



## Spis treści

1. Definicje używane w dokumencie:.....	3
2. Serwery wirtualizacyjne .....	4
2.1. Parametry ogólne .....	4
2.2. Wymagania na pamięć, dyski, procesor i interfejsy sieciowe .....	9
3. Oprogramowanie do wykonywania kopii zapasowych .....	11
4. Oprogramowanie do wirtualizacji .....	20
4.1. Wymagania wspólne dla wszystkich modułów oprogramowania do wirtualizacji .....	20
4.2. Oprogramowanie do wirtualizacji zasobów serwerowych i ich mocy obliczeniowej .....	20
4.3. Oprogramowanie do zarządzania klastrem wirtualizacyjnym .....	23
4.4. Oprogramowanie do wirtualizacji przestrzeni dyskowej .....	24
5. Przełączniki sieciowe .....	27
6. Wdrożenie systemu.....	32
6.1. Ramowy plan wdrożenia .....	32
6.2. Dostawa i instalacja.....	35
6.2.1. Ogólne wytyczne dotyczące dostawy i instalacji.....	35
6.2.2. Warunki instalacji zapewnione przez Zamawiającego .....	36
6.2.3. Szczegółowe wymagania dotyczące dostawy i instalacji, które musi spełnić Wykonawca .....	37
6.3. Dokumentacja .....	41
6.4. Dokumentacja Techniczna .....	41
6.5. Dokumentacja Powykonawcza.....	42
6.6. Wytyczne do testów .....	44
6.6.1. Testy weryfikacyjne .....	44
6.6.2. Testy akceptacyjne (podstawowe i niezawodnościowe) .....	45
6.6.3. Testy wydajnościowe .....	46
6.6.4. Testy odbiorcze .....	47
6.7. Odbiory.....	48
7. Gwarancja.....	49
7.1. Ogólne warunki Gwarancji .....	49
7.2. Opis usługi Gwarancji .....	50
7.2.1. Diagnostyka i rozwiązywanie problemów .....	50
7.2.2. Klasyfikacja problemów.....	50





# POZNAŃSKIE CENTRUM SUPERKOMPUTEROWO - SIECIOWE

PN 14/02/2023 – system wizualizacji oraz środowisko serwerowe QKD

7.2.3.	Poziomy świadczenia usługi .....	51
7.2.4.	Wymiana informacji pomiędzy Zamawiającym a Wykonawcą .....	52
7.2.5.	Zgłaszanie problemów.....	53
7.2.6.	Czas reakcji .....	53
7.2.7.	Rozwiązanie problemu .....	53
7.2.8.	Czas rozwiązania problemu .....	54
7.2.9.	Przywrócenie systemu.....	54
7.2.10.	Czas przywrócenia systemu.....	54
7.2.11.	Rozwiązanie zgłoszenia problemu.....	55
7.2.12.	Konsultacje .....	55
7.2.13.	Dostarczanie i wsparcie w instalacji Oprogramowania.....	56
7.2.14.	Szczegółowe wymagania gwarancji dotyczące elementów Systemu .....	57





## 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 wirtualizacyjne

### 2.1. Parametry ogólne

Parametr	Charakterystyka (wymagania minimalne)
Obudowa	<ol style="list-style-type: none"> <li>1) Wysokość 1 lub 2 RU</li> <li>2) Obudowa zapewniająca poprawny montaż w szafie teleinformatycznej 19" o głębokości 120 cm wraz z akcesoriami opisanym w podpunkcie poniżej (2).</li> <li>3) 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.</li> <li>4) Obudowa umożliwiająca instalację dysków 2,5" SATA/SAS/NVMe.</li> <li>5) Obudowa musi umożliwiać instalację co najmniej 8 dysków w rozmiarze 2,5".</li> </ol>
Płyta główna	<ol style="list-style-type: none"> <li>1) Płyta główna z możliwością zainstalowania dwóch procesorów.</li> <li>2) Na płycie głównej muszą znajdować się minimum 32 gniazda przeznaczone do instalacji pamięci.</li> <li>3) Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym.</li> <li>4) Płyta główna musi obsługiwać interfejs PCIe 4.0</li> </ol>
Wbudowane porty	<ol style="list-style-type: none"> <li>1) Minimum 1 port Type-A USB w standardzie 2.0 lub wyższy na przednim panelu serwera.</li> <li>2) Minimum 1 port Type-A w standardzie USB 3.0 lub wyższy na tylnym panelu.</li> <li>3) Minimum 1 port VGA.</li> </ol>
Wentylatory	<ol style="list-style-type: none"> <li>1) Redundantne typu Hot-Plug.</li> </ol>
Bezpieczeństwo	<ol style="list-style-type: none"> <li>1) Panel przedni zamykany na klucz służący do ochrony przed nieautoryzowanym dostępem do dysków twardej.</li> <li>2) Funkcja wyłączenia w BIOS funkcji przycisku zasilania.</li> <li>3) BIOS musi mieć możliwość przejścia do bezpiecznego trybu rozruchowego z funkcją zarządzania blokadą zasilania, zmianą ustawień BIOS, zmianą hasła do BIOS.</li> <li>4) Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą.</li> <li>5) Wbudowany moduł TPM minimum 2.0.</li> <li>6) Funkcjonalność włączania i wyłączenia portów USB na obudowie.</li> </ol>



# POZNAŃSKIE CENTRUM SUPERKOMPUTEROWO - SIECIOWE

PN 14/02/2023 – system wizualizacji oraz środowisko serwerowe QKD

	<ol style="list-style-type: none"><li>7) Możliwość wymazania danych z dysków znajdujących się wewnątrz serwera:<ol style="list-style-type: none"><li>a) niezależne od zainstalowanego systemu operacyjnego,</li><li>b) uruchamiane z poziomu systemu zarządzania serwerem.</li></ol></li><li>8) Serwer musi spełniać wymagania normy NIST SP 800-193 ochrony przed cyberatakami.</li><li>9) Serwer musi być wyposażony w rozwiązanie zapewniające ochronę oprogramowania układowego (ang. firmware) przed manipulacją ze strony złośliwego oprogramowania.<ol style="list-style-type: none"><li>a) Ochrona taka musi być zgodna z zaleceniami NIST SP 800-147B.</li><li>b) Zamawiający wymaga, aby dostarczony serwer posiadał zaimplementowane sprzętowo mechanizmy kryptograficzne poświadczające integralność oprogramowania BIOS (Root of Trust).</li></ol></li><li>10) Serwer musi umożliwiać utworzenie bezpiecznego profilu w oparciu o konfigurację sprzętową oraz o konfigurację wewnętrznego oprogramowania komponentów serwera. Jakikolwiek odchylenie od profilu musi zostać automatycznie zgłoszone administratorowi.</li><li>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.</li></ol>
Karta Zarządzania	<p>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:</p> <ol style="list-style-type: none"><li>1) zdalny dostęp do graficznego interfejsu www karty zarządzającej, interfejs www musi być wykonany w standardzie HTML5</li><li>2) szyfrowane połączenie (TLS) oraz uwierzytelnienie i autoryzację użytkownika</li><li>3) funkcję zdalnego włączenia, wyłączenia, restartu serwera</li><li>4) odczyt dzienników zdarzeń (ang. logs) dotyczących serwera</li><li>5) podmontowanie zdalnych napędów wirtualnych</li><li>6) uruchomienie wirtualnej konsoli z dostępem do myszy i klawiatury</li><li>7) wsparcie dla protokołu IPv4 i IPv6</li><li>8) wsparcie dla protokołów: SNMP, IPMI2.0, VLAN tagging, SSH, RedFish</li><li>9) funkcję zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer, dane historyczne muszą być dostępne dla min. 7 dni wstecz</li><li>10) funkcję zdalnego ustawienia limitu poboru prądu przez serwer</li><li>11) integrację z Microsoft Active Directory lub LDAP w zakresie uwierzytelnienia i autoryzacji kont dostępowych</li></ol>





# POZNAŃSKIE CENTRUM SUPERKOMPUTEROWO - SIECIOWE

PN 14/02/2023 – system wizualizacji oraz środowisko serwerowe QKD

	<ol style="list-style-type: none"><li>12) obsługę przez minimum trzech administratorów jednocześnie</li><li>13) wsparcie dla automatycznej rejestracji w systemie DNS</li><li>14) wysyłanie do administratorów wiadomości e-mail z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej</li><li>15) zarządzanie bezpośrednio poprzez złącze USB</li><li>16) monitorowanie zużycia dysków SSD</li><li>17) automatyczne zgłaszanie alertów do centrum serwisowego producenta</li><li>18) aktualizacje oprogramowania układowego (ang. firmware) dla wszystkich komponentów serwera</li><li>19) przywrócenie poprzednich wersji oprogramowania układowego</li><li>20) funkcję eksportu/importu konfiguracji (ustawienie karty zarządzającej, BIOSu, kart sieciowych, HBA oraz konfiguracji kontrolera RAID) serwera do/z pliku XML lub JSON</li><li>21) funkcję automatycznego tworzenia kopii konfiguracji serwera w oparciu o zdefiniowany harmonogram</li><li>22) wykrywanie odchyleń konfiguracji na poziomie konfiguracji UEFI oraz wersji oprogramowania układowego serwera</li><li>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 Android i Apple iOS) używając jednego z protokołów BLE lub WIFI</li><li>24) zdalne wyłączenia i włączenia portów USB</li><li>25) mechanizm bezpiecznego wycofywania z eksploatacji poprzez automatyczne usuwanie poufnych danych w tym minimum:<ol style="list-style-type: none"><li>a) konfiguracji BIOS</li><li>b) konfiguracji kontrolera RAID</li><li>c) dzienników systemowych</li><li>d) danych konfiguracyjnych</li><li>e) wszystkich danych z nośników wewnętrznych (dyski twarde, DCPMM, NVDIMM).</li></ol></li></ol> <p>Jeśli wymagana jest dodatkowa licencja na jakąkolwiek funkcjonalność wskazaną przez zamawiającego, to musi ona być dostarczona wraz z serwerem w wersji bez ograniczeń czasowych i terytorialnych (dotyczy terytorium EU). Ponadto Zamawiający wymaga, aby żadna z powyższych funkcjonalności nie wymagała okresowego sprawdzania licencji na zewnętrznych systemach (np. producenta).</p>
System do zarządzania	<ol style="list-style-type: none"><li>1) System do zarządzania serwerami wraz z niezbędną licencją, który musi spełniać niżej wymienione wymagania:<ol style="list-style-type: none"><li>a) integracja z Microsoft Active Directory lub LDAP w zakresie uwierzytelnienia i autoryzacji kont dostępowych</li></ol></li></ol>







# POZNAŃSKIE CENTRUM SUPERKOMPUTEROWO - SIECIOWE

PN 14/02/2023 – system wizualizacji oraz środowisko serwerowe QKD

- b) zarządzanie dostarczonymi serwerami bez udziału dedykowanego agenta
- c) wsparcie dla protokołów SNMP, IPMI, Linux SSH, Redfish
- d) uruchamianie procesu wykrywania urządzeń w oparciu o harmonogram
- e) szczegółowy opis wykrytych systemów oraz ich komponentów
- f) funkcja eksportu raportu do min. CSV, HTML, XLS, PDF
- g) funkcja tworzenia własnych raportów w oparciu o wszystkie informacje zawarte w inwentarzu
- h) grupowanie serwerów w oparciu o kryteria użytkownika
- 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



	<ul style="list-style-type: none"><li>vi) aktualne informacje o stanie i poziomie gwarancji</li><li>vii) adresy IP kart sieciowych</li><li>viii) występujące alerty</li><li>ix) adresy MAC kart sieciowych</li><li>x) stan poszczególnych komponentów serwerów</li><li>y) możliwość tworzenia sprzętowej konfiguracji bazowej i na jej podstawie weryfikacji środowiska w celu wykrycia rozbieżności</li><li>z) wdrażanie serwerów w oparciu o profile konfiguracji</li><li>aa) możliwość migracji ustawień serwera wraz z wirtualnymi adresami sieciowymi (MAC, WWN, IQN) między serwerami</li><li>bb) tworzenie gotowych paczek informacji umożliwiających zdiagnozowanie awarii serwera przez serwis producenta</li><li>cc) zdalne uruchamianie diagnostyki serwera.</li></ul> <p>2) System może być zaoferowany jako prekonfigurowany obraz maszyny wirtualnej (ang. virtual appliance) dla zaoferowanego oprogramowania do wirtualizacji mocy obliczeniowej.</p> <p>3) Musi być dostępna dedykowana aplikacja na urządzenia mobilne (wyposażone w system operacyjny Android/Apple iOS) integrująca się z wyżej opisanym systemem do zarządzania.</p> <p>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 4.3) i spełniać następujące wymagania:</p> <ul style="list-style-type: none"><li>a) możliwość instalowania poprawek podnoszących wersję oprogramowania układowego (ang. firmware) serwera wprost z konsoli wirtualizatora (wymagana zgodność z zaoferowanym oprogramowaniem wirtualizacyjnym)</li><li>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</li><li>c) konsola wirtualizatora musi prezentować szczegółowe informacje o serwerze takie jak ilość oraz typ komponentu dla co najmniej:<ul style="list-style-type: none"><li>a. procesor</li><li>b. pamięć RAM</li><li>c. karty I/O</li><li>d. wentylatory</li><li>e. dyski pamięci masowej</li></ul></li><li>d) konsola wirtualizatora musi prezentować informacje wspierające serwisowanie takie jak:</li></ul>
--	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------



	<ul style="list-style-type: none"> <li>a. numer serwisowy/seryjny serwera</li> <li>b. data obowiązywania gwarancji</li> <li>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</li> <li>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.</li> </ul> <p>Jeśli wymagana jest dodatkowa licencja na jakąkolwiek funkcjonalność wskazaną przez zamawiającego, to musi ona być dostarczona wraz z serwerem w wersji bez ograniczeń czasowych i terytorialnych (dotyczy terytorium EU). Ponadto Zamawiający wymaga, aby żadna z powyższych funkcjonalności nie wymagała okresowego sprawdzania licencji na zewnętrznych systemach (np. producenta).</p>
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	<ul style="list-style-type: none"> <li>1) Microsoft Windows Server min. w wersji 2022 – zgodność potwierdzona dla oferowanego modelu serwera na stronie: <a href="https://www.windowsservercatalog.com/">https://www.windowsservercatalog.com/</a></li> <li>2) Red Hat Enterprise Linux (RHEL) min. w wersji 9 – zgodność potwierdzona dla oferowanego modelu serwera na stronie: <a href="https://access.redhat.com/ecosystem/hardware">https://access.redhat.com/ecosystem/hardware</a></li> <li>3) VMware ESXi min. w wersji 7 – zgodność potwierdzona dla oferowanego modelu serwera na stronie: <a href="https://www.vmware.com/resources/compatibility/search.php">https://www.vmware.com/resources/compatibility/search.php</a></li> </ul>
Dokumentacja użytkownika	1) Zamawiający wymaga dostarczenia dokumentacji technicznej w języku polskim lub angielskim w wersji elektronicznej.

## 2.2. Wymagania na pamięć, dyski, procesor i interfejsy sieciowe

Parametr	Charakterystyka (wymagania minimalne)
----------	---------------------------------------



# POZNAŃSKIE CENTRUM SUPERKOMPUTEROWO - SIECIOWE

PN 14/02/2023 – system wizualizacji oraz środowisko serwerowe QKD

Pamięć RAM	<ol style="list-style-type: none"><li>1) Minimum 1 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.</li></ol>
Interfejsy sieciowe	<ol style="list-style-type: none"><li>1) Dwa interfejsy sieciowe o przepustowości 1 Gb/s Ethernet w standardzie Base-T.</li><li>2) Dwuportowa karta sieciowa zainstalowana w serwerze jako karta rozszerzeń w slotcie PCIe 4.0, z gniazdami o przepustowości 25 Gb/s Ethernet, posiadająca:<ol style="list-style-type: none"><li>a) interfejs PCIe 4.0 x16</li><li>b) wsparcie dla wirtualizacji SR-IOV oraz VirtIO</li><li>c) sprzętowe wsparcie dla szyfrowania AES-GCM 128/256 dla protokołów IPsec i TLS, wsparcie dla AES-XTS</li><li>d) wydajność min. 215 Mpps</li><li>e) wsparcie dla RoCE Programmable Congestion Control</li><li>f) wsparcie dla IEEE 1588v2</li><li>g) sprzętowe wsparcie enkapsulacji i dekapulacji dla protokołów VxLAN, NVGRE, Geneve</li><li>h) wsparcie dla Jumbo Frames o rozmiarach minimum 9 KB.</li></ol></li><li>3) Dwuportowa karta sieciowa zainstalowana w serwerze jako karta rozszerzeń w slotcie PCIe lub w slotcie z interfejsem OCP 3.0, z gniazdami o przepustowości 25 Gb/s Ethernet w standardzie SFP28, wspierająca również gniazda 10 Gb/s Ethernet w standardzie SFP+, posiadająca:<ol style="list-style-type: none"><li>a) wsparcie dla wirtualizacji SR-IOV</li><li>b) wsparcie dla enkapsulacji i dekapulacji dla protokołów VxLAN, NVGRE, Geneve</li><li>c) wsparcie dla RoCE</li><li>d) wsparcie dla Jumbo Frames o rozmiarach minimum 9 KB.</li></ol></li></ol> <p>Karty opisane w pkt. 2) i 3) muszą poprawnie współpracować z modułami optycznymi (zgodnymi z ogólnie przyjętymi normami właściwymi dla danego typu interfejsu) pochodzącymi od różnych producentów. Obsługa modułów optycznych innych producentów nie może wymagać instalacji dodatkowego oprogramowania lub zmian w konfiguracji karty.</p>
Procesor	<ol style="list-style-type: none"><li>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. 515 punktów w teście CPU2017 Floating Point Rate. Wynik dla zaoferowanego modelu serwera w konfiguracji z zaproponowanymi procesorami musi być dostępny na stronie <a href="http://www.spec.org">www.spec.org</a></li><li>2) Procesor musi obsługiwać interfejs PCIe 4.0.</li></ol>



Dyski twarde	<ol style="list-style-type: none"><li>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.</li><li>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.</li><li>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.</li></ol>
Kontroler	<ol style="list-style-type: none"><li>1) Sprzętowy kontroler dyskowy HBA, wspierający interfejs PCIe 4.0, zgodny z zaoferowanym oprogramowaniem do wirtualizacji oraz znajdujący się na liście zgodności zaoferowanego oprogramowania do wirtualizacji przestrzeni dyskowej opisanego w punkcie Oprogramowanie do wirtualizacji przestrzeni dyskowej <b>4.4</b>.</li></ol>

### 3. 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 niezvirtualizowanych 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 na systemie operacyjnym Windows / Linux.



## POZNAŃSKIE CENTRUM SUPERKOMPUTEROWO - SIECIOWE

PN 14/02/2023 – system wizualizacji oraz środowisko serwerowe QKD

- 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 medium deduplikacyjne zarówno poprzez sieć LAN jak również SAN.
- 10) Wymagane jest by istniała możliwość wyboru miejsca deduplikacji
  - a) na źródle
  - b) na medium backupowymzarówno dla backupu po LAN jak i SAN
- 11) Backup z 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 urządzeniu do przechowywania kopii zapasowych (medium deduplikacyjne) bez pośrednictwa jakichkolwiek innych serwerów. Funkcjonalność musi być dostępna dla minimum następujących systemów: Windows, RedHat, SuSE, HP-UX, Solaris, AIX.
- 13) Oprogramowanie backupowe musi zapewniać bezpośredni backup z deduplikacją na źródle z każdej zabezpieczanej maszyny znajdującej się w sieci LAN bezpośrednio na medium deduplikacyjne bez pośrednictwa jakichkolwiek innych serwerów. Funkcjonalność musi być dostępna dla minimum następujących systemów: Windows, RedHat, SuSE, HP-UX, Solaris, AIX.
- 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 jakiegokolwiek interwencji administratora oraz bez wznawiania procesu backupu.
- 15) Wymagane jest by oprogramowanie backupowe zapewniało szybki backup blokowy wielomilionowych systemów plików na maszynach 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 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.





## POZNAŃSKIE CENTRUM SUPERKOMPUTEROWO - SIECIOWE

PN 14/02/2023 – system wizualizacji oraz środowisko serwerowe QKD

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) 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 de-duplikatora sprzętowego na taśmę), oferowany system musi generować dla każdego backupu samopisujące się taśmy dla całości zapisywanych taśm. Oznacza to, że wyjęcie jakiegokolwiek 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 samo-opisujące się zbiory danych zarówno na de-duplikatorze sprzętowym jak i na taśmach. Utraty wszystkich wewnętrznych danych oprogramowania backupowego nie może powodować braku możliwości odtworzenia jakichkolwiek zbiorów z 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 też trwałego.
- 27) Oprogramowanie backupowe musi umożliwiać zarządzanie replikacją backupów między kilkoma urządzeniami de-duplikacyjnymi bezpośrednio z poziomu interfejsu oprogramowania backupowego przy spełnieniu wszystkich poniższych wymagań







## POZNAŃSKIE CENTRUM SUPERKOMPUTEROWO - SIECIOWE

PN 14/02/2023 – system wizualizacji oraz środowisko serwerowe QKD

- a) replikacji podlegają tylko te bloki które nie znajdują się na docelowym urządzeniu deduplikacyjnym
- b) replikacja między urządzeniami deduplikacyjnymi 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 deduplikacyjnych.

W trakcie odtwarzania, z graficznego GUI, oferowane oprogramowanie backupowe musi pozwalać na wybór urządzenia deduplikacyjnego 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 deduplikacją zmiennym blokiem
  - b) z deduplikacją 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 muszą być przesłane tylko te kawałki danych, które się tam jeszcze nie znajdują. Funkcjonalność ta musi być dostępna minimum dla zabezpieczanych systemów 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 dowolnymi mediami, minimum:
  - a) deduplikacyjnymi
  - 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 deduplikatora na pojedynczy napęd taśmowy, wszystkie 20 klonowane/duplikowane zadania muszą być jednocześnie w tym samym czasie zapisywane na pojedynczy napęd taśmowy.

- 35) Oprogramowanie backupowe musi pozwalać na backup systemu plików:







## POZNAŃSKIE CENTRUM SUPERKOMPUTEROWO - SIECIOWE

PN 14/02/2023 – system wizualizacji oraz środowisko serwerowe QKD

- 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 urządzenie deduplikacyjne. Jedynie zarządzanie (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 urządzeniu deduplikacyjnym. 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 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 muszą być automatycznie usuwane.
- 47) Oprogramowanie musi umożliwiać kopię zapasową:
- a) pojedynczych plików





## POZNAŃSKIE CENTRUM SUPERKOMPUTEROWO - SIECIOWE

PN 14/02/2023 – system wizualizacji oraz środowisko serwerowe QKD

- b) całych systemów plików
  - c) baz danych w trakcie ich normalnej pracy
  - d) ustawień 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) 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 aplikacji i baz danych: MS Exchange, MS SQL, 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 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 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) bazą danych Oracle. Muszą 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 (przeźren FRA, media oferowanego rozwiązania backupowego).





## POZNAŃSKIE CENTRUM SUPERKOMPUTEROWO - SIECIOWE

PN 14/02/2023 – system wizualizacji oraz środowisko serwerowe QKD

- 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:
- lokalny backup na medium de-duplikacyjne z retencją miesięczną
  - replikę zmian do medium de-duplikacyjnego w zdalnej lokalizacji (retencja 60 dni)  
replikacja odbywa się między urządzeniami de-duplikacyjnymi
  - replikacja backupu z lokalnego medium de-duplikacyjnego na medium taśmowe (retencja 5 lat)
  - 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:
- zabezpieczanego serwera / komputera
  - konsoli systemu backupowego.
- 58) Dla zaoferowanego środowiska wirtualizacji mocy obliczeniowej oprogramowanie backupowe musi umożliwiać następujące typy backupu:
- backup pojedynczych plików i baz danych z maszyny wirtualnej ze środka maszyny wirtualnej
  - backup całych maszyn wirtualnych (obrazów, plików reprezentujących wirtualną maszynę). W trakcie backupu odczytowi z systemu dyskowego mają podlegać tylko zmienione bloki wirtualnych maszyn
  - backup tylko wybranych dysków maszyny wirtualnej (wybranych plików systemu do wirtualizacji)
  - w trakcie backupu odczytowi z systemu dyskowego mają podlegać tylko zmienione bloki wirtualnych maszyn
  - Wszystkie backupy obrazów maszyn wirtualnych muszą być wykonywane do medium backupowego przy pomocy technologii transferującej tylko zmienione bloki.





## POZNAŃSKIE CENTRUM SUPERKOMPUTEROWO - SIECIOWE

PN 14/02/2023 – system wizualizacji oraz środowisko serwerowe QKD

Jednocześnie z punktu widzenia systemu backupowego muszą 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-duplikacyjnego.

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 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 równoległe, w tym samym czasie minimum 100 maszyn wirtualnych. Wykonywane równoległe backupy maszyn wirtualnych muszą 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.





PN 14/02/2023 – system wizualizacji oraz środowisko serwerowe QKD

- 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:
- odtworzenie całej maszyny wirtualnej
  - odtworzenie pojedynczego dysku z wcześniej zrobionej kopii całej maszyny wirtualnej
  - odtworzenie plików / katalogów z backupu obrazów maszyny wirtualnej
  - uruchomienie maszyny wirtualnej z medium backupowego bez odtwarzania
  - 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 też 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 polityką zdefiniowaną 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:
- automatyczne dodanie do odpowiednich polityk backupowych wszystkich maszyn wirtualnych zawierających w nazwie maszyny wirtualnej podany tekst
  - automatyczne dodanie do odpowiednich polityk backupowych wszystkich maszyn wirtualnych znajdujących się we wszystkich folderach zawierających w nazwie podany tekst
  - 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:
- wszystkie nowo utworzone maszyny wirtualne zawierające w nazwie frazę „krytyczna” muszą być backupowane automatycznie co godzinę
  - wszystkie nowo utworzone maszyny wirtualne zawierające w nazwie frazę „produkcja” muszą być backupowane automatycznie raz na dzień







PN 14/02/2023 – system wizualizacji oraz środowisko serwerowe QKD

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 jakiegokolwiek 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 usuniętej 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/odtworzenia obrazów maszyn wirtualnych pomiędzy dostępne serwery pośredniczące,

## 4. Oprogramowanie do wirtualizacji

Zaoferowane oprogramowanie do wirtualizacji musi być w pełni kompatybilne ze sobą w ramach wszystkich zaoferowanych modułów, których specyfikację zawarto w poniższych podpunktach.

### 4.1. Wymagania wspólne dla wszystkich modułów oprogramowania do wirtualizacji

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

### 4.2. Oprogramowanie do wirtualizacji zasobów serwerowych i ich mocy obliczeniowej

- 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







## POZNAŃSKIE CENTRUM SUPERKOMPUTEROWO - SIECIOWE

PN 14/02/2023 – system wizualizacji oraz środowisko serwerowe QKD

- c) potrafić obsłużyć i wykorzystać zasoby fizyczne serwera: 2 procesory fizyczne, co najmniej 128 logicznych wątków procesora, 2TB pamięci fizycznej RAM
- d) zapewniać możliwość skonfigurowania maszyn wirtualnych z możliwością przydzielenia od 1 do minimum 256 procesorów wirtualnych
- e) zapewniać możliwość skonfigurowania maszyn wirtualnych z możliwością przydzielenia minimum 4 TB pamięci operacyjnej RAM
- f) zapewniać możliwość skonfigurowania maszyn wirtualnych z możliwością przydzielenia od 1 do 10 wirtualnych kart sieciowych dla każdej z nich. Dodatkowo, oprogramowanie musi posiadać możliwość utworzenia maszyny wirtualnej bez przydzielonej wirtualnej karty sieciowej
- g) zapewniać możliwość skonfigurowania maszyn wirtualnych, z których każda może mieć 32 porty szeregowo, 3 porty równoległe i 20 urządzeń USB
- h) wspierać następujące systemy operacyjne: Windows Server 2012, Windows Server 2016, Windows Server 2019, Windows 7, Windows 8, Windows 10, SLES 12, SLES 11, SLES 10, RHEL 8, REHL 7, Solaris 11, Debian, CentOS, FreeBSD, Ubuntu, Oracle Linux
- 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 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





## POZNAŃSKIE CENTRUM SUPERKOMPUTEROWO - SIECIOWE

PN 14/02/2023 – system wizualizacji oraz środowisko serwerowe QKD

- r) w celu zapewnienia bezpieczeństwa połączenia ethernetowego w razie awarii fizycznej karty sieciowej pojedynczy wirtualny przełącznik, musi posiadać możliwość przyłączenia 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 obsługiwanie dysków wirtualnych maszyn do rozmiaru co najmniej 60 TB
- dd) posiadać funkcjonalność zarządzania poprzez ustandaryzowany interfejs programistyczny (API)
- ee) posiadać wbudowany interfejs programistyczny (API) zapewniający pełną integrację zewnętrznych rozwiązań wykonywania kopii zapasowych z istniejącymi mechanizmami warstwy wirtualizacyjnej
- ff) być kompatybilne z TPM 2.0. Minimalne wymaganie Zamawiającego dla TPM oznacza, że TPM zapewnia mechanizm gwarantujący, że serwer fizyczny, na którym zainstalowane jest zaoferowane oprogramowanie, uruchomił się z włączoną opcją Secure Boot. Po potwierdzeniu, że Secure Boot jest włączone, system gwarantuje, poprzez weryfikację





## POZNAŃSKIE CENTRUM SUPERKOMPUTEROWO - SIECIOWE

PN 14/02/2023 – system wizualizacji oraz środowisko serwerowe QKD

podpisu cyfrowego, że serwer wirtualizacyjny (ang. hypervisor) uruchomił się w niezmienionej formie

- gg) posiadać funkcjonalność wirtualnego TPM 2.0 dla maszyn wirtualnych z zainstalowanym Microsoft Windows 10, Microsoft Windows 2016 i nowszych. Zamawiający wymaga aby z punktu widzenia maszyny wirtualnej z systemem operacyjnym Microsoft Windows 10, Microsoft Windows 2016 i nowszym wirtualny TPM widziany był jako standardowy TPM, gdzie można przechowywać bezpiecznie wrażliwe dane, np. certyfikaty. Zawartość wirtualnego TPM musi być przechowywana w pliku przynależnym do maszyny wirtualnej oraz musi być szyfrowana
- hh) posiadać funkcjonalność szybkiego uruchamiania oprogramowania wirtualizacyjnego po przeprowadzonym procesie jego aktualizacji. Zamawiający wymaga, aby w procesie aktualizacji oprogramowania, jeśli wymagany jest jego restart, funkcjonalność szybkiego uruchamiania powodowała eliminację czasochłonnej fazy inicjalizacji serwera fizycznego
- ii) wspierać protokół precyzyjnej synchronizacji czasu PTP (ang. Precision Time Protocol) i NTP (ang. Network Time Protocol)
- jj) posiadać mechanizm, który ogranicza dostęp do indywidualnego zarządzania warstwą wirtualizacji na serwerach fizycznych, w ramach klastra serwerów, w celu zwiększenia bezpieczeństwa dostępu warstwy wirtualizacji
- kk) mieć funkcjonalność migracji w trybie rzeczywistym dysków działających maszyn wirtualnych z jednego podsystemu dyskowego do innego bez konieczności przerywania pracy maszyny wirtualnej, której dysk jest migrowany
- ll) zapewniać podstawowe funkcje serwera zarządzania kluczami (KMS), które upraszcza włączenie szyfrowania i zaawansowanych funkcji bezpieczeństwa
- mm) mieć możliwość przenoszenia maszyn wirtualnych w czasie ich pracy pomiędzy serwerami fizycznymi, pamięciami masowymi (niezależnie od dostępności współdzielonej przestrzeni dyskowej), różnymi rodzajami wirtualnych przełączników sieciowych
- nn) posiadać co najmniej 2 niezależne mechanizmy wzajemnej komunikacji między serwerami z zainstalowanym oprogramowaniem wirtualizacyjnym oraz z serwerem zarządzającym tym oprogramowaniem, gwarantujące właściwe działanie mechanizmów wysokiej dostępności na wypadek izolacji sieciowej serwerów fizycznych lub partycjonowania sieci.

### 4.3. Oprogramowanie do 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”)





## POZNAŃSKIE CENTRUM SUPERKOMPUTEROWO - SIECIOWE

PN 14/02/2023 – system wizualizacji oraz środowisko serwerowe QKD

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

#### 4.4. Oprogramowanie do wirtualizacji przestrzeni dyskowej

- 1) Zaoferowane oprogramowanie do wirtualizacji przestrzeni dyskowej 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)





## POZNAŃSKIE CENTRUM SUPERKOMPUTEROWO - SIECIOWE

PN 14/02/2023 – system wizualizacji oraz środowisko serwerowe QKD

- 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 obsługi 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







## POZNAŃSKIE CENTRUM SUPERKOMPUTEROWO - SIECIOWE

PN 14/02/2023 – system wizualizacji oraz środowisko serwerowe QKD 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 do zarządzania klastrem wirtualizacyjnym
- 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 wyłączania 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







## POZNAŃSKIE CENTRUM SUPERKOMPUTEROWO - SIECIOWE

PN 14/02/2023 – system wizualizacji oraz środowisko serwerowe QKD

- bb) mieć możliwość włączania na żądanie i wyłączenia na żądanie dostępnej w ramach funkcjonalności zaoferowanego oprogramowania dedupikacji i kompresji
  - cc) zapewniać mechanizmy optymalizacji wykorzystania przestrzeni dyskowych (ang. erasure coding) dla RAID 5 i RAID 6 konfigurowane z dokładnością do dysku maszyny wirtualnej
- 2) Każdy serwer fizyczny, na którym zostanie zainstalowane zaoferowane oprogramowanie, 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.

### 5. Przetącniki sieciowe

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

I.p	Wymaganie	25GbE	1GbE
<b>Typy i minimalne ilości wymaganych portów</b>			
1	Ilość portów 100GbE (QSFP)	4	
2	Ilość portów 1/10GbE (SFP+)		4
3	Ilość portów 1/10/25GbE (SFP28+)	24	
4	Ilość portów 1GbE (1000Base-T), wykluczając porty dedykowane do zarządzania.		48
<b>Parametry fizyczne i zasilanie</b>			
1	Wysokość przetącnika liczona w jednostkach Rack Units [RU].	1RU	1RU
2	Przetącnik musi poprawnie pracować w temperaturze od 0 do 40 °C.	Tak	Tak
3	Przetącnik musi poprawnie pracować przy względnej wilgotności powietrza co najmniej w zakresie od 5% do 90% zakładając brak występowania zjawiska kondensacji pary wodnej.	Tak	Tak
4	W celu zachowania redundancji zasilania, każdy przetącnik 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 przetącnika oraz ograniczenia jego funkcjonalności i wydajności (w zakresie wymaganym przez Zamawiającego). Przetącnik musi być wyposażony w co najmniej dwa zasilacze. Dostarczone zasilacze muszą umożliwiać poprawną pracę przetącnika w pełnej	Tak	Tak





# POZNAŃSKIE CENTRUM SUPERKOMPUTEROWO - SIECIOWE

PN 14/02/2023 – system wizualizacji oraz środowisko serwerowe QKD

I.p	Wymaganie	25GbE	1GbE
	(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. <b>UWAGA:</b> możliwa zmiana kierunku zgodnie z zapisami w punkcie 6.2.3, które należy uwzględnić.	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
7	Przełącznik musi umożliwiać instalację lub wymianę zasilaczy w trakcie pracy urządzenia (hot-swap).	Tak	Nie
<b>Wymagania licencyjne i status urządzeń</b>			
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
2	Wszystkie przełączniki wraz z działającym na nich oprogramowaniem sterującym muszą pochodzić od jednego producenta.	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 EU), ani w żaden inny sposób wpływający na cel ich wykorzystania. Restart elementów nie może powodować konieczności wykonania prac serwisowych, utrzymaniowych lub konfiguracyjnych potrzebnych do odblokowania wszystkich wymaganych funkcjonalności. Licencje powinny być lokalne dla każdego urządzenia – nie dopuszcza się komunikacji z systemami trzecimi w celu utrzymywania/weryfikacji licencji.	Tak	Tak
4	Wszystkie interfejsy liniowe przełączników muszą być odblokowane. Oznacza to, że nie mogą posiadać żadnych blokad umożliwiających ich wykorzystanie dopiero po wprowadzeniu jakiegokolwiek licencji, klucza, kodu lub innego mechanizmu	Tak	Nie





# POZNAŃSKIE CENTRUM SUPERKOMPUTEROWO - SIECIOWE

PN 14/02/2023 – system wizualizacji oraz środowisko serwerowe QKD

I.p	Wymaganie	25GbE	1GbE
	odblokowującego. Dotyczy to wszystkich interfejsów znajdujących się fizycznie w oferowanych przełącznikach.		
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
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. Niedopuszczalne jest wykorzystanie oprogramowania prototypowego, wytwarzanie wersji oprogramowania wyłącznie na potrzeby zamawiającego, nieoferowanej innym klientom.	Tak	Tak
<b>Wymagania wydajnościowe i pojemnościowe</b>			
1	Wydajność przełączania co najmniej	4.0 Tbps	290 Gbps
2	Liczba przetwarzanych pakietów na sekundę	1 Bpps	200 Mpps
3	Czas przełączania ramek nie dłuższy niż	1 $\mu$ s	3 $\mu$ s
4	Całkowita wielkość buforów	32MB	4MB
5	Minimalna liczba obsługiwanych adresów MAC	280 000	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	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	4 000
8	Ilość jednocześnie aktywnych VLANów	4000	1024
9	Całkowita maksymalna moc pobierana przez urządzenie, nie większa niż	650W	250W





# POZNAŃSKIE CENTRUM SUPERKOMPUTEROWO - SIECIOWE

PN 14/02/2023 – system wizualizacji oraz środowisko serwerowe QKD

I.p	Wymaganie	25GbE	1GbE
10	Maksymalna typowa moc pobierana przez urządzenie, nie większa niż	400W	250W
<b>Wymagania operacyjne</b>			
1	Moduły optyczne dla interfejsów muszą umożliwiać sprawdzenie mocy odbieranego sygnału.	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	Nie
3	Przełączniki muszą umożliwiać konfigurację wykorzystując modele OpenConfig. Musi być zapewniona obsługa następujących protokołów: gRPC, RESTCONF, NETCONF.	Tak	Nie
4	Przełączniki muszą zapewniać strumieniowanie danych telemetrycznych wykorzystując protokół NETCONF/gRPC lub w formacie GPB.	Tak	Nie
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	Nie
6	Wszystkie przełączniki muszą obsługiwać protokoły NTP i NTP6.	Tak	Tak
7	Wszystkie Elementy przełączające muszą wspierać Precision Time Protocol (PTP, IEEE 1588v2).	Tak	Nie
8	Wszystkie przełączniki muszą obsługiwać protokół LLDP.	Tak	Tak
9	Wszystkie przełączniki muszą umożliwiać dodanie wydzielonej tablicy routingu dla funkcji zarządzania (ang. Management VRF).	Tak	Nie
10	Wszystkie przełączniki muszą zapewniać mechanizm sprzętowej ochrony przeciw atakowi przeciążającemu (ang. DoS) na jednostkę sterującą CPU (ang. Control Plane Protection).	Tak	Nie
<b>Wymagania dla obsługi VXLAN</b>			
1	Przełączniki muszą zapewniać sprzętową obsługę enkapsulacji VXLAN. Jednocześnie przy enkapsulacji musi być możliwa obsługa przełączania w warstwie L2 (ang. bridging).	Tak	Nie
2	Przełączniki muszą zapewniać sprzętową obsługę enkapsulacji VXLAN. Jednocześnie, przy enkapsulacji musi być możliwa obsługa routingu IP.	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	Nie





# POZNAŃSKIE CENTRUM SUPERKOMPUTEROWO - SIECIOWE

PN 14/02/2023 – system wizualizacji oraz środowisko serwerowe QKD

I.p	Wymaganie	25GbE	1GbE
4	<p>Przełączniki muszą obsługiwać mechanizm protekcji grup linków Ethernet (LAG z LACP) poprzez podłączenie ich do co najmniej dwóch Elementów przełączających. To znaczy, pojedyncza wiązka LAG musi mieć możliwość zakończenia na co najmniej dwóch Elementach przełączających zapewniając w pełni aktywną komunikację na wszystkich linkach grupy. Protekcja musi zapewniać nieprzerwaną pracę w przypadku awarii dowolnego pojedynczego komponentu. Protekcja musi poprawnie współpracować z VXLAN, EVPN, SpanningTree.</p> <p>Jeśli implementacja protekcji wymaga dodatkowych portów które przenoszą ruch w czasie awarii wykonawca musi dostarczyć odpowiednie okablowanie o długości minimum 2.5m</p>	Tak	Nie
<b>Wymagania sieciowe</b>			
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
2	Wszystkie przełączniki muszą obsługiwać funkcję IGMP snooping (dla IGMPv2 oraz IGMPv3).	Tak	Tak
3	Wszystkie przełączniki muszą obsługiwać agregację interfejsów z wykorzystaniem protokołu LACP (IEEE 802.3ad).	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
5	Wszystkie przełączniki muszą obsługiwać 802.1w RSTP, 802.1s MSTP.	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
7	Wszystkie przełączniki muszą obsługiwać protokół 802.1Qbb PFC (Priority-based Flow Control).	Tak	Nie
8	Wszystkie przełączniki muszą umożliwiać regulację (ang. Shaping) wielkości ruchu wyjściowego.	Tak	Nie



I.p	Wymaganie	25GbE	1GbE
9	Wszystkie przełączniki zapewniać statyczny routing IP oraz dynamiczny routing IP zgodny z OSPFv2, OSPFv3, BGP.	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
11	Wszystkie przełączniki muszą zapewniać możliwość tworzenia polityk dla routing IP (ang. Route Maps).	Tak	Nie
12	Wszystkie przełączniki muszą zapewniać możliwość dystrybucji informacji routingowych pomiędzy różnymi wirtualnymi tablicami routingowymi (ang. VRF route leaking).	Tak	Nie
13	Wszystkie przełączniki muszą obsługiwać protokół BFD.	Tak	Nie

## 6. Wdrożenie systemu

W ramach wdrożenia Systemu Wykonawca zobowiązany jest do:

- 1) realizacji planu wdrożenia zawartego w punkcie 6.1
- 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, 61-139 Poznań

### 6.1. Ramowy plan wdrożenia

Plan realizacji przedmiotu zamówienia:

Lp.	Element wdrożenia	Dni robocze* (terminy maksymalne)
<b>OPRACOWANIE DOKUMENTACJI TECHNICZNEJ</b>		
1.	Wykonanie Dokumentacji Technicznej zgodnie z wytycznymi zawartymi w punkcie 6.4	10 dni od daty złożenia zapotrzebowania przez zamawiającego, ale przed rozpoczęciem dostawy
2.	Weryfikacja dokumentacji technicznej przez Zamawiającego	3 dni robocze od dnia jej dostarczenia przez Wykonawcę
3.	Naniesienie poprawek w dokumentacji technicznej przez Wykonawcę zgodnie z wytycznymi Zamawiającego	2 dni robocze od dnia zgłoszenia konieczności dokonania poprawek przez Zamawiającego
<b>DOSTAWA I INSTALACJA SYSTEMU</b>		



4.	Dostawa urządzeń i oprogramowania	40 dni roboczych od daty złożenia zapotrzebowania przez Zamawiającego
5.	<p>Instalacja i konfiguracja obejmująca 4 etapy:</p> <ol style="list-style-type: none"> <li>1. Instalacja urządzeń w szafach telekomunikacyjnych zlokalizowanych w obiektach Zamawiającego wraz z ułożeniem okablowania i podłączenie urządzeń do przełączników sieciowych i zasilania.</li> <li>2. Instalacja i konfiguracja logiczna całego środowiska (serwery wraz z systemem do zarządzania, platforma wirtualizacyjna wraz z modułami, przełączniki sieciowe, pozostałe elementy) zgodnie z wykonaną wcześniej przez Wykonawcę i zaakceptowaną przez Zamawiającego Dokumentacją Techniczną.</li> <li>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 Zamawiającego Dokumentacją Techniczną.</li> <li>4. Przygotowanie i przeprowadzenie przez Wykonawcę testów weryfikacyjnych instalacji i konfiguracji Systemu zgodnie z wytycznymi w punkcie 6.6. Przygotowanie raportu podsumowującego wyniki testów.</li> </ol>	5 dni roboczych od daty dostarczenia urządzeń i oprogramowania do siedziby Zamawiającego
<b>OPRACOWANIE DOKUMENTACJI POWYKONAWCZEJ</b>		
6.	Wykonanie Dokumentacji Powykonawczej przez Wykonawcę zgodnie z wytycznymi w punkcie 6.5	5 dni roboczych po zakończeniu instalacji i konfiguracji Systemu u Zamawiającego
7.	Weryfikacja Dokumentacji Powykonawczej przez Zamawiającego	2 dni robocze od dnia jej dostarczenia przez Wykonawcę
8.	Naniesienie poprawek do Dokumentacji Powykonawczej przez Wykonawcę zgodnie z wytycznymi Zamawiającego	2 dni robocze od dnia zgłoszenia konieczności dokonania poprawek przez Zamawiającego
<b>WERYFIKACJA POPRAWNOŚCI INSTALACJI SYSTEMU (PRZEPROWADZENIE TESTÓW)</b>		
9.		3 dni robocze zakończeniu instalacji i

	Przegotowanie przez Wykonawcę planu testów akceptacyjnych i wydajnościowych instalacji i konfiguracji Systemu zgodnie z wytycznymi w punkcie <b>6.6.2</b> i <b>6.6.3</b>	konfiguracji Systemu u Zamawiającego
10.	Weryfikacja planu testów akceptacyjnych i wydajnościowych przez Zamawiającego	2 dni robocze od dnia jego dostarczenia przez Wykonawcę
11.	Naniesienie poprawek na planie testów akceptacyjnych i wydajnościowych przez Wykonawcę zgodnie z wytycznymi Zamawiającego	2 dni robocze od dnia zgłoszenia konieczności dokonania poprawek przez Zamawiającego
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.	Przegotowanie przez Wykonawcę planu testów odbiorczych instalacji i konfiguracji Systemu zgodnie z wytycznymi w punkcie <b>6.6.4</b>	3 dni robocze od zgłoszenia gotowości do testów odbiorczych przez Zamawiającego
14.	Weryfikacja planu testów odbiorczych przez Zamawiającego	2 dni robocze od dnia jego dostarczenia przez Wykonawcę
15.	Naniesienie poprawek na planie testów odbiorczych przez Wykonawcę zgodnie z wytycznymi Zamawiającego	2 dni robocze od dnia zgłoszenia konieczności dokonania poprawek przez Zamawiającego
16.	Wykonanie testów odbiorczych przez Wykonawcę i Zamawiającego i wykonanie przez Wykonawcę raportu podsumowującego wyniki testów	3 dni robocze
17.	Podpisanie przez Zamawiającego protokołu zdawczo - odbiorczego przedmiotu zamówienia	3 dni robocze po pozytywnym zakończeniu testów odbiorczych u Zamawiającego



## POZNAŃSKIE CENTRUM SUPERKOMPUTEROWO - SIECIOWE

PN 14/02/2023 – system wizualizacji oraz środowisko serwerowe QKD  
\*przez „dzień roboczy” Zamawiający rozumie poniedziałek, wtorek, środę, czwartek i piątek z wyjątkiem dni ustawowo wolnych od pracy w Polsce.

### 6.2. Dostawa i instalacja

Wykonawca zobowiązany jest dostarczyć wszelkie urządzenia i oprogramowanie będące przedmiotem zamówienia do lokalizacji Zamawiającego oraz wykonania ich fizycznej instalacji w tej lokalizacji z uwzględnieniem warunków opisanych poniższych podpunktach (6.2.1, 6.2.2, 6.2.3).

#### 6.2.1. Ogólne wytyczne dotyczące dostawy i instalacji

- 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 m<sup>3</sup> 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.





## POZNAŃSKIE CENTRUM SUPERKOMPUTEROWO - SIECIOWE

PN 14/02/2023 – system wizualizacji oraz środowisko serwerowe QKD

- 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 m<sup>3</sup> 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.

### 6.2.2. Warunki instalacji zapewnione przez Zamawiającego

- 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 teletechnicznych.
- 3) Każda z szaf teletechnicznych posiada wymiary:
  - i. wysokość 47U,
  - ii. szerokość 80cm,
  - iii. głębokość 120cm,
  - iv. nośność szafy 1500kg,
  - v. nośność belek/profilu nośnych (pionowych) 1500kg,
  - vi. odległość między belkami umożliwiającą montaż urządzeń z uchwytyami 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. 18 gniazd C13,
  - iv. 6 gniazd C19.
- 6) Sumaryczne chłodzenie na cały kiosk o mocy 200kW, realizowane za pomocą klimatyzatorów międzyrzędowych.
- 7) W kiosku znajduje się dedykowany łącznik z włóknami światłowodowymi na potrzeby komunikacji z infrastrukturą Zamawiającego (na potrzeby dostępu do infrastruktury Zamawiającego oraz systemu zdalnego) – parametry łącznika:
  - i. złącza SC/APC;
  - ii. włókna SM w kablu to G.652d firmy Corning E9/125 SMF-28e+





## POZNAŃSKIE CENTRUM SUPERKOMPUTEROWO - SIECIOWE

PN 14/02/2023 – system wizualizacji oraz środowisko serwerowe QKD

6.2.3. Szczegółowe wymagania dotyczące dostawy i instalacji, które musi spełnić  
Wykonawca

- 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 duplexowe (dwa włókna), jednomodowe lub wielomodowe, złącze typu LC,
  - iii. Zamawiający nie dopuszcza możliwości stosowania kabli typu „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, dostępu do infrastruktury sieciowej Zamawiającego z dostarczonych serwerów,
  - ii. zarządzania dostarczoną infrastrukturą Out-of-Band wszystkich dostarczonych urządzeń posiadających taką funkcjonalność
- 4) Zamawiający przewiduje następujące kategorie przełączników sieciowych podzielone wg. ich przeznaczenia, które nie będą ze sobą współdzielone:
  - i. „25G” – na potrzeby realizacji infrastruktury sieciowej opisanej w ustępie **3)i**, tj. przełączniki, do których muszą być podłączone dostarczone serwery oraz do których muszą być podłączone przełączniki „1G”. Przełączniki te są również przeznaczone do integracji ze szkieletową infrastrukturą sieciową i usługową Zamawiającego.
  - ii. „1G” – na potrzeby realizacji infrastruktury sieciowej opisanej w ustępie **3)ii**
- 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) Infrastruktura podana w ustępie **3)i** zakłada wyposażenie w dwa przełączniki typu „25G” pracujące w trybie redundantnym
- 7) Dostarczone serwery na potrzeby realizacji infrastruktury opisanej w ustępie **3)i** muszą zostać podłączone interfejsami 25G w sposób redundantny do obu przełączników sieciowych typu „25G” w celu zapewnienia bezprzerwowego dostępu do serwera w przypadku awarii jednego z tych przełączników do którego jest podłączony. Każde połączenie musi zostać zrealizowane z wykorzystaniem włókien światłowodowych zgodnie z wymaganiami opisanymi w ustępie 2).







## POZNAŃSKIE CENTRUM SUPERKOMPUTEROWO - SIECIOWE

PN 14/02/2023 – system wizualizacji oraz środowisko serwerowe QKD

- 8) Przełączniki „25G” muszą zostać połączone ze sobą za pomocą 2 (dwóch) połączeń o przepustowości 100G, każde z wykorzystaniem włókien światłowodowych zgodnie z wymaganiami opisanymi w ustępie 2).
- 9) Każdy z przełączników typu „25G” musi zostać połączony w sposób redundantny do obu przełączników typu „1G” za pomocą połączenia o przepustowości 10G, każde z wykorzystaniem włókien światłowodowych zgodnie z wymaganiami opisanymi w ustępie 2).
- 10) Oprócz modułów optycznych służących do połączenia z dostarczonymi serwerami, połączenia między sobą oraz z przełącznikami „1G”, każdy przełącznik „25G” musi zostać dodatkowo wyposażony w następujące moduły optyczne zgodne i poprawnie pracujące z zaoferowanymi przełącznikami:
  - i) 2 x 100GEth LR
  - ii) 10 x 25GEth LR
  - iii) 4 x 10GEth LR

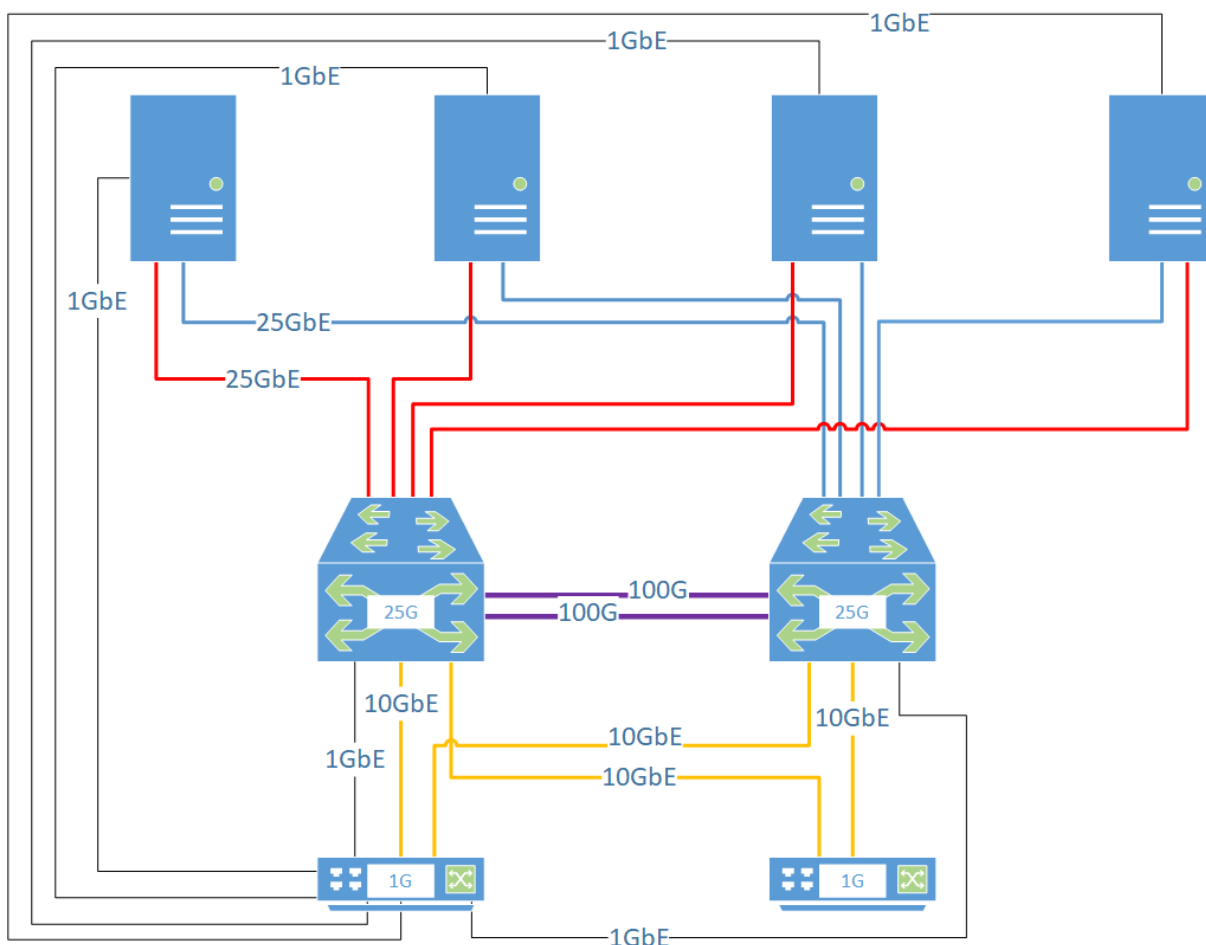
Każdy z dostarczonych modułów musi umożliwiać realizację połączenia o danej przepustowości z wykorzystaniem patchordów duplexowych (dwa włókna), jednomodowych, ze złączem LC na odległość co najmniej 2km.

- 11) Infrastruktura podana w ustępie 3)ii zakłada wyposażenie w dwa przełączniki typu „1G” pracujące w trybie redundantnym. Każdy z przełączników „1G” musi zostać połączony z każdym z przełączników „25G” za pomocą 1 (jednego) połączenia o przepustowości 10G z wykorzystaniem włókien światłowodowych zgodnie z wymaganiami opisanymi w ustępie 2).
- 12) Oprócz modułów optycznych służących do połączenia z przełącznikami „25G”, każdy z dwóch przełączników „1G” infrastruktury podanej w ustępie 3)ii musi zostać wyposażony w następujące dodatkowe, nie wykorzystywane do połączeń, moduły optyczne zgodne i poprawnie pracujące z zaoferowanymi przełącznikami:
  - i) 2 x 10GEth LR

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

- 13) Poglądowy schemat wymagań Zamawiającego w zakresie ogólnej architektury systemu (topologii połączeń) przedstawiono na poniższym rysunku:





14) Poza dwoma przełącznikami „1G” dostarczonymi w ramach infrastruktury podanej w ustępie 3)ii Zamawiający wymaga dodatkowo dostarczenia 2 przełączników typu „1G” z których każdy musi być wyposażony w następujące moduły optyczne zgodne i poprawnie pracujące z zaoferowanymi przełącznikami:

i) 4 x 10GEth LR

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

15) Wymaga się by wszystkie dostarczone moduły mogły być instalowane w urządzeniu i wyjmowane z urządzenia podczas jego pracy (ang. Hot-Pluggable).

16) Wykonanie wszystkich niezbędnych połączeń teletechnicznych i elektrycznych na potrzeby instalacji dostarczonych urządzeń, w tym także wszystkich wymaganych przewodów ochronnych.

17) Wszystkie dostarczone urządzenia oraz elementy infrastruktury teletechnicznej i elektrycznej muszą być jednoznacznie oznaczone zgodnie z uzgodnionym z Zamawiającym schematem nazewnictwa.

18) Wszystkie dostarczone urządzenia muszą być zainstalowane w sposób zapewniający przepływ powietrza z zewnątrz kiosku do wewnątrz.



## POZNAŃSKIE CENTRUM SUPERKOMPUTEROWO - SIECIOWE

PN 14/02/2023 – system wizualizacji oraz środowisko serwerowe QKD

- 19) Wszystkie połączenia muszą być prowadzone w zgodzie 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.
- 20) Wszystkie dostarczone elementy okablowania muszą być jednoznacznie oznaczone w sposób uzgodniony z Zamawiającym, zgodnie z uzgodnionym z Zamawiającym schematem nazewnictwa.
- 21) Adresacja IP musi zostać zaplanowana w uzgodnieniu z Zamawiającym dla każdego z urządzeń i segmentów sieci.
- 22) Zaplanowanie i wykonanie dedykowanej infrastruktury zarządzania Out-of-Band (pkt. 3)ii przy użyciu przełączników typu „1G”. Każdy rodzaj urządzeń na potrzeby zdalnego dostępu Out-of-Band musi posiadać oddzielną adresację IP (adresacja musi zostać uzgodniona z Zamawiającym na etapie planowania).
- 23) Wykonania integracji wdrożonego Systemu, w szczególności platformy wirtualizacyjnej, infrastruktury sieciowej zdefiniowanej w ustępie 3) z infrastrukturą Zamawiającego zainstalowaną w siedzibie Zamawiającego (uzgodnienie adresacji, dostarczenie i ułożenie okablowania). Należy wykonać integrację następujących segmentów:
  - i. dostępu do dostarczonych zasobów serwerowych z Internetu przy pomocy dwóch redundantnych połączeń z wykorzystaniem przełączników typu „25G”
  - ii. dostępu do interfejsów zarządzania Out-of-Band z Internetu musi zostać zrealizowany przy użyciu połączeń z wykorzystaniem przełączników typu „1G”

Integracji należy dokonać z wykorzystaniem łącznika opisanego w punkcie 6.2.2. Na potrzeby integracji należy dostarczyć patchordy zgodnie z wytycznymi z ustępu 2) oraz informacjami nt. złącz w łączniku. Łączna długość każdego połączenia nie przekroczy 2 km.
- 24) Dostarczenie wszelkiego okablowania zasilającego niezbędnego do realizacji wdrożenia Systemu zgodnie z zapisami SWZ i Dokumentacją Techniczną.
- 25) Wykonanie wszystkich niezbędnych połączeń, w tym także połączeń przewodów ochronnych.
- 26) Wszystkie dostarczone i instalowane urządzenia muszą być jednoznacznie oznaczone zgodnie z uzgodnionym w ramach Dokumentacji Technicznej schematem nazewnictwa.
- 27) Wszystkie dostarczone i instalowane elementy okablowania muszą być jednoznacznie oznaczone zgodnie z uzgodnionym w ramach Dokumentacji Technicznej schematem nazewnictwa.
- 28) Wszystkie dostarczone urządzenia muszą być zainstalowane w sposób zapewniający przepływ powietrza z zewnątrz kiosku do wewnątrz.
- 29) Przełączniki sieciowe muszą być zainstalowane na tyle szafy patrząc od zewnątrz kiosku i przepływ powietrza musi odbywać się w kierunku od tyłu urządzenia do frontu (porty we/wy).





PN 14/02/2023 – system wizualizacji oraz środowisko serwerowe QKD

- 30) 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.
- 31) Wykonanie wszystkich pozostałych czynności zawartych w niniejszym dokumencie oraz znajdujących się w wykonanej przez Wykonawcę i zaakceptowanej przez Zamawiającego Dokumentacji Technicznej.
- 32) Jeżeli instalowane oprogramowanie lub dostarczany Komponent wymaga przypisania licencji do świadczenia wymaganej funkcjonalności licencja ta musi zostać przypisana oraz aktywowana.

### 6.3. Dokumentacja

- 1) Przygotowane przez Wykonawcę, w terminach wynikających ze planu wdrożenia opisanego w punkcie **6.1**, dokumenty:
  - a) Dokumentacja Techniczna,
  - b) Plany testów zgodnie z wytycznymi opisanymi w punkcie **6.6**,
  - 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 **6.1** 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 **6.1**, od dnia zgłoszenia uwag, natomiast Zamawiający nie później niż w terminie podanym w punkcie **6.1**, 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 **6.1** 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 **6.4** i **6.5**.
- 6) Szczegółowe wytyczne dla testów zostały wskazane punkcie **6.6**.

### 6.4. 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 oparty 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:





## POZNAŃSKIE CENTRUM SUPERKOMPUTEROWO - SIECIOWE

PN 14/02/2023 – system wizualizacji oraz środowisko serwerowe QKD

- a) listę wymagań funkcjonalnych Zamawiającego,
- b) sposób realizacji wymagań funkcjonalnych,
- c) architekturę Systemu,
- 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 3,
- f) architekturę połączeń elementów sieciowych na potrzeby realizacji poszczególnych funkcjonalności
- g) architekturę połączeń wszystkich elementów sieciowych (co najmniej: adresacja IP, diagramy połączeń, sposób realizacji redundancji połączeń pomiędzy urządzeniami),
- h) aranżację poszczególnych elementów w szafach teletechnicznych,
- i) schemat nazewnictwa wszystkich dostarczonych elementów,
- j) schemat nazewnictwa wszystkich wykorzystywanych interfejsów,
- k) plany konfiguracji sieci w tym adresacji, portów itd. (IP design) wszystkich podłączonych do sieci Komponentów,
- l) plany instalacji urządzeń i podłączenia do sieci LAN i zasilania, w tym porty itd. (obwody prądowe),
- m) opis integracji, a w tym:
  - i. architektura i sposób zapewnienia zdalnego dostępu do poszczególnych Komponentów,
- n) listę wdrażanych Komponentów wraz z ich ilościami,
- o) szczegółowy wykaz dostarczonych licencji na oprogramowanie,
- p) dokumentacje producentkie wszystkich użytych Komponentów i elementów systemu (może być dostarczona w wersji elektronicznej),
- q) inne, wg uznania Wykonawcy.

### 6.5. Dokumentacja Powykonawcza

Dokumentacja Powykonawcza musi spełniać poniższe wymagania.

- 1) Dokumentacja Powykonawcza musi być opracowana na podstawie założeń zapisanych w Dokumentacji Technicznej (opisanej w punkcie 6.4) 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







## POZNAŃSKIE CENTRUM SUPERKOMPUTEROWO - SIECIOWE

PN 14/02/2023 – system wizualizacji oraz środowisko serwerowe QKD 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 bezpieczeństwa Systemu
  - h) opis konfiguracji elementów Systemu zgodnie z wymaganiami z punktu 6.2.3
  - i) architektura, opis działania oraz parametry HA,
  - j) szczegółowa architektura i konfiguracja wszystkich przewidzianych integracji,
  - k) szczegółowy opis procedur eksploatacyjnych, utrzymaniowych i awaryjnych Systemu i wszystkich Komponentów wchodzących w skład Systemu,
  - l) szczegółowy opis monitorowania, raportowania i automatyzacji Komponentów wchodzących w skład Systemu,
  - m) szczegółowy opis i konfiguracja Systemu w zakresie dostępu administracyjnego, uwierzytelniania i autoryzacji dla użytkowników,
  - n) 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:





## POZNAŃSKIE CENTRUM SUPERKOMPUTEROWO - SIECIOWE

PN 14/02/2023 – system wizualizacji oraz środowisko serwerowe QKD

- a) model urządzenia, parametry sprzętowe (np. kontrolery, półki dyskowe, dyski, przełączniki, moduły optyczne, itp.), konfigurację pamięci dyskowej (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.

### 6.6. Wytyczne do testów

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.

#### 6.6.1. Testy weryfikacyjne

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





# POZNAŃSKIE CENTRUM SUPERKOMPUTEROWO - SIECIOWE

PN 14/02/2023 – system wizualizacji oraz środowisko serwerowe QKD  
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.

## 6.6.2. 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) tworzenie i zarządzanie wirtualnymi zasobami dyskowymi,
- 6) korzystanie z narzędzenia do monitorowania i rozwiązywania problemów,
- 7) weryfikację poprawności konfiguracji klastra i wykorzystania kompatybilnych Komponentów serwera,





## POZNAŃSKIE CENTRUM SUPERKOMPUTEROWO - SIECIOWE

PN 14/02/2023 – system wizualizacji oraz środowisko serwerowe QKD

- 8) weryfikacja wszystkich elementów serwera i ich parametrów,
- 9) weryfikacja możliwości zarządzania serwerami,
- 10) weryfikacja wszystkich elementów infrastruktury sieciowej,
- 11) weryfikacja możliwości zarządzania poszczególnymi elementami infrastruktury sieciowej,
- 12) weryfikacja poprawności działania usługi zdalnego dostępu do infrastruktury dla administratorów,
- 13) weryfikacja możliwości zarządzania poszczególnymi elementami systemu za pomocą usługi zdalnego dostępu,
- 14) wykonanie kopii zapasowej maszyny wirtualnej,
- 15) 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 przypisaną polityką odporności na awarię minimum jednego hosta,
- 2) symulacje awarii połączenia sieciowego w serwerze,
- 3) symulacje awarii przełącznika LAN,
- 4) wprowadzenie serwera w tryb konserwacji i wyprowadzenie go z tego trybu i obserwacje dostępności wirtualnych maszyn w klastrze,
- 5) symulacje awarii każdego z Komponentów Systemu dla potwierdzenia pełnej redundancji.

### 6.6.3. 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.





## POZNAŃSKIE CENTRUM SUPERKOMPUTEROWO - SIECIOWE

PN 14/02/2023 – system wizualizacji oraz środowisko serwerowe QKD  
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.

#### 6.6.4. 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.







## POZNAŃSKIE CENTRUM SUPERKOMPUTEROWO - SIECIOWE

PN 14/02/2023 – system wizualizacji oraz środowisko serwerowe QKD

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: 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) weryfikacji wydajności w komunikacji maszyna wirtualna z maszyną wirtualną:
  - a) test wydajnościowy w komunikacji IP między maszynami wirtualnymi,
- 4) wykonania kopii zapasowej w środowisku:
  - a) wykonanie i odtworzenie kopii maszyny wirtualnej
- 5) całości Systemu:
  - a) symulacja awarii jednego z torów zasilania dla zasilaczy w urządzeniach,
  - b) symulacja awarii sieci LAN poprzez wyłączenie portów komunikacyjnych LAN.

### 6.7. Odbiory

Odbiór oznacza przeprowadzenie testów odbiorczych oraz potwierdzenie protokołem zdawczo – odbiorczym zgodności przedmiotu zamówienia z warunkami umowy.

Protokolem odbioru przez Zamawiającego podlegać będą:

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





## 7. Gwarancja

### 7.1. 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 Błąd! Nie można odnaleźć źródła odwołania..
- 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,





PN 14/02/2023 – system wizualizacji oraz środowisko serwerowe QKD

- 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.

## 7.2. Opis usługi Gwarancji

### 7.2.1. Diagnostyka i rozwiązywanie problemów

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

### 7.2.2. 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.





# POZNAŃSKIE CENTRUM SUPERKOMPUTEROWO - SIECIOWE

PN 14/02/2023 – system wizualizacji oraz środowisko serwerowe QKD

**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.

### 7.2.3. 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 <sup>1</sup> (przywrócenia normalnego działania Systemu)	Maksymalny czas dostarczenia rozwiązania docelowego <sup>2</sup>	Tryb Serwisowania (godzin na dobę x liczbę dni w tygodniu)
Awaria Krytyczna	8 godzin	8 godzin	10 dni roboczych	24x7





# POZNAŃSKIE CENTRUM SUPERKOMPUTEROWO - SIECIOWE

PN 14/02/2023 – system wizualizacji oraz środowisko serwerowe QKD

Awaria Poważna	24 godziny	8 godzin	20 dni roboczych	24x7
Awaria Istotna	24 godziny	16 godzin	80 dni roboczych	8x5 <sup>3</sup>
Usterka	24 godziny	40 godzin	100 dni roboczych	8x5 <sup>3</sup>

Maksymalny czas reakcji na zgłoszenie	Maksymalny czas dostarczenia rozwiązania docelowego <sup>2</sup>
	Maksymalny czas Rozwiązania Problemu <sup>1</sup> (przywrócenia normalnego działania)

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.

Czas usunięcia awarii nalicza się od momentu zakończenia czasu reakcji na zgłoszenie.

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

<sup>2</sup> – w przypadku zastosowania obejścia

<sup>3</sup> – należy to rozumieć jako tylko w dni robocze

## 7.2.4. Wymiana informacji pomiędzy Zamawiającym a Wykonawcą

1) Strony dopuszczają następujące kanały komunikacyjne:

- system zgłoszeń problemowych Wykonawcy,
- poczta elektroniczna,
- strona WWW,
- systemy VC,
- telefon.

2) Zgłoszenia kierowane przez Zamawiającego za pośrednictwem telefonu, będą również potwierdzane niezwłocznie, poprzez wysłanie e-mail do Wykonawcy, z podaniem czasu zgłoszenia za pośrednictwem telefonu. W takiej sytuacji za czas Zgłoszenia Problemu, uważa się moment zgłoszenia za pośrednictwem telefonu.

3) Wykonawca zobowiązany jest przyjmować i rejestrować Zgłoszenia Problemów składane przez Zamawiającego w trybie 24/7/365.

4) Wykonawca będzie aktualizował wszelkie dane o Problemie takie jak postępy prac, statusy, priorytet, typ w systemie zgłoszeń problemowych, a cała historia korespondencji oraz statusów będzie dostępna dla Zamawiającego.

5) Wszelka korespondencja między stronami będzie odbywała się w języku polskim.

6) Szczegóły przekazania dostępu do systemu zgłoszeń problemowych Wykonawcy zostaną przekazane Zamawiającemu w trybie roboczym.







## POZNAŃSKIE CENTRUM SUPERKOMPUTEROWO - SIECIOWE

PN 14/02/2023 – system wizualizacji oraz środowisko serwerowe QKD

- 7) Strony, w trakcie trwania usługi gwarancji, mogą umówić się na integrację między systemami zgłoszeń problemowych Wykonawcy i Zamawiającego. Szczegóły zostaną uzgodnione w trybie roboczym.

### 7.2.5. 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.

### 7.2.6. 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.

### 7.2.7. Rozwiązanie problemu

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





## 7.2.8. Czas rozwiązania problemu

- 1) Czas rozwiązania problemu liczony jest oddzielnie dla każdego zgłoszenia problemu.
- 2) Czas rozwiązania problemu liczony jest od momentu zgłoszenia problemu do momentu poinformowania Zamawiającego przez Wykonawcę o rozwiązaniu problemu.
- 3) Czas potwierdzenia przez Zamawiającego do Wykonawcy rozwiązania problemu nie liczy się do czasu rozwiązania problemu – na ten czas Wykonawca zawiesza zgłoszenie problemu.
- 4) W przypadku skierowania przez Zamawiającego do Wykonawcy informacji o braku rozwiązania problemu, tj. dalszego występowania problemu, Wykonawca odwołuje zgłoszenie problemu i czas rozwiązania problemu jest kontynuowany o czas oczekiwania na dostęp do urządzeń.
- 5) Jeżeli Wykonawca uchybi terminowi rozwiązania problemu, wskazanemu w punkcie **7.2.3**, 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

## 7.2.9. 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 **7.2.3**
- 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.

## 7.2.10. 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.





PN 14/02/2023 – system wizualizacji oraz środowisko serwerowe QKD

- 4) W przypadku skierowania przez Zamawiającego do Wykonawcy informacji o braku przywrócenia Systemu, tj. dalszego występowania problemu, Wykonawca odwołuje zgłoszenie problemu i czas przywrócenia Systemu jest kontynuowany.
- 5) W przypadku, gdy w celu przywrócenia systemu występuje konieczność wymiany lub naprawy urządzeń, na czas wymiany lub naprawy urządzeń, Zamawiający ma obowiązek zapewnić dostęp do Urządzeń upoważnionym pracownikom Wykonawcy. W przypadku braku takiego dostępu, czas przywrócenia systemu odpowiednio wydłuża się o czas oczekiwania na dostęp do urządzeń.
- 6) Zgłoszenie problemu po przywróceniu Systemu zostaje ustawione w odpowiedni stan ze stosowną adnotacją, do momentu ostatecznego rozwiązania problemu, zgodnie z czasami określonymi w punkcie **7.2.3**.

#### 7.2.11. 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 **7.2.4**, 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.

#### 7.2.12. 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 **7**,
  - 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,





## POZNAŃSKIE CENTRUM SUPERKOMPUTEROWO - SIECIOWE

PN 14/02/2023 – system wizualizacji oraz środowisko serwerowe QKD

- 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

### 7.2.13. 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





## 7.2.14. Szczegółowe wymagania gwarancji dotyczące elementów Systemu

W ramach usługi gwarancji, Wykonawca zobowiązany jest do:

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

