ramki do kategorii o wysokim, średnim lub niskim priorytecie. 11) Wsparcie dla N_Port ID Virtualization (NPIV). Obsługa, co najmniej 255 wirtualnych urządzeń na pojedynczym porcie przełącznika.

Diagnostyka	1) Przełącznik FC musi być dostarczony z następującymi narzędziami diagnostycznymi i mechanizmami obsługi ruchu FC: a) logowanie zdarzeń poprzez mechanizm „syslog” b) port diagnostyczny tzw. D_port. Port diagnostyczny musi umożliwiać wykonanie testów sprawdzających komunikację portu przełącznika z wkładką SFP, połączenie optyczne pomiędzy dwoma przełącznikami, testowe obciążenie połączenia pełną przepustowością 16Gbps/32Gbps oraz pomiar opóźnienia i odległości między przełącznikami z dokładnością co najmniej do 5m dla wkładek SFP 16Gbps lub 32Gbps. Testy wykonywane przez port diagnostyczny nie mogą wpływać w żaden sposób na działanie pozostałych portów przełącznika i całej sieci fabric c) FC ping d) FC traceroute e) kopiowanie danych wymienianych pomiędzy dwoma wybranymi portami na inny wybrany port przełącznika
Licencje	1) Jeżeli jakakolwiek funkcjonalność wymieniona powyżej wymaga dostarczenia dodatkowych licencji w celu jej realizacji to należy je dostarczyć wraz z urządzeniem w takiej ilości, aby zapewnić działanie funkcjonalności dla każdego portu przełącznika

15. System zdalnego dostępu

15.1. Terminal zdalnego dostępu

Parametr	Szczegółowy opis wymagania
Obudowa	1) Obudowa przystosowana do zainstalowania w szafie teleinformatycznej 19” o wysokości 1 RU, musi być dostarczona wraz z zestawem szyn montażowych.
Typ	1) Cyfrowy
Wbudowane porty/złącza	1) Terminal musi posiadać następujące porty/złącza: a) min. 32 porty do podłączania serwerów/urządzeń szeregowych b) min. 4-y porty USB Type-A w standardzie USB 2.0 lub wyższym c) min. 1 port do podłączenia kolejnych KVM-ów d) min. 2 porty Gigabit Ethernet do podłączenia do sieci LAN e) 2 porty do podłączenia zasilania w standardzie IEC C14
Dostęp	1) Terminal musi zapewniać możliwość: a) podłączenia min. 4 użytkowników zdalnych (przez sieć TCP/IP) b) podłączenia min. 1 użytkownika lokalnego
Wideo	1) Obsługa obrazu o rozdzielczości co najmniej 1680x1050
Funkcjonalność	1) Terminal musi posiadać wsparcie dla: a) True Serial over Telnet/SSH b) Virtual Media over USB c) szyfrowania 128-bit SSL, AES, DES and 3DES d) CAC/Smart Card
Okablowanie	1) Urządzenie musi być dostarczone z a) 24 kablami typ SIP wyposażonymi w interfejs szeregowy b) 8 kablami typu SIP wyposażonymi w złącze VGA i USB Type-A 2) Kabel typu SIP musi posiadać interfejs RJ-45 do podłączenia do terminala zdalnego dostępu. 3) Terminal musi zapewniać połączenia przez kabel CAT 5 i zasięg do 50 m.
Zasilanie	1) Musi być wyposażone w redundantne zasilacze 230V

15.2. Urządzenie dostępowe typ D1

Parametr	Szczegółowy opis wymagania
Obudowa	1) Obudowa przystosowana do zainstalowania w szafie teleinformatycznej 19” o wysokości 1 RU, musi być dostarczona wraz z zestawem elementów montażowych.
Typ	1) Urządzenie zapewniające zdalny bezpieczny dostęp do terminala zdalnego dostępu posiadające funkcjonalność firewalla z funkcją zdalnego dostępu z sieci zewnętrznych (VPN).

Wbudowane porty/złącza/pamięć	1) Urządzenie musi posiadać następujące porty/złącza: a) min. 8 portów Gigabit Ethernet (10/100/1000Base-T) oraz min. 8 portów SFP (gotowych do użycia bez konieczności zakupu dodatkowych modułów i licencji), wymagane jest dostarczenie wraz z urządzeniem min. 8 wkładek jednomodowych 1000-LX na potrzeby podłączenia do sieci LAN b) min. jeden zintegrowany z urządzeniem modem 4G/LTE z zewnętrznymi antenami radiowymi, które można zainstalować poza szafą, w której jest zainstalowane urządzenie dostępowe c) co najmniej trzy wolne sloty zapewniające możliwość rozbudowy o dodatkowe moduły 4G/LTE lub Wifi min. 802.11 AC d) port zarządzania Out of Band w standardzie Ethernet (RJ45) e) port konsoli w standardzie w postaci złącza min. RJ45 f) port USB Type-A w standardzie USB 3.0 lub wyższym na potrzeby podłączenie dodatkowego nośnika danych. Musi być zapewniona opcja umożliwiająca uruchomienie urządzenia za pomocą systemu operacyjnego znajdującego się na nośniku danych podłączonym do tego portu g) musi być wyposażony w co najmniej 8 GB pamięci typu Flash oraz co najmniej 4 GB pamięci typu RAM.
Funkcjonalność	1) Urządzenie musi zapewniać co najmniej: a) system operacyjny musi posiadać budowę modułową (moduły muszą działać w odseparowanych obszarach pamięci) i zapewniać całkowitą separację płaszczyzny kontrolnej od płaszczyzny przetwarzania ruchu użytkowników, np. moduł routingu IP, odpowiedzialny za ustalenie tras routingu oraz zarządzanie urządzenia musi być oddzielony od modułu przekazywania pakietów, odpowiedzialnego za przełączanie pakietów pomiędzy segmentami sieci obsługiwanymi przez urządzenie, b) system operacyjny śledzi stan sesji użytkowników (ang. stateful processing), tworząc i zarządzając tablicą stanu sesji. Musi być możliwość przełączenia urządzenia w tryb pracy bez śledzenia stanu sesji użytkowników, oraz wyłączenia części ruchu ze śledzenia stanu sesji, c) realizację zadania Stateful Firewall z mechanizmami ochrony przed atakami DoS, wykonując kontrolę na poziomie sieci oraz aplikacji pomiędzy nie mniej niż 64 strefami bezpieczeństwa z wydajnością nie mniejszą niż 1500 Mb/s liczoną dla ruchu IMIX. Firewall obsługuje nie mniej niż 350 000 równoległych sesji oraz zestawia nie mniej niż 15 000 nowych połączeń/sekundę, d) zestawianie zabezpieczonych kryptograficznie tuneli VPN w oparciu o standardy IPSec i IKE w konfiguracji site-to-site oraz client-to-site. IPSec VPN jest realizowany sprzętowo. Urządzenie musi obsługiwać nie mniej niż 2000 równoległych tuneli VPN oraz

	ruch szyfrowany o przepustowości nie mniej niż 300 Mb/s dla ruchu IMIX, e) definiowanie polityk bezpieczeństwa systemu zabezpieczeń w oparciu o strefy bezpieczeństwa, adresy IP klientów i serwerów, protokoły i usługi sieciowe, użytkowników aplikacji, reakcje zabezpieczeń oraz metody rejestrowania zdarzeń. Musi być możliwość zdefiniowania nie mniej niż 4000 reguł polityki bezpieczeństwa, f) obsługę protokołów dynamicznego routingu: RIP, OSPF oraz BGP, g) możliwość skonfigurowanie nie mniej niż 120 wirtualnych routerów, h) możliwość uruchomienia funkcji MPLS z sygnalizacją LDP i RSVP w zakresie VPLS i L3 VPN, i) obsługę co najmniej 2.500 sieci VLAN z tagowaniem 802.1Q, j) obsługę protokołów: Spanning Tree (802.1D), Rapid STP (802.1W) oraz Multiple STP (802.1S), k) obsługę protokółu LACP w celu agregowania fizycznych połączeń Ethernet, l) posiadanie mechanizmów priorytetyzowania i zarządzania ruchem sieciowym QoS – wygładzanie (shaping) oraz obcinanie (policing) ruchu. Mapowanie ruchu do kolejek wyjściowych odbywa się na podstawie DSCP, IP ToS, 802.1p, oraz parametrów z nagłówków TCP i UDP. Urządzenie posiada mechanizm tworzenia osobnych kolejek dla różnych klas ruchu. Musi posiadać zaimplementowany mechanizm WRED w celu przeciwdziałania występowaniu przeciążeń w kolejkach, m) pracę w konfiguracji odpornej na awarie w klastrze HA muszą funkcjonować w trybie Active-Passive z synchronizacją konfiguracji i tablicy stanu sesji. Przełączenie pomiędzy urządzeniami w klastrze HA odbywa się przezroczyście dla sesji ruchu użytkowników. Mechanizm ochrony przed awariami musi monitorować i wykrywać uszkodzenia elementów sprzętowych i programowych systemu zabezpieczeń oraz łączy sieciowych, n) zarządzanie urządzeniem za pomocą graficznej konsoli Web GUI oraz z wiersza linii poleceń (CLI) poprzez port szeregowy oraz protokoły telnet i SSH, o) mechanizm szybkiego odtwarzania systemu i przywracania konfiguracji. W urządzeniu musi być przechowywanych nie mniej niż 25 poprzednich, kompletnych konfiguracji, p) musi mieć możliwość rozbudowy o funkcję wykrywania i blokowania ataków intruzów (IPS, ang. intrusion prevention) realizowaną sprzętowo. System zabezpieczeń musi identyfikować próby skanowania, penetracji i włamań, ataki typu exploit (poziomu sieci i aplikacji), ataki destrukcyjne i destabilizujące DoS/DDoS oraz inne techniki stosowane przez hakerów. Ustalenie

	blokowanych ataków (intruzów, robaków) odbywa się w regułach polityki bezpieczeństwa. Musi realizować zadania IPS z wydajnością nie mniejszą niż 500 Mb/s dla rekomendowanej polityki producenta. Baza sygnatur IPS musi być utrzymywana i udostępniana przez producenta urządzenia firewall. Baza sygnatur ataków aktualizowana przez producenta min. raz w tygodniu, q) musi mieć możliwość rozbudowy o funkcję moduł kontroli antywirusowej kontrolujący pocztę elektroniczną (SMTP, POP3, IMAP), FTP oraz HTTP. Włączenie kontroli antywirusowej nie może wymagać dodatkowego serwera. r) urządzenie musi mieć możliwość rozbudowy o moduł kontroli antyspamowej działający w oparciu o mechanizm blacklist. Włączenie kontroli antyspamowej nie może wymagać dodatkowego serwera, s) urządzenie musi mieć możliwość rozbudowy o moduł filtrowania stron WWW w zależności od kategorii treści stron. Włączenie filtrowania stron WWW nie może wymagać dodatkowego serwera, t) urządzenie musi posiadać funkcję filtrowania zawartości ruchu HTTP, FTP i protokołów poczty elektronicznej (SMTP, POP3, IMAP) w celu blokowania potencjalnie szkodliwych obiektów. Urządzenie filtruje ruch na podstawie kryteriów obejmujących co najmniej: typy MIME, rozszerzenia plików, elementy ActiveX, Java i cookies, u) urządzenie musi mieć możliwość obsługi nie mniej niż 250 jednoczesnych zdalnych sesji/SSL VPN. Wymagane jest dostarczenie urządzenia w konfiguracji umożliwiającej nie mniej niż 2 jednoczesnych zdalnych sesji/SSL VPN. Jeżeli na potrzeby realizacji zdalnych sesji wymagana jest licencja to musi być ona dostarczona w wersji bez ograniczeń czasowych. Wymagane jest aby klient zdalnego dostępu umożliwiał połączenie z posiadanych i wykorzystywanych lub planowanych do wykorzystania w projekcie przez Zamawiającego urządzeń pracujących pod kontrolą systemu Windows 10/11 oraz macOS.
Zasilanie	1) Musi być wyposażone w co najmniej 2 redundantne zasilacze zasilane 230V

15.3. Urządzenie dostępowe typ D2

Parametr	**Szczegółowy opis wymagania**
Obudowa	1) Obudowa typu. desktop fabrycznie przystosowana do zainstalowania wraz z zasilaczem w szafie teleinformatycznej 19” za pomocą dedykowanego zestawu elementów montażowych. Zamawiający wymaga aby taki zestaw został dostarczony wraz z urządzeniem.

	2) Obudowa zapewniająca pasywne odprowadzeniem ciepła – poziom hałasu podczas pracy urządzenia na poziomie 0dB (brak wbudowanego wiatraka, ang. fanless).
Typ	1) Urządzenie zapewniające zdalny bezpieczny dostęp do terminala zdalnego dostępu posiadające funkcjonalność firewalla z funkcją zdalnego dostępu z sieci zewnętrznych (VPN).
Wbudowane porty/złącza/pamięć	1) Urządzenie musi posiadać następujące porty/złącza: a) min. 6 portów Gigabit Ethernet (10/100/1000Base-T) oraz min. 2 portów SFP (gotowych do użycia bez konieczności zakupu dodatkowych modułów i licencji), b) port zarządzania Out of Band w standardzie Ethernet (RJ45) c) port konsoli w standardzie w postaci złącza min. RJ45 d) port USB Type-A w standardzie USB 3.0 lub wyższym na potrzeby podłączenie dodatkowego nośnika danych. Musi być zapewniona opcja umożliwiająca uruchomienie urządzenia za pomocą systemu operacyjnego znajdującego się na nośniku danych podłączonym do tego portu e) musi być wyposażony w co najmniej 8 GB pamięci typu Flash oraz co najmniej 4 GB pamięci typu RAM.
Funkcjonalność	1) Urządzenie musi zapewniać co najmniej: a) system operacyjny musi posiadać budowę modułową (moduły muszą działać w odseparowanych obszarach pamięci) i zapewniać całkowitą separację płaszczyzny kontrolnej od płaszczyzny przetwarzania ruchu użytkowników, np. moduł routingu IP, odpowiedzialny za ustalenie tras routingu oraz zarządzanie urządzenia musi być oddzielony od modułu przekazywania pakietów, odpowiedzialnego za przełączanie pakietów pomiędzy segmentami sieci obsługiwanymi przez urządzenie, b) system operacyjny śledzi stan sesji użytkowników (ang. stateful processing), tworząc i zarządzając tablicą stanu sesji. Musi być możliwość przełączenia urządzenia w tryb pracy bez śledzenia stanu sesji użytkowników, oraz wyłączenia części ruchu ze śledzenia stanu sesji, c) realizację zadania Stateful Firewall z mechanizmami ochrony przed atakami DoS, wykonując kontrolę na poziomie sieci oraz aplikacji pomiędzy nie mniej niż 16 strefami bezpieczeństwa z wydajnością nie mniejszą niż 600 Mb/s liczoną dla ruchu IMIX. Firewall obsługuje nie mniej niż 64 000 równoległych sesji oraz zestawia nie mniej niż 5 000 nowych połączeń/sekundę, d) zestawianie zabezpieczonych kryptograficznie tuneli VPN w oparciu o standardy IPSec i IKE w konfiguracji site-to-site oraz client-to-site. IPSec VPN jest realizowany sprzętowo. Urządzenie musi obsługiwać nie mniej niż 250 równoległych tuneli VPN oraz ruch szyfrowany o przepustowości nie mniej niż 100 Mb/s dla ruchu IMIX,

Usunięte: 8

	e) definiowanie polityk bezpieczeństwa systemu zabezpieczeń w oparciu o strefy bezpieczeństwa, adresy IP klientów i serwerów, protokoły i usługi sieciowe, użytkowników aplikacji, reakcje zabezpieczeń oraz metody rejestrowania zdarzeń. Musi być możliwość zdefiniowania nie mniej niż 1.000 reguł polityki bezpieczeństwa, f) obsługę protokołów dynamicznego routingu: RIP, OSPF oraz BGP, g) możliwość skonfigurowanie nie mniej niż 30 wirtualnych routerów, h) możliwość uruchomienia funkcji MPLS z sygnalizacją LDP i RSVP w zakresie VPLS i L3 VPN, i) obsługę co najmniej 1000 sieci VLAN z tagowaniem 802.1Q, j) obsługę protokołów: Spanning Tree (802.1D), Rapid STP (802.1W) oraz Multiple STP (802.1S), k) obsługę protokółu LACP w celu agregowania fizycznych połączeń Ethernet, l) posiadanie mechanizmów priorytetyzowania i zarządzania ruchem sieciowym QoS – wygładzanie (shaping) oraz obcinanie (policing) ruchu. Mapowanie ruchu do kolejek wyjściowych odbywa się na podstawie DSCP, IP ToS, 802.1p, oraz parametrów z nagłówków TCP i UDP. Urządzenie posiada mechanizm tworzenia osobnych kolejek dla różnych klas ruchu. Musi posiadać zaimplementowany mechanizm WRED w celu przeciwdziałania występowaniu przeciążeń w kolejkach, m) pracę w konfiguracji odpornej na awarie w klastrze HA muszą funkcjonować w trybie Active-Passive z synchronizacją konfiguracji i tablicy stanu sesji. Przełączenie pomiędzy urządzeniami w klastrze HA odbywa się przezroczyście dla sesji ruchu użytkowników. Mechanizm ochrony przed awariami musi monitorować i wykrywać uszkodzenia elementów sprzętowych i programowych systemu zabezpieczeń oraz łączy sieciowych, n) zarządzanie urządzeniem za pomocą graficznej konsoli Web GUI oraz z wiersza linii poleceń (CLI) poprzez port szeregowy oraz protokoły telnet i SSH, o) mechanizm szybkiego odtwarzania systemu i przywracania konfiguracji. W urządzeniu musi być przechowywanych nie mniej niż 25 poprzednich, kompletnych konfiguracji, p) musi mieć możliwość rozbudowy o funkcję wykrywania i blokowania ataków intruzów (IPS, ang. intrusion prevention) realizowaną sprzętowo. System zabezpieczeń musi identyfikować próby skanowania, penetracji i włamań, ataki typu exploit (poziomu sieci i aplikacji), ataki destrukcyjne i destabilizujące DoS/DDoS oraz inne techniki stosowane przez hakerów. Ustalenie blokowanych ataków (intruzów, robaków) odbywa się w regułach polityki bezpieczeństwa. Musi realizować zadania IPS z wydajnością nie mniejszą niż 200 Mb/s dla rekomendowanej polityki

	producenta. Baza sygnatur IPS musi być utrzymywana i udostępniana przez producenta urządzenia firewall. Baza sygnatur ataków aktualizowana przez producenta min. raz w tygodniu, q) musi mieć możliwość rozbudowy o funkcję moduł kontroli antywirusowej kontrolujący pocztę elektroniczną (SMTP, POP3, IMAP), FTP oraz HTTP. Włączenie kontroli antywirusowej nie może wymagać dodatkowego serwera, r) urządzenie musi mieć możliwość rozbudowy o moduł kontroli antyspamowej działający w oparciu o mechanizm blacklist. Włączenie kontroli antyspamowej nie może wymagać dodatkowego serwera, s) urządzenie musi mieć możliwość rozbudowy o moduł filtrowania stron WWW w zależności od kategorii treści stron. Włączenie filtrowania stron WWW nie może wymagać dodatkowego serwera, t) urządzenie musi posiadać funkcję filtrowania zawartości ruchu HTTP, FTP i protokołów poczty elektronicznej (SMTP, POP3, IMAP) w celu blokowania potencjalnie szkodliwych obiektów. Urządzenie filtruje ruch na podstawie kryteriów obejmujących co najmniej: typy MIME, rozszerzenia plików, elementy ActiveX, Java i cookies, u) urządzenie musi mieć możliwość obsługi nie mniej niż 25 jednoczesnych zdalnych sesji/SSL VPN. Wymagane jest dostarczenie urządzenia w konfiguracji umożliwiającej nie mniej niż 2 jednoczesnych zdalnych sesji/SSL VPN. Jeżeli na potrzeby realizacji zdalnych sesji wymagana jest licencja to musi być ona dostarczona w wersji bez ograniczeń czasowych. Wymagane jest aby klient zdalnego dostępu umożliwiał połączenie z posiadanych i wykorzystywanych lub planowanych do wykorzystania w projekcie przez Zamawiającego urządzeń pracujących pod kontrolą systemu Windows 10/11 oraz macOS.
Zasilanie	1) Musi być wyposażone w zasilacz zasilany 230V 2) Średnie zużycie energii – nie więcej niż 25W

15.4. System dostępowy typ D3

System dostępowy typ D3 składa się z:

1) 12 sztuk urządzenia dostępowego typ D3 opisanego w punkcie **15.4.1**
2) 1 sztuki systemu zarządzającego typ D3 opisanego w punkcie **0**.

15.4.1. Urządzenie dostępowe typ D3

Parametr	**Szczegółowy opis wymagania**

Typ	1) Punkt dostępowy sieci wifi min. dwu-radiowy/trzy-zakresowy 2,4GHz, 5GHz i 6GHz umożliwiający zdalny bezpieczny dostęp ze zdalnej lokalizacji do lokalizacji podstawowej z wykorzystaniem tunelu VPN poprzez system zarządzający (kontroler).
Obudowa	1) Obudowa przeznaczona do instalacji wewnątrz budynków. Fabrycznie przystosowana do zainstalowania na płaskich powierzchniach (ściana, sufit, sufit podwieszany) za pomocą dedykowanego zestawu montażowego. Zamawiający wymaga aby taki zestaw został dostarczony wraz z urządzeniem. 2) Wymiary obudowy (bez uchwytu montażowego) nie więcej niż: 160 mm (szer.) x 160 mm (gł.) x 40 mm (wys.) 3) Waga urządzenia nie więcej niż 550g (bez uchwytu montażowego).
Wbudowane anteny Wi-Fi	1) Zintegrowane anteny dookólne typu downtilt dla technologii min. 2x2 MIMO ze szczytowym zyskiem anteny: a) min. 2,8 dBi w paśmie 2,4 GHz, b) min. 4,5 dBi w paśmie 5 GHz, c) min. 4,5 dBi w paśmie 6 GHz.
Specyfikacja radia Wi-Fi	Minimalne parametry poszczególnych modułów radiowych: 1) Radio 2,4GHz: dwa strumienie przestrzenne MIMO dla bezprzewodowej szybkości transmisji danych zapewniając transfer 574 Mb/s z zgodnymi urządzeniami klienckimi 2) Radio 5GHz: dwa strumienie przestrzenne MIMO dla bezprzewodowej szybkości transmisji danych zapewniając transfer 1,2 Gb/s z zgodnymi urządzeniami klienckimi 802.11ax 3) Radio 6GHz: dwa strumienie przestrzenne MIMO dla bezprzewodowej szybkości transmisji danych zapewniając transfer 2,4 Gb/s z zgodnymi urządzeniami klienckimi 802.11ax 4) Poprawna obsługa min. 512 powiązanych urządzeń klienckich na radio 5) Zgodność z WIFI 6E oraz 802.11b/a/g/n/ax
Wbudowane porty/złącza	1) Urządzenie musi posiadać następujące porty/złącza: a) min. 1 port Ethernet (RJ45) o parametrach: i) automatyczne wykrywanie prędkości (100/1000/2500Base-T), ii) zgodność z 802.3bz i NBase-T, iii) POE-PD: 48 Vdc 802.3af/at POE (klasa 3 lub wyższa), iv) zgodność z 802.3az (EEE); b) interfejs zasilania prądem stałym: 12V; c) szeregowy port konsoli; d) port USB Type-A w standardzie min. USB 2.0 na potrzeby podłączenie zewnętrznego modemu LTE.
Funkcjonalność	Urządzenie dostępowe musi zapewniać co najmniej: 1) jednoczesną pracy w co najmniej dwóch zakresach w dowolnej konfiguracji tj: 2,4GHz i 5GHz; 2,4GHz i 6GHz; 5GHz i 6GHz; 2) poprawną pracę w jednym z trzech trybów: a) zarządzanie centralne za pomocą zewnętrznego systemu zarządzającego urządzeniami dostępowymi (kontroler sieci

Usunięte: zakresowy

Usunięte: trójradiowy

	bezprzewodowej) dostarczanego przez producenta urządzeń dostępowych w trybie punktu dostępowego wifi; b) zarządzanie centralne za pomocą zewnętrznego systemu zarządzającego urządzeniami dostępowymi (kontroler sieci bezprzewodowej) dostarczanego przez producenta urządzeń dostępowych w trybie zdalnego punktu dostępowego wifi. W tym trybie urządzenie dostępowe po podłączenia do Internetu w zdalnej lokalizacji musi poprawnie i automatycznie zestawić tunel VPN z systemem zarządzającym oraz zapewnić tunelowanie całego ruchu od urządzeń klienckich, podłączonych do urządzenia dostępowego, do systemem zarządzającym za pomocą tego tunelu VPN. Wymagana jest przepustowość tunelu IPsec co najmniej 500Mbps; c) tryb pracy autonomicznej bez nadzoru centralnego kontrolera: i) urządzenie musi zapewniać funkcjonalność zarządzania przez przeglądarkę internetową i protokół HTTPS oraz protokół SSH; ii) wszystkie operacje konfiguracyjne muszą być możliwe do przeprowadzenia z poziomu przeglądarki lub terminala (CLI); 3) musi być zapewniona możliwość wspólnej konfiguracji urządzeń dostępowych w jedną sieć LAN w warstwie 2 (w przypadku pracy w trybie autonomicznym): a) system operacyjny zainstalowany w urządzeni dostępowym musi zapewniać automatyczny wybór jednego z urządzeń jako urządzenia zarządzającego, b) w przypadku awarii urządzenia pełniącego funkcję urządzenia zarządzającego kolejne urządzenie w sieci musi przejąć jego rolę w sposób automatyczny, c) modyfikacja konfiguracji musi się automatycznie propagować na pozostałe urządzenia, d) obraz systemu operacyjnego musi się automatycznie propagować na pozostałe urządzenia dostępowe, aby wszystkie urządzenia miały tą samą jego wersję; e) musi być zapewniona poprawna obsługa trybu sieci typu MESH – dowolne urządzenie dostępowe po odłączeniu od infrastruktur Ethernet musi poprawnie i automatycznie zestawić bezpieczną (szyfrowanie AES) łączność radiową z najbliższym urządzeniem dostępowym i zapewnić wszystkie usługi, tak jakby był podłączony do sieci Ethernet. Urządzenie dostępowe musi być w pełni zarządzane z poziomu systemu operacyjnego urządzenia pełniącego funkcję urządzenia zarządzającego. 4) w system operacyjny musi być: a) wbudowana pełnostanowa zapora sieciowa z funkcją rozpoznawania aplikacji; b) wbudowany serwer DHCP;

	c) wbudowany serwer RADIUS umożliwiający terminowanie sesji EAP bezpośrednio na urządzeniach, bez pośrednictwa zewnętrznych elementów; 5) musi być obsługiwane terminowanie sesji EAP co najmniej w następujących opcjach: a) EAP-TLS b) PEAP-MSCHAPv2 c) PEAP-GTC d) TTLS-MSCHAPv2 6) musi istnieć możliwość integracji z zewnętrznymi serwerami uwierzytelniania RADIUS oraz LDAP; 7) urządzenie dostępowy musi obsługiwać nie mniej niż 16 niezależnych SSID (Zamawiający dopuszcza aby w przypadku radia 6 GHz urządzenie poprawnie obsługiwało min. 4 BSSID); 8) każde SSID musi mieć możliwość przypisania w sposób statyczny lub dynamiczny do sieci VLAN; 9) musi być zapewniona możliwość zdefiniowania odseparowanej sieci gościnnej z funkcją NAT; 10) zarządzanie pasmem radiowym w sieci urządzeń dostępowych musi się odbywać automatycznie za pomocą auto-adaptacyjnych mechanizmów, w tym nie mniej niż: a) automatyczne definiowanie kanału pracy oraz mocy sygnału dla poszczególnych punktów dostępowych przy uwzględnieniu warunków oraz otoczenia, w którym pracują punkty dostępowe, b) stałe monitorowanie pasma oraz usług w celu zapewnienia niezakłóconej pracy systemu, c) rozkład ruchu pomiędzy różnymi punkami dostępowym bazując na ilości użytkowników oraz utylizacji pasma, d) wykrywanie interferencji oraz miejsc bez pokrycia sygnału, e) wyrównywanie czasów dostępu do pasma dla klientów pracujących w standardzie 802.11n oraz starszych (802.11a/b/g), f) wsparcie dla 802.11d oraz 802.11h, g) obsługa tzw. „Sticky Clients” polegająca na automatycznym przełączaniu klientów do punktu dostępowego oferującego najlepszy sygnał, h) możliwość przełączenia urządzenia dostępowego w tryb analizatora widma w celu analizy zakłóceń pochodzących od innych źródeł interferencji niż sieci WiFi; 11) obsługa roamingu klientów w warstwie 2 12) obsługa roamingu klientów w warstwie 3 pomiędzy różnymi grupami punktów dostępowych, z zachowaniem adresu IP klienta 13) obsługa szybkiego roamingu klientów pomiędzy punktami dostępowymi z wykorzystaniem nie mniej niż: a) 802.11r b) 802.11v

	c) 802.11k 14) obsługa monitoringu przez SNMP v1/2/3 15) obsługa logowania na zewnętrznym serwerze SYSLOG 16) w system musi być wbudowany mechanizm wykrywania ataków na sieć bezprzewodową w zakresie ataków na infrastrukturę i klientów sieci; 17) w system musi być wbudowany mechanizm zapobiegania atakom na sieć bezprzewodową w zakresie ataków na infrastrukturę i klientów sieci 18) punkt dostępowy musi obsługiwać klientów 2x2:2 w trybie SU-MIMO dla 5GHz i 6GHz oraz 2x2:2 w trybie SU-MIMO dla 2,4GHz 19) punkt dostępowy musi oferować następujące mechanizmy poprawiające efektywność działania sieci radiowej, nie mniej niż: a) moc transmisji konfigurowalna przez administratora – możliwość dwukrotnego zwiększenia/zmniejszenia mocy (o +/-3dB) b) prędkości transmisji (parametry minimalne): i) 802.11a/g: 6, 9, 12, 18, 24, 36, 48, 54 Mbps ii) 802.11n: 6,5Mbps do 300Mbps iii) 802.11ac: 6,5Mbps do 867Mbps iv) 802.11ax (2,4GHz): 3,6Mbps do 574Mbps v) 802.11ax (2,4GHz): 3,6Mbps do 1201Mbps vi) 802.11ax (2,4GHz): 3,6Mbps do 2402Mbps c) obsługa HT – kanały 20/40MHz d) obsługa VHT – kanały 20/40/80MHz e) obsługa HE – kanały 20/40/80/160MHz 20) Urządzenie dostępowe musi posiadać certyfikat Wi-Fi Alliance (WFA) dla min.: WIFI 6/ 802.11/a/b/g/n/ac /WPA3.
Zasilanie	1) musi zapewniać możliwość zasilania prądem stały (12V) lub przez sieć Ethernet (PoE) 802.3af/at PoE (klasa 3 lub wyższa). 2) maksymalne zużycie energii (bez urządzenia USB): a) przy zasilaniem prądem stałym do 13W b) przy zasilaniu PoE: do 15W

15.4.2. Systemem zarządzający typ D3

Parametr	**Szczegółowy opis wymagania**
Typ	1) Kontroler sieci wifi dedykowany przez producenta urządzeń dostępowych TYP 3 w postaci maszyny wirtualnej umożliwiającej instalacje na środowisku zgodnym z wykorzystywanym lub planowanym do wykorzystania w projekcie przez Zamawiającego oprogramowaniem VMWare oraz Hyper-V.
Funkcjonalność	1) Dostarczone rozwiązanie musi zarządzać siecią bezprzewodową złożoną z dostarczonych punktów dostępowych. Zamawiający zapewni wymaganą przez rozwiązanie infrastrukturę wirtualną.

	2) Zamawiający wymaga, aby ruch pomiędzy kontrolerem a punktem dostępowym był tunelowany. 3) Dostarczone rozwiązanie musi w pełni obsługiwać dostarczane urządzenia dostępowe TYP 3. 4) Dostarczone rozwiązanie musi posiadać funkcje pełnostanowej zapory sieciowej (stateful firewall). 5) Dostarczone rozwiązanie musi zapewniać centralne zarządzanie wszystkimi urządzeniami dostępowymi TYP 3 w sieci, łącznie z tworzeniem i zarządzaniem obrazami konfiguracyjnymi oraz aktualizacją oprogramowania. 6) Dostarczone rozwiązanie musi posiadać następujące parametry sieciowe: a) możliwość wdrożenia w warstwie 2 i 3 ISO/OSI; b) wsparcie dla sieci VLAN w tym również trunk 802.1q; c) wbudowany serwer DHCP; d) obsługa SNMPv2, SNMPv3; e) routing dynamiczny OSPF. 7) Dostarczone rozwiązanie musi obsługiwać co najmniej: a) Metody szyfrowania i kontroli połączeń: WEP, dynamic WEP, TKIP WPA, WPA2,WPA3, AES-CCMP, EAP, PEAP, TLS, TTLS; b) Obsługę szyfrowania AES-CCM, TKIP i WEP centralnie na kontrolerze; c) Obsługę SSL i TLS, RC4 128-bit oraz RSA 1024 i 2048 bit; d) Autoryzację dostępu użytkowników: i. Typy uwierzytelnienia: IEEE 802.1X (EAP,LEAP,PEAP,EAP-TLS,EAP-TTLS, EAP-FAST), RFC 2548, RFC 2716 PPP EAP-TLS, RFC 2865 Radius Authentication, RFC 3576 dynamic Auth Ext for Radius, RFC 3579 Radius suport for EAP, RFC 3580, 3748, captive portal", 802.1X i MAC; ii. Funkcję wykorzystania nazwy użytkownika, adresu IP, adresu MAC i klucza szyfrowanego do uwierzytelnienia; iii. Wsparcie dla autoryzacji, minimum: Microsoft NAP, CISCO NAC, Pulse Secure NAC, Aruba NAC; iv. Musi umożliwiać utworzenie nie mniej niż 16 SSID na jednym punkcie dostępowym. Dla każdego SSID musi istnieć możliwość definiowania oddzielnego typu szyfrowania, oddzielnych vlan-ów i oddzielnego portalu „captive portal"; v. Musi umożliwiać wykorzystanie mieszanego szyfrowania dla określonych SSID (np. WPA/TKIP i WPA2/AES); vi. Terminowanie sesji użytkowników sieci; bezprzewodowej musi odbywać się na kontrolerze, nie na urządzeniu dostępowym; vii. Uwierzytelnienie oraz autoryzacja musi być możliwa przy wykorzystaniu lokalnej bazy danych na urządzeniu zarządzającym oraz zewnętrznych serwerów uwierzytelniających. Urządzenie zarządzające musi

	wspierać co najmniej następujące serwery AAA: Radius, LDAP, SSL Secure LDAP, TACACs+; e) Urządzenie zarządzające musi gwarantować automatyczne przełączenie z zewnętrznego serwera AAA na lokalną bazę danych w przypadku awarii serwerów uwierzytelniających. f) Musi istnieć mechanizm definiowania ról użytkowników oraz bazując na nich egzekwowania polityki dostępu. g) Urządzenie zarządzające musi zapewniać obsługę XML API do uwierzytelnienia. 8) Urządzenie zarządzające musi posiadać obsługę transmisji różnego typu danych w jednej sieci: a) integracja jednoczesnej transmisji danych i głosu; b) musi obsługiwać szybkie przełączanie się klientów pomiędzy punktami dostępowymi (tzw. fast roaming); c) ograniczanie pasma dla użytkownika oraz dla roli użytkownika; d) ograniczenie pasma dla poszczególnych aplikacji; e) ograniczenie pasma dla poszczególnych SSID. 9) Urządzenie zarządzające musi umożliwiać stworzenie strony dla gości (tzw. Captive Portal). 10) Urządzenie zarządzające musi umożliwiać stworzenie dedykowanej strony (interfejsu) do tworzenia kont dostępu do sieci dla gości – strona przeznaczona dla osób nie pracujących w dziale IT (np. dla pracownika recepcji bądź portierni). 11) Urządzenie zarządzające musi posiadać funkcję adaptacyjnego zarządzania pasmem radiowym: a) automatyczne definiowanie kanału pracy oraz mocy sygnału dla poszczególnych punktów dostępowych przy uwzględnieniu warunków oraz otoczenia, w którym pracują punkty dostępowe; b) stałe monitorowanie pasma oraz usług; c) przełączenie AP w tryb pracy monitorowania sieci bezprzewodowej w przypadku wystąpienie interferencji między kanałowymi; d) rozkład ruchu pomiędzy różnymi punkami dostępowymi bazując na ilości użytkowników oraz utylizacji pasma; e) przełączania użytkowników zdolnych pracować w paśmie 5Ghz do pracy w tymże paśmie; f) zapewnienie sprawiedliwego dostępu do medium w środowisku, w który znajdują się klienci pracujący zgodnie ze standardami (802.11ax, 11ac, 11n, 11g, 11a, 11b); g) wykrywanie interferencji oraz miejsc bez pokrycia sygnału. h) wsparcie dla 802.11h, 802.11k, 802.11r, 802.11v, 802.11w; 12) Urządzenie zarządzające musi posiadać funkcję wbudowanej zapory sieciowej, posiadającej co najmniej następujące własności: a) inspekcja pakietów z uwzględnieniem reguł bazujących na: użytkownikach, rolach, protokołach i portach, adresacji IP, lokalizacji, czasie dnia; b) kopiowanie (mirroring) sesji; c) szczegółowe logi (per pakiet) do późniejszej analizy; d) ALG (Application Layer Gateway); e) translacja źródłowa, docelowa adresów IP; f) identyfikacja i blokowanie ataków DoS;

	g) obsługa protokołu GRE; h) deep packet inspection (DPI); i) możliwość rozpoznawania oraz tworzenia reguł opartych na aplikacjach których używają klienci wifi. 13) Urządzenie zarządzające musi posiadać funkcję systemu WIDS/ WIPS. Moduł WIPS musi posiadać co najmniej następujące funkcje: a) detekcja i identyfikacja lokalizacji obcych punktów dostępowych (rogue AP). Automatyczna klasyfikacja obcych urządzeń i możliwość ich blokowania poprzez wysyłanie odpowiednio spreparowanych pakietów; b) identyfikacja i możliwość blokowania sieci Adhoc; c) identyfikacja anomalii sieciowych, np.: wireless bridge; d) ochrona przed atakami sieciowymi na sieć bezprzewodową, m.in. DoS, Management Frame Flood, fake AP, Airjack, ASLEAP, null probe response detection, Netstumbler; e) identyfikacja błędów konfiguracji klientów WLAN; f) identyfikacja podszywania się pod autoryzowane punkty dostępowe. 14) Urządzenie zarządzające musi posiadać funkcję analizatora widma. 15) Zarządzanie urządzeniem zarządzającym musi odbywać się poprzez co najmniej następujące metody: interfejs przeglądarki Web (https) i linia komend przez SSH. 16) Kontroler musi zapewniać wsparcie dla protokołów Bonjour, UPnP i DLNA. 17) Wszystkie dostarczone licencje i obsługiwane funkcje muszą być permanentne, nie dopuszcza się licencji ograniczonych czasowo.
Dodatkowe elementy	1) Z systemem zarządzającym muszą zostać dostarczone co najmniej 4 kable konsolowe umożliwiające zarządzanie poprzez port konsolowy urządzeniami dostępowymi typ D3 ze złączem typu USB.

15.5. Mobilne urządzenie monitorujące

Mobilne urządzenie monitorujące posiadające następujące cechy:

1. Rozmiar i masa urządzenia:
   a) wysokość: nie więcej niż 250 mm,
   b) szerokość: nie więcej niż 180 mm,
   c) grubość: nie więcej niż 6 mm,
   d) masa: nie więcej niż 500 g;
2. Funkcję procesora oraz układu graficznego pełni system jednoukładowy (SoC), w którego skład wchodzi:
   a) co najmniej 8 fizycznych rdzeni, w dwóch klasach wydajności (4 rdzenie zapewniające wydajność i 4 rdzenie energooszczędne),
   b) wbudowany procesor graficznym z co najmniej 10 rdzeniami,
   c) wbudowany co najmniej 16 rdzeniowy system wspomagający proces uczenia maszynowego,

d) zunifikowana pamięć RAM o pojemności co najmniej 16 GB;

3. Posiadające pojemność wewnętrznej pamięci przeznaczonej na oprogramowanie układowe oraz dane użytkownika min. 1TB;
4. Posiadające dedykowane fizyczne przyciski do regulacji głośności oraz wyłącznik;
5. Wyposażone w wyświetlacz o następujących parametrach:
   e) wyświetlacz True Tone o przekątnej 11 cali z podświetleniem LED, w technologii IPS z obsługą wielo-dotyku – Zamawiający dopuszcza aby zaoferowane urządzenie miało przekątną mniejszą (np. z powodu zaokrąglonych kątów ekranu) pod warunkiem, że jego ekran wpisuje się w kształt regularnego prostokąta. Przyjmując, że powierzchnia ekranu jest prostokątem, jego przekątna wynosi 11 cali,
   f) rozdzielczość min. 2388 na 1668 pikseli przy 264 pikselach na cal (ppi),
   g) wyposażony w powłokę oleofobowa odporna na odciski palców oraz powłokę antyodblaskową,
   h) musi posiadać pełną laminację wyświetlacza,
   i) posiadać jasność min. 600 nitów;
6. Wyposażone w system aparatów o następujących parametrach:
   a) z przodu obudowy min.12MP ,
   b) z tyłu obudowy zestawem obiektywów:
      i. ultra-szerokokątny: min. 10MP i pole widzenia 125°,
      ii. szerokokątny: min. 12MP,

   umożliwiające rejestrowanie zdjęć i nagrywanie z stabilizacją obrazu (wideo: 4K, 1080p i 720p),
7. Posiadające zainstalowane min. cztery głośniki;
8. Obsługujące sieci komórkowe i bezprzewodowe:
   a) Wi-Fi min. 6E (802.11ax); min. dwa zakresy jednocześnie (2,4 GHz i 5 GHz);
   b) Bluetooth min. 5.3,
   c) 5G,
   d) LTE,
9. Poprawnie obsługujące funkcjonalność e-SIM;
10. Posiadające gniazdo na kartę typu nano-SIM;
11. Obsługujące systemy lokalizacji:
   a) GPS/GNSS,
   b) kompas cyfrowy,
   c) Wi-Fi,
   d) łączność komórkowa,
12. Wyposażone co najmniej w następujące czujniki:
   a) barometr,
   b) żyroskop trójosiowy,
   c) przyspieszeniomierz,
   d) czujnik oświetlenia zewnętrznego,
   e) skaner LiDAR,
   f) czujnik umożliwiający odblokowywanie urządzenia za pomocą twarzy;
13. Poprawnie obsługiwać odblokowywanie urządzenia za pomocą technologii rozpoznawania twarzy;
14. Wyposażone w Thunderbolt / USB 4 realizowane w postaci gniazda typu USB-C obsługujące:
   a) zasilanie,

b) standard DisplayPort,
c) standard Thunderbolt 3 (do 40Gb/s),
d) standard USB 4 (do 40Gb/s),
e) standard USB 3.1 drugiej generacji (do 10Gb/s).

1. Posiadające wbudowany akumulator litowo-jonowy o pojemności min. 28Wh do wielokrotnego ładowania, zapewniającą (po pełnym naładowaniu) co najmniej 9 godzin przeglądania Internetu przez sieć Wi-Fi;
2. Dostarczony z licencją na system IPadOS w wersji min. 16 lub równoważny.
3. Urządzenie musi być dostarczone bez blokad SIM LOCK;
4. Urządzenie musi być przeznaczone na rynek europejski oraz być fabrycznie nowe oraz fabrycznie zapakowane i tworzyć handlowy komplet tak, jak przewiduje to producent.
5. Preferowany przez Zamawiającego kolor czarny lub ciemno szary
6. Wraz z urządzeniem muszą zostać dostarczone dedykowane przez producenta:
   a) ładowarka ze gniazdem typu USB-C o mocy min. 20W z przewodem ze złączami typu USB-C – USB-C do ładowania urządzenia o długości min. 1 m.
   b) urządzenie do sporządzania notatek. Urządzenie to musi posiadać następujące cechy:
      i. podświetlane klawisze z mechanizmem nożycowym
      ii. wyposażone w gładzik, obsługujący kursor oraz gesty Multi-Touch
      iii. zapewniać swobodną regulację kąta nachylenia ekranu w celu jego optymalne ustawienie
      iv. być wyposażone w port typu USB-C, zapewniający możliwość ładowania urządzenia głównego oraz umożliwiający podłączenie akcesoriów zewnętrznych
      v. po złożeniu zapewniać ochronę z przodu i z tyłu urządzenia (funkcja etui)
      vi. preferowany przez Zamawiającego kolor czarny
   c) etui zapewniające ochronę z przodu i z tyłu urządzenia z funkcją automatycznego budzenia (po otwarciu etui) oraz usypiania (po zamknięciu). Etui musi zapewniać połączenie magnetyczne oraz zapewniać możliwość jego składania na różne sposoby, aby uzyskać podstawkę do czytania, oglądania oraz pisania. Preferowany przez Zamawiającego kolor czarny.
   d) urządzenie do sporządzania odręcznych notatek. Urządzenie to musi posiadać następujące cechy:
      i. zapewniać bezprzewodowe (automatyczne) parowanie i bezprzewodowe ładowanie
      ii. zapewniać magnetyczne połączenie z obudową urządzenia, podczas którego następuję bezprzewodowe ładowanie
      iii. zapewniać wrażliwość na siłę nacisku i kąt pochylenia.

15.6. Opis równoważności

Poniżej opisano kryteria, jakie Zamawiający będzie stosował w celu oceny równoważności rozwiązania zaproponowanego przez wykonawcę jako równoważne dla systemu operacyjnego IPadOS (w wersji 16 lub nowszy) lub równoważny.

Przez równoważność zamawiający rozumie konieczność:

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

16. Stacje zarządzania

16.1. Stacja Zarządzania Typ 1

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

16.1.1. Jednostka główna spełniająca poniższe wymagania:

1) Wyświetlacz: 14” cala, rozdzielczość 1920x1200, jasność min. 500 nit, z powłoką przeciwodblaskową i technologią niskiej emisji niebieskiego światła (ang. Low Blue Light);
2) Procesor: zgodny z x64, posiadający co najmniej 14 fizycznych rdzeni, w dwóch klasach wydajności (co najmniej 6 rdzenie zapewniające wydajność i co najmniej 8 rdzenie energooszczędne), co najmniej 20 wątków. Zaprojektowany do pracy w mobilnych stacjach roboczych (pobór mocy w podstawowym trybie pracy nie więcej niż 45W , w trybie turbo nie więcej niż 115W), co najmniej 24MB cache, osiągający wydajność minimum: 31900 punktów Passmark CPU Mark w teście wydajności Pass Mark Perfomance Test (stan na 05.04.2023) pracujący z minimalną częstotliwością w trybie turbo dla rdzeni energooszczędnych 4,10GHz oraz dla rdzeni zapewniających wydajność 5,4GHz;
3) Pamięć RAM: nie mniej niż 64 GB min DDR5;
4) Dysk twardy: nie mniej niż jeden dysk o pojemności min. 2TB w technologii M.2 SSD PCIe Gen4 x4 NVMe class min. 40;
5) dodatkowa karta graficzna z min. 8GB RAM o wydajności min. 19 TFLOPS (Single Precision Floating-Point Performance);
6) Zintegrowane porty (co najmniej):
   a) min. 4x gniazdo Thunderbolt 4 (USB Type-C) z obsługą PowerDelivery i DisplayPort,
   b) zintegrowany czytnik kart microSD,
   c) złącze słuchawkowo-mikrofonowe – Jack 3,5 mm,
7) Komunikacja:
   a) Wi-Fi 6E min. trzyzakresowa zgodna z co najmniej IEEE 802.11 ax/ac/a/b/g/n,
   b) Bluetooth min. 5.2.
8) Bateria: nie mniej niż 70Wh;
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) wbudowane gniazdo czytnika kart SmartCard Reader,
   g) wbudowany czytnik kart SmartCard Reader/NFC,
   h) 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,
   i) wbudowany układ zabezpieczający TPM (Trusted Platform Module) lub równoważny,
   j) 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 wykorzystywanych lub planowanych do wykorzystania w projekcie przez Zamawiającego następujących systemów operacyjnych:
    a) Microsoft Windows 11 Pro 64-bit,
    b) Ubuntu w wersji min. 20.04 LTS 64-bit,
    c) Red Hat Enterprise Linux w wersji min. 8.6.
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.

16.1.2. Monitor

Jeden monitor opisany w punkcie 16.3

16.1.3. Stacja dokująca

Jedna stacja dokująca opisana w punkcie 16.4

16.1.4. Zestaw klawiatura z myszą

Jeden zestaw klawiatura z myszą Typ A opisany w punkcie 16.5

16.2. Stacja Zarządzania Typ 2

Pojedyncza Stacja Zarządzania Typ 2 składa się z następujących części składowych:

16.2.1. Jednostka główna spełniająca poniższe wymagania:

1) Wyświetlacz: min. 14,2” cala, rozdzielczość min. 3024x1964, o jasność min. 1000 nit na całej powierzchni ekranu, kontraście min. 1 000 000:1 z funkcją dopasowania temperatury barw wyświetlacza do panującego oświetlenia;

2) Funkcję procesora oraz układu graficznego pełni system jednoukładowy (SoC), w którego skład wchodzi:
   a) co najmniej 12 fizycznych rdzeni, w dwóch klasach wydajności (co najmniej 8 rdzenie zapewniające wydajność i co najmniej 4 rdzenie energooszczędne),
   b) wbudowany procesor graficznym z co najmniej 38 rdzeniami,
   c) wbudowany co najmniej 16 rdzeniowy system wspomagający proces uczenia maszynowego,
3) zunifikowana pamięć RAM o pojemności co najmniej 96 GB;
4) Dysk twardy: nie mniej 2TB w technologii SSD;
5) Karta graficzna umożliwiająca jednoczesne wyświetlanie obrazu w pełnej natywnej rozdzielczości na wbudowanym wyświetlaczu oraz obsługę trzech wyświetlaczy zewnętrznych o rozdzielczości 6K przy 60Hz każdy;
6) Zintegrowane porty:
   a) min. 3x gniazda Thunderbolt 4 (USB-C) Type-C z obsługą:
      i. Display Port,
      ii. USB 4 (do 40Gb/s),
      iii. Power Delivery (ładowania),
      iv. Thunderbolt 4 (do 40Gb/s).
   b) Gniazdo HDMI
   c) Gniazdo na kartę SDXC
   d) magnetyczne złącze do zasilania
   e) złącze słuchawkowo-mikrofonowe – Jack 3,5 mm.
7) Komunikacja:
   a) Wi-Fi min. dwuzakresowa zgodna z co najmniej 6E IEEE 802.11 ax,
   b) Bluetooth min. 5.3.
8) Bateria: nie mniej niż 70Wh zapewniające min. 12 godzin bezprzewodowego przeglądania Internetu;
9) Wraz ze stacją zarządzającą musi zostać dostarczony dedykowane przez producenta zasilacz o mocy min. 96W ze złączem USB Type-C, z dedykowanym kablem USB Type-C – magnetyczne złącze do zasilania o długości 2 metrów. Zasilacz musi poprawnie pracować w zakresie od 100V do 240V oraz umożliwiać podłączenie do zasilania z gniazdek używanych na terenie PL bez dodatkowych przejściówek lub adapterów. Wraz z zasilaczem musi zostać dostarczony dedykowany przez producenta przedłużacz o długości min. 1,8 m zwiększający zasięg oryginalnego zasilacza;
10) Waga: nie więcej niż 1,7 kg;
11) Dodatkowe wymagania:
   a) klawiatura: QWERTY, podświetlana w układzie angielski (międzynarodowy),
   b) gładzik z obsługa siły nacisku oraz obsługą gestów Multi-Touch,
   c) co najmniej sześć wbudowanych głośników z układem min. trzech mikrofonów,
   d) obsługa przestrzennego dźwięku stereo oraz Dolby Atmos,
   e) wbudowana kamera HD o rozdzielczości min. 1080p,
   f) zintegrowany czytnik linii papilarnych.
12) System operacyjny: Licencja na system macOS Ventura lub nowszy lub równoważny.
13) Wsparcie producenta dla następujących systemów operacyjnych:
   a) macOS w oferowanej wersji,
14) Preferowany przez zamawiającego kolor ciemno szary.

16.2.2. Monitor

Jeden monitor opisany w punkcie 16.3

16.2.3. Stacja dokująca

Jedna stacja dokująca opisana w punkcie 16.4

16.2.4. Zestaw klawiatura z myszą

Jeden zestaw klawiatura z myszą Typ B opisany w punkcie 16.6

16.3. Monitor

Kompatybilny ze stacjami zarządzania Typu 1-2 monitor LCD 27” 4K ze złączem USB Type-C o następującej parametrach technicznych:

a) przekątna „27” – widoczna matryca min. 26.96" w formacie 16:9,
b) rozdzielczość 3840 x 2160 (WQHD),
c) matowa matryca IPS,
d) kontrast min. 2000:1,
e) jasność min. 400 cd/m^2
f) czas reakcji monitora – 5 ms,
g) obsługa kolorów – min, 1 miliard;
h) paleta kolorów – 100% Rec 709, 100% sRGB, 98% DCI-P3
i) kąty widzenia: 178° w pionie i poziomie,
j) 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;
k) funkcje: funkcja obrotowego ekranu (PIVOT -90° /+90°), regulacja wysokości (min. 150mm), regulacja kąta pochylenia (w zakresie min. -5° /+20°)
l) dołączone przewody (min): 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,
m) zasilanie – napięcie 100-240VAC,
n) z monitorem musi zostać dostarczony przewód umożliwiającym zasilanie z gniazdek używanych na terenie PL,
o) Waga z podstawką: nie więcej niż 6.65 kg.

16.4. Stacja dokująca

Stacja dokująca kompatybilna ze stacjami zarządzania Typu 1-2 podłączana poprzez Thunderbolt 4 (USB Type-C) za pomocą złącza USB Type-C. Musi być wyposażona co najmniej w następujące złącza (gniazda):

a) 1x USB Type-C w standardzie co najmniej USB 3.2 Gen 2,
b) 3x USB Type-A w standardzie co najmniej 3.2 Gen 1 w tym co najmniej 1 z funkcjonalnością PowerShare
c) 2x DisplayPort 1.4,
d) 1x HDMI min. 2.0,
e) 1x USB-C w standardzie co najmniej USB 3.2 Gen 2 z funkcją DisplayPort 1.4

f) 1x LAN 10/100/1000 Ethernet (RJ-45)
g) 2x Thunderbolt 4 w postaci złącza USB Type-C,
h) gniazdo do podłączenia zewnętrznego dedykowanego do stacji 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. 0,8m.

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

Ze stacją musi zostać dostarczony dedykowany do niej zasilacz, zapewniający zasilanie podłączonego do stacji dokującej komputera o mocy min. 90W (130W w przypadku podłączenie komputera, którego producentem jest producent 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 1-2 bez potrzeby podłączania ich do dodatkowego zasilania.

Dodatkowa wymagana poprawna obsługa: PXE Boot, Wake-On-LAN, Wake-On-Dock. Stacja dokująca musi poprawnie współpracować z wykorzystywanymi lub planowanymi do wykorzystania w projekcie przez Zamawiającego następującymi systemami operacyjnymi: Windows 10 i 11, Ubuntu min. 20.04, macOS (w przypadku systemu macOS nie jest wymagana obsługa funkcjonalności PXE Boot, Wake-On-LAN, Wake-On-Dock oraz praca z 3 monitorami w rozdzielczości 4k).

16.5. Zestaw klawiatura z myszą Typ A

1) Kompatybilny ze stacjami zarządzania Typu 1 zestaw klawiatury i myszy.
2) Musi posiadać następującą funkcjonalność:
   a) zasilanie za pomocą baterii 2x AAA (klawiatura) oraz 1xAA (mysz) – poprawność pracy na jednym komplecie baterii 36 miesięcy,
   b) możliwość jednoczesnego bezprzewodowego podłączenia do trzech różnych komputerów – jednego za pomocą odbiornika USB, pozostałych dwóch za pomocą Bluetooth. Przełączania pomiędzy poszczególnymi komputerami muszą być realizowane przy użyciu klawisza lub przycisku na klawiaturze lub myszy. Aktualne 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. 1000dpi,
   e) mysz musi posiadać co najmniej 7 przycisków,
   f) poprawna współpraca z wykorzystywanymi lub planowanymi do wykorzystania w projekcie przez Zamawiającego systemami: Microsoft Windows 10, Android, Apple macOS.
3) Do zestawu muszą zostać dołączone baterie w liczbie i modelu umożliwiającym poprawną pracę zestawu.

16.6. Zestaw klawiatura z myszą Typ B

Dedykowana przez producenta klawiatura oraz mysz bezprzewodowa do stacji zarządzania Typu 2 o następujących parametrach technicznych:

1) bezprzewodowa klawiatura z wydzielonym polem numerycznym:
    a) układ klawiatury: angielski (międzynarodowy),
    b) wyposażona w oddzielny blok numeryczny,
    c) dedykowane klawisze do obsługi wykorzystywanego lub planowanego do wykorzystania w projekcie przez Zamawiającego systemu macOS oraz multimediów,
    d) komunikacja za pomocą Bluetooth,
    e) wbudowane gniazdo Lightning służące do ładowania wbudowanego akumulatora oraz parowania myszy ze zgodnym komputerem,
    f) parowanie klawiatury musi odbywać się automatycznie poprzez podłączenie za pomocą dostarczonego kabla do portu USB zgodnego komputera,
    g) wbudowany akumulator wielokrotnego ładowania (jednorazowe naładowanie wystarcza na miesiąc pracy),
    h) zintegrowany z klawiaturą czytnik linii papilarnych,
    i) z klawiaturą musi zostać dostarczony przewód z USB Type-C na Lightning, który umożliwia ładowanie oraz parowanie ze zgodnym komputerem,
    j) waga nie więcej niż 0,4 kg,
    k) kolor identyczny jak myszy z pozycji 2).
    l) Preferowany przez zamawiającego kolor szary lub biały
2) bezprzewodowa mysz:
    a) symetryczna budowa zapewniająca wygodną pracę osobom prawo i leworęcznym,
    b) obsługa standardu Multi-Touch z obsługa gestów,
    c) komunikacja za pomocą Bluetooth,
    d) wbudowane gniazdo Lightning służące do ładowania wbudowanego akumulatora oraz parowania mysz ze zgodnym komputerem,
    e) parowanie myszy musi odbywać się automatycznie poprzez podłączenie za pomocą dostarczonego kabla do portu USB zgodnego komputera,
    f) wbudowany akumulator wielokrotnego ładowania (jednorazowe naładowanie wystarcza na miesiąc pracy),
    g) z myszą musi zostać dostarczony przewód z USB Type-C na Lightning, który umożliwia ładowanie oraz parowanie ze zgodnym komputerem,
    h) waga nie więcej niż 0,1 kg,
    i) kolor identyczny jak klawiatury z pozycji 1).

16.7. 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.

Poniżej opisano kryteria, jakie Zamawiający będzie stosował w celu oceny równoważności rozwiązania zaproponowanego przez Wykonawcę jako równoważne dla systemu operacyjnego macOS (Ventura lub nowszy) lub równoważny.

Przez równoważność Zamawiający rozumie konieczność:

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

17. Przełączniki warstwy trzeciej

1) Przełączniki muszą być przystosowane do instalacji w standardowych 19” szafach teleinformatycznych (EIA-310). Przełączniki muszą posiadać wszystkie elementy potrzebne do zainstalowania w szafie.

2) Przełącznik musi obsługiwać przełączanie ramek o długości co najmniej 9216 oktetów/bajtów.

3) Urządzenie musi obsługiwać edycję konfiguracji implementowanej na urządzeniu bez natychmiastowego uruchamiania poszczególnych elementów podlegających edycji, cofanie zmian konfiguracyjnych do poprzedniej wersji. Ponadto urządzenie musi obsługiwać automatyczne przywrócenie poprzedniej wersji konfiguracji po zdefiniowanym czasie, w którym użytkownik nie potwierdzi powtórnie wprowadzonych zmian (np. w przypadku utraty łączności administracyjnej z urządzeniem w wyniku ostatniej wprowadzonej zmiany). Na urządzeniu musi być przechowywane co najmniej 10 ostatnich konfiguracji.

4) Urządzenie musi obsługiwać dostęp do interfejsu CLI za pomocą protokołu SSHv2 oraz obsługiwać transfer plików za pomocą protokołu SFTP (wymagana jest obsługa funkcji serwera).

5) Urządzenie musi być wyposażone w port konsolowy do dołączenia konsoli RS-232 z gniazdem RJ45.

6) Urządzenie musi obsługiwać protokół NETCONF z wykorzystaniem komunikacji za pośrednictwem protokołu SSH.

7) Urządzenie musi obsługiwać mechanizm ochrony swojej warstwy kontrolnej przed atakami typu DoS (DDoS).

8) Wszystkie moduły optyczne wskazane poniżej w sekcji „Wymagania Szczegółowe” muszą być dostarczone przez Wykonawcę wraz z przełącznikami.

9) Urządzenie musi obsługiwać filtrowanie niepożądanego ruchu definiowanego przez administratora związanego z działaniem protokołów sygnalizacyjnych (np. protokoły routingu) i procesów zarządzania urządzeniem (np. protokoły SNMP, dostęp SSH) kierowanego do modułu sterującego (ang. control plane).

10) **UWAGA**: Jeżeli zaaplikowanie działającego globalnie filtra dla ruchu kierowanego do modułu zarządzania (np. na wewnętrznym interfejsie typu loopback) nie jest możliwe, urządzenie musi obsługiwać mechanizm automatycznej implementacji takiego filtra na pozostałych interfejsach, na których jest to konieczne, aby zapewnić filtrowanie ruchu kierowanego do modułu zarządzającego.

11) Przełącznik musi być wyposażony w co najmniej w następującą liczbę i typy interfejsów:

    a) **23** interfejsy pracujące w następujących trybach w zależności od zainstalowanego modułu optycznego:

i. 10GE po zainstalowaniu modułu typu SFP+

ii. 25GE po zainstalowaniu modułu typu SFP28

iii. 1GE po zainstalowaniu modułu typu SFP

b) **4** interfejsy 100GE do obsadzenia modułami QSFP28 oraz QSFP+ umożliwiające pracę w następujących trybach:

i. 100GE po obsadzeniu modułem typu QSFP28

ii. 40GE po obsadzeniu modułem typu QSFP+

12) Przełącznik musi być wyposażony co najmniej w następującą liczbę i typy modułów:

a) **5** modułów QSFP28 100GBASE-LR4

UWAGA: Moduły typu QSFP28 100GBASE-LR4 o zasięgu do 10 km. 3 moduły zostaną wykorzystane po stronie bieżącego urządzenia a 2 moduły po stronie przełączników sieciowych 100G-core (po jednym na każdy przełącznik).

13) W przypadku stosowania modelu licencjonowania przepustowości sumarycznie wykorzystywanych interfejsów, przełącznik musi być wyposażony w licencje umożliwiające jednoczesną pracę interfejsom o sumarycznej przepustowości co najmniej **400** Gb/s

14) Niezależnie od wymogu określonego w punkcie 3) powyżej przepustowość urządzenia nie może być mniejsza niż **360** Gb/s oraz **300** Mp/s (milionów pakietów na sekundę)

15) Przełącznik musi być wyposażony w co najmniej dwa zasilacze przystosowane do zasilania napięciem 230V AC. Przełącznik musi poprawnie pracować poprawnie z jednym zasilaczem. Przełącznik musi obsługiwać funkcję wymiany pojedynczego zasilacza przy zachowaniu ciągłości pacy całego urządzenia (ang. hot swap).

16) Przełącznik musi poprawnie obsługiwać co najmniej 256 000 prefiksów IPv4 w tablicy RIB

17) Przełącznik musi poprawnie obsługiwać co najmniej 64 000 prefiksów IPv6 w tablicy RIB

18) Przełącznik musi poprawnie obsługiwać jednocześnie co najmniej:

a) 256 000 prefiksów IPv4 w tablicy FIB oraz
b) 64 000 prefiksów IPv6 w tablicy FIB oraz
c) 256 000 adresów MAC

19) Przełącznik musi poprawnie obsługiwać co najmniej 8 000 grup multicast dla protokołu IPv4

20) Przełącznik musi poprawnie obsługiwać co najmniej 2 000 grup multicast dla protokołu IPv6

21) Przełącznik musi poprawnie obsługiwać co najmniej 10 000 etykiet MPLS w tablicy FIB

22) Przełącznik musi obsługiwać co najmniej 14 grup zagregowanych interfejsów (ang. LAG)

23) Przełącznik musi obsługiwać co najmniej 16 interfejsów fizycznych w pojedynczej grupie interfejsów zagregowanych (LAG)

24) Przełącznik musi obsługiwać co najmniej 1000 nawiązanych sesji BGP

25) Przełącznik musi obsługiwać co najmniej 2000 instancji EVPN

26) Przełącznik musi obsługiwać co najmniej 32 instancje L3VPN (VRF)

27) Przełącznik musi obsługiwać co najmniej 8 000 instancji typu pseudowire (E-LINE w oparciu o enkapsulację MPLS)

28) Przełącznik musi obsługiwać co najmniej 1000 połączeń lokalnych warstwy 2 OSI (ang. local cross connect)

29) Przełącznik musi obsługiwać co najmniej 8 instancji wirtualnych sieci typu NG-MVPN (multicast)

30) Urządzenie musi obsługiwać agregację interfejsów fizycznych z wykorzystaniem protokołu LACP (IEEE 802.3ad).

31) Urządzenie musi obsługiwać identyfikatory VLAN o znaczeniu lokalnym dla portu fizycznego (ang. local vlan significance). Oznacza to m.in. iż ten sam identyfikator VLAN może być użyty na dowolnej liczbie pozostałych portów fizycznych niezależnie.

32) Urządzenie musi obsługiwać znakowanie ramek Ethernet zgodnie z 802.1Q w pełnym zakresie VLANów (1-4094).

33) Urządzenie musi obsługiwać możliwość podziału domeny rozgłoszeniowej na wiele odizolowanych domen rozgłoszeniowych (Private VLAN).

34) Urządzenie musi obsługiwać oznaczanie pakietów dwoma znacznikami 802.1Q (VLAN) na interfejsie.

35) Urządzenie musi obsługiwać ograniczenia dla ruchu typu broadcast, multicast i unknown unicast. Musi obsługiwać możliwość odrzucania ruchu przekraczającego wyznaczone progi wielkości ruchu.

36) Urządzenie musi obsługiwać możliwość wyłączenia funkcjonalności uczenia się adresów MAC dostępnych poprzez dany interfejs (ang. MAC learning).

37) Urządzenie musi obsługiwać możliwość ograniczania ilości interfejsów przypisanych do danej instancji przełączania.

38) Urządzenie musi obsługiwać możliwość jednoczesnej konfiguracji na tym samym interfejsie fizycznym usług typu E-LINE (znakowanych zgodnie z IEEE 802.1Q) realizowanych w technologii MPLS oraz przełączania warstwy trzeciej OSI wykorzystujących IPv4 oraz IPv6. Rozróżnianie usług na interfejsie fizycznym musi być realizowane z wykorzystaniem znaczników VLAN ID (IEEE 802.1Q).

39) Urządzenie musi obsługiwać możliwość skonfigurowania portu w trybie przełącznika pozwalając jednocześnie na przenoszenie wskazanej listy wielu VLANów, wraz z określeniem VLAN, który nie będzie wymagał oznaczania tagiem 802.1Q (native VLAN).

40) Urządzenie musi obsługiwać możliwość skonfigurowania interfejsów warstwy 3 (L3) OSI przypisanych do danego VLANu i pozwalających na zapewnienie funkcjonalności bramy domyślnej dla urządzeń w danym VLANie tzw. Integrated Routing and Bridging (IRB).

41) Urządzenie musi obsługiwać protokół Spanning Tree i Rapid Spanning Tree, zgodnie z IEEE 802.1D-2004, oraz protokół Multiple Spanning Tree zgodnie z IEEE 802.1Q-2003.

42) Urządzenie musi pozwalać na konfigurację zachowania w sytuacji, gdy pakiety STP BPDU nie są odbierane na danym interfejsie.

43) Urządzenie musi obsługiwać możliwość określenia zachowania interfejsu w przypadku otrzymania pakietów STP BPDU (tzw. BPDU protection).

44) Urządzenie musi obsługiwać protokół ERPS, opisanego w ramach ITU-T G.8032, zarówno dla wersji v1, jak i v2.

45) Urządzenie musi obsługiwać protokół LLDP (IEEE 802.1ab, Link Layer Discovery Protocol)

46) Urządzenie musi umożliwiać określenie listy lub zakresu VLANów obsługiwanych na danym interfejsie logicznym.

47) Urządzenie musi obsługiwać manipulację znacznikiem VLAN w ramkach otrzymanych na interfejsie logicznym. Dostępne muszą być co najmniej następujące akcje: zdjęcie znacznika VLAN ID (pop), dodanie znacznika VLAN ID (push), zamiana znacznika VLAN ID (swap).

48) Urządzenie musi obsługiwać podwójne znaczniki VLAN ID (IEEE 802.1q) dla interfejsów warstwy trzeciej OSI (ang. double tagging).

49) Urządzenie musi obsługiwać protokół VRRP zgodnie z RFC 3768, Virtual Router Redundancy Protocol (VRRP).

50) Urządzenie musi obsługiwać protokół BGP oraz następujące jego funkcje

    a) RFC 1745, BGP4/IDRP for IP—OSPF Interaction
    b) RFC 1772, Application of the Border Gateway Protocol in the Internet
    c) RFC 1997, BGP Communities Attribute
    d) RFC 2283, Multiprotocol Extensions for BGP-4
    e) RFC 2385, Protection of BGP Sessions via the TCP MD5 Signature Option
    f) RFC 2439, BGP Route Flap Damping
    g) RFC 2545, Use of BGP-4 Multiprotocol Extensions for IPv6 Inter-Domain Routing
    h) RFC 2796, BGP Route Reflection – An Alternative to Full Mesh IBGP
    i) RFC 2858, Multiprotocol Extensions for BGP-4
    j) RFC 2918, Route Refresh Capability for BGP-4
    k) RFC 3065, Autonomous System Confederations for BGP
    l) RFC 3107, Carrying Label Information in BGP-4
    m) RFC 3345, Border Gateway Protocol (BGP) Persistent Route Oscillation Condition
    n) RFC 3392, Capabilities Advertisement with BGP-4
    o) RFC 4271, A Border Gateway Protocol 4 (BGP-4)
    p) RFC 4273, Definitions of Managed Objects for BGP-4
    q) RFC 4360, BGP Extended Communities Attribute

r) RFC 4364, BGP/MPLS IP Virtual Private Networks (VPNs)
s) RFC 4456, BGP Route Reflection: An Alternative to Full Mesh Internal BGP (IBGP)
t) RFC 4486, Subcodes for BGP Cease Notification Message
u) RFC 4659, BGP-MPLS IP Virtual Private Network (VPN) Extension for IPv6 VPN
v) RFC 4632, Classless Inter-domain Routing (CIDR): The Internet Address Assignment and Aggregation Plan
w) RFC 4684, Constrained Route Distribution for Border Gateway Protocol/MultiProtocol Label Switching (BGP/MPLS) Internet Protocol (IP) Virtual Private Networks (VPNs)
x) RFC 4724, Graceful Restart Mechanism for BGP
y) RFC 4760, Multiprotocol Extensions for BGP-4
z) RFC 4781, Graceful Restart Mechanism for BGP with MPLS
aa) RFC 4798, Connecting IPv6 Islands over IPv4 MPLS Using IPv6 Provider Edge Routers (6PE) z wyjątkiem opcji 4b
bb) RFC 4893, BGP Support for Four-octet AS Number Space
cc) RFC 5004, Avoid BGP Best Path Transitions from One External to Another
dd) RFC 5065, Autonomous System Confederations for BGP
ee) RFC 5082, The Generalized TTL Security Mechanism (GTSM)
ff) RFC 5396, Textual Representation of Autonomous System (AS) Numbers
gg) RFC 5492, Capabilities Advertisement with BGP-4
hh) RFC 5512, The BGP Encapsulation Subsequent Address Family Identifier (SAFI) and the BGP Tunnel Encapsulation Attribute
ii) RFC 5549, Advertising IPv4 Network Layer Reachability Information with an IPv6 Next Hop
jj) RFC 5575, Dissemination of flow specification rules
kk) RFC 5668, 4-Octet AS Specific BGP Extended Community
ll) RFC 6286, Autonomous-System-Wide Unique BGP Identifier for BGP-4- fully compliant
mm) RFC 6368, Internal BGP as the Provider/Customer Edge Protocol for BGP/MPLS IP Virtual Private Networks (VPNs)
nn) RFC 6810, The Resource Public Key Infrastructure (RPKI) to Router Protocol
oo) RFC 6811, BGP Prefix Origin Validation
pp) RFC 6996, Autonomous System (AS) Reservation for Private Use
qq) RFC 7300, Reservation of Last Autonomous System (AS) Numbers
rr) RFC 7611, BGP ACCEPT_OWN Community Attribute
ss) RFC 7752, North-Bound Distribution of Link-State and Traffic Engineering (TE) Information Using BGP
tt) RFC 7854, BGP Monitoring Protocol (BMP)
uu) RFC 7911, Advertisement of Multiple Paths in BGP
vv) RFC 8212, Default External BGP (EBGP) Route Propagation Behavior without Policies
ww) RFC 8326, Graceful BGP session Shutdown"

51) Urządzenie musi obsługiwać możliwość określenia maksymalnej liczby prefiksów, jaka może być otrzymana w ramach sesji BGP.

52) Urządzenie musi obsługiwać funkcjonalność BGP Additional Paths dla sesji eBGP.

53) Urządzenie musi obsługiwać przenoszenie przez sesję BGP dla protokołu IPv4 prefiksów protokołu IPv6 (ang. IPv4 transport for IPv4 and IPv6 routes).

54) Urządzenie musi obsługiwać zestawienie sesji BGP protokołu IPv6.

55) Urządzenie musi obsługiwać sesje BGP typu labeled unicast (RFC 3107, Carrying Label Information in BGP-4)

56) Urządzenie musi obsługiwać mechanizm BGP MTU Discovery.

57) Urządzenie musi obsługiwać mechanizm BGP Multipath, czy możliwość balansowania (rozkładania) pakietów IPv4 oraz IPv6 na różne (równoległe) trasy do prefiksu docelowego otrzymane poprzez sesje BGP.

58) Urządzenie musi obsługiwać możliwość priorytetyzacji określonych prefiksów wysyłanych w ramach sesji BGP.

59) Urządzenie musi obsługiwać mechanizm Route Reflection protokołu BGP (RFC4456).

60) Urządzenie musi obsługiwać możliwość zerwania sesji BGP w przypadku gdy określony przez administratora limit dla prefiksów otrzymywanych zostanie przekroczony.

61) Urządzenie musi obsługiwać mechanizm BGP Graceful Shutdown (RFC8326).

62) Urządzenie musi obsługiwać protokół IS-IS oraz następujące jego funkcje opisane w poniższych standardach

    a) International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 8473, Information technology — Protocol for providing the connectionless-mode network service
    b) ISO 9542, End System to Intermediate System Routing Exchange Protocol for Use in Conjunction with the Protocol for the Provision of the Connectionless-mode Network Service
    c) ISO/IEC 10589, Information technology — Telecommunications and information exchange between systems — Intermediate System to Intermediate System intra-domain routeing information exchange protocol for use in conjunction with the protocol for providing the connectionless-mode network service (ISO 8473)
    d) RFC 1195, Use of OSI IS-IS for Routing in TCP/IP and Dual Environments
    e) RFC 3719, Recommendations for Interoperable Networks using Intermediate System to Intermediate System (IS-IS)
    f) RFC 3847, Restart Signaling for Intermediate System to Intermediate System (IS-IS)
    g) RFC 5120, M-ISIS: Multi Topology (MT) Routing in Intermediate System to Intermediate Systems (ISISs)
    h) RFC 5130, A Policy Control Mechanism in IS-IS Using Administrative Tags
    i) RFC 5286, Basic Specification for IP Fast Reroute: Loop-Free Alternates
    j) RFC 5301, Dynamic Hostname Exchange Mechanism for IS-IS
    k) RFC 5302, Domain-Wide Prefix Distribution with Two-Level IS-IS
    l) RFC 5303, Three-Way Handshake for IS-IS Point-to-Point Adjacencies
    m) RFC 5304, IS-IS Cryptographic Authentication
    n) RFC 5305, IS-IS Extensions for Traffic Engineering
    o) RFC 5306, Restart Signaling for IS-IS

p) RFC 5307, IS-IS Extensions in Support of Generalized Multi-Protocol Label Switching (GMPLS)
q) RFC 5308, Routing IPv6 with IS-IS
r) RFC 5310, IS-IS Generic Cryptographic Authentication
s) RFC 5880, Bidirectional Forwarding Detection (BFD)
t) RFC 6232, Purge Originator Identification TLV for IS-IS

63) Urządzenie musi obsługiwać przenoszenie informacji o prefiksach protokołu IPv4 w ramach działania protokołu IS-IS.

64) Urządzenie musi obsługiwać przenoszenie informacji o prefiksach protokołu IPv6 w ramach działania protokołu IS-IS.

65) Urządzenie musi obsługiwać możliwość skonfigurowania różnych topologii IS-IS dla protokołów IPv4 i IPv6.

66) Urządzenie musi obsługiwać mechanizm LFA (Loop Free Alternate) w ramach protokołu IS-IS.

67) Urządzenie musi obsługiwać możliwość wykorzystania ścieżek MPLS LSP jako bramy (ang. next-hop) dla prefiksów obsługiwanych w ramach protokół IS-IS.

68) Urządzenie musi obsługiwać mechanizm autentykacji sesji IS-IS przy pomocy MD5.

69) Urządzenie musi obsługiwać mechanizm autentykacji sesji IS-IS przy pomocy klucza statycznego.

70) Urządzenie musi obsługiwać protokół OSPFv2, OSPFv3 oraz następujące funkcje opisane w poniższych standardach

a) RFC 1583, OSPF Version 2
b) RFC 1765, OSPF Database Overflow
c) RFC 1793, Extending OSPF to Support Demand Circuits
d) RFC 1850, OSPF Version 2 Management Information Base
e) RFC 2154, OSPF with Digital Signatures
f) RFC 2328, OSPF Version 2
g) RFC 2370, The OSPF Opaque LSA Option
h) RFC 3101, The OSPF Not-So-Stubby Area (NSSA) Option
i) RFC 3623, Graceful OSPF Restart
j) RFC 3630, Traffic Engineering (TE) Extensions to OSPF Version 2
k) RFC 4136, OSPF Refresh and Flooding Reduction in Stable Topologies
l) RFC 4203, OSPF Extensions in Support of Generalized Multi-Protocol Label Switching (GMPLS)
m) RFC 4552, Authentication/Confidentiality for OSPFv3
n) RFC 4576, Using a Link State Advertisement (LSA) Options Bit to Prevent Looping in BGP/MPLS IP Virtual Private Networks (VPNs)
o) RFC 4577, OSPF as the Provider/Customer Edge Protocol for BGP/MPLS IP Virtual Private Networks (VPNs)
p) RFC 4811, OSPF Out-of-Band Link State Database (LSDB) Resynchronization
q) RFC 4812, OSPF Restart Signaling

r) RFC 4813, OSPF Link-Local Signaling
s) RFC 4915, Multi-Topology (MT) Routing in OSPF
t) RFC 5185, OSPF Multi-Area Adjacency
u) RFC 5187, OSPFv3 Graceful Restart
v) RFC 5250, The OSPF Opaque LSA Option
w) RFC 5286, Basic Specification for IP Fast Reroute: Loop-Free Alternates
x) RFC 5340, OSPF for IPv6 (RFC 2740 is obsoleted by RFC 5340)
y) RFC 5838, Support of Address Families in OSPFv3
z) Internet draft draft-ietf-ospf-af-alt-10.txt, Support of address families in OSPFv3
aa) Internet draft draft-katz-ward-bfd-02.txt, Bidirectional Forwarding Detection
bb) RFC 8665, OSPF Extensions for Segment Routing
cc) Internet draft draft-ietf-lsr-flex-algo-07.txt, IGP Flexible Algorithm
dd) RFC 3137, OSPF Stub Router Advertisement
ee) RFC 3509, Alternative Implementations of OSPF Area Border Routers
ff) RFC 5309, Point-to-Point Operation over LAN in Link State Routing Protocols
gg) RFC 8920, OSPF Application-Specific Link Attributes
hh) RFC 8920, OSPFv2 Prefix/Link Attribute Advertisement

71) Urządzenie musi obsługiwać mechanizm autentykacji sesji OSPF przy pomocy klucza statycznego.

72) Urządzenie musi obsługiwać mechanizm autentykacji sesji OSPF przy pomocy MD5.

73) Urządzenie musi obsługiwać mechanizm ochrony bazy danych OSPF i OSPFv3 poprzez ograniczenie liczby LSA generowanych w ramach pojedynczej instancji OSPF.

74) Urządzenie musi obsługiwać konfigurację filtrów LSA typu 3 otrzymywanych i wysyłanych w ramach OSPF i OSPFv3.

75) Urządzenie musi obsługiwać konfigurację różnych topologii w ramach protokołu OSPF (Multi-Topology Routing), czyli różne topologie dla różnych klas ruchu przenoszonych przez urządzenie.

76) Urządzenie musi obsługiwać możliwość wykorzystania ścieżek MPLS LSP jako bramy (ang. next-hop) dla prefiksów obsługiwanych w ramach protokół OSPF.

77) Urządzenie musi obsługiwać mechanizmy balansowania (rozdzielania) pakietów na różne łącza w oparciu o nagłówek warstwy trzeciej.

78) Urządzenie musi obsługiwać mechanizmy balansowania (rozdzielania) pakietów na różne łącza w oparciu o nagłówek warstwy czwartej.

79) Urządzenie musi obsługiwać mechanizmy balansowania (rozdzielania) pakietów na różne łącza w oparciu o etykietę MPLS.

80) Urządzenie musi obsługiwać mechanizmy balansowania (rozdzielania) pakietów MPLS w oparciu o zawartość nagłówków warstwy trzeciej i czwartej tychże pakietów.

81) Urządzenie musi obsługiwać wirtualne sieci L3VPN dla protokołów IPv4 i IPv6, bazujące na technologii MPLS.

82) Urządzenie musi obsługiwać mechanizm VRRP w ramach instancji sieci wirtualnych L3VPN bazujących na technologii MPLS.

83) Urządzenie musi obsługiwać sieci L3VPN realizujące następujące funkcjonalności:

a) RFC 2283, Multiprotocol Extensions for BGP-4
b) RFC 2685, Virtual Private Networks Identifier
c) RFC 2858, Multiprotocol Extensions for BGP-4
d) RFC 4364, BGP/MPLS IP Virtual Private Networks (VPNs)
e) RFC 4379, Detecting Multi-Protocol Label Switched (MPLS) Data Plane Failures
f) RFC 4576, Using a Link State Advertisement (LSA) Options Bit to Prevent Looping in BGP/MPLS IP Virtual Private Networks (VPNs)
g) RFC 4577, OSPF as the Provider/Customer Edge Protocol for BGP/MPLS IP Virtual Private Networks (VPNs)
h) RFC 4659, BGP-MPLS IP Virtual Private Network (VPN) Extension for IPv6 VPN
i) RFC 4684, Constrained Route Distribution for Border Gateway Protocol/MultiProtocol Label Switching (BGP/MPLS) Internet Protocol (IP) Virtual Private Networks (VPNs)"

84) Urządzenie musi obsługiwać protokoły BGP, IS-IS, OSPF oraz OSPFv3 działające w ramach (wewnątrz) wirtualnych sieci L3VPN

85) Urządzenie musi obsługiwać wariant Inter-AS L3VPN Option B (opisaney w ramach RFC 4364, BGP/MPLS IP Virtual Private Networks (VPNs) dla sieci L3VPN wykorzystujących technologię MPLS.

86) Urządzenie musi obsługiwać wariant Inter-AS L3VPN Option C (opisany w ramach RFC 4364, BGP/MPLS IP Virtual Private Networks (VPNs) dla sieci L3VPN wykorzystujących technologię MPLS.

87) Urządzenie musi obsługiwać wirtualne sieci VPLS oraz następujące ich funkcjonalności:

a) RFC 4761, Virtual Private LAN Service (VPLS) Using BGP for Auto-Discovery and Signaling
b) RFC 4762, Virtual Private LAN Service (VPLS) Using Label Distribution Protocol (LDP) Signaling
c) FEC128
d) BGP Discovery FEC129

88) Urządzenie musi obsługiwać wirtualne sieci punkt-punkt VPWS/PWE i ich następujące funkcje:
d) RFC 4447, Pseudowire Setup and Maintenance Using the Label Distribution Protocol (LDP)
e) RFC 4448, Encapsulation Methods for Transport of Ethernet over MPLS Networks
f) RFC 6074, Provisioning, Auto-Discovery, and Signaling in Layer 2 Virtual Private Networks (L2VPNs)
g) RFC 6391, Flow-Aware Transport of Pseudowires over an MPLS Packet Switched Network
h) RFC 6790, The Use of Entropy Labels in MPLS Forwarding

89) Urządzenie musi obsługiwać połączenia punkt-punkt (VPWS/PWE) sygnalizowane przy pomocy LDP z wykorzystaniem control word.

90) Urządzenie musi obsługiwać połączenia punkt-punkt (VPWS/PWE) sygnalizowane przy pomocy LDP bez wykorzystania control word.

91) Urządzenie musi obsługiwać połączenia punkt-punkt (VPWS/PWE), których oba końce znajdują się na tym samym urządzeniu.

92) Urządzenie musi obsługiwać połączenia punkt-punkt (VPWS/PWE), w ramach których wykonywana jest manipulacja/przepisywanie wartości VID (VLAN)

93) Urządzenie musi obsługiwać połączenia punkt-punkt (VPWS/PWE) sygnalizowane przy pomocy BGP.

94) Urządzenie musi obsługiwać połączenia punkt-punkt (VPWS/PWE) sygnalizowane przy pomocy BGP z wykorzystaniem control word.

95) Urządzenie musi obsługiwać połączenia punkt-punkt (VPWS/PWE) sygnalizowane przy pomocy BGP bez wykorzystania control word.

96) Urządzenie musi obsługiwać połączenia punkt-punkt (VPWS/PWE) sygnalizowane przy pomocy LDP.

97) Urządzenie musi obsługiwać automatyczne wykrywanie routerów PE będące drugim końcem połączenia VPWS przy pomocy FEC 129 również dla połączeń sygnalizowanych przy pomocy LDP.

98) Urządzenie musi obsługiwać połączenia punkt-punkt (VPWS/PWE) sygnalizowane przy pomocy LDP z równoczesnym wparciem dla modyfikacji wartości pola VID (VLAN) (akcje pop/swap/push).

99) Urządzenie musi obsługiwać połączenia punkt-punkt (VPWS/PWE) sygnalizowane przy pomocy LDP na łączach zagregowanych (ang. LAG).

100) Urządzenie musi obsługiwać zestawianie połączeń typu PWE na ścieżkach LSP sygnalizowanych przy pomocy mechanizmów Segment Routing.

101) Urządzenie musi obsługiwać zestawianie połączeń typu L3VPN na ścieżkach LSP sygnalizowanych przy pomocy mechanizmów Segment Routing.

102) Urządzenie musi obsługiwać zestawianie połączeń typu EVPN ELAN na ścieżkach LSP sygnalizowanych przy pomocy mechanizmów Segment Routing.

103) Urządzenie musi obsługiwać zestawianie połączeń typu EVPN VPWS (virtual private wire service) na ścieżkach LSP sygnalizowanych przy pomocy mechanizmów Segment Routing.

104) Urządzenie musi obsługiwać tryb pracy jako router typu P/PE/LSR i obsługiwać następujące funkcje:

a) sygnalizację ścieżek LSP z wykorzystaniem protokołu LDP zgodnie z RFC 3212, Constraint-Based LSP Setup using LDP

b) LDP Downstream on Demand mode opisany w RFC 5036, LDP Specification
c) sygnalizację ścieżek LSP z wykorzystaniem protokołu RSVP
d) Traffic Engineering RFC 3209, RSVP-TE: Extensions to RSVP for LSP Tunnels
e) Fast Reroute RFC 4090, Fast Reroute Extensions to RSVP-TE for LSP Tunnels

105) Urządzenie musi obsługiwać mechanizmy dostępnych w ramach MPLS, takich jak:
a) statystyki ruchu w ramach poszczególnych ścieżek LSP
b) LSP ping
c) BFD dla poszczególnych ścieżek LSP
d) możliwość tunelowania pakietów wykorzystujących LDP LSP w ramach RSVP LSP

106) Urządzenie musi obsługiwać protokół PCEP (Path Computation Element Protocol), opisanego w ramach RFC 5440, Path Computation Element (PCE) Communication Protocol (PCEP)—Stateful PCE

107) Urządzenie musi obsługiwać protokół LDP (Label Distribution Protocol).

108) Urządzenie musi obsługiwać mechanizm autentykacji protokołu LDP z wykorzystaniem haseł i kluczy MD5.

109) Urządzenie musi obsługiwać możliwość określenia czasu o jaki będzie opóźnione wycofywanie etykiet LDP podczas konwergencji IGP.

110) Urządzenie musi obsługiwać funkcję wskazania prefiksów rozgłaszanych w ramach LDP.

111) Urządzenie musi obsługiwać rozgłaszanie etykiety 0 do routera LSR kończącego ścieżkę LSP (egress).

112) Urządzenie musi obsługiwać mechanizm mechanizmu Graceful Restart dla protokołu LDP.

113) Urządzenie musi obsługiwać synchronizację stanu protokołu LDP z protokołami IGP (przynajmniej OSPF i IS-IS).

114) Urządzenie musi obsługiwać wskazanie prefiksów przyjmowanych w ramach LDP.

115) Urządzenie musi obsługiwać sesje transportowych LDP zestawianych na łączach wykorzystujących IPv6.

116) Urządzenie musi obsługiwać ograniczenie zestawiania sąsiedztwa LDP tylko z sąsiadami wskazanymi w konfiguracji.

117) Urządzenie musi obsługiwać wykorzystania przez protokół LDP metryk wykorzystywanych przez protokół IGP.

118) Urządzenie musi obsługiwać tunelowanie pakietów wykorzystujących LDP LSP w ramach RSVP LSP (LDP over RSVP).

119) Urządzenie musi obsługiwać mechanizm 6PE - RFC 4798, Connecting IPv6 Islands over IPv4 MPLS Using IPv6 Provider Edge Routers (6PE).

120) Urządzenie musi obsługiwać mechanizm 6VPE - RFC 4659, BGP-MPLS IP Virtual Private Network (VPN) Extension for IPv6 VPN.

121) Urządzenie musi obsługiwać mechanizm explicit-null label w ścieżkach LSP (Ultimate Hop Popping).

122) Urządzenie musi obsługiwać mechanizm tunelowania pakietów ICMP (TTL Exceeded) w ścieżkach LSP.

123) Urządzenie obsługiwać możliwość wyłączenia modyfikacji pola TTL pakietów w przypadku transport MPLS.

124) Urządzenie musi obsługiwać przełączanie MPLS na interfejsach tagowanych IEE 802.1Q (VLAN).

125) Urządzenie musi obsługiwać przełączanie MPLS na interfejsach bez tagowania IEEE 802.1Q (VLAN).

126) Urządzenie musi obsługiwać mechanizm sprawdzenia komunikacji w ramach ścieżki LSP przy pomocy komendy traceroute. W wyniku działania mechanizmu zwracane (prezentowane) muszą być etykiety wykorzystywane w ramach ścieżki LSP.

127) Urządzenie musi obsługiwać protokół RSVP-TE oraz jego następujące funkcje

a) RFC 2205, Resource ReSerVation Protocol (RSVP)—Version 1 Functional Specification
b) RFC 2210, The Use of RSVP with IETF Integrated Services
c) RFC 2211, Specification of the Controlled-Load Network Element Service
d) RFC 2212, Specification of Guaranteed Quality of Service
e) RFC 2215, General Characterization Parameters for Integrated Service Network Elements
f) RFC 2745, RSVP Diagnostic Messages
g) RFC 2747, RSVP Cryptographic Authentication (updated by RFC 3097)
h) RFC 2961, RSVP Refresh Overhead Reduction Extensions
i) RFC 3097, RSVP Cryptographic Authentication—Updated Message Type Value
j) RFC 3209, RSVP-TE: Extensions to RSVP for LSP Tunnels
k) RFC 3473, Generalized Multi-Protocol Label Switching (GMPLS) Signaling Resource Reservation Protocol-Traffic Engineering (RSVP-TE) Extensions (section 9)
l) RFC 3477, Signalling Unnumbered Links in Resource ReSerVation Protocol - Traffic Engineering (RSVP-TE)
m) RFC 4090, Fast Reroute Extensions to RSVP-TE for LSP Tunnels
n) RFC 4203, OSPF Extensions in Support of Generalized Multi-Protocol Label Switching (GMPLS)
o) RFC 4558, Node-ID Based Resource Reservation Protocol (RSVP) Hello: A Clarification Statement
p) RFC 4561, Definition of a Record Route Object (RRO) Node-Id Sub-Object
q) RFC 4875, Extensions to RSVP-TE for Point-to-Multipoint TE LSPs
r) RFC 5420, Encoding of Attributes for MPLS LSP Establishment Using Resource Reservation Protocol Traffic Engineering (RSVP-TE)
s) RFC 7570, Label Switched Path (LSP) Attribute in the Explicit Route Object (ERO)

t) RFC 8370, Techniques to Improve the Scalability of RSVP-TE Deployments
u) RFC 2209, Resource ReSerVation Protocol (RSVP)—Version 1 Message Processing Rules
v) RFC 2216, Network Element Service Specification Template
w) RFC 4125, Maximum Allocation Bandwidth Constraints Model for Diffserv-aware MPLS Traffic Engineering
x) RFC 4127, Russian Dolls Bandwidth Constraints Model for Diffserv-aware MPLS Traffic Engineering
y) RFC 8577, Signaling RSVP-TE Tunnels on a Shared MPLS Forwarding Plane

128) Urządzenie musi obsługiwać mechanizm przypisywania interfejsom tranzytowym atrybutów pozwalających na ich włączenie/wykluczenie przy wyznaczaniu ścieżki LSP.

129) Urządzenie musi obsługiwać mechanizm autentykacji urządzeń z którymi zestawiane jest sąsiedztwo RSVP.

130) Urządzenie musi obsługiwać mechanizm Graceful Restart dla protokołu RSVP.

131) Urządzenie musi obsługiwać mechanizm wskazania ścieżki LSP do określonych adresów docelowych.

132) Urządzenie musi obsługiwać mechanizm zestawienia zapasowych ścieżek LSP przed przełączeniem na nie ruchu (ang. Make before break) bez zbędnych opóźnień.

133) Urządzenie musi obsługiwać mechanizm sygnalizacji wartości MTU w ramach protokołu RSVP.

134) Urządzenie musi obsługiwać mechanizm RSVP Refresh Reduction, zgodnie z RFC 2961, RSVP Refresh Overhead Reduction Extensions.

135) Urządzenie musi obsługiwać mechanizm LSP Self-Ping zgodnie z RFC 7746, Label Switched Path (LSP) Self-Ping.

136) Urządzenie musi obsługiwać dystrybucję informacji o etykietach MPLS Segment Routing z wykorzystaniem protokołu IS-IS.

137) Urządzenie musi obsługiwać dystrybucję informacji o etykietach MPLS Segment Routing z wykorzystaniem protokołu OSPF.

138) Urządzenie musi obsługiwać dystrybucję informacji o Adjacency SID (Segment Routing) w ramach protokołu ISIS.

139) Urządzenie musi obsługiwać dystrybucję informacji o Adjacency SID (Segment Routing) w ramach protokołu OSPF.

140) Urządzenie musi obsługiwać dystrybucję informacji o Node i Link SID w ramach protokołu IS-IS.

141) Urządzenie musi obsługiwać dystrybucję etykiet Segment Routing pomiędzy różnymi obszarami (area) protokołu OSPF.

142) Urządzenie musi obsługiwać dystrybucję informacji o Node i Link SID w ramach protokołu OSPF.

143) Urządzenie musi obsługiwać filtrowanie pakietów wysyłanych i odbieranych na interfejsach warstwy trzeciej z protokołem IPv4.

144) Urządzenie musi obsługiwać filtrowanie pakietów wysyłanych i odbieranych na interfejsach warstwy trzeciej z protokołem IPv6.

145) Urządzenie musi obsługiwać filtrowanie pakietów wysyłanych i odbieranych na interfejsach warstwy drugiej dla przełączania w warstwie drugiej (przełącznik/bridge).

146) Urządzenie musi obsługiwać filtrowanie pakietów wysyłanych i odbieranych na interfejsach warstwy drugiej dla usług VPLS i PWE.

147) Urządzenie musi obsługiwać filtrowanie pakietów wysyłanych i odbieranych na interfejsach warstwy drugiej dla usług EVPN.

148) Urządzenie musi obsługiwać zliczanie filtrowanych pakietów dla poszczególnych reguł filtrowania.

149) Urządzenie musi obsługiwać logowanie filtrowanych pakietów w zakresie podstawowych parametrów, takich jak adresy źródłowe i docelowe, protokół, porty źródłowe i docelowe.

150) Urządzenie musi obsługiwać mechanizm ograniczania przepustowości ruchu odbieranego na interfejs logicznym (np. znakowanym VLAN/802.1q) w trybach 'Single Rate Three Color Marker' i 'Two Rate Three Color Marker'.

151) Urządzenie musi obsługiwać mechanizm ograniczania przepustowości ruchu wysyłanego na interfejsie logicznym (np. znakowanym VLAN/802.1q) w trybach 'Single Rate Three Color Marker' i 'Two Rate Three Color Marker'.

152) Urządzenie musi obsługiwać wykonanie dla filtrowanych pakietów akcji polegającej na przekierowaniu tych pakietów do wskazanej instancji logicznej typu router wirtualny lub VRF.

153) Urządzenie musi obsługiwać filtrowanie pakietów na interfejsach typu IRB (ang. Integrated Routing and Bridging).

154) Urządzenie musi obsługiwać filtrowanie pakietów na podstawie wartości pola DSCP oraz kolejki do jakiej pakiety zostały zaklasyfikowane.

155) Urządzenie musi obsługiwać filtrowanie pakietów na podstawie ich adresów źródłowych (IPv4 i IPv6), docelowych (IPv4 i IPv6), protokołu, portów źródłowych i docelowych oraz wartości pola DSCP.

156) Urządzenie musi obsługiwać filtrowanie pakietów pofragmentowanych.

157) Urządzenie musi obsługiwać filtrowanie pakietów na podstawie zakresów portów źródłowych i docelowych.

158) Urządzenie musi obsługiwać filtrowanie pakietów na podstawie wartości flag protokołu TCP.

159) Urządzenie musi obsługiwać filtrowanie pakietów na podstawie wartości pola TTL.

160) Urządzenie musi obsługiwać klasyfikowanie ruchu do kolejek zarządzania ruchem w następujących konfiguracjach

a) na podstawie pól 802.1p (wewnętrzny/zewnętrzny VLAN tag) oraz DSCP dla interfejsów pracujących w trybie bridge (przełączanie L2 OSI)
b) na podstawie pól 802.1p (wewnętrzny/zewnętrzny VLAN tag) oraz DSCP dla interfejsów przełączających pakiety w warstwie 3 OSI (routing)
c) na podstawie pól 802.1p (wewnętrzny/zewnętrzny VLAN tag) , DSCP oraz bitu EXP dla interfejsów będących zakończeniami usług VPLS, EVPN oraz typu pseudowire

161) Urządzenie musi obsługiwać przepisywanie (zmianę wartości) znaczników 802.1p, DSCP oraz EXP

162) Urządzenie musi obsługiwać klasyfikowanie pakietów na podstawie filtrów (ang. filter, access-list) dla wszystkich rodzajów ruchu, jakie mogą być odebrane na interfejsach (warstwy 3 OSI, usług typu pseudowire, VPLS, EVPN).

163) Urządzenie musi obsługiwać następujące mechanizmy kolejkowania pakietów:

d) Strict
e) WFQ
f) DWRR
g) WRED

164) Urządzenie musi obsługiwać kolejkowanie pakietów multicast.

165) Urządzenie musi obsługiwać określanie w jaki sposób będą odrzucane pakiety nie mieszczące się w buforach interfejsów (ang. tail drop profiles).

166) Urządzenie musi obsługiwać funkcję zmiany wartości pól ToS/DSCP (IPv4) i Traffic Class (IPv6) pakietów.

167) Urządzenie musi obsługiwać funkcję dodania lub zamiany wartości pola MPLS EXP pakietów.

168) Urządzenie musi obsługiwać konfigurację rozmiaru bufora używanego do kolejkowania pakietów oraz kształtowania pasma.

169) Urządzenie musi obsługiwać kolejkowanie pakietów w ramach interfejsu fizycznego.

170) Urządzenie musi obsługiwać mechanizm kształtowania pasma (ang. shaping) w ramach interfejsu fizycznego.

171) Urządzenie musi obsługiwać konfigurację dokładnej wartości przepustowości kształtowania pasma (ang. exact rate).

172) Urządzenie musi obsługiwać skonfigurowanie kolejki o bezwzględnym priorytecie (ang. strict priority).

173) Urządzenie musi obsługiwać mechanizm klasyfikacji pakietów do odpowiednich kolejek na podstawie bitu EXP na interfejsach fizycznych i logicznych.

174) Urządzenie musi obsługiwać mechanizm zmiany wartości bitu EXP pakietów na interfejsach fizycznych i logicznych.

175) Urządzenie musi obsługiwać kolejkowanie pakietów multicast wraz z ich replikacją na interfejsach wyjściowych (ang. egress replication).

176) Urządzenie musi zapewniać możliwość statycznej konfiguracji wpisów w tablicy ARP.

177) Urządzenie musi obsługiwać mechanizm okresowego wysyłania do zdalnego serwera (kolektora) podstawowych informacji telemerycznych dotyczących działania samego urządzenia. Raportowanie musi obejmować liczniki dotyczące działania:

h) filtrów zainstalowanych na interfejsach,
i) kolejek na interfejsach,
j) mechanizmów związanych z kontrolą wielkości ruchu (ang. policer).

178) Urządzenie musi obsługiwać wirtualne sieci EVPN zgodnie z następującymi standardami:

a) RFCs and Internet drafts that define standards for EVPNs:
b) RFC 4364, BGP/MPLS IP Virtual Private Networks (VPNs)
c) RFC 4761, Virtual Private LAN Service (VPLS) Using BGP for Auto-Discovery and Signaling
d) RFC 7209, Requirements for Ethernet VPN (EVPN)
e) RFC 7432, BGP MPLS-Based Ethernet VPN
f) RFC 7623, Provider Backbone Bridging Combined with Ethernet VPN (PBB-EVPN)
g) RFC 8214, Virtual Private Wire Service Support in Ethernet VPN
h) RFC 8317, Ethernet-Tree (E-Tree) Support in Ethernet VPN (EVPN) and Provider Backbone Bridging EVPN (PBB-EVPN)
i) RFC 8365, A Network Virtualization Overlay Solution Using Ethernet VPN (EVPN)
j) RFC 8667, IS-IS Extensions for Segment Routing
k) RFC 9047, Propagation of ARP/ND Flags in an Ethernet Virtual Private Network (EVPN)
l) RFC 9135, Integrated Routing and Bridging in Ethernet VPN (EVPN)
m) RFC 9136, IP Prefix Advertisement in Ethernet VPN (EVPN)

179) Urządzenie musi obsługiwać sieci EVPN typu E-LAN

180) Urządzenie musi obsługiwać sieci EVPN typu E-LINE (VPWS) zgodnie z RFC 8214, Virtual Private Wire Service Support in Ethernet VPN

181) Urządzenie musi obsługiwać sieci EVPN wykorzystując dla przenoszonych ramek transport MPLS.

182) Urządzenie musi obsługiwać protokoły IGMPv1, IGMPv2, IGMPv3, MLD

183) Urządzenie musi obsługiwać protokół PIM w następujących trybach:

a) PIM-DM
b) PIM-SM dla protokołu IPv4
c) PIM-SM dla protokołu IPv6
d) PIM-SSM

184) Urządzenie musi obsługiwać protokół PTP w następujących trybach:

e) PTP G.8275.1.

f) PTP G.8275.2.

185) Urządzenie musi obsługiwać mechanizm BFD oraz następujące jego funkcje:

a) RFC 5880, Bidirectional Forwarding Detection
b) RFC 5881, Bidirectional Forwarding Detection (BFD) for IPv4 and IPv6
c) RFC 5882, Generic Application of Bidirectional Forwarding Detection (BFD)
d) RFC 5883, Bidirectional Forwarding Detection (BFD)
e) RFC 5884, Bidirectional Forwarding Detection (BFD) for MPLS Label Switched Paths (LSPs)
f) RFC 5885, Bidirectional Forwarding Detection (BFD) for the Pseudowire Virtual Circuit Connectivity Verification (VCCV)

186) Urządzenie musi obsługiwać mechanizm IEEE 802.1ag Ethernet OAM connectivity fault management (CFM) co najmniej w następujących przypadkach:

a) w ramach VPLS w zakresie Up i Down maintenance endpoints (MEP).
b) w ramach EVPN w zakresie Up i Down maintenance endpoints (MEP).
c) w ramach PWE (pseudowire) w zakresie Up i Down maintenance endpoints (MEP).

187) Urządzenie musi obsługiwać mechanizm typu sFlow, NetFlow lub jFlow, (próbkowania i wysyłania do kolektora informacji o przetwarzanym ruchu sieciowym)

18. Wdrożenie systemu

W ramach wdrożenia Systemu dla Zadania nr 1 Wykonawca zobowiązany jest do:

1) realizacji planu wdrożenia zawartego w punkcie **18.1** zgodnie z punktami obwiązującymi dla danego Zadania
2) dostawy przedmiotu zamówienia zgodnie z Załącznikiem nr 1 do SWZ
3) dostawy, instalacji i konfiguracji urządzeń w siedzibie Zamawiającego:
   PCSS – Poznańskie Centrum Superkomputerowo-Sieciowe, Budynek Sal Technologicznych (BST) ul. Jana Pawła II 10 (zwanym dalej lokalizacją „BST"), 61-139 Poznań oraz sala techniczna ul. Wieniawskiego 17-19, 61-713 Poznań (zwanym dalej lokalizacją „DCW"),
4) przeprowadzenie instruktażu dla pracowników Zamawiającego zgodnie z wytycznymi opisanymi w punkcie **19**.

W ramach wdrożenia Systemu dla Zadania nr 2 Wykonawca zobowiązany jest do:

1) realizacji planu wdrożenia zawartego w punkcie **18.1** zgodnie z punktami obwiązującymi dla danego Zadania
2) dostawy przedmiotu zamówienia zgodnie z Załącznikiem nr 1 do SWZ
3) dostawy, instalacji i konfiguracji urządzeń w lokalizacji wskazanej przez INSTYTUT NENCKIEGO:
   - lokalizacja docelowa Budynek Naukowo - Badawczy Krajowego Centrum Zaawansowanych Analiz Obrazowania w Naukach Biologicznych I Biomedycznych ul. Leśna 13, 11-730 Mikołajki;
   - lokalizacja tymczasowa Budynek Sal Technologicznych (BST) ul. Jana Pawła II 10 (zwanym dalej lokalizacją „BST"), 61-139 Poznań oraz sala techniczna ul. Wieniawskiego 17-19, 61-713 Poznań,
4) przeprowadzenie instruktażu dla pracowników Zamawiającego zgodnie z wytycznymi opisanymi w punkcie **20**.

18.1. Ramowy plan wdrożenia

Plan realizacji przedmiotu zamówienia (wspólny dla obu Zadań):

Lp.	Element wdrożenia	Dni robocze* (terminy maksymalne)
OPRACOWANIE DOKUMENTACJI TECHNICZNEJ		
1.	Wykonanie Dokumentacji Technicznej w zakresie dotyczącym danego podmiotu odbierającego zgodnie z wytycznymi zawartymi w punkcie **18.3**	30 dni od daty złożenia zapotrzebowania przez poszczególne podmioty odbierające, ale przed rozpoczęciem dostawy
2.	Weryfikacja dokumentacji technicznej przez poszczególne podmioty odbierające	10 dni roboczych od dnia jej dostarczenia dokumentacji przez Wykonawcę

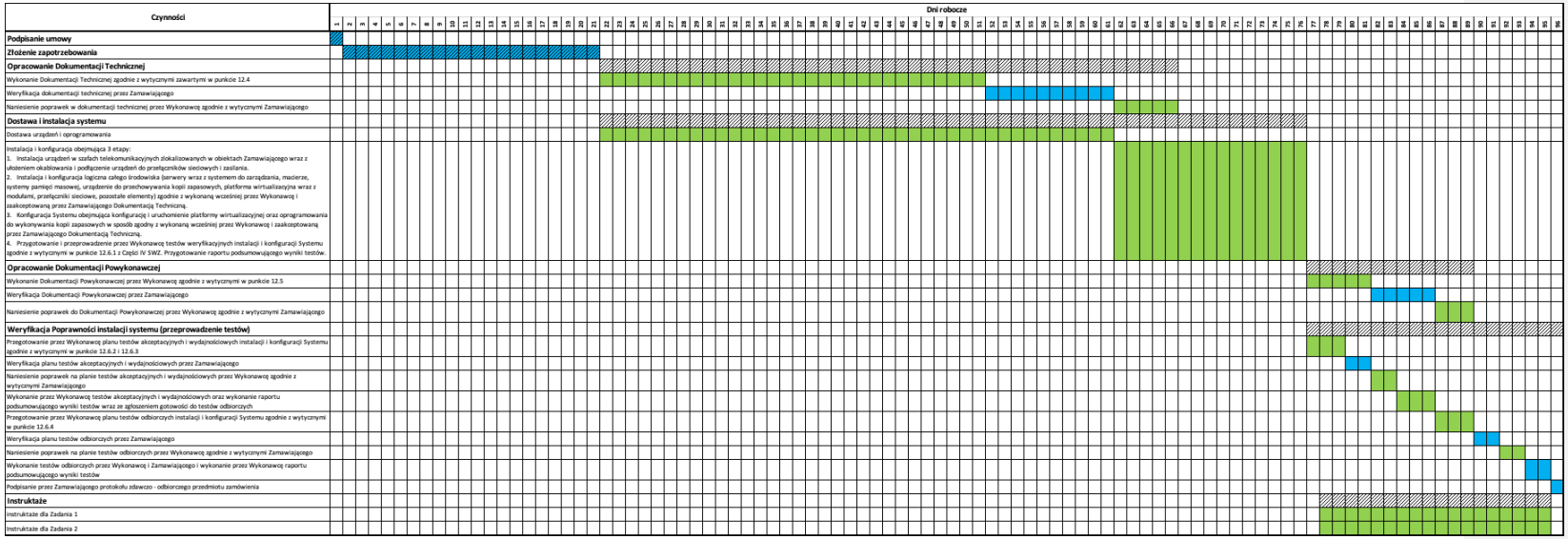
3.	Naniesienie poprawek w dokumentacji technicznej przez Wykonawcę zgodnie z wytycznymi poszczególnych podmiotów odbierających	5 dni roboczych od dnia zgłoszenia konieczności dokonania poprawek przez poszczególne podmioty odbierające
DOSTAWA I INSTALACJA SYSTEMU		
4.	Dostawa urządzeń i oprogramowania	40 dni roboczych od daty złożenia zapotrzebowania przez poszczególne podmioty odbierające (w przypadku zadania nr 1), natomiast w przypadku zadania nr 2 dostawa może się rozpocząć nie wcześniej niż 1 października 2023 r., przy czym za termin dostawy uważa się datę sporządzenia protokołu dostawy dla danego zadania
5.	Wdrożenie (Instalacja i konfiguracja) obejmująca 4 etapy: 1. Instalacja urządzeń w szafach telekomunikacyjnych zlokalizowanych w obiektach poszczególnych podmiotów odbierających wraz z ułożeniem okablowania i podłączenie urządzeń do przełączników sieciowych i zasilania. 2. Instalacja i konfiguracja logiczna całego środowiska (serwery wraz z systemem do zarządzania, macierze, systemy pamięci masowej, urządzenie do przechowywania kopii zapasowych, platforma wirtualizacyjna wraz z modułami, przełączniki sieciowe, pozostałe elementy) zgodnie z wykonaną wcześniej przez Wykonawcę i zaakceptowaną przez poszczególne podmioty odbierające Dokumentacją Techniczną. 3. Konfiguracja Systemu obejmująca konfigurację i uruchomienie platformy wirtualizacyjnej oraz oprogramowania do wykonywania kopii zapasowych w sposób zgodny z wykonaną wcześniej przez Wykonawcę i zaakceptowaną przez poszczególne podmioty odbierające Dokumentacją Techniczną. 4. Przygotowanie i przeprowadzenie przez Wykonawcę testów weryfikacyjnych instalacji i konfiguracji Systemu zgodnie z wytycznymi w punkcie **18.5.1** z Części IV SWZ. Przygotowanie raportu podsumowującego wyniki testów.	15 dni roboczych od daty dostarczenia urządzeń i oprogramowania do danego podmiotu odbierającego przy czym za termin zakończenia wdrożenia dla danego zadania uważa się datę sporządzenia protokołu zdawczo-odbiorczego dla danego zadania
OPRACOWANIE DOKUMENTACJI POWYKONAWCZEJ		

6.	Wykonanie Dokumentacji Powykonawczej w zakresie dotyczącym danego podmiotu odbierającego przez Wykonawcę zgodnie z wytycznymi w punkcie **18.4**	5 dni roboczych po zakończeniu instalacji i konfiguracji Systemu u poszczególnego podmiotu odbierającego
7.	Weryfikacja Dokumentacji Powykonawczej przez poszczególne podmioty odbierające	5 dni roboczych od dnia jej dostarczenia przez Wykonawcę
8.	Naniesienie poprawek do Dokumentacji Powykonawczej przez Wykonawcę zgodnie z wytycznymi poszczególnych podmiotów odbierających	3 dni robocze od dnia zgłoszenia konieczności dokonania poprawek przez poszczególne podmioty odbierające
WERYFIKACJA POPRAWNOŚCI INSTALACJI SYSTEMU (PRZEPROWADZENIE TESTÓW)		
9.	Przygotowanie przez Wykonawcę planu testów akceptacyjnych i wydajnościowych instalacji i konfiguracji Systemu zgodnie z wytycznymi w punkcie **18.5.2** i **18.5.3**	3 dni robocze po zakończeniu instalacji i konfiguracji Systemu u poszczególnego podmiotu odbierającego
10.	Weryfikacja planu testów akceptacyjnych i wydajnościowych przez poszczególny podmiot odbierający	2 dni robocze od dnia jego dostarczenia przez Wykonawcę
11.	Naniesienie poprawek na planie testów akceptacyjnych i wydajnościowych przez Wykonawcę zgodnie z wytycznymi poszczególnych podmiotów odbierających	2 dni robocze od dnia zgłoszenia konieczności dokonania poprawek przez poszczególny podmiot odbierający
12.	Wykonanie przez Wykonawcę testów akceptacyjnych i wydajnościowych oraz wykonanie raportu podsumowującego wyniki testów wraz ze zgłoszeniem gotowości do testów odbiorczych	3 dni robocze
13.	Przygotowanie przez Wykonawcę planu testów odbiorczych instalacji i konfiguracji Systemu zgodnie z wytycznymi w punkcie **18.5.4**	3 dni robocze od zgłoszenia gotowości do testów odbiorczych przez poszczególny podmiot odbierający
14.	Weryfikacja planu testów odbiorczych przez poszczególny podmiot odbierający	2 dni robocze od dnia jego dostarczenia przez Wykonawcę
15.	Naniesienie poprawek na planie testów odbiorczych przez Wykonawcę zgodnie z wytycznymi poszczególnego podmiotu odbierającego	2 dni robocze od dnia zgłoszenia konieczności dokonania poprawek przez poszczególne podmioty odbierające

16.	Wykonanie testów odbiorczych przez Wykonawcę i poszczególne podmioty odbierające i wykonanie przez Wykonawcę raportu podsumowującego wyniki testów	2 dni robocze
17.	Podpisanie przez poszczególny podmiot odbierający protokołu zdawczo - odbiorczego przedmiotu zamówienia objętego danym zadaniem	1 dzień roboczy po pozytywnym zakończeniu testów odbiorczych u poszczególnego podmiotu odbierającego i zakończeniu instruktaży

*przez „dzień roboczy" Zamawiający rozumie poniedziałek, wtorek, środę, czwartek i piątek z wyjątkiem dni ustawowo wolnych od pracy w Polsce.

Poniżej przedstawiono ramowy plan wdrożenia w skali czasu (wykres Gantta)



18.1.1. Ogólne wytyczne dotyczące dostawy i instalacji

Podane poniżej zapisy są wspólne dla obu Zadań.

Wykonawca zobowiązany jest dostarczyć wszelkie urządzenia i oprogramowanie będące przedmiotem zamówienia dla danego Zadania do lokalizacji podmiotu Zamawiającego oraz wykonania ich fizycznej instalacji w tej lokalizacji z uwzględnieniem warunków opisanych poniższych podpunktach (**18.1.1** - **18.1.5**).

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 i montażu urządzeń do lokalizacji Zamawiającego. Dostawę Wykonawca musi zrealizować własnym sprzętem oraz zobowiązany jest do pokrycia wszelkich kosztów związanych z transportem, montażem i ubezpieczeniem dostawy.
5) Prace objęte umową prowadzone będą w obiektach udostępnionych Wykonawcy i pod nadzorem Zamawiającego.
6) Wykonawca zobowiązany jest do prowadzenia na bieżąco prac porządkowych, zarówno w pomieszczeniach objętych montażem jak i na trasie transportu materiałów oraz sprzątanie po wykonaniu każdego etapu prac. Wywóz odpadów należy zrealizować we własnym zakresie (kartony, palety, odpady materiałowe itp.), przy czym odpady można składować w kontenerze nie większym niż 1,7 m3 chyba, że na etapie realizacji zostanie to ustalone inaczej.
7) Wykonawca zobowiązany jest do przestrzegania przepisów porządkowych obowiązujących na terenie budynku Zamawiającego.
8) Zamawiający wymaga, aby pracownicy Wykonawcy oraz jego podwykonawcy przebywali na terenie prowadzenia prac w ubraniach roboczych jednoznacznie identyfikujących firmę dla jakiej pracują (mogą to być np. koszulki odblaskowe z nazwą Wykonawcy). Za każdorazowe nieprzestrzeganie tego wymogu zostanie naliczona kara w wysokości 500,00 zł.
9) 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.
10) Zabronione jest spożywanie posiłków i napojów w salach komputerowych.
11) Wywóz odpadów z dostaw sprzętu musi odbywać się sukcesywnie w czasie dostawy. Zabronione jest korzystanie z kontenerów Zamawiającego. Wykonawca zobowiązany jest do wywozu całości odpadów na swój koszt i swoimi siłami. Dozwolone jest posadowienie dodatkowego kontenera przy budynku o pojemności nie większej niż 1,7 m3 chyba, że na etapie realizacji zostanie to ustalone inaczej. Za każdy rozpoczęty metr sześcienny pozostawianych odpadów zostanie naliczona kara umowna w wysokości 2 000,00 zł. Warunkiem podpisania protokołu zdawczo - odbiorczego przedmiotu zamówienia jest usunięcie wszystkich odpadów powstałych w trakcie instalacji.
12) Wszystkie prace instalacyjne muszą być wykonane w oparciu o najlepsze praktyki, standardy, najnowszą wiedzę w zakresie który obejmuje zamówienie oraz obowiązujące przepisy.

18.1.2. Warunki instalacji zapewnione przez Zamawiającego dla Zadania nr 1

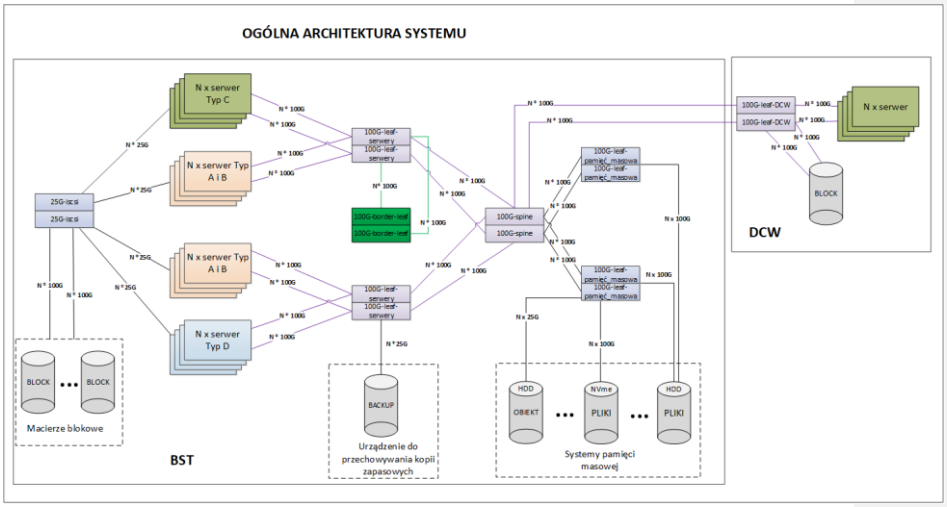
1) Miejsce na instalację urządzeń w przeznaczonym do tego celu pomieszczeniu wyposażonym m.in. w podłogę techniczną z szachtami technicznymi na potrzeby prowadzenia okablowania pomiędzy szafami, klimatyzację, system kontroli dostępu i monitoring.
2) Jeden kiosk składający się z 16 szaf teletechniczny dla lokalizacji „BST" oraz jedna szafa teletechniczna dla lokalizacji „DCW".
3) Każda z szaf teletechnicznych posiada wymiary:
    i. wysokość 47 RU w „BST", 45 RU w „DCW",
    ii. szerokość 80cm,
    iii. głębokość 120cm w „BST", 100cm w „DCW",
    iv. nośność szafy 1500kg,
    v. nośność belek/profili nośnych (pionowych) 1500kg,
    vi. odległość między belkami umożliwiająca montaż urządzeń z uchwytami w rozstawie 19".
4) Warunki techniczne:
    i. lokalizacja „BST":
        1. W każdej z szaf jest zasilanie z dwóch niezależnych torów w postaci 2 listew zasilających PDU.
        2. Każda z listew PDU posiada:
            a. zasilanie 3 fazowe,
            b. zabezpieczenie o łącznej mocy 32A na każdą szafę,
            c. 18 gniazd C13,
            d. 6 gniazd C19.
        3. Sumaryczne chłodzenie na cały kiosk o mocy 200kW, realizowane za pomocą klimatyzatorów międzyrzędowych.
        4. W kiosku znajduje się dedykowany łącznik z włóknami światłowodowymi na potrzeby komunikacji z infrastrukturą Zamawiającego (na potrzeby dostępu do infrastruktury Zamawiającego, systemu zdalnego oraz drugą lokalizacją – „DCW") – parametry łącznika:
            a. złącza SC/APC;
            b. włókna SM w kablu to G.652d E9/125 SMF-28e+
            c. długość włókien światłowodowych pomiędzy lokalizacjami nie przekracza 10 km
    ii. lokalizacja „DCW":
        1. W szafie jest zasilanie z dwóch niezależnych torów w postaci 4 listew PDU, po 2 na każdy tor zasilania.
        2. Para PDU na dany tor zasilania posiada:
            a. zabezpieczenie o łącznej mocy 32A,
            b. 13 gniazd typ E.

18.1.3. Szczegółowe wymagania dotyczące dostawy i instalacji, które musi spełnić Wykonawca dla Zadania nr 1

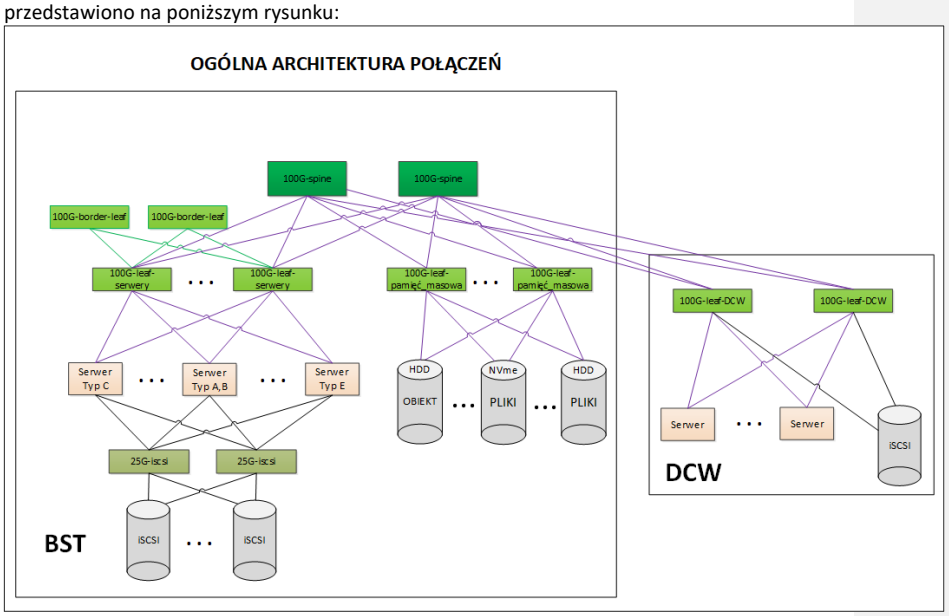
1) Dostarczenie wszystkich niezbędnych elementów (urządzeń, okablowania, elementów montażowych, itp.) potrzebnych do realizacji zadania zgodnie z zapisami SWZ i Dokumentacją Techniczną.

2) Dostawa i instalacja urządzeń do dwóch lokalizacji Zamawiającego („BST” oraz „DCW”). Ilość sprzętu zlokalizowanego w lokalizacji „DCW” nie będzie sumarycznie zajmować więcej przestrzeni niż 30 RU (szczegółowy wykaz sprzętu zostanie ustalony z Zamawiającym na etapie przygotowania Dokumentacji Technicznej).
3) Wykonanie infrastruktury teletechnicznej z wykorzystaniem:
    i. dla połączeń Out-of-Band z wykorzystaniem okablowania miedzianego kategorii min. 6,
    ii. dla pozostałych połączeń z wykorzystaniem okablowania światłowodowego – patchordy dupleksowe (dwa włókna), jednomodowe lub wielomodowe, złącze typu LC,
    iii. Zamawiający nie dopuszcza możliwości stosowania kabli typy „DAC” (ang. Direct Attach Cable), z wyjątkiem połączeń typu „back-end” w systemach pamięci masowej,
    iv. Zamawiający nie dopuszcza stosowania kabli typu „breakout” z wyjątkiem podłączenia systemu pamięci masowej o dostępie obiektowym opisanego w punkcie **9** oraz połączeń realizowanych na przełącznikach zlokalizowanych w lokalizacji „DCW”.
4) Wykonanie osobnej dedykowanej (odseparowanej fizycznie i logicznie w lokalizacji „BST” oraz odseparowanej logicznie w lokalizacji „DCW”) infrastruktury sieciowej (zgodnie z zaakceptowaną Dokumentacją Techniczną) na potrzeby:
    i. dostępu do dostarczonych zasobów serwerowych, platformy wirtualizacyjnej, systemów pamięci masowych (opisanych w punktach **5**, **7**, **9**),
    ii. dostępu do systemu przestrzeni dyskowej (macierzy blokowej) z dostarczonych serwerów realizowanej za pomocą protokołu iSCSI,
    iii. zarządzania dostarczoną infrastrukturą Out-of-Band wszystkich dostarczonych urządzeń posiadających taką funkcjonalność.
5) Zamawiający przewiduje następujące kategorie przełączników sieciowych podzielone wg. ich przeznaczenia, które nie będą ze sobą współdzielone:
    i. „1G-mgmt” – na potrzeby realizacji infrastruktury sieciowej opisanej w ustępie **4) iii.**
    ii. „25G-iscsi” – na potrzeby realizacji infrastruktury sieciowej opisanej w ustępie **4) ii.**
    iii. „100G-leaf-serwery” – na potrzeby realizacji infrastruktury sieciowej opisanej w ustępie **4) i**., przełączniki, do których muszą być podłączone tylko dostarczone serwery oraz urządzenie do przechowywania kopii zapasowych,
    iv. „100G-leaf-pamięć_masowa” – na potrzeby realizacji infrastruktury sieciowej opisanej w ustępie **4) i**., przełączniki, do których muszą być podłączone tylko dostarczone systemy pamięci masowej,
    v. „100G-border-leaf” – na potrzeby realizacji infrastruktury sieciowej opisanej w ustępie **4) i.**, przełączniki przeznaczone do integracji z infrastrukturą Zamawiającego
    vi. „100G-spine” – do realizacji infrastruktury sieciowej opisanej w ustępie **4) i.**, przełączniki pełniące funkcję „spine”,
    vii. „100G-leaf-DCW” – przełączniki umiejscowione w lokalizacji „DCW” na potrzeby podłączenia serwerów oraz macierzy w tej lokalizacji.
6) Każda z podanych w ustępie **4)** infrastruktur musi zostać wykonana za pomocą osobnych i przeznaczonych tylko do jej realizacji urządzeń sieciowych oraz dedykowanego dla niej okablowania teletechnicznego.
7) Infrastruktura podana w ustępie **4) i.** musi zostać zrealizowana w architekturze „leaf and spine fabirc” (architektura „leaf and spine” używająca do połączeń między poszczególnymi przełącznikami warstwy trzeciej modelu ISO/OSI (IP)).

8) Dostarczone serwery na potrzeby realizacji infrastruktury opisanej w ustępie **4) i.** muszą zostać podłączone redundantnie do dedykowanych tylko dla nich przełączników sieciowych w sposób zapewniający optymalne wykorzystanie infrastruktury sieciowej, nie powodujący generowania zbędnego ruchu pomiędzy przełącznikami, tj.:
    i. interfejsy dostępowe (100G) serwerów **Typu C** należy podłączyć do tej samej pary przełączników typu „100G-leaf-serwery”,
    ii. interfejsy dostępowe (100G) serwerów **Typu E** należy podłączyć do tej samej pary przełączników typu „100G-leaf-serwery”,
    iii. pozostałe wolne porty na przełącznikach typu „100G-leaf-serwery” należy równomiernie obsadzić interfejsami dostępowymi (100G) serwerów **Typu A i B**,
    iv. w lokalizacji „DCW” serwery należy podłączyć do tej samej pary przełączników typu „100G-leaf-DCW”.
9) Dostarczone serwery oraz macierze blokowe, na potrzeby realizacji infrastruktury opisanej w ustępie **4) ii.** muszą zostać podłączone w sposób redundantny do dedykowanych tylko do tego celu przełączników sieciowych typu „25G-iscsi”. Zamawiający dopuszcza, aby w lokalizacji „DCW” dostarczone serwery oraz macierze blokowe, na potrzeby realizacji infrastruktury opisanej w ustępie **4) ii.** zostały podłączone w sposób redundantny do przełączników sieciowych typu „100G-leaf-DCW”, w takiej sytuacji Zamawiający wymaga użycia połączeń typu „breakout”.
10) Dostarczone systemy pamięci masowej muszą zostać podłączone wszystkimi dostępnymi interfejsami typu „front-end” oraz w sposób zapewniający optymalne wykorzystanie infrastruktury sieciowej, nie powodujący generowania zbędnego ruchu pomiędzy przełącznikami, tj.:
    i. interfejsy dostępowe (100G) systemu szybkiej i archiwalnej pamięci masowej o dostępie plikowym należy podłączyć do przełączników typu „100G-leaf-pamięć_masowa”,
    ii. interfejsy dostępowe (25G) systemu pamięci masowej o dostępie obiektowym należy podłączyć do przełączników „100G-leaf-pamięć_masowa„ oraz Zamawiający dopuszcza zastosowanie kabli/połączeń typu „breakout”.
11) Urządzenie do przechowywania kopii zapasowych musi zostać podłączone do przełączników sieciowych typu „100G-leaf-serwery”. Zamawiający wymaga aby urządzenie to było podłączone bez użycia kabli typu „breakout”.
12) Każdy z przełączników typu „100G-leaf-serwery” musi zostać połączony z każdym z przełączników typu „100G-spine” za pomocą 3 (trzech) połączeń o przepustowości 100G, każde połączenie z wykorzystaniem włókien światłowodowych zgodnie z wymaganiami opisanymi w ustępie **3)**.
13) Każdy z przełączników typu „100G-DCW” musi zostać połączony z każdym z przełączników typu „100G-spine” za pomocą 2 (dwóch) połączeń o przepustowości 100G, każde połączenie z wykorzystaniem włókien światłowodowych zgodnie z wymaganiami opisanymi w ustępie **3)**.
14) Każdy z przełączników typu „100G-leaf-pamięć_masowa” musi zostać połączony z każdym z przełączników typu „100G-spine” za pomocą 4 (czterech) połączeń o przepustowości 100G, każde połączenie z wykorzystaniem włókien światłowodowych zgodnie z wymaganiami opisanymi w ustępie **3)**.
15) Poglądowy schemat wymagań Zamawiającego w zakresie ogólnej architektury systemu (topologii połączeń) przedstawiono na poniższym rysunku:



16) Każde urządzenie podłączone do infrastruktury sieciowej musi być podłączone redundantnie (tj. co najmniej do 2 niezależnych przełączników sieciowych) w celu zapewnienia bezprzerwowego dostępu do urządzenia w przypadku awarii jednego z przełączników do którego podłączone jest to urządzenie – poglądowy schemat wymagań Zamawiającego przedstawiono na poniższym rysunku:



17) Infrastruktura podana ustępie **4) i.** zakłada wyposażenie w dwa przełączniki typu „100G-border-leaf" pracujące w trybie redundantnym. Każdy z przełączników musi zostać połączony z parą przełączników „100G-leaf-serwery" za pomocą 2 (dwóch) połączeń o przepustowości 100G każde z wykorzystaniem włókien światłowodowych zgodnie z wymaganiami opisanymi w ustępie **3)**. Oprócz modułów optycznych służących do połączenia z przełącznikami „100G-leaf-

serwery”, każdy przełącznik musi zostać wyposażony w następujące moduły optyczne zgodne i poprawnie pracujące z zaoferowanymi przełącznikami:

i) 10 x 100GEth LR
ii) 15 x 25GEth LR
iii) 5 x 10GEth LR

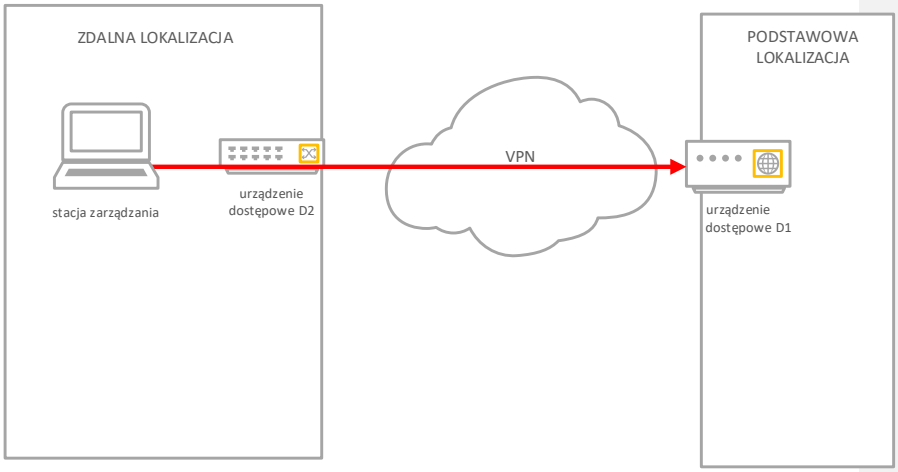
Każdy z dostarczonych modułów musi umożliwiać realizację połączenia o danej przepustowości z wykorzystaniem patchcordów dupleksowych (dwa włókna), jednomodowych, ze złączem LC na odległość co najmniej 2km.

18) Każdy z przełączników służących do realizacji infrastruktury opisanej w ustępie **4) i.** oprócz wkładek służących do realizacji tej infrastruktury musi zostać wyposażony w dodatkowe, nie wykorzystane do połączeń, 4 (cztery) wkładki typu 100G-LR (o ile w danym przełączniku zostaną niewykorzystane porty) zgodne i poprawnie pracujące z zaoferowanymi przełącznikami.
19) Wymaga się by wszystkie dostarczone moduły mogły być instalowane w urządzeniu i wyjmowane z urządzenia podczas jego pracy (ang. Hot-Pluggable).
20) Wykonanie wszystkich niezbędnych połączeń teletechnicznych i elektrycznych na potrzeby instalacji dostarczonych urządzeń, w tym także wszystkich wymaganych przewodów ochronnych.
21) Wszystkie dostarczone urządzenia oraz elementy infrastruktury teletechnicznej i elektrycznej muszą być jednoznacznie oznaczone zgodnie z uzgodnionym z Zamawiającym schematem nazewnictwa.
22) Wszystkie dostarczone urządzenia muszą być zainstalowane w sposób zapewniający przepływ powietrza z zewnątrz kiosku do wewnątrz w lokalizacji „BST”.
23) Wszystkie połączenia muszą być prowadzone w zgodnie z obowiązującymi normami oraz wytycznymi producentów. Wszystkie połączenia prowadzone pomiędzy szafami muszą być ułożone pod podłogą techniczną. Wszystkie połączenia prowadzone wewnątrz szaf muszą być ułożone w dedykowanych do tego celu uchwytach oraz w sposób umożliwiający przeprowadzenie prac serwisowych na dostarczonych urządzeniach. W tym celu należy wykorzystać m.in. ramiona i uchwyty/organizery do prowadzenia okablowania. Okablowanie musi być ułożone w sposób estetyczny.
24) Wszystkie dostarczone elementy okablowania muszą być jednoznacznie oznaczone w sposób uzgodniony z Zamawiającym, zgodnie z uzgodnionym z Zamawiającym schematem nazewnictwa.
25) Adresacja IP musi zostać zaplanowana w uzgodnieniu z Zamawiającym dla każdego z urządzeń i segmentów sieci.
26) Zaplanowanie i wykonanie dedykowanej infrastruktury zarządzania Out of Band (**4) iii.**) przy użyciu przełączników typu „1G-mgmt” oraz z wykorzystaniem urządzeń opisanych w punkcie **15**. Każdy rodzaj urządzeń na potrzeby zdalnego dostępu Out of Band musi posiadać oddzielną adresację IP (adresacja musi zostać uzgodniona z Zamawiającym na etapie planowania).
27) Zaplanowanie i wykonanie dedykowanej infrastruktury zdalnego dostępu konsolowego (**4) iii.)** do urządzeń sieciowych oraz pozostałych urządzeń z wykorzystaniem urządzeń opisanych w punkcie **15**.
28) Wykonania integracji wdrożonego Systemu, w szczególności platformy wirtualizacyjnej, systemu pamięci masowej, infrastruktury dostępowej (zdefiniowanej w ustępie **4) i.**) oraz zarządzania (zdefiniowanej w ustępie **4) iii.**) z infrastrukturą Zamawiającego zainstalowaną w siedzibie Zamawiającego (uzgodnienie adresacji, dostarczenie i ułożenie okablowania). Należy wykonać integrację następujących segmentów:

i. dostępu do dostarczonych zasobów serwerowych i pamięci masowych z Internetu przy pomocy dwóch redundantnych podłączeń z wykorzystaniem przełączników typu „100G-border-leaf”

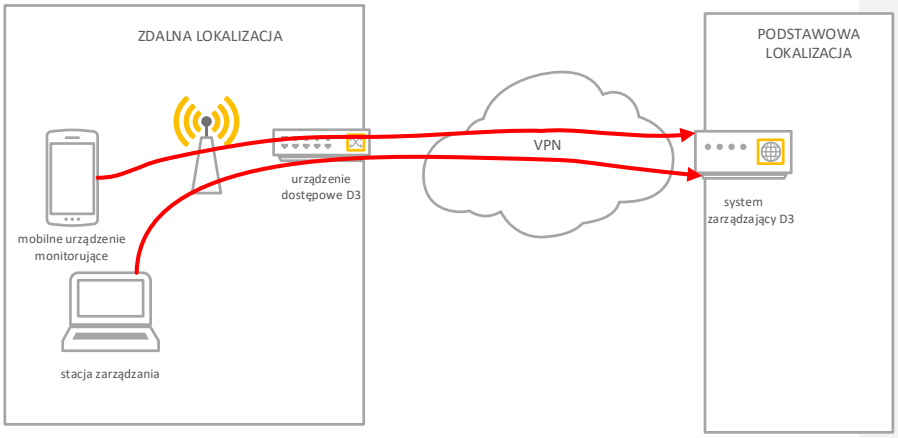
ii. dostępu do interfejsów zarządzania Out-of-Band oraz dostępu konsolowego z Internetu musi zostać zrealizowany przy użyciu dwóch redundantnych podłączeń z wykorzystaniem urządzenia dostępowego typ D1 (opisanego w punkcie **15.2**) oraz połączenia zapasowego poprzez wbudowany w nie modem LTE.

iii. skonfigurować urządzenia dostępowe typ D2 (opisanego w punkcie **15.3**) na potrzeby bezpiecznego dostępu do interfejsów zarządzania Out-of-Band oraz dostępu konsolowego z Internetu poprzez urządzenie dostępowego typ D1 z wykorzystaniem tuneli VPN. Tunel VPN musi poprawnie oraz automatycznie zestawiać się niezależnie od sposobu podłączenia urządzenia dostępowego typ D2 do Internetu (adres publiczny, adres prywatny za NAT-em).
Poglądowy schemat wymagań Zamawiającego przedstawiono na poniższym rysunku:



iv. skonfigurować urządzenia dostępowe typ D3 (opisanego w punkcie **15.2**) na potrzeby bezpiecznego dostępu do interfejsów zarządzania Out-of-Band oraz dostępu konsolowego z Internetu poprzez systemem zarządzającym typ D3 (opisany w punkcie **15.4**) z wykorzystaniem tuneli VPN. Tunel VPN musi poprawnie oraz automatycznie zestawiać się niezależnie od sposobu podłączenia urządzenia dostępowego typ D3 do Internetu (adres publiczny, adres prywatny za NAT-em).

Po poprawnym zestawieniu tunelu VPN na urządzeniu dostępowym typ D3 musi być rozgłaszana sieci Wi-Fi z dostępem WPA3-PSK, poprzez którą musi być zapewniony dostęp do interfejsów zarządzania Out-of-Band oraz dostęp konsolowy. Cały ruch z tej sieci musi być tunelowany poprzez tunel VPN do systemu zarządzającego typ D3.
Poglądowy schemat wymagań Zamawiającego przedstawiono na poniższym rysunku:



29) Dostarczenie wszelkiego okablowania zasilającego niezbędnego do realizacji wdrożenia Systemu zgodnie z zapisami SWZ i Dokumentacją Techniczną.
30) Wykonanie wszystkich niezbędnych połączeń, w tym także podłączeń przewodów ochronnych.
31) Wszystkie dostarczone i instalowane urządzenia muszą być jednoznacznie oznaczone zgodnie z uzgodnionym w ramach Dokumentacji Technicznej schematem nazewnictwa.
32) Wszystkie dostarczone i instalowane elementy okablowania muszą być jednoznacznie oznaczone zgodnie z uzgodnionym w ramach Dokumentacji Technicznej schematem nazewnictwa.
33) Wszystkie dostarczone urządzenia muszą być zainstalowane w sposób zapewniający przepływ powietrza z zewnątrz kiosku do wewnątrz w lokalizacji „BST".
34) Przełączniki sieciowe muszą być zainstalowane na tyle szafy patrząc od zewnątrz kiosku i przepływ powietrza musi odbywać się w kierunku od tył urządzenia do frontu (porty we/wy).
35) Dostarczone oprogramowanie do wirtualizacji wraz z modułami oraz oprogramowaniem do wykonywania kopii zapasowych musi zostać zainstalowane na wszystkich dostarczonych serwerach i skonfigurowane zgodnie z wykonaną przez Wykonawcę na podstawie wytycznych Zamawiającego Dokumentacją Techniczną. Konfiguracja oprogramowania do wirtualizacji musi zapewnić działanie usług (maszyn wirtualnych) w modelu wysokiej dostępności między ośrodkami (lokalizacjami). Zasoby dyskowe zapewniane przez oprogramowanie do wirtualizacji przestrzeni dyskowej muszą być skonfigurowane w modelu pełnej replikacji synchronicznej pomiędzy ośrodkami. Sieć zapewniona przez oprogramowanie do wirtualizacji sieci musi działać w modelu obsługującym oba ośrodki umożliwiającym rozciągnięcie tej samej sieci na dwa ośrodki. Konfiguracja całej dostarczonej infrastruktury musi zapewniać poprawne działanie usług (maszyn wirtualnych) w przypadku niedostępności (awarii) jednego z ośrodków.
36) Macierze blokowe, systemy pamięci masowej muszą zostać zainstalowane, skonfigurowane zgodnie z wykonaną przez Wykonawcę i zaakceptowaną przez Zamawiającego Dokumentacją Techniczną.
37) Wykonanie wszystkich pozostałych czynności zawartych w niniejszym dokumencie oraz znajdujących się w wykonanej przez Wykonawcę i zaakceptowanej przez Zamawiającego Dokumentacji Technicznej.
38) Jeżeli instalowane oprogramowanie lub dostarczany Komponent wymaga przypisania licencji do świadczenia wymaganej funkcjonalności licencja ta musi zostać przypisana oraz aktywowana.

18.1.4. Warunki instalacji zapewnione przez Zamawiającego dla Zadania nr 2

1) Miejsce na instalację urządzeń w przeznaczonym do tego celu pomieszczeniu wyposażonym m.in. w podłogę techniczną z szachtami technicznymi lub w dedykowane dukty kablowe nad szafami serwerowymi na potrzeby prowadzenia okablowania pomiędzy szafami, klimatyzację, system kontroli dostępu i monitoring.
2) Jeden kiosk składający się z 10 szaf teletechnicznych.
3) Każda z szaf teletechnicznych posiada wymiary:
   i. wysokość 47U,
   ii. szerokość 80cm,
   iii. głębokość 120cm,
   iv. wysokość 219cm,
   v. nośność szafy 1500kg,
   vi. nośność belek/profili nośnych (pionowych) 1500kg,
   vii. odległość między belkami umożliwiająca montaż urządzeń z uchwytami w rozstawie 19".
4) W każdej z szaf zasilanie z dwóch niezależnych torów w postaci 2 listew zasilających PDU.
5) Każda z listew PDU posiada:
   i. zasilanie 3 fazowe,
   ii. zabezpieczenie o łącznej mocy 32A na każdą szafę,
   iii. 21 gniazd C13,
   iv. 3 gniazd C19.
6) Sumaryczne chłodzenie na cały kiosk o mocy 210kW, realizowane za pomocą klimatyzatorów międzyrzędowych.
7) Dostarczony sprzęt zostanie zainstalowany w 5-6 szafach teletechnicznych.

18.1.5. Szczegółowe wymagania dotyczące dostawy i instalacji, które musi spełnić Wykonawca dla Zadania nr 2

1) Dostarczenie wszystkich niezbędnych elementów (urządzeń, okablowania, elementów montażowych itp.,) potrzebnych do realizacji zadania zgodnie z zapisami SWZ i Dokumentacją Techniczną.
2) Wykonanie infrastruktury teletechnicznej z wykorzystaniem:
   i. dla połączeń Out-of-Band z wykorzystaniem okablowania miedzianego kategorii min. 6,
   ii. dla pozostałych połączeń z wykorzystaniem okablowania światłowodowego – patchordy dupleksowe (dwa włókna), jednomodowe lub wielomodowe, złącze typu LC.:
      1. dla połączeń 100G wkładki typu LR: QSFP28 100GBase LR4, QSFP28 100G LR4 lite
      2. dla połączeń 25G i 10G wkładki typu SR: SFP28 25GbE SR, SFP+ 10GbE SR
   iii. Zamawiający nie dopuszcza możliwości stosowania kabli typy „DAC" (ang. Direct Attach Cable), z wyjątkiem połączeń typu „back-end" w systemach pamięci masowej,
   iv. Zamawiający nie dopuszcza stosowania kabli typu „breakout".
3) Wykonanie osobnej dedykowanej (odseparowanej fizycznie i logicznie) infrastruktury

sieciowej (zgodnie z zaakceptowaną Dokumentacją Techniczną) na potrzeby:

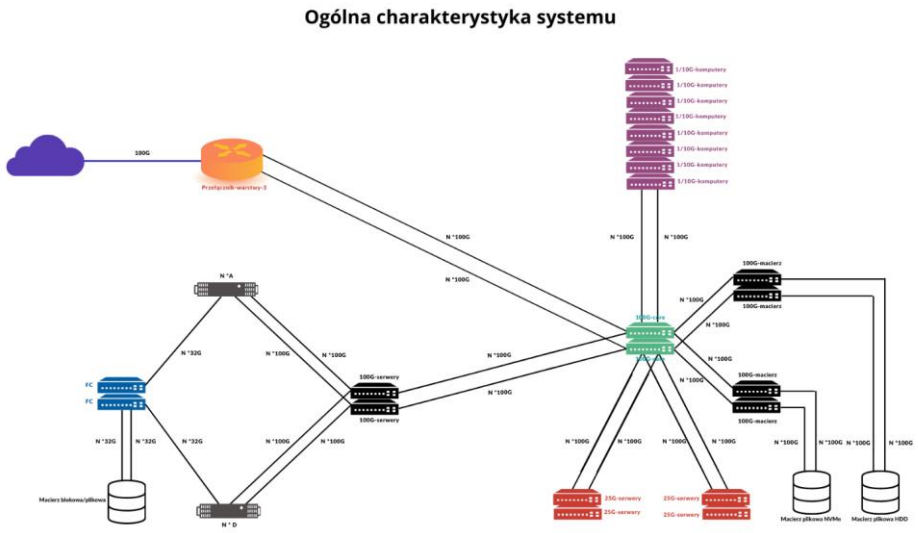
i. dostępu do dostarczonych zasobów serwerowych, platformy wirtualizacyjnej, systemu pamięci masowych,
ii. dostępu do systemu przestrzeni dyskowej z dostarczonych serwerów realizowanej za pomocą Fibre Channel ,
iii. zarządzania dostarczoną infrastrukturą Out-of-Band wszystkich dostarczonych urządzeń posiadających taką funkcjonalność.
iv. dostępu do zasobów serwerowych przewidzianych w przyszłości.

4) Zamawiający przewiduje następujące kategorie przełączników sieciowych podzielone wg. ich przeznaczenia, które nie będą ze sobą współdzielone:
   a) „1G-mgmt" – na potrzeby realizacji infrastruktury sieciowej opisanej w ustępie **3) iii**,
   b) „32G FC" – na potrzeby realizacji infrastruktury sieciowej opisanej w ustępie **3) ii**.
   c) „100G-serwery" – na potrzeby realizacji infrastruktury sieciowej opisanej w ustępie **3) i**., przełączniki, do których muszą być podłączone tylko dostarczone serwery,
   d) „100G-macierz" – na potrzeby realizacji infrastruktury sieciowej opisanej w ustępie **3) i**., przełączniki, do których muszą być podłączone tylko dostarczone systemy pamięci masowej
   e) „100G-core" – na potrzeby realizacji infrastruktury sieciowej opisanej w ustępie **3) i.**, przełączniki przeznaczone do integracji z infrastrukturą Zamawiającego, przełączniki pełniące funkcję „spine".
   f) „25G-serwery" – na potrzeby realizacji infrastruktury sieciowej opisanej w ustępie **3) iv**., przełączniki przeznaczone do rozbudowy infrastruktury serwerowej.
   g) „1/10G-komputery" – przełączniki dostępowe LAN na potrzeby realizacji infrastruktury sieciowej opisanej w ustępie **3) i**.
5) Każda z podanych w ustępie **3)** infrastruktur musi zostać wykonana za pomocą osobnych i przeznaczonych tylko do jej realizacji urządzeń sieciowych oraz dedykowanego dla niej okablowania teletechnicznego.
6) Dostarczone serwery na potrzeby realizacji infrastruktury opisanej w ustępie **3) i.** muszą zostać podłączone do dedykowanych tylko dla nich przełączników sieciowych w sposób zapewniający optymalne wykorzystanie infrastruktury sieciowej, nie powodujący generowania zbędnego ruchu pomiędzy przełącznikami, tj.:
   a) interfejsy dostępowe (100G) serwerów **Typu A** należy podłączyć do tej samej pary przełączników typu „100G-serwery" w topologii „leaf and spine", pierwszy interfejs do pierwszego przełącznika typu „100G-serwery, drugi interfejs do drugiego przełącznika „100G-serwery,
   b) interfejsy dostępowe (100G) serwerów **Typu D** należy podłączyć do tej samej pary przełączników typu „100G-serwery" w topologii „leaf and spine", pierwszy interfejs do pierwszego przełącznika typu „100G-serwery, drugi interfejs do drugiego przełącznika typu „100G-serwery,
7) Dostarczone serwery oraz macierze blokowe, na potrzeby realizacji infrastruktury opisanej w ustępie **3) ii.** muszą zostać podłączone w sposób redundantny dodedykowanych tylko do tego celu przełączników FC.
8) Dostarczone systemy pamięci masowej muszą zostać podłączone wszystkimi dostępnymi interfejsami typu „front-end" oraz w sposób zapewniający optymalne wykorzystanie infrastruktury sieciowej, nie powodujący generowania zbędnego ruchu pomiędzy przełącznikami, tj.:
   a) interfejsy dostępowe (100G) systemu szybkiej pamięci masowej o dostępie plikowym należy podłączyć do tej samej pary przełączników typu „100G-macierz"

w topologii „leaf and spine”, każdy interfejs należy podpiąć jednym linkiem do jednego przełącznika i drugim linkiem do drugiego przełącznika.

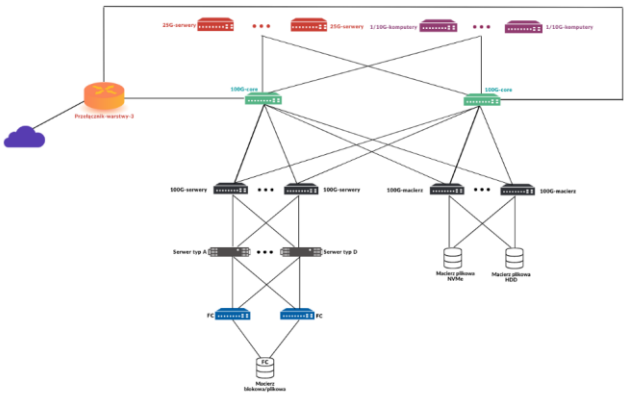
9) Każdy z przełączników typu „100G-serwery” musi zostać połączony z każdym z przełączników typu „100G-core” za pomocą 2 (dwóch) połączeń o przepustowości 100G, każde z wykorzystaniem włókien światłowodowych zgodnie z wymaganiami opisanymi w ustępie 2).
    a) Pierwszy przełącznik sieciowy 100G-serwery połączyć 2 linkami z pierwszym przełącznikiem 100G-core i 2 linkami z drugim przełącznikiem 100G-core.
    b) Drugi przełącznik sieciowy 100G-serwery połączyć 2 linkami z pierwszym przełącznikiem 100G-core i 2 linkami z drugim przełącznikiem 100G-core.
10) Każdy z przełączników typu „100G-macierz” musi zostać połączony z każdym z przełączników typu „100G-core” za pomocą 2 (dwóch) połączeń o przepustowości 100G, każde z wykorzystaniem włókien światłowodowych zgodnie z wymaganiami opisanymi w ustępie 2).
    a) Pierwszy przełącznik sieciowy 100G-macierz połączyć 2 linkami z pierwszym przełącznikiem 100G-core i 2 linkami z drugim przełącznikiem 100G-core.
    b) Drugi przełącznik sieciowy 100G-macierz połączyć 2 linkami z pierwszym przełącznikiem 100G-core i 2 linkami z drugim przełącznikiem 100G-core.
    c) Trzeci przełącznik sieciowy 100G-macierz połączyć 2 linkami z pierwszym przełącznikiem 100G-core i 2 linkami z drugim przełącznikiem 100G-core.
    d) Czwarty przełącznik sieciowy 100G-macierz połączyć 2 linkami z pierwszym przełącznikiem 100G-core i 2 linkami z drugim przełącznikiem 100G-core.
2) Każdy z przełączników typu „25G-serwery” musi zostać połączony z każdym z przełączników typu „100G-core” za pomocą 2 (dwóch) połączeń o przepustowości 100G, każde z wykorzystaniem włókien światłowodowych zgodnie z wymaganiami opisanymi w ustępie 2).
    a) Pierwszy przełącznik sieciowy 25G-serwery połączyć 2 linkami z pierwszym przełącznikiem 100G-core i 2 linkami z drugim przełącznikiem 100G-core.
    b) Drugi przełącznik sieciowy 25G-serwery połączyć 2 linkami z pierwszym przełącznikiem 100G-core i 2 linkami z drugim przełącznikiem 100G-core.
2) Każdy z przełączników typu „1/10G-komputery” musi zostać połączony z każdym z przełączników typu „100G-core” za pomocą 1 (jednego) połączenia o przepustowości 100G, każde z wykorzystaniem włókien światłowodowych zgodnie z wymaganiami opisanymi w ustępie 2).
    a) Pierwszy przełącznik sieciowy 1/10G-komputery połączyć 1 linkiem z pierwszym przełącznikiem 100G-core i 1 linkiem z drugim przełącznikiem 100G-core.
    b) Drugi przełącznik sieciowy 1/10G-komputery połączyć 1 linkiem z pierwszym przełącznikiem 100G-core i 1 linkiem z drugim przełącznikiem 100G-core.
    c) Trzeci przełącznik sieciowy 1/10G-komputery połączyć 1 linkiem z pierwszym przełącznikiem 100G-core i 1 linkiem z drugim przełącznikiem 100G-core.
    d) Czwary przełącznik sieciowy 1/10G-komputery połączyć 1 linkiem z pierwszym przełącznikiem 100G-core i 1 linkiem z drugim przełącznikiem 100G-core.
    e) Piąty przełącznik sieciowy 1/10G-komputery połączyć 1 linkiem z pierwszym przełącznikiem 100G-core i 1 linkiem z drugim przełącznikiem 100G-core.
    f) Szósty przełącznik sieciowy 1/10G-komputery połączyć 1 linkiem z pierwszym przełącznikiem 100G-core i 1 linkiem z drugim przełącznikiem 100G-core.
    g) Siódmy przełącznik sieciowy 1/10G-komputery połączyć 1 linkiem z pierwszym przełącznikiem 100G-core i 1 linkiem z drugim przełącznikiem 100G-core.
    h) Ósmy przełącznik sieciowy 1/10G-komputery połączyć 1 linkiem z pierwszym przełącznikiem 100G-core i 1 linkiem z drugim przełącznikiem 100G-core.

2) Jeden z dwóch dostarczonych urządzeń typu „Przełącznik-warstwy-3” musi zostać podłączony do przełączników typu „100G-core” za pomocą 1 (jednego) połączenia o przepustowości 100G, każde z wykorzystaniem włókien światłowodowych zgodnie z wymaganiami opisanymi w ustępie 2).
    a) „Przełącznik-warstwy-3” połączyć 1 linkiem z pierwszym przełącznikiem 100G-core i 1 linkiem z drugim przełącznikiem 100G-core.
    b) Dodatkowo urządzenie musi zostać podłączone jednym linkiem 100G z urządzeniem DWDM – będącym w posiadaniu Zamawiającego.
    c) Połączenia należy zrealizoawać za pomocą wkładek światłowodowych wyszczególnionych w specyfikacji technicznej „Przełącznik-warstwy-3”.
    d) Drugi „Przełącznik-warstwy-3” przeznaczony jest do późniejszego wykorzystania.
2) Poglądowy schemat wymagań Zamawiającego w zakresie ogólnej architektury systemu (topologii połączeń) przedstawiono na poniższym rysunku:



3) Każde urządzenie podłączone do infrastruktury sieciowej musi być podłączone redundantnie (tj. co najmniej do 2 niezależnych przełączników sieciowych) w celu zapewnienia bezprzerwowego dostępu do urządzenia w przypadku awarii jednego z przełączników, do którego podłączone jest to urządzenie – poglądowy schemat wymagań Zamawiającego przedstawiono na poniższym rysunku:

Ogólna architektura połączeń



4) Infrastruktura podana ustępie **3) i.** zakłada wyposażenie w przełączniki sieciowe pracujące w trybie redundantnym. Każdy z przełączników musi zostać wyposażony w następujące moduły optyczne zgodne i poprawnie pracujące z zaoferowanymi przełącznikami:
    a) Dwa przełączniki sieciowe „100G-core”:
        i. Jeden port w każdym przełączniku powinien zostać obsadzony modułami optycznymi QSFP28 100G LR4, dostarczonymi razem z urządzeniem typu „Przełącznik-warstwy-3” (w sumie 2). Każdy z dostarczonych modułów musi umożliwiać realizację połączenia o danej przepustowości z wykorzystaniem patchordów dupleksowych (dwa włókna), jednomodowych, ze złączem LC na odległość co najmniej 2km.
        ii. Dodatkowo, każdy przełącznik powinien zostać wyposażony w dodatkowe wkładki QSFP28 100G LR4 do późniejszego wykorzystania w liczbie 5 sztuk na przełącznik (w sumie 10 modułów). Każdy z dostarczonych modułów musi umożliwiać realizację połączenia o danej przepustowości z wykorzystaniem patchordów dupleksowych (dwa włókna), jednomodowych, ze złączem LC na odległość co najmniej 2km.
        iii. Wszystkie pozostałe porty w każdym przełączniku powinny zostać obsadzone modułami optycznymi QSFP28 100G LR4 lite.
        iv. Dodatkowo, każdy przełącznik zostanie wyposażony w 2 dodatkowe wkładki QSFP28 100G LR4 lite do późniejszego wykorzystania (w sumie 4).
    b) Dwa przełączniki typu „100G- serwery”:
        i. Wykorzystywane porty powinny zostać obsadzone modułami optycznymi QSFP28 100G LR4 lite.
    c) Cztery przełączniki „100G-macierz”:
        i. Wykorzystywane porty powinny zostać obsadzone modułami optycznymi QSFP28 100G LR4 lite.
    d) Cztery przełączniki typu „25G-serwery”:
        i. Porty w każdym przełączniku należy odpowiednio obsadzić modułami optycznymi:
            1. 4 x QSFP28 100G LR4 lite (w sumie 8 sztuk)
            2. 50 % - 25 GbE, SR SFP28 (w sumie 96 sztuk)

3. 50 % - 10GbE, SR SFP+ (w sumie 96 sztuk)

e) Osiem przełączników „1/10G-komputery”:
   i. Wszystkie porty optyczne we wszystkich przełącznikach należy wypełnić odpowiednio modułami optycznymi QSFP28 100G LR4 lite.

f) Dwa przełączniki „Przełącznik-warstwy-3” należy wyposażyć zgodnie ze specyfikacją podaną w punkcie **17**.

5) Wymaga się by wszystkie dostarczone moduły mogły być instalowane w urządzeniu i wyjmowane z urządzenia podczas jego pracy (ang. Hot-Pluggable).
6) Wykonanie wszystkich niezbędnych połączeń teletechnicznych i elektrycznych na potrzeby instalacji dostarczonych urządzeń, w tym także wszystkich wymaganych przewodów ochronnych.
7) Wszystkie dostarczone urządzenia oraz elementy infrastruktury teletechnicznej i elektrycznej muszą być jednoznacznie oznaczone zgodnie z uzgodnionym z Zamawiającym schematem nazewnictwa.
8) Wszystkie dostarczone urządzenia muszą być zainstalowane w sposób zapewniający przepływ powietrza z zewnątrz kiosku do wewnątrz.
9) Wszystkie połączenia muszą być prowadzone w zgodnie z obowiązującymi normami oraz wytycznymi producentów. Wszystkie połączenia prowadzone pomiędzy szafami muszą być ułożone pod podłogą techniczną. Wszystkie połączenia prowadzone wewnątrz szaf muszą być ułożone w dedykowanych do tego celu uchwytach oraz w sposób umożliwiający przeprowadzenie prac serwisowych na dostarczonych urządzeniach. W tym celu należy wykorzystać m.in. ramiona i uchwyty/organizery do prowadzenia okablowania. Okablowanie musi być ułożone w sposób estetyczny.
10) Wszystkie dostarczone elementy okablowania muszą być jednoznacznie oznaczone w sposób uzgodniony z Zamawiającym, zgodnie z uzgodnionym z Zamawiającym schematem nazewnictwa.
11) Adresacja IP musi zostać zaplanowana w uzgodnieniu z Zamawiającym dla każdego z urządzeń i segmentów sieci.
12) Zaplanowanie i wykonanie dedykowanej infrastruktury zarządzania Out of Band (**3) iii.**) przy użyciu przełącznika typu „1G-mgmt” oraz z wykorzystaniem urządzeń opisanych w punkcie **15.1**. Urządzenie na potrzeby zdalnego dostępu Out of Band musi posiadać oddzielną adresację IP (adresacja musi zostać uzgodniona z Zamawiającym na etapie planowania).
13) Zaplanowanie i wykonanie dedykowanej infrastruktury zdalnego dostępu konsolowego (**3) iii.)** do urządzeń sieciowych oraz pozostałych urządzeń z wykorzystaniem urządzeia opisanego w punkcie **15.1**.
14) Dostarczenie wszelkiego okablowania zasilającego niezbędnego do realizacji wdrożenia Systemu zgodnie z zapisami SWZ i Dokumentacją Techniczną.
15) Wykonanie wszystkich niezbędnych połączeń, w tym także podłączeń przewodów ochronnych.
16) Wszystkie dostarczone i instalowane urządzenia muszą być jednoznacznie oznaczone zgodnie z uzgodnionym w ramach Dokumentacji Technicznej schematem nazewnictwa.
17) Wszystkie dostarczone i instalowane elementy okablowania muszą być jednoznacznie oznaczone zgodnie z uzgodnionym w ramach Dokumentacji Technicznej schematem nazewnictwa.
18) Wszystkie dostarczone urządzenia muszą być zainstalowane w sposób zapewniający przepływ powietrza z zewnątrz kiosku do wewnątrz.
19) Przełączniki sieciowe muszą być zainstalowane na tyle szafy patrząc od zewnątrz kiosku i przepływ powietrza musi odbywać się w kierunku od tył urządzenia do frontu (porty we/wy).
20) Dostarczone oprogramowanie do wirtualizacji wraz z modułami oraz oprogramowaniem do

wykonywania kopii zapasowych musi zostać zainstalowane na wszystkich dostarczonych serwerach i skonfigurowane zgodnie z wykonaną przez Wykonawcę na podstawie wytycznych Zamawiającego Dokumentacją Techniczną.

21) Macierze blokowe, systemy pamięci masowej muszą zostać zainstalowane, skonfigurowane zgodnie z wykonaną przez Wykonawcę i zaakceptowaną przez Zamawiającego Dokumentacją Techniczną.
22) Wykonanie wszystkich pozostałych czynności zawartych w niniejszym dokumencie oraz znajdujących się w wykonanej przez Wykonawcę i zaakceptowanej przez Zamawiającego Dokumentacji Technicznej.
23) Jeżeli instalowane oprogramowanie lub dostarczany Komponent wymaga przypisania licencji do świadczenia wymaganej funkcjonalności licencja ta musi zostać przypisana oraz aktywowana.

18.2. Dokumentacja

Podane poniżej zapisy są wspólne dla obu Zadań.

1) Przygotowane przez Wykonawcę, w terminach wynikających ze planu wdrożenia opisanego w punkcie **18.1**, dokumenty:
   a) Dokumentacja Techniczna,
   b) plany testów zgodnie z wytycznymi opisanymi w punkcie **18.5**,
   c) Dokumentacja Powykonawcza podlegają akceptacji Zamawiającego.
2) Zamawiający może zgłosić uwagi do dokumentów, o których mowa w ust. 1 powyżej, w terminach podanych w punkcie z **18.1** od ich otrzymania.
3) W przypadku zgłoszenia przez Zamawiającego uwag i zastrzeżeń do dokumentów, o których mowa w ust. 1 powyżej, Wykonawca zobowiązany jest ustosunkować się do stanowiska Zamawiającego nie później niż w terminie podanym w punkcie z **18.1**, od dnia zgłoszenia uwag, natomiast Zamawiający nie później niż w terminie podanym w punkcie **18.1**, od otrzymania odpowiedzi Wykonawcy, o której mowa powyżej, wypowiada się co do akceptacji poprawionej wersji dokumentu. Wykonawca zobowiązany jest do wprowadzenia wszystkich uwag i zastrzeżeń zgłoszonych przez Zamawiającego w terminach podanych w punkcie z **18.1** od ich otrzymania.
4) W celu uniknięcia wątpliwości strony ustalają, że zaakceptowanie przez Zamawiającego dokumentów, o których mowa w ust. 1 powyżej, nie zwalnia Wykonawcy z odpowiedzialności za spełnienie funkcjonalności określonych w SWZ.
5) Szczegółowe wytyczne dla dokumentacji zostały wskazane punktach **18.3** i **18.4**.
6) Szczegółowe wytyczne dla testów zostały wskazane punkcie **18.5**.

18.3. Dokumentacja Techniczna

Przed przystąpieniem do realizacji dostawy przez Wykonawcę musi zostać zaakceptowana przez Zamawiającego Dokumentacja Techniczna w celu weryfikacji poprawności koncepcji realizacji przedmiotu zamówienia z wymaganiami Zamawiającego. Dokumentacja techniczna musi spełniać następujące wymagania:

1) musi być oparta o najlepsze praktyki, standardy i najnowszą wiedzę w zakresie który obejmuje,
2) musi zostać zaakceptowana przez Zamawiającego przed rozpoczęciem dostaw,
3) musi zawierać co najmniej:
   a) listę wymagań funkcjonalnych Zamawiającego,

b) sposób realizacji wymagań funkcjonalnych,
c) architekturę Systemu, dodatkowo dla Zadania nr 1 z uwzględnieniem dwóch ośrodków (lokalizacje „BST" i „DCW") wraz z uzgodnionym z Zamawiającym podziałem ilościowym sprzętu na lokalizacje,
d) fizyczny i logiczny model połączeń poszczególnych Komponentów,
e) architekturę platformy wirtualizacyjnej zbudowanej na bazie dostarczanego oprogramowania do wirtualizacji wraz z modułami opisanymi w punkcie **12**,
f) architekturę systemu przestrzeni dyskowej zbudowanej na bazie dostarczonych macierzy blokowych,
g) architekturę systemu pamięci masowej zbudowanej na bazie dostarczonych systemów pamięci masowej,
h) architekturę połączeń elementów sieciowych na potrzeby realizacji poszczególnych funkcjonalności (dostęp do systemów pamięci masowej z serwerów, dostęp do Internetu z serwerów, zdalny dostęp, zarządzanie Out of Band, itd.)
i) architekturę połączeń wszystkich elementów sieciowych (co najmniej: adresacja IP, diagramy połączeń, sposób realizacji redundancji połączeń pomiędzy urządzeniami),
j) architekturę systemu do wykonywania kopii zapasowych przy użyciu dostarczonego urządzenia do przechowywania kopii zapasowych opisanego w punkcie **10** (o ile było dostarczane w ramach danego Zadania) oraz oprogramowania do wykonywania kopii zapasowych opisanego w punkcie **11**,
k) aranżację poszczególnych elementów w szafach teletechnicznych,
l) schemat nazewnictwa wszystkich dostarczonych elementów,
m) schemat nazewnictwa wszystkich wykorzystywanych interfejsów,
n) plany konfiguracji sieci w tym adresacji, portów itd. (IP design) wszystkich podłączonych do sieci Komponentów,
o) plany instalacji urządzeń i podłączenia do sieci LAN i zasilania, w tym porty itd. (obwody prądowe),
p) opis integracji, a w tym:
    i. architektura i sposób zapewnienia zdalnego dostępu do poszczególnych Komponentów,
q) listę wdrażanych Komponentów wraz z ich ilościami,
r) szczegółowy wykaz dostarczonych licencji na oprogramowanie,
s) dokumentacje producenckie wszystkich użytych Komponentów i elementów systemu (może być dostarczona w wersji elektronicznej),
t) inne, wg uznania Wykonawcy.

18.4. Dokumentacja Powykonawcza

Podane poniżej zapisy są wspólne dla obu Zadań. Dokumentacja Powykonawcza musi spełniać poniższe wymagania.

1) Dokumentacja Powykonawcza musi być opracowana na podstawie założeń zapisanych w Dokumentacji Technicznej (opisanej w punkcie **18.3**) i jeśli od niego odbiega powinien być załączony opis z czego ta różnica wynika
2) Dokumentacja Powykonawcza musi zawierać szczegółowe procedury eksploatacyjne i utrzymaniowe, a także procedury zgłaszania do Wykonawcy awarii i problemów z Systemem w okresie gwarancji.
3) Dokumentacja Powykonawcza musi zawierać szczegółową konfigurację dostępów administracyjnych do Komponentów.
4) Dokumentacja Powykonawcza musi zawierać procedury zarządzania użytkownikami i ich uprawnieniami.

5) Dokumentacja Powykonawcza musi zawierać procedury tworzenia kopii zapasowych i odzyskiwania danych z utworzonych kopii.
6) Dokumentacja Powykonawcza musi zawierać dokumentację producentów elementów składowych Komponentów Systemu i dokumentację rozwiązań technologicznych, w postaci elektronicznej oraz dostępu do zasobów elektronicznych producenta na stronie WWW przez okres gwarancji.
7) Dokumentacja Powykonawcza musi także zawierać co najmniej:
   a) listę zainstalowanych urządzeń z numerami seryjnymi, wersją zainstalowanego oprogramowania oraz opis wykonanej instalacji fizycznej,
   b) schemat rozmieszczenia poszczególnych urządzeń w szafach,
   c) zestawienie wykonanych połączeń fizycznych pomiędzy zainstalowanymi urządzeniami na potrzeby sieci, z uwzględnieniem nazw i numerów interfejsów, typów połączeń i oznaczeniem połączeń,
   d) dokumentację infrastruktury sieciowej wybudowanej na potrzeby realizacji wdrożenia – co najmniej: schemat połączeń logicznych i fizycznych, zestawienie użytych adresacji IP, konfiguracja urządzeń sieciowych,
   e) dokumentację zarządzania Out-of-Band dostarczonymi urządzeniami – co najmniej: schemat połączeń logicznych i fizycznych, zestawienie użytych adresacji IP, konfiguracja urządzeń zapewniających dostęp zarządzania Out-of-Band,
   f) dokumentacja fotograficzna wykonanej instalacji,
   g) opis konfiguracji poszczególnych urządzeń,
   h) zestawienie informacji o podłączeniu zainstalowanych urządzeń do zasilania.
8) Procedury administracyjne opisujące czynności dla Systemu muszą zawierać co najmniej następujące opisy:
   a) procedury instalacji poszczególnych Komponentów,
   b) procedury utrzymaniowe,
   c) procedury diagnostyczne w przypadku awarii.
9) Opis architektury systemu obejmujący co najmniej następujące elementy:
   d) szczegółowy model architektury Komponentów rozwiązania wraz z integracjami,
   e) opis scenariuszy i raportów wszystkich testów,
   f) szczegółowa architektura platformy wirtualizacyjnej wraz z jej modułami,
   g) szczegółowa architektura dostarczonych macierzy i systemów pamięci masowej,
   h) szczegółowa architektura bezpieczeństwa Systemu
   i) szczegółowa architektura systemu do wykonywania kopii zapasowych,
   j) opis konfiguracji elementów Systemu zgodnie z wymaganiami z punktu **18.1.3** dla Zadania nr 1 lub **18.1.5** dla Zadania nr 2,
   k) architektura, opis działania oraz parametry HA,
   l) szczegółowa architektura i konfiguracja wszystkich przewidzianych integracji,
   m) szczegółowy opis procedur eksploatacyjnych, utrzymaniowych i awaryjnych Systemu i wszystkich Komponentów wchodzących w skład Systemu,
   n) szczegółowy opis monitorowania, raportowania i automatyzacji Komponentów wchodzących w skład Systemu,
   o) szczegółowy opis i konfiguracja Systemu w zakresie dostępu administracyjnego, uwierzytelniania i autoryzacji dla użytkowników,
   p) instrukcje administratora systemu (co najmniej na poziomie zarządzania i używania, oraz analizy możliwych problemów).
10) Dokumentacja Powykonawcza w zakresie konfiguracji musi obejmować wszystkie elementy wdrożone, zainstalowane w ramach realizacji przedmiotu zamówienia. Minimalny zestaw wymaganych danych konfiguracyjnych obejmuje:
   a) model urządzenia, parametry sprzętowe (np. kontrolery, półki dyskowe, dyski, przełączniki, moduły optyczne, itp.), konfigurację macierzy blokowych i systemów pamięci masowej (grupy dyskowe, zasoby dyskowe itp.), sposób podłączenia wszystkich Komponentów do infrastruktury Zamawiającego,

b) schemat infrastruktury wraz z opisem,
c) licencje dla dostarczonych elementów Systemu,
d) informacje o ograniczeniach technologicznych (liczba dysków, rozmiar cache, itp.) dostarczonych elementów infrastruktury,
e) procedury utrzymaniowe dla poszczególnych komponentów,
f) procedury aktualizacji oprogramowania,
g) procedury zgłaszania problemów,
h) opracowanie procedur eksploatacyjnych dla pierwszej linii wsparcia: diagnostyka, monitoring, analiza awarii,
i) opracowanie dokumentacji w zakresie procedur awaryjnych dla pierwszej linii wsparcia, umożliwiających diagnozowanie Systemu i podstawowej weryfikacji przyczyny problemu.

11) Do Dokumentacji Powykonawczej musi być załączony raport z testów wykonanych po realizacji wdrożenia.

18.5. Wytyczne do testów

Podane poniżej zapisy są wspólne dla obu Zadań. Proces testowania Systemu związany z wdrożeniem i ewentualnymi zmianami w Systemie składa się następujących działań:

1) przygotowanie Systemu – Wykonawca przygotowuje System do wdrożenia i opracowuje scenariusze testowe oraz zakres testów akceptacyjnych, które muszą być zaakceptowane przez Zamawiającego,
2) testy weryfikacyjne na dostarczonym Systemie – realizowane samodzielnie przez Wykonawcę; ich wyniki nie przesądzają o odbiorze Systemu,
3) testy akceptacyjne – realizowane przez Wykonawcę we współpracy z Zamawiającym, na podstawie wcześniej przygotowanego i zaakceptowanego zakresu testów akceptacyjnych, celem sprawdzenia poprawności przygotowania Systemu,
4) testy wydajnościowe – realizowane przez Wykonawcę we współpracy z Zamawiającym, na podstawie wcześniej przygotowanego i zaakceptowanego zakresu testów wydajnościowych, celem sprawdzenia wydajności Systemu,
5) zaakceptowane wyniki testów – zakończone z sukcesem testy akceptacyjne Systemu,
6) testy odbiorcze – realizowane przez Wykonawcę we współpracy z Zamawiającym, na podstawie zaakceptowanych wcześniej scenariuszy testowych.

18.5.1. Testy weryfikacyjne

Nazwa testów	Testy weryfikacyjne
Cel testów	weryfikacja czy dostarczone i zainstalowane środowisko jest gotowe do pełnienia funkcji produkcyjnej
Realizujący	Wykonawca

Wykonawca samodzielnie przygotowuje zakres, scenariusze testowe, dane testowe i realizuje testy. Po zakończeniu testów Wykonawca jest zobowiązany do dostarczenia Zamawiającemu raportu z realizacji testów.
W zakres testów weryfikacyjnych muszą wchodzić przynajmniej poniższe elementy:

1) testy zdalnego dostępu do Systemu i jego wszystkich elementów,
2) weryfikacja instalacji wszystkich elementów Komponentów Systemu,
3) testowanie składników zarządzania Systemem,
4) testowanie i zatwierdzanie projektu architektury Systemu.

18.5.2. Testy akceptacyjne (podstawowe i niezawodnościowe)

Nazwa testów	Testy akceptacyjne (podstawowe i niezawodnościowe)
Cel testów	weryfikacja poprawności działania poszczególnych elementów Systemu
Realizujący	Wykonawca we współpracy z Zamawiającym
Wejście	Raport z testów weryfikacyjnych
Wyjście	Raport z testów akceptacyjnych (podstawowych i niezawodnościowych)

Celem przeprowadzonych testów jest weryfikacja poprawności działania dostarczonych Komponentów.

Testy akceptacyjne składają się z następujących elementów:

1) testów podstawowych – podstawowy zakres testów zdefiniowany przez Wykonawcę i zaakceptowany przez Zamawiającego, którego celem jest weryfikacja Komponentów Systemu,
2) testów niezawodnościowych.

W ramach procesu testowania należy zrealizować wszystkie testy, pozytywne zakończenie testów każdego typu jest podstawą do zaakceptowania instalacji Systemu.

Testy podstawowe

Podstawowy zakres testów akceptacyjnych musi obejmować weryfikację:

1) poprawności działania,
2) funkcjonalności,
3) poprawnej konfiguracji,
4) możliwości zarządzania

w odniesieniu do wszystkich dostarczonych Komponentów.

Podstawowy zakres testów akceptacyjnych musi obejmować co najmniej poniższe scenariusze:

1) tworzenie maszyn wirtualnych,
2) wykonywanie snapshot-ów maszyn wirtualnych,
3) klonowanie maszyn wirtualnych,
4) migrowanie maszyn między hostami zarówno dla warstwy obliczeniowej jak i danych,
5) przygotowanie infrastruktury do korzystania z programowalnej sieci komputerowej (ang. SDN),
6) tworzenie i zarządzanie logicznymi segmentami sieci,
7) tworzenie i zarządzanie logicznym routingiem,
8) tworzenie i zarządzanie serwisami/usługami logicznymi (dhcp, load balancer, nat),
9) tworzenie i zarządzanie regułami bezpieczeństwa – koncepcja zero trust security,
10) tworzenie i zarządzanie wirtualnymi zasobami dyskowymi,
11) korzystanie z narzędzenia do monitorowania i rozwiązywania problemów,
12) weryfikację poprawności konfiguracji klastra i wykorzystania kompatybilnych Komponentów serwera,
13) weryfikacja wszystkich elementów serwera i ich parametrów,
14) weryfikacja możliwości zarzadzania serwerami,
15) weryfikacja wszystkich parametrów macierzy blokowych i systemów pamięci masowej,

16) weryfikacja możliwości zarzadzania macierzami blokowymi i systemami pamięci masowej,
17) weryfikacja wszystkich elementów infrastruktury sieciowej,
18) weryfikacja możliwości zarządzania poszczególnymi elementami infrastruktury sieciowej,
19) weryfikacja poprawności działania usługi zdalnego dostępu do infrastruktury dla administratorów,
20) weryfikacja możliwości zarządzania poszczególnymi elementami systemu za pomocą usługi zdalnego dostępu,
21) wykonanie kopii zapasowej maszyny wirtualnej,
22) odtworzenie maszyny wirtualnej z kopii zapasowej.

Za realizację testów odpowiada Wykonawca, realizując je wspólnie z Zamawiającym. Zakres testów powinien być spójny ze scenariuszami testów odbiorczych, jednakże może zostać zmodyfikowany w trakcie prac projektowych po akceptacji Zamawiającego. Do realizacji testów akceptacyjnych należy przygotować listy funkcjonalności / procesów wymagających przetestowania, nie muszą to być pełne scenariusze testowe.

Zakończenie testów akceptacyjnych jest możliwe po zamknięciu wszystkich zgłoszonych błędów, czy to poprzez ich rozwiązanie, czy poprzez ustalenie pomiędzy Zamawiającym i Wykonawcą, że dany błąd nie jest błędem istotnym.

Testy niezawodnościowe

Zakres testów niezawodnościowych musi obejmować weryfikację możliwych awarii w odniesieniu do wszystkich dostarczonych Komponentów.

Podstawowy zakres testów niezawodnościowych musi obejmować co najmniej poniższe symulacje:

1) symulacje awarii hosta w klastrze z wyłączeniem HA oraz test z włączonym HA dla maszyn wirtualnych z przypisana polityką odporności na awarię minimum jednego hosta,
2) symulacje awarii dysku z danymi w macierzach dyskowych oraz w systemach pamięci masowej,
3) symulacje awarii dysku cache w systemach pamięci masowej,
4) symulacje awarii połączenia sieciowego w serwerze,
5) symulacje awarii przełącznika LAN,
6) wprowadzenie serwera w tryb konserwacji i wyprowadzenie go z tego trybu i obserwacje dostępności wirtualnych maszyn w klastrze,
7) symulacje awarii każdego z Komponentów Systemu dla potwierdzenia pełnej redundancji.

18.5.3. Testy wydajnościowe

Nazwa testów	Testy wydajnościowe
Cel testów	Weryfikacja czy dostarczony System zapewnia wystarczającą wydajność
Realizujący	Wykonawca we współpracy z Zamawiającym
Wejście	Raport z testów akceptacyjnych (podstawowych i niezawodnościowych)
Wyjście	Raport z testów wydajnościowych

Wykonawca jest zobowiązany do przygotowania i przeprowadzenia we współpracy z Zamawiającym testów wydajnościowych, których celem jest weryfikacja, czy System zapewnia odpowiednie parametry zgodnie z wymaganiami zamieszczonymi w opisie technicznym.

Wykonawca jest zobowiązany do przeprowadzenia testów w oparciu o gotowe, istniejące na rynku, narzędzia/programy.

Wynikiem przeprowadzonych testów musi być potwierdzenie parametrów wydajnościowych wymaganych przez Zamawiającego w niniejszym SWZ. Zakres parametrów wydajnościowych musi obejmować co najmniej:

1) w przypadku serwerów – potwierdzenie wydajności w teście CPU2017 Floating Point Rate zgodnie z wymaganiami zawartymi w SWZ,
2) w przypadku elementów sieciowych – przepustowości interfejsów dla ruchu typu IMIX zgodnie z wymaganiami zawartymi w SWZ lub w karcie katalogowej producenta jeśli nie podano w SWZ.

Pozytywne zakończenie testów każdego typu jest podstawą do zaakceptowania instalacji Systemu.

18.5.4. Testy odbiorcze

Nazwa testów	Testy odbiorcze
Cel testów	Weryfikacja poprawności działania wszystkich procesów w ramach dostarczonego Systemu
Realizujący	Wykonawca we współpracy z Zamawiającym
Wejście	Raport z testów akceptacyjnych i niezawodnościowych oraz wydajnościowych
Wyjście	Protokół zdawczo – odbiorczy

Wykonawca w ustalonym harmonogramie i terminie zgłasza Zamawiającemu gotowość Systemu do przeprowadzenia testów odbiorczych.

1) Zgłaszając Zamawiającemu gotowość Systemu do przeprowadzenia testów odbiorczych, Wykonawca zobligowany jest przedstawić raport z przeprowadzonych przez siebie testów potwierdzających gotowość do testów odbiorczych i zgodność Systemu z wymaganiami Zamawiającego.
2) Procedury testów odbiorczych muszą zawierać co najmniej następujące elementy:
   a) wprowadzenie
   b) opis przedmiotu testów
   c) zakres testów – testowane obszary
   d) wyłączenia z zakresu
   e) podejście do testowania
   f) kryteria zaliczenia/niezaliczenia testów
   g) kryteria zawieszenia i wznowienia testowania
   h) czynności i zadania testowania
   i) środowiska testowe
   j) harmonogram
   k) ryzyka i plany awaryjne
   l) zatwierdzenie planu.

W celu weryfikacji poszczególnych funkcjonalności Systemu, Zamawiający określi dodatkowe testy funkcjonalne potwierdzające prawidłowe działanie tych funkcjonalności.

Zamawiający wymaga przeprowadzenia co najmniej następujących testów:

1) dostępności:
   a) odporność na awarie dysku w macierzach blokowych oraz w systemach pamięci masowej: wyjęcie jednego, dwóch dysków,

b) odporność na awarie klastra: wyłączenie jednego, dwóch serwerów,

2) monitorowania warstwy fizycznej urządzenia Systemu:
   a) symulacja awarii/niedostępności zasilania,
   b) symulacja awarii/niedostępności dysku,
3) mikro-segmentacji ruchu sieciowego dla maszyn wirtualnych, weryfikacji kontroli ruchu w warstwie L3 i L4 w jednym segmencie L2 dla komunikacji IP między dwoma maszynami wirtualnymi
   a) testy realizowane na maszynach wirtualnych umieszczonych na jednym i dwóch serwerach fizycznych,
4) weryfikacji wydajności w komunikacji maszyna wirtualna z maszyną wirtualną:
   a) test wydajnościowy w komunikacji IP między maszynami wirtualnymi,
5) wykonania kopi zapasowej w środowisku:
   a) wykonanie i odtworzenie kopii maszyny wirtualnej
6) dostępności danych dla macierzy blokowej i systemów pamięci masowej:
   a) uruchamianie i zatrzymywanie urządzeń,
   b) symulacja awarii pojedynczego węzła,
   c) symulacja awarii pojedynczego portu LAN,
   d) symulacja awarii pojedynczego dysku,
7) całości Systemu:
   a) symulacja awarii jednego z torów zasilania dla zasilaczy w urządzeniach,
   b) symulacja awarii sieci LAN poprzez wyłączenie portów komunikacyjnych LAN.

18.6. Odbiory

Podane poniżej zapisy są wspólne dla obu Zadań. Odbiór oznacza przeprowadzenie testów odbiorczych oraz potwierdzenie protokołem zdawczo – odbiorczym zgodności przedmiotu zamówienia z warunkami umowy.

Protokolarnemu odbiorowi przez Zamawiającego podlegać będą:

1) dostawa sprzętu, oprogramowania i licencji,
2) dokumentacja techniczna,
3) raporty z testów,
4) instruktaży,
5) wykonanie całości odbieranego przedmiotu zamówienia.

19. Instruktaż dla Zadania nr 1

19.1. Wstęp

W ramach realizacji przedmiotu zamówienia Wykonawca jest zobowiązany do przeprowadzenia instruktaży zgodnie z przedstawionymi poniżej wymaganiami Zamawiającego. Instruktaże muszą być przeznaczone dla grupy administratorów – osób odpowiedzialnych za nadzór, utrzymanie oraz prace operacyjne (przeprowadzanie zmian i konfiguracji Systemu), a także monitorowanie elementów Systemu.

19.2. Zbiór wymagań dla instruktaży

1) Wykonawca zapewni materiały instruktażowe w języku polskim lub angielskim dla wszystkich uczestników instruktaży (prezentacje, książki/podręczniki, ćwiczenia).
2) Maksymalna liczba osób w danej grupie nie przekroczy 15 osób.
3) Wykonawca przeprowadzi instruktaże w formule praktycznych zadań, istnieje możliwość przeprowadzenia ich na dostarczonym i wdrożonym środowisku będącym przedmiotem tego postępowania. Nie może dojść do sytuacji, że wdrożone środowisko po przeprowadzeniu instruktażu będzie niefunkcjonalne.
4) Instruktaże muszą obejmować zakres merytoryczny dotyczący obsługi funkcjonalności wymaganych przez Zamawiającego w ramach wdrożonego Systemu.
5) Instruktaże muszą być przeprowadzone przez instruktorów posiadających certyfikaty poświadczające ich wiedzę, wydane przez producenta/producentów dostarczonego Systemu lub poszczególnych Komponentów/modułów tego Systemu.
6) Instruktaż musi być przeprowadzony stacjonarnie w siedzibie Zamawiającego w języku polskim. Zamawiający zastrzega sobie prawo do zmiany formy instruktarzu z trybu stacjonarnego na tryb zdalny (przez system wideokonferencyjny zapewniony przez Wykonawcę).
7) Nie dopuszcza się instruktażu w formie szkolenia typu „e-learning”.
8) Termin instruktażu musi zostać ustalony z Zamawiającym.
9) Zakres poszczególnych instruktaży musi być uzgadniany i zaakceptowany przez Zamawiającego.
10) W każdym instruktarzu należy uwzględnić czas na pytania od uczestników.
11) Szczegółowy zakres merytoryczny instruktaży:
    a) instruktaż wstępny:
        i) omówienie architektury Systemu, w tym na podstawie dokumentacji wykonawczej m.in.
            (1) architektury serwerów
            (2) architektury platformy wirtualizacyjnej wraz z wszystkimi jej modułami
            (3) architektury macierzy blokowej i systemu pamięci masowej
            (4) architektury urządzeń sieciowych
            (5) architektury wdrożonego systemu wirtualizacyjnego
            (6) architektury systemu kopii zapasowych
            (7) podstawowej funkcjonalności wdrożonego systemu wirtualizacyjnego w szczególności w zakresie:
                (a) tworzenie alertów, raportów i widoków
                (b) omówienie procesów tworzenia i odzyskiwania kopii zapasowej
                (c) omówienie procesu odzyskania środowisk po awarii
                (d) aspekty związane z monitorowaniem infrastruktury Systemu
                (e) aspekty związane z platformą wirtualizacyjną wraz z wszystkimi jej modułami
                (f) aspekty związane z zarządzaniem wirtualizacją zasobów obliczeniowych
                (g) aspektów związanych z macierzami blokowymi i systemami pamięci masowej

(h) aspektów związanych z urządzeniami sieciowymi

ii) techniczne omówienie architektury wdrożonego Systemu
iii) zarządzanie infrastrukturą serwerów fizycznych i zwirtualizowanych
iv) zarządzanie platformą wirtualizacji obejmującą wszystkie jej moduły dostarczone w ramach postępowania
v) omówienie i zarządzanie procesami tworzenia i odzyskiwania kopii zapasowej
vi) omówienie i zarządzanie procesami odzyskania środowisk po awarii
vii) omówienie i zarządzanie macierzą blokową oraz systemami pamięci masowej
viii) zarządzanie monitorowaniem warstwy wirtualizacji wraz z serwerami fizycznymi
ix) aspekty związane z zarządzaniem oprogramowaniem monitorującym wirtualizację
x) zarządzanie użytkownikami, rolami, poziomami dostępu.

b) instalacja, konfiguracja i zarządzanie serwerami:
i) proces instalacji, konfiguracji, zarządzania serwerem,
ii) proces aktualizacji oprogramowania Komponentów serwerów,
iii) proces aktualizacji oprogramowania zainstalowanego na serwerach,
iv) omówienie funkcjonalności systemu do zarządzania serwerem.

c) implementacja i zarządzanie macierzą blokową, w tym ćwiczenia praktyczne z poniższej tematyki:
i) omówienie architektury macierzy blokowej,
ii) omówienie elementów składowych macierzy blokowej (sprzętowe i programowe składniki),
iii) omówienie konfiguracji macierzy blokowej,
iv) omówienie konfiguracji pod kątem odporności na awarie oraz wydajności,
v) omówienie protokołów dostępu i ich konfiguracji,
vi) omówienie udostępniania urządzeń blokowych przez protokół iSCSI,
vii) kopie migawkowe,
viii) „tiering" bloków danych pomiędzy dyskami,
ix) wymagania pracy całkowicie bez przestojów z zapewnieniem najwyższego poziomu trwałości danych,
x) redukcja danych (deduplikacja),
xi) naprawa po awarii sprzętowej,
xii) hot-spare lub przestrzeń nadmiarowa,
xiii) zabezpieczenie danych przed złośliwym oprogramowaniem szyfrującym,
xiv) gwarancja niezmienności danych,
xv) stosowanie wielu protokołów dostępu działających jednocześnie,
xvi) mechanizmy ochrony danych (synchronizacje, replikacje w wielu różnych topologiach) pomiędzy lokalizacjami i ich zastosowanie,
xvii) sposoby monitorowania macierzy blokowej,
xviii) diagnozowanie problemów i awarii,
xix) punkty zarządzania macierzą blokową,
xx) aktualizacja oprogramowania.

d) implementacja i zarządzanie systemem szybkiej pamięci masowej o dostępie plikowym, w tym ćwiczenia praktyczne z poniższej tematyki:
i) omówienie architektury systemu,
ii) omówienie elementów składowych systemu (sprzętowe i programowe składniki systemu),
iii) niezmienność przechowywanych danych w wielu kopiach (sumy kontrolne, technologia WORM, retencja),
iv) sposób/oby przechowywania nieusystematyzowanych danych m.in. dane multimedialne (zdjęcia, filmy),

v) sposób/oby przechowywania danych analitycznych,
vi) repozytoria danych na potrzeby klastrów obliczeniowych,
vii) sposoby efektywnego przetwarzania metadanych (dane opisujące przechowywane obiekty),
viii) omówienie protokołów dostępu, m.in. NFS, CIFS, HTTP, S3 i ich konfiguracji,
ix) omówienie, konfiguracja HDFS,
x) dostępne scenariusze replikacji danych między węzłami/kontrolerami,
xi) elastyczne mechanizmy ochrony danych, mirroring i kody korekcyjne,
xii) wymagania pracy całkowicie bez przestojów z zapewnieniem najwyższego poziomu trwałości danych,
xiii) naprawa po awarii sprzętowej,
xiv) skalowalność i rozbudowa systemu,
xv) sposoby zapewniania należytej wydajności całego systemu odpowiednio do wzrostu pojemności i wymagań na przepustowość,
xvi) retencja i ochrona danych WORM,
xvii) zapewnienie gwarancji niezmienności danych i ochrona przed ich skasowaniem,
xviii) omówienie funkcjonalności trwałego nośnika zwanego WORM i ustawianie czasu retencji danych i metadanych z gwarancją, że przed upływem tego czasu nie zostaną one usunięte,
xix) zabezpieczenie danych przed złośliwym oprogramowaniem szyfrującym,
xx) gwarancja niezmienności danych,
xxi) stosowanie wielu protokołów dostępu działających jednocześnie,
xxii) mechanizmy ochrony danych (synchronizacje, replikacje w wielu różnych topologiach) pomiędzy lokalizacjami i ich zastosowanie,
xxiii) sposoby monitorowania systemu,
xxiv) diagnozowanie problemów i awarii,
xxv) punkty zarządzania systemem,
xxvi) aktualizacja oprogramowania.

e) implementacja i zarządzanie systemem archiwalnej pamięci masowej o dostępie plikowym, w tym ćwiczenia praktyczne z poniższej tematyki:
i) omówienie architektury systemu,
ii) omówienie elementów składowych systemu (sprzętowe i programowe składniki systemu),
iii) niezmienność przechowywanych danych w wielu kopiach (sumy kontrolne, technologia WORM, retencja),
iv) sposób/oby przechowywania nieusystematyzowanych danych m.in. dane multimedialne (zdjęcia, filmy),
v) sposób/oby przechowywania danych analitycznych,
vi) repozytoria danych na potrzeby klastrów obliczeniowych,
vii) sposoby efektywnego przetwarzania metadanych (dane opisujące przechowywane obiekty),
viii) omówienie protokołów dostępu, m.in. NFS, CIFS, HTTP, S3 i konfiguracji,
ix) omówienie i konfiguracja HDFS,
x) omówienie dostępnych scenariuszy replikacji danych między węzłami/kontrolerami,
xi) elastyczne mechanizmy ochrony danych, mirroring i kody korekcyjne,
xii) wymagania pracy całkowicie bez przestojów z zapewnieniem najwyższego poziomu trwałości danych,
xiii) naprawa po awarii sprzętowej,
xiv) skalowalność i rozbudowa systemu,

xv) sposoby zapewniania należytej wydajności całego systemu odpowiednio do wzrostu pojemności i wymagań na przepustowość,
xvi) retencja i ochrona danych WORM,
xvii) zapewnienie gwarancji niezmienności danych i ochrona przed ich skasowaniem,
xviii) omówienie funkcjonalności trwałego nośnika zwanego WORM i ustawianie czasu retencji danych i metadanych z gwarancją, że przed upływem tego czasu nie zostaną one usunięte,
xix) zabezpieczenie danych przed złośliwym oprogramowaniem szyfrującym,
xx) gwarancja niezmienności danych,
xxi) stosowanie wielu protokołów dostępu działających jednocześnie,
xxii) mechanizmy ochrony danych (synchronizacje, replikacje w wielu różnych topologiach) pomiędzy lokalizacjami i ich zastosowanie,
xxiii) sposoby monitorowania systemu,
xxiv) diagnozowanie problemów i awarii,
xxv) punkty zarządzania systemem,

f) implementacja i zarządzanie systemem pamięci masowej o dostępie obiektowym, w tym ćwiczenia praktyczne z poniższej tematyki:
i) omówienie architektury systemu,
ii) omówienie elementów składowych systemu (sprzętowe i programowe składniki systemu),
iii) niezmienność przechowywanych danych w wielu kopiach (sumy kontrolne, technologia WORM, retencja),
iv) sposób/oby przechowywania nieusystematyzowanych danych m.in. dane multimedialne (zdjęcia, filmy),
v) sposób/oby przechowywania danych analitycznych,
vi) repozytoria danych na potrzeby klastrów obliczeniowych,
vii) sposoby efektywnego przetwarzania metadanych (dane opisujące przechowywane obiekty),
viii) omówienie protokołów dostępu, w tym S3 i jego konfiguracji oraz innych protokołów m.in. NFS, CIFS, HTTP,
ix) omówienie dostępnych scenariuszy replikacji danych między węzłami/kontrolerami,
x) elastyczne mechanizmy ochrony danych, mirroring i kody korekcyjne,
xi) wymagania pracy całkowicie bez przestojów z zapewnieniem najwyższego poziomu trwałości danych,
xii) naprawa po awarii sprzętowej,
xiii) skalowalność i rozbudowa systemu,
xiv) sposoby zapewniania należytej wydajności całego systemu odpowiednio do wzrostu pojemności i wymagań na przepustowość,
xv) retencja i ochrona danych WORM,
xvi) zapewnienie gwarancji niezmienności danych i ochrona przed ich skasowaniem,
xvii) omówienie funkcjonalności trwałego nośnika zwanego WORM i ustawianie czasu retencji danych i metadanych z gwarancją, że przed upływem tego czasu nie zostaną one usunięte,
xviii) zabezpieczenie danych przed złośliwym oprogramowaniem szyfrującym,
xix) gwarancja niezmienności danych,
xx) stosowanie wielu protokołów dostępu działających jednocześnie,
xxi) mechanizmy ochrony danych (synchronizacje, replikacje w wielu różnych topologiach) pomiędzy lokalizacjami i ich zastosowanie,
xxii) sposoby monitorowania systemu,
xxiii) diagnozowanie problemów i awarii,

xxiv) punkty zarządzania systemem,

g) implementacja i zarządzanie komponentem do wykonywania kopii zapasowych (urządzenie do przechowywania kopii zapasowych wraz z oprogramowaniem do wykonywania kopii zapasowych), w tym ćwiczenia praktyczne z poniższej tematyki:
   i) omówienie funkcjonalności oprogramowania i zapoznanie z interfejsem,
   ii) omówienie architektury urządzenia do przechowywania kopii zapasowych,
   iii) urządzenie do przechowywania kopii zapasowych – konfiguracja, utrzymanie, monitorowanie, optymalizacja, dobre praktyki,
   iv) omówienie zarządzania danymi archiwalnymi w środowiskach wirtualnych,
   v) omówienie zagadnień obejmujących cel i czas odzyskiwania (RTO) i (RPO),
   vi) omówienie metod konfiguracji zapewniających skuteczną ochronę danych i maksymalizację wydajności procesora, sieci i pamięci w środowisku zwirtualizowanym,
   vii) prowadzenie testów odzyskiwania dla różnych scenariuszy,
   viii) omówienie architektury komponentów i relacji między nimi,
   ix) sposoby odzyskiwania danych plikowych,
   x) omówienie interfejsów raportujących i pulpitów nawigacyjnych do monitorowania wydajności i minimalizacji ryzyka utraty danych,
   xi) omówienie metod rozwiązywania problemów i analizy raportów,
   xii) omówienie komponentów do tworzenia kopii zapasowych i replikacji,
   xiii) omówienie oznaczania lokalizacji przechowywanych danych,
   xiv) ustawianie powiadomień globalnych,
   xv) omówienie zarządzania połączeniami IP dla przesyłania danych,
   xvi) omówienie reguł ruchu sieciowego,
   xvii) omówienie procesu wykonywania kopii zapasowych maszyn wirtualnych,
   xviii) omówienie metod tworzenia kopii zapasowych,
   xix) omówienie optymalizacji wielkości danych,
   xx) omówienie dostępnych integracji dla pamięci masowej,
   xxi) tworzenie zadań kopiowania maszyn wirtualnych / plików,
   xxii) planowanie i tworzenie punktów przywracania,
   xxiii) tworzenie kopii zapasowych za pomocą agentów,
   xxiv) odzyskiwanie z kopii zapasowej,
   xxv) natychmiastowe odzyskiwanie maszyn wirtualnych,
   xxvi) omówienie procesu pełnego odzyskiwania maszyn wirtualnych,
   xxvii) omówienie procesu odzyskiwania plików wirtualnych maszyn,
   xxviii) omówienie procesu odzyskiwania obiektów,
   xxix) omówienie odzyskiwania elementu z wspieranych aplikacji i baz danych,
   xxx) omówienie odzyskiwania plików systemu operacyjnego gościa,
   xxxi) tworzenie replik,
   xxxii) omówienie wglądu w replikację,
   xxxiii) omówienie procesu zmniejszenia ilości przesyłanych danych,
   xxxiv) odzyskiwanie z repliki,
   xxxv) omówienie przełączania awaryjnego,
   xxxvi) omówienie powrotu po awarii,
   xxxvii) omówienie planu pracy awaryjnej,
   xxxviii) omówienie planu przełączeń awaryjnych,
   xxxix) tworzenie kopii zapasowych,
   xl) omówienie funkcjonalności zadania kopii zapasowej,
   xli) omówienie procesu tworzenia kopii zapasowej,
   xlii) architektura kopii zapasowych,

xliii) zasady przechowywania archiwum,
xliv) tworzenie kopii zapasowych w archiwum,
xlv) monitorowanie poziomu wydajności i pojemności,
xlvi) deduplikacja systemów pamięci masowej,
xlvii) automatyczne testowanie odzyskiwania,
xlviii) przywracanie etapowe,
xlix) omówienie zarządzania użytkownikami i ich prawami dostępu do kopii zapasowych,
l) omówienie architektury urządzenia do przechowywania kopii zapasowych,
li) omówienie funkcjonalności uruchamiania kopii zapasowych maszyn wirtualnych bezpośrednio z urządzenia do przechowywania kopii zapasowych bez odtwarzania na jakikolwiek zewnętrzny magazyn danych.

h) instalacja, konfiguracja i zarządzanie modułem oprogramowania do wirtualizacji zasobów serwerowych i ich mocy obliczeniowej oraz modułem oprogramowania do zarządzania klastrem wirtualizacyjnym, w tym ćwiczenia praktyczne z poniższej tematyki:
   i) proces instalacji, konfiguracji, zarządzania oprogramowaniem do wirtualizacji zasobów serwerowych i ich mocy obliczeniowej oraz oprogramowaniem do zarządzania klastrem wirtualizacyjnym,
   ii) omówienie instalacji oraz konfiguracji i funkcjonalności konsoli graficznej do zarządzania maszynami wirtualnymi,
   iii) opcje konfiguracji wirtualizatora i przełącznika sieciowego,
   iv) konfiguracja wirtualizatora i przełącznika sieciowego w zakresie migracji maszyn wirtualnych w trakcie pracy, między serwerami,
   v) omówienie koncepcji pamięci masowej i stosowania wirtualizacji,
   vi) konfiguracja interfejsu zarządzania wirtualizatorem w serwerze, tworzenie magazynów danych,
   vii) omówienie mechanizmów rozkładania obciążenia i migracji maszyn wirtualnych i plików maszyn wirtualnych,
   viii) konfiguracja automatyzacji migracji maszyn wirtualnych,
   ix) omówienie koncepcji i narzędzia do aktualizacji środowiska,
   x) wykonanie aktualizacji serwerów,
   xi) profilowanie serwerów dla uproszczenia konfiguracji,
   xii) konfiguracja wysokiej dostępności wirtualizacji poprzez klastry,
   xiii) tworzenie szablonów maszyn wirtualnych i bibliotek scenariuszy,
   xiv) tworzenie, modyfikacja, przenoszenie, usuwanie maszyn wirtualnych,
   xv) wdrażanie maszyn wirtualnych z szablonów,
   xvi) klonowanie maszyn wirtualnych,
   xvii) monitorowanie zasobów maszyn wirtualnych,
   xviii) konfiguracja przekazywania logów do zewnętrznych systemów np. SIEM,
   xix) konfiguracja wysokiej dostępności dla głównej konsoli zarządzającej,
   xx) monitoring poprzez konsolę zarządzającą,
   xxi) konfiguracja wbudowanego serwera zapory sieciowej w oprogramowaniu do zarządzania klastrem wirtualizacyjnym,
   xxii) konfiguracja uwierzytelniania użytkowników logujących się do oprogramowania zarządzającego klastrem wirtualizacyjnym w oparciu o domenę Microsoft Active Directory lub Open LDAP.

i) instalacja, konfiguracja i zarządzanie modułem oprogramowania do wirtualizacji sieci, w tym ćwiczenia praktyczne z poniższej tematyki:
   i) sposoby instalacji, konfiguracji i zarządzania modułem oprogramowania do wirtualizacji sieci

ii) wyjaśnienie i omówienie tematyki: logiczne przełączanie, logiczny routing, usługi sieciowe i bezpieczeństwo, mikro-segmentacja, zapory ogniowe i inne komponenty,
iii) wyjaśnienie funkcjonalności, wymagań technicznych i ograniczeń w module oprogramowania do wirtualizacji sieci
iv) przeprowadzenie laboratorium z zakresu praktycznych zadań na temat instalacji, konfiguracji i zarządzania modułem,
v) budowanie architektury sieci zdefiniowanej programowo,
vi) omówienie Komponentów i głównych funkcjonalności,
vii) omówienie kluczowych funkcji i zalet stosowania,
viii) sposoby powoływania środowisk testowych jako kopii środowiska produkcyjnego,
ix) omówienie procesu wdrażania i konfiguracji infrastruktury sieci zdefiniowanej programowo,
x) omówienie wymagań na sieć podkładową,
xi) omówienie metod łączenia sieci zdefiniowanej programowo z siecią podkładową i usługami takimi jak Firewall, LoadBalancer, itp.,
xii) omówienie konfiguracji logicznego przełączania i mostkowania warstwy 2,
xiii) omówienie wielopoziomowej architektury routingu i konfiguracji bramy IP,
xiv) omówienie zaawansowanych usług, takich jak VPN i równoważenie obciążenia, sposoby implementacji,
xv) omówienie bezpieczeństwa usług w sieci programowej poprzez stosowanie mikrosegmentacji, izolacja ruchu L2/VLAN,
xvi) omówienie bezpieczeństwa modeli zapór ogniowych w celu chronienia ruchu wschód-zachód i północ-południe,
xvii) omówienie zaawansowanego wymuszania bezpieczeństwa w połączeniu ze środowiskiem produktów podmiotów trzecich,
xviii) omówienie konfiguracji kontroli dostępu opartej na rolach,
xix) sposoby zabezpieczania usług między centrami danych,
xx) sposoby monitorowania sieci zdefiniowanej programowo,
xxi) diagnostyka problemów z siecią podkładową,
xxii) sposoby aktualizacji oprogramowania.

j) instalacja, konfiguracja i zarządzanie modułem oprogramowania do wirtualizacji przestrzeni dyskowej, w tym ćwiczenia praktyczne z poniższej tematyki:
i) omówienie procesu uruchamiania pamięci masowej zdefiniowanej programowo
ii) omówienie funkcjonalności oprogramowania
iii) szczegółowa prezentacja architektury
iv) rodzaje funkcjonalności i przypadki ich użycia
v) konfiguracja oprogramowania i wymagane składniki sieciowe do pracy
vi) konfiguracja klastra pamięci masowej zdefiniowanej programowo i typy klastrów
vii) typy zabezpieczeń danych w pamięci masowej zdefiniowanej programowo i implementacja zmiany
viii) przedstawienie możliwych zmian w sposobie zabezpieczania danych i implementacja zmiany
ix) konfiguracja zasobów do przechowywania maszyn wirtualnych
x) wdrażanie maszyn wirtualnych w magazynie danych pamięci masowej zdefiniowanej programowo
xi) wykonywanie bieżących zadań administracyjnych z zarządzania
xii) aktualizacja pamięci masowej zdefiniowanej programowo
xiii) konfiguracja szyfrowania dla zwirtualizowanej pamięci masowej
xiv) konfiguracja replikacji synchronicznej i asynchronicznej między centrami danych

xv) zarządzanie stanem, monitorowanie kondycji i wydajności pamięci masowej zdefiniowanej programowo
xvi) konfiguracja klastra między dwoma centrami danych i analiza scenariuszy przełączania awaryjnego
xvii) planowanie i projektowanie klastrów
xviii) wykonanie praktycznych ćwiczeń laboratoryjnych z rozwiązywania problemów, przypadków awarii oraz metodologia rozwiązywania problemów narzędziami diagnostycznymi
xix) sposoby monitorowania klastrów, kondycji i wydajności
xx) używanie narzędzi diagnostycznych
xxi) sposoby rozwiazywania problemów związanych z wdrażaniem i zmianami w architekturze
xxii) sposoby łączenia różnych metod dostępu do pamięci NAS, iSCSI i Fibre Channel z pamięcią masową zdefiniowaną programowo
xxiii) magazyny danych i sposoby implementacji
xxiv) omówienie sposobów aktualizacji oprogramowania

k) instalacja, konfiguracja i zarządzanie modułem oprogramowania do automatyzacji zadań w ramach środowiska zwirtualizowanego, w tym ćwiczenia praktyczne z poniższej tematyki:
i) omówienie procesu uruchamiania,
ii) omówienie funkcjonalności i możliwości wykorzystania oprogramowania,
iii) szczegółowa prezentacja architektury,
iv) rodzaje funkcjonalności i przypadki ich użycia,
v) omówienie kluczowych funkcji i zalet stosowania,
vi) identyfikacja funkcji i zalet automatyzacji zadań/orkiestracji,
vii) konfiguracja oprogramowania i wymagane składniki sieciowe do pracy,
viii) konfiguracja i zarządzanie portalem typu „Self-Service" do tworzenia i uruchamiania maszyn wirtualnych i całych zestawów/systemów maszyn wirtualnych,
ix) omówienie interfejsu graficznego i jego możliwości i funkcji,
x) omówienie ról użytkowników dostępnych w oprogramowaniu,
xi) omówienie integracji z modułem oprogramowania do wirtualizacji sieci,
xii) wykorzystanie komponentów z modułu oprogramowania do wirtualizacji sieci do zaprojektowania wielowarstwowego szablonu chmury aplikacyjnej,
xiii) tworzenie oraz zarządzanie sieciami i grupami zabezpieczeń na żądanie,
xiv) wdrożenie w ramach katalogu usług informacji o kosztach danej usługi,
xv) modyfikację wirtualnego sprzętu przypisanego do obiektu po jego wdrożeniu ("provisioningu"),
xvi) definiowanie logicznych obiektów zawierających wiele wirtualnych elementów w tym wiele maszyn wirtualnych powiązanych ze sobą zależnościami,
xvii) rezerwacja zasobów fizycznych przez użytkowników,
xviii) tworzenia wielu logicznych, izolowanych od siebie grup maszyn wirtualnych z określanymi dla nich zasobami fizycznymi, grupami użytkowników oraz wzorcami usług,
xix) integracja z innymi systemami zewnętrznymi typu DNS, IPAM, Load Balancer, Puppet, Chef, SaltStack,
xx) projektowania usługi opartej na systemie operacyjnym, aplikacjach, usługach sieciowych (tj. Load Balancing, Routing, Switching oraz tworzenia reguł bezpieczeństwa podczas wdrożenia ("provisioningu")),
xxi) omówienie zaawansowanych przypadków użycia.

l) instalacja, konfiguracja i zarządzanie modułem oprogramowania do monitorowania i zarządzania platformą wirtualizacyjną, w tym ćwiczenia praktyczne z poniższej tematyki:
i) omówienie procesu uruchamiania,

ii) omówienie funkcjonalności i możliwości wykorzystania oprogramowania,
iii) szczegółowa prezentacja architektury,
iv) rodzaje funkcjonalności i przypadki ich użycia,
v) omówienie kluczowych funkcji i zalet stosowania,
vi) konfiguracja oprogramowania i wymagane składniki sieciowe do pracy,
vii) monitorowanie stanu całego systemu opartego o dostarczone oprogramowanie do wirtualizacji,
viii) konfiguracja użytkowników i grup użytkowników w celu kontrolowanego dostępu do modułu,
ix) omówienie interfejsu graficznego jego możliwości i funkcji,
x) tworzenie własnych definicji alertów, raportów i widoków,
xi) przedstawienie modeli planowania pojemności,
xii) ocena ogólnej pojemności centrum danych i określenie zaleceń optymalizacyjnych,
xiii) omówienie scenariuszy typu "co-jeśli",
xiv) optymalizacji wydajności i kalkulacja kosztów,
xv) planowanie wydajności, modele planowania wydajności,
xvi) planowanie pojemności centrum danych,
xvii) raportowanie wyników potencjału optymalizacyjnego,
xviii) przewidywanie trendów pojemnościowych i zasobowych,
xix) konfiguracja głównych metryk,
xx) automatyzacja procesu optymalizacji i równoważenia obciążeń,
xxi) metodyka sposobów rozwiązywania problemów poprzez monitorowanie alertów,
xxii) wykorzystanie przepływów pracy krok po kroku do rozwiązywania problemów z różnymi modułami oprogramowania wirtualizacyjnego,
xxiii) konfiguracja monitorowania aplikacji,
xxiv) tworzenie zaleceń, akcji i powiadomień,
xxv) tworzenie definicji alertów, które monitorują zapotrzebowanie na zasoby w serwerach i maszynach wirtualnych,
xxvi) tworzenie i wykorzystywanie w środowisku widoków niestandardowych,
xxvii) diagnostyka środowiska za pomocą pulpitów nawigacyjnych,
xxviii) tworzenie pulpitów nawigacyjnych z wykorzystaniem widżetów predefiniowanych i niestandardowych,
xxix) zarządzanie konfiguracjami i rozwiązywanie problemów,
xxx) sposoby rozwiązywania problemów poprzez monitorowanie alertów,
xxxi) monitorowanie systemu operacyjnego i aplikacji.

m) instalacja, konfiguracja i zarządzanie modułem oprogramowania do centralnego zbierania logów, w tym ćwiczenia praktyczne z poniższej tematyki:
i) omówienie procesu uruchamiania,
ii) omówienie funkcjonalności i możliwości wykorzystania oprogramowania,
iii) szczegółowa prezentacja architektury,
iv) rodzaje funkcjonalności i przypadki ich użycia,
v) omówienie kluczowych funkcji i zalet stosowania,
vi) konfiguracja oprogramowania i wymagane składniki sieciowe do pracy,
vii) omówienie interfejsu graficznego i jego możliwości i funkcji,
viii) omówienie efektywnego zarządzania logami,
ix) personalizacja i wizualizacja logów w postaci wykresów,
x) korelacja wybranych zdarzeń w infrastrukturze fizycznej/wirtualnej oraz ich graficzna prezentacja,
xi) przeszukiwanie logów w oparciu o zdefiniowane przez użytkownika kryteria,

xii) konfiguracja czasu retencji danych,
xiii) konfiguracja powiadomień systemowych,
xiv) zbieranie logów z zewnętrznych systemów,
xv) zarządzanie dostępem do logów dla użytkowników oraz grup użytkowników.

n) instalacja, konfiguracja i zarządzanie modułem oprogramowania do wirtualizacji mocy obliczeniowej akceleratorów graficznych, w tym ćwiczenia praktyczne z poniższej tematyki:
   i) omówienie procesu uruchamiania,
   ii) omówienie funkcjonalności i możliwości wykorzystania oprogramowania,
   iii) szczegółowa prezentacja architektury,
   iv) rodzaje funkcjonalności i przypadki ich użycia,
   v) omówienie kluczowych funkcji i zalet stosowania,
   vi) konfiguracja oprogramowania i wymagane składniki sieciowe do pracy,
   vii) omówienie interfejsu graficznego i jego możliwości i funkcji,
   viii) tworzenie puli dostępnych zasobów GPU dla aplikacji pracujących na maszynach wirtualnych,
   ix) instalacja klienta na stacji końcowej,
   x) przydzielanie/pobieranie zasobów GPU w sposób dynamiczny.
o) instalacja, konfiguracja i zarządzanie modułem oprogramowania dostarczającym zintegrowaną platformę Kubernetes, w tym ćwiczenia praktyczne z poniższej tematyki:
   i) omówienie procesu uruchamiania,
   ii) omówienie funkcjonalności i możliwości wykorzystania oprogramowania,
   iii) szczegółowa prezentacja architektury,
   iv) rodzaje funkcjonalności i przypadki ich użycia,
   v) omówienie kluczowych funkcji i zalet stosowania,
   vi) konfiguracja oprogramowania i wymagane składniki sieciowe do pracy,
   vii) omówienie interfejsu graficznego jego możliwości i funkcji,
   viii) omówienie architektury klastrów Kubernetes i zarządzania obrazami, prezentacja przypadków implementacji,
   ix) omówienie najważniejszych obiektów platformy Kubernetes,
   x) omówienie wymagań dotyczących sieci opartych o moduł oprogramowania do wirtualizacji sieci,
   xi) omówienie topologii sieci,
   xii) tworzenie i zarządzanie przestrzeniami nazw,
   xiii) konfiguracja i zarządzanie limitami,
   xiv) wdrażanie i uruchamianie aplikacji na platformie Kubernetes,
   xv) skalowanie klastra Kubernetes,
   xvi) tworzenie trwałego wolumenu,
   xvii) omówienie zasad przechowywania maszyn wirtualnych i trwałych wolumenów,
   xviii) omówienie repozytorium obrazów kontenerów i integracji z nim platformy,
   xix) omówienie integracji z pozostałymi dostarczonymi modułami oprogramowania,
   xx) współdzielenie wolumenu pomiędzy pod-ami,
   xxi) zarządzanie uprawnieniami (RBAC).
p) instalacja, konfiguracja i zarządzanie oprogramowanie do wirtualizacji stacji roboczych, w tym ćwiczenia praktyczne z poniższej tematyki:
   i) zapoznanie się z możliwościami i zaletami oprogramowania
   ii) użycie narzędzia do tworzenia maszyn wirtualnych używanych jako wirtualne stacje robocze
   iii) tworzenie i optymizowanie planowanych do wykorzystania w projekcie przez Zamawiającego maszyn z MS Windows dla wirtualnych stacji roboczych
   iv) instalacja i konfiguracja agenta w wirtualnych stacjach roboczych

v) konfiguracja i zarządzanie systemami z zainstalowanym agentem i łączenie klienta z serwerami
vi) przegląd typów wirtualnych stacji roboczych
vii) tworzenie, konfiguracja, zarządzanie i przypisywanie pul wirtualnych stacji roboczych opartych o różne typy wirtualnych stacji roboczych
viii) tworzenie i wykorzystywanie desktopów Remote Desktop Services (RDS) oraz pul aplikacji
ix) przegląd narzędzi do monitorowania środowiskiem wirtualnych stacji roboczych
x) określenie wymagań, architektury i prowadzenie instalacji głównego komponentu, który łączy użytkownika z pulpitem lub aplikacją jakim jest Serwer
xi) omówienie opcji autoryzacji i certyfikacji dla środowiska wirtualnych stacji roboczych
xii) możliwości integracji i zapoznanie z procesem integracji
xiii) omówienie opcji wydajności i skalowalności, dostępnych w środowisku wirtualnych stacji roboczych
xiv) omówienie bezpieczeństwa w środowisku wirtualnych stacji roboczych

q) instalacja, konfiguracja i zarządzanie urządzeniami sieciowymi:
i) omówienie architektury w tym w szczególności architektury „leaf-spine”,
ii) omówienie topologii połączeń między przełącznikami,
iii) omówienie metod zarządzania przełącznikami, w tym interfejsu CLI,
iv) omówienie kluczowych aspektów i zalet architektury „leaf-spine”,
v) omówienie, konfiguracja i zarządzanie przełącznikami w architekturze „leaf-spine” na poziomie warstwy IP,
vi) omówienie, konfiguracja i zarządzanie trybem wysokiej dostępności przełączników (ang. HA),
vii) wykonanie praktycznych ćwiczeń laboratoryjnych z rozwiązywania problemów, przypadków awarii oraz metodologia rozwiązywania problemów,
viii) sposoby monitorowania przełączników,
ix) diagnozowanie problemów i awarii,
x) aktualizacja oprogramowania,
xi) bieżące prace administracyjne na przełącznikach,
xii) omówienie architektury systemów zdalnego dostępu,
xiii) omówienie konfiguracji i zarządzania systemami zdalnego dostępu,
xiv) diagnozowanie problemów i awarii w systemach zdalnego dostępu.

r) pozostałe
i) koncepcja działania Systemu:
(1) źródła danych i typy obiektów w Systemie,
(2) użyte protokoły i interfejsy dostępu oraz ich konfiguracja,
(3) systemy klienckie,
(4) przepływ danych w poszczególnych warstwach,
(5) zabezpieczenie danych w kolejnych warstwach.
ii) procesy archiwizacyjne:
(1) omówienie procesu archiwizacji i przywracania danych w zależności od źródła danych, użytych protokołów i interfejsów,
(2) omówienie automatycznych i półautomatycznych procesów archiwizacji danych,
(3) omówienie bieżących zadań dla administratorów,
(4) omówienie zadań z perspektywy poszczególnych konsol zarządzających,
(5) omówienie polityk sterujących przenoszeniem danych pomiędzy warstwami,
(6) tworzenie i modyfikacja polityk.
iii) utrzymanie i konserwacja Systemu:
(1) procedura całkowitego wyłączenia Systemu i jej wpływ na systemy produkcyjne,

(2) przywracanie Systemu po awarii – omówienie scenariuszy,
(3) weryfikacja poprawności pracy Systemu,
(4) analiza obciążenia Systemu,
(5) analiza zajętości Systemu, obowiązki administratorów w codziennym utrzymaniu Systemu,
(6) integracja z zewnętrznymi systemami monitorowania.

iv) rozwiązywanie problemów:
(1) sposoby poszukiwania przyczyn problemów w komunikacji sieciowej
(2) praktyczne ćwiczenia zapewniające pozyskanie zaawansowanej wiedzy i umiejętności w zakresie monitorowania, diagnostyki i rozwiązywania problemów

v) rozwój i planowanie zmian:
(1) omówienie skalowalności Systemu,
(2) omówienie zakresu elastyczności w poszczególnych punktach Systemu,
(3) przedstawienie dobrych praktyk w zakresie rozbudowy Systemu i zmian w Oprogramowaniu,
(4) omówienie wsparcia dla procesu wymiany technologii (technology refresh).

vi) gwarancja i utrzymanie:
(1) przedstawienie obowiązków Wykonawcy,
(2) omówienie procesu zgłaszania problemów.

12) Szczegółowy zakres instruktaży zawiera obszary, które muszą zostać zawarte w trakcie instruktażu, jednakże Zamawiający dopuszcza ich modyfikację przez Wykonawcę po uzgodnieniu tego z Zamawiającym i uzyskaniu od niego akceptacji zmiany zakresu.

19.3. Czas trwania

Zamawiający wymaga przeprowadzenia instruktażu w wymiarze 18 dni roboczych (gdzie jeden dzień roboczy rozumiany jest jako 8 godzin) obejmującego zakres przedstawiony w punkcie **19.2**. Szczegółowy zakres i harmonogram Zamawiający ustali z Wykonawcą w toku prac wdrożeniowych.

20. Instruktaż dla Zadania nr 2

20.1. Wstęp

W ramach realizacji przedmiotu zamówienia Wykonawca jest zobowiązany do przeprowadzenia instruktaży zgodnie z przedstawionymi poniżej wymaganiami Zamawiającego. Instruktaże muszą być przeznaczone dla grupy administratorów – osób odpowiedzialnych za nadzór, utrzymanie oraz prace operacyjne (przeprowadzanie zmian i konfiguracji Systemu), a także monitorowanie elementów Systemu.

20.2. Zbiór wymagań dla instruktaży

1) Wykonawca zapewni materiały instruktażowe w języku polskim lub angielskim dla wszystkich uczestników instruktaży (prezentacje, książki/podręczniki, ćwiczenia).
2) Maksymalna liczba osób w danej grupie nie przekroczy 15 osób.
3) Wykonawca przeprowadzi instruktaże w formule praktycznych zadań, istnieje możliwość przeprowadzenia ich na dostarczonym i wdrożonym środowisku będącym przedmiotem tego postępowania. Nie może dojść do sytuacji, że wdrożone środowisko po przeprowadzeniu instruktażu będzie niefunkcjonalne.
4) Instruktaże muszą obejmować zakres merytoryczny dotyczący obsługi funkcjonalności wymaganych przez Zamawiającego w ramach wdrożonego Systemu.
5) Instruktaże muszą być przeprowadzone przez instruktorów posiadających certyfikaty poświadczające ich wiedzę, wydane przez producenta/producentów dostarczonego Systemu lub poszczególnych Komponentów/modułów tego Systemu.
6) Instruktaż musi być przeprowadzony stacjonarnie w siedzibie Zamawiającego w języku polskim. Zamawiający zastrzega sobie prawo do zmiany formy instruktarzu z trybu stacjonarnego na tryb zdalny (przez system wideokonferencyjny zapewniony przez Wykonawcę).
7) Nie dopuszcza się instruktażu w formie szkolenia typu „e-learning”.
8) Termin instruktażu musi zostać ustalony z Zamawiającym.
9) Zakres poszczególnych instruktaży musi być uzgadniany i zaakceptowany przez Zamawiającego.
10) W każdym instruktarzu należy uwzględnić czas na pytania od uczestników.
11) Szczegółowy zakres merytoryczny instruktaży:
    a) instruktaż wstępny:
        i) omówienie architektury Systemu, w tym na podstawie dokumentacji wykonawczej m.in.
            (1) architektury serwerów
            (2) architektury platformy wirtualizacyjnej wraz z wszystkimi jej modułami
            (3) architektury macierzy blokowej i systemu pamięci masowej
            (4) architektury urządzeń sieciowych
            (5) architektury wdrożonego systemu wirtualizacyjnego
            (6) architektury systemu kopii zapasowych
            (7) podstawowej funkcjonalności wdrożonego systemu wirtualizacyjnego w szczególności w zakresie:
                (a) tworzenie alertów, raportów i widoków
                (b) omówienie procesów tworzenia i odzyskiwania kopii zapasowej
                (c) omówienie procesu odzyskania środowisk po awarii

(d) aspekty związane z monitorowaniem infrastruktury Systemu
(e) aspekty związane z platformą wirtualizacyjną wraz z wszystkimi jej modułami
(f) aspekty związane z zarządzaniem wirtualizacją zasobów obliczeniowych
(g) aspektów związanych z macierzami blokowymi i systemami pamięci masowej
(h) aspektów związanych z urządzeniami sieciowymi

ii) techniczne omówienie architektury wdrożonego Systemu
iii) zarządzanie infrastrukturą serwerów fizycznych i zwirtualizowanych
iv) zarządzanie platformą wirtualizacji obejmującą wszystkie jej moduły dostarczone w ramach postępowania
v) omówienie i zarządzanie procesami tworzenia i odzyskiwania kopii zapasowej
vi) omówienie i zarządzanie procesami odzyskania środowisk po awarii
vii) omówienie i zarządzanie macierzą blokową oraz systemami pamięci masowej
viii) zarządzanie monitorowaniem warstwy wirtualizacji wraz z serwerami fizycznymi
ix) aspekty związane z zarządzaniem oprogramowaniem monitorującym wirtualizację
x) zarządzanie użytkownikami, rolami, poziomami dostępu.

b) instalacja, konfiguracja i zarządzanie serwerami:
i) proces instalacji, konfiguracji, zarządzania serwerem,
ii) proces aktualizacji oprogramowania Komponentów serwerów,
iii) proces aktualizacji oprogramowania zainstalowanego na serwerach,
iv) omówienie funkcjonalności systemu do zarządzania serwerem.

c) implementacja i zarządzanie macierzą blokową, w tym ćwiczenia praktyczne z poniższej tematyki:
i) omówienie architektury macierzy blokowej,
ii) omówienie elementów składowych macierzy blokowej (sprzętowe i programowe składniki),
iii) omówienie konfiguracji macierzy blokowej,
iv) omówienie konfiguracji pod kątem odporności na awarie oraz wydajności,
v) omówienie protokołów dostępu i ich konfiguracji,
vi) kopie migawkowe,
vii) „tiering" bloków danych pomiędzy dyskami,
viii) wymagania pracy całkowicie bez przestojów z zapewnieniem najwyższego poziomu trwałości danych,
ix) redukcja danych (deduplikacja),
x) naprawa po awarii sprzętowej,
xi) hot-spare lub przestrzeń nadmiarowa,
xii) zabezpieczenie danych przed złośliwym oprogramowaniem szyfrującym,
xiii) gwarancja niezmienności danych,
xiv) stosowanie wielu protokołów dostępu działających jednocześnie,
xv) mechanizmy ochrony danych (synchronizacje, replikacje w wielu różnych topologiach) pomiędzy lokalizacjami i ich zastosowanie,
xvi) sposoby monitorowania macierzy blokowej,
xvii) diagnozowanie problemów i awarii,
xviii) punkty zarządzania macierzą blokową,
xix) aktualizacja oprogramowania.

d) implementacja i zarządzanie systemem szybkiej pamięci masowej o dostępie plikowym, w tym ćwiczenia praktyczne z poniższej tematyki:
i) omówienie architektury systemu,

ii) omówienie elementów składowych systemu (sprzętowe i programowe składniki systemu),
iii) niezmienność przechowywanych danych w wielu kopiach (sumy kontrolne, technologia WORM, retencja),
iv) sposób/oby przechowywania nieusystematyzowanych danych m.in. dane multimedialne (zdjęcia, filmy),
v) sposób/oby przechowywania danych analitycznych,
vi) repozytoria danych na potrzeby klastrów obliczeniowych,
vii) sposoby efektywnego przetwarzania metadanych (dane opisujące przechowywane obiekty),
viii) omówienie protokołów dostępu, m.in. NFS, CIFS, HTTP, S3 i konfiguracji,
ix) omówienie i konfiguracja HDFS,
x) dostępne scenariusze replikacji danych między węzłami/kontrolerami,
xi) elastyczne mechanizmy ochrony danych, mirroring i kody korekcyjne,
xii) wymagania pracy całkowicie bez przestojów z zapewnieniem najwyższego poziomu trwałości danych,
xiii) naprawa po awarii sprzętowej,
xiv) skalowalność i rozbudowa systemu,
xv) sposoby zapewniania należytej wydajności całego systemu odpowiednio do wzrostu pojemności i wymagań na przepustowość,
xvi) retencja i ochrona danych WORM,
xvii) zapewnienie gwarancji niezmienności danych i ochrona przed ich skasowaniem,
xviii) omówienie funkcjonalności trwałego nośnika zwanego WORM i ustawianie czasu retencji danych i metadanych z gwarancją, że przed upływem tego czasu nie zostaną one usunięte,
xix) zabezpieczenie danych przed złośliwym oprogramowaniem szyfrującym,
xx) gwarancja niezmienności danych,
xxi) stosowanie wielu protokołów dostępu działających jednocześnie,
xxii) mechanizmy ochrony danych (synchronizacje, replikacje w wielu różnych topologiach) pomiędzy lokalizacjami i ich zastosowanie,
xxiii) sposoby monitorowania systemu,
xxiv) diagnozowanie problemów i awarii,
xxv) punkty zarządzania systemem,
xxvi) aktualizacja oprogramowania.

e) implementacja i zarządzanie systemem archiwalnej pamięci masowej o dostępie plikowym, w tym ćwiczenia praktyczne z poniższej tematyki:
i) omówienie architektury systemu,
ii) omówienie elementów składowych systemu (sprzętowe i programowe składniki systemu),
iii) niezmienność przechowywanych danych w wielu kopiach (sumy kontrolne, technologia WORM, retencja),
iv) sposób/oby przechowywania nieusystematyzowanych danych m.in. dane multimedialne (zdjęcia, filmy),
v) sposób/oby przechowywania danych analitycznych,
vi) repozytoria danych na potrzeby klastrów obliczeniowych,
vii) sposoby efektywnego przetwarzania metadanych (dane opisujące przechowywane obiekty),

viii) omówienie protokołów dostępu, m.in. NFS, CIFS, HTTP, S3 i konfiguracji,
ix) omówienie i konfiguracja HDFS,
x) omówienie dostępnych scenariuszy replikacji danych między węzłami/kontrolerami,
xi) elastyczne mechanizmy ochrony danych, mirroring i kody korekcyjne,
xii) wymagania pracy całkowicie bez przestojów z zapewnieniem najwyższego poziomu trwałości danych,
xiii) naprawa po awarii sprzętowej,
xiv) skalowalność i rozbudowa systemu,
xv) sposoby zapewniania należytej wydajności całego systemu odpowiednio do wzrostu pojemności i wymagań na przepustowość,
xvi) retencja i ochrona danych WORM,
xvii) zapewnienie gwarancji niezmienności danych i ochrona przed ich skasowaniem,
xviii) omówienie funkcjonalności trwałego nośnika zwanego WORM i ustawianie czasu retencji danych i metadanych z gwarancją, że przed upływem tego czasu nie zostaną one usunięte,
xix) zabezpieczenie danych przed złośliwym oprogramowaniem szyfrującym,
xx) gwarancja niezmienności danych,
xxi) stosowanie wielu protokołów dostępu działających jednocześnie, xxii)mechanizmy ochrony danych (synchronizacje, replikacje w wielu różnych topologiach) pomiędzy lokalizacjami i ich zastosowanie,
xxiii) sposoby monitorowania systemu,
xxiv) diagnozowanie problemów i awarii,
xxv) punkty zarządzania systemem,

f) implementacja i zarządzanie komponentem do wykonywania kopii zapasowych (oprogramowanie do wykonywania kopii zapasowych, medium backupowe), w tym ćwiczenia praktyczne z poniższej tematyki:
i) omówienie funkcjonalności oprogramowania i zapoznanie z interfejsem,
ii) omówienie mediów backupowych do przechowywania kopii zapasowych,
iii) medium backupowe do przechowywania kopii zapasowych – konfiguracja, utrzymanie, monitorowanie, optymalizacja, dobre praktyki,
iv) omówienie zarządzania danymi archiwalnymi w środowiskach wirtualnych,
v) omówienie zagadnień obejmujących cel i czas odzyskiwania (RTO) i (RPO),
vi) omówienie metod konfiguracji zapewniających skuteczną ochronę danych i maksymalizację wydajności procesora, sieci i pamięci w środowisku zwirtualizowanym,
vii) prowadzenie testów odzyskiwania dla różnych scenariuszy,
viii) omówienie architektury komponentów i relacji między nimi,
ix) sposoby odzyskiwania danych plikowych,
x) omówienie interfejsów raportujących i pulpitów nawigacyjnych do monitorowania wydajności i minimalizacji ryzyka utraty danych,
xi) omówienie metod rozwiązywania problemów i analizy raportów,
xii) omówienie komponentów do tworzenia kopii zapasowych i replikacji,
xiii) omówienie oznaczania lokalizacji przechowywanych danych,
xiv) ustawianie powiadomień globalnych,
xv) omówienie zarządzania połączeniami IP dla przesyłania danych,
xvi) omówienie reguł ruchu sieciowego,
xvii) omówienie procesu wykonywania kopii zapasowych maszyn wirtualnych,

xviii) omówienie metod tworzenia kopii zapasowych,
xix) omówienie optymalizacji wielkości danych,
xx) omówienie dostępnych integracji dla pamięci masowej,
xxi) tworzenie zadań kopiowania maszyn wirtualnych / plików,
xxii) planowanie i tworzenie punktów przywracania,
xxiii) tworzenie kopii zapasowych za pomocą agentów,
xxiv) odzyskiwanie z kopii zapasowej,
xxv) natychmiastowe odzyskiwanie maszyn wirtualnych,
xxvi) omówienie procesu pełnego odzyskiwania maszyn wirtualnych,
xxvii) omówienie procesu odzyskiwania plików wirtualnych maszyn,
xxviii) omówienie procesu odzyskiwania obiektów,
xxix) omówienie odzyskiwania elementu z wspieranych aplikacji i baz danych,
xxx) omówienie odzyskiwania plików systemu operacyjnego gościa,
xxxi) tworzenie replik,
xxxii) omówienie wglądu w replikację,
xxxiii) omówienie procesu zmniejszenia ilości przesyłanych danych,
xxxiv) odzyskiwanie z repliki,
xxxv) omówienie przełączania awaryjnego,
xxxvi) omówienie powrotu po awarii,
xxxvii) omówienie planu pracy awaryjnej,
xxxviii) omówienie planu przełączeń awaryjnych,
xxxix) tworzenie kopii zapasowych,
xl) omówienie funkcjonalności zadania kopii zapasowej,
xli) omówienie procesu tworzenia kopii zapasowej,
xlii) architektura kopii zapasowych,
xliii) zasady przechowywania archiwum,
xliv) tworzenie kopii zapasowych w archiwum,
xlv) monitorowanie poziomu wydajności i pojemności,
xlvi) automatyczne testowanie odzyskiwania,
xlvii) przywracanie etapowe,
xlviii) omówienie zarządzania użytkownikami i ich prawami dostępu do kopii zapasowych,
xlix) omówienie funkcjonalności uruchamiania kopii zapasowych maszyn wirtualnych bezpośrednio z urządzenia do przechowywania kopii zapasowych bez odtwarzania na jakikolwiek zewnętrzny magazyn danych.

g) instalacja, konfiguracja i zarządzanie modułem oprogramowania do wirtualizacji zasobów serwerowych i ich mocy obliczeniowej oraz modułem oprogramowania do zarządzania klastrem wirtualizacyjnym, w tym ćwiczenia praktyczne z poniższej tematyki:

i) proces instalacji, konfiguracji, zarządzania oprogramowaniem do wirtualizacji zasobów serwerowych i ich mocy obliczeniowej oraz oprogramowaniem do zarządzania klastrem wirtualizacyjnym,
ii) omówienie instalacji oraz konfiguracji i funkcjonalności konsoli graficznej do zarządzania maszynami wirtualnymi,
iii) opcje konfiguracji wirtualizatora i przełącznika sieciowego,
iv) konfiguracja wirtualizatora i przełącznika sieciowego w zakresie migracji maszyn wirtualnych w trakcie pracy, między serwerami,
v) omówienie koncepcji pamięci masowej i stosowania wirtualizacji,

vi) konfiguracja interfejsu zarządzania wirtualizatorem w serwerze, tworzenie magazynów danych,
vii) omówienie mechanizmów rozkładania obciążenia i migracji maszyn wirtualnych i plików maszyn wirtualnych,
viii) konfiguracja automatyzacji migracji maszyn wirtualnych,
ix) omówienie koncepcji i narzędzia do aktualizacji środowiska,
x) wykonanie aktualizacji serwerów,
xi) profilowanie serwerów dla uproszczenia konfiguracji,
xii) konfiguracja wysokiej dostępności wirtualizacji poprzez klastry,
xiii) tworzenie szablonów maszyn wirtualnych i bibliotek scenariuszy,
xiv) tworzenie, modyfikacja, przenoszenie, usuwanie maszyn wirtualnych,
xv) wdrażanie maszyn wirtualnych z szablonów,
xvi) klonowanie maszyn wirtualnych,
xvii) monitorowanie zasobów maszyn wirtualnych,
xviii) konfiguracja przekazywania logów do zewnętrznych systemów np. SIEM,
xix) konfiguracja wysokiej dostępności dla głównej konsoli zarządzającej,
xx) monitoring poprzez konsolę zarządzającą,
xxi) konfiguracja wbudowanego serwera zapory sieciowej w oprogramowaniu do zarządzania klastrem wirtualizacyjnym,
xxii) konfiguracja uwierzytelniania użytkowników logujących się do oprogramowania zarządzającego klastrem wirtualizacyjnym w oparciu o domenę Microsoft Active Directory lub Open LDAP.

h) instalacja, konfiguracja i zarządzanie modułem oprogramowania do wirtualizacji sieci, w tym ćwiczenia praktyczne z poniższej tematyki:
i) sposoby instalacji, konfiguracji i zarządzania modułem oprogramowania do wirtualizacji sieci
ii) wyjaśnienie i omówienie tematyki: logiczne przełączanie, logiczny routing, usługi sieciowe i bezpieczeństwo, mikro-segmentacja, zapory ogniowe i inne komponenty,
iii) wyjaśnienie funkcjonalności, wymagań technicznych i ograniczeń w module oprogramowania do wirtualizacji sieci
iv) przeprowadzenie laboratorium z zakresu praktycznych zadań na temat instalacji, konfiguracji i zarządzania modułem,
v) budowanie architektury sieci zdefiniowanej programowo,
vi) omówienie Komponentów i głównych funkcjonalności,
vii) omówienie kluczowych funkcji i zalet stosowania,
viii) sposoby powoływania środowisk testowych jako kopii środowiska produkcyjnego,
ix) omówienie procesu wdrażania i konfiguracji infrastruktury sieci zdefiniowanej programowo,
x) omówienie wymagań na sieć podkładową,
xi) omówienie metod łączenia sieci zdefiniowanej programowo z siecią podkładową i usługami takimi jak Firewall, LoadBalancer, itp.,
xii) omówienie konfiguracji logicznego przełączania i mostkowania warstwy 2,
xiii) omówienie wielopoziomowej architektury routingu i konfiguracji bramy IP,
xiv) omówienie zaawansowanych usług, takich jak VPN i równoważenie obciążenia, sposoby implementacji,
xv) omówienie bezpieczeństwa usług w sieci programowej poprzez stosowanie mikrosegmentacji, izolacja ruchu L2/VLAN,

xvi) omówienie bezpieczeństwa modeli zapór ogniowych w celu chronienia ruchu wschód-zachód i północ-południe,
xvii) omówienie zaawansowanego wymuszania bezpieczeństwa w połączeniu ze środowiskiem produktów podmiotów trzecich,
xviii) omówienie konfiguracji kontroli dostępu opartej na rolach,
xix) sposoby zabezpieczania usług między centrami danych,
xx) sposoby monitorowania sieci zdefiniowanej programowo,
xxi) diagnostyka problemów z siecią podkładową,
xxii) sposoby aktualizacji oprogramowania.

i) instalacja, konfiguracja i zarządzanie modułem oprogramowania do wirtualizacji mocy obliczeniowej akceleratorów graficznych, w tym ćwiczenia praktyczne z poniższej tematyki:
   i) omówienie procesu uruchamiania,
   ii) omówienie funkcjonalności i możliwości wykorzystania oprogramowania,
   iii) szczegółowa prezentacja architektury,
   iv) rodzaje funkcjonalności i przypadki ich użycia,
   v) omówienie kluczowych funkcji i zalet stosowania,
   vi) konfiguracja oprogramowania i wymagane składniki sieciowe do pracy,
   vii) omówienie interfejsu graficznego i jego możliwości i funkcji,
   viii) tworzenie puli dostępnych zasobów GPU dla aplikacji pracujących na maszynach wirtualnych,
   ix) instalacja klienta na stacji końcowej,
   x) przydzielanie/pobieranie zasobów GPU w sposób dynamiczny.
j) instalacja, konfiguracja i zarządzanie urządzeniami sieciowymi:
   i) omówienie architektury w tym w szczególności architektury „leaf-spine”,
   ii) omówienie topologii połączeń między przełącznikami,
   iii) omówienie metod zarządzania przełącznikami, w tym interfejsu CLI,
   iv) omówienie kluczowych aspektów i zalet architektury „leaf-spine”,
   v) omówienie, konfiguracja i zarządzanie przełącznikami w architekturze „leaf- spine” na poziomie warstwy IP,
   vi) omówienie, konfiguracja i zarządzanie trybem wysokiej dostępności przełączników (ang. HA),
   vii) wykonanie praktycznych ćwiczeń laboratoryjnych z rozwiązywania problemów, przypadków awarii oraz metodologia rozwiązywania problemów,
   viii) sposoby monitorowania przełączników,
   ix) diagnozowanie problemów i awarii,
   x) aktualizacja oprogramowania,
   xi) bieżące prace administracyjne na przełącznikach.
k) instalacja, konfiguracja i zarządzanie Przełącznikiem warstwy trzeciej
   i. System operacyjny Routera
      (1) Oprogramowanie
      (2) Przetwarzanie pakietów
   ii) Zarządzanie
      (1) Interfejsy użytkownika
      (2) CLI
      (3) Konsola graficzna
   iii) Przygotowanie urządzeń do pracy
      (1) Konfiguracja fabryczna

(2) Konfiguracja początkowa
(3) Konfiguracja interfejsów sieciowych

iv) Konfiguracja podstawowych ustawień sieciowych
(1) Konta użytkowników i uwierzytelnianie
(2) Praca z logami i debug
(3) NTP
(4) Zarządzanie plikami konfiguracyjnymi
(5) SNMP

v) Monitorowanie pracy i utrzymanie systemu
(1) Monitorowanie urządzeń i interfejsów
(2) Narzędzia sieciowe
(3) Aktualizowanie systemu operacyjnego
(4) Procedura odzyskiwania hasła

vi) Przykłady konfiguracji interfejsów
(1) Hierarchia interfejsów
(2) Przykłady
(3) Używanie grup konfiguracji

vii) Interfejs graficzny
(1) GUI
(2) Konfiguracja w interfejsie graficznym

viii) Podstawy routingu
(1) Koncepcja routingu
(2) Routing statyczny
(3) Routing dynamiczny (OSPF)

ix) Polityki routingu i filtrowanie pakietów
(1) Wstęp do polityk routingu
(2) Zastosowanie polityk routingu: redystrybucja
(3) Wstęp do filtrowania pakietów (firewall filters)
(4) Przykład zastosowania filtrów ruchu
(5) Zabezpieczenia antyspoofingowe: Unicast RPF

x) Class of Service
(1) Wstęp do zagadnień zapewniania odpowiedniego poziomu obsługi ruchu
(2) Klasyfikacja ruchu
(3) Kolejkowanie
(4) Szeregowanie ruchu (scheduling)
(5) Przykład zastosowania mechanizmów CoS

l) instalacja, konfiguracja i zarządzanie oprogramowanie do wirtualizacji desktopów, w tym ćwiczenia praktyczne z poniższej tematyki:
i) zapoznanie się z możliwościami i zaletami oprogramowania
ii) użycie narzędzia do tworzenia maszyn wirtualnych używanych jako wirtualne stacje robocze
iii) tworzenie i optymizowanie planowanych do wykorzystania w projekcie przez Zamawiającego maszyn z MS Windows dla wirtualnych stacji roboczych
iv) instalacja i konfiguracja agenta w wirtualnych stacjach roboczych
v) konfiguracja i zarządzanie systemami z zainstalowanym agentem i łączenie klienta z serwerami
vi) przegląd typów wirtualnych stacji roboczych
vii) tworzenie, konfiguracja, zarządzanie i przypisywanie pul wirtualnych stacji

roboczych opartych o różne typy wirtualnych stacji roboczych

viii) tworzenie i wykorzystywanie desktopów Remote Desktop Services (RDS) oraz pul aplikacji

ix) przegląd narzędzi do monitorowania środowiskiem wirtualnych stacji roboczych

x) określenie wymagań, architektury i prowadzenie instalacji głównego komponentu, który łączy użytkownika z pulpitem lub aplikacją jakim jest Serwer

xi) omówienie opcji autoryzacji i certyfikacji dla środowiska wirtualnych stacji roboczych

xii) możliwości integracji i zapoznanie z procesem integracji

xiii) omówienie opcji wydajności i skalowalności, dostępnych w środowisku wirtualnych stacji roboczych

xiv) omówienie bezpieczeństwa w środowisku wirtualnych stacji roboczych

xv) omówienie bezpieczeństwa w środowisku wirtualnych desktopów

m) pozostałe

i) koncepcja działania Systemu:

(1) źródła danych i typy obiektów w Systemie,

(2) użyte protokoły i interfejsy dostępu oraz ich konfiguracja,

(3) systemy klienckie,

(4) przepływ danych w poszczególnych warstwach,

(5) zabezpieczenie danych w kolejnych warstwach.

ii) procesy archiwizacyjne:

(1) omówienie procesu archiwizacji i przywracania danych w zależności od źródła danych, użytych protokołów i interfejsów,

(2) omówienie automatycznych i półautomatycznych procesów archiwizacji danych,

(3) omówienie bieżących zadań dla administratorów,

(4) omówienie zadań z perspektywy poszczególnych konsol zarządzających,

(5) omówienie polityk sterujących przenoszeniem danych pomiędzy warstwami,

(6) tworzenie i modyfikacja polityk.

iii) utrzymanie i konserwacja Systemu:

(1) procedura całkowitego wyłączenia Systemu i jej wpływ na systemy produkcyjne,

(2) przywracanie Systemu po awarii – omówienie scenariuszy,

(3) weryfikacja poprawności pracy Systemu,

(4) analiza obciążenia Systemu,

(5) analiza zajętości Systemu, obowiązki administratorów w codziennym utrzymaniu Systemu,

(6) integracja z zewnętrznymi systemami monitorowania.

iv) rozwiązywanie problemów:

(1) sposoby poszukiwania przyczyn problemów w komunikacji sieciowej

(2) praktyczne ćwiczenia zapewniające pozyskanie zaawansowanej wiedzy i umiejętności w zakresie monitorowania, diagnostyki i rozwiązywania problemów

v) rozwój i planowanie zmian:

(1) omówienie skalowalności Systemu,

(2) omówienie zakresu elastyczności w poszczególnych punktach Systemu,

(3) przedstawienie dobrych praktyk w zakresie rozbudowy Systemu i zmian w Oprogramowaniu,

(4) omówienie wsparcia dla procesu wymiany technologii (technology refresh).

vi) gwarancja i utrzymanie:

(1) przedstawienie obowiązków Wykonawcy,
(2) omówienie procesu zgłaszania problemów.

12) Szczegółowy zakres instruktaży zawiera obszary, które muszą zostać zawarte w trakcie instruktażu, jednakże Zamawiający dopuszcza ich modyfikację przez Wykonawcę po uzgodnieniu tego z Zamawiającym i uzyskaniu od niego akceptacji zmiany zakresu.

20.3. Czas trwania

Zamawiający wymaga przeprowadzenia instruktażu w wymiarze 18 dni roboczych (gdzie jeden dzień roboczy rozumiany jest jako 8 godzin) obejmującego zakres przedstawiony w punkcie 20.2. Szczegółowy zakres i harmonogram Zamawiający ustali z Wykonawcą w toku prac wdrożeniowych.

21. Gwarancja

21.1. Ogólne warunki Gwarancji

1) Wykonawca zobowiązuje się do udzielenia gwarancji na dostarczone urządzenia, oprogramowanie oraz wykonane prace i zobowiązuje się do wykonywania świadczeń gwarancyjnych zgodnie z poniższymi warunkami.
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 **21.2.15.**
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 w ramach realizacji przedmiotu zamówienia, 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.
5) Wykonywanie praw wynikających z udzielonej gwarancji nie wyłącza wykonywania uprawnień Zamawiającego wynikających z rękojmi za wady urządzeń i/lub oprogramowania. Zamawiający jest uprawniony do wykonywania uprawnień wynikających z rękojmi na warunkach analogicznych jak realizacja uprawnień Zamawiającego wynikających z gwarancji.
6) W ramach gwarancji Wykonawca zobowiązany jest do:
    a) diagnostyki i rozwiązywania problemów zgłaszanych przez Zamawiającego,
    b) wsparcia w zakresie dostarczonego oprogramowania poprzez zapewnienie:
        i. dostępu do poprawek (aktualizacji) oprogramowania, w szczególności poprzez udostępnienie odpowiednich haseł, kodów, itp. narzędzi do systemów serwisowych producentów lub dostawców,
        ii. zapewnienie dostępu do najnowszych komercyjnie dostępnych wersji oprogramowania wraz z zapewnieniem niezbędnych licencji na warunkach nie gorszych niż wynikających z SWZ, i to bez dodatkowych kosztów dla Zamawiającego, w szczególności poprzez udostępnienie odpowiednich haseł, kodów, itp. narzędzi do systemów serwisowych producentów lub dostawców,
    c) udzielania konsultacji dotyczących instalacji, funkcjonowania i aktualizacji Systemu,
    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 Komponentów 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 Komponentu 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 niewyłączających sprzedaży na rynku polskim zapewniających w szczególności realizację uprawnień gwarancyjnych,
n) W przypadku, gdy Wykonawca podczas realizacji usług gwarancyjnych dostarczy nową fabrycznie część Komponentu, 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.

21.2. Opis usługi Gwarancji

21.2.1. Diagnostyka i rozwiązywanie problemów

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

21.2.2. 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. W szczególności możliwe są problemy z bezpieczeństwem, naruszenia zgodności, straty i szkody dla reputacji. Spełniona zostaje co najmniej 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,
5) brak możliwości realizacji usług.

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

1) brak możliwości zarządzania elementami Systemu,
2) wydajność lub pojemność Systemu uległa obniżeniu, o co najmniej 20% w stosunku do wartości dostarczonej.

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 co najmniej 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.

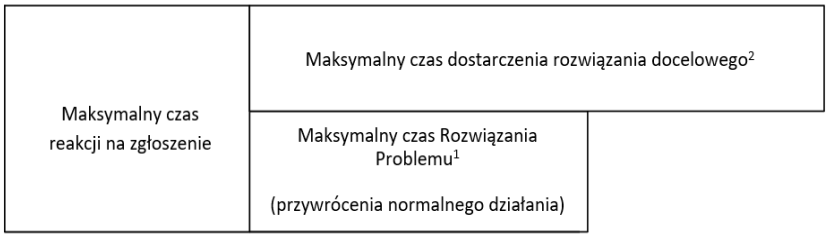
Usterka – pozostałe Problemy.

21.2.3. 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] (przywrócenia normalnego	Maksymalny czas dostarczenia rozwiązania docelowego[2]	Tryb Serwisowania (godzin na dobę

		działania Systemu)		x liczbę dni w tygodniu)
Awaria Krytyczna	8 godzin	8 godzin	10 dni roboczych	24x7
Awaria Poważna	24 godziny	8 godzin	20 dni roboczych	24x7
Awaria Istotna	24 godziny	16 godzin	80 dni roboczych	8x5[3]
Usterka	24 godziny	40 godzin	100 dni roboczych	8x5[3]



Powyższy diagram przedstawia zależność poszczególnych czasów obsługi zgłoszenia – czas rozwiązania problemu i/lub czas na dostarczenie rozwiązania docelowego nalicza się od momentu zakończenia czasu reakcji na zgłoszenie.

[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

21.2.4. 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 dostępów do systemu zgłoszeń problemowych Wykonawcy zostaną przekazane Zamawiającemu w trybie roboczym.
7) Strony, w trakcie trwania usługi gwarancji, mogą umówić się na integracje między systemami zgłoszeń problemowych Wykonawcy i Zamawiającego. Szczegóły zostaną uzgodnione w trybie roboczym.

21.2.5. Zgłaszanie problemów

1) Zamawiający jest odpowiedzialny za przekazanie w zgłoszeniu problemu kompletu znanych mu 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.

21.2.6. Czas reakcji

1) Oznacza czas, który upłynie od wysłania 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.

21.2.7. 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.

21.2.8. 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 odwiesza zgłoszenie problemu i czas rozwiązania problemu jest kontynuowany o czas oczekiwania na dostęp do urządzeń.
5) Jeżeli Wykonawca uchybi terminowi rozwiązania problemu, wskazanemu w punkcie **21.2.3**, z przyczyn leżących po jego stronie, Zamawiający będzie miał prawo do rozwiązania problemu samodzielnie lub poprzez zlecenie innemu podmiotowi przez siebie wybranemu. Takie zastępcze rozwiązanie problemu jest dokonywane na koszt i ryzyko Wykonawcy

21.2.9. Przywrócenie systemu

1) Rozwiązanie problemu polega na przywróceniu normalnego funkcjonowania Systemu za pomocą rozwiązania docelowego.
2) W ramach tymczasowego rozwiązywania Problemu, Wykonawca może zaproponować Zamawiającemu Przywrócenie Systemu poprzez wykorzystanie Obejścia. W takim wypadku maksymalny czas dostarczenia rozwiązania docelowego wydłuża się do czasu wskazanego w kolumnie 4 tabeli zamieszczonej w punkcie **21.2.3**
3) Wykonawca informuje Zamawiającego o stanie prac mających na celu Przywrócenie Systemu.
4) Przywrócenie Systemu z wykorzystaniem Obejścia nie zwalnia Wykonawcy z obowiązku Rozwiązania Problemu, zgodnie z czasami określonymi w niniejszym Załączniku.
5) W przypadku wystąpienia Problemu z Oprogramowaniem, Wykonawca będzie współpracował z producentem Oprogramowania w celu Rozwiązania Problemu.
6) Przywrócenie Systemu zostaje uznane za skuteczne w przypadku, gdy Wykonawca zgłosi Zamawiającemu fakt Przywrócenia Systemu, a Zamawiający ten fakt potwierdzi.

21.2.10. 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 odwiesza 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 **21.2.3**.

21.2.11. 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 **21.2.4**, 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.

21.2.12. 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 w rozumieniu zapisów punktu **0**,
   b) osoby świadczące pomoc techniczną po stronie Wykonawcy muszą posiadać odpowiednią wiedzę fachową 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

21.2.13. 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). Dostęp do uaktualnienia musi być zapewniony bez dodatkowych opłat i 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 Komponentu.
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

21.2.14. Szczegółowe wymagania gwarancji dotyczące elementów Systemu, z wyłączeniem stacji zarządzania, mobilnego urządzenia monitorującego oraz systemu dostępowego typu D.

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 wygaśnięcia gwarancji na urządzenie,
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.

21.2.15. Szczegółowe wymagania gwarancji dotyczące stacji zarządzania oraz mobilnego urządzenia monitorującego oraz systemu dostępowego typu D.

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 Typ A – stacja dokująca	1 dzień roboczy od zgłoszenia	Następny dzień roboczy od zgłoszenia jednostka główna, 2 dni robocze od zgłoszenia pozostałe elementy	60 miesięcy
Stacja zarządzania Typ 2: – jednostka główna – monitor – zestaw klawiatura mysz Typ B – stacja dokująca	1 dzień roboczy od zgłoszenia	10 dni roboczych od zgłoszenia jednostka główna i pozostałe elementy, 2 dni robocze od zgłoszenia monitor i stacja dokująca	36 miesięcy jednostka główna 60 miesięcy monitor i stacja dokująca

			12 miesięcy pozostałe elementy
Mobilne urządzenie monitorujące	1 dzień roboczy od zgłoszenia	10 dni roboczych od zgłoszenia	12 miesięcy
System dostępowy typ D3 – urządzenie dostępowe typ D3	1 dzień roboczy od zgłoszenia	10 dni roboczych od zgłoszenia	84 miesięcy
System dostępowy typ D3 – system zarządzający typ D3	1 dzień roboczy od zgłoszenia	10 dni roboczych od zgłoszenia	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.

Wymaganie dotyczące stacji zarządzania Typu 1:

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 (przepięcie) lub usterka zintegrowanego ekranu. W takim wypadku udzielający gwarancji zobowiązuje się do pokrycia pełnych kosztów naprawy, a w przypadku niemożności lub nieopłacalności 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.

Wymaganie dotyczące wszystkich typów stacji zarządzania:

1) prawo do pobieranie uaktualnień oprogramowania układowego oraz sterowników także po wygaśnięcia gwarancji na urządzenie,
2) 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,
3) 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.

Wymaganie dotyczące systemu dostępowego typ D3:

1) Zamawiający wymaga aby przez cały okres gwarancji:
   a) był zapewniony bezpośredni dostęp do wsparcia technicznego producenta,
   b) był zapewniony dostęp poprzez portal producenta do najnowszych wersji oraz poprawek oprogramowania, w tym także oprogramowania układowego (firmware) dla urządzeń dostępowych oraz systemu zarządzania.
   c) całość świadczeń gwarancyjnych musi być realizowana bezpośrednio przez producenta sprzętu lub podmiot przez niego autoryzowany.

22. Szczegółowy wykaz zamówienia

22.1. Zadanie nr 1 – PCSS

Podana cena dla każdej z pozycji musi obejmować wszystkie składniki kosztów, tj. koszty sprzętu/oprogramowania, dostawy, instalacji, dokumentacji, testów, instruktaży oraz gwarancji.

Lp.	**Nazwa pozycji z specyfikacji technicznej**	**Liczba sztuk sprzętu/serwerów do objęcia licencją**	**Termin dostawy (proszę zaznaczyć możliwe terminy realizacji dostawy zgodnie z Ramowym planem wdrożenia, podpunkt 4, w formie TAK/NIE)**		
			6 tygodni	**8 tygodni**	**12 tygodni**
-1-	**-2-**	**-3-**	**-4-**	**-5-**	**-6-**
a)	Serwer obliczeniowy typu „A”	20			
b)	Serwer obliczeniowy typu „B”	8			
c)	Serwer obliczeniowy typu „C”	10			
d)	Serwer obliczeniowy typu „E”	3			
e)	Macierz blokowa typu „A”	4			
f)	System szybkiej pamięci masowej o dostępie plikowym typu „A”	1			
g)	System archiwalnej pamięci masowej o dostępie plikowym typu „A”	1			
h)	System pamięci masowej o dostępie obiektowym	1			
i)	Urządzenie do przechowywania kopii zapasowych	2			
j)	Oprogramowanie do wykonywania kopii zapasowych	Na wszystkie dostarczone serwery			
k)	Oprogramowanie do wirtualizacji zasobów serwerowych i ich mocy obliczeniowej w wersji rozszerzonej	Na wszystkie dostarczone serwery			
l)	Oprogramowanie do zarządzania klastrem wirtualizacyjnym	1			
m)	Oprogramowanie do wirtualizacji sieci w wersji rozszerzonej	Na wszystkie dostarczone serwery			
n)	Oprogramowanie do wirtualizacji przestrzeni dyskowej w wersji rozszerzonej	Na dostarczone serwery typu „C”			

o)	Oprogramowanie do automatyzacji zadań w ramach środowiska zwirtualizowanego	Na wszystkie dostarczone serwery			
p)	Oprogramowanie do monitorowania i zarządzania platformą wirtualizacyjną	Na wszystkie dostarczone serwery			
q)	Oprogramowanie do centralnego zbierania logów	Na wszystkie dostarczone serwery			
r)	Oprogramowanie do wirtualizacji mocy obliczeniowej akceleratorów graficznych	Na dostarczone serwery typu „E”			
s)	Oprogramowanie dostarczające zintegrowaną platformę Kubernetes	Na dostarczone serwery typu „C”			
t)	Oprogramowanie do wirtualizacji stacji roboczych	Licencja umożliwiająca jednoczesną pracę 20 użytkowników			
u)	Przełącznik sieciowy 1GbE	4			
v)	Przełącznik sieciowy 25GbE	2			
w)	Przełącznik sieciowy 100Gb	14			
x)	System zdalnego dostępu – Terminal zdalnego dostępu	2			
y)	System zdalnego dostępu – Urządzenie dostępowe typ D1	1			
z)	System zdalnego dostępu – Urządzenie dostępowe typ D2	4			
aa)	System zdalnego dostępu – System dostępowy typ D3	1			
bb)	System zdalnego dostępu – Mobilne urządzenie monitorujące	2			
cc)	Stacja Zarządzania Typ 1	10			
dd)	Stacja Zarządzania Typ 2	10			
CENA netto sumaryczna (PLN) **cena musi obejmować wszystkie składniki kosztów, tj. koszty sprzętu, oprogramowania, dostawy, instalacji, dokumentacji, testów, instruktaży oraz gwarancji**					
W tym cena netto (PLN) kosztów dostawy sprzętu i oprogramowania wraz z gwarancją					
W tym cena netto (PLN) kosztów instalacji, wykonania dokumentacji i testów, instruktaży, pozostałych					
Oprogramowanie do wirtualizacji pochodzi od jednego producenta			**TAK/NIE** **(proszę skreślić niepotrzebne)**		

22.2. Zadanie nr 2 – NENCKI

Podana cena dla każdej z pozycji musi obejmować wszystkie składniki kosztów, tj. koszty sprzętu/oprogramowania, dostawy, instalacji, dokumentacji, testów, instruktaży oraz gwarancji.

Lp.	**Nazwa pozycji z specyfikacji technicznej**	**Liczba sztuk sprzętu/serwerów do objęcia licencją**	**Termin dostawy (proszę zaznaczyć możliwe terminy realizacji dostawy zgodnie z Ramowym planem wdrożenia, podpunkt 4, w formie TAK/NIE)**		
			6 tygodni	**8 tygodni**	**12 tygodni**
-1-	**-2-**	**-3-**	**-4-**	**-5-**	**-6-**
a)	Serwer obliczeniowy typu „A”	4			
b)	Serwer obliczeniowy typu „D”	2			
c)	Interfejsy Fibre Channel do serwera typu „A”	4			
d)	Macierz blokowa typu „B”	1			
e)	System szybkiej pamięci masowej o dostępie plikowym typu „B”	1			
f)	System archiwalnej pamięci masowej o dostępie plikowym typu „B”	1			
g)	Oprogramowanie do wykonywania kopii zapasowych	Na wszystkie dostarczone serwery			
h)	Oprogramowanie do wirtualizacji zasobów serwerowych i ich mocy obliczeniowej w wersji rozszerzonej	Na wszystkie dostarczone serwery			
i)	Oprogramowanie do zarządzania klastrem wirtualizacyjnym	1			
j)	Oprogramowanie do wirtualizacji sieci w wersji rozszerzonej	Na wszystkie dostarczone serwery			
k)	Oprogramowanie do wirtualizacji mocy obliczeniowej akceleratorów graficznych	Na dostarczone serwery typu „D”			
l)	Oprogramowanie do wirtualizacji stacji roboczych	Licencja umożliwiająca jednoczesną pracę 20 użytkowników			
m)	Przełącznik sieciowy 1GbE	1			
n)	Przełącznik sieciowy 25GbE	4			
o)	Przełącznik sieciowy 100Gb	8			

p)	Przełącznik sieciowy 10GbE (10GBase-T)	8			
q)	Przełączniki Fibre Channel	2			
r)	System zdalnego dostępu – Terminal zdalnego dostępu	1			
s)	Przełączniki warstwy trzeciej	2			
CENA netto sumaryczna (PLN) **cena musi obejmować wszystkie składniki kosztów, tj. koszty sprzętu, oprogramowania, dostawy, instalacji, dokumentacji, testów, instruktaży oraz gwarancji**					
W tym cena netto (PLN) kosztów dostawy sprzętu i oprogramowania wraz z gwarancją					
W tym cena netto (PLN) kosztów instalacji, wykonania dokumentacji i testów, instruktaży, pozostałych					
Oprogramowanie do wirtualizacji pochodzi od jednego producenta			**TAK/NIE** **(proszę skreślić niepotrzebne)**		