Załącznik nr 1.1 do SIWZ

Szczegółowy opis przedmiotu zamówienia

dla zamówienia na dostawę i wdrożenie infrastruktury serwerowej do długoterminowego zachowania i prezentacji zdigitalizowanych zbiorów piśmiennictwa i obiektów 3D Biblioteki Śląskiej w Katowicach

realizowanego w ramach projektu pn.: „Śląskie Digitarium. Digitalizacja i udostępnianie zasobów instytucji kultury województwa śląskiego”,

Zadanie 1 - serwery, macierze, urządzenia sieciowe, backup

Katowice, dnia 27.02.2020r.

SPIS TREŚCI

1. Serwery i macierze dyskowe.

1.1 Szafa dystrybucyjna 19" z modułami PDU – ilość 4 szt.

Lp.	Nazwa elementu/cechy	Wymagane minimalne parametry techniczne
1.	Pojemność	Szafa musi być dostosowana do montowania urządzeń o rozmiarze 19". Szafa musi mieścić elementy o łącznej wysokości 42U. Głębokość szafy nie mniejsza niż 1000 mm. Szerokość szafy nie mniejsza niż 800mm.
2.	Wentylacja	W szafie musi być zamontowany panel wentylacyjny z co najmniej 4 wentylatorami oraz czujnikiem temperatury pozwalającym na uruchamianie panelu przy odpowiedniej temperaturze.
3.	Drzwi	Drzwi w szafie muszą być perforowane z możliwością otwarcia do 180 stopni.
4.	Ściany boczne i tylne	Ściana tylna musi być perforowana. Ściany boczne muszą być zdejmowane. Ściana tylna musi być zdejmowana. Musi istnieć możliwość trwałego złączenia szaf bokami w celu zapewnienia stabilności i estetyki zespołu szaf.
5.	Stabilizacja	Jeżeli producent szafy tego wymaga, szafa może zawierać stabilizator.
6.	Zasilanie	Szafa musi zawierać niezbędną ilość modułów PDU oraz gniazd dla podłączenia dostarczonego sprzętu komputerowego do zasilania..
7.	Okablowanie	Zamawiający musi dostarczyć niezbędne elementy do podłączenia całego sprzętu komputerowego w tym m.in. okablowanie, elementy stałe, itp. Szafa powinna być wyposażona w elementy umożliwiające prowadzenie kabli w pionie i w poziomie, które służą do organizacji przestrzeni w szafach. Panele porządkujące 19" wyposażone w szczotki, zatrzaski oraz pierścienie, aby zapewnić

		optymalną ochronę kabli krosowych.
8.	Dostawa	Trzy szafy muszą zostać dostarczone i zamontowane w budynku Biblioteki Śląskiej przy Placu Rady Europy 1 oraz jedna szafa w budynku Biblioteki Śląskiej na ul. Ligonia 7. Szafa rack w lokalizacji zapasowej w budynku Biblioteki Śląskiej na ul. Ligonia 7 musi zostać dostarczona i zamontowana na co najmniej 10 centrymentrowych dedykowanych do szaf rack cokołach.

1.2 Serwer fizyczny systemu wysokiej dostępności (12 szt) wraz ze stanowiskiem dostępu i zarządzania.

Lp.	Nazwa elementu/cechy	Wymagane minimalne parametry techniczne
1.	Ogólne	Środowisko systemu wysokiej dostępności będzie pracować w oparciu o serwery rack w ilości 12 serwerów fizycznych w ramach których planuje się utworzyć 24 serwery wirtualne.
2.	Obudowa	Obudowa typu rack o wysokości max 1U z możliwością instalacji min. 8 dysków 2.5" Hot-Plug wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych oraz organizatorem do kabli.
3.	Definicja serwera	Przez serwer zamawiający rozumie pojedynczą płytę główną wraz z procesorami, pamięcią operacyjną, dyskami i kontrolerami dysków oraz interfejsami do komunikacji co najmniej z siecią 10GbE, 16Gb/s FC.
4.	Płyta główna	Płyta główna z możliwością zainstalowania minimum dwóch procesorów.
5.	Chipset	Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych
6.	Wydajność	Zainstalowane dwa procesory wielordzeniowe klasy x86 dedykowane do pracy z zaoferowanym serwerem umożliwiające osiągnięcie wyniku min. 36000 punktów w teście Passmark CPU Multiple CPU Systems zgodnie z załączonym plikiem „PassMark Software - CPU Benchmarks - Multiple CPU Systems_2020.01.03.pdf”.
7.	Pamięć operacyjna RAM	Sumarycznie 256GB DDR4 RDIMM 2933MT/s, na płycie głównej musi znajdować się minimum 24 slotów przeznaczonych do instalacji pamięci. Płyta główna musi umożliwiać obsługę do 3TB pamięci RAM.RAM.
8.	Zabezpieczenie pamięci RAM	Advanced ECC, Online Spare lub technologia równoważna.

9.	Gniazda PCI	Minimum trzy sloty generacji 3, w tym minimum 2 x16.
10.	Kontroler RAID	Sprzętowy kontroler dyskowy posiadający minimum 1 GB nieulotnej pamięci Cache, obsługujący co najmniej 8 dysków SAS. Wymagane możliwe konfiguracje poziomów RAID: 0, 1, 5, 10, 50.
11.	Obudowa na dyski	Możliwość zainstalowania minimalnie 8 dysków w wewnętrznych zatokach serwera. Możliwość jednoczesnej instalacji dysków SAS, SATA i SSD. typu Hot-Swap/Plug.
12.	Dysk twardy	Zainstalowane 2x480 GB SSD Read Intensive. Możliwość instalacji modułu dedykowanego dla hypervisora wirtualizacyjnego
13.	Interfejs sieciowe	Cztery interfejsy sieciowe 10Gb Ethernet w standardzie Base-T. Zainstalowane dwa interfejsy FC16Gb/s.
14.	Zasilacze	Redundantne zasilacze Hot Plug o mocy dopasowanej do samodzielnego zapewnienia zasilania dla całego serwera, pracujące w sieci 230V 50Hz.
15.	Wentylatory	Redundantne.
16.	Napęd optyczny	Możliwość zamontowania wbudowanego lub zewnętrznego DVD-ROM.
17.	Wbudowane porty	Min. 3 portów USB 3.0, 4 porty RJ45, 1 port VGA.
18.	Karta Grafiki	Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1920x1200.
19.	Karta Zarządzania	Niezależna od systemu operacyjnego, zintegrowana z płytą główną serwera lub jako dodatkowa karta w slocie PCI Express, jednak nie może ona powodować zmniejszenia minimalnej liczby gniazd PCIe w serwerze, posiadająca minimalną funkcjonalność: • monitorowanie podzespołów serwera: temperatura, zasilacze, wentylatory, procesory, pamięć RAM, kontrolery macierzowe i dyski(fizyczne i logiczne), karty sieciowe

		• wparcie dla agentów zarządzających oraz możliwość pracy w trybie bezagentowym – bez agentów zarządzania instalowanych w systemie operacyjnym z generowaniem alertów SNMP • dostęp do karty zarządzającej poprzez: - dedykowany port RJ45 z tyłu serwera, - przez współdzielony port zintegrowanej karty sieciowej serwera, • dostęp do karty możliwy: - z poziomu przeglądarki webowej (GUI), - z poziomu linii komend zgodnie z DMTF System Management Architecture for Server Hardware, Server Management Command Line Protocol (SM CLP), - z poziomu skryptu (XML/Perl), - poprzez interfejs IPMI 2.0 (Intelligent Platform Management Interface). • wbudowane narzędzia diagnostyczne, • zdalna konfiguracji serwera(BIOS) i instalacji systemu operacyjnego, • wbudowany mechanizm logowania zdarzeń serwera i karty zarządzającej w tym włączanie/wyłączanie serwera, restart, zmiany w konfiguracji, logowanie użytkowników, • przesyłanie alertów poprzez e-mail • obsługa zdalnego serwera logowania (remote syslog), • wirtualna zadalna konsola, tekstowa i graficzna, z dostępem do myszy i klawiatury i możliwością podłączenia wirtualnych napędów FDD, CD/DVD i i wirtualnych folderów, • mechanizm przechwytywania, nagrywania i odtwarzania sekwencji video dla ostatniej awarii i ostatniego restartu serwera a także nagrywanie na żądanie, • monitorowanie zasilania oraz zużycia energii przez serwer w czasie rzeczywistym z możliwością graficznej prezentacji, • konfiguracja maksymalnego poziomu pobieranej mocy przez serwer (capping), • zdalna aktualizacja oprogramowania (firmware),

		• możliwość równoczesnej obsługi przez 6 administratorów, • autentykacja dwuskładnikowa (Kerberos), • wsparcie dla Microsoft Active Directory, • obsługa SSL i SSH, • enkrypcja AES/3DES lub TLS dla zdalnej konsoli, • wsparcie dla IPv4 oraz iPv6, obsługa SNMP v3 • możliwość autokonfiguracji sieci karty zarządzającejj (DNS/DHCP).
20.	Certyfikaty	Serwer musi posiadać deklarację CE. Serwer musi być wyprodukowany zgodnie z normą ISO-9001 oraz ISO-14001 lub równoważne. Oferowany serwer musi znajdować się na liście kompatybilności producenta systemu operacyjnego dostarczonego wraz z serwerem. Oferowany model serwera musi być certyfikowany co najmniej dla systemów operacyjnych: RHEL, SLESoraz systemów wirtualizacyjnych, minimum VMware,
21.	System operacyjny	Wraz z każdym serwerem należy dostarczyć co najmniej 5 letnią subskrypcję/wsparcie na oprogramowanie z rodziny systemów operacyjnych linux klasy enterprise dla ilości CPU, w które wyposażony jest dostarczony serwer. Subskrypcja/wsparcie musi obejmować wszystkie pakiety oprogramowania z aktualnie dostępną dystrybucją oprogramowania z rodziny systemów operacyjnych linux klasy enterprise. Dostarczone subskrypcje muszą uprawniać Zamawiającego do dostępu do najnowszych wersji instalacyjnych oprogramowania z rodziny systemów operacyjnych linux klasy enterprise w formie dystrybucji. Wymagany jest dostęp do bazy wiedzy o dostarczonym oprogramowaniu z rodziny systemów operacyjnych linux klasy enterprise, co najmniej w zakresie znanych błędów i publikowanych poprawek, poprzez dedykowany portal kliencki. Wymagany jest dostęp do bazy wiedzy o dostarczonym oprogramowaniu z rodziny systemów operacyjnych linux klasy enterprise, co najmniej w zakresie znanych błędów i publikowanych poprawek, poprzez dedykowany portal kliencki.
22.	Dostawa	Serwery muszą zostać dostarczone i zamontowane w budynku Biblioteki Śląskiej przy Placu Rady Europy 1.

		Wraz z dostawą musi zostać dostarczony niezbędny zestaw do zamontowania serwerów na wysuwanych szynach w szafie dystrybucyjnej 19” w tym m.in., kable zasilające, logiczne, elementy stałe, itp. oraz podłączenia i konfiguracji z pozostałym zamówionym sprzętem komputerowym.

Lp.	Nazwa elementu/cechy	Wymagane minimalne parametry techniczne
1.	Ogólne	Urządzenie KVM wyposażone w 32 porty do podłączenia 19 dostarczonych fizycznych serwerów za pomocą specjalnego zestawu kabli, umożliwiające zarządzanie ww. serwerami przy pomocy konsoli z monitorem 17 calowym, klawiaturą i touchpadem. Dołączone zestawy kabli z odpowiednimi złączami do podłączenia 19 serwerów. Co najmniej 1 złącze Fast Ethernet pozwalające na zdalne zarządzanie poprzez interfejs Web w sieci IP i dostęp do wszystkich 19 podłączonych serwerów. Przełącznik KVM o wysokości nie większej niż 1U montowany do szafy wraz z zestawem do montażu do dostarczonej przez Wykonawcę szafy dystrybucyjnej 19". Konsola z monitorem 17", klawiaturą i touchpadem o wysokości nie większej niż 1U podłączona do przełącznika KVM oraz montowana do dostarczonej przez Wykonawcę szafy dystrybucyjnej 19".
2.	Dostawa	Przełącznik musi zostać dostarczony i zamontowany w budynku Biblioteki Śląskiej przy Placu Rady Europy 1. Wraz z dostawą musi zostać dostarczony niezbędny zestaw do zamontowania przełącznika KVM, konsoli z monitorem na wysuwanych szynach w szafie teleinformatycznej 19” w tym m.in., kable zasilające, logiczne, elementy stałe, itp. . oraz podłączenia i konfiguracji z pozostałym zamówionym sprzętem komputerowym.

1.3 Oprogramowanie do wirtualizacji 12 serwerów fizycznych – ilość 1 szt.

Oprogramowanie do wirtualizacji Vmware Vsphere Enterprise Plus 6 z 5-letnią subskrypcją lub równoważne. Za rozwiązanie równoważne uznaje się takie oprogramowanie, które posiada wbudowane mechanizmy, bez użycia dodatkowych aplikacji, zapewniające:

Lp.	Nazwa elementu/cechy	Wymagane minimalne parametry techniczne
1.	Wirtualizacja mocy obliczeniowej	Zamawiający wymaga dostarczenia oprogramowania do wirtualizacji wraz z licencjami umożliwiającymi uruchamianie wirtualizacji na 12 serwerach fizycznych o łącznej liczbie minimum 24 procesorów fizycznych (dwa procesory na jeden serwer) oraz jednej konsoli do zarządzania całym środowiskiem. Oferowana równoważna warstwa wirtualizacji musi być rozwiązaniem systemowym tzn. musi być zainstalowana bezpośrednio na sprzęcie fizycznym, nie może być częścią innego systemu operacyjnego oraz musi spełniać poniższe warunki: Warstwa wirtualizacji nie może dla własnych celów alokować więcej niż 200MB pamięci operacyjnej RAM serwera fizycznego. Oprogramowanie do wirtualizacji zainstalowane na serwerze fizycznym musi potrafić obsłużyć i wykorzystać procesory fizyczne wyposażone w 576 logicznych wątków oraz do 12TB pamięci fizycznej RAM. Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych 1-128 procesorowych. Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych z możliwością przydzielenia do 6 TB pamięci operacyjnej RAM. Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych, z których każda może mieć 1-10 wirtualnych kart sieciowych. Oprogramowanie do wirtualizacji musi wspierać minimum następujące systemy operacyjne: Windows Server 2012, Windows Server 2016, Windows 7, Windows 8, SLES 12, SLES 11, SLES 10, REHL 7, Solaris 11 ,Solaris 10, Debian, CentOS, FreeBSD, Asianux, Mandriva, Ubuntu, Oracle Linux. Oprogramowanie do wirtualizacji musi umożliwiać przydzielenie większej ilości pamięci RAM dla maszyn wirtualnych niż fizyczne zasoby RAM serwera w celu osiągnięcia maksymalnego współczynnika konsolidacji. Oprogramowanie do wirtualizacji musi umożliwiać udostępnienie maszynie wirtualnej większej ilości zasobów dyskowych niż jest

		fizycznie zarezerwowane na zasobach dyskowych. Oprogramowanie do wirtualizacji musi zapewniać sprzętowe wsparcie dla wirtualizacji zagnieżdżonej, a także instalacji wszystkich funkcjonalności w tym Hyper-V pakietu Windows Server 2012 na maszynie wirtualnej. Oprogramowanie do wirtualizacji musi zapewniać zdalny i lokalny dostęp administracyjny do wszystkich serwerów fizycznych poprzez protokół SSH, z możliwością nadawania uprawnień do takiego dostępu nazwanym użytkownikom bez konieczności wykorzystania konta root. Oprogramowanie do wirtualizacji musi zapewnić możliwość klonowania systemów operacyjnych wraz z ich pełną konfiguracją i danymi. Oprogramowanie do wirtualizacji musi zapewnić możliwość wykonywania kopii migawkowych instancji systemów operacyjnych na potrzeby tworzenia kopii zapasowych bez przerywania ich pracy z możliwością wskazania konieczności zachowania stanu pamięci pracującej maszyny wirtualnej. Oprogramowanie zarządzające musi posiadać możliwość przydzielania i konfiguracji uprawnień z możliwością integracji z usługami katalogowymi, w szczególności: Microsoft Active Directory, Open LDAP. Oprogramowanie do wirtualizacji musi zapewniać możliwość dodawania zasobów w czasie pracy maszyny wirtualnej, w szczególności w zakresie ilości procesorów, pamięci operacyjnej i przestrzeni dyskowej. Oprogramowanie do wirtualizacji musi posiadać funkcjonalność wirtualnego przełącznika (virtual switch) umożliwiającego tworzenie sieci wirtualnej w obszarze hosta i pozwalającego połączyć maszyny wirtualne w obszarze jednego hosta, a także na zewnątrz sieci fizycznej. Pojedynczy przełącznik wirtualny powinien mieć możliwość konfiguracji do 4000 portów. Pojedynczy wirtualny przełącznik musi posiadać możliwość przyłączania do niego dwóch i więcej fizycznych kart sieciowych, aby zapewnić bezpieczeństwo połączenia ethernetowego w razie awarii karty sieciowej. Wirtualne przełączniki musza obsługiwać wirtualne sieci lokalne (VLAN). Oprogramowanie do wirtualizacji musi zapewniać możliwość konfigurowania polityk separacji sieci w warstwie trzeciej, tak aby zapewnić oddzielne grupy wzajemnej komunikacji pomiędzy

		maszynami wirtualnymi. Oprogramowanie do wirtualizacji musi umożliwiać wykorzystanie technologii 10GbE w tym agregację połączeń fizycznych do minimalizacji czasu przenoszenia maszyny wirtualnej pomiędzy serwerami fizycznymi. Oprogramowanie do wirtualizacji musi obsługiwać przełączenie ścieżek LAN (bez utraty komunikacji) w przypadku awarii jednej ze ścieżek. Oprogramowanie do wirtualizacji musi zapewnić możliwość zdefiniowania alertów informujących o przekroczeniu wartości progowych. Oprogramowanie do wirtualizacji musi zapewniać możliwość replikacji maszyn wirtualnych z dowolnej pamięci masowej w tym z dysków wewnętrznych serwerów fizycznych na dowolną pamięć masową w tym samym lub oddalonym ośrodku przetwarzania. Oprogramowanie do wirtualizacji replikujące musi gwarantować współczynnik RPO na poziomie minimum 5 minut. Czas planowanego przestoju usług związany z koniecznością prac serwisowych (np. rekonfiguracja serwerów, macierzy, switchy) musi być ograniczony do minimum. Konieczna jest możliwość przenoszenia maszyn wirtualnych pomiędzy serwerami fizycznymi bez przerywania pracy usług. Oprogramowane do wirtualizacji musi mieć możliwość przenoszenia maszyn wirtualnych w czasie ich pracy pomiędzy serwerami fizycznymi oraz różnymi konsolami do zarządzania wirtualizacją. Rozwiązanie musi posiadać natywne mechanizmy szyfrowania, podczas przenoszenia maszyn wirtualnych, w czasie ich pracy pomiędzy serwerami fizycznymi. Musi zostać zapewniona odpowiednia redundancja i nadmiarowość zasobów tak by w przypadku awarii np. serwera fizycznego usługi na nim świadczone zostały automatycznie przełączone na inne serwery infrastruktury. Oprogramowane do wirtualizacji musi umożliwiać łatwe i szybkie ponowne uruchomienie systemów/usług w przypadku awarii poszczególnych elementów infrastruktury bez utraty danych. Oprogramowane do wirtualizacji musi zapewnić bezpieczeństwo danych mimo poważnego uszkodzenia lub utraty sprzętu lub oprogramowania. Oprogramowane do wirtualizacji musi zapewniać mechanizm bezpiecznego, bezprzerwowego i automatycznego uaktualniania warstwy wirtualizacyjnej wliczając w to zarówno poprawki

		bezpieczeństwa jaki zmianę jej wersji bez potrzeby wyłączania wirtualnych maszyn. Oprogramowane do wirtualizacji musi posiadać co najmniej 2 niezależne mechanizmy wzajemnej komunikacji między serwerami oraz z serwerem zarządzającym, gwarantujące właściwe działanie mechanizmów wysokiej dostępności na wypadek izolacji sieciowej serwerów fizycznych lub partycjonowania sieci. Decyzja o próbie przywrócenia funkcjonalności maszyny wirtualnej w przypadku awarii lub niedostępności serwera fizycznego powinna być podejmowana automatycznie, jednak musi istnieć możliwość określenia przez administratora czasu po jakim taka decyzja jest wykonywana. Oprogramowane do wirtualizacji musi zapewniać pracę bez przestojów dla wybranych maszyn wirtualnych (o maksymalnie dwóch procesorach wirtualnych), niezależnie od systemu operacyjnego oraz aplikacji, podczas awarii serwerów fizycznych, bez utraty danych i dostępności danych podczas awarii serwerów fizycznych. Oprogramowanie do wirtualizacji musi obsługiwać przełączenie ścieżek SAN (bez utraty komunikacji) w przypadku awarii jednej ze ścieżek Oprogramowanie do wirtualizacji musi zapewniać możliwość stworzenia dysku maszyny wirtualnej o wielkości do 62 TB. Oprogramowanie do wirtualizacji musi posiadać wbudowany interfejs programistyczny (API) zapewniający pełną integrację zewnętrznych rozwiązań wykonywania kopii zapasowych z istniejącymi mechanizmami warstwy wirtualizacyjnej. Oprogramowanie do wirtualizacji musi umożliwiać konfiguracje HA dla każdego swojego komponentu w celu unikania awarii pojedynczego elementu. Oprogramowanie do wirtualizacji musi być wspierane przez producenta oferowanego rozwiązania do automatyzacji procesów (Automatyzacja) oraz wirtualizacji sieci (SDN) na wszystkich poziomach wsparcia (L1-L3). Wsparcie musi odbywać się poprzez jednorodny kanał serwisowy (jeden numer telefonów dla wszystkich zgłoszeń, jeden portal www pozwalający zarządzać licencjami i zgłaszać zlecenia serwisowe). Oprogramowanie do wirtualizacji musi wspierać mechanizmy zaawansowanego uwierzytelniania do systemu operacyjnego wirtualnej maszyny za pomocą technologii Smart Card Reader. Wirtualizator musi wspierać TPM 2.0 oznacza to min. że TPM zapewnia mechanizm gwarantujący, że serwer fizyczny uruchomił

		się z włączoną opcją Secure Boot. Po potwierdzeniu, że Secure Boot jest włączone, system gwarantuje, że wirtualizator uruchomił w prawidłowej, niezmienionej formie poprzez weryfikację podpisu cyfrowego. Wirtualizator musi mieć włączenia funkcji "Microsoft virtualization-based security", tzw. Microsoft VBS dla systemów operacyjnych maszyn wirtualnych opatrych o system operacyjny Windows 10 oraz Windows Server 2016. Oprogramowanie do wirtualizacji musi posiadać certyfikację FIPS-140-2 min. dla modułu jądra wirtualizatora odpowiedzialnego za szyfrowanie danych. Wirtualizator musi posiadać funkcjonalność wirtualnego TPM 2.0 dla maszyn wirtualnych Windows 10 oraz Windows 2016. Oznacza to, że punktu widzenia maszyny wirtualnej z systemem operacyjnym Windows 10 lub Windows 2016 wirtualny TPM widziany jest jako standardowy TPM, gdzie można przechowywać bezpiecznie wrażliwe dane np. certyfikaty. Zawartość wirtualnego TPM przechowywana jest w pliku przynależnym do maszyny wirtualnej oraz musi być szyfrowana. W związku z tym wszystkie standardowe funkcjonalności wirtualizatora tj. wysoka dostępność, czy przenoszenie maszyn wirtualnych bez ich wyłączania pomiędzy różnymi serwerami fizycznymi działa prawidłowo. Wirtualizator musi posiadać rolę administratora odpowiedzialnego za zarządzanie kluczami szyfrującymi. Rola ta powinna być odseparowana od roli administratora wirtualizatora. Oznacza, to, że tylko administrator odpowiedziany za szyfrowanie ma dostęp do kluczy szyfrujących oraz może zarządzać procesem szyfrowania w obrębie wirtualizatora. Wirtualizator musi posiadać funkcjonalność szybkiego uruchamiania wirtualizatora po przeprowadzonym procesie jego aktualizacji. Taka funkcjonalność powoduje, że w procesie aktualizacji wirtualizatora, jeśli wymagany jest jego restart, eliminowana jest czasochłonna faza inicjalizacji serwera fizycznego – następuje skrócenia czasu wymaganego do ponownego uruchomienia serwera fizycznego podczas operacji aktualizacji Dostarczone oprogramowanie musi zapewniać możliwość wirtualizacji dla wszystkich dostarczonych w ramach postępowania serwerów. Oprogramowanie do wirtualizacji musi posiadać wsparcie dla natywnych dysków 4K. Oprogramowanie do wirtualizacji musi posiadać mechanizm, który ogranicza dostęp do indywidualnego zarządzania warstwą wirtualizacji na serwerach fizycznych w ramach klastra serwerów w celu utwardzenia/hardening (maksymalnego zwiększenia bezpieczeństwa dostępu) systemu wirtualizacji. Oprogramowanie

		do wirtualizacji musi umożliwiać zarządzanie całą warstwą wirtualizacji z jednego bezpiecznego systemu do zarządzania z kontrolą dostępu. Oprogramowanie do wirtualizacji musi posiadać mechanizmy proaktywnej wysokiej dostępności. Oznacza, to, że jeśli serwer fizyczny posiad funkcję przekazania do wirtualizatora informacji o stanie serwera, to wirtualizatora na podstawie tych danych, wirtualizator jest w stanie, proaktywnie przenieść wszystkie maszyny wirtualne na inne prawidłowo działające serwery fizyczne w klastrze, zanim dojdzie do całkowitej awarii serwera fizycznego. Oprogramowanie do wirtualizacji musi umożliwiać automatyczne równoważenie obciążenia CPU/MEM serwerów fizycznych pracujących jako platforma dla infrastruktury wirtualnej. Oprogramowanie do wirtualizacji musi zapewniać mechanizm pozwalający tworzyć profil (szablon konfiguracji) wybranego serwera wirtualizującego, a następnie wymuszać ten profil/konfigurację na innych serwerach lub sprawdzać zgodność konfiguracji pomiędzy zdefiniowanym wcześniej profilem a wskazanym serwerem fizycznym. Oprogramowanie do wirtualizacji musi umożliwiać utworzenie jednorodnego, wirtualnego przełącznika sieciowego, rozproszonego na wszystkie serwery fizyczne platformy wirtualizacyjnej. Przełącznik taki musi zapewniać możliwość konfiguracji parametrów sieciowych maszyny wirtualnej z granulacją na poziomie portu tego przełącznika. Pojedyncza maszyna wirtualna musi mieć możliwość wykorzystania jednego lub wielu portów przełącznika z niezależną od siebie konfiguracją Przełącznik rozproszony musi współpracować z protokołem NetFlow. Platforma wirtualizacji powinna w ramach przełącznika sieciowego musi zapewniać możliwość integracji z produktami (przełącznikami wirtualnymi) firm trzecich, tak aby umożliwić granularną delegację zadań w zakresie zarządzania konfiguracją sieci do zespołów sieciowych. Przełącznik rozproszony musi umożliwiać funkcjonalność duplikowania ruchu sieciowego dowolnego jego portu wirtualnego na inny port. Przełącznik musi mieć wbudowane mechanizmy składowania kopii konfiguracji, przywracania tej kopii a także mechanizmy automatycznie zapobiegające niewłaściwej konfiguracji sieciowej, które w całości lub w części mogą eliminować błędy ludzkie i utratę łączności sieciowej Oprogramowanie do wirtualizacji musi mieć wbudowany mechanizm

		kontrolowania i monitorowania ruchu sieciowego oraz ustalania priorytetów w zależności od jego rodzaju na poziomie konkretnych maszyn wirtualnych. Oprogramowanie do wirtualizacji musi mieć możliwość uruchamiania fizycznych serwerów z centralnie przygotowanego obrazu poprzez protokół PXE. Oprogramowanie do wirtualizacji musi zapewnić możliwość bieżącego monitorowania wykorzystania zasobów fizycznych infrastruktury wirtualnej (np. wykorzystanie procesorów, pamięci RAM, wykorzystanie przestrzeni na dyskach/wolumenach) oraz przechowywać i wyświetlać dane maksymalnie sprzed roku. Oprogramowanie do wirtualizacji musi 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 oraz pomiędzy różnymi centrami przetwarzania danych platformami wirtualnej. Oprogramowanie do wirtualizacji musi zapewniać pracę bez przestojów dla wybranych maszyn wirtualnych (o maksymalnie czterech procesorach wirtualnych), niezależnie od systemu operacyjnego oraz aplikacji, podczas awarii serwerów fizycznych, bez utraty danych i dostępności danych podczas awarii serwerów fizycznych. Oprogramowanie do wirtualizacji musi posiadać proaktywnie działający mechanizm, który wymigruje wirtualne maszyny po wykryciu potencjalnego problemu z serwerem fizycznym, zanim on ulegnie awarii. Oprogramowanie do wirtualizacji musi mieć wbudowany mechanizm kontrolowania i monitorowania ruchu do pamięci masowych oraz ustalania priorytetów dostępu do nich na poziomie konkretnych wirtualnych maszyn. Oprogramowanie do wirtualizacji musi mieć możliwość grupowania pamięci masowych o podobnych parametrach w grupy i przydzielania ich do wirtualnych maszyn zgodnie z ustaloną przez administratora polityką. Oprogramowanie do wirtualizacji musi umożliwiać udostępnianie pojedynczego urządzenia fizycznego (PCIe) jako logicznie separowane wirtualne urządzenia dedykowane dla poszczególnych maszyn wirtualnych. Oprogramowanie do wirtualizacji musi mieć możliwość równoważenia obciążenia i zajętości pamięci masowych wraz z pełną automatyką i przenoszeniem plików wirtualnych maszyn z bardziej zajętych na mniej zajęte przestrzenie dyskowe lub/i z

		przestrzeni dyskowych bardziej obciążonych operacjami I/O na mniej obciążone. Oprogramowanie do wirtualizacji jako funkcja wirtualizatora (jądra) musi umożliwiać szyfrowanie wirtualnych maszyn oraz szyfrowanie maszyny wirtualnej podczas przenoszenia bez przerywania jej pracy na innych host lub zasób dyskowy. Oprogramowanie do wirtualizacji musi zapewniać mechanizm weryfikujący integralność komponentów systemowych i plików hosta wirtualizującego i wirtualnej maszyny podczas ich uruchamiania (ochrona systemu hypervizor i OS wirtualnej maszyny na wypadek sfałszowania lub podmiany). Oprogramowanie do wirtualizacji musi umożliwiać uruchamianie kontenerów zbudowanych w topologii Docker Image w wirtualnych maszynach. Oprogramowanie do wirtualizacji musi umożliwiać instalowanie uruchamianie i zarządzanie aplikacjami Big Data oraz Hadoop z poziomu platformy wirtualizującej. Oprogramowanie do wirtualizacji musi wspierać technologię rozproszonego udostępniania procesora graficznego Nvidia Grid vGPU do maszyn wirtualnych. Oprogramowanie do wirtualizacji musi wspierać tzw. rozwiązanie trwałej, nieulotnej pamięć (Persistent Memory) zbliżonej do szybkości pamięci DRAM. W ten sposób wirtualizator może udostępnić dla maszyn wirtualnych dyski, które wspierają taką funkcjonalność - ultraszybką pamięć masową zbliżoną do pamięci DRAM. Oprogramowanie do wirtualizacji musi wspierać protokół Remote Direct memory Access (RDMA) poprzez konwergentny Ethernet, lub RoCE (“rocky”) v2, Fiber Channel over Ethernet (FCoE) adapter, i iSCSI rozszerzenie dla RDMA (iSER). Dzięki temu maszyny wirtualne można skonfigurować z wykorzystaniem protokołu RDMA.
2.	Monitorowanie, zarządzanie pojemnością	Oprogramowanie do wirtualizacji musi posiadać centralną konsolę graficzną do zarządzania maszynami wirtualnymi i do konfigurowania innych funkcjonalności. Centralna konsola graficzna powinna działania, jako aplikacja na maszynie wirtualnej, jako gotowa, wstępnie skonfigurowana maszyna wirtualna tzw. virtual appliance. Konsola graficzna musi być dostępna poprzez dedykowanego klienta (za pomocą przeglądarek, minimum IE i Firefox) lub poprzez konsolę graficzną, która zbudowana jest z wykorzystaniem standardu HTML5. Dostęp przez przeglądarkę do konsoli graficznej musi być skalowalny tj. powinien umożliwiać rozdzielenie komponentów na

		wiele instancji w przypadku zapotrzebowania na dużą liczbę jednoczesnych dostępów administracyjnych do środowiska. Oprogramowanie do wirtualizacji musi posiadać natywne mechanizmy do wykonywania kopii zapasowej swojej konfiguracji. Dodatkowo musi być możliwość ustawienia harmonogramu wykonywania kopii zapasowej. Oprogramowanie do wirtualizacji musi posiadać interfejs graficzny do prowadzenia prac administracyjnych w zakresie swojej konfiguracji oraz monitoringu (możliwość monitorowania obciążenia min. vCPU, vRAM, vHDD, sieci, bazy danych). Interfejs graficzny powinien być wykonany w standardzie HTML5. Oprogramowanie do wirtualizacji musi zapewniać natywne mechanizmy HA w niezawodnej architekturze Active-Passive-Witness dla wszystkich składowych komponentów centralnej konsoli graficznej zarządzającej platformą wirtualną.
3.	Monitoring środowiska wirtualnego	Oprogramowanie do wirtualizacji musi zbierać informacji na temat wydajności pod kątem zarządzania pojemnością. Oprogramowanie do wirtualizacji musi w sposób inteligentny przewidywać trendy związane z pojemnością środowiska. Oprogramowanie do wirtualizacji musi posiadać moduł odpowiedzialny za analizę środowiska pod kątem optymalizacji wykorzystania zasobów (CPU, RAM, HDD). Oprogramowanie do wirtualizacji musi mieć możliwość tworzenia unikalnego/dedykowanego Data Center, tzw. będzie możliwe grupowanie obiektów w logiczne zbiory dla których będzie istniała możliwość informowania o alertach, pojemności, ryzykach zgromadzonych w zbiorze obiektach. Obiekty mogą pochodzić z różnych Data Center objętych tym rozwiązaniem. Oprogramowanie do wirtualizacji musi mieć możliwość tworzenia unikalnego/dedykowanego profilu pojemności, tzn. będzie możliwe grupowanie obiektów w logiczne zbiory dla których będzie istniała możliwość informowania o alertach, pojemności, ryzykach zgromadzonych w zbiorze obiektach. Oprogramowanie do wirtualizacji musi mieć możliwość tworzenia scenariuszy pojemnościowych na zasadzie, "co jeśli", dla minimum, co jeśli dodamy kolejne maszyn wirtualne. Rozwiązanie będzie umożliwiało definiowanie poziomów buforów potrzebnych do zachowania wysokiej dostępności. Analiza pojemności będzie odnosiła się zarówno do średniego obciążenia środowiska, jak również do tzw. skoków obciążenia. Oprogramowanie do wirtualizacji musi samodzielnie się uczyć pod względem monitorowanych parametrów wraz z dynamicznymi poziomami powiadomień. Oprogramowanie do wirtualizacji musi monitorować infrastrukturę dostarczonego w ramach tego zamówienia środowiska wirtualnego

		oraz vSAN. Oprogramowanie do wirtualizacji w obrębie monitorowania będzie posiadało rozwiązanie generowania alertów na podstawie szeregu anomalii i symptomów, a nie pojedynczych monitorowanych metryk Oprogramowanie do wirtualizacji będzie dostarczało informacji na temat rekomendowanych działań mających na celu utrzymanie środowiska wirtualnego dostarczonego w ramach tego zamówienia. Oprogramowanie do wirtualizacji musi dostarczać analizę głównego problemu (root-cause) oraz rekomendacji z nimi związane. Oprogramowanie do wirtualizacji powinno posiadać wbudowane integracje z zewnętrznym kolektorem logów i zdarzeń. Oprogramowanie do wirtualizacji będzie posiadało funkcjonalność monitorowania i alertowania na temat zgodności serwerów wirtualnych utworzonych w ramach tego zamówienia z najlepszymi praktykami bezpieczeństwa DISA, FISMA, ISO, CIS, PCI i HIPAA. Oprogramowanie do wirtualizacji musi posiadać bazę wiedzy eksperckiej, która będzie używana przez administratorów, jako źródło dobrych praktyk, sugestii, opisu typowych problemów i błędów. Oprogramowanie do wirtualizacji musi wizualizować online obciążenie środowiska wirtualnego wraz z tzw. funkcjonalnością „drill down”. Oprogramowanie do wirtualizacji musi posiadać funkcjonalność graficznej prezentacji wyników (dashboard). Oprogramowanie do wirtualizacji musi posiadać funkcjonalność aktywnych map graficznych ukazujących elementy lub całe środowisko wirtualne bez konieczności korzystania z usługi wsparcia technicznego producenta do ich wytworzenia. Oprogramowanie do wirtualizacji powinien automatycznie tworzyć linie bazowe określające typowe zachowanie elementów systemu w danym czasie. Oprogramowanie do wirtualizacji będzie miało dostępne mechanizmy planowania pojemności środowiska, w zakresie nie mniejszym niż dodaniu określonej liczby maszyn wirtualnych. Oprogramowanie do wirtualizacji powinno dokonywać predykcji wykorzystania zasobów maszyn fizycznych na podstawie analiz zebranych danych, informacji pochodzących z modułu zarządzania cyklem życia maszyn wirtualnych oraz planów uruchomienia kolejnych serwerów wirtualnych. Oprogramowanie do wirtualizacji powinno dokonywać predykcji wykorzystania zasobów maszyn wirtualnych na podstawie analiz

		zebranych danych. Oprogramowanie do wirtualizacji powinno umożliwiać przeglądanie linii trendu monitorowanych parametrów. System musi umożliwiać tworzenie raportów pojemnościowych dla monitorowanego środowiska, zarówno dla urządzeń fizycznych jak i wirtualnych. System musi umożliwiać monitorowanie w czasie rzeczywistym (przeglądane informacje w trybie rzeczywistym - maksymalne dopuszczalne opóźnienie nie większe niż 5 min.). System musi zbierać oraz prezentować w formie wykresów oraz tabelaryczno-tekstowej zbiorczo oraz osobno dla każdego OS aktualne i historyczne dane dotyczące utylizacji CPU, RAM, HDD oraz interfejsów sieciowych. System musi umożliwiać przeglądanie wszystkich zbieranych statystyk w dowolnie wybranym zakresie czasu w postaci wykresów. System powinien umożliwiać szczegółowe monitorowanie komponentów serwerów fizycznych (CPU, Ethernet, RAM, HDD). System musi wskazywać „wąskie gardła” a także umożliwiać definiowanie progów wydajności i pojemności w celu identyfikacji przypadków wąskich gardeł. Możliwość uruchamiania zadań operatorskich np. modyfikujących parametry maszyn wirtualnych . Oprogramowanie do wirtualizacji musi automatycznie przeszukiwać składy danych w celu wynajdywania nadmiarowo przyznanych zasobów (CPU, RAM, HDD). Alarmowanie sytuacji nietypowych (system monitoringu obserwuje i analizuje zachowanie platformy wirtualnej, na tej podstawie podnosi alarmy o np. nie normalnym w tym dniu zwiększonym obciążeniu elementu platformy wirtualnej). Możliwość dowolnego konfigurowania alertów w środowisku dla różnych grup odbiorców (także z użyciem alertów stworzonych we własnym zakresie). System powinien pozwalać na odczyt wyświetlanych alarmów w środowisku wirtualnym wraz z powiązanymi z nimi poradami eksperckim. System umożliwia definiowanie alertów związanych z: • zarządzaniem pojemnością,

		• zarządzenie wydajnością, • anomaliami w środowisku, • zarządzanie dostępnością. Narzędzie musi mieć możliwość przypisania alertu do administratora/operatora rozwiązującego problem. Oprogramowanie do wirtualizacji musi mieć możliwość realizacji funkcji półautomatycznego równoważenia obciążenia serwerów fizycznych w obrębie klastra logicznego serwerów do zarządzania dostarczoną i utworzoną w ramach tego zamówienia infrastrukturą wirtualną, jak również pomiędzy logicznymi klastrami. Oprogramowanie do wirtualizacji musi mieć możliwość automatycznego i/lub półautomatycznego z konsoli do zarządzania, zmiany parametrów maszyny wirtualnej w zakresie ilości (vCPU, vRAM, uśnięcie snapshot, wyłączenie/włączenie maszyn wirtualnej) na podstawie rekomendacji zmian otrzymywanych przy generowaniu alertu z systemu. Oprogramowanie do wirtualizacji musi mieć możliwość generowania gotowych raportów. Oprogramowanie do wirtualizacji musi integrować się z rozwiązaniem wirtualnym SAN – to znaczy, musi mieć możliwość przeglądu staniu środowiska wirtualnego SAN poprzez panel zarządczy (z ang. Dashboard).
4.	Wymagania licencyjne	Dostarczona licencja musi umożliwiać wirtualizacją serwerów fizycznych z pkt 1.3 z 2 serwerami wirtualnymi (2 „gości”) na każdym serwerze fizycznym. Dostarczona licencja na powyższe oprogramowanie do wirtualizacji musi posiadać możliwość swobodnego przeniesienia na dowolny podmiot wymieniony w umowie ramowej i dowolny serwer fizyczny będący w posiadaniu Zamawiającego (bez ograniczeń licencji OEM). Dostarczona licencja musi być dostępna w modelu licencjonowania na procesor fizyczny (nielimitowana ilość rdzeni procesora). Dostarczone licencje muszą być dostępne w modelu licencjonowania per monitorowany system operacyjny (np. system operacyjny wirtualizatora, system operacyjny typu Windows, Linux, AIX, itp.) z ograniczeniem do maksymalnie 24 monitorowanych źródeł.

1.4 Serwer fizyczny systemu baz danych NoSQL – ilość 6 szt.

Lp.	Nazwa elementu/cechy	Wymagane minimalne parametry techniczne
1.	Ogólne	System baz danych NoSQL to grupa 6 fizycznych serwerów na których zostanie zainstalowanie oprogramowania bazodanowe NoSQL. Ze względu na wymagania wydajnościowe dla tych serwerów nie są zalecane mechanizmy wirtualizacji.
2.	Obudowa	Obudowa typu rack o wysokości max 1U z możliwością instalacji min. 8 dysków 2.5" Hot-Plug wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych wraz z organizatorem do kabli.
3.	Definicja serwera	Przez serwer zamawiający rozumie pojedynczą płytę główną wraz z procesorami, pamięcią operacyjną, dyskami i kontrolerami dysków oraz interfejsami do komunikacji co najmniej z siecią 10GbE, 16Gb/s FC.
4.	Płyta główna	Płyta główna z możliwością zainstalowania minimum dwóch procesorów.
5.	Chipset	Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych.
6.	Wydajność	Zainstalowane dwa procesory wielordzeniowe klasy x86 dedykowany do pracy z zaoferowanym serwerem umożliwiający osiągnięcie wyniku min. 20000 punktów w teście Passmark CPU Multiple CPU Systems zgodnie z załączonym plikiem „PassMark Software - CPU Benchmarks - Multiple CPU Systems_2020.01.03.pdf”.
7.	Pamięć operacyjna RAM	Sumarycznie 128GB DDR4 RDIMM 2933MT/s, na płycie głównej musi znajdować się minimum 24 slotów przeznaczonych do instalacji pamięci. Płyta główna musi mieć możliwość obsługi do 3TB pamięci RAM.
8.	Zabezpieczenie pamięci RAM	Advanced ECC, Online Spare lub technologia równoważna.

9.	Gniazda PCI	Minimum trzy sloty generacji 3, w tym minimum dwa x16.
10.	Kontroler RAID	Sprzętowy kontroler dyskowy posiadający minimum 1 GB nieulotnej pamięci Cache, obsługujący co najmniej 8 dysków SAS. Wymagane możliwe konfiguracje poziomów RAID: 0, 1, 5, 10, 50.
11.	Obudowa na dyski	Możliwość zainstalowania minimalnie 8 dysków w wewnętrznych zatokach serwera. Możliwość jednoczesnej instalacji dysków SAS, SATA i SSD. typu Hot-Swap/Plug.
12.	Dysk twardy	Zainstalowane 2x minimum 1TB SAS 10k 12Gb/s oraz 1x minimum 512GB SSD SAS. Dostarczone dyski SSD muszą być dyskami o parametrze DWPD (drive writes per day) nie mniejszym niż 3.
13.	Interfejs sieciowe	Cztery interfejsy sieciowe 10Gb Ethernet w standardzie Base-T. Zainstalowane dwa interfejsy FC16Gb/s.
14.	Zasilacze	Redundantne zasilacze Hot Plug o mocy dopasowanej do samodzielnego zapewnienia zasilania dla całego serwera, pracujące w sieci 230V 50Hz.
15.	Wentylatory	Redundantne.
16.	Napęd optyczny	Możliwość zamontowania wbudowanego lub zewnętrznego napędu DVD-ROM.
17.	Wbudowane porty	Min. 3 portów USB 3.0, 4 porty RJ45, 1 port VGA .
18.	Karta Grafiki	Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1920x1200.
19.	Karta Zarządzania	Niezależna od systemu operacyjnego, zintegrowana z płytą główną serwera lub jako dodatkowa karta w slocie PCI Express, jednak nie może ona powodować zmniejszenia minimalnej liczby gniazd PCIe w serwerze, posiadająca minimalną funkcjonalność: • monitorowanie podzespołów serwera: temperatura, zasilacze, wentylatory, procesory, pamięć RAM, kontrolery macierzowe i dyski(fizyczne i logiczne), karty sieciowe, • wparcie dla agentów zarządzających oraz możliwość pracy w

		trybie bezagentowym – bez agentów zarządzania instalowanych w systemie operacyjnym z generowaniem alertów SNMP, • dostęp do karty zarządzającej poprzez: • dedykowany port RJ45 z tyłu serwera, • przez współdzielony port zintegrowanej karty sieciowej serwera, • dostęp do karty możliwy: • z poziomu przeglądarki webowej (GUI), • z poziomu linii komend zgodnie z DMTF System Management Architecture for Server Hardware, Server Management Command Line Protocol (SM CLP), • z poziomu skryptu (XML/Perl), • poprzez interfejs IPMI 2.0 (Intelligent Platform Management Interface). • wbudowane narzędzia diagnostyczne, • zdalna konfiguracji serwera(BIOS) i instalacji systemu operacyjnego, • wbudowany mechanizm logowania zdarzeń serwera i karty zarządzającej w tym włączanie/wyłączanie serwera, restart, zmiany w konfiguracji, logowanie użytkowników, • przesyłanie alertów poprzez e-mail • obsługa zdalnego serwera logowania (remote syslog), • wirtualna zadalna konsola, tekstowa i graficzna, z dostępem do myszy i klawiatury i możliwością podłączenia wirtualnych napędów FDD, CD/DVD i USB i i wirtualnych folderów, • mechanizm przechwytywania, nagrywania i odtwarzania sekwencji video dla ostatniej awarii i ostatniego restartu serwera a także nagrywanie na żądanie, • monitorowanie zasilania oraz zużycia energii przez serwer w czasie rzeczywistym z możliwością graficznej prezentacji, • konfiguracja maksymalnego poziomu pobieranej mocy przez serwer (capping), • zdalna aktualizacja oprogramowania (firmware),

		• możliwość równoczesnej obsługi przez 6 administratorów, • autentykacja dwuskładnikowa (Kerberos), • wsparcie dla Microsoft Active Directory, • obsługa SSL i SSH, • enkrypcja AES/3DES lub TLS dla zdalnej konsoli, • wsparcie dla IPv4 oraz iPv6, obsługa SNMP v3, • możliwość autokonfiguracji sieci karty zarządzającejj (DNS/DHCP).
20.	Certyfikaty	Serwer musi posiadać deklaracja CE. Serwer musi być wyprodukowany zgodnie z normą ISO-9001 oraz ISO-14001 lub równoważne. Oferowany serwer musi znajdować się na liście kompatybilności producenta systemu operacyjnego dostarczonego wraz z serwerem. Oferowany model serwera musi być certyfikowany co najmniej dla systemów operacyjnych: RHEL, SLES, Windows Server 2012.
21.	System operacyjny	Wraz z każdym serwerem należy dostarczyć co najmniej 5 letnią subskrypcję/wsparcie na oprogramowanie z rodziny systemów operacyjnych linux klasy enterprise dla ilości CPU, w które wyposażony jest dostarczony serwer. Subskrypcja/wsparcie musi obejmować wszystkie pakiety oprogramowania z aktualnie dostępną dystrybucją oprogramowania z rodziny systemów operacyjnych linux klasy enterprise. Dostarczone subskrypcje muszą uprawniać Zamawiającego do dostępu do najnowszych wersji instalacyjnych oprogramowania z rodziny systemów operacyjnych linux klasy enterprise w formie dystrybucji. Wymagany jest dostęp do bazy wiedzy o dostarczonym oprogramowaniu z rodziny systemów operacyjnych linux klasy enterprise, co najmniej w zakresie znanych błędów i publikowanych poprawek, poprzez dedykowany portal kliencki. Wymagany jest dostęp do bazy wiedzy o dostarczonym oprogramowaniu z rodziny systemów operacyjnych linux klasy enterprise, co najmniej w zakresie znanych błędów i publikowanych poprawek, poprzez dedykowany portal kliencki.
22.	Dostawa	Serwery muszą zostać dostarczone i zamontowane w budynku Biblioteki Śląskiej przy Placu Rady Europy 1.

		Wraz z dostawą musi zostać dostarczony niezbędny zestaw do zamontowania serwerów na wysuwanych szynach w szafie dystrybucyjnej 19” w tym m.in., kable zasilające, logiczne, elementy stałe, itp. . oraz podłączenia i konfiguracji z pozostałym zamówionym sprzętem komputerowym.

1.5 Macierz 1 – centralna macierz dyskowa – ilość 1 szt.

Lp.	Nazwa elementu/cechy	Wymagane minimalne parametry techniczne
1.	Definicja	a) Przez macierz dyskową Zamawiający rozumie zestaw dysków twardych kontrolowanych przez redundantne dedykowane kontrolery macierzowe, bez dodatkowych urządzeń pośrednich, oprogramowania czy też urządzeń wirtualizujących. Udostepnienie zasobu blokowego i NAS musi być realizowane przez jedno urządzenie. Niedopuszczalne jest zastosowanie wielu urządzeń lub kontrolerów łączonych poprzez urządzenia zewnętrzne, tj. przełączniki i zewnętrzne oprogramowanie. b) Zamawiający dopuszcza zaoferowanie rozwiązania składającego się z zasobu dyskowego tj. macierzy dyskowej oraz dedykowanych kontrolerów plikowych tzw. Gateway jednocześnie udostępniających zasoby protokołami plikowymi: CIFS (w tym SMB v3) i NFS (w tym NFS v4), które korzystają z zasobu dyskowego macierzy. Takie rozwiązanie musi pochodzić od jednego producenta tj. macierzy dyskowa, Gateway oraz oprogramowanie.
2.	Typ obudowy	Macierz musi być przystosowana do montażu w szafie rack 19”
3.	Przestrzeń dyskowa	Macierz w dostarczonej konfiguracji musi oferować pojemność netto w warstwach: • SSD/Flash: 50TB, • HDD: 250TB SAS minimum 6G 10K obr./min, Z zastrzeżeniem: • Minimalna ilość dysków/modułów SSD/Flash/NVMe: 14, wszystkie dyski muszą być tego samego typu i pojemności, • Minimalna ilość dysków HDD: 128, • Interfejs dostępowy do dysków minimum 6Gbps, • Minimalny procent przestrzeni/dysków spare: zgodnie z wytycznymi producenta macierzy, • Minimalny poziom zabezpieczenia RAID5 (lub równoważny DP). W dostarczonej konfiguracji macierz musi wspierać rozbudowę do 800 dysków w tym minimum do 800 SSD, wyłącznie przez dodanie

		półek dyskowych i dysków. Zaoferowana macierz powinna wspierać zarówno kompresję jak i deduplikację w locie (dla przestrzeni dyskowej opartej o dyski/moduły SSD/Flash/NVMe). W przypadku, gdy oferowana macierz nie wspiera kompresji i deduplikacji należy zaoferować o 50% więcej dysków/modułów SSD/NVMe/Flash.
4.	Sposób zabezpieczenia danych	Macierz musi pozwalać na równoczesne zabezpieczenie dysków w grupach RAID10, RAID5 (lub równoważny DP (dual parity) oraz RAID6 realizowane sprzętowo za pomocą dedykowanego układu, z możliwością dowolnej ich kombinacji w obrębie oferowanej macierzy w tym z wykorzystaniem puli wszystkich dysków twardych (tzw. wide-striping). Rozłożenie dysków w macierzy musi zapewniać redundancję pozwalającą na nieprzerwaną pracę i dostęp do wszystkich danych w sytuacji awarii pojedynczego komponentu sprzętowego typu: dysk, port, kontroler, zasilacz, kabel.
5.	Tryb pracy kontrolerów macierzowych	Macierz musi posiadać minimum 2 redundantne, dedykowane kontrolery do obsługi dysków i protokołów blokowych w tym FC oraz iSCSI pracujące w trybie Active-Active. Pod określeniem tryb Active-Active Zamawiający rozumie, że zasób jest równolegle dostępny na co najmniej 4 portach należących do co najmniej 2 różnych kontrolerów. Niedopuszczalna jest praca kontrolerów dyskowych w architekturze ALUA. Każdy z kontrolerów musi mieć możliwość prezentacji wszystkich wolumenów utworzonych w ramach całego systemu dyskowego Jeżeli dla realizacji powyższych funkcjonalności wymagane są dodatkowe licencje, lub komponenty sprzętowe należy je dostarczyć dla nominalnej pojemności urządzenia i infrastruktury SAN. Macierz musi posiadać minimum 2 redundantne, dedykowane, zintegrowane lub występujące jako tzw gateway, kontrolery jednocześnie udostępniające zasoby protokołami plikowymi: CIFS (w tym SMB v3) i NFS (w tym NFS v4). Kontrolery realizujące dostęp do zasobów macierzy protokołami plikowymi nie mogą odpowiadać za obsługę dysków wewnętrznych macierzy (dedykowane układy/procesory) i muszą pracować w trybie pojedynczego logicznego klastra Active-Active. W przypadku awarii pojedynczego kontrolera, posiadać możliwość automatycznego przełączania udostępnianych udziałów sieciowych na drugi kontroler. Jeżeli dla realizacji powyższych funkcjonalności wymagane są dodatkowe licencje, lub komponenty sprzętowe należy je dostarczyć dla nominalnej pojemności urządzenia i infrastruktury SAN.

6.	Pamięć cache	Macierz musi być wyposażona w 512GB pamięć cache klasy RAM. Pamięć zapisu musi być mirrorowana (kopie lustrzane) pomiędzy kontrolerami dyskowymi. Dane niezapisane na dyskach (np. zawartość pamięci kontrolera) muszą zostać zabezpieczone w przypadku awarii zasilania za pomocą podtrzymania bateryjnego lub z zastosowaniem innej technologii przez okres nie mniejszy niż 72 godziny. Jeżeli dla realizacji powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla nominalnej pojemności dostarczanego urządzenia.
7.	Interfejsy	Macierz musi być wyposażona, w dedykowane porty dla usług wyszczególnionych poniżej: • 8 portów FC 32 Gbps z wkładkami SFP+ 16Gbps, • 8 portów 10GbE SFP+, do obsługi protokołów plikowych NFS i CIFS, • 2 porty Ethernet GbE dla zarządzania.
8.	Zasilacze	Redundantne, typu Hot-Plug, o mocy dopasowanej do samodzielnego zapewnienia zasilania dla całego urządzenia przy pełnym obłożeniu dyskami, pracujące w sieci 230V 50Hz.
9.	Zarządzenie	Zarządzanie macierzą dyskową musi być możliwe z poziomu interfejsu graficznego oraz linii komend oraz umożliwiać tworzenie skryptów użytkownika wspomagających automatyzację czynności administracyjnych i integrację z oprogramowaniem serwerowym, aplikacjami i oprogramowaniem backupowym. Oprogramowanie do zarządzania musi pozwalać na stałe monitorowanie stanu macierzy oraz umożliwiać konfigurowanie jej zasobów dyskowych. Narzędzie musi pozwalać na obserwację danych wydajnościowych oraz prezentację ich w postaci wykresów oraz czytelnych raportów. Wymagane jest jest bieżące monitorowanie przepustowości i liczby operacji I/O dla interfejsów zewnętrznych, pul dyskowych lub grup RAID, dysków logicznych (LUN) oraz kontrolerów a także prezentowanie danych historycznych z okresu 12mc z wbudowanej bazy danych lub za pomocą dodatkowego oprogramowania producenta dostarczanej macierzy (wymagane dostarczenie). Oprogramowanie zarządzające dostarczane wraz z macierzą musi umożliwiać: monitorowanie stanu technicznego macierzy i na bieżąco informowanie administratora oraz producenta o wykrytych

		awariach i błędach; informowanie o wykorzystaniu zasobów dyskowych macierzy m.in. całkowitej pojemności przestrzeni dyskowej macierzy, wykorzystanej przestrzeni dyskowej, skonfigurowanej przestrzeni przydzielonej do serwerów i nie przydzielonej do serwerów oraz przestrzeni nie skonfigurowanej (wolnej); monitorowanie zasobów wykorzystujących funkcjonalność thin-provisioning i ostrzeganie z wyprzedzeniem o możliwości wyczerpania zasobów. Jeżeli dla realizacji powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla nominalnej pojemności urządzenia i infrastruktury SAN.
10.	Zarządzanie grupami dyskowymi oraz dyskami logicznymi	Macierz musi zapewniać możliwość dynamicznego zwiększania pojemności woluminów logicznych oraz wielkości grup dyskowych (przez dodanie dysków) z poziomu kontrolera macierzowego bez przerywania dostępu do danych. Musi być możliwość zdefiniowania, co najmniej 8000 LUN w ramach oferowanej macierzy dyskowej. Macierz musi wspierać LUN'y o wielkości do 64TB. Każdy LUN/wolumin powinien korzystać z wydajności i pojemności wszystkich dysków fizycznych macierzy (tzw. wide striping). Jeżeli dla realizacji powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla nominalnej pojemności dostarczanego urządzenia.
11.	Thin Provisioning	Macierz musi umożliwiać udostępnianie zasobów dyskowych do serwerów w trybie tradycyjnym, jak i w trybie typu Thin Provisioning. Macierz musi umożliwiać odzyskiwanie przestrzeni dyskowych po usuniętych danych w ramach wolumenów typu Thin. Odzyskiwania przestrzeni musi zachodzić automatycznie bez konieczności uruchamiania dodatkowych procesów na kontrolerach macierzowych - wymagana obsługa standardu T10 SCSI UNMAP. Jeżeli dla realizacji powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla nominalnej pojemności dostarczanego urządzenia.
12.	Wewnętrzne kopie migawkowe	Macierz musi umożliwiać dokonywania na żądanie tzw. migawkowej kopii danych (snapshot, point-in-time) w ramach macierzy za pomocą wewnętrznych kontrolerów macierzowych. Kopia migawkowa wykonuje się bez konieczności wcześniejszego alokowania dodatkowej przestrzeni dyskowej na potrzeby kopii. Zajmowanie dodatkowej przestrzeni dyskowej następuje w momencie zmiany danych na dysku źródłowym lub na jego kopii. Oferowane urządzenie musi wspierać minimum 4000 kopii migawkowych (255 per udział/LUN).

		Macierz musi zapewniać, że zmiana wielkości woluminu źródłowego nie wpłynie na zawartość i dostępność istniejących migawek. Macierz musi zapewniać możliwość tworzenia migawek dla LUN o wielkości, co najmniej 16TB. Jeżeli dla realizacji powyższych funkcjonalności wymagane są dodatkowe licencje lub moduły sprzętowe, należy je dostarczyć dla nominalnej pojemności dostarczanego urządzenia.
13.	Migracja danych w obrębie macierzy	Macierz dyskowa musi umożliwiać migrację danych bez przerywania do nich dostępu pomiędzy różnymi warstwami technologii dyskowych na poziomie części wolumenów logicznych (ang. Sub-LUN). Zmiany te muszą się odbywać wewnętrznymi mechanizmami macierzy. Funkcjonalność musi umożliwiać zdefiniowanie zasobu LUN, który fizycznie będzie znajdował się na min. 3 typach dysków obsługiwanych przez macierz, a jego części będą realokowane na podstawie analizy ruchu w sposób automatyczny i transparentny (bez przerywania dostępu do danych) dla korzystających z tego wolumenu serwerów. Zmiany te muszą być realizowane wewnętrznymi mechanizmami macierzy Jeżeli dla realizacji powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla nominalnej pojemności dostarczanego urządzenia
14.	Integralność danych	Macierz musi oferować sprzętowe wsparcie dla zachowania integralności danych na całej ścieżce transferu (ang. End-to-End) zgodnego ze standardem/specyfikacją T10-DIF/PI (Protection Information). Integracja musi być realizowana w czasie rzeczywistym (ang. In-line), bezagentowo, niezależnie o typu OS, aplikacji. Dodatkowe 8 Bajtów “Data Integrity Field (DIF)” ma być przechowywane razem ze standardowym blokiem dyskowym 512-byte.
15.	Lista kompatybilności	Macierz musi umożliwiać jednoczesne podłączenie wielu serwerów w trybie wysokiej dostępności - co najmniej dwoma ścieżkami. Macierz dyskowa musi wspierać obsługę minimum 128 hostów podłączonych poprzez sieć SAN. Macierz musi wspierać podłączenie następujących systemów operacyjnych: Windows, Linux, VMware, IBM AIX, Sun Solaris, HP-UX. Wsparcie dla wymienionych systemów operacyjnych musi być potwierdzone wpisem na ogólnodostępnej liście kompatybilności producentów. Dla wymienionych systemów operacyjnych należy dostarczyć oprogramowanie do przełączania ścieżek i równoważenia

		obciążenia poszczególnych ścieżek. Wymagane jest oprogramowanie minimium dla zaoferowanej w niniejszym postępowaniu liczby serwerów. W przypadku stosowania rozwiązań firmowych/własnych – konieczna jest ich certyfikacja dla platform: Windows 2012+, Linux RedHat 7.x+, Suse12+, VMware 6+. Jeżeli dla realizacji powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla maksymalnej liczby serwerów/pojemności obsługiwanych przez oferowane urządzenie.
16.	Zintegrowana Ochrona Danych	Oprogramowanie macierzy musi zapewniać tworzenie kopii zapasowych: • jako migawek na tej samej trzymającej replikę LUN'u macierzy, Oprogramowanie musi zapewniać przywrócenie: • kopii zapasowej na - LUN źródłowy lub jego migawke przez nadpisanie wyłącznie zmienionych bloków, - inny LUN, • przy współpracy z oprogramowaniem do backupu uruchomienie maszyny wirtualnej z: - migawki macierzowej, Posiadać gotowe moduły producenta dostarczanej macierzy zapewniające integrację z przynajmniej dwoma systemami ochrony danych z listy: Veeam Backup and Replication, HPE Data Protector, VERITAS NetBackup, VERITAS BackupExec, EMC Networker, IBM Spectrum Protect, CommVault Simpana (w bieżących wersjach). Jeżeli dla realizacji powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla maksymalnej liczby serwerów/pojemności obsługiwanych przez oferowane urządzenie. Oferent jest zobowiązany do przesłania linków do oficjalnej, ogólnodostępnej dokumentacji producenta potwierdzającej spełnienie tej funkcjonalności.
17.	Dostępność i opcje serwisowe urządzenia	Macierz nie może posiadać pojedynczego punktu awarii, który powodowałby brak dostępu do danych. Musi być zapewniona pełna redundancja komponentów, w szczególności zdublowanie kontrolerów, zasilaczy i wentylatorów. Macierz musi umożliwiać wymianę elementów systemu w trybie „hot-swap", a w szczególności takich, jak: dyski, kontrolery, zasilacze, wentylatory. Macierz musi mieć możliwość zasilania z dwóch niezależnych źródeł

		zasilania –odporność na zanik zasilania jednej fazy lub awarię jednego z zasilaczy macierzy. Macierz musi umożliwiać wykonywanie aktualizacji mikrokodu/firmware'u macierzy w trybie online bez wyłączania żadnego z interfejsów macierzy. Macierz musi umożliwiać zdalne zarządzanie oraz automatyczne informowanie centrum serwisowego o awarii.
18.	Dostęp plikowy	Macierz musi umożliwiać udostępnianie danych plikowych po protokołach CIFS (w tym SMB v3) i NFS (w tym NFS v4) bezpośrednio ze wszystkich kontrolerów macierzowych obsługujących ruch plikowy. Jeżeli dla realizacji powyższych funkcjonalności wymagane są: • dodatkowe licencje, • dodatkowe kontrolery/bramy (ang. Gateway), należy je dostarczyć dla maksymalnej liczby serwerów/pojemności obsługiwanych przez oferowane urządzenie...
19.	Wymagania jakościowe	Łączna wydajność IOPS dla puli dysków SSD przy: * 70% odczytów, * bloku 8kB, * 20% ruchu losowego,i * bez trafień w cache nie mniej niż 370 000 IOPS. Do oferty należy załączyć wydruk z oficjalnego kalkulatora wydajności dla oferowanej konfiguracji macierzy zgodnie z ww, parametrami które będą weryfikowane w trakcie testu będącego częścią procedury obiorowej. W ramach prodcedury odbiorowej Zamawiający wymaga potwierdzenia wydajności oferowanej konfiguracji przez przeprowadzenie w obecności pracownika zamawiającego testu z wykorzystaniem narzędzia vdbench https://www.oracle.com/technetwork/server-storage/vdbench-1901683.pdf Środowisko testowe ma składać się 4 maszyn wirtualnych pracujących pod kontrolą sytemu operacyjnego CentOS 7.x na

		których zostanie zainstalowane ww. oprogramowanie Vdbench. Co najmniej 95% przestrzeni oferowanej na dyskach/modułach SSD/Flash/NVMe, ma zostać podzielona na 8 równych części i udostępniona maszynom testowym jako dyski RDM (Raw Device Mappings), po dwa do każdej maszyny wirtualnej. W ramach testu wygenerowany zostanie ruch IO przy parametrach 70% odczytu, 30% zapisu, blokiem 8KB, jednocześnie na wszystkich 4 maszynach wirtualnych. Plik konfiguracyjny *paramfile* programu Vdbench dla każdej instancji: *sd=sdb,lun=/dev/sdb,openflags=o_direct* *sd=sdc,lun=/dev/sdb,openflags=o_direct* *wd=worker,sd=(sdb,sdc),xfersize=8192,rdpct=70,rhpct=0,whpct=0, seekpct=20* *rd=test1,wd=worker,iorate=max,elapsed=7200,interval=5,warmup= 60* Wynik testu zostanie wyliczony jako suma wyników cząstkowych z każdej z 4 maszyn wirtualnych, pobranych z plików Vdbench summary report „summary.html", z kolumny „i/o rate", wiersz podsumowania „avg_x-yyy".
20.	Dostawa	Macierz dyskowa musi zostać dostarczona i zamontowana w budynku Biblioteki Śląskiej przy Placu Rady Europy 1. Wraz z dostawą musi zostać dostarczony niezbędny zestaw do zamontowania macierzy na wysuwanych szynach w szafie teleinformatycznej 19" w tym m.in., kable zasilające, logiczne, elementy stałe, itp. oraz podłączenia i konfiguracji z pozostałym zamówionym sprzętem komputerowym.

1.6 Macierz 2 i Macierz 3 (archiwum obiektowe) - obiektowy system składowania danych – ilość 1 szt.

Lp.	Nazwa elementu/cechy	Wymagane minimalne parametry techniczne
1.	Ogólne wymagania techniczne dla obiektowego systemu składowania danych	Dostawa, instalacja i konfiguracja obiektowego systemu składowania danych o efektywnej, dostępnej dla danych i metadanych pojemności nie mniejszej niż 4400 TB netto. Wymagana pojemność minimum 4400 TB netto dla środowiska produkcyjnego nie uwzględnia wykorzystania mechanizmów redukcji danych (przed procesem kompresji). Wymagana pojemność musi być dostarczona i zainstalowana w sposób symetryczny (wymagana dostawa dwóch macierzy, tworzących system w dwóch ośrodkach przetwarzania danych (serwerownia główna i zapasowa) Zamawiającego po minimum 2200 TB efektywnej przestrzeni (netto) w każdej serwerowni. Dane muszą być składowane symetrycznie pomiędzy oboma serwerowniami (wykorzystanie replikacji). System rozlokowany pomiędzy oboma ośrodkami powinien działać w trybie active-active oraz oferować wspólną przestrzeń danych (tzw. single name space). Biorąc pod uwagę powyższe dostępna przestrzeń produkcyjną netto (przy symetrycznym składowaniu danych) powinna wynosić minimum 2200TB. Oferowane rozwiązanie powinno umożliwiać asynchroniczną replikację obiektów pomiędzy serwerownią główną i zapasową za pomocą istniejących łącz Ethernet. Całe rozwiązanie powinno być zamontowane w dostarczonych szafach rack (po jednej dla każdej z serwerowni). Ze względu, że oferowane rozwiązanie będzie przechowywać przez bardzo długi okres kluczowe i bardzo ważne zbiory dla funkcjonowania Zamawiającego, które stanowią Dziedzictwo Narodowe, dostarczany obiektowy system składowania danych musi być: - produktem rozpoznawalnym na rynku, co oznacza, że musi być wymieniony w raportach niezależnych organizacji, co najmniej w Gartner oraz IDC z 2019r. - produktem, w którym (oprogramowanie zarządzające składowaniem danych) jest dostępne na rynku od co najmniej 3 lat. Oferowany obiektowy system składowania danych musi być

		produktem gotowym, posiadającym na moment składania oferty wszystkie wymagane przez Zamawiającego funkcjonalności. Do oferty należy załączyć listę wszystkich komponentów urządzenia. Lista ma zawierać co najmniej nazwy urządzeń, modeli oraz inne informacje pozwalające w sposób jednoznaczny zidentyfikować poszczególne komponenty sprzętowe i programowe. Oferowany obiektowy system składowania danych i wszystkie jego elementy składowe muszą być fabrycznie nowe i wyprodukowane nie wcześniej niż pół roku przed terminem dostawy do Zamawiającego. Oferowany obiektowy system składowania danych i wszystkie jego elementy muszą pochodzić od autoryzowanego dostawcy producenta. Obiektowy system składowania danych musi być oznakowany przez producenta w taki sposób, aby możliwa była identyfikacja zarówno produktu jak i producenta. Wraz obiektowym systemem składowania danych musi być dostarczony komplet nośników, bądź wskazany inny sposób umożliwiający odtworzenie oprogramowania systemowego urządzeń, z których zbudowane jest dostarczony obiektowy system składowania danych. Obiektowy system składowania danych musi mieć możliwość podłączenia go do centrum serwisowego producenta, w celu zdalnego monitorowania poprawności funkcjonowania komponentów rozwiązania.
2.	Wymagania dotyczące skalowalności, budowy i architektury obiektowego systemu składowania danych	Wszystkie elementy dostarczonego obiektowego systemu składowania danych mające wpływ na działanie produkcyjne (w przeciwieństwie do elementów dedykowanych do zarządzania samym urządzeniem) muszą być redundantne, a jego architektura musi zapewniać odporność na wystąpienie pojedynczego punktu awarii w obrębie poszczególnych grup elementów, to jest min.: interfejsów dostępowych, kontrolerów, zasilaczy, wentylatorów, dysków. Odporność na awarię oznacza, że dostęp do urządzenia oraz do składowanych na nim danych musi być realizowany bez przerywania pracy korzystającej z niego aplikacji/systemu, zapewniając możliwość odczytów wszystkich składowanych danych oraz wykonywania zapisów na urządzenie nawet w przypadku awarii lub wymiany pojedynczego elementu urządzenia z ww. grup urządzeń. Obiektowy system składowania danych musi posiadać możliwość pracy w architekturze, w której przestrzeń dyskowa jest dostarczana na dyskach zainstalowanych wewnątrz węzłów klastra (scale-out, RAIN).

		Obiektowy system składowania danych musi być odporny na awarię dowolnego z ośrodków tzn. w przypadku całkowitego zniszczenia infrastruktury oferowanego rozwiązania w jednym z ośrodków wszystkie dane powinny być dostępne, obiektowy system składowania danych musi umożliwiać kontynuację pracy aplikacji, dostępna przestrzeń podczas awarii jednego z ośrodków powinna cały czas wynosić 2200TB netto, po usunięciu awarii dane powinny zostać automatycznie zsynchronizowane pomiędzy oboma ośrodkami. Pojedyncza macierz dyskowa musi w oferowanej konfiguracji osiągać wydajność zgodnie z poniszym testem przy pomocy narzędzia COSBench (https://github.com/intel-cloud/cosbench), tj. wydajność zapisu i odczytu dla obiektów o wielkości 32KB oraz dla obiektów o wielkości 100MB: a. dla zapisu obiektów 32KB – 1600 obiektów/sekundę, b. dla odczytu obiektów 32KB – 3200 obiektów/sekundę, c. dla zapisu obiektów 100MB – 700 MB/sekundę, d. dla odczytu obiektów 100MB – 1000 MB/sekundę Dostarczony obiektowy system składowania danych dla środowiska produkcyjnego musi umożliwiać rozbudowę do co najmniej 800PB netto bez uwzględnienia kompresji, poprzez dołożenie kolejnych macierzy (wymagana możliwość rozlokowania dodatkowych macierzy w różnych lokalizacjach geograficznych), przy zachowaniu single name space (działającej w trybie ciągłym, nie wymagającej operacji typu DNS Failover) dla całego obiektowego systemu składowania danych (przed i po rozbudowie). Wszystkie macierze w rozbudowanym środowisku muszą działać w trybie active-active lub równoważnym opisanym w punkcie 1 oraz umożliwiać rozbudowę pojedynczej macierzy do co najmniej 80 węzłów. Rozbudowany obiektowy system składowania danych musi być odporny na awarię dowolnej z macierzy składowych: nie może dojść do utraty zapisanych danych, powinien być utrzymany dostęp oraz możliwość zapisu danych. Komunikacja z obiektowym systemem składowania danych w każdej z lokalizacji powinna być realizowana za pomocą redundantnych switch'y, będących częścią składową oferowanego obiektowego systemu składowania danych, w każdej z lokalizacji wymagane 2-a switche 10 GbE min. 48 portowe w standardzie SFP+, co najmniej po 4 porty (dedykowane do zewnętrznej komunikacji z urządzeniem) w każdym z dwóch switch'y powinny być obsadzone wkładkami SFP+ Zarządzanie wewnętrznymi elementami obiektowego systemu

		składowania danych w każdej z lokalizacji musi być realizowana poza w/w switch'ami dostępowymi, za pomocą dedykowanego do tego switch'a będącego częścią składową oferowanego rozwiązania. Wymagany mechanizm umożliwiający monitoring obejmujący m.in.: utylizację zasobów on-line (w tym CPU, Memory), kondycję HW, parametry systemu (w tym wydajnościowe).
3.	Szczegółowe wymagania funkcjonalne dla obiektowego systemu składowania danych	Dane w obiektowym systemie danych muszą być składowane jako obiekty składające się z danych podlegających archiwizacji oraz opisujących je metadanych. Identyfikacja składowanych danych musi być realizowana na podstawie zawartości obiektu a nie fizycznego położenia na dysku - czyli poprzez tzw. content address), aplikacja odwołująca się do obiektu za pomocą identyfikatora nie musi znać położenia obiektu (nie ma znaczenia na której z macierzy znajduje się obiekt). Rozmiar użytych dysków nie może przekraczać 16TB. Oferowany obiektowy system składowania danych musi umożliwiać dostęp do danych za pośrednictwem REST Web Service API, S3 API, CIFS oraz NFS. Jeżeli wykorzystanie któregokolwiek z wymienionych protokołów i interfejsów wymaga zastosowania dodatkowej licencji lub oprogramowania, to należy je dostarczyć wraz z obiektowym systemem składowania danych. Wymagane wsparcie dla HTTP oraz HTTPS dla wszytkich wspieranych API. Obiektowy system składowania danych musi posiadać wbudowane mechanizmy zapewniające możliwość potwierdzania autentyczności składowanych danych. Mechanizmy te muszą opierać się o wyliczenie przez urządzenie sumy kontrolnej dla każdego składowanego obiektu. Wymagane jest wsparcie dla co najmniejalgorytmu minimum MD5. Wymagana możliwość wieloprotokołowego dostępu do danych. Oferowany obiektowy system składowania danych musi zapewniać poprzez REST API możliwość przeszukiwania metadanych przechowywanych obiektów zapisanych z wykorzystaniem S3 na poziomie tzw. BUCKETS w oparciu o wbudowany mechanizm oferowanego rozwiązania (bez konieczności tworzenia zewnętrznych systemów bazodanowych). Obiektowy system składowania danych powinien posiadać wbudowane mechanizmy protekcji danych, które gwarantują

		odczyt wszystkich składowanych danych w przypadku awarii pojedynczego, losowego komponentu architektury. Zabezpieczenie składowanych obiektów w obrębie obiektowego systemu składowania danych musi być realizowane poprzez ich podział oraz „nadmiarową" dystrybucję poszczególnych części obiektów (erasure coding) w ramach przestrzeni dyskowej macierzy, wymagana możliwość wymiany uszkodzonych dysków w sposób on-line. Jednoczesne uszkodzenie dwóch kontrolerów poj. macierzy nie może skutkować zaburzeniami w pracy oferowanej macierzy w szczególności: • dostępności do wszystkich zapisanych dotychczas danych, • standardowego odczytu dowolnych wcześniej zapisanych danych, • standardowego trybu zapisu z wykorzystaniem ERASURE CODING, Macierz powinna być odporna na jednoczesne uszkodzenie dwóch dysków. Dostarczony obiektowy system składowania danych musi zapewniać i gwarantować niezmienność składowanych w nim obiektów, poprzez wykorzystanie wbudowanej technologii WORM (Write Once Read Many) dla protokołu S3 oraz dla pozostałych wymaganych protokołów. Wymagana funkcjonalność musi być realizowana przez macierze będące przedmiotem zapytania. Obiektowy system składowania danych musi posiadać możliwość definiowania różnych poziomów retencji przechowywania danych, gwarantujących brak możliwości skasowania danych przed upływem zdefiniowanego czasu. Obiektowy system składowania danych musi dostarczać mechanizmy integracji z aplikacją w postaci API, umożliwiające: • izolację na poziomie dostępu różnych typów archiwów w obrębie jednej oraz wielu macierzy obiektowych („MULTI-TENANCY") tego samego typu, tworzących jeden system, • definiowanie polityki retencji obiektów w obrębie całego systemu jak i poszczególnych części logicznych (tzw. TENANTS) oraz BUCKET, przy czym administrator musi mieć możliwość zdefiniowania co najmniej 1000 Tenantów i 10000 Bucketów, • przekazywanie przez aplikację do użytkownika końcowego ścieżki do obiektu zapisanego w systemie.

		Obiektowy system składowania danych musi posiadać możliwość tworzenie logicznie odseparowanych obszarów tzw. „MULTI-TENANCY". Wymagana możliwość rozdzielnego administrowania (np.: przypisywanie użytkowników, tworzenie praw dostępu, polityki składowania danych, monitorowanie wykorzystania) tak tworzonymi obszarami. Obiektowy system składowania danych musi posiadać wbudowane mechanizmy redukcji danych, kompresję i deduplikację. W przypadku, gdy oferowany obiektowy system składowania danych nie posiada funkcjonalności opisanych w poprzednim punkcie, wówczas należy dostarczyć rozwiązanie o pojemności powiększonej o 50% wymaganej przestrzeni. Obiektowy system składowania danych musi posiadać wbudowany mechanizm wersjonowania obiektów w przypadku wykorzystania protokołu S3. Obiektowy system składowania danych musi umożliwiać grupowanie przechowywanych obiektów oraz przypisywanie różnych polityk replikacyjnych (np.: brak replikacji, replikacja pojedyncza, podwójna). Obiektowy system składowania danych musi zapewnić automatyzacje procesu „odświeżania" i zarządzania przechowywanymi danymi (automatyczna weryfikacja poprawności danych poprzez porównywanie z funkcją skrótu – hash). Obiektowy system składowania danych musi zapewnić definiowanie różnych poziomów retencji przechowywania danych, gwarantujących niezmienność i brak możliwości usunięcia archiwizowanych danych przez zadany parametr czasu. Rozwiązanie powinno posiadać wbudowany mechanizm zatrzymania retencji danych, co oznacza, że w przypadku, gdy taki mechanizm zostanie włączony dla danego obiektu, retencja danych musi być utrzymywana dla tego obiektu do momentu jego wyłączenia, niezależnie od zadanego parametru czasu w definicji polityki retencji. Obiektowy system składowania danych musi posiadać mechanizm umożliwiający samoczynnego (ustawienie polityki) usuwania danych, dla których okres retencji został przekroczony.
4.	Protokoły dostępu do danych	http(s), S3, Rest Web Api

5.	Dostawa	Obiektowy system składowania danych musi zostać dostarczony i zamontowany w budynku Biblioteki Śląskiej przy Placu Rady Europy 1 oraz Ligonia 7. Wraz z dostawą musi zostać dostarczony niezbędny zestaw do zamontowania systemu u Zamawiającego oraz podłączenia go i konfiguracji z pozostałym zamówionym sprzętem komputerowym.

1.7 Instalacja i konfiguracja części od 1.2 do 1.8 – ilość 1 szt.,

Lp.	Nazwa elementu/cechy	Wymagane minimalne parametry techniczne
1.	Ogólne	Zamawiający obecnie posiada serwerownię główną w lokalizacji budynku Biblioteki Śląskiej na Placu Rady Europy 1 w Katowicach oraz serwerownię zapasową w budynku Biblioteki Śląskiej na ul. Ligonia 7 w Katowicach. Obydwie serwerownie połączone są szybką siecią o przepustowości co najmniej 1Gpbs. Opracowanie przez Wykonawcę zgodnie z wytycznymi Zamawiającego oraz akceptacja przez Zamawiającego projektu technicznego dla pozycji od 1.2 do 1.8 uwzględniającego m.in.: • Instalacje i konfiguracje pozycji od 1.2 do 1.8, • Instalacje i konfiguracje 18 fizycznych serwerów z poz. 1.3 i 1.5 z stanowiskiem dostępu i zarządzania KVM z poz. 1.6, oraz posiadanego serwera kompresji, • Instalacje systemu wysokiej dostępności w oparciu o serwery z poz. 1.3 i system wirtualnego środowiska z poz. 1.4 w tym: – dwóch serwerów wirtualnych na każdym z 12 serwerów fizycznych (łącznie wymagane jest utworzenie 24 serwerów wirtualnych) z systemem operacyjnym wskazanym przez Zamawiającego (licencje dostarcza Zamawiający), silnik oprogramowania wirtualizacyjnego musi być zainstalowany na dyskach wewnętrznych serwera, system operacyjny i przestrzeń na dane „gościa" musi być na udostępnionym zasobie składającym się z dysków SSD z macierzy z poz. 1.7 – 8 z 24 serwerów wirtualnych każdy w konfiguracji: 8 rdzeni procesora, 16GB RAM, 270GB pojemność dysków SSD, – 3 z 24 serwerów wirtualnych każdy w konfiguracji: 16 rdzeni procesora, 32GB RAM, 512GB pojemność dysków SSD, – 10 z 24 serwerów wirtualnych każdy w konfiguracji: 8 rdzeni procesora, 16GB RAM, 270GB pojemność dysków SSD, – 3 z 24 serwerów wirtualnych każdy w konfiguracji: 16 rdzeni procesora, 32GB RAM, 512GB pojemność dysków SSD, – serwery muszą korzystać z zasobów macierzy dyskowej z poz. 1.7, w zależności od potrzeb aplikacje, baza danych, oprogramowanie systemowe lub narzędziowe Zamawiającego musi komunikować się z macierzą dyskową

		z poz. 1.7 za pośrednictwem protokołów plikowych (CIFS, NFS) i/lub blokowych (FC, iSCSI). • Instalacje i konfiguracje serwerów z poz. 1.5, • Instalacje i uruchomienie macierzy dyskowej z poz. 1.7 wraz z dedykowanym oprogramowaniem do zarządzania macierzą dyskową w tym: – konfiguracja grup RAID na dyskach SSD, SAS, – konfiguracja dysków logicznych, – prezentacja zasobów dyskowych SSD dla serwerów za pomocą sieci FC, – utworzenie systemów plików na zaprezentowanych zasobach blokowych, – prezentacja zasobów dyskowych SSD dla serwerów, stacji roboczych Zamawiającego za pomocą protokołów FC, CIFS lub NFS, – prezentacja zasobów dyskowych SAS dla serwerów, stacji roboczych Zamawiającego za pomocą protokołów FC, CIFS lub NFS (jeden zasób o wielkości 100TB, drugi zasób o wielkości 150TB), – konfiguracja ustawień sieciowych, – utworzenie udziałów sieciowych do prezentacji dla systemów operacyjnych, – konfiguracja praw dostępu do zasobów. • Instalacje i konfiguracje obiektowego systemu składowania danych z poz. 1.8, jako magazynu cyfrowej reprezentacji posiadanych przez Bibliotekę Śląską zbiorów dokumentów • Instalacje i konfiguracje dostarczonego sprzętu komputerowego w sieci SAN, • Instalacje i konfiguracje dostarczonego sprzętu komputerowego w sieci LAN, • Wykonanie instalacji światłowodowej pomiędzy serwerownią zapasową (nową w piwnicy Biblioteki Śląskiej na ul. Ligonia 7) a obecnym miejscem zakończenia światłowodu (pomieszczenie Biblioteki Śląskiej na ul. Ligonia 7, serwerownia I piętro) o długości około 20m wraz z przyłączami i wszystkimi elementami niezbędnymi do jej wykonania umożliwiającymi podłączenie jednej z macierzy obiektowych z poz. 1.8 do infrastruktury LAN Biblioteki Śląskiej na ul. Ligonia 7.

		Instalacja światłowodowa zakończona na przełącznicach na obu końcach i obejmuje wykonanie jednej w nowej szafie w pomieszczeniu piwnicznym a druga w szafie obecnej serwerowni w serwerowni na I piętrze. Instalacja, konfiguracja oraz produkcyjne uruchomienie pozycji od 1.2 do 1.8 zgodnie z zaakceptowanym przez Zamawiającego projektem technicznym. Wykonawca w ramach instalacji i konfiguracji macierzy dyskowej z poz. 1.7 wykona w okresie obowiązywania gwarancji migrację danych o łącznej pojemności 150TB z aktualnie wykorzystywanych systemów składowania i przetwarzania danych na macierz dyskową z poz. 1.7 lub obiektowy system składowania danych z poz. 1.8 jeśli będzie to wymagane przez Zamawiającego. Proces migracji musi zagwarantować zachowanie spójności i integralności przenoszonych danych. Zamawiający wymaga aby posiadane przez Zamawiającego dane zgromadzone i przetwarzane na systemach HDS AMS 2300 i Hitachi NAS Platform 3080 były dostępne poprzez dowolne protokoły wymiany danych/systemy plików w nowym dostarczonym środowisku. Opracowanie dokumentacji technicznej powdrożeniowej dla pozycji od 1.2 do 1.8.

1.8 Szkolenia – ilość 1 szt.

Lp.	Nazwa szkolenia	Wymagane minimalne parametry techniczne
1.	Szkolenie z administracji oprogramowaniem z rodziny systemów operacyjnych linux klasy enterprise dostarczonym z fizycznymi serwerami z poz. 1.3 i 1.5	Rodzaj szkolenia: • autoryzowane, • przygotowujące uczestnika szkolenie do zdania egzaminu na poziomie certyfikowanego administratora dostarczonego oprogramowania z rodziny systemów operacyjnych linux klasy enterprise (CSA), • szkolenie musi zakończyć się egzaminem na poziomie certyfikowanego administratora dostarczonego oprogramowania z rodziny systemów operacyjnych linux klasy enterprise (CSA). Szkolenie i egazamin musi być przeznaczony dla 3 osób.
2.	Szkolenie z administracji oprogramowania do wirtualizacji poz. 1.4	Rodzaj szkolenia: • autoryzowane lub • wykonane przez inżyniera Wykonawcy lub • wykonane przez producenta dostarczonego sprzętu lub oprogramowania. Szkolenie musi być co najmniej pięciodniowe. Szkolenie musi być z zakresu oprogramowania do wirtualizacji poz. 1.4. Szkolenie musi obejmować tematykę z zakresu instalacji, konfiguracji oraz zarządzania oprogramowaniem do wirtualizacji z poz. 1.4. Szkolenie musi obejmować swoim zakresem co najmniej tematykę: • wprowadzenia do software defined Data Center, • wpływ wirtualizatora na pamięć i procesory serwerów, • tworzenie, dostarczanie i usuwanie maszyn wirtualnych, • wyjaśnienie narzędzi związanych z wirtualizatorem,

		• narzędzia zarządzania systemem wirtualizacji, • rozwiązywanie problemów związanych z systemami operacyjnymi serwerów i wirtualizatorem, • opis architektury systemu zarządzania wirtualizacją, • opis komunikacji hostów z systemem zarządzania, • identyfikacja usług systemu zarządzania, • zasady kontroli dostępu, • monitorowanie, backup i odtworzenie systemu zarządzania wirtualizatorem, • konfiguracja i zarządzanie wirtuanymi sieciami, • opis, zarządzanie i konfigurowanie wirtualnego switcha, • opis rodzajów połączeń w ramach zwirtualizowanego przełącznika, • opis architektury stosu TCP/IP zwirtualizowanego przełącznika, • komunikacja z sieciami VLAN fizycznych przelaczników, • konfigurajca i zarządzanie wirtualną pamięcią masową, • identyfikacja protokołów zwirtualizowanej pamięci masowej, • omówienie wykorzystania w zwirtualizowanych hostach protokołów iSCSI, NFS i FC, • konfiguracja, uruchomienie i zarządzanie wirtualnymi sieciami SAN • zarządzanie maszynami wirtualnymi (tworzenie maszyn wirtualnych, klony i szablony maszyn wirtualnych, tworzenie i zarządzania snapshotami maszyn wirtualnych), • monitoring i zarządzanie zasobami zwirtualizowanymi (konfiguracja i zarządzanie zasobami, rozwiązywanie probllemów związanych z nadmiernym obciazaniem zasobów, wykorzystanie technologii optymalizacji wykorzystania zasobow), • tworzenie klastrów HA. Po ukończeniu szkolenia, każdy uczestnik ma otrzymać stosowny dokument potwierdzający uzyskanie kompetencji do administrowania dostarczonym oprogramowaniem do wirtualizacji

		poz. 1.4 oraz pozwalający na przystąpienie do egzaminu certyfikującego na poziomie co najmniej podstawowym z zakresu instalacji, konfiguracji oraz zarządzania oprogramowaniem do wirtualizacji z poz. 1.4. Po ukończeniu szkolenia uczestnik ma otrzymać voucher pozwalający na przystąpienie do egzaminu certyfikującego na poziomie co najmniej podstawowym z zakresu instalacji, konfiguracji oraz zarządzania oprogramowaniem do wirtualizacji z poz. 1.4. Szkolenie będzie się odbywało na terenie Katowic lub wykonawca pokryje koszty transportu i noclegu w przypadku miejsca szkolenia innego niż Katowice. Szkolenie przeznaczone dla trzech osób.
3.	Szkolenie z administracji macierzą dyskową poz. 1.7	Rodzaj szkolenia: • autoryzowane lub • wykonane przez inżyniera Wykonawcy lub • wykonane przez producenta dostarczonego sprzętu lub oprogramowania. Szkolenie musi być co najmniej trzydniowe. Szkolenie musi być z zakresu zarządzania macierzą dyskową. Szkolenie musi być przeprowadzone w postaci warsztatów co najmniej w zakresie: • teorii dotyczącej zasad funkcjonowania sieci SAN • konfiguracji oraz obsługi macierzy blokowej • omówienia budowy i zasady działania urządzenia • tworzenia zasobów logicznych • konfiguracji funkcjonalności LUN masking • prezentacji zasobów do systemów operacyjnych • migracji zasobów logicznych • diagnozy pracy urządzenia • replikacji danych • omówienia budowy urządzenia

		• tworzenia systemów plików • praw dostępu do plików, quota • rodzajów i zasad konfiguracji • protokołów dostępu do danych plikowych • prezentacji zasobów serwerom • diagnozy pracy urządzenia • funkcjonowania i konfiguracji tieringu Po ukończeniu szkolenia, każdy uczestnik ma otrzymać stosowny dokument potwierdzający uzyskanie kompetencji do administrowania dostarczoną macierzą dyskową. Szkolenie będzie się odbywało na terenie Katowic lub wykonawca pokryje koszty transportu i noclegu w przypadku miejsca szkolenia innego niż Katowice. Szkolenie przeznaczone dla trzech osób.
4.	Szkolenie z administracji obiektowym systemem składowania danych poz. 1.8	Rodzaj szkolenia: • autoryzowane lub • wykonane przez inżyniera Wykonawcy lub • wykonane przez producenta dostarczonego sprzętu lub oprogramowania. Szkolenie musi być co najmniej trzydniowe. Szkolenie musi być z zakresu zarządzania obiektowym systemem składowania danych. Szkolenie musi być przeprowadzone w postaci warsztatów, Po ukończeniu szkolenia, każdy uczestnik ma otrzymać stosowny dokument potwierdzający uzyskanie kompetencji do administrowania dostarczoną macierzą dyskową, Szkolenie będzie się odbywało na terenie Katowic lub wykonawca pokryje koszty transportu i noclegu w przypadku miejsca szkolenia innego niż Katowice, Szkolenie przeznaczone dla trzech osób

2. Urządzenia sieciowe.

1.1 Switche LAN 48 port 10Gbit/s – ilość 3 szt.

Lp.	Nazwa elementu/cechy	Wymagane minimalne parametry techniczne
1.	Obudowa	Do montażu w szafie dystrybucyjnej 19", o wysokości nie więcej niż 2U, głębokość: max 60 cm wraz z kompletem odpowiednich szyn. Zasilacze zmiennoprądowe pracujące w konfiguracji redundantnej. Redundantne moduły wentylatorów z możliwością wymiany na gorąco (ang. hot-swap)
2.	Porty	Minimum 48 portów 10GBase-T w tym minimum 40 zapewniających pracę z prędkościami 1/10G Minimum 6 portów 40GE definiowanych za pomocą wkładek QSFP, przy czym każdy z tych portów QSFP musi posiadać możliwość pracy zarówno w trybie 40Gbps– obsadzone wkładkami 40GBase-SR (dopuszczalne wykorzystanie zamiennie z portami 10GE SFP) Dedykowany interfejs GE 100/1000 na potrzeby zarządzania.
3.	Wydajność	Prędkość przełączania „wirespeed” dla każdego portu przełącznika. Urządzenie sprzętowo przełącza pakiety w warstwie L2 i L3. Obsługiwana łączna przepływność (pasmo) min. 1,44 Tbps. Obsługiwana łączna przepustowość pakietowa przełącznika min. 800 Mpps.
4.	Funkcjonalność warstwy drugiej	Trunking IEEE 802.1Q VLAN. Wsparcie sprzętowe dla co najmniej 4000 sieci VLAN. Funkcjonalność izolowania portów znajdujących się w tym samym VLAN. Wsparcie sprzętowe dla minimum 208 000 adresów MAC. IEEE 802.1w Rapid Spanning Tree (RST).

		IEEE 802.1s Multiple Spanning Tree (MST) – co najmniej 32 instancje. Wsparcie sprzętowe dla tunelowania QinQ. Zabezpieczenie przeciwko incydentom w topologii Spanning Tree. Internet Group Management Protocol (IGMP) Versions 2, 3. Terminowanie pojedynczej wiązki EtherChannel na 2 niezależnych przełącznikach. Link Aggregation Control Protocol (LACP): IEEE 802.3ad z możliwością zgrupowania minimum 8 interfejsów fizycznych w wiązce. Ramki Jumbo dla wszystkich portów (minimum 9100 bajtów).
5.	Funkcjonalność wartstwy trzeciej	Sprzętowe przełączanie pakietów w warstwie L3. Obsługa co najmniej 256 000 tras IPv4 / 128 000 IPv6. Routing w oparciu o trasy statyczne. Routing w oparciu o OSPF, BGP, ISIS dla protokołów IPv4 oraz IPv6. Policy Based Routing (PBR) dla IPv4. VRRP v3. Wsparcie dla BFDv6 (Bidirectional Forwarding Protocol). Wsparcie dla IPv4 multicast w oparciu o protokół PIMv2 SM (Sparse Mode) i SSM (Source Specific Multicast). Wsparcie dla IGMPv3 oraz MSDP. Wsparcie sprzętowe dla minimum 8 000 tras multicastowych. Wsparcie dla minimum 1.000 instancji VRF wraz z funkcjonalnością importu/eksportu tras (route leaking). Wybór do 32 jednoczesnych ścieżek o równej metryce (ECMP). Minimum 1.000 wejściowych oraz 1.000 wyjściowych wpisów dla ACL - access control list.
6.	Mechanizmy związane z funkcjonalnością VXLAN	Obsługa co najmniej 250 sprzętowych VTEP (VXLAN Tunnel Endpoint).

		Sprzętowy VXLAN Bridging (VXLAN/VLAN Gateway). Obsługa ruchu rozgłoszeniowego (multicast, broadcast, unknown unicast) z mapowaniem VXLAN do IP Multicast Group i wykorzystaniem funkcjonalności PIM Anycast RP. Obsługa ruchu rozgłoszeniowego (multicast, broadcast, unknown) poprzez statyczną replikację (bez konieczności wykorzystania IP Multicast). Implementacja VXLAN BGP EVPN (Ethernet VPN) z dystrybucją informacji o adresach MAC i adresach IP poprzez MP-BGP i ograniczeniem ruchu ARP (Address Resolution Protocol). Obsługa routingu między VXLAN-ami (VXLAN Routing) z wykorzystaniem BGP EVPN oraz funkcjonalności Anycast Gateway (obsługą danego SVI na wszystkich VTEP w domenie VXLAN). Jeżeli funkcjonalność VXLAN wymaga licencji to w ramach postępowania należy ją dostarczyć.
7.	Mechanizmy związane z zapewnieniem jakości usług w sieci	Layer 2 IEEE 802.1p (CoS). Klasyfikacja QoS w oparciu o listy (ACL (Access control list) – w warstwach 2, 3, 4. Kolejkowanie na wyjściu w oparciu o CoS 802.1p. Bezwzględne (strict-priority) kolejkowanie na wyjściu. Kolejkowanie WRR (Weighted Round-Robin) na wyjściu lub mechanizm równoważny. Ograniczanie ruchu (policing) do zadanej przepływności na interfejsach wejściowych i wyjściowych. Kształtowanie (shaping) ruchu do zadanej przepływności na interfejsach wyjściowych. Protokół PFC (Priority Flow Control) IEEE 802.1Qbb.
8.	Bezpieczeństwo	Wejściowe ACL (standardowe oraz rozszerzone). Standardowe oraz rozszerzone ACL dla warstwy 2 w oparciu o: adresy MAC adresy, typ protokołu. Standardowe oraz rozszerzone ACL dla warstw 3 oraz 4 w oparciu o: IPv4 i IPv6, Internet Control Message Protocol (ICMP), TCP, User Datagram Protocol (UDP).

		ACL oparte o VLAN-y (VACL). ACL oparte o porty (PACL). DHCP Snooping. ARP Inspection. IP Source Guard. Prewencja niekontrolowanego wzrostu ilości ruchu (storm control), dla ruchu unicast, multicast, broadcast.
9.	Programowanie i zarządzanie	Interfejs programistyczny REST API
10.	Funkcjonalności dla obszaru zarządzania i zabezpieczenia przełącznika	RMON (przynajmniej grupy Events, Alarms). Openflow 1.3/1.4. sFlow lub netFlow. IEEE 802.1ab LLDP. Możliwość zachowania stanu (checkpoint) i powrotu do poprzedniej konfiguracji (rollback). Ograniczanie ruchu kierowanego do warstwy sterowania (control plane policing). Kopiowanie ruchu ze źródłowych fizycznych portów Ethernet, wiązek PortChannel, sieci VLAN, na interfejs docelowy za pośrednictwem specjalnego mechanizmu. (mirror). Network Time Protocol (NTP). Ping, traceroute.
11.	Certyfikaty i standardy	Zamawiający wymaga aby oferowany przełącznik: • posiadał deklarację CE, • był zgodny z standardem RoHS.
12.	Dostawa	Switche LAN 48 port 10 Gbit/s muszą zostać dostarczone i zamontowane w budynku Biblioteki Śląskiej przy Placu Rady Europy 1. Wraz z dostawą musi zostać dostarczony niezbędny zestaw do

		zamontowania switchów LAN 48 port 10 Gbit/s na szynach w szafie dystrybucyjnej 19” w tym m.in., kable zasilające, logiczne, elementy stałe, itp. oraz podłączenia i konfiguracji z pozostałym zamówionym sprzętem komputerowym.

1.2 Switche LAN 48 port 10/40 Gbit/s – ilość 6 szt.

Lp.	Nazwa elementu/cechy	Wymagane minimalne parametry techniczne
1.	Obudowa	Do montażu w szafie dystrybucyjnej 19", o wysokości nie więcej niż 1U, głębokość: max 60 cm wraz z kompletem odpowiednich szyn. Zasilacze zmiennoprądowe pracujące w konfiguracji redundantnej.
2.	Porty	Minimum 48 portów 10GBase-T umożliwiające pracę z prędkościami 100M/1G/10G. Minimum 6 portów 40GE definiowanych za pomocą wkładek QSFP, przy czym każdy z tych portów QSFP musi posiadać możliwość pracy zarówno w trybie 40Gbps– obsadzone wkładkami 40GBase-SR. Dedykowany interfejs GE 100/1000 na potrzeby zarządzania.
3.	Wydajność	Prędkość przełączania „wirespeed” dla każdego portu przełącznika. Urządzenie sprzętowo przełącza pakiety w warstwie L2 i L3. Obsługiwana łączna przepływność (pasmo) min. 1,44 Tbps. Obsługiwana łączna przepustowość pakietowa przełącznika min. 800 Mpps.
4.	Funkcjonalność wartstwy drugiej	Trunking IEEE 802.1Q VLAN. Wsparcie sprzętowe dla co najmniej 4000 sieci VLAN. Funkcjonalność izolowania portów znajdujących się w tym samym VLAN. Wsparcie sprzętowe dla minimum 256 000adresów MAC. IEEE 802.1w Rapid Spanning Tree (RST). IEEE 802.1s Multiple Spanning Tree (MST) – co najmniej 32 instancje.. Wsparcie sprzętowe dla tunelowania QinQ

		Zabezpieczenie przeciwko incydentom w topologii Spanning Tree. Internet Group Management Protocol (IGMP) Versions 2, 3. Terminowanie pojedynczej wiązki EtherChannel na 2 niezależnych przełącznikach. Link Aggregation Control Protocol (LACP): IEEE 802.3ad z możliwością zgrupowania minimum 8 interfejsów fizycznych w wiązce. Ramki Jumbo dla wszystkich portów (minimum 9100 bajtów).
5.	Funkcjonalność wartstwy trzeciej	Sprzętowe przełączanie pakietów w warstwie L3. Obsługa co najmniej 256 000 tras IPv4 / 128 000 IPv6. Routing w oparciu o trasy statyczne. Routing w oparciu o OSPF, BGP, ISIS dla protokołów IPv4 oraz IPv6. Policy Based Routing (PBR) dla IPv4. VRRP v3. Wsparcie dla BFDv6 (Bidirectional Forwarding Protocol). Wsparcie dla IPv4 multicast w oparciu o protokół PIMv2 SM (Sparse Mode) i SSM (Source Specific Multicast). Wsparcie dla IGMPv3 oraz MSDP. Wsparcie sprzętowe dla minimum 8 000 tras multicastowych. Wsparcie dla minimum 1.000 instancji VRF wraz z funkcjonalnością importu/eksportu tras (route leaking). Wybór do 32 jednoczesnych ścieżek o równej metryce (ECMP). Minimum 1.000 wejściowych oraz 1.000 wyjściowych wpisów dla ACL - access control list.
6.	Mechanizmy związane z funkcjonalnością VXLAN	Obsługa co najmniej 250 sprzętowych VTEP (VXLAN Tunnel Endpoint). Sprzętowy VXLAN Bridging (VXLAN/VLAN Gateway). Obsługa ruchu rozgłoszeniowego (multicast, broadcast, unknown unicast) z mapowaniem VXLAN do IP Multicast Group i wykorzystaniem funkcjonalności PIM Anycast RP.

		Obsługa ruchu rozgłoszeniowego (multicast, broadcast, unknown) poprzez statyczną replikację (bez konieczności wykorzystania IP Multicast). Implementacja VXLAN BGP EVPN (Ethernet VPN) z dystrybucją informacji o adresach MAC i adresach IP poprzez MP-BGP i ograniczeniem ruchu ARP (Address Resolution Protocol). Obsługa routingu między VXLAN-ami (VXLAN Routing) z wykorzystaniem BGP EVPN oraz funkcjonalności Anycast Gateway (obsługą danego SVI na wszystkich VTEP w domenie VXLAN). Jeżeli funkcjonalność VXLAN wymaga licencji to w ramach postępowania należy ją dostarczyć.
7.	Mechanizmy związane z zapewnieniem jakości usług w sieci	Layer 2 IEEE 802.1p (CoS). Klasyfikacja QoS w oparciu o listy (ACL (Access control list) – w warstwach 2, 3, 4. Kolejkowanie na wyjściu w oparciu o CoS 802.1p. Bezwzględne (strict-priority) kolejkowanie na wyjściu. Kolejkowanie WRR (Weighted Round-Robin) na wyjściu lub mechanizm równoważny. Ograniczanie ruchu (policing) do zadanej przepływności na interfejsach wejściowych i wyjściowych. Kształtowanie (shaping) ruchu do zadanej przepływności na interfejsach wyjściowych. Protokół PFC (Priority Flow Control) IEEE 802.1Qbb.
8.	Bezpieczeństwo	Wejściowe ACL (standardowe oraz rozszerzone). Standardowe oraz rozszerzone ACL dla warstwy 2 w oparciu o: adresy MAC adresy, typ protokołu. Standardowe oraz rozszerzone ACL dla warstw 3 oraz 4 w oparciu o: IPv4 i IPv6, Internet Control Message Protocol (ICMP), TCP, User Datagram Protocol (UDP). ACL oparte o VLAN-y (VACL). ACL oparte o porty (PACL). DHCP Snooping.

		ARP Inspection. IP Source Guard. Prewencja niekontrolowanego wzrostu ilości ruchu (storm control), dla ruchu unicast, multicast, broadcast.
9.	Programowanie i zarządzanie	Interfejs programistyczny REST API.
10.	Funkcjonalności dla obszaru zarządzania i zabezpieczenia przełącznika	RMON (przynajmniej grupy Events, Alarms). Openflow 1.3/1.4. sFlow lub netFlow. IEEE 802.1ab LLDP. Możliwość zachowania stanu (checkpoint) i powrotu do poprzedniej konfiguracji (rollback). Ograniczanie ruchu kierowanego do warstwy sterowania (control plane policing). Kopiowanie ruchu ze źródłowych fizycznych portów Ethernet, wiązek PortChannel, sieci VLAN, na interfejs docelowy za pośrednictwem specjalnego mechanizmu. (mirror). Network Time Protocol (NTP). Ping, traceroute.
11.	Certyfikaty i standardy	Zamawiający wymaga aby oferowany przełącznik: • posiadał deklarację CE. • był zgodny z standardem RoHS.
12.	Dostawa	Switche LAN 48 Port 10/40 Gbit/s muszą zostać dostarczone i zamontowane w budynku Biblioteki Śląskiej przy Placu Rady Europy 1 i Ligonia 7. Wraz z dostawą musi zostać dostarczony niezbędny zestaw do zamontowania switchów LAN 48 Port 10/40 Gbit/s na szynach w szafie dystrybucyjnej 19” w tym m.in., kable zasilające, logiczne, elementy stałe, itp. oraz podłączenia i konfiguracji z pozostałym zamówionym sprzętem komputerowym.

1.3 Switche FC 48 port 16 Gbps – ilość 2 szt.

Lp.	Nazwa elementu/cechy	Wymagane minimalne parametry techniczne
1.	Obudowa	Przełącznik FC musi mieć wysokość maksymalnie 1U oraz zapewniać techniczną możliwość montażu w szafie dystrybucyjnej 19”.
2.	Ogólne	Przełączniki FibreChannel obsługujące technologię 32 Gb/s i zapewniające możliwość pracy portów z prędkościami 32, 16, 8 Gb/s w zależności od rodzaju zastosowanych wkładek SFP lub QSFP. Wszystkie porty przełącznika FC muszą umożliwiać działanie bez tzw. nadsubskrypcji (wszystkie porty w maksymalnie rozbudowanej konfiguracji przełącznika muszą umożliwiać pracę równocześnie z pełną prędkością 32Gb/s). Obsługa portów co najmniej E oraz F. Możliwość standardowego przydziału minimum 320 kredytów (FC buffer credits) Możliwość zwiększenia liczby kredytów (FC buffer credits) do co najmniej 3840 dla co najmniej czterech portów przełącznika.
3.	Ilość portów FC	Przełącznik FC musi posiadać minimum 48 sloty na moduły FC. Wszystkie wymagane funkcje muszą być dostępne dla minimum 48 portów FC przełącznika. Przełącznik FC musi zapewniać możliwość aktywowania portów za pomocą zakupionych kluczy licencyjnych.
4.	Ilość modułów SFP oraz kabli	Przełącznik musi być dostarczony wraz z wszystkimi portami obsadzonymi interfejsami SFP FC 16 Gb/s, 48 x LC-LC 5m.
5.	Typ portów FC	Przełącznik musi być kompatybilny z dostarczona macierzą dyskową 1.7 oraz kartami FC będącymi częścią dostarczonych serwerów poz. 1.3 i 1.5.
6.	Obsługa mechanizmow FC	Sprzętowo implementowany zoning. Tryb NPV (N-Port Virtualization). Zamawiający dopuszcza jako równoważną funkcjonalność Brocade Access Gateway.

		Funkcjonalność N-Port ID Virtualization (NPIV) dla każdego portu. Obsluga NVMe over Fabric.
7.	Wymagania funkcjonalne	Podział sieci SAN na wirtualne fabryki SAN (logiczne przełączniki SAN) – obsługa co najmniej 4 wirtualnych fabryk. Łączenie fabryk SAN poprzez routowanie (routing FC-FC). Obsługa agregacji nie mniej niż 8 portów fizycznych FC 32G w jedno połączenie logiczne („trunk", „channel") – możliwość włączenia w skład zagregowanego połączenia logicznego dowolnego aktywnego portu przełącznika. Jednoczesna obsługa mechanizmów agregowanego połączenia logicznego („trunk", „channel") oraz podziału ruchu w oparciu o parametry DID/SID/OXID. Wykrywanie i eliminacja ramek FC z błędnym kodem CRC na portach we/wy lub obsługa mechanizmu FEC (Forward Error Correction) w celu uniknięcia przesyłania błędnych ramek. Możliwość aktualizacji oprogramowania bez przerwy w działaniu urządzenia (tzw. nondisruptive software upgrades). Wsparcie dla mechanizmów gwarancji jakości usług (QoS).
8.	Obsługiwane typy portów	Rodzaj obsługiwanych portów: D, E, EX, F, M lub równoważny Flow Mirror, N.
9.	Zarządzanie przełącznikiem	Transfer plików za pomocą SFTP. Standard zarządzający SMI-S.
10.	Bezpieczeństwo	Autoryzacja dostępu administracyjnego do przełącznika za pomocą RADIUS i TACACS+, LDAP, Microsoft Active Directory. Mechanizm tzw. Fabric Binding, umożliwiający zdefiniowanie listy przełączników FC mających prawo do uczestnictwa w fabryce FC. Definiowanie filtrów IP (list kontroli ACL) dla interfejsu zarządzającego. Protokół FC-SP (Fibre Channel Security Protocol). Bezpieczne ładowanie systemu wraz z zapewnieniem że obraz systemu pochodzi z legalnego i wiarygodnego źródła. Możliwość sprzętowego szyfrowania danych przesyłanych na 12

		portach FC z wykorzystaniem kluczy AES minimum 128 bit.
11.	Monitorowanie i diagnostyka	Sprzętowe monitorowanie połączeń (flows). Inspekcja nagłówków FC z pełną wydajnością (wirespeed). Wykrywanie i eliminowanie problemów zatykania (slow-drain) w sieci SAN. Rejestrowanie zdarzeń poprzez mechanizm „syslog”. Monitorowanie ruchu na portach przez kopiowanie ruchu z określonego portu na wybrany port monitorujący (np. z dołączonym zewnętrznym analizatorem) – tzw „port mirroring”. Narzędzia i metody diagnostyki dla Fibre Channel pozwalające identyfikować ścieżkę przepływu ruchu poprzez fizyczną fabrykę.
12.	Wentylatory	Przełącznik FC musi posiadać redundantne wentylatory oraz zasilacze.
13.	Dostawa	Dwa przełączniki światłowodowe muszą zostać dostarczone i zamontowane w budynku Biblioteki Śląskiej przy Placu Rady Europy 1. Wraz z dostawą musi zostać dostarczony niezbędny zestaw do zamontowania przełączników światłowodowych na wysuwanych szynach w szafie dystrybucyjnej 19” w tym m.in., kable zasilające, logiczne, elementy stałe, itp. oraz podłączenia i konfiguracji z pozostałym zamówionym sprzętem komputerowym.

1.4 System ochrony sieci UTM w klastrze – ilość 1 szt.

Lp.	Nazwa elementu/cechy	Wymagane minimalne parametry techniczne
1.	Ogólne	Klaster zapór sieciowych dostarczony w postaci zestawu **dwóch identycznych urządzeń sieciowych UTM (2 sztuki)** wraz z zainstalowanym oprogramowaniem, pochodzących od jednego producenta. Każde z dostarczonych dwóch urządzeń musi być przystosowane do zamontowania w szafie RACK 19" i ma zostać dostarczone wraz z niezbędnym do montażu sprzętem i okablowaniem oraz licencją na zewnętrzny centralny system zarządzania. Urządzenia w formie appliance posiadające minimum: • 4 porty 10G SFP+ wyposażone we wkładki w standardzie 10GBase-SR • 8 portow 10/100/1000Base-T • 1 USB Port • 1 Consola Port Urządzenie powinno posiadać: • wysokość nie więcej niż1U, • pamięć DRAM o pojemności nie mniejszej niż 32GB pozwalająca jednocześnie na zrealizowanie wszystkich wymagań zdefiniowanych w opisie przedmiotu zamówienia, • dysk SSD o pojemności nie mniejszej niż 240GB, • 2 redundantne zasilacze umożliwiające zasilanie prądem przemiennym 230V (niedopuszczalne rozwiązania zewnętrzne) z możliwością wymiany w trakcie pracy urządzenia (ang. hot-swap).
2.	Wymagania dotyczące architektury i funkcjonalności	Firewall: • Urządzenie powinno posiadać inspekcję stanową opartą na granularnej analizie komunikacji oraz stanu aplikacji w celu poprawnego śledzenia i kontroli przepływu ruchu. • Urządzenie powinno posiadać przepustowość firewalla nie mniejszą niż 31 Gbps dla pakietów UDP 1518B mierzoną w warunkach laboratoryjnych.

		• Urządzenie powinno posiadać możliwość zaraportowania ilości „trafień" wybranej polityki do aplikacji zarządzającej. • Tworzenie reguł powinno pozwalać na ich konfiguracje w określonych interwałach czasowych wraz z podaniem daty lub godziny ich wygaśnięcia. • Urządzenie musi posiadać możliwość konfiguracji reguł filtrowania ruchu w oparciu o tożsamość użytkownika (Identity Firewall), integrując się ściśle z usługą katalogową Microsoft Active Directory. • Klaster powinien posiadać możliwość skorzystania z lokalnej bazy użytkowników pozwalając na ich autentykację bez potrzeby korzystania z zewnętrznych rozwiązań. • Urządzenie pracujące w klastrze musi umożliwiać pracę w trybie Transparent/Bridge. • Rozwiązanie powinno wspierać wysoką dostępność (HA) Active/Active oraz Active/Passive wraz z dzieleniem obciążenia i synchronizacją stanu. • Urządzenie nie powinno posiadać ograniczenia na ilość jednocześnie pracujących użytkowników w sieci chronionej. • Rozwiązanie posiada możliwość komunikacji z serwerami uwierzytelnienia i autoryzacji za pośrednictwem protokołów RADIUS i TACACS+. • Powinno pozwalać na obsłużenie minimum 8.000.000 jednoczesnych sesji/połączeń z prędkością zestawiania 116.000 połączeń na sekundę. Wsparcie dla IPv6: • Rozwiązanie powinno pozwalać na obsługę IPv6 przez moduł Firewall, Kontroli Aplikacji, Antymalware, Filtrowania URL. • Rozwiązanie powinno wspierać 6 do 4 NAT lub 6 do 4 tuneli. • Powinno być zgodne z poniższymi RFC dotyczącymi IPv6: • RFC 1981 Path Maximum Transmission Unit Discovery for IPv6 • RFC 2460 IPv6 Basic specification • RFC 2464 Transmission of IPv6 Packets over Ethernet Networks • RFC 4007 IPv6 Scoped Address Architecture

		• RFC 4193 Unique Local IPv6 Unicast Addresses
		• RFC 4213 Basic Transition Mechanisms for IPv6 Hosts and Routers – wsparcie dla tuneli 6w4
		• RFC 4443 ICMPv6
		• RFC 4862 IPv6 Stateless Address Auto-configuration
		Intrusion Prevention System (IPS) musi:
		• Posiadać możliwość pracy w trybie in-line (wszystkie pakiety, które mają być poddane inspekcji muszą przechodzić przez system).
		• Posiadać możliwość pracy zarówno w trybie pasywnym (IDS) jak i aktywnym (z możliwością blokowania ruchu).
		• Posiadać możliwość wykrywania i uniemożliwiania szerokiej gamie zagrożeń (np.: złośliwe oprogramowanie, skanowanie sieci, ataki na usługi VoIP, próby przepełnienia bufora, ataki na aplikacje P2P, itp.).
		• Zapewniać co najmniej poniższe sposoby wykrywania zagrożeń:
		  • sygnatury ataków opartych na exploitach
		  • reguły oparte na zagrożeniach
		  • mechanizm wykrywania anomalii w protokołach
		• mieć możliwość inspekcji nie tylko warstwy sieciowej i informacji zawartych w nagłówkach pakietów, ale również szerokiego zakres protokołów na wszystkich warstwach modelu sieciowego włącznie z możliwością sprawdzania zawartości pakietu
		• posiadać wiele możliwości reakcji na zdarzenia takie jak: tylko monitorowanie, blokowanie ruchu zawierającego zagrożenia,
		• posiadać możliwość automatycznej inspekcji i ochrony dla ruchu wysyłanego na niestandardowych portach używanych do komunikacji
		• zapewniać możliwość obrony przed atakami skonstruowanym tak, aby uniknąć wykrycia przez IPS. W tym celu musi stosować najodpowiedniejszy mechanizm defragmentacji i składania strumienia danych w zależności od charakterystyki hosta docelowego
		• zapewniać mechanizm bezpiecznej aktualizacji sygnatur. Zestawy sygnatur/reguł muszą byś pobierane z serwera w

		sposób uniemożliwiający ich modyfikację przez osoby postronne • zapewniać możliwość definiowania wyjątków dla sygnatur z określeniem adresów IP źródła, przeznaczenia lub obu jednoczenie być zarządzany tylko poprzez system centralnego zarzadzania za pomocą szyfrowanego połączenia • zapewniać możliwość wykorzystanie informacji o sklasyfikowanych aplikacjach do tworzenia reguł IPS • mieć możliwość detekcji ataków i zagrożeń opartych na protokole IPv6 • mechanizm wykrywania anomalii w ogólnym zachowaniu ruchu sieciowego • posiadać możliwość wykorzystania mechanizmów obsługi ruchu asymetrycznego firewalla dla uzyskania pełnej widoczności ruchu - w szczególności musi posiadać możliwość pracy w trybie failover firewalla oraz w trybie klastrowania • powinien pozwalać na pracę z przepustowością co najmniej 3.6 Gbps mierzoną w warunkach typu Enterprise (Zamawiający nie dopuszcza urządzeń, gdzie w/w wartość jest zdefiniowana jako „lab" „ideal" itp. zbliżone w nazwie definiujące warunki idealne lub laboratoryjne) przy uruchomionych co najmniej modułach Stateful Firewall, kontrola aplikacji, IPS, anty-wirus, anty-bot, filtrowanie URL'i • powinien posiadać dostępną publicznie informację o przepustowości urządzenia nie mniejszą niż 6.1 Gbps mierzoną w warunkach typu Enterprise (zamawiający nie dopuszcza urządzeń, gdzie w/w wartość jest zdefiniowana jako „lab" „ideal" itp. zbliżone w nazwie definiujące warunki idealne lub laboratoryjne) przy uruchomionych co najmniej modułach Statefull Firewall, kontrola aplikacji, IPS • powinien posiadać dostępną publicznie informację o przepustowości urządzenia nie mniejszą niż 10 Gbps mierzoną w warunkach typu Enterprise (zamawiający nie dopuszcza urządzeń, gdzie w/w wartość jest zdefiniowana jako „lab" „ideal" itp. zbliżone w nazwie definiujące warunki idealne lub laboratoryjne) przy uruchomionym module IPS • powinien posiadać dostępną publicznie informację o przepustowości urządzenia nie mniejszą niż 18 Gbps mierzoną w warunkach typu Enterprise (zamawiający nie dopuszcza urządzeń, gdzie w/w wartość jest zdefiniowana jako „lab" „ideal" itp. zbliżone w nazwie definiujące warunki idealne lub laboratoryjne) przy uruchomionym module Stateful Firewall

		• pozwalać na ochronę protokołów VOIP Zamawiający oczekuje, że urządzenie w zakresie Identyfikacja użytkownika (User Identity) musi: • w oparciu o zdarzenia być zdolne do identyfikacji użytkownika poprzez zadanie zapytań do Microsoft Active Directory, • pozwalać na identyfikację i autentykację użytkownika dla zasobów nie związanych z domeną, • integrować się z usługami katalogowymi RADIUS, • powodować minimalny wpływ na kontrolery domeny, • wspierać nagłówki pozwalającą na identyfikację użytkownika (np. X-forwarded), System automatycznego wykrywania i klasyfikacji aplikacji wraz z filtrowaniem URL: • Baza znanych aplikacji powinna zawierać nie mniej niż 6000 pozycji. • Urządzenie musi pozwalać na kategoryzację adresów URL w liczbie przekraczającej 200 000 000. • Urządzenie powinno pozwalać na musi umożliwiać tworzenie reguł zawierających wiele kategorii. • Rozwiązanie powinno posiadać mechanizm ograniczenia użycia pasma. • Rozwiązanie powinno posiadać mechanizm definiowania wyjątków na poziomie zdefiniowanego obiektu. • Strona informująca o zablokowanym zasobie powinna być możliwa do zdefiniowania, dodatkowo powinna umożliwiać na przekierowanie użytkownika na inna stronę. • Urządzenie powinno wspierać mechanizmy białych i czarnych list. Wykrywanie malware oraz komunikacji z serwerami C&C: • Moduł wykrywający malware i botnety powinien być zintegrowaną z platformą aplikacją. • System Anti-Bot powinien umożliwiać wykrycie oraz blokadę podejrzanego zachowania w chronionych segmentach sieci. • Wykrycie zdarzenia powinno opierać na wielowarstwowej

		analizie
		• Urządzenie powinno umożliwiać wykrycie malware poprzez statyczną i dynamiczną analizę próbki.
		• Funkcjonalność powinna być zarządzana z centralnej konsoli.
		• Funkcjonalność powinna posiadać możliwość:
		  • inspekcji ruchu SSL,
		  • inspekcji plików skompresowanych,
		Inspekcja SSL (ruch przychodzący / wychodzący):
		• Funkcjonalność powinna pozwalać na wykorzystanie przez administratora filtrowania URL.
		Wykrywanie wiadomości SPAM:
		• Mechanizmy wykrywania wiadomości SPAM powinny być niezależne od języka i dodatkowo zawierać dane o reputacji adresu IP nadawcy w celu uniknięcia fałszywej klasyfikacji.
		Brama IPSec VPN:
		• Urządzenie powinno wspierać CA wewnętrzne oraz zewnętrzne.
		• Wsparcie dla 3DES oraz AES-256 dla fazy IKE I i II oraz IKEv2 oraz „Suite-B-GCM-128” i „Suite-B-GCM-256” dla fazy II
		• Rozwiązanie powinno wspierać site-to-site VPN w następujących topologiach:
		  • każdy do każdego (full mesh),
		  • gwiazda,
		  • połącznie poprzez huby.
		• Urządzenie powinno pozwalać na pracę z przepustowością 4.8Gbps dla VPN AES-128 mierzoną w warunkach laboratoryjnych.
		Ochrona przed wyciekiem informacji (Data Loss Prevention):
		• Urządzenie UTM musi umożliwiać zrealizowanie funkcjonalności pozwalającej na wykrywanie wycieków informacji (Data Loss Prevention).

3.	Zarządzanie	Centralny System Zarządzania musi spełniać co najmniej poniższe wymagania dotyczące architektury i funkcjonalności: • Poprzez zarządzanie należy rozumieć konfigurację polityki bezpieczeństwa (polityka firewall, VPN, polityka ochrony antywirusowej, antyspamowej, ochrony przed atakami sieciowymi, atakami typu botnet, kontrola aplikacji), zarządzanie kontami administratorów i użytkowników, obsługę zdarzeń generowanych przez moduły zapór sieciowych. • Centralny System Zarządzania posiada wewnętrzny, zintegrowany urząd certyfikacji /Certificate Authority/. • Centralny System Zarządzania jest obsługiwany za pomocą konsoli użytkownika, która ma być dostarczona w postaci dedykowanej graficznej konsoli administratora (GUI) działającej pod systemem operacyjnym Windows. Konsola zarządzania posiada możliwości automatycznej weryfikacji spójności i niesprzeczności wprowadzonej polityki bezpieczeństwa. • Komunikacja pomiędzy modułem zapory sieciowej (funkcjonujących na zewnętrznych urządzeniach) i modułem zarządzania i raportowania (Centralny System Zarządzania) jest szyfrowana i uwierzytelniona z użyciem certyfikatów cyfrowych generowanych przez moduł zarządzania i raportowania (Centralny System Zarządzania). • Komunikacja pomiędzy interfejsem GUI i modułem zarządzania i raportowania (Centralny System Zarządzania) jest szyfrowana. • Uwierzytelnianie administratorów odbywa się za pomocą haseł statycznych, haseł dynamicznych lub certyfikatów cyfrowych. Istnieje możliwość definiowania szczegółowych uprawnień administratorów (np. tylko do odczytu logów, tylko do zarządzania użytkowników). • System zarządzania (Centralny System Zarządzania) jest w stanie wyświetlić z graficznej konsoli listę aktywnych połączeń obsługiwanych przez moduły zapór sieciowych. Informacja o połączeniu powinna zawierać minimum adres źródła, adres przeznaczenia, port źródła, port przeznaczenia oraz identyfikator usługi sieciowej. • System zarządzania i raportowania (Centralny System Zarządzania) umożliwia wyszukiwanie i filtrację zdarzeń wygenerowanych przez moduły zabezpieczeń. Administrator jest w stanie zdefiniować własne szablony wyszukiwania i wyświetlania zdarzeń. • Centralny System Zarządzania umożliwia monitorowanie i prezentowanie za pomocą graficznej konsoli takich parametrów sprzętowych zarządzanych zapór sieciowych jak: średnie obciążenie procesora, zajętość pamięci

		operacyjnej, zajętość przestrzeni dyskowej, wersję oprogramowania zapory sieciowej, nazwę i wersję zainstalowanej polityki bezpieczeństwa. • Centralny System Zarządzania umożliwia graficzne wyświetlanie statystyk ruchu sieciowego, przetwarzanego przez zapory sieciowe, takich jak: najczęściej wykorzystywane usługi sieciowe, najczęstsze źródła transmisji, najczęstsze adresy docelowe, aktywne i zerwane tunele VPN. • System zarządzania (Centralny System Zarządzania) umożliwia integrację z usługą katalogową LDAP, w szczególności z Microsoft Active Directory. Integracja ma co najmniej polegać na możliwości zaimportowania grup użytkowników z LDAP oraz wykorzystywanie tych grup w regułach polityki bezpieczeństwa. • Centralny System Zarządzania musi pobierać dzienniki zdarzeń (logi) z wielu różnych elementów systemu informatycznego, w tym z Centralny System Zarządzania, poddawać je korelacji i na tej podstawie przedstawiać administratorom informacje na temat stanu bezpieczeństwa i wykrytych incydentów. • Centralny System Zarządzania musi mieć możliwość dokonywać wykrywania anomalii w systemie informatycznym za pomocą analizy behawioralnej. W tym celu musi istnieć możliwość budowania profili normalnego stanu i zachowania sieci oraz identyfikowane odchylenia (m.in. nagłe odchylenia natężenia ruchu i przekroczenie wartości progowych). Centralny serwer zarządzania może zostać dostarczony jako maszyna wirtualna instalowana na środowisku VMWare. Licencja powinna pozwalać na zarządzanie do 5 bram przy parametrach sprzętowych i wydajnościowych nie mniejszych niż: • pamięć DRAM o pojemności nie mniejszej niż 16GB • dysk twardy nie mniejszy niż 1TB • 2 porty USB pozwalające na podłączenie zewnętrznych urządzeń
4.	Dostawa	Klaster zapór sieciowych musi zostać dostarczony i zamontowany w budynku Biblioteki Śląskiej przy Placu Rady Europy 1. Wraz z dostawą musi zostać dostarczony niezbędny zestaw do zamontowania klastra zapór sieciowych na wysuwanych szynach w szafie dystrybucyjnej 19” w tym m.in., kable zasilające, logiczne, elementy stałe, itp. oraz podłączenia i konfiguracji z pozostałym zamówionym sprzętem komputerowym.

1.5 Oprogramowanie do zarządzania komputerami – ilość 96 szt. (96 licencji na urządzenia aktywne).

Lp.	Nazwa elementu/cechy	Wymagane minimalne parametry techniczne
1.	Ogólne	Oprogramowanie musi posiadać budowę modułową, składającą się z serwera zarządzającego, zdalnych konsoli oraz agentów. Komunikacja pomiędzy serwerem a agentami i konsolami nawiązywana musi być przy użyciu szyfrowanego protokołu TLS 1.2. Moduły muszą umożliwiać kompleksowy monitoring sieci, monitoring sprzętu komputerowego na stanowiskach użytkowników pod kątem zmian sprzętowych i programowych oraz pomocy w formie interaktywnego połączenia sieciowego z obsługiwanym użytkownikiem. Dane, które dotyczą działań pracownika na komputerze, a więc: historia aktywności, polityka korzystania z Internetu oraz aplikacji, dostęp do zewnętrznych nośników danych itp., muszą być odseparowane od danych stricte technicznych tj. informacji o stacji roboczej. Muszą one być pogrupowane w osobnym, dedykowanym oknie. Musi to pozwalać na, zgodne z RODO, usuwanie danych wybranego użytkownika bez konieczności usunięcia informacji o stacji roboczej. Dostęp do danych osobowych oraz danych z monitoringu, zgodnie z RODO, objęty jest kontrolą na poziomie wybranych Administratorów – w programie można nadawać kontom administracyjnym różne poziomy dostępu oraz uprawnień zarówno do grup urządzeń, jak i użytkowników **Oprogramowanie musi być dostarczone z licencją bezterminową na co najmniej 96 dodatkowych urządzeń aktywnych dla których możliwa jest instalacja i konfiguracja agenta. Zamawiający obecnie posiada oprogramowanie Axence nVision Server oraz 30 licencji nVision axence dla wszystkich modułów. Dostawa musi zostać zrealizowana jako rozszerzenie istniejących/posiadanych przez Zamawiającego 30 licencji oprogramowania nVision axence lub 30 licencji oprogramowania kompatybilnego. Przez kompatybilność z istniejącym oprogramowaniem należy rozumieć możliwość centralnego zarządzania wszystkimi licencjami łącznie przy pomocy konsoli.**
2.	Monitorowanie infrastruktury	Bezagentowo, musi obejmować serwery Windows, Linux, Unix, Mac; routery, przełączniki, urządzenia VoIP i firewalle w zakresie: • wykrywania urządzeń w sieci poprzez skanowanie ping (oraz arp-ping),

		• wizualizacji stanu urządzeń w postaci ikon urządzeń na mapach sieci, • wizualizacji połączeń pomiędzy urządzeniami a przełącznikami i informacji, do którego portu przełącznika podłączone jest dane urządzenie, • serwisów TCP/IP, HTTP, POP3, SMTP, FTP i innych wraz z możliwością definiowania własnych serwisów. Program monitoruje czas ich odpowiedzi i procent utraconych pakietów, • serwerów pocztowych: – program monitoruje zarówno serwis odbierający, jak i wysyłający pocztę, – program ma możliwość monitorowania stanu systemów i wysyłania powiadomienia (e-mail, SMS i inne), w razie gdyby przestały one odpowiadać lub funkcjonowały wadliwie (np. gdy ważne parametry znajdą się poza zakresem), – program ma możliwość wykonywania operacji testowych, – program ma możliwość wysłania powiadomienia jeśli serwer pocztowy nie działa, • monitorowania serwerów WWW i adresów URL, • obsługi szyfrowania TLS w powiadomieniach e-mail, • obsługi urządzeń SNMP wspierających SNMP v1/2/3 (np. przełączniki, routery, drukarki sieciowe, urządzenia VoIP, temperatura, wilgotność, napięcie zasilania, itp.), • obsługi komunikatów syslog i pułapek SNMP, • monitoringu routerów i przełączników wg: – zmian stanu interfejsów sieciowych, – ruchu sieciowego, – podłączonych stacji roboczych, – ruchu generowanego przez podłączone stacje robocze. • serwisów Windows: monitor serwisów Windows alarmuje gdy serwis przestanie działać oraz pozwala na jego uruchomienie/zatrzymanie/zrestartowanie

		• wydajności systemów Windows - obciążenie CPU, pamięci, zajętość dysków, transfer sieciowy. Oprogramowanie musi posiadać możliwość tworzenia dynamicznych map tworzonych wg. własnych filtrów, pozwalających na logiczną strukturę organizację zarządzania urządzeniami.
3.	Inwentaryzacja infrastruktury teleinformatycznej	Oprogramowanie musi automatycznie gromadzić informację o sprzęcie komputerowym i oprogramowaniu na komputerach oraz: • prezentować szczegóły dotyczące sprzętu: modelu, procesora, pamięci, płyty głównej, napędów, kart itp., • prezentować m.in.: zestawienie posiadanych konfiguracji sprzętowych, wolne miejsce na dyskach, średnie wykorzystanie pamięci, informacje pozwalające na wytypowanie systemów, dla których konieczny jest upgrade, • informować o zainstalowanych aplikacjach oraz aktualizacjach Windows co bezpośrednio umożliwia audytowanie i weryfikację użytkowania licencji w organizacji, • zbierać informacje w zakresie wszystkich zmian przeprowadzonych na wybranym komputerze: instalacji/deinstalacji aplikacji, zmian adresu IP itd., • posiadać możliwość wysyłania powiadomienia np. e-mailem w przypadku zainstalowania programu lub jakiejkolwiek zmiany konfiguracji sprzętowej komputera, • umożliwiać odczytanie numeru seryjnego (klucze licencyjne), • umożliwiać automatyczne zarządzanie instalacjami i deinstalacjami oprogramowania poprzez określenie paczek aplikacji wymaganych oraz nieautoryzowanych, • umożliwiać przegląd informacji o konfiguracji systemu, np. komend startowych, zmiennych środowiskowych, kontach lokalnych użytkowników, harmonogramie zadań itp. Oprogramowanie inwentaryzacji sprzętu musi umożliwiać prowadzenie bazy ewidencji majątku IT w zakresie: • przechowywania wszystkich informacji dotyczących infrastruktury IT w jednym miejscu oraz automatycznego aktualizowania zgromadzonych informacji, • definiowania własnych typów (elementów wyposażenia), ich atrybutów oraz wartości - dla danego urządzenia lub oprogramowania istnieje możliwość dodawania dodatkowych informacji, np. numer inwentarzowy, osoba odpowiedzialna,

		numer i skan faktury zakupu, wartość sprzętu lub oprogramowania, nazwa sprzedawcy, termin upływu i skan gwarancji, termin kolejnego przeglądu (można podać datę, po której administrator otrzyma powiadomienie o zbliżającym się terminie przeglądu lub upływie gwarancji), nazwa firmy serwisującej, inny dowolny załącznik (np. plik .DOCX, .XLSX, .PDF), skan dowolnego dokumentu, czy też własny komentarz; dodatkowo istnieje możliwość importu danych z zewnętrznego źródła (.CSV), • generowania zestawienia wszystkich środków trwałych, w tym urządzeń i zainstalowanego na nich oprogramowania, • archiwizacji i porównywania audytów środków trwałych, • tworzenia kodów kreskowych w środkach trwałych, • drukowania kodów kreskowych oraz dwuwymiarowych kodów alfanumerycznych (QR Code) dla środków trwałych, które posiadają numer inwentarzowy, • inwentaryzacji sprzętu posiadającego kody kreskowe za pomocą aplikacji mobilnej na system Android, • inwentaryzacji komputerów niepodłączonych do sieci (bez instalacji Agenta poprzez manualne wykonanie skanów inwentaryzacji offline). Dodatkowo muszą być dostępni agenci inwentaryzacji na systemy Android, macOS oraz Linux. Inwentaryzacja oprogramowania musi zapewnić funkcjonalność w zakresie pozyskiwania informacji o oprogramowaniu i audycie licencji poprzez: • skanowanie plików wykonywalnych i multimedialnych na komputerach, skanowanie archiwów ZIP, • zarządzanie posiadanymi licencjami, • łatwy audyt legalności oprogramowania oraz powiadamianie tylko w razie przekroczenia liczby posiadanych licencji - w każdej chwili istnieje możliwość wykonania aktualnych raportów audytowych, • zarządzanie posiadanymi licencjami: raport zgodności licencji. • możliwość przypisania do programów numerów seryjnych, wartości itp. Okna audytowe posiadają możliwość filtrowania elementów per

		oddział.
4.	Obsługa użytkowników	Oprogramowanie musi umożliwiać monitorowanie aktywności użytkowników pracujących na komputerach z systemem Windows poprzez monitorowanie: • faktycznego czasu aktywności (dokładny czas pracy z godziną rozpoczęcia i zakończenia pracy), • procesów (każdy proces ma całkowity czas działania oraz czas aktywności użytkownika) wraz informacją o uruchomieniu na podwyższonych uprawnieniach, • rzeczywistego użytkowania programów (m.in. procentowa wartość wykorzystania aplikacji, obrazująca czas jej używania w stosunku do łącznego czasu, przez który aplikacja była uruchomiona), • informacji o edytowanych przez użytkownika dokumentach, • historii pracy (cykliczne zrzuty ekranowe), • listy odwiedzanych stron WWW (liczba odwiedzin stron z nagłówkami, liczbą i czasem wizyt), • transferu sieciowego użytkowników (ruch lokalny i transfer internetowy generowany przez użytkownika), • wydruków m.in. informacje o dacie wydruku, informacje o wykorzystaniu drukarek, raporty dla każdego użytkownika (kiedy, ile stron, jakiej jakości, na jakiej drukarce, jaki dokument był drukowany), zestawienia pod względem komputera (kiedy, ile stron, jakiej jakości, na jakiej drukarce, jaki dokument drukowano z danej stacji roboczej), możliwość "grupowania" drukarek poprzez identyfikację drukarek. Program musi mieć możliwość monitorowania kosztów wydruków, • nagłówków przesyłanej poczty e-mail. Oprogramowanie ponadto musi posiadać możliwość: • blokowania stron internetowych poprzez możliwość zezwolenia lub zablokowania całego ruchu WWW dla danej stacji roboczej z możliwością definiowania wyjątków – zarówno zezwalających, jak i zabraniających korzystania z danych domen oraz wybranych lub dowolnych sub-domen (np. *.domena.pl), • blokowania ruchu na wskazanych portach TCP/IP,

		• blokowania pobierania poprzez przeglądarki internetowe plików z określonym rozszerzeniem, • wysyłania powiadomień gdy użytkownik: odwiedzi stronę z określonej grupy domeny; pobierze lub wyśle określoną ilość danych w ciągu dnia w sieci lokalnej lub Internet; wydrukuje określoną ilość stron w ciągu dnia. • generowania raportów dla użytkowników Active Directory niezależnie od tego, na jakich komputerach pracowali w danym czasie. • blokowania uruchamiania aplikacji. • tworzenia grup użytkowników do których można przypisywać określonych użytkowników
5.	Zdalna pomoc użytkownikom	Musi umożliwiać podgląd pulpitu użytkownika i możliwość przejęcia nad nim kontroli. Podczas dostępu zdalnego, zarówno użytkownik jak i administrator widzą ten sam ekran. Administrator w trakcie zdalnego dostępu ma możliwość zablokowania działania myszy oraz klawiatury dla użytkownika. W niniejszym module musi znajdować się baza zgłoszeń umożliwiająca użytkownikom zgłaszanie problemów technicznych, które z kolei są przetwarzane i przyporządkowywane odpowiednim administratorom, otrzymującym automatycznie powiadomienie o przypisanym im problemie. Musi umożliwiać użytkownikom monitorowania procesu rozwiązywania zgłoszonych przez nich problemów i ich aktualnych statusów, jak również możliwość wymiany informacji z administratorem poprzez komentarze, które są wpisywane i widoczne dla obu stron. Moduł musi zawierać komunikator (czat), który umożliwia przesyłanie wiadomości pomiędzy zalogowanymi użytkownikami i administratorami (wraz z wyszukiwarką wiadomości) oraz bazę wiedzy pomagającą użytkownikom samodzielnie rozwiązywać najprostsze, powtarzające się problemy. Moduł pomocy zdalnej musi umożliwiać: • pobieranie listy użytkowników z Active Directory, • przypisywanie pracowników helpdesk do kategorii zgłoszeń, • procesowanie zgłoszeń użytkowników z wiadomości e-mail, • wykonywanie operacji na wielu zgłoszeniach równocześnie,

		• dołączanie załączników do zgłoszeń, • zrzuty ekranowe (podgląd pulpitu), • dystrybucję oprogramowania przez agenta, • dystrybucję oraz uruchamianie plików za pomocą agentów (w tym plików MSI), • zadania dystrybucji plików, jeśli komputer jest wyłączony w trakcie zlecania operacji następuje kolejkowanie zadania dystrybucji pliku, • możliwość skonfigurowania automatyzacji procesowania zgłoszeń, • planowanie nieobecności pracowników helpdesk, • obsługę umów o gwarantowanym poziomie świadczenia usług (SLA), • generowanie raportów obsługi helpdesk, • zdalne wykonywanie poleceń poprzez Agenty (np. utworzenie / edycja konta lokalnego użytkownika systemu).
6.	Ochrona danych przed wyciekiem danych	Oprogramowanie musi umożliwiać blokowanie urządzeń w tym: • blokowanie urządzeń i nośników danych, program ma możliwość zarządzania prawami dostępu do wszystkich urządzeń wejścia i wyjścia oraz urządzeń fizycznych, na które użytkownik może skopiować pliki z komputera firmowego lub uruchomić z nich program zewnętrzny, • blokowanie urządzeń i interfejsów fizycznych: USB, FireWire, gniazda kart pamięci, SATA, dyski przenośne, napędy CD/DVD, stacje dyskietek, • blokowanie interfejsów bezprzewodowych: Wi-Fi, Bluetooth, IrDA, • blokownie dotyczy tylko urządzeń służących do przenoszenia danych - inne urządzenia (drukarka, klawiatura, mysz itp.) mogą być podłączane. Zarządzanie prawami dostępu do urządzeń: • definiowanie praw użytkowników/grup do odczytu, zapisu czy wykonania plików,

		• autoryzowanie urządzeń firmowych (przykładowo szyfrowanych): pendrive'ów, dysków itp. - urządzenia prywatne są blokowane, • całkowite zablokowanie określonych typów urządzeń dla wybranych użytkowników, • centralna konfiguracja poprzez ustawienie reguł (polityk) dla całej sieci. Audyt operacji na urządzeniach przenośnych: • zapisywanie informacji o zmianach w systemie plików na urządzeniach przenośnych. • podłączenie/odłączenie urządzenia przenośnego. Integracja z Active Directory - zarządzanie prawami dostępu przypisanymi do użytkowników oraz grup domenowych. Przydzielanie uprawnień również do kont użytkowników lokalnych. Program musi być zabezpieczony hasłem przed ingerencją użytkownika w jego działanie i próbą usunięcia, nawet jeśli użytkownik ma prawa administratora. Program musi być dostępny w języku polskim i angielskim wraz z podręcznikiem użytkownika w formie strony internetowej.
7.	Monitorowanie temperatury i wilgotności powietrza w serwerowni głównej i zapasowej	W ramach zamówienia Wykonawca musi dostarczyć i skonfigurować fizyczne urządzenia/czujniki współpracujące z dostarczonym oprogramowaniem z poz. 2.6, co najmniej po jednym dla serwerowni głównej i zapasowej, które będą umożliwiały odczytywanie aktualnej temperatury i wilgotności, a następnie tą informację przekazywały on-line do oprogramowania z poz. 2.6. Kolejno administrator będzie mógł ją odczytać na monitorze swojego komputera z poziomu oprogramowania z poz. 2.6.
8.	Dostawa	Oprogramowanie musi zostać dostarczone i zainstalowane w budynku Biblioteki Śląskiej przy Placu Rady Europy 1 oraz w budynku Biblioteki Śląskiej na ul. Ligonia 7.

1.6 Instalacja i konfiguracja części od 2.2 do 2.6 – ilość 1 szt.

Lp.	Nazwa elementu/cechy	Wymagane minimalne parametry techniczne
1	Ogólne	Opracowanie przez Wykonawcę zgodnie z wytycznymi Zamawiającego oraz akceptacją przez Zamawiającego projektu technicznego dla pozycji od 2.2 do 2.6 uwzględniającego w tym m.in.: • Instalacja i konfiguracja pozycji od 2.2 do 2.6 w dostarczonych 19” szafach, • Instalacja i uruchomienie pozycji od 2.2 do 2.6 wraz z serwerami wysokiej dostępności, macierzą dyskową oraz obiektowym systemem składowania danych. Instalacja, konfiguracja oraz produkcyjne uruchomienie pozycji od 2.2 do 2.6 zgodnie z zaakceptowanym przez Zamawiającego projektem technicznym.

1.7 Szkolenia – ilość 1 szt.

Lp.	Nazwa szkolenia	Wymagane minimalne parametry techniczne
1.	Szkolenie z administracji switchem LAN i FC	Rodzaj szkolenia: • autoryzowane lub • wykonane przez inżyniera Wykonawcy lub • wykonane przez producenta dostarczonego sprzętu lub oprogramowania. Szkolenie musi być co najmniej jednodniowe, Szkolenie musi być z zakresu dostarczonego switcha LAN I FC. Szkolenie musi obejmować pełen zakres informacji na temat zarządzania dostarczonym przełącznikiem sieciowym i światłowodowym, Po ukończeniu szkolenia, każdy uczestnik ma otrzymać stosowny dokument potwierdzający uzyskanie kompetencji do administrowania dostarczonym przełącznikiem sieciowym i światłowodowym, Szkolenie będzie się odbywało na terenie Katowic lub wykonawca pokryje koszty transportu i noclegu w przypadku miejsca szkolenia innego niż Katowice. Szkolenie przeznaczone dla trzech osób.
2.	Szkolenie z administracji klastrem zapór sieciowych	Rodzaj szkolenia: • autoryzowane lub • wykonane przez inżyniera Wykonawcy lub • wykonane przez producenta dostarczonego sprzętu lub oprogramowania. Szkolenie musi być co najmniej pięciodniowe, Szkolenie musi być z zakresu dostarczonego klastra zapór sieciowych jego administracji i konfiguracji w tym m.in.: • budowa klastra zapór sieciowych, • omówienie funkcjonalności jaka jest dostępna dla klastra

		zapór sieciowych, • omówienie zasad budowania zapór i konfigurowania zapór w oparciu o klaster zapór sieciowych. Po ukończeniu szkolenia, każdy uczestnik ma otrzymać stosowny dokument potwierdzający uzyskanie kompetencji do administrowania dostarczonym klastrem zapór sieciowych. Szkolenie będzie się odbywało na terenie Katowic lub wykonawca pokryje koszty transportu i noclegu w przypadku miejsca szkolenia innego niż Katowice. Szkolenie przeznaczone dla trzech osób.

3. System do wykonywania kopii zapasowych.

3.1 System do wykonywania kopii zapasowych – identyczne serwery backupu – ilość 3 szt.

Lp.	Wymagane minimalne parametry techniczne
1.	Rozwiązanie powinno być dostarczone w formie platformy sprzętowej lub sprzętowo-programowej.
2.	Urządzenie musi posiadać na swej liście wsparcia i znajdować się na listach wsparcia bieżących wersji wersji oprogramowania backupowego: HP Data Protector, Veeam. Commvault, Networker
3.	Urządzenie, musi być przystosowane do montażu w szafach teleinformatycznych Zamawiającego o rozmiarach 42U – 19” i dostarczone z zestawem elementów niezbędnych do montażu w w/w szafach.
4.	Urządzenie zostanie dostarczone z wszystkimi niezbędnymi przewodami umożliwiającymi podłączenie i uruchomienie z obecną infrastrukturą Zamawiającego.
5.	Urządzenie musi być wyposażone w minimum dwa redundantne obwody zasilania. Awaria jednego ze źródeł zasilania, nie może spowodować spadku wydajności oraz przerwy w działaniu systemów informatycznych korzystających z zasobów urządzenia.
6.	Urządzenie musi zapewniać replikację zdeduplikowanych zasobów poprzez sieć WAN/LAN (bez tzw. rehydracji) zarządzaną bezpośrednio przez oprogramowanie kopii zapasowych przez interfejsy OST lub dedykowane moduły integracyjne.
7.	Wszystkie zabezpieczane dane składowane na oferowanym urządzeniu powinny być deduplikowane.
8.	Proces deduplikacji musi odbywać się in-line w pamięci oferowanego urządzenia, przed zapisem danych na nośnik dyskowy. Zapisowi na system dyskowy muszą podlegać jedynie unikalne bloki danych nie zapisane dotychczas na system dyskowy. Dotyczy to każdego fragmentu przychodzących do oferowanego urządzenia.
9.	Urządzenie musi posiadać pojemność netto 140 TB na składowanie danych

	zdeduplikowanych.
10.	Urządzenie musi posiadać możliwość rozbudowy do pojemności netto 200 TB w przypadku spełnienia wymagań dot. deduplikacji bez konieczności wymiany i dokładania kontrolerów.
11.	Urządzenie musi posiadać minimum następujące porty: • 2x minimum 1Gb/s Eth BaseT, • 2x16Gb/s FC.
12.	Minimalne poziomy wydajności urządzenia dla maksymalnej konfiguracji (znajdujące się w oficjalnej ogólnodostępnej dokumentacji producenta): • w przypadku deduplikacji na źródle: 30TB/h, • bez deduplikacji na źródle: 15TB/h, • w przypadku wątpliwości Zamawiający zastrzega sobie możliwość przeprowadzenia testów akceptacyjnych w oparciu o oferowane urządzenie, w przypadku nieosiągnięcia wymaganej wydajności urządzenie nie zostanie odebrane.
13.	Urządzenie musi umożliwiać replikację danych do drugiego urządzenia takiego samego typu jak oferowane. Replikacja musi się odbywać w trybie asynchronicznym, transmitowane muszą być tylko te fragmenty danych (bloki), które nie znajdują się na docelowym urządzeniu. W przypadku wykorzystania portów Ethernet do replikacji urządzenie musi umożliwiać przyjmowanie backupów, odtwarzanie danych, przyjmowanie strumienia replikacji, wysyłanie strumienia replikacji tymi samymi portami. Wymagana możliwość ograniczenia pasma używanego do replikacji między dwoma urządzeniami.
14.	Urządzenie ze względów bezpieczeństwa powinno zabezpieczać dane przed możliwością nadpisania. Dane przeterminowane powinny być usuwane w procesie czyszczenia lub na żądanie administratora.
15.	Urządzenie musi być dostarczone z licencją zapewniającą przechowywanie zdeduplikowanych danych na obiektowej pamięci masowej lub bibliotece podłączonej do systemu. Zarządzanie wyniesieniem danych na zewnątrz musi być zarządzane z interfejsu oprogramowania zarządzającego kopiami zapasowymi.
16.	Urządzenia muszą zostać dostarczone i zamontowane po jednej sztuce w budynku Biblioteki Śląskiej przy Placu Rady Europy 1 i przy ulicy Ligonia 7. Wraz z dostawą musi zostać dostarczony niezbędny zestaw do zamontowania serwera backupu na wysuwanych szynach w szafie teleinformatycznej 19” w tym m.in., kable zasilające, logiczne, elementy stałe, itp. oraz podłączenia i konfiguracji z pozostałym zamówionym

	sprzętem komputerowym.

3.2 System do wykonywania kopii zapasowych - oprogramowanie do backupu – ilość 1 szt.

Lp.	**Wymagane minimalne parametry techniczne**
1.	Zamawiający wymaga dostarczenia, uruchomienia i wdrożenia oprogramowania do zabezpieczania środowiska Data Center Zamawiającego (baz danych, maszyn wirtualnych, serwerów plików, serwerów wolnostojących) zwanego dalej oprogramowaniem. Zabezpieczone backupem powinny być objęte wszystkie dostarczone w ramach niniejszego postępowajnia serwery oraz będący w posiadaniu Zamawiającego serwer kompresji (jako serwer fizyczny)
2.	Wymagane jest dostarczenie wszystkich modułów oprogramowania tak, aby zapewnić backup całości wyspecyfikowanego środowiska oraz spełnić wszystkie wymienione w niniejszej tabeli funkcjonalności.
Wymagania dotyczące backupu serwerów zwirtualizowanych	
3.	Oprogramowanie do musi współpracować z infrastrukturą VMware w wersji 5.0, 5.1, 5.5, 6.0, 6.5 oraz 6.7. Oprogramowanie musi współpracować z hostami zarządzanymi przez VMware vCenter oraz pojedynczymi hostami. Oprogramowanie musi zapewniać tworzenie kopii zapasowych wszystkich systemów operacyjnych maszyn wirtualnych wspieranych przez vSphere. Oprogramowanie musi być niezależne sprzętowo i umożliwiać wykorzystanie dowolnej platformy serwerowej i dyskowej. Oprogramowanie musi tworzyć “samowystarczalne” archiwa do odzyskania których nie wymagana jest osobna baza danych z metadanymi deduplikowanych bloków. Oprogramowanie musi mieć mechanizmy deduplikacji i kompresji w celu zmniejszenia wielkości archiwów. Włączenie tych mechanizmów nie może skutkować utratą jakichkolwiek funkcjonalności wymienionych w tej specyfikacji. Oprogramowanie musi zapewniać warstwę abstrakcji nad poszczególnymi urządzeniami pamięci masowej, pozwalając utworzyć jedną wirtualną pulę pamięci na kopie zapasowe.

	Wymagane jest wsparcie dla nieograniczonej liczby pamięci masowych to takiej puli. Oprogramowanie nie może przechowywać danych o deduplikacji w centralnej bazie. Utrata bazy danych używanej przez oprogramowanie nie może prowadzić do utraty możliwości odtworzenia backupu. Oprogramowanie musi zapewniać backup jednoprzebiegowy - nawet w przypadku wymagania granularnego odtworzenia. Oprogramowanie musi mieć możliwość uruchamiania dowolnych skryptów przed i po zadaniu backupowym lub przed i po wykonaniu zadania snapshota. Oprogramowanie musi oferować portal samoobsługowy, umożliwiający odtwarzanie użytkownikom wirtualnych maszyn, obiektów baz danych MS SQL oraz Oracle. Oprogramowanie musi zapewniać możliwość delegacji uprawnień do odtwarzania na portalu webowym. Oprogramowanie musi mieć możliwość integracji z innymi systemami poprzez wbudowane RESTful API Oprogramowanie musi mieć wbudowane mechanizmy backupu konfiguracji w celu prostego odtworzenia systemu po całkowitej reinstalacji Oprogramowanie musi mieć wbudowane mechanizmy szyfrowania zarówno plików z backupami jak i transmisji sieciowej. Włączenie szyfrowania nie może skutkować utratą jakiejkolwiek funkcjonalności wymienionej w tej specyfikacji. Oprogramowanie musi posiadać architekturę klient/serwer z możliwością instalacji wielu instancji konsoli administracyjnych. Oprogramowanie musi wykorzystywać mechanizmy Change Block Tracking na wszystkich wspieranych platformach wirtualizacyjnych. Mechanizmy muszą być certyfikowane przez dostawcę platformy wirtualizacyjnej. Oprogramowanie musi integrować się bezpośrednio z HPE StoreServe, Nimble Storage Dell EMC VNX, VNXe, Unity, IBM Spectrum Virtualize (IBM Storwize, IBM SVC, Lenovo Storage V-series), Huawei OceanStor, Pure Storage FlashArray, i musi zapewniać tworzenie kopii zapasowych z bezpośrednim wykorzystaniem snapshotów macierzowych. Musi też zapewniać odtwarzanie maszyn wirtualnych z takich snapshotów. Proces wykonania kopii zapasowej nie może wymagać użycia jakichkolwiek hostów tymczasowych. Opisana funkcjonalność powinna działać w środowisku VMware. Takie same funkcjonalności powinny być zapewnione dla macierzy Netapp z oprogramowaniem ONTAP 8.1 i nowsze włączając możliwość wykonania backupów z zmirrorowanych snapshotów SnapVault lub SnapMirror. Rozwiązanie musi wspierać dowolną metodę wdrożenia macierzy (klaster i 7-mode). Oprogramowanie musi wspierać kopiowanie backupów na taśmy wraz z pełnym śledzeniem wirtualnych maszyn. Oprogramowanie musi mieć możliwość wydzielenia osobnej roli typu tape server.

	Oprogramowanie musi mieć możliwość kopiowania backupów do lokalizacji zdalnej. Oprogramowanie musi mieć możliwość tworzenia retencji GFS (Grandfather-Father-Son). Oprogramowanie musi umieć korzystać z protokołu DDBOOST w przypadku gdy repozytorium backupów jest umiejscowione na Dell EMC DataDomain. Funkcjonalność powinna wspierać łącze sieciowe lub FC. Oprogramowanie musi umieć korzystać z protokołu Catalyst w przypadku gdy repozytorium backupów jest umiejscowione na HPE StoreOnce. Funkcjonalność powinna wspierać łącze sieciowe lub FC. Oprogramowanie musi mieć możliwość kopiowania backupów oraz replikacji wirtualnych maszyn z wykorzystaniem wbudowanej akceleracji WAN. Oprogramowanie musi mieć możliwość replikacji włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere, pomiędzy hostami ESXi, włączając asynchroniczną replikacją ciągłą. Dodatkowo oprogramowanie musi mieć możliwość użycia plików kopii zapasowych jako źródła replikacji. Oprogramowanie musi umożliwiać przechowywanie punktów przywracania dla replik. Oprogramowanie musi umożliwiać wykorzystanie istniejących w infrastrukturze wirtualnych maszyn jako źródła do dalszej replikacji (replica seeding). Oprogramowanie musi wykorzystywać wszystkie oferowane przez hypervisor tryby transportu (sieć, hot-add, LAN Free-SAN). Oprogramowanie musi dawać możliwość tworzenia backupów ad-hoc z konsoli jak i z klienta webowego vSphere. Oprogramowanie musi przetwarzać wiele wirtualnych dysków jednocześnie (parallel processing). Oprogramowanie musi umożliwiać uruchomienie wielu maszyn wirtualnych bezpośrednio ze zdeduplikowanego i skompresowanego pliku backupu, z dowolnego punktu przywracania, bez potrzeby kopiowania jej na storage produkcyjny. Oprogramowanie musi pozwalać na migrację on-line tak uruchomionych maszyn na storage produkcyjny. Migracja powinna odbywać się mechanizmami wbudowanymi w hypervisor. Jeżeli licencja na hypervisor nie posiada takich funkcjonalności - oprogramowanie musi realizować taką migrację swoimi mechanizmami. Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny, plików konfiguracji i dysków. Oprogramowanie musi umożliwić odtworzenie plików na maszynę operatora, lub na serwer produkcyjny bez potrzeby użycia agenta instalowanego wewnątrz wirtualnej maszyny. Funkcjonalność ta nie powinna być ograniczona wielkością i liczbą przywracanych plików. Oprogramowanie musi mieć możliwość odtworzenia plików bezpośrednio do maszyny wirtualnej poprzez sieć, przy pomocy VIX API dla platformy VMware.

	Oprogramowanie musi wspierać odtwarzanie plików z następujących systemów plików: • Linux: ext2, ext3, ext4, ReiserFS, JFS, XFS, Btrfs, • Windows: NTFS, FAT, FAT32, ReFS. Oprogramowanie musi wspierać przywracanie plików z partycji Linux LVM oraz Windows Storage Spaces.Oprogramowanie musi wspierać granularne odtwarzanie dowolnych obiektów i dowolnych atrybutów Active Directory włączając hasło, obiekty Group Policy, rekordy DNS zintegrowane z AD, Microsoft System Objects, elementy AD Sites. Oprogramowanie musi wspierać granularne odtwarzanie Microsoft SQL 2005 i nowsze włączając bazy danych z opcją odtwarzania point-in-time, tabele, schemat. Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Sharepoint 2010 i nowsze. Opcja odtworzenia elementów, witryn, uprawnień. Oprogramowanie musi wspierać granularne odtwarzanie baz danych Oracle z opcją odtwarzanie point-in-time wraz z włączonym Oracle DataGuard. Funkcjonalność ta musi być dostępna dla baz uruchomionych w środowiskach Windows oraz Linux. Funkcjonalność ta nie może wymagać pełnego odtworzenia wirtualnej maszyny ani jej uruchomienia. Oprogramowanie musi indeksować pliki Windows i Linux w celu szybkiego wyszukiwania plików w plikach backupowych. Oprogramowanie musi używać mechanizmów VSS wbudowanych w system operacyjny Microsoft Windows Oprogramowanie musi pozwalać na odtworzenie maszyn wirtualnych z macierzowych snapshotów ze wspieranych macierzy. Oprogramowanie musi wspierać także specyficzne metody odtwarzania w tym "reverse CBT" oraz odtwarzanie z wykorzystaniem sieci SAN. Oprogramowanie musi dawać możliwość stworzenia laboratorium (izolowane środowisko) używając wirtualnych maszyn uruchamianych bezpośrednio z plików backupu. Oprogramowanie musi pozwalać na uruchomienie takiego środowiska bezpośrednio ze snapshotów macierzowych stworzonych na wspieranych urządzeniach. Oprogramowanie musi umożliwiać weryfikację odtwarzalności wielu wirtualnych maszyn jednocześnie z dowolnego backupu według własnego harmonogramu w izolowanym środowisku. Testy powinny uwzględniać możliwość uruchomienia dowolnego skryptu testującego również aplikację uruchomioną na wirtualnej maszynie. Testy muszą być przeprowadzone bez interakcji z administratorem. Oprogramowanie musi mieć podobne mechanizmy dla replik. Oprogramowanie musi umożliwiać dwuetapowe, automatyczne, odtwarzanie maszyn wirtualnych z możliwością wstrzyknięcia dowolnego skryptu przed odtworzeniem danych do środowiska produkcyjnego.

Wymagania dotyczące backupu serwerów fizycznych	
4.	Oprogramowanie musi wykonywać kopię zapasową systemu Windows oraz Linux wykorzystując agenta znajdującego się wewnątrz systemu operacyjnego. Oprogramowanie musi wspierać Windows 8 lub nowsze oraz Windows Server 2008 R2 SP1 lub nowsze. Oprogramowanie musi wspierać Linux kernel 2.6.32 lub nowsze (zarówno 32 jak i 64bit) oraz wspierać następujące dystrybucje: • Debian 6 – 9.7, • Ubuntu 10.04 – 18.10, • CentOS / Oracle Linux / RHEL 6 – 7.6, • Oracle Linux (UEK) R4 U6, R4 U7, • Fedora 23 – 29, • openSUSE 11.3 - 13.2, • openSUSE Leap 42.2 – 42.3, • SLES 11 SP4 – 15, • SLES for SAP 11 SP4 – 15, Oprogramowanie musi wspierać wykonywanie kopi zapasowych następujących systemów plików: • NTFS, • ReFS, • FAT32, • ext2, ext3, ext4, • ReiserFS, • JFS, • XFS, • F2FS, • HFS, HFS+,

	• NILFS2, • Btrfs (dla kernela 3.16 i nowszych). Oprogramowanie musi mieć możliwość instalacji oraz zarządzania poprzez centralną konsolę zarządzającą. Oprogramowanie musi wspierać systemy oparte o Microsoft Failover Cluster. Oprogramowanie musi wspierać zabezpieczanie do oraz odzyskiwanie z urządzeń blokowych pozwalając na odzysk całej maszyny (tzw. bare metal recovery) wybranych wolumenów, oraz wybranych plików i folderów. Oprogramowanie musi wspierać backup podłączonych dysków USB. Kopia zapasowa całej maszyny oraz pojedynczych wolumenów musi być wykonywana na poziomie blokowym. Oprogramowanie musi pozwalać na przechowywanie kopii zapasowych na: • Lokalnych (wewnętrznych) dyskach zabezpieczanej maszyny. • Direct Attached Storage (DAS), takich jak zewnętrzne dyski USB, eSATA lub Firewire. • Network Attached Storage (NAS) pozwalającym na wystawienie swoich zasobów poprzez SMB (CIFS) lub NFS. • Zcentralizowanym repozytorium danych. • Bezpośrednio na zasobach Chmury. • Microsoft OneDrive/OneDrive for Business. Oprogramowanie musi wspierać deduplikacje oraz kompresję na źródle. Dane wysyłane na repozytorium muszą być już odpowiednio przetworzone. Oprogramowanie musi wspierać kontrolę pasma sieciowego. Oprogramowanie musi wspierać ograniczenie wykonywania backupów dla konkretnych sieci bezprzewodowych. Oprogramowanie musi wspierać ograniczenia wykonywania backupów dla połączeń VPN. Oprogramowanie musi wspierać śledzenie zmienionych bloków podczas wykonywania blokowych kopii zapasowych. Technologia śledzenia bloków dla systemów Windows Server musi być certyfikowana przez Microsoft. Oprogramowanie musi wspierać technologię BitLocker. Oprogramowanie musi wspierać uruchamianie z nośnika odtwarzania. Nośnik odtwarzania musi być automatycznie tworzony przez oprogramowanie. Oprogramowanie musi wspierać wgrywanie dodatkowych sterowników podczas

	odtwarzania z wykorzystaniem nośnika odtwarzania. Oprogramowanie musi wspierać odzysk do konkretnego punktu w czasie (point-in-time) dla wspieranych systemów bazodanowych. Oprogramowanie musi wspierać szyfrowanie. Oprogramowanie musi wspierać tworzenie kopii zapasowych wykorzystując konsolę tekstową lub CLI na maszynie zabezpieczanej. Oprogramowanie musi wspierać tworzenie wielu zadań backupowych.
Monitoring środowiska oprogramowania	
5.	Oprogramowanie musi umożliwiać monitorowanie środowiska wirtualizacyjnego zaoferownego w miniejszym przetargu i być certyfikowany przed producenta oprogramowania wirtualizacyjnego. Oprogramowanie musi umożliwiać kategoryzacje obiektów infrastruktury wirtualnej niezależnie od hierarchii stworzonej w systemie zarządzania środowiskiem wirtualnym. Oprogramowanie musi umożliwiać tworzenie alarmów dla całych grup wirtualnych maszyn jak i pojedynczych wirtualnych maszyn. Oprogramowanie musi dawać możliwość układania terminarza raportów i wysyłania tych raportów przy pomocy poczty elektronicznej w formacie HTML oraz Excel. Oprogramowanie musi mieć wbudowane predefiniowane zestawy alarmów wraz z możliwością tworzenia własnych alarmów i zdarzeń przez administratora. Oprogramowanie musi mieć wbudowane połączenie z bazą wiedzy opisującą problemy z predefiniowanych alarmów. Oprogramowanie musi mieć centralną konsolę z sumarycznym podglądem wszystkich obiektów infrastruktury wirtualnej (ang. Dashboard). Oprogramowanie musi mieć możliwość monitorowania platformy sprzętowej, na której jest zainstalowana infrastruktura wirtualna. Oprogramowanie musi zapewnić możliwość podłączenia się do wirtualnej maszyny (tryb konsoli) bezpośrednio z narzędzia monitorującego. Oprogramowanie musi mieć możliwość integracji z oprogramowaniem do tworzenia kopii zapasowych tego samego producenta. Oprogramowanie musi mieć możliwość monitorowania obciążenia serwerów backupowych, ilości zabezpieczanych danych oraz statusu zadań kopii zapasowych, replikacji oraz weryfikacji odzyskiwalności maszyn wirtualnych. Oprogramowanie musi oferować inteligentną diagnostykę rozwiązania backupowego poprzez monitorowanie logów celem wykrycia znanych problemów oraz błędów

	konfiguracyjnych w celu wskazania rozwiązania bez potrzeby otwierania zgłoszenia suportowego oraz bez potrzeby wysyłania jakichkolwiek danych diagnostycznych do producenta oprogramowania backupu. Oprogramowanie musi mieć możliwość granularnego monitorowania infrastruktury, zależnego od uprawnień nadanym użytkownikom dla platformy wirtualizacyjnej.
	Raportowanie
6.	Oprogramowanie raportowania musi umożliwić tworzenie raportów z dostarczonej infrastruktury wirtualnej. Oprogramowanie musi być certyfikowany przez producenta dostarczonego systemu wirtualizacji. Oprogramowanie musi być systemem bezagentowym. Nie dopuszcza się możliwości instalowania przez system agentów na monitorowanych hostach. Oprogramowanie musi mieć możliwość eksportowania raportów do formatów Microsoft Word, Microsoft Excel, Microsoft Visio, Adobe PDF. Oprogramowanie musi mieć możliwość ustawienia harmonogramu kolekcji danych z monitorowanych systemów jak również możliwość tworzenia zadań kolekcjonowania danych ad-hoc. Oprogramowanie musi mieć możliwość ustawienia harmonogramu generowania raportów i dostarczania ich do odbiorców w określonych przez administratora interwałach. Oprogramowanie w raportach musi mieć możliwość uwzględniania informacji o zmianach konfiguracji monitorowanych systemów. Oprogramowanie musi mieć możliwość generowania raportów z dowolnego punktu w czasie zakładając, że informacje z tego czasu nie zostały usunięte z bazy danych. Oprogramowanie musi posiadać predefiniowane szablony z możliwością tworzenia nowych jak i modyfikacji wbudowanych. Oprogramowanie musi mieć możliwość analizowania „przeszacowanych” wirtualnych maszyn wraz z sugestią zmian w celu optymalnego wykorzystania fizycznej infrastruktury. Oprogramowanie musi mieć możliwość generowania raportów na podstawie danych uzyskanych z oprogramowania do tworzenia kopii zapasowych tego samego producenta. Oprogramowanie musi mieć możliwość generowania raportu dotyczącego zabezpieczanych maszyn, zdefiniowanych zadań tworzenia kopii zapasowych oraz replikacji jak również wykorzystania zasobów serwerów backupowych. Oprogramowanie musi mieć możliwość generowania raportu planowania pojemności (capacity planning) bazującego na scenariuszach ‘what-if’. Oprogramowanie musi mieć możliwość granularnego raportowania infrastruktury, zależnego od uprawnień nadanym użytkownikom dla platformy wirtualizacyjnej.

	Oprogramowanie musi mieć możliwość generowania raportów dotyczących tzw. migawek-sierot (orphaned snapshots). Oprogramowanie musi mieć możliwość generowania personalizowanych raportów zawierających informacje z dowolnych predefiniowanych raportów w pojedynczym dokumencie.

3.3 Instalacja i konfiguracja części od 3.2 do 3.3 – ilość 1 szt.

Lp.	Nazwa elementu/cechy	Wymagane minimalne parametry techniczne
1.	Ogólne	Opracowanie przez Wykonawcę zgodnie z wytycznymi Zamawiającego oraz akceptacja przez Zamawiającego projektu technicznego dla pozycji od 3.2 do 3.3 uwzględniającego m.in.: • Instalacja i konfiguracja pozycji od 3.2 do 3.3 w dostarczonych 19” szafach, • Instalacja i konfiguracja systemu backup w tym opracowanie polityk dla kopii zapasownych. Instalacja, konfiguracja oraz produkcyjne uruchomienie pozycji od 3.2 do 3.3 zgodnie z zaakceptowanym przez Zamawiającego projektem technicznym. Opracowanie dokumentacji technicznej powdrożeniowej.

3.4 Szkolenia – ilość 1 szt.

Lp.	Nazwa szkolenia	Wymagane minimalne parametry techniczne
1.	Szkolenie administracji: backup	Rodzaj szkolenia: • autoryzowane lub • wykonane przez inżyniera Wykonawcy lub • wykonane przez producenta dostarczonego sprzętu lub oprogramowania. Szkolenie musi być co najmniej 4 dniowe. Szkolenie musi obejmować pełen zakres możliwości oprogramowania do wykonywania kopii zapasowych z 3.3. Szkolenie musi być co najmniej 1 dniowe z zakresu obsługi serwera backupu z poz. 3.2. Po ukończeniu szkolenia, każdy uczestnik ma otrzymać stosowny dokument potwierdzający uzyskanie kompetencji do administrowania dostarczonym systemem backupu. Szkolenie będzie się odbywało na terenie Katowic lub wykonawca pokryje koszty transportu i noclegu w przypadku miejsca szkolenia innego niż Katowice. Szkolenie przeznaczone dla trzech osób.

3.5 Warunki gwarancji.

Lp.	Nazwa elementu/cechy	Wymagane minimalne parametry techniczne
1.	Wymagane warunki gwarancji	1. Wykonawca udziela Zamawiającemu nieodpłatnej gwarancji na SYSTEM, realizowanej w siedzibie Zamawiającego. 2. Zamawiający jako SYSTEM rozumie platformę sprzętowo-programową, tworzącą współdziałającą infrastrukturę, obejmującą Oprogramowanie Standardowe, Urządzenia i wytworzone przez Wykonawcę Oprogramowanie Autorskie, zgodną z Dokumentacją Powykonawczą, realizującą wszystkie wymagania funkcjonalne i niefunkcjonalne zawarte w Szczegółowym Opisie Przedmiotu Zamówienia 3. Wykonawca zapewni możliwość zgłaszania awarii w trybie 7/24/365. 4. Wykonawca dostarczy pisemnie w dniu podpisania Protokołu Odbioru Końcowego przedmiotu zamówienia wszelkie dane teleadresowe niezbędne do prawidłowej obsługi zgłoszeń serwisowych. Dopuszcza się zgłoszenia w formie mailowej lub poprzez dedykowany portal Wykonawcy typu HelpDesk. W uzasadnionych przypadkach dopuszcza się zgłoszenie telefoniczne, pod warunkiem potwierdzenia go w ciągu 4 godz. mailowo lub na portalu HelpDesk, w takim przypadku czas podjęcia czynności będzie liczony od momentu telefonicznego zgłoszenia. 5. Zamawiający dostarczy pisemnie w dniu podpisania protokołu Protokołu Odbioru Końcowego przedmiotu zamówienia wszelkie dane teleadresowe osób uprawnionych do zgłaszania i potwierdzania usunięcia awarii. 6. W celu obsługi gwarancyjnej Zamawiający wyróżnia trzy następujące poziomy awarii: 1) Awaria Krytyczna – występuje gdy: a) Zamawiający nie może korzystać z SYSTEMU, b) SYSTEM przerwał swoje działanie i nie da się go uruchomić pomimo podejmowanych prób, c) nastąpiła utrata danych (lub ich części). 2) Awaria Istotna – występuje, wtedy gdy: a) awarii uległ jeden z redundantnych elementów SYSTEMU powodujący degradację wydajności, b) istnieje zagrożenie utraty danych (lub ich części) lub istnieje zagrożenie utraty spójności danych. 3) Awaria Zwykła – oznacza wszelką inną awarię niebędącą Awarią Krytyczną lub Awarią Istotną. Terminy usuwania Awarii Krytycznej, Awarii Istotnej oraz

		Awarii Zwykłej zostaną określone przez Wykonawcę w formularzu ofertowym. 7. Przez czas naprawy Zamawiający rozumie czas liczony od momentu zgłoszenia awarii do momentu dokonania skutecznej naprawy. 8. Okres gwarancji liczony będzie od daty sporządzenia Protokołu Odbioru Końcowego przedmiotu zamówienia. 9. Urządzenia muszą być fabrycznie nowe i nieużywane wcześniej w żadnych projektach, nieużywane przed dniem dostarczenia z wyłączeniem używania niezbędnego dla przeprowadzenia testu ich poprawnej pracy. 10. Urządzenia muszą pochodzić z autoryzowanego kanału dystrybucji producenta przeznaczonego na teren Unii Europejskiej, a korzystanie przez Zamawiającego z dostarczonego produktu nie może stanowić naruszenia majątkowych praw autorskich osób trzecich. 11. Zamawiający wymaga, aby przy dostawie sprzętu Wykonawca dostarczył odpowiednie oświadczenie producenta lub przedstawiciela producenta o wykupieniu serwisu producenta na dostarczony sprzęt, dostępności części zamiennych oraz aktualizacji oprogramowania przez cały okres trwania umowy. 12. Nieodpłatny dostęp do uaktualnień oprogramowania mikrokodów (tzw. firmware'ów) urządzeń i dostarczonego oprogramowania będących przedmiotem umowy w okresie trwania gwarancji i serwisu.
2.	Wymagane dodatkowe warunki gwarancji	Oferowane produkty muszą być zgodne z obowiązującymi normami technicznymi oraz będą posiadać oznakowanie symbolem CE - zgodnie z wymaganiami określonymi w Rozporządzeniu Ministra Gospodarki, Pracy i Polityki Społecznej z dnia 12 marca 2003 r. Sprzęt wprowadzany na rynek po 1 lipca 2006 r. musi być zgodny z normą ROHS. Wraz ze sprzętem i oprogramowaniem Wykonawca dostarczy komplet standardowej dokumentacji w formie papierowej lub elektronicznej w języku polskim lub angielskim, tj. instrukcje eksploatacji urządzeń, dokumentację techniczną, dokumentację użytkownika i administratora. Na dzień złożenia oferty urządzenia nie mogą mieć ogłoszonego statusu end-of-sale (koniec produkcji) w okresie co najmniej 6 miesięcy od dnia składania oferty. Do każdego urządzenia musi być dostarczony komplet nośników umożliwiających odtworzenie oprogramowania zainstalowanego w urządzeniu lub zostanie zapewniony dostęp do stron ww

		producenta, z których można pobrać ww oprogramowanie. Wszystkie urządzenia zostaną dostarczone z niezbędnym okablowaniem zasilającym i transmisyjnym.