Spis treści

[1. Wprowadzenie 3](#_Toc39613803)

[2. Definicje 4](#_Toc39613804)

[3. Sieć OSE 12](#_Toc39613805)

[3.1. Sieć szkieletowa 12](#_Toc39613806)

[3.2. Świadczenie usług dla szkół 13](#_Toc39613807)

[3.3. Infrastruktura Przełączająca w Ośrodkach Przetwarzania Danych 14](#_Toc39613808)

[4. Bezpieczeństwo OSE 16](#_Toc39613809)

[4.1. Architektura Infrastruktury Bezpieczeństwa 17](#_Toc39613810)

[4.2. Urządzenia w Centrach Danych 18](#_Toc39613811)

[5. Opis przedmiotu zamówienia 19](#_Toc39613812)

[5.1. Opis ogólny 19](#_Toc39613813)

[5.1.1. Założenia techniczne 20](#_Toc39613814)

[5.2. Wymagania w zakresie celu i architektury 21](#_Toc39613815)

[5.3. Skalowalność rozwiązania 23](#_Toc39613816)

[5.4. Ośrodki przetwarzania danych 24](#_Toc39613817)

[5.5. Charakterystyka techniczna Systemu 27](#_Toc39613818)

[5.5.1. Warstwa przetwarzania 28](#_Toc39613819)

[5.5.2. Compute - Wirtualizacja mocy obliczeniowej 29](#_Toc39613820)

[5.5.3. SDS - wirtualizacja przestrzeni na dane 29](#_Toc39613821)

[5.5.4. SDN - wirtualizacja funkcji sieciowych 29](#_Toc39613822)

[5.5.5. Warstwa orkiestracji, administracji, zarządzania, eksploatacji i monitorowania zwirtualizowaną infrastrukturą obliczeniową 30](#_Toc39613823)

[5.5.6. Moduł obiektowego składowania danych 31](#_Toc39613824)

[5.5.7. Moduł tworzenia kopii zapasowych 31](#_Toc39613825)

[5.6. Wdrożenie infrastruktury docelowej 32](#_Toc39613826)

[5.7. Opcje rozbudowy Systemu, wydłużenia okresu Utrzymania i Prac Zleconych 35](#_Toc39613827)

[6. Szczegółowe wymagania funkcjonalne 37](#_Toc39613828)

[6.1. Infrastruktura docelowa 37](#_Toc39613829)

[6.2. Wymagania wspólne dla wszystkich Komponentów Systemu 37](#_Toc39613830)

[6.3. Wirtualizacja mocy obliczeniowej 40](#_Toc39613831)

[6.3.1. Architektura HCI – wymagania funkcjonalne 40](#_Toc39613832)

[6.3.2. Serwery HCI - wymagania sprzętowe 41](#_Toc39613833)

[6.3.3. Compute - wirtualizacji mocy obliczeniowej 44](#_Toc39613834)

[6.3.4. SDS wirtualizacji przestrzeni dyskowej 49](#_Toc39613835)

[6.3.5. SDN wirtualizacji funkcji sieciowych 51](#_Toc39613836)

[6.3.6. Skalowanie Klastrów obliczeniowych Komponent HCI 55](#_Toc39613837)

[6.3.7. Moduł orkiestracji, zarządzania i administracji 58](#_Toc39613838)

[6.3.8. Monitorowanie i eksploatacja środowiska 61](#_Toc39613839)

[6.3.9. Chmura Publiczna 64](#_Toc39613840)

[Komponent Macierz obiektowa 66](#_Toc39613841)

[6.3.10. Architektura i wymagania funkcjonalne 66](#_Toc39613842)

[6.3.11. Wymagania sprzętowe 69](#_Toc39613843)

[6.4. Komponent kopii zapasowych i archiwów 70](#_Toc39613844)

[6.4.1. Założenia, architektura i wymagania funkcjonalne środowiska kopii zapasowych 70](#_Toc39613845)

[6.4.2. Kopie zapasowe i archiwum –wymagania sprzętowe 79](#_Toc39613846)

[6.5. Wymagania wdrożeniowe 81](#_Toc39613847)

[6.5.1. Zakres testów weryfikacyjnych 82](#_Toc39613848)

[6.5.2. Zakres dokumentacji powdrożeniowej 84](#_Toc39613849)

[6.5.3. Zakres instruktaży 84](#_Toc39613850)

[6.5.4. Gwarancja 86](#_Toc39613851)

[6.5.5. Okres stabilizacji Systemu 87](#_Toc39613852)

[6.5.6. Okres utrzymania 88](#_Toc39613853)

# Wprowadzenie

Ogólnopolska Sieć Edukacyjna ma na celu zapewnienie dostępu do szybkiego, bezpiecznego Internetu dla szkół. OSE jest publiczną siecią telekomunikacyjną. Za uruchomienie i utrzymanie Sieci, oraz w szczególności za dostarczenie szkołom usługi dostępu do Internetu o symetrycznej przepustowości co najmniej 100 Mb/s wraz z kompleksowymi usługami bezpieczeństwa sieciowego, w tym ochrony przed zagrożeniami dla prawidłowego rozwoju uczniów, odpowiedzialny jest Operator OSE.

Operatorem OSE został, na podstawie Ustawy z dnia 27 października 2017 r., o Ogólnopolskiej Sieci Edukacyjnej, NASK - Państwowy Instytut Badawczy (zwany dalej” „NASK”).

W Polsce istnieje ok 25 tyś. szkół zlokalizowanych w blisko 20 tyś. lokalizacji. Podstawowym zadaniem OSE ma być zapewnienie szkołom w Polsce możliwości dostępu do bezpiecznego Internetu i zasobów edukacyjnych wraz z szeregiem usług powiązanych, w tym:  
1) Zapewnienie usług dostępu do sieci Internet o przepływności minimum 100 Mb/s symetrycznie,  
2) Zapewnienie usług bezpieczeństwa umożliwiających ochronę Użytkowników sieci OSE,  
3) Zapewnienie dostawcom treści edukacyjnych dostępu do Użytkowników sieci OSE.  
4) Umożliwienia wspomagania procesu kształcenia w szkole.

W ramach budowy OSE została uruchomiona sieć rozległa, obejmująca swym zasięgiem terytorium Polski, zbudowana z węzłów zlokalizowanych na terenie 16 województw, która została uzupełniona o systemy bezpieczeństwa wraz z systemami wsparcia obejmującymi m.in. zarządzanie tożsamością, OSS, jak również urządzenia abonenckie (CPE), przełączniki, AP sieci bezprzewodowej.

NASK, jako operator OSE zapewniający dostęp do Internetu dla szkół, realizuje swoje działania w oparciu o trzy podstawowe obszary:

1. Sieć OSE - infrastruktura telekomunikacyjna wykorzystywana do świadczenia przez Operatora OSE usług dostarczanych Użytkownikom sieci OSE  (takich jak m.in dostęp do Internetu).
2. Systemy OSS i BSS - złożony z komponentów informatycznych zbiór systemów, których celem jest wsparcie wszelkiej działalności NASK, jako Operatora OSE (w tym m.in. zarządzanie infrastrukturą sieciową, obsługa procesów podłączania i obsługi usług w szkołach, czy rozliczanie wydatków) składające się z dwóch typów komponentów:
   1. Systemy OSE - systemy informatyczne tworzone lub rozwijane na potrzeby operatora OSE
   2. Systemy NASK - systemy informatyczne wykorzystywane w ramach podstawowej działalności NASK PIB, które zostaną zintegrowane z rozwiązaniem na potrzeby OSE
3. Bezpieczeństwo OSE - komponenty warstwy sieciowej, sprzęt oraz oprogramowanie, których celem jest zapewnienie  bezpieczeństwa teleinformatycznego sieci OSE oraz jej użytkownikom.

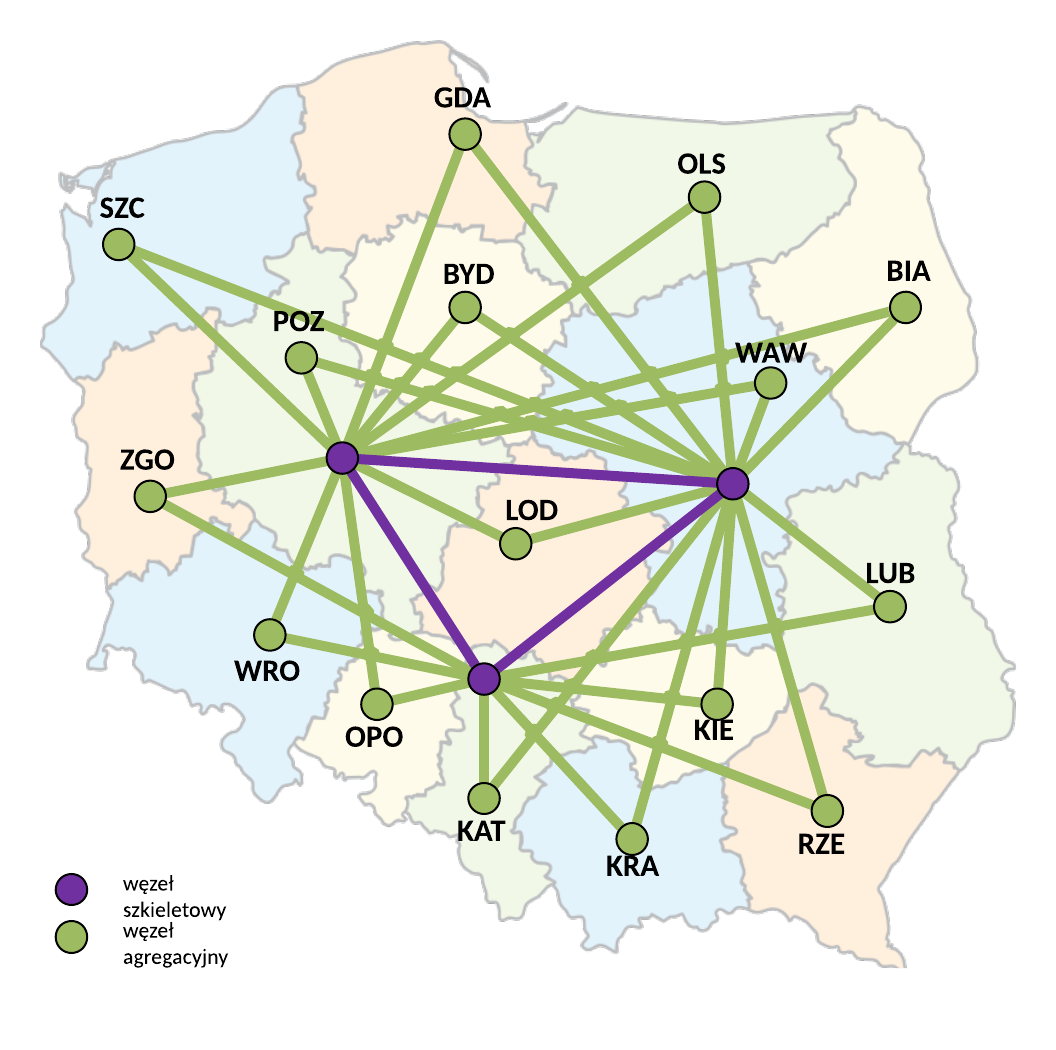
# Definicje

|  |  |
| --- | --- |
| Definicja | Wyjaśnienie |
| ACPI (Advanced Configuration and Power Interface) | Zaawansowany interfejs zarządzania konfiguracją i energią, umożliwiający systemowi operacyjnemu kontrolowanie ilości energii dostarczanej do poszczególnych urządzeń, ich wyłączanie, gdy nie są używane, a konieczne jest oszczędzanie energii. |
| ADC (Application Delivery Controller) | Urządzenia realizujące równomierne rozłożenie obciążenia na instancje systemów należące do operatora OSE. |
| API (Application Programming Interface) | Zbiór reguł ściśle opisujący sposób, w jaki programy lub podprogramy komunikują się ze sobą. |
| Backup/Restore | Pojęcia związane z mechanizmem wykonywania kopii zapasowych danych (Backup) oraz ich odtwarzaniem (Restore). Funkcjonalność realizowana przez Komponent Kopie zapasowe/archiwum |
| BGP (Border Gateway Protocol) | Protokół routingu zewnętrznego, używany także do sygnalizacji wewnątrz systemu autonomicznego.  Opisany w dokumentach RFC 4271. |
| CBT (Changed Block Tracking) | Technologia wykonywania przyrostowych kopii zapasowych maszyn wirtualnych polegająca na tworzeniu kopii zapasowych tylko tych bloków, które uległy zmianie. |
| Centralny Węzeł Bezpieczeństwa (CWB) | Węzeł Bezpieczeństwa zlokalizowany w Węźle Centralnym, dostarczający mechanizmy ochrony Zasobów obliczeniowych OSE. |
| HCI (Hyper-Converged Infrastructure) | Hiperkonwergentna łatwo skalowalna infrastruktura centrum danych budowana z powtarzalnych komponentów - serwery x86. Technologia dostarczająca zbiór zasobów: moc obliczeniową (procesory), współdzielony system pamięci masowej i rozwiązania sieciowe, przy zastosowaniu oprogramowania Compute, SDS, SDN.  Składniki rozwiązania mogą być zarządzane za pomocą wspólnej konsoli administracyjnej upraszając proces rozbudowy i aktualizacji środowiska. |
| Dysk Cache | Dysk wykorzystywany w rozwiązaniach HCI jako urządzenie do poprawy wydajności funkcji odczytu i zapisu. |
| Dysk capacity | Dysk wykorzystywany w rozwiązaniach HCI jako urządzenie do składowania danych. |
| Deduplikacja danych | Eliminowanie powtarzających się części w zbiorze danych. Jest to proces stosowany przy zapisie danych, którego celem jest ograniczanie ilości miejsca potrzebnego do przechowywania danych. |
| Failover/Failback | Failover - przełączenie na element zapasowy Systemu w momencie awarii elementu podstawowego.  Failback - przełączenie na element podstawowy Systemu z systemu zapasowego po usunięciu awarii. |
| GENEVE (Generic Network Virtualization Encapsulation) | Standard wirtualizacji sieci opracowywany aktualnie przez IETF (Internet Engineering Task Force) – „https://tools.ietf.org/html/draft-gross-geneve-02”, oferujący podejście do enkapsulacji, które ma na celu zapewnienie niezależności kontrolnej pomiędzy punktami końcowymi tunelu. Standard określa tylko schemat płaszczyzny danych przy użyciu wielu opcji o zmiennej długości. |
| HDD (Hard Disk Drive) | Urządzenie pamięci masowej zbudowane w oparciu o nośnik magnetyczny do przechowywania danych. |
| Hot-spare | Mechanizm zabezpieczający, używany w celu zapewnienia niezawodności konfiguracji systemów. Jest aktywnym i podłączonym zapasowym elementem działającego systemu. W przypadku awarii kluczowego elementu, urządzenie hot-spare automatycznie przejmuje rolę urządzenia uszkodzonego. |
| IPMI (Intelligent Platform Management Interface) | Zestaw specyfikacji, które udostępniają unormowany interfejs do zarządzania i monitorowania. Pojęcie zarządzanie i monitorowanie używane jest w tym kontekście do monitoringu sprzętu (temperatur systemu, wentylatorów, zasilaczy itd.), jego zarządzania (włączanie/wyłączanie serwera) jak i dokumentację (logging) stanów „out-of-range“. |
| JBOD (Just a Bunch Of Disks) | Standard obsługi dysków twardych przy pomocy kontrolera macierzowego, który pełni rolę kontrolera dysków twardych. |
| Klaster | Zbiór połączonych jednostek komputerowych (serwerów), które współpracują ze sobą w celu udostępnienia zintegrowanego środowiska umożliwiającego uzyskanie odpowiedniej: wydajności, niezawodności i równoważenia obciążenia. |
| Klony (klonowanie) | Możliwość utworzenia dokładnej kopii maszyny wirtualnej czyli skopiowanie wszystkich plików (w tym sprzętu wirtualnego, systemu operacyjnego gościa i zainstalowanego oprogramowania) z wzorca do nowej, niezależnej maszyny; kopia systemu jest niezależna od systemu macierzystego. |
| Komponenty | Bloki funkcjonalne składające się na System, tj.: HCI, Macierz obiektowa, Kopie zapasowe/archiwum, Oprogramowanie, Compute, SDS, SDN. |
| Komponent HCI | Architektura składająca się serwerów HCI zapewniających zasoby (CPU, RAM, Storage) i oprogramowania zapewniającego wirtualizację zasobów. |
| Komponent SDN | Architektura sieci polegająca na wydzieleniu z urządzenia sieciowego obszaru kontrolnego (zarządczo-sterującego) i realizacji centralnego sterowania urządzeniami. Urządzenia sieciowe realizują wyłącznie zadania polegające na obsłudze pakietów zgodnie z przypisanymi zadaniami. SDN składa się z kontrolerów zarządzających zwirtualizowaną siecią, polityk opisujących działanie sieci SDN i urządzeń sieciowych wykonujących przypisane zadania. |
| Komponent Macierz obiektowa | Architektura serwerowa służąca do przechowywania i udostępniania danych w formie obiektów, co oznacza, że oprócz danych przechowywane są również metadane opisujące przechowywane dane, a także unikalny globalnie identyfikator. |
| Komponent Kopie zapasowe/archiwum | Architektura serwerowa służąca do tworzenia i przechowywania kopii systemów produkcyjnych, umożliwiająca w przypadku awarii systemów produkcyjnych ich odtworzenie z zapisanych danych. Archiwum jest to wydzielona część Komponentu, zapewniająca przechowywanie kopii systemów produkcyjnych przez długi okres czasu. |
| Kompresja danych | Zmiana sposobu zapisu informacji tak w taki sposób aby zmniejszyć powtarzalność i tym samym objętość zbioru. Innymi słowy chodzi o wyrażenie tego samego zestawu informacji, lecz za pomocą mniejszej liczby bitów. |
| Kopia migawkowa | Kopia pamięci dyskowej maszyny wirtualnej z określonego momentu czasu, umożliwiająca przywrócenie stanu maszyny wirtualnej na dany moment utworzenia kopii migawkowej; stan danych plikowych z momentu utworzenia migawki jest stały, niezmienny w czasie przez działającą maszynę wirtualną. |
| LDAP (Lightweight Directory Access Protocol) | Protokół przeznaczony do korzystania z usług katalogowych. Jest to również nazwa własna usługi katalogowej przechowującej informacje o użytkownikach i ich atrybutach. |
| Węzeł / Kolokacja | Miejsce fizyczne, powierzchnia kolokacyjna, w którym pracuje Węzeł sieci OSE/ Węzeł Bezpieczeństwa OSE. |
| LTR (Long-term Retention) | Archiwum długoterminowego przechowywania danych. |
| NVGRE (Network Virtualization Using Generic Routing Encapsulation) | Technologia wirtualizacji sieci opisana w RFC 7637, umożliwiająca tunelowanie pakietów warstwy 2 modelu OSI w sieciach warstwy 3. |
| NVMe (Non-Volatile Memory Express) | Interfejs komunikacyjny wraz ze sterownikami, definiujący zestaw poleceń i zestaw funkcji dla dysków SSD opartych na interfejsie PCIe. |
| OPD | W OSE istnieją 3 Ośrodki Przetwarzania Danych, oznaczone odpowiednio:  OPD1 - WARSZAWA  OPD2 - POZNAŃ  OPD3 - KATOWICE |
| Operator OSE | Przedsiębiorca telekomunikacyjny świadczący usługi dostępu do Internetu za pośrednictwem OSE na rzecz Jednostek edukacyjnych. Operator OSE odpowiada za podłączanie Jednostek Oświatowych, a następnie obsługuje je na bazie wewnętrznych i zewnętrznych struktur organizacyjnych, zawierających między innymi Centrum Kontaktu, Centrum Zarządzania Siecią oraz Centrum Zarządzania Bezpieczeństwem; |
| Plug-in | Inaczej „wtyczka”, dodatkowy moduł do programu komputerowego, który komunikuje się z nim poprzez interfejs API (Application Programming Interface), rozszerzając możliwości produktu wyjściowego. |
| Portal OSE | Portal umożliwiający obsługę usług w sieci OSE, w tym zgłaszanie problemów technicznych, zmian w zakresie świadczonych usług, kreowanie i modyfikowanie kont Użytkowników Sieci OSE oraz parametrów tych kont. |
| Półka dyskowa | Element infrastruktury fizycznej storage pozwalający na rozbudowę posiadanej przestrzeni dyskowej o kolejne dyski, nieposiadający kontrolera. |
| Regionalny Węzeł Bezpieczeństwa (RWB) | Węzeł Bezpieczeństwa zlokalizowany w Węźle Regionalnym i obsługujący Szkoły podłączone do danego Węzła Regionalnego. |
| ROPD | Regionalny Ośrodek Przetwarzania Danych w poszczególnych miastach. |
| RPO (Recovery Point Objective) | Dopuszczalny okres czasu niedostępności (utraty) danych biznesowych. Odpowiada na pytanie do jakiego momentu odzyskanie danych przez proces biznesowy może przebiegać w sposób tolerowany, biorąc pod uwagę ilość danych utraconych w tym przedziale czasu. |
| RTO (Recovery Time Objective) | Maksymalny czas w jakim usługi biznesowe muszą zostać przywrócone po awarii. |
| SAML (Security Assertion Markup Language) | Protokół służący do wymiany danych uwierzytelniania i autoryzacji w domenach zabezpieczeń. W modelu domeny SAML dostawca tożsamości jest specjalnym typem urzędu uwierzytelniania. Dostawca tożsamości SAML jest jednostką systemową, która wydaje zapewnienie uwierzytelniania w połączeniu z profilem SSO SAML. Strona ufająca, która zużywa te zapewnienie uwierzytelniania, jest nazywana dostawcą usług SAML. |
| SDS (Software-Defined Storage) | Rozwiązanie polegające na uniezależnieniu storage’u od warstwy sprzętowej poprzez wirtualizację pamięci masowej, oferując często szereg funkcjonalności typu replikacja, thin provisioning, snapshoty czy backup. |
| SDN (Software-Defined Network) | Rozwiązanie polegające na centralnym programowaniu i kontrolowaniu pracy sieci, w którym zbiór urządzeń realizuje zadania zgodnie z logiką centralnej warstwy kontrolnej. |
| SIEM | System tożsamy z funkcjami Log Management (LM) odpowiedzialny za logowanie zdarzeń z urządzeń sieciowych, systemów operacyjnych oraz aplikacji. System LM posiada funkcjonalności takie jak: zbieranie logów, agregację logów oraz przeszukiwanie, raportowanie i tworzenie reguł korelacyjnych. |
| SNAT/DNAT (Source/Destination Network Address Translation) | Technika polegająca na zmianie adresu źródłowego/docelowego pakietu IP na inny. |
| SNMP | Rodzina protokołów sieciowych wykorzystywanych do zarządzania urządzeniami sieciowymi i serwerami za pośrednictwem sieci IP. Opisany w standardzie STD 62, STD 58 i kolejnych. |
| SoL (Serial over LAN) | Mechanizm umożliwiający przekierowanie wejścia i wyjścia portu szeregowego zarządzanego systemu przez IP. |
| SSD (Solid-State Drive) | Urządzenie pamięci masowej zbudowane w oparciu o pamięć flash do przechowywania danych. |
| SSH (Secure Sockets Layer) | Standard protokołów szyfrowania komunikacji typu klient-serwer, a także serwer-klient.  Protokół SSH jest zaimplementowany na warstwie aplikacji modelu OSI w ramach połączenia TCP. Protokół SSH jest opisany RFC 4251 i kolejnych. |
| SSL (Secure Sockets Layer) | Protokół służący do bezpiecznej transmisji zaszyfrowanego strumienia danych. |
| SWG (Security Web Gateway) | System zapewniający funkcje ochrony Użytkownika sieci OSE przed potencjalnym dostępem do treści nielegalnych i szkodliwych w Internecie. |
| SYSLOG | Protokół umożliwiający rejestrowanie zachodzących zdarzeń przy pomocy scentralizowanego mechanizmu logowania, działający na porcie 514 udp / tcp. Cały mechanizm jest opisany w RFC 5424 i 3164. |
| System | Kompleksowe rozwiązanie sprzętowo-programowe tworzące infrastrukturę zwirtualizowanej mocy obliczeniowej i przestrzeni dyskowej oraz zapewniające przestrzeń do przechowywania i udostępniania danych obiektowych oraz kopii zapasowych i archiwum. System składa się z Komponentów: HCI, SDN, Macierz obiektowa, Kopie zapasowe i archiwum oraz oprogramowanie do monitoringu, zarządzania i orkiestracji. |
| System NG Firewall (NGFW – Next Generation Firewall) | System kontrolujący dostęp do sieci w oparciu o polityki, klasyfikujące ruch bazujący na informacjach pozyskanych z protokołów działających w 4 i 7 warstwie modelu OSI, z wykorzystaniem mechanizmów statefull packet inspection, intrusion prevetion system, application control, antivirus. |
| System Retencji | System odpowiedzialny za zbieranie logów i zdarzeń z urządzeń sieciowych, posiadający funkcjonalności takie jak: zbieranie logów, agregację logów, retencję logów oraz przeszukiwanie i raportowanie. |
| Szyfrowanie danych | Proces ukrywania danych w taki sposób, aby ich odczytanie możliwe było przez osoby posiadające „klucz” deszyfrujący. |
| ThinProvisioning | Technologia wirtualizacji umożliwiająca przydzielenie większej ilości zasobów fizycznych niż są one faktycznie dostępne. |
| ThickProvisioning | Technologia wirtualizacji umożliwiająca przydzielenie wymaganej ilości zasobów fizycznych zapewniając ich rezerwację i dostępność. |
| TPM (Trusted Platfom Module) | Standard układu scalonego (nazywany jest tak również sam układ) opracowany przez Trusted Computing Group, wykonujący wszystkie operacje obliczeniowe związane z kryptografią. |
| Ustawa OSE | Ustawa z dnia 27 października 2017 r. o Ogólnopolskiej Sieci Edukacyjnej. |
| Użytkownicy Sieci OSE | Użytkownicy usług Sieci OSE w tym m. in.: uczniowie, nauczyciele, pracownicy administracyjni oraz inni upoważnieni przez administratora danych usług Sieci OSE. |
| VPN | Tunel, przez który płynie prywatny ruch w ramach dostępnej sieci transmisyjnej pomiędzy klientami końcowymi, w taki sposób, że węzły tranzytowe są przezroczyste dla przesyłanych pakietów. |
| VSS (Volume Snapshot Service/ Volume Shadow Copy) | Technologia umożliwiająca tworzenie kopii zapasowych lub migawek plików lub woluminów komputerowych, nawet gdy są one używane. |
| VTL (Virtual Tape Library) | Technologia wirtualizacji pamięci masowej danych używana do tworzenia kopii zapasowych i odzyskiwania danych. VTL przedstawia komponent pamięci masowej (zazwyczaj dysk twardy) jako biblioteki taśmowe lub napędy taśmowe do użytku z istniejącym oprogramowaniem do tworzenia kopii zapasowych. |
| VXLAN (Virtual eXtensible Local Area Network) | Technologia wirtualizacji sieci opisana w RFC 7348, umożliwiająca tunelowanie pakietów warstwy 2 modelu OSI w sieciach warstwy 4. |
| Węzeł agregacyjny | Zestaw urządzeń pracujących w jednej lokalizacji, do którego dołączone są łącza dostępowe do szkół, węzeł ten nie ma bezpośredniego połączenia do sieci Internet. |
| Węzeł bezpieczeństwa | Zestaw urządzeń wraz z Oprogramowaniem, realizujących funkcje bezpieczeństwa (m. in. dekrypcja SSL, funkcjonalność IPS, NG Firewall itd.). Zamawiający wyróżnia dwa typy takich węzłów: Regionalny Węzeł Bezpieczeństwa oraz Centralny Węzeł Bezpieczeństwa |
| Węzeł HCI | Serwer HCI dostarczający wspólne zasoby (CPU, RAM, Storage) w sposób bezpieczny poprzez zabezpieczenie przechowywanych danych na więcej jak jednym dysku lub innych Węzłach HCI. |
| Węzeł sieci | Zespół urządzeń pracujących w jednej lokalizacji, zapewniających komunikację Użytkownikom sieci OSE z siecią Internet. Węzeł wraz z innymi węzłami, z którymi jest połączony za pośrednictwem łączy szkieletowych, stanowi sieć OSE. Częścią węzła są Regionalne i Centralne Węzły Bezpieczeństwa. |
| Węzeł szkieletowy | Zespół urządzeń zapewniających przeniesienie ruchu z węzłów agregacyjnych do sieci Internet, a także inżynierię ruchu na styku sieci OSE z Internetem. |
| WORM (Write Once Read Many) | Technologia pozwalająca na jednorazowe zapisanie danych i wielokrotny odczyt. Raz zapisane dane nie mogą zostać zmienione ani usunięte. |
| Zasoby obliczeniowe OSE | Infrastruktura serwerowa udostępniona w celu zapewnienia mocy obliczeniowej t.j. procesory, pamięć RAM, przestrzeń dyskowa wybudowana na potrzeby systemów i usług OSE. Zasoby są rozmieszczone w dwóch węzłach centralnych OSE w lokalizacjach: Warszawa i Poznań. |
| BFD | Protokół sieciowy zapewniający szybkie wykrycia utraty sąsiedztwa sieciowego.  Został on opisany w RFC 5880 i kolejnych. |
|  |  |

# Sieć OSE

## Sieć szkieletowa

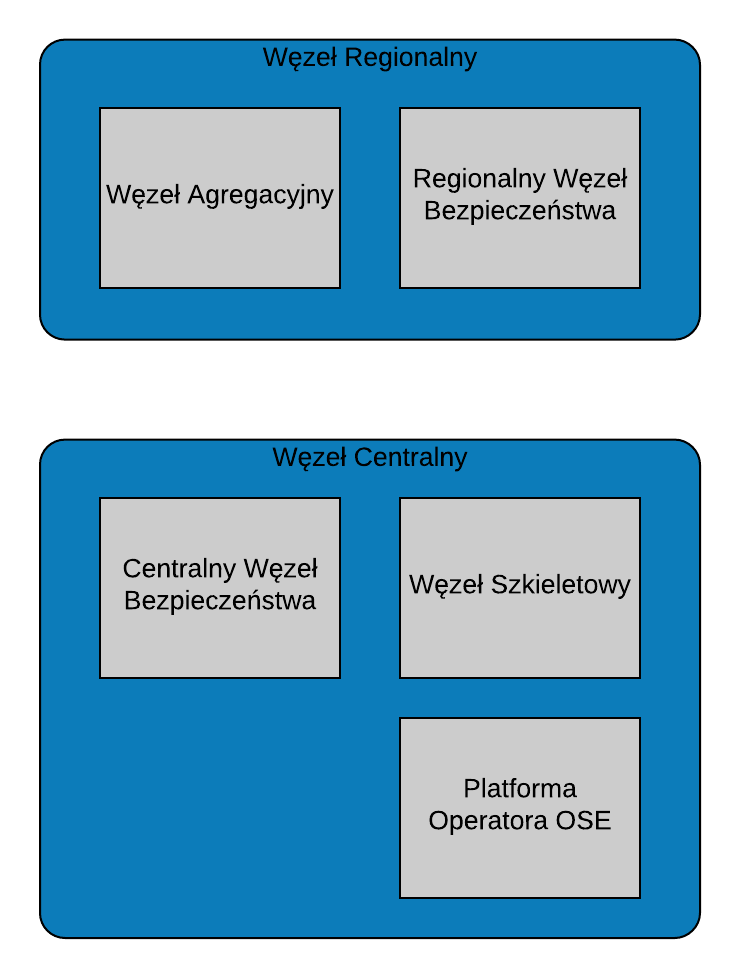
W zakresie sieci szkieletowej operator OSE opiera się na łączach dzierżawionych od operatorów telekomunikacyjnych, nie jest rozważana budowa własnej infrastruktury kablowej. Węzły OSE są zlokalizowane w 16 miastach wojewódzkich, w celu agregowania ruchu z jednostek oświatowych z terenu całego kraju (Węzły agregacyjne). Trzy spośród tych węzłów (Warszawa, Poznań i Katowice) pełnią również rolę węzłów centralnych (Węzły szkieletowe). Pozostałe węzły są połączone z węzłami centralnymi. Lokalizacje węzłów zostały wybrane przez NASK w ramach odrębnych procesów zakupowych, w wyniku których zostali wyłonieni dostawcy usług kolokacji w poszczególnych miastach.



**Węzły sieci**

W sieci OSE wyróżnia się dwa funkcjonalne rodzaje węzłów:

* Węzły Regionalne, w których skład wchodzą: Węzły Agregacyjne (do których są dołączone łącza ze szkół) oraz Regionalne Węzły Bezpieczeństwa;
* Węzły Centralne, w których skład wchodzą Węzły Szkieletowe, Centralne Węzły Bezpieczeństwa oraz Zasoby Obliczeniowe OSE (będące platformą dla systemów OSE). Do Węzłów Szkieletowych dołączone są Węzły Agregacyjne. Węzły te zapewniają także łączność do sieci Internet.



Węzły Szkieletowe są zlokalizowane w tych samych miejscach co Węzły Agregacyjne, za wyjątkiem węzła WAW / WAW Core, w którym Węzeł Agregacyjny jest umieszczony w innej lokalizacji niż Węzeł Szkieletowy (oba węzły są zlokalizowane na terenie Warszawy). Urządzenia pełniące funkcje obu węzłów są oddzielne.

Każdy węzeł OSE wyposażony został w urządzenia sieciowe, infrastrukturę bezpieczeństwa, przełączniki sieci lokalnej, routery shadow oraz urządzenia sieci zarządzającej, zapewniające dostęp administracyjny do wszystkich urządzeń zlokalizowanych w węźle. Infrastruktura sieciowa w węzłach OSE opiera się o następujące typy/modele urządzeń:

* routery szkieletowe i agregacyjne - Juniper MX (960 i 10003)
* CG-NAT - Juniper SRX (4600)
* LAN - Juniper QFX [(10008, 10002, 5110](file:///C:/Users/tomaszcie/Desktop/Załącznik%20nr%201_%20Szczegółowy%20opis%20przedmiotu%20zamówienia.docx#scroll-bookmark-1) i 5120)
* routery shadow - Juniper SRX320

## Świadczenie usług dla szkół

W szkołach zainstalowane są urządzenia CPE, świadczące usługi dla sieci lokalnych.

Ruch od urządzeń CPE umieszczonych w szkołach przenoszony jest przez łącza zrealizowane w technologii Ethernet, operatorów agregujących do Węzłów Agregacyjnych sieci OSE, gdzie jest oddawany do urządzeń agregujących sieci OSE na interfejsach 10GE oraz 1GE.

Ruch odebrany w Węźle Agregacyjnym kierowany jest do Regionalnego Węzła Bezpieczeństwa.

Następnie ruch odebrany z Regionalnego Węzła Bezpieczeństwa kierowany jest do Węzłów Szkieletowych, a później do sieci Internet. Pomiędzy Regionalnym Węzłem Bezpieczeństwa, a wyjściem do sieci Internet ruch IPv4 przechodzi przez instancję CG-NAT, gdzie jest translowany do publicznych adresów IPv4 przydzielonych dla sieci OSE.

**Separacja ruchu**

Ruch zarządzania (zarówno dla urządzeń CPE jak też urządzeń sieci OSE) traktowany jest jako ruch zaufany i jest oddzielony od ruchu produkcyjnego do / ze szkół.

## Infrastruktura Przełączająca w Ośrodkach Przetwarzania Danych

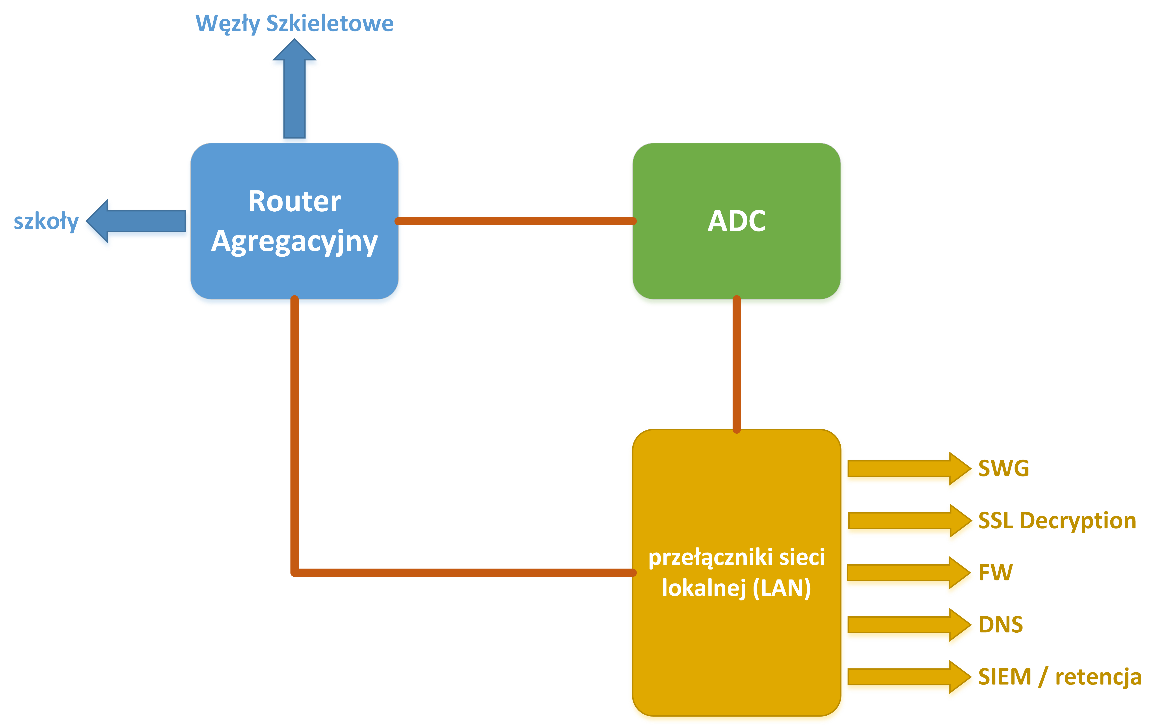
Istniejąca infrastruktura przełączająca przeznaczona do podłączenia dostarczanej infrastruktury sprzętowej Systemu, została zaprojektowana i wykonana w oparciu o dwa rodzaje węzłów:

1. Węzeł z Regionalnym Ośrodkiem Przetwarzania Danych (ROPD) przygotowany został w oparciu o strukturę przełączników Juniper QFX w modelu Spine-Leaf.

Tabela przedstawia dostępne interfejsy komunikacyjne

|  |  |  |  |
| --- | --- | --- | --- |
| **Lokalizacja** | **Urządzenie** | **wolne porty 10GBase-SR** | **wolne porty SFP+** |
| Dolnośląskie ROPD | przełącznik dostępowy nr 1 | 4 | 28 |
| przełącznik dostępowy nr 2 | 4 | 28 |
| przełącznik dostępowy nr 3 | 12 | 36 |
| Kujawsko-pomorskie ROPD | przełącznik dostępowy nr 1 | 4 | 32 |
| przełącznik dostępowy nr 2 | 4 | 32 |
| przełącznik dostępowy nr 3 | 16 | 32 |
| Lubelskie ROPD | przełącznik dostępowy nr 1 | 4 | 30 |
| przełącznik dostępowy nr 2 | 4 | 30 |
| przełącznik dostępowy nr 3 | 13 | 32 |
| Lubuskie ROPD | przełącznik dostępowy nr 1 | 9 | 30 |
| przełącznik dostępowy nr 2 | 9 | 30 |
| Łódzkie ROPD | przełącznik dostępowy nr 1 | 7 | 19 |
| przełącznik dostępowy nr 2 | 7 | 19 |
| przełącznik dostępowy nr 3 | 0 | 48 |
| Małopolskie ROPD | przełącznik dostępowy nr 1 | 0 | 26 |
| przełącznik dostępowy nr 2 | 0 | 26 |
| przełącznik dostępowy nr 3 | 0 | 48 |
| Opolskie ROPD | przełącznik dostępowy nr 1 | 9 | 31 |
| przełącznik dostępowy nr 2 | 9 | 31 |
| Podkarpackie ROPD | przełącznik dostępowy nr 1 | 4 | 30 |
| przełącznik dostępowy nr 2 | 4 | 30 |
| przełącznik dostępowy nr 3 | 16 | 32 |
| Podlaskie ROPD | przełącznik dostępowy nr 1 | 12 | 26 |
| przełącznik dostępowy nr 2 | 12 | 26 |
| Pomorskie ROPD | przełącznik dostępowy nr 1 | 4 | 30 |
| przełącznik dostępowy nr 2 | 4 | 30 |
| przełącznik dostępowy nr 3 | 16 | 32 |
| Świętokrzyskie ROPD | przełącznik dostępowy nr 1 | 16 | 26 |
| przełącznik dostępowy nr 2 | 16 | 26 |
| Warmińsko-Mazurskie ROPD | przełącznik dostępowy nr 1 | 13 | 23 |
| przełącznik dostępowy nr 2 | 13 | 23 |
| Zachodniopomorskie ROPD | przełącznik dostępowy nr 1 | 12 | 26 |
| przełącznik dostępowy nr 2 | 12 | 26 |

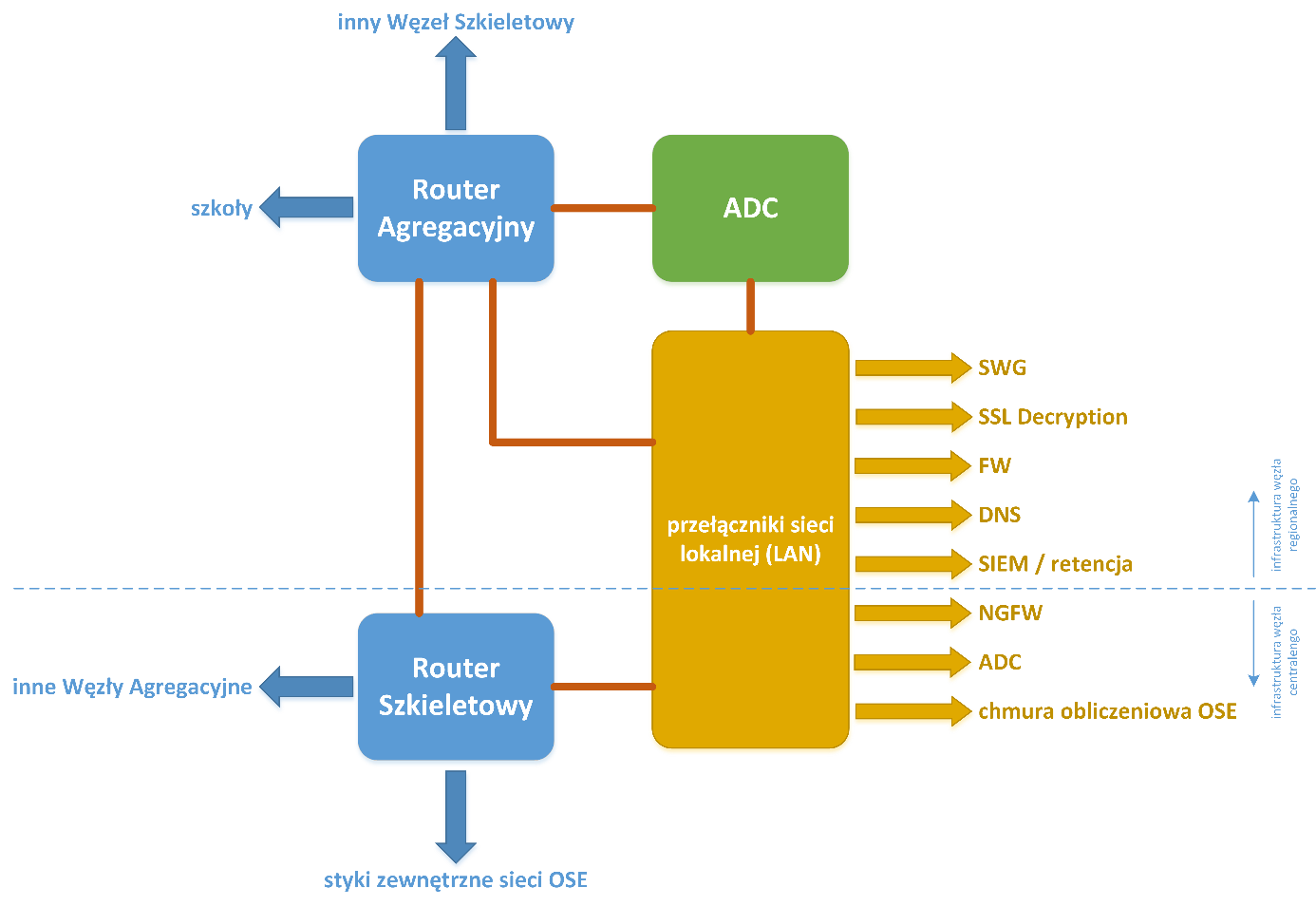
Rysunek prezentuje strukturę połączeń poszczególnych elementów w zakresie komunikacji i integracji z komponentami bezpieczeństwa w trzynastu ROPD.



1. Węzeł z Centralnym Ośrodkiem Przetwarzania Danych przygotowany został w oparciu o przełącznik modularny 8 slotowy Juniper QFX serii 10008.

|  |  |  |  |
| --- | --- | --- | --- |
| **Lokalizacja** | **Urządzenie** | **Liczba wolnych portów 10GBase-SR** | **Liczba wolnych slotów na porty SFP+** |
| OPD1 Warszawa / ROPD Mazowieckie | przełącznik z kartami dostępowymi | 126 | 0 |
| OPD2 Poznań / ROPD Wielkopolskie | przełącznik z kartami dostępowymi | 172 | 0 |
| OPD3 Katowice / Śląskie ROPD | przełącznik z kartami dostępowymi | 76 | 0 |

Rysunek prezentuje strukturę połączeń poszczególnych elementów w zakresie komunikacji i integracji z komponentami bezpieczeństwa w trzech wspólnych środkach OPD i ROPD.



W każdej lokalizacji ROPD i OPD Zamawiający dysponuje przełącznikami 10/100/1000Mbps umożliwiając podłączenie portów zarządzających Ethernet 10/100/1000.

# Bezpieczeństwo OSE

Na potrzeby systemów bezpieczeństwa utworzono 2 funkcjonalne rodzaje węzłów:

* + - 1. Regionalny Węzeł Bezpieczeństwa (RWB) - podłączony do Węzła Agregacyjnego OSE,

1. Centralny Węzeł Bezpieczeństwa (CWB) – podłączony do Węzła Szkieletowego OSE.

Każdy z 16 Regionalnych Węzłów Bezpieczeństwa zawiera komponenty realizujące podstawowe funkcjonalności, m.in:

* zapewnianie bezpieczeństwa teleinformatycznego Użytkownikom sieci OSE,
* wykrywanie i zapobieganie włamaniom poprzez wykrywanie i blokowanie ataków sieciowych w czasie rzeczywistym,
* wykrywanie i blokowanie zdefiniowanych aplikacji webowych,
* monitorowanie ruchu sieciowego i zapisywanie najważniejszych wydarzeń do logu.

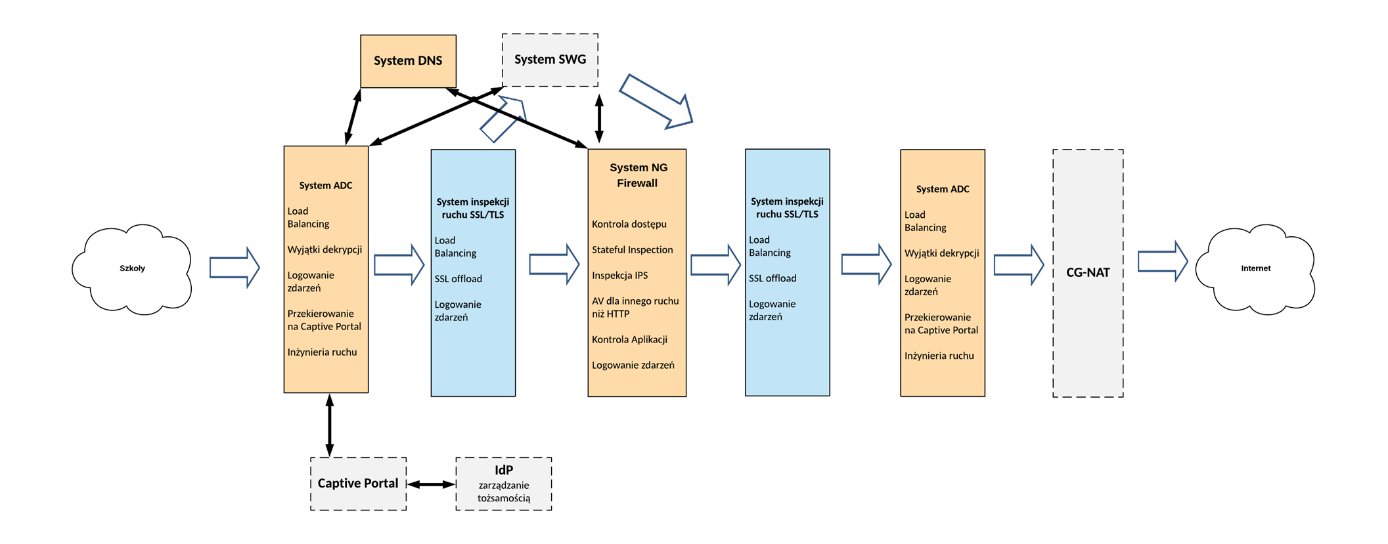
Dwa Centralne Węzły Bezpieczeństwa zawierają komponenty realizujące funkcjonalności ochrony Zasobów obliczeniowych OSE:

* bezpieczeństwo teleinformatyczne Zasobów obliczeniowych OSE i systemów wsparcia,
* wykrywanie i zapobieganie włamaniom poprzez wykrywanie i blokowanie ataków sieciowych w czasie rzeczywistym.

## Architektura Infrastruktury Bezpieczeństwa

Architektura Infrastruktury bezpieczeństwa RWB składa się z Systemu ADC, Systemu inspekcji SSL/TLS, Systemu NG Firewall, Systemu DNS Firewall oraz Systemu SWG.

Poniżej zaprezentowano schemat blokowy przepływu danych w Regionalnych Węzłach Bezpieczeństwa. Schemat zawiera systemy Zamawiającego, składające się na Infrastrukturę bezpieczeństwa.



Infrastruktura bezpieczeństwa została oparta o urządzenia/systemy następujących producentów:

* ADC (LTM) – F5 Networks
* SSLO (deszyfracja) – F5 Networks
* SSL VPN, ADC, WAF – F5 Networks
* Firewall – Fortigate
* DNS – Infoblox
* SWG – Symantec (do 12.2020r.)

## Urządzenia w Centrach Danych

Zamawiający posiada zakupione urządzenia bezpieczeństwa dedykowane do zastosowania w dostarczonym Systemie. Są to urządzenia realizujące funkcjonalność zapory Firewall Nowej Generacji w raz usługami m.in. AV, IPS. Natomiast do ochrony ruchu HTTP, HTTPS (bezpiecznego dostępu do usług) i rozkładania obciążenia Zamawiający posiada urządzenia typu ADC.

Zamawiający zbudował dwa Centralne Węzły Bezpieczeństwa w obu Centrach Danych OPD1 i OPD2 składające się lustrzanych kompletów urządzeń.

Lista urządzeń w OPD:

1. Dwa NG Firewall - Fortinet Fortigate 3000D
2. Dwa F5 Networks i11800

Zamawiający założył następujące wymagania wydajnościowe dla CWB.

W poniższej tabeli przedstawiono wymagane skalowanie Infrastruktury bezpieczeństwa dla

poszczególnych Węzłów:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Lokalizacja** | **Ilość sesji SSLVPN** | **Przep ustowość NG Firewall** | **Przepustowość ADC** | **Przepustowość WAF** |
| OPD1 | 500 | 20 Gbps | 20 Gbps | 8 Gbps |
| OPD2 | 500 | 20 Gbps | 20 Gbps | 8 Gbps |

# Opis przedmiotu zamówienia

## Opis ogólny

Przedmiotem zamówienia jest wdrożenie wraz z dostawą, instalacją, uruchomieniem i integracją Systemu (zwirtualizowanej infrastruktury obliczeniowej), zgodnie z przedstawionymi w dokumencie warunkami wdrożenia, w szesnastu węzłach OSE. W ramach realizacji przedmiotu zamówienia Wykonawca jest zobowiązany do:

1. wykonania szczegółowego projektu Systemu, obejmującego wymagane funkcjonalności i integrację z OSE (Projekt Techniczny Infrastruktury HLD i LLD);
2. wdrożenia (dostawa, instalacja, konfiguracja, uruchomienie i integracja) Systemu, zgodnie z wykonanym wcześniej przez Wykonawcę i zaakceptowanym przez Zamawiającego Projektem Technicznym HLD;
3. przeprowadzenia instruktaży dla pracowników Zamawiającego, zgodnie z wymaganiami opisanymi w niniejszym dokumencie;
4. dostarczenia dokumentacji poszczególnych modułów i dokumentacji powykonawczej całego Systemu w zakresie: administracji, procedur eksploatacyjnych, awaryjnych i wykonanych testów odbiorczych;
5. świadczenia usług gwarancyjnych dla dostarczonego Systemu, zgodnie z wymaganiami Zamawiającego opisanymi w niniejszym dokumencie.
6. zapewnienia dostępu do aktualizacji oprogramowania, wsparcia dla dostarczonego i wdrożonego Systemu, zgodnie z wymaganiami Zamawiającego opisanymi w niniejszym dokumencie;
7. zapewnienia wsparcia dla Zamawiającego w okresie stabilizacji Systemu, na warunkach opisanych w niniejszym dokumencie;
8. realizacji czynności wchodzących w zakres utrzymania i administrowania Systemem w okresie przejściowym, na warunkach opisanych w niniejszym dokumencie;
9. przekazania utrzymania Systemu po okresie przejściowym Zamawiającemu lub podmiotowi świadczącemu na rzecz Zamawiającego usługi w tym zakresie;
10. realizacji procesów automatyzujących użytkowanie Systemu, upraszczając operacyjność i minimalizując wymagany czas na administrowanie i nadzór, poprzez przygotowanie szablonów konfiguracyjnych nowych usług i widoków uproszczających procesy nadzorcze;
11. wykonania projektu architektury prezentującej możliwe scenariusze implementacji usług w oparciu o dostarczany System i posiadane przez zamawiającego bloki bezpieczeństwa CWB;
12. realizacji czynności wchodzących w zakres prawa opcji, którymi objęte są prace obejmujące rozbudowę składników Systemu.

### Założenia techniczne

Architektura Systemu zrealizowana w modelu zwirtualizowanej infrastruktury obliczeniowej. Założono rozciągnięcie infrastruktury obliczeniowej pomiędzy dwoma centralnymi aktywnymi ośrodkami przetwarzania danych (OPD) – OPD1 i OPD2 oraz szesnastoma regionalnymi ośrodkami przetwarzania (ROPD) – ROPD1-16.

System obejmujący centralne OPD1 i OPD2 będzie dostosowany do potrzeb systemów OSS, BSS, systemów NASK OSE (takich jak. np. Portal OSE, zasoby wideo, aplikacje), systemu zarządzania kolokacjami OSE, systemów zarządzania, monitorowania i automatyzacji zwirtualizowanej infrastruktury obliczeniowej, Systemu Retencji Logów, systemów wspierających infrastrukturę OSE (Element Manager, systemy zarządzania itp.).

Środowiska w regionalnych ROPD1-16 będą dostosowane do potrzeb systemów NASK OSE, systemów wspierających sieci OSE i Platformy Security Web Gateway i innych. Trzy regionalne ośrodki danych: Warszawa, Poznań i Katowice będą mieściły się w tych samych fizycznych lokalizacjach co centralne OPD (OPD1, 2 i 3).

Do zapewnienia odpowiedniej dostępności i ciągłości działania, OPD 1,2,3 są oddalone od siebie na odległość nie mniejszą niż 300 km) co minimalizuje wpływ zdarzeń losowych na ciągłość działania systemu.

Pomiędzy ROPD i OPD jest dostępna wydajna sieć OSE IP/MPLS (10/100 Gbps) umożliwiająca synchronizację i replikację danych, która w normalnym stanie pracy zapewnia   
opóźnienie <= 8ms i stały minimalny Jitter. W sytuacji awarii łącza opóźnienie może przekroczyć dwukrotnie określoną wcześniej wartość, jak również i Jitter może być zmienny. Charakterystyka sieci OSE wymagała takiego doboru łączy transmisyjnych, aby zapewniać wymagane parametry komunikacyjne we zmożonym oknie transmisyjnym od 07:00- 19:00 w dni robocze.

Projekt sieci OSE zakłada połączenie infrastruktury obliczeniowej łączem 80Gbps (min. 40Gbps) do sieci OSE. Założono wykorzystanie do 5Gbps dostępnych łączy transmisyjnych w ciągu dnia i do 90% w porze nocnej oraz poza dniami roboczymi. Wymagane jest rozdzielenie ruchu zarządzającego Systemem od pozostałego.

Na potrzeby składowania danych obiektowych (z funkcjonalnością WORM) i zapewniania wysokiej wydajności Komponentu obiektowego składowania danych, dane obiektowe będą przechowywane i dostępne również w ośrodku przetwarzania danych OPD3.

Dane składowane w Systemie, w Komponencie HCI, będą zabezpieczone kopiami zapasowymi i przechowywane w obu OPD.

Przyjęty model realizacji rozwiązania zakłada minimalizację nakładu pracy ludzkiej związanej z procesem utrzymania i integracji stosu obliczeniowego, sieciowego, pamięci masowych oraz wirtualizacji. Wymagane jest użycie rozwiązań pozwalających zautomatyzować zarządzanie infrastrukturą.

System musi zostać wdrożony zgodnie z wymaganiami Zamawiającego zawartymi w niniejszym dokumencie. Wszystkie wymagania i parametry, w tym techniczne, funkcjonalne i wydajnościowe zawarte w niniejszym dokumencie mają charakter obligatoryjny.

## Wymagania w zakresie celu i architektury

Podstawowy zadaniem w zakresie przedmiotu przedsięwzięcia jest dostarczenie infrastruktury programowo-sprzętowej. Wymagany System będzie stanowił zwirtualizowaną infrastrukturę obliczeniową, dostarczając zasobów dla środowisk produkcyjnych, deweloperskich i testowych.

System będzie zapewniał zasoby dla następujących systemów Zamawiającego:

1. systemów OSS i BSS,
2. systemów Zamawiającego (takich jak. np. Portal OSE, zasoby wideo, aplikacje),
3. systemu zarządzania kolokacjami OSE,
4. Systemu Retencji Logów,
5. Platformy Security Web Gateway.
6. Systemów Analitycznych
7. Systemów wspomagających nauczanie na odległość
8. innych

Projektując rozwiązanie Wykonawca musi uwzględnić następujące oczekiwania Zamawiającego:

1. minimalizacji komponentów różnych producentów;
2. wzajemna integracja Komponentów wchodzących w skład Systemu;
3. otwartość na rozbudowę Systemu poprzez dodawanie powtarzalnych elementów;
4. zapewnienie wymaganej mocy obliczeniowej przez Komponent HCI;
5. zapewnienie wymaganej pojemności dyskowej przez Komponent HCI;
6. możliwość przenoszenia Węzłów HCI pomiędzy regionami – w wyniku zmiany charakterystyki wymaganych potrzeb;
7. architektura Systemu umożliwiająca rozbudowę poprzez dodawanie powtarzalnych elementów składowych takich jak np.: Serwery HCI, przestrzeń dyskowa do składowania danych obiektowych oraz kopii zapasowych i archiwum, licencje na wirtualizację (Compute, SDS i SDN), licencje powiększające przestrzeń dla danych obiektowych oraz kopii zapasowych i archiwum itp.;
8. architektura Systemu umożliwiająca dodawanie elastyczne zasobów zewnętrznych i funkcjonalności poprzez integrację z zewnętrznymi Chmurami obliczeniowymi;
9. przechowywanie i analiza logów Systemu;
10. automatyczne przełączanie usług w przypadku awarii jednego OPD (OPD1, OPD2);
11. zapewnienie wymaganej ilości licencji na dostarczane oprogramowanie i infrastrukturę, z uwzględnieniem aspektów przełączania usług w przypadku awarii OPD;
12. zapewnienie wymaganej mocy obliczeniowej i powierzchni do składowania danych dla powyższych systemów jak również dla systemów pomocniczych;
13. skalowalność rozwiązania i efektywne wykorzystanie zasobów sprzętowych w Systemie;
14. zapewnienie wysokiej dostępności, integralności i poufności informacji przechowywanych w środowisku;
15. zapewnienie niezmienności przechowywanych danych;
16. tworzenie kopii zapasowych zapewniających możliwość odtworzenia systemu oraz bezstratnego odtworzenia danych i dokumentów na wypadek awarii OPD i ROPD;
17. zapewnienie jednolitej platformy sieci definiowanej programowo (SDN) dla Systemu pracującego w OPD1 i OPD2;
18. uproszczenie zarządzania infrastrukturą, przechowywaniem danych, bezpieczeństwem i wprowadzaniem zmian w infrastrukturze;
19. minimalizacja nakładów administracyjnych Systemu przez automatyzację procesów zarządczych i ograniczenie punktów kontaktu serwisowego producentów zastosowanych rozwiązań;
20. uproszczenie procesów dokonywania zmian i aktualizacji w systemach na poziomie komponentu sieci SDN, HCI, Compute, SDS, w sposób scentralizowany i automatyczny dla ośrodków przetwarzania danych OPD i ROPD;
21. uruchomienie niezbędnych elementów odpowiedzialnych za obsługę, nadzorowanie i zarządzanie infrastrukturą w formie maszyn wirtualnych na zasobach dostarczonej infrastruktury lub dedykowanych rozwiązaniach sprzętowo-programowych (appliance);
22. ujednolicenie technologii używanej do budowy Systemu i wzajemna zgodność oraz kompatybilność zastosowanych komponentów programowych i infrastrukturalnych;
23. wszystkie oferowane komponenty mają być objęte gwarancją zapewniając dostęp do wsparcia technicznego oraz aktualizacji oprogramowania przez okres obowiązywania umowy;
24. zarządzanie wszystkimi składnikami Systemu w ośrodkach przetwarzania danych OPD i ROPD ma być realizowane centralnie, musi zapewniać możliwość centralnego kreowania nowych usług;
25. System musi zapewniać dostępność usług w lokalizacjach OPD i ROPD przy awarii pojedynczego elementu np. serwera;
26. System musi zapewniać dostępność usług świadczonych w obu centralnych ośrodkach przetwarzania danych ODP1 i ODP2;
27. Wykonawca przeprowadzi analizę dostępnych i wymaganych interfejsów komunikacyjnych Ethernet 10Gbps SFP+ i przedstawi Zamawiającemu rekomendację w zakresie wymaganej rozbudowy np. dodania kart liniowych do przełączników w OPD;
28. Architektura Systemu musi zapewniać ochronę przetwarzanych w nim danych, w tym gwarantować rozliczanie działań osób, które uzyskały dostęp do informacji na podstawie mechanizmów identyfikacji i uwierzytelnienia, ochronę przed nieautoryzowanymi i niezamierzonymi modyfikacjami informacji, zapewniać kontrolowany dostęp do informacji;
29. Każdy z OPD i ROPD musi zostać zaprojektowany w modelu nadmiarowym, zapewniając wysoką dostępność (HA) w przypadku awarii pojedynczego elementu w Komponencie Systemu;
30. Architektura Systemu musi wzorować się na architekturze referencyjnej producentów oferowanych rozwiązań.

## Skalowalność rozwiązania

Architektura Systemu musi zapewniać możliwość zwiększenia pojemności. Komponenty Systemu oparte zostaną o bloki funkcjonalne („building blocks"), zapewniając możliwość elastycznego skalowania infrastruktury zarówno przez rozbudowę poszczególnych bloków, jak też poprzez dodawanie kolejnych.

System musi posiadać budowę modularną i charakteryzować się elastycznością w tworzeniu połączeń konfiguracyjnych poszczególnych Komponentów. Poszczególne elementy infrastruktury przetwarzania muszą być zwirtualizowane, przy zachowaniu przez infrastrukturę fizyczną wymaganej zdolności do przeprowadzania dynamicznych zmian przy zapewnieniu wysokiej niezawodności. Rozwiązanie ma łączyć w sobie elastyczność systemów ogólnego przeznaczenia i środowisk przetwarzania w zwirtualizowanej infrastrukturze obliczeniowej oraz prostotę dedykowanego urządzenia (ew. bloku).

W warstwie fizycznej Komponenty muszą zapewniać:

1. zestandaryzowane modele serwerów HCI zapewniające moc obliczeniową, bezpieczne przechowywanie danych i możliwą rozbudowę poprzez dodanie kolejnych serwerów;
2. możliwość rozbudowy Komponentu HCI o serwery minimum trzech producentów;
3. zintegrowany system kopii zapasowych z oprogramowaniem do wirtualizacji (Compute i SDS) pozwalający na bezpieczne przechowywanie danych zgodnie z polityką archiwizacji;
4. Oprogramowanie musi umożliwiać przeniesienie licencji (Compute, SDS, SDN) na nowszy sprzęt serwerowy przy zmianie potrzeb;
5. System pamięci, macierze obiektowe, pozwalające na bezpieczne i długoterminowe przechowywanie danych i zapewniające rozbudowę poprzez dodanie kolejnych serwerów;
6. wszystkie elementy Systemu muszą być chronione z poziomem nadmiarowości minimum N+1. Awaria pojedynczego elementu w Komponencie w OPD i ROPD nie może powodować niedostępności usługi, a jedynie ew. spadek jej wydajności;
7. Klastry obliczeniowe HCI w lokalizacji ODP1 i OPD2 muszą umożliwiać konfigurację nadmiarowości minimum N+2. Awaria dwóch serwerów w klastrze nie może skutkować przełączeniem usług między OPD;
8. umożliwienie podłączenia Systemu do Chmury Publicznej dedykowanym łączem (min. 10Gbps):
9. możliwość rozszerzenia dostępnej mocy obliczeniowej i przestrzeni do składowania danych,
10. umożliwienie dostępu systemom do usług w Chmurze Publicznej
11. Macierz obiektowa musi zapewniać skalowalność rzędu 3 mld obiektów 25KB przy 100 atrybutach/metadanych opisujących dane.

W warstwie funkcjonalnej rozwiązanie musi zapewniać:

1. narzędzia do nadzorowania, administrowania, monitorowania i zarządzania dostarczoną infrastrukturą muszą w skalowalny sposób być rozbudowywalne do min. trzykrotnego zwiększenia potrzeb wraz z obsługą środowisk Chmury Publicznej;
2. System musi integrować się z minimum dwoma Chmurami Publicznymi typu OCHK, AWS, Azure, GCP, IBM, itp. Musi istnieć możliwość wykorzystywania następujących usług: CDN, Storage obiektowy, AI/ML, Kontenery, BigData, bazy danych (relacyjne i nierelacyjne) i rozszerzenie zasobów przetwarzania (Compute, SDS, SDN) o zasoby Chmury Publicznej;
3. systemy administracji, monitorowania i zarządzania dostarczoną infrastrukturą muszą umożliwiać jednocześnie objęcie nadzorem zasobów w Chmurze Publicznej;
4. sieć SDN musi umożliwiać integrację z Chmurą Publiczną poprzez uzyskanie tych samych lub analogicznych polityk bezpieczeństwa;
5. elementy Systemu muszą posiadać natywne interfejsy programistyczne (API) oparte o powszechnie wykorzystywane standardy komunikacji, umożliwiające integrację z innymi systemami;
6. musi być możliwość zastosowania na serwerach HCI innego wirtualizatora od dostarczonego;
7. Oprogramowanie SDS do wirtualizacji przestrzeni dyskowej musi umożliwiać zmianę modelu stosowanych dysków i płynnego przejścia z rozwiązania Hybrydowego do ALL-Flash, poprzez wymianę dysków HDD na dyski SSD;
8. rozwiązanie musi obsługiwać środowiska zbudowane w modelu mikro usług, kontenerów.

## Ośrodki przetwarzania danych

Infrastruktura Systemu będzie zainstalowana w trzech ośrodkach centralnych (OPD1, OPD2, OPD3) oraz szesnastu ośrodkach regionalnych (ROPD 1 – 16).

W dwóch centralnych ośrodkach przetwarzania danych (OPD1 i OPD2) osadzone będą Komponenty realizujące przetwarzanie i składowanie danych oraz systemy kopii zapasowych. Komponent macierz obiektowa systemu składowania danych zostanie umieszczony w trzech ośrodkach przetwarzania danych (OPD1, OPD2 i OPD3). W każdym z tych ośrodków będzie dostępna infrastruktura sieci lokalnej dostarczonej przez Zamawiającego. Odpowiednia przepustowość sieci pomiędzy OPD i ROPD będzie zapewniona przez sieć OSE.

System ulokowany w OPD1 i OPD2 będzie stanowił uzupełniającą się i wzajemnie zabezpieczającą się parę (Active/Active, HA/DR[High Availability and Disaster Recovery]), gwarantując utrzymanie działania wszystkich usług przy braku dostępności jednego z dwóch ośrodków centralnych.

Komponent HCI zainstalowany w poszczególnych lokalizacjach (OPD1, OPD2, szesnastu ROPD) zapewni pulę zasobów, stanowiącą infrastrukturę wirtualizacyją w węzłach sieci OSE.

Infrastruktura sieciowa Zamawiającego jest ujednolicona w każdym z OPD/ROPD. Zamawiający wymaga w OPD1 i OPD2 sieci definiowanej programowo typu SDN (Software Defined Networking) podłączonej do sieci Zamawiającego.

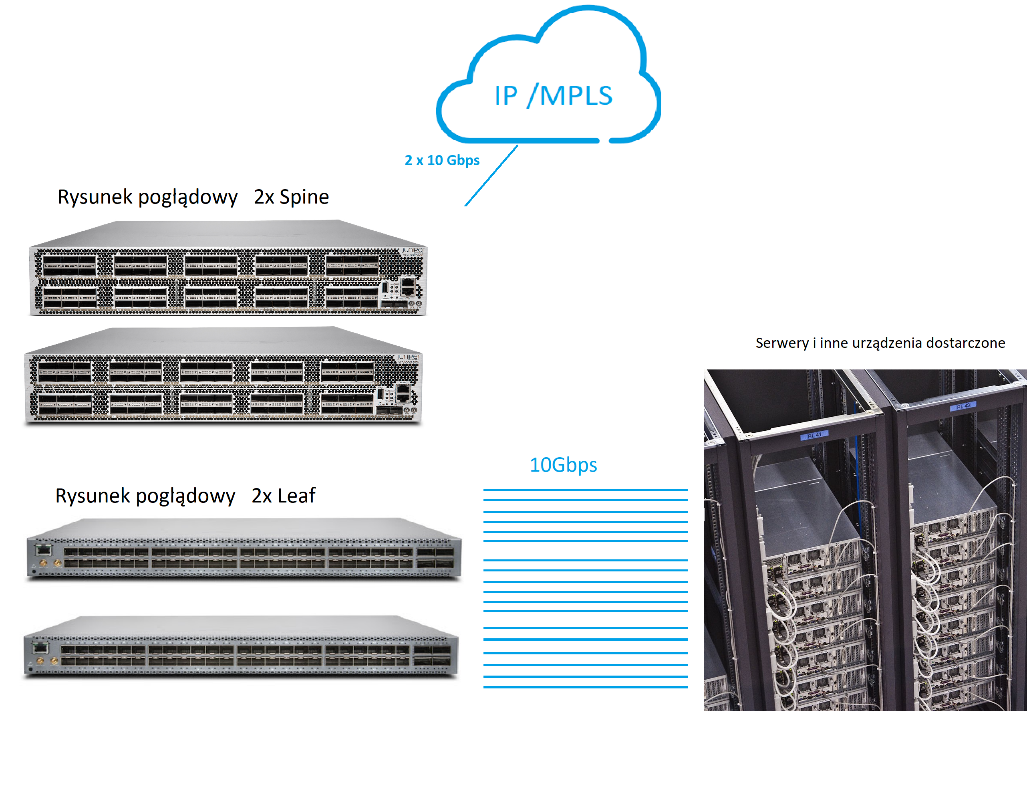
OPD1 i OPD2 będą miejscem przechowywania kopii zapasowych środowiska na potrzeby zapewnienia ciągłości działania po awariach OPD.

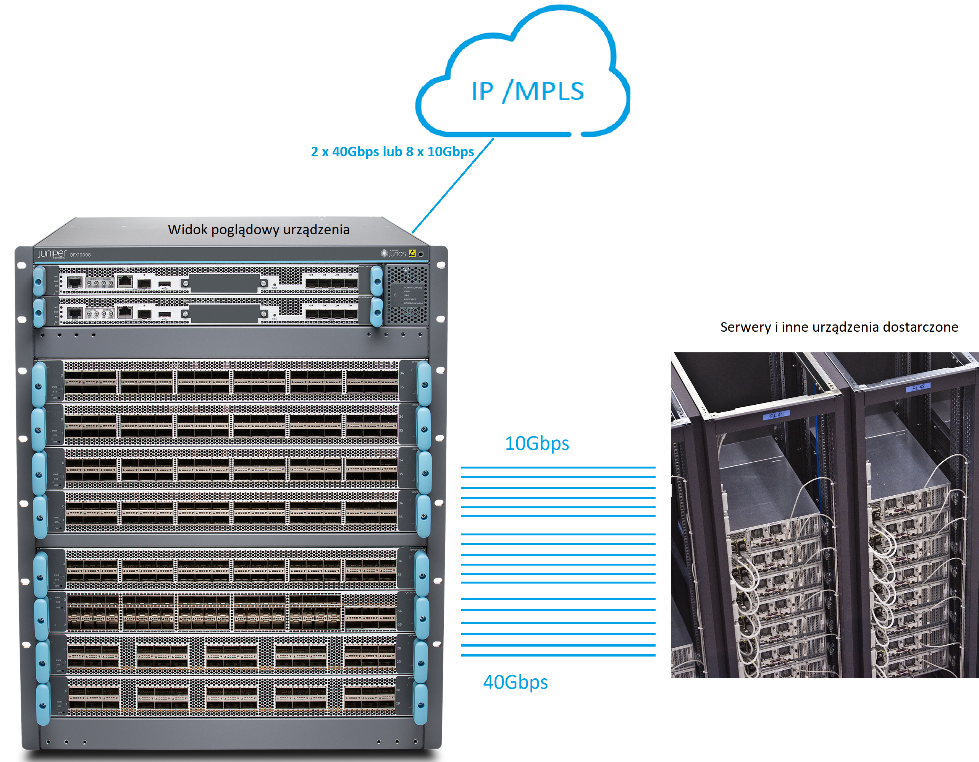
Oprogramowanie odpowiedzialne za orkiestrację, administrację, zarządzanie, eksploatację i monitoring Systemu będzie ulokowane w dwóch lokalizacjach OPD1 i OPD2 i będzie pracować w modelu Active/Passive lub Active/Active.

Planowaną topologię węzła sieci OSE w raz ze zwirtualizowaną infrastrukturą obliczeniową przedstawia poniższy rysunek:



Sposób podłączenia Systemu do sieci LAN Zamawiającego prezentuje schemat poniżej.

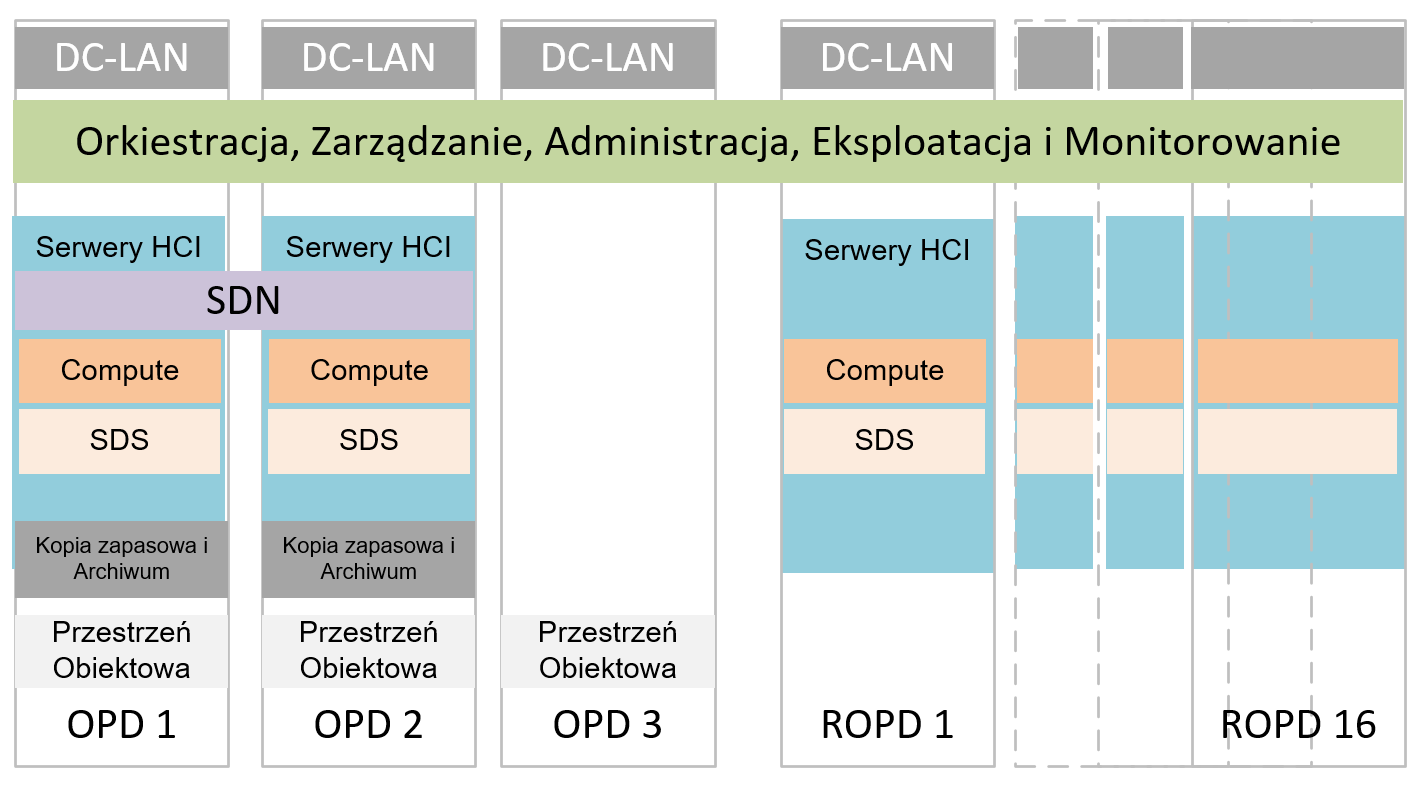
* Model podłączenia infrastruktury w ROPD1-13. 
* Model podłączenia infrastruktury w OPD/ROPD1-3



## Charakterystyka techniczna Systemu

System składać się będzie z oprogramowania i niezbędnego sprzętu. Zgodnie z wcześniej przedstawionymi założeniami, System będzie miał budowę blokową, przy czym poszczególne bloki będą tworzyły warstwy logiczne o zróżnicowanym zasięgu.

Ogólną architekturę logiczną Systemu przedstawia poniższy rysunek, kolejne akapity zawierają opis charakterystyki poszczególnych warstw i bloków funkcyjnych. Szczegółowe wymagania dla rozwiązań wchodzących w skład poszczególnych bloków zawarte są w punkcie 6.



W każdym Węźle sieci Wykonawca zainstaluje serwery HCI i wymagane oprogramowanie do wirtualizacji. Regionalne węzły sieci będą dostarczały moc obliczeniową (Compute) w większości dla systemu SWG. Zamawiający przywidział odpowiedni zapas mocy dla systemu SWG, zapewniający dostępność usług z założonym modelu (N+1).

Usługi SWG wymagają dedykowanych zasobów obliczeniowych do analizy treści realizowanej w dni robocze w godzinach 7:00-19:00. Oprogramowanie nadzorujące infrastrukturę musi umożliwiać monitorowanie wykorzystania zasobów, stanu infrastruktury, umożliwiać przenoszenie w trakcie pracy maszyn wirtualnych między serwerami HCI w wyniku zmiany charakterystyki wykorzystania zasobów obliczeniowych. Musi być także możliwe jednoczesne uruchamianie nowych usług w szesnastu ROPD. Wybrane usługi będą wymagały wykonywania kopii zapasowych zgodnie z harmonogramem.

W dwóch lustrzanych i centralnych i środkach OPD1 i OPD2 umieszczone będą usługi Zamawiającego. Zasoby obliczeniowe będą umożliwiały rozbudowę w miarę zwiększających się potrzeb, a także umożliwiały konsumpcję usług i zasobów w chmurze publicznej. Usługi uruchamiane będą w kilku modelach (usługi w jednym OPD, usługi w dwóch OPD, usługa przenoszona między OPD) umożliwiając bezpieczne świadczenie usług do sieci Internet i sieci OSE. W centralnych OPD będą dostępne zasoby obliczeniowe dla systemów produkcyjnych, przedprodukcyjnych, testowo/laboratoryjnych oraz dostępne będzie środowisko do odtwarzania i weryfikacji kopii zapasowych. Infrastruktura centralna musi się charakteryzować automatyzacją zadań, analityką wykorzystania i przewidywania możliwych do wystąpienia problemów. Musi zapewniać możliwość automatyzacji procesów nadzorczo-analitycznych, minimalizując procesy administracyjne i operacyjne. Infrastruktura centralna musi zachowywać ciągłość działania usług w przypadku awarii. Wybrane usługi będą wymagały replikacji asynchronicznej danych między centralnymi OPD. Wymagana replikacja danych musi być realizowana z interwałem nie większym niż 5min. i w sposób bezpieczny (bezpiecznie - szyfrowanie transmisji).

Przełączenie usług musi następować automatycznie. Zarządzanie infrastrukturą musi łączyć w sobie zarządzanie obszarem mocy obliczeniowej, procesory, pamięć RAM, programowalną pamięć masową i programowalną sieć lokalną (środowiska wirtualnego) w centrum danych. Sieć w centrum danych musi zapewniać kontrolę ruchu na poziomie interfejsu maszyny wirtualnej, zapewniać możliwość grupowania usług i kontroli ruchu w jednym segmencie warstwy drugiej modelu OSI. Cała infrastruktura musi podlegać szczegółowemu harmonogramowi wykonywania kopii zapasowych i politykom retencji kopii zapasowych.

Macierze obiektowe muszą zapewniać bezpieczną przestrzeń do składowania danych. Zamawiający oczekuje architektury w której będą udostępniane zasoby lokalnie w OPD1 i lokalnie w OPD2, a niezależnie te same zasoby będą dostępne w pozostałych OPD. Rozwiązanie powinno pracować w tak zwanym trybie aktywnych trzech ośrodków z replikacją asynchroniczną danych między ośrodkami.

### Warstwa przetwarzania

Zgodnie z założeniami, System zbudowany będzie z Komponentu HCI stanowiącego podstawę dla warstwy Compute wirtualizacji mocy obliczeniowej, SDS wirtualizacji przestrzeni dyskowej i SDN wirtualizacji sieci definiowanej programowo. Odpowiednio skompletowane grupy serwerów i uruchomione funkcjonalności będą umieszczone w każdym z szesnastu węzłów sieci OSE. Skala rozwiązania będzie odpowiadać oszacowanym dla danego węzła wymaganiom.

W poszczególnych lokalizacjach Komponenty HCI będą stanowiły osobne klastry obliczeniowe, dostarczające zasobów przetwarzania i składowania danych. Zastosowane rozwiązanie ma za zadanie zapewnić:

1. wysoką elastyczność podziału dostępnej puli zasobów i jej modyfikacji w miarę zmiennych potrzeb;
2. uproszczoną implementację i rozbudowę klastrów HCI;
3. możliwość przenoszenia zasobów i rozbudowy już istniejących;
4. mechanizmy wysokiej dostępności (HA) wbudowane w oprogramowanie zarządzające środowiskiem wirtualnym;
5. wykorzystywanie mechanizmów replikacji danych między głównymi OPD1 i OPD2;
6. zarządzanie przez administratorów komponentami Systemu w sposób bezpieczny, poprzez przeglądarkę internetową;
7. mechanizmy kontroli dostępu współpracujące z systemami kontroli dostępu/uwierzytelniania i autoryzacji AD i RADIUS).

### Compute - Wirtualizacja mocy obliczeniowej

Uruchomione na serwerach HCI oprogramowanie wirtualizacyjne będzie umożliwiać współdzielenie zasobów serwera. Zainstalowany (wirtualizator) na poszczególnych serwerach zapewnia pule zasobów CPU i RAM do wykorzystania. Zakłada się, że w każdym węźle będą osobne klastry wirtualizacyjne, zapewniając wysoką dostępność usług. Wirtualizacja zapewni wysoką dostępność usług w obu OPD (OPD1 i OPD2) poprzez mechanizmy umożliwiające uruchomienie maszyn wirtualnych w drugiej lokalizacji w sytuacji awarii. Zaplanowano w tym celu odpowiedni zapas mocy obliczeniowej. Rozwiązanie może wykorzystywać moc obliczeniową z Chmur Publicznych.

### SDS - wirtualizacja przestrzeni na dane

W celu uzyskania elastyczności i dostępności danych (w tym szybkiej rozbudowy) oraz udostępniania przestrzeni na dane dla środowisk wirtualnych w Systemie, wymagane jest zrealizowanie warstwy wirtualizacji przestrzeni danych, opartej na modelu Software-Defined Storage.

Warstwa wirtualizacji przestrzeni danych musi zapewnić przede wszystkim:

1. centralizację kontroli i zarządzania pojemnością danych w Systemie,
2. niezawodność przechowywanych danych poprzez posiadanie dwóch lub więcej replik danych,
3. automatyzację zarządzania w oparciu o polityki dostępności i wydajności danych,
4. odporność na awarie i minimalizację prac wymaganych przy utrzymaniu,
5. elastyczną zmianę polityk ochrony danych w trakcie pracy,
6. rozwiązanie może wykorzystywać powierzchnię danych w Chmurze Publicznej.

### SDN - wirtualizacja funkcji sieciowych

W celu zapewniania bezpieczeństwa w komunikacji sieciowej w środowisku wirtualnym w OPD1 i OPD2 oraz automatyzacji zarządzania funkcjami sieciowymi, wymagane jest zrealizowanie warstwy wirtualizacji funkcji sieciowych, opartej na modelu Software-Defined Networking.

Warstwa wirtualizacji funkcji sieciowych musi zapewnić przede wszystkim:

1. centralizację kontroli i zarządzania warstwą sieciową środowiska wirtualnego,
2. mikrosegmentację (na poziomie warstwy drugiej modelu OSI) środowiska sieciowego i kontroli ruchu już na poziomie wirtualnego interfejsu maszyny wirtualnej,
3. automatyzację zarządzania w oparciu o polityki aplikacyjne,
4. monitoring środowiska wirtualnego poprzez wgląd w komunikację maszyn wirtualnych,
5. elastyczne przenoszenie usług między centrami danych ODP1 i OPD2 jak również danych do Chmury Publicznej,
6. izolację maszyn wirtualnych, których reputacja wymaga weryfikacji,
7. równoważenie obciążenia bezpośrednio w środowisku wirtualnym.

### Warstwa orkiestracji, administracji, zarządzania, eksploatacji i monitorowania zwirtualizowaną infrastrukturą obliczeniową

Uproszczenie zarządzania Systemem wymaga stosowania narzędzi automatyzujących codzienne zadania. Wymagane jest rozwiązanie dokonujące dokładnej analizy środowiska wirtualnego w lokalizacjach centralnych (ODP1 i ODP2) i podstawowej w zakresie kontroli stanu w lokalizacji ROPD.

Rozwiązanie musi umożliwiać w zakresie orkiestracji:

1. uproszczenie procesu aktualizacji infrastruktury obliczeniowej Komponentu HCI i oprogramowania Compute, SDS, SDN poprzez stosowanie referencyjnych przygotowanych szablonów aktualizacyjnych,
2. ułatwienie procesu rozbudowy i modyfikacji infrastruktury serwerów HCI poprzez umożliwienie rozbudowy o nowe serwery i zasoby podczas pracy, przy zastosowaniu narzędzi centralnych,
3. zapewnienie automatyzacji zadań związanych z zarządzaniem oraz cyklem życia usług implementowanych.

Zarządzanie infrastrukturą musi umożliwiać minimalizację zaangażowania personelu administracyjnego w utrzymanie Systemu.

Muszą zostać zrealizowane następujące funkcjonalności:

1. zapewnienie mechanizmów umożliwiających budowę szablonów usług i aplikacji,
2. automatyzacja czynności związanych z uruchamianiem usług i aplikacji poprzez kontrolę wirtualizacji mocy obliczeniowej, wirtualizacji sieci, wirtualizacji przestrzeni dyskowej i tworzenie ciągów akcji,
3. automatyzacja procesów analitycznych, wykorzystania zasobów, błędów i monitoringu stanu infrastruktury; infrastruktura musi umożliwiać skonfigurowanie dla centralnych lokalizacji przewidywania i raportowania problemów, które mogą się pojawić np. z brakiem miejsca na dane z dużym zapotrzebowaniem na moc obliczeniową.

Monitoring rozwiązania musi umożliwiać zbieranie danych ze składników realizujących moc obliczeniową i kopie zapasowe, umożliwiając pozyskanie takich informacji jak:

1. stan infrastruktury sprzętowej i programowej,
2. raportowanie o problemach i ich prawdopodobnych przyczynach,
3. przygotowywanie akcji raportujących stan infrastruktury,
4. cykliczne generowanie raportów o stanie wykorzystania infrastruktury i poziomie dostępności zasobów.

### Moduł obiektowego składowania danych

Poza zasobami dyskowymi realizowanymi programowo przez SDS, będącymi elementem bloków warstwy przetwarzania, w architekturze Systemu przewidziano Komponent Macierzy Obiektowej, zapewniający składowanie danych obiektowych (ang. Object Storage). Głównym celem jego zastosowania jest zapewnienie optymalnej kosztowo i wydajnościowo dużej przestrzeni umożliwiającej przechowywanie danych wymagających dłuższej retencji (np. dane logów, video, audio, dokumenty).

Rozwiązanie musi posiadać funkcjonalność, która nie pozwoli na zmianę ani wykasowanie danych (WORM) przed upływem określonego czasu i będzie równolegle przechowywało dane w trzech ośrodkach (OPD1 / OPD2 / OPD3) celem zapewnienia bezpieczeństwa danych po awarii dowolnego OPD w modelu N+2. Rozwiązanie zapewnia dostęp do danych poprzez popularne protokoły komunikacyjne.

### Moduł tworzenia kopii zapasowych

Zapewnienie możliwości odzyskania danych po awarii wymaga cyklicznego tworzenia kopii zapasowych. System będzie dysponował Komponentem Kopii Zapasowych i Archiwum, wykorzystywanym w środowisku wirtualnym.

Rozwiązanie musi być zoptymalizowane dla infrastruktury zwirtualizowanej i wykorzystywać istniejące w niej mechanizmy wykonywania kopii zapasowych i odtwarzania, przy uwzględnieniu standardów charakterystycznych dla obszaru wirtualizacji i dostarczonego oprogramowania Compute i SDS.

Rozwiązanie musi umożliwiać Backup i Restore danych dla wszystkich szesnastu lokalizacji, zapewniać możliwość tworzenia, przenoszenia, wykonywania i odtwarzania kopii zapasowych maszyn wirtualnych i jednorodnego zarządzania.

W celu zapewnienia możliwie wysokiego poziomu ochrony danych, nawet w przypadku krytycznych awarii, Komponent przechowywania kopii zapasowych i archiwum musi być niezależny sprzętowo od pozostałych Komponentów Systemu.

W OPD1 i OPD2 będą przechowywane kopie zapasowe środowiska wirtualnego na potrzeby zapewnienia ciągłości działania po awarii OPD.

Zamawiający zakłada składowanie m.in. następujących danych:

1. kopie zapasowe obrazów maszyn wirtualnych wraz z ich konfiguracją,
2. konfiguracje Systemu zawierające konfigurację oprogramowania zarządzającego Systemem,
3. kopie zapasowe baz danych.

System w zakresie kopii zapasowych musi umożliwiać natychmiastowe odzyskiwanie danych i w trakcie procesu odtwarzania musi umożliwiać bezpośrednie uruchomienie maszyny wirtualnej z systemu kopii zapasowych.

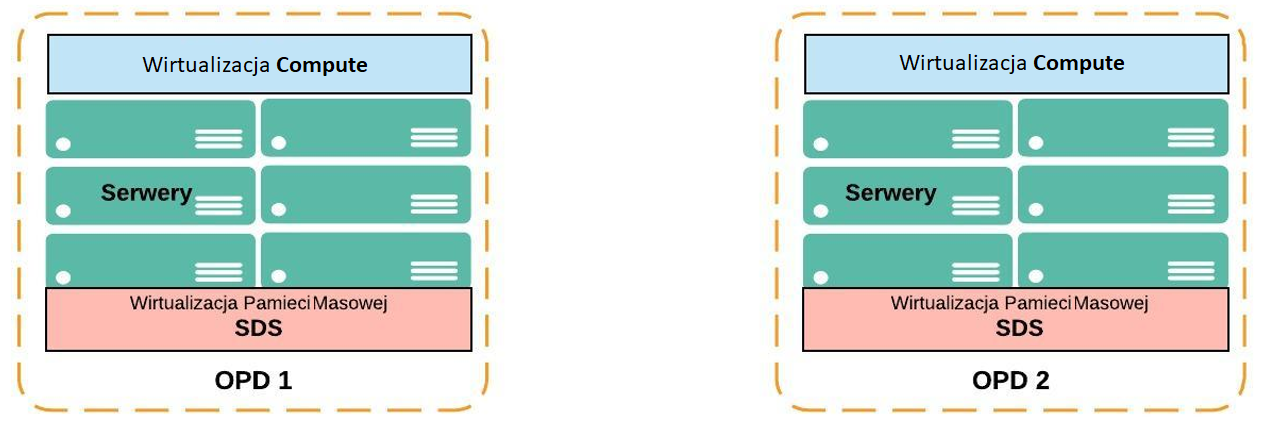
W celu zapewnienia bezpieczeństwa danych przesyłanych, oszczędzania pasma i szybkiego przesyłania i składowania danych pomiędzy ośrodkami, rozwiązanie musi realizować deduplikację danych, kompresję i szyfrowanie danych.

## Wdrożenie infrastruktury docelowej

Sprawna implementacja rozwiązania wymaga odpowiedniego scenariusza realizacji prac. Zamawiający oczekuje wykonania następującego planu prac:

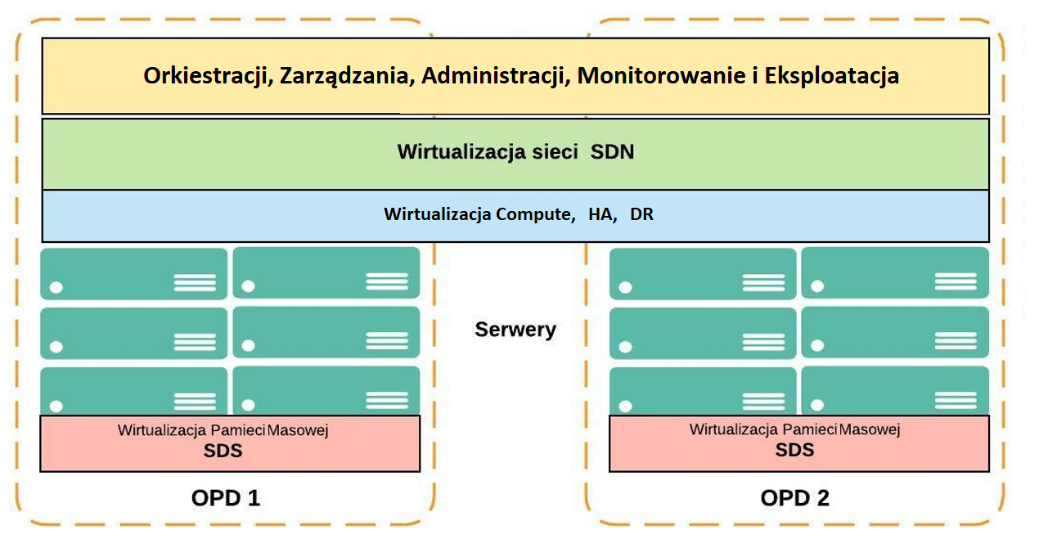
1. **Instalacja sprzętu pod wirtualizację**

W tej fazie w dwóch głównych ośrodkach przetwarzania danych (Warszawa i Poznań) Wykonawca zainstaluje serwery i pozostały sprzęt, a następnie podłączy je do zainstalowanej już sieci LAN. Przy braku odpowiedniej liczby portów, zgodnie z rekomendacją Wykonawcy, Zamawiający doposaży urządzenia Juniper QFX w wymagane karty liniowe w OPD1 i OPD2. Kolejne zadanie to instalacja warstwy wirtualizacyjnej mocy obliczeniowej wraz z wirtualizacją przestrzeni dyskowej SDS, która będzie zapewniać przestrzeń danych do uruchomienia pozostałych usług w modelu zwirtualizowanym. Uzyskane rozwiązanie przedstawiono na poglądowym rysunku poniżej.



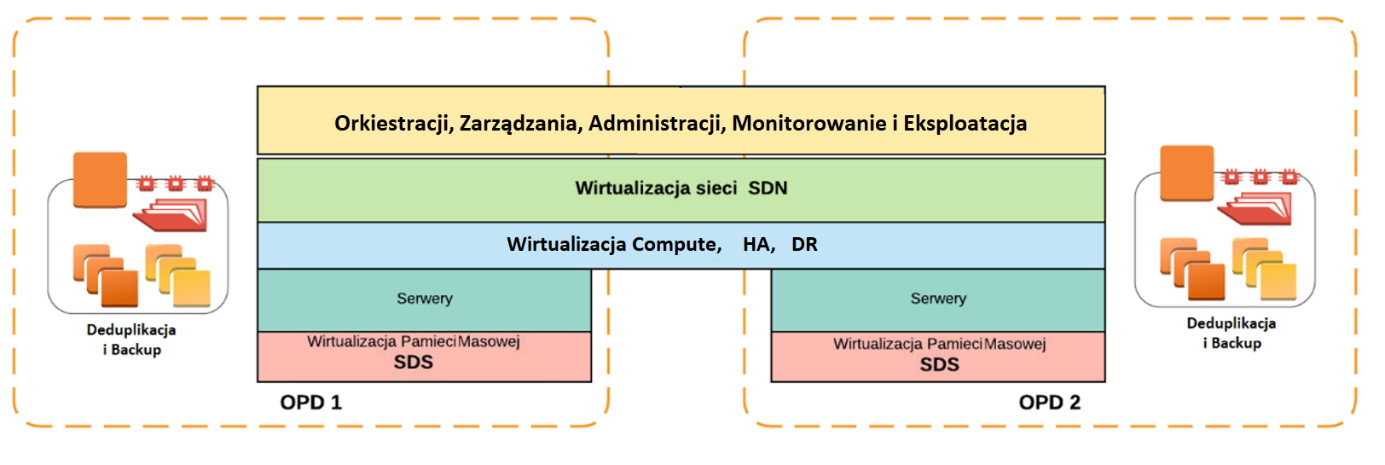
1. **Instalacja modułu zarządzającego warstwą wirtualizacji, SDS, SDN wraz z orkiestracją, zarządzaniem, eksploatacją i monitorowaniem.**

W tej fazie Wykonawca zainstaluje moduły zarządzania pojemnością i efektywnością platformy, a także moduł zbierania logów z infrastruktury. Zainstalowana zostanie warstwa wirtualizacji funkcji sieciowych SDN i zarządzania SDS. Na zakończenie Wykonawca zintegruje rozwiązanie z siecią OSE i zapewni zarządzanie całością Systemu.



1. **Instalacja systemu backup.**

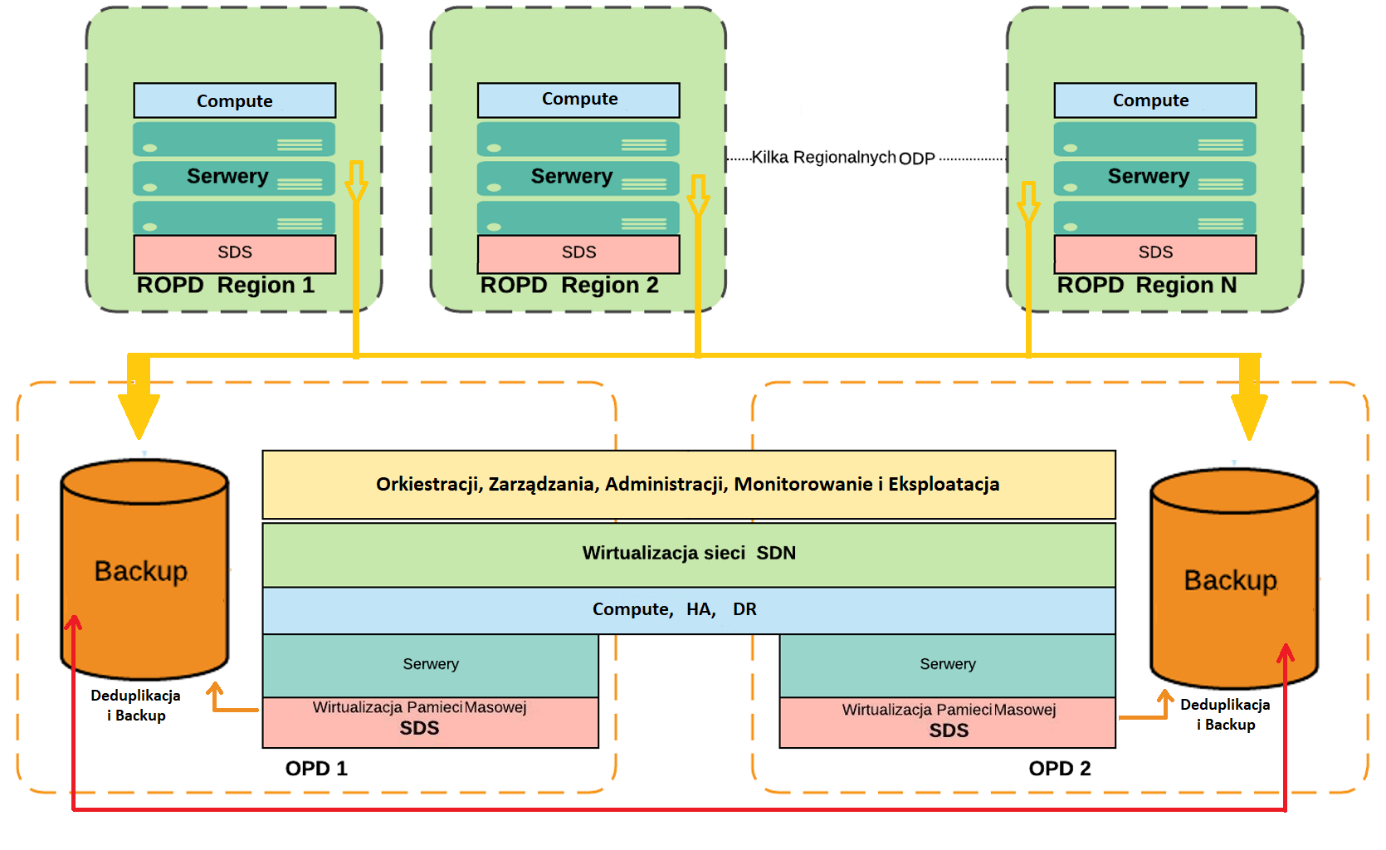
W tej fazie Wykonawca zainstaluje rozwiązania do backup-u oraz system odtwarzania po awarii w OPD1 i OPD2.



1. **Instalacja regionalnych ośrodków przetwarzania danych i konfiguracja systemów backup i SDS**

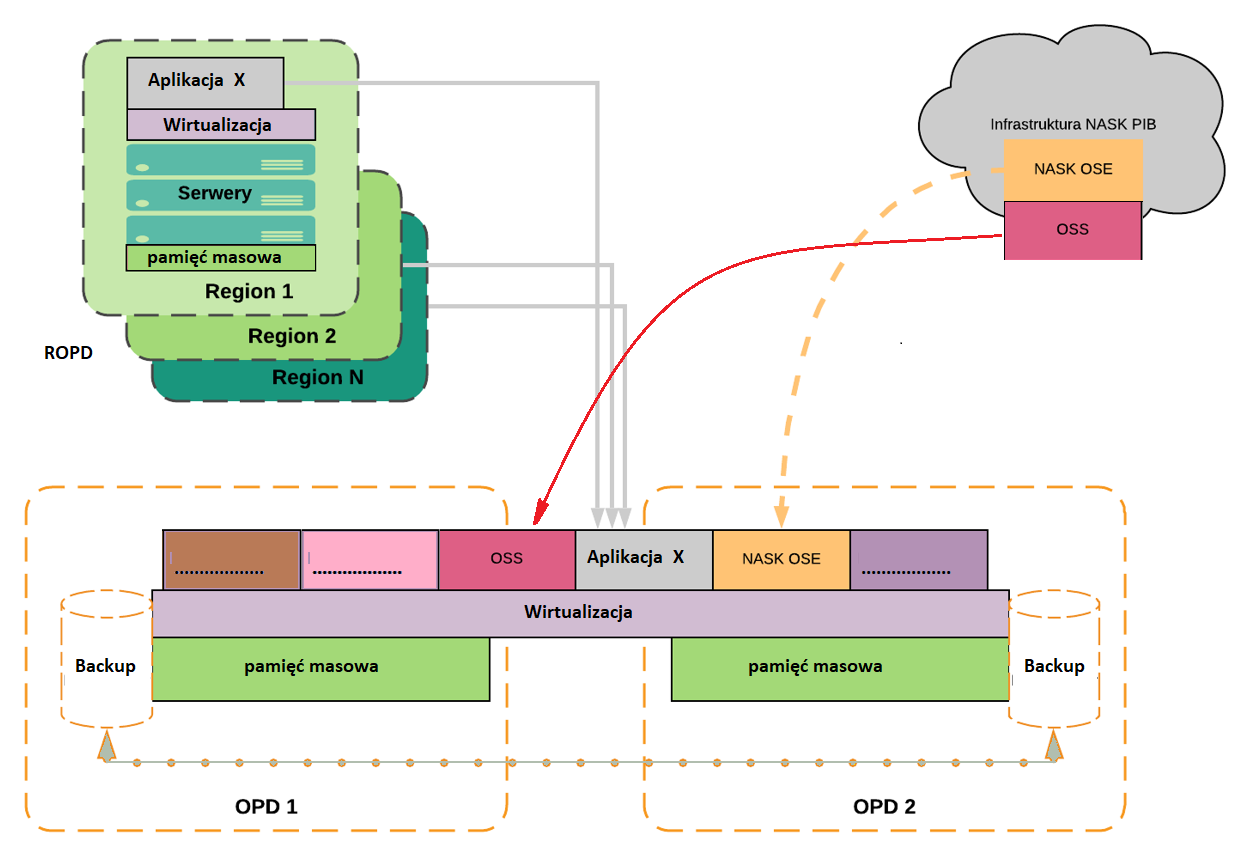
W tej fazie w regionalnych ośrodkach przetwarzania danych (w tym w 2 centralnych ośrodkach pełniących podwójną rolę) Wykonawca zainstaluje serwery i podłączy je do zainstalowanej sieci LAN urządzeń Juniper QFX. Zainstalowana zostanie warstwa wirtualizacyjna mocy obliczeniowej wraz z wirtualizacją przestrzeni dyskowej SDS. Skonfigurowane zostaną podstawowe zabezpieczania zasobów w ROPD poprzez mechanizm backupowy przechowujący dane w OPD z wykorzystaniem sieci OSE.

Większość z instalowanych serwerów będą to serwery obsługujące system Platformy Security Web Gateway w każdym z regionalnych ośrodków przetwarzania danych.



1. **Gotowość platformy do instalowania i migrowania aplikacji.**

Centralna platforma wirtualizacyjna jest gotowa do instalowania systemów zgodnie potrzebami Zamawiającego.



1. **Instalacja komponentów systemu przestrzeni obiektowej w trzech centrach danych.**

W tej fazie w głównych ośrodkach przetwarzania danych OPD1, ODP2, ODP3 Wykonawca zainstaluje infrastrukturę sprzętową, oprogramowanie i podłączy system do sieci LAN.

1. **Testy i Audyt zrealizowanego systemu i Komponentów.**

W tej fazie Zrealizowane będą testy odbiorcze, potwierdzające wymagane funkcjonalności wykonanych elementów i całości Systemu.

## Opcje rozbudowy Systemu, wydłużenia okresu Utrzymania i Prac Zleconych

W ramach przedmiotu zamówienia Zamawiającemu przysługuje uprawnienie do skorzystania z prawa opcji na zasadach określonych w Zapytaniu Ofertowym i we Wzorze Umowy. Prawo opcji dotyczy rozbudowy/rozbudów Rozwiązania oraz wydłużenia okresu, w którym w ramach Gwarancji, Wykonawca realizuje na rzecz Zamawiającego czynności z zakresu utrzymania Rozwiązania.

* + - 1. Przedmiotem opcji rozbudowy jest wdrożenie wraz z dostawą, instalacją, uruchomieniem i integracją oraz udzieleniem 5-letniej Gwarancji, na zasadach określonych w niniejszym dokumencie:

1. serwerów HCI w węzłach centralnych (spełniających wymagania na platformę HCI, dla węzłów w OPD1 i OPD2) wraz z wymaganymi licencjami realizującymi rozbudowę Komponentów obliczeniowych, obejmując m.in. SDS, SDN, Backup, Monitoring i Automatyzację (wymagana pamięć dyskowa brutto Capacity=60TB, Cache=1,8TB, RAM=512GB, Procesory 2 lub 3Ghz) - maksymalnie 40 sztuk;
2. serwerów HCI w węzłach regionalnych (spełniających wymagania na platformę HCI, dla węzłów w ROPD) wraz z wymaganymi licencjami realizującymi rozbudowę Komponentów obliczeniowych, obejmując m.in. SDS, Backup, Monitoring (wymagana pamięć dyskowa brutto Capacity=12TB, Cache=[zgodnie z tech. HDD/SSD], RAM=384GB, Procesory 2 lub 3Ghz) - maksymalnie 80 sztuk;
3. dodatkowej pojemności dyskowej brutto w serwerze do przechowywania danych 36TB, powierzchni dyskowej dla serwerów w węzłach centralnych (spełniających wymagania na platformę HCI) i regionalnych (na platformę HCI) – obejmuje maksymalnie liczbę dostarczonych serwerów wraz z prawem opcji;
4. dodatkowej pamięci RAM=256GB lub 512GB w serwerze dla serwerów w węzłach – maksymalnie liczba dostarczonych serwerów wraz z prawem opcji;
5. licencji na oprogramowanie do wirtualizacji mocy obliczeniowej i funkcjonalności SDS dla węzłów regionalnych – maksymalnie dla 50 serwerów dwuprocesorowych;
6. licencji na oprogramowanie do wirtualizacji mocy obliczeniowej i funkcjonalności SDS i SDN dla węzłów centralnych – maksymalnie dla 30 serwerów dwuprocesorowych;
7. przeniesienie i integracja serwera regionalnego do innego regionu – maksymalnie 30 sztuk;
8. dodatkowej przestrzeni netto 1PB (bez mechanizmów kompresji i deduplikacji) do przechowywania danych dla zaoferowanego obiektowego systemu przechowywania danych w ramach OPD1, OPD2, OPD3 – jednokrotne.

W ramach skorzystania z prawa opcji, Zamawiający jest uprawniony do składania Wykonawcy oświadczeń w przedmiocie rozbudowy w zakresie wszystkich bądź dowolnie wybranych opcji rozbudowy oraz ilości wskazanych w pkt a), b), c), d), e), f), g), h) i i) powyżej, w ilościach nie przekraczających wskazanych ilości maksymalnych.

1. Przedmiotem opcji utrzymania jest przedłużenie usługi Utrzymania Systemu, polegającej na kontroli działania Systemu, świadczonej przez Wykonawcę zgodnie z zakresem opisanym w dokumencie, o dalsze 3 miesiące, 2 razy po 3 miesiące lub o 6 miesięcy, ponad okres objęty zamówieniem podstawowym. Czynności Utrzymania są realizowane w obrębie dostarczonego rozwiązania.
2. W zakresie Gwarancji Wykonawca zapewni Zamawiającemu usługę Prac Zleconych na realizację prac dodatkowych w zakresie funkcjonowania rozwiązań dostarczonych przez Wykonawcę, w liczbie godzin:

**Liczba godzin:**

1. 1 rok świadczenia usług Prac Zleconych w ramach Gwarancji – 240 godzin
2. 2 rok świadczenia usług Prac Zleconych w ramach Gwarancji – 240 godzin
3. 3 rok świadczenia usług Prac Zleconych w ramach Gwarancji – 80 godzin
4. 4 rok świadczenia usług Prac Zleconych w ramach Gwarancji – 80 godzin
5. 5 rok świadczenia usług Prac Zleconych w ramach Gwarancji – 80 godzin

Rok definiowany jest jako dwanaście miesięcy od daty uruchomienia pierwszego Węzła.

# Szczegółowe wymagania funkcjonalne

## Infrastruktura docelowa

Wymagania szczegółowe dla Systemu zostały podzielone na obszary dotyczące poszczególnych Komponentów i przedstawione w oddzielnych punktach.

|  |  |  |
| --- | --- | --- |
| Obszar wymagań (Komponent) | Typ wymagań | Oznaczenie obszaru pkt. |
| Wymagania wspólne | Wymagania dla całości rozwiązania | 6.2 |
| Architektura HCI | Wymagania funkcjonalne | 6.3.1 |
| Serwery HCI | Wymagania sprzętowe | 6.3.2 |
| Compute | Moduł wirtualizacji mocy obliczeniowej CPU i RAM | 6.3.3 |
| SDS | Moduł wirtualizacji pamięci masowej | 6.3.4 |
| SDN | Moduł wirtualizacji funkcji sieciowych | 6.3.5 |
| Zasoby HCI | Skalowanie Klastrów wymagana | 6.3.6 |
| Zarządzanie HCI | Moduł orkiestracji, zarządzania i automatyzacji zwirtualizowanej infrastruktury obliczeniowej | 6.3.7 |
| Monitorowanie SDDC | Moduł monitorowania i ochrony środowiska wirtualnego | 6.3.8 |
| Chmura Publiczna | Wymagana możliwość integracji dla rozwiązania | 6.3.9 |
| Macierz obiektowa | Architektura i wymagania funkcjonalne | 6.4.1 |
| Macierz obiektowa | Wymagania sprzętowe | 6.4.2 |
| Kopie zapasowe i archiwum | Założenia architektura i wymagania funkcjonalne | 6.5.1 |
| Kopie zapasowe i archiwum | Wymagania funkcjonalne w zakresie monitorowania, raportowania oraz przeszukiwania kopii zapasowych i archiwów | 6.5.2 |
| Wymagania wdrożeniowe | Zakres prac wdrożeniowych | 6.6 |
| Testy weryfikacyjne | Testowanie Systemu i poszczególnych Komponentów | 6.6.1 |
| Dokumentacja | Wymagana dokumentacja Systemu | 6.6.2 |
| Instruktaże | Zakres instruktaży dla pracowników Zamawiającego | 6.6.3 |
| Gwarancja | Zakres świadczonych usług gwarancyjnych | 6.6.4 |
| Okres Stabilizacji | Zakres świadczenia usług wsparcia w okresie stabilizacji Systemu | 6.6.5 |
| Okres Utrzymania | Zakres świadczenia usług wsparcia w okresie utrzymania | 6.6.6 |

## Wymagania wspólne dla wszystkich Komponentów Systemu

Zamawiający wymaga dostarczenia Systemu spełniającego poniższe wymagania:

1. W zakresie dostarczania platformy sprzętowej czy programowej dla poszczególnych obszarów, wymagane jest aby dany komponent rozwiązania pochodził w całości od jednego producenta, np. w przypadku oferowania serwerów pod platformę HCI, wszystkie serwery mają pochodzić od jednego producenta, tak aby całość stanowiła spójne, możliwe do rozbudowy w sposób modułowy rozwiązanie.
2. Uszczegółowienie wymagań pkt 1:
   1. Wymagane jest dostarczenie sprzętu tego samego producenta w zakresie serwerów Komponentu HCI do wszystkich Węzłów sieci OSE.
   2. Wymagane jest dostarczenie oprogramowania jednego producenta w zakresie Compute (wirtualizatora) do wszystkich Węzłów sieci OSE.
   3. Wymagane jest dostarczenie oprogramowania jednego producenta w zakresie SDS (wirtualizacji pamięci) do wszystkich Węzłów sieci OSE.
   4. Wymagane jest dostarczenie oprogramowania jednego producenta w zakresie SDN (wirtualizatora sieci ) do dwóch Węzłów sieci OSE.
   5. Wymagane jest dostarczenie urządzeń macierzy obiektowej tego samego producenta w zakresie sprzętu do trzech Węzłów sieci OSE.
   6. Wymagane jest dostarczenie oprogramowania macierzy obiektowej tego samego producenta do trzech Węzłów sieci OSE.
   7. Wymagane jest dostarczenie sprzętu tego samego producenta w zakresie kopii zapasowej i archiwum do dwóch Węzłów sieci OSE.
   8. Wymagane jest dostarczenie oprogramowania kopia zapasowej i archiwum tego samego producenta do dwóch Węzłów sieci OSE.
3. Wymagane jest aby procesory w serwerach HCI pochodziły od jednego producenta w ROPD i OPD.
4. Jeżeli do poprawnego działania dostarczanego Komponentu, modułu, elementu oprogramowania, niezbędne jest wykorzystanie dodatkowych elementów, licencji (np. związanych z aspektem przełączania usług w przypadku awarii OPD), nieujętych wprost w szczegółowym opisie wymagań, to należy je przewidzieć i dostarczyć w ramach oferowanego Systemu i wynagrodzenia z tytułu realizacji przedmiotu zamówienia.
5. Oferowane urządzenia muszą pochodzić z bieżącej linii produkcyjnej, być wyprodukowane nie wcześniej niż 6 miesięcy przed dostawą, muszą być produktem rozwijanym, w najnowszej stabilnej wersji i nie może być dla nich ogłoszone zakończenie produkcji, koniec sprzedaży, ani koniec wsparcia. Jeżeli oferowany sprzęt posiada nowszą wersję, następcę, oficjalnie wskazaną przez producenta – należy zaoferować sprzęt najnowszy.
6. Oferowane oprogramowanie ma być produktem rozwijanym, w najnowszej stabilnej wersji i nie może być dla niego ogłoszone zakończenie produkcji, koniec sprzedaży, ani koniec wsparcia. Jeżeli oferowane oprogramowanie posiada nowszą wersję, następcę oprogramowania - należy zaoferować rozwiązanie najnowsze.
7. Środowisko zbudowane w centralnych ośrodkach OPD1 i OPD2 musi być wykonane jako lustrzane kopie.
8. Środowisko musi zapewniać pełną redundancję i przejmowanie funkcjonalności ODP1 przez OPD2 i OPD2 przez OPD1.
9. W przypadku awarii jednego OPD (OPD1 lub ODP2) zarządzanie Systemem (Komponentami i Oprogramowaniem) w pozostałych piętnastu węzłach musi być dostępne po 15min. od wystąpienia awarii.
   1. Należy rozumieć jako zarządzanie całością Systemu z wyłączeniem uszkodzonej lokalizacji w sposób analogiczny jak przed awarią.
   2. Proces odtworzenia usług musi odbywać się automatycznie i ręcznie, w zależności od polityki przypisanej do usług świadczonych tylko w jednym OPD.
10. Wszystkie Komponenty muszą:
    1. zapewniać funkcjonalność umożliwiającą zarządzanie poprzez ustandaryzowany interfejs API, zapewniając możliwość integracji z zewnętrznymi narzędziami do monitoringu i automatyzacji zadań.
    2. zapewniać funkcjonalność umożliwiającą raportowanie stanu wykonywanych zadań, zgłaszanie awarii, informowanie o przekroczeniu progowych wartości poprzez wysłanie wiadomości email.
11. Wykonawca zobowiązany jest dostarczyć niezbędne ilości odpowiednich wkładek (modułów oraz kabli połączeniowych (iDAC, optycznych i miedzianych) w celu podłączenia dostarczanej infrastruktury fizycznej do istniejących przełączników LAN Zamawiającego i sieci elektrycznej.
12. Wykonawca zobowiązany jest podłączyć wszystkie dostarczone urządzenia w sposób nadmiarowy (min. 2 połączenia dla ruchu produkcyjnego, w wyłączeniem portów typu OOB zarządzających). Każde urządzenie musi być podłączone do min. dwóch przełączników lub min. dwóch kart liniowych.
13. Urządzenia wchodzące w skład Systemu montowane w poszczególnych ośrodkach przetwarzania danych nie mogą zajmować więcej przestrzeni w szafach teleinformatycznych, jak również nie mogą zużywać więcej mocy elektrycznej niż wartości podane w poniższej tabeli. Poniższe wartości określają całkowite zasoby jakie zostały zarezerwowane dla Systemu w kolokacjach.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Region** | **Miasto** | **Typ** | **Ilość miejsca w szafie/szafach** | **Moc dostępna** |
| **[U]** | **[kW]** |
| **MAZOWIECKIE** | Warszawa | OPD1i ROPD | 280 | 160 |
| **WIELKOPOLSKIE** | Poznań | OPD2 i ROPD | 160 | 100 |
| **ŚLĄSKIE** | Katowice | OPD3 i ROPD | 80 | 38,5 |
| **DOLNOŚLĄSKIE** | Wrocław | ROPD | 40 | 24 |
| **KUJAWSKO-POMORSKIE** | Toruń | ROPD | 40 | 23 |
| **LUBELSKIE** | Lublin | ROPD | 40 | 24 |
| **LUBUSKIE** | Zielona Góra | ROPD | 40 | 19 |
| **ŁÓDZKIE** | Łódź | ROPD | 40 | 24 |
| **MAŁOPOLSKIE** | Kraków | ROPD | 40 | 29 |
| **OPOLSKIE** | Opole | ROPD | 40 | 19 |
| **PODKARPACKIE** | Rzeszów | ROPD | 40 | 25 |
| **PODLASKIE** | Białystok | ROPD | 40 | 21 |
| **POMORSKIE** | Gdańsk | ROPD | 40 | 23 |
| **ŚWIĘTOKRZYSKIE** | Kielce | ROPD | 40 | 21 |
| **WARMIŃSKO-MAZURSKIE** | Olsztyn | ROPD | 40 | 21 |
| **ZACHODNIOPOMORSKIE** | Szczecin | ROPD | 40 | 22 |

1. Oprogramowanie musi być rozwijane przez okres obowiązywania umowy:
   1. Posiadać minimum jedną główną aktualizację oprogramowania na rok.
   2. Posiadać bieżące aktualizacje błędów oprogramowania co 4 miesiące.
2. Środowisko testowe do odtwarzania kopii zapasowych musi zostać ulokowane w OPD1

## Wirtualizacja mocy obliczeniowej

### Architektura HCI – wymagania funkcjonalne

Zamawiający wymaga dostarczenia rozwiązania spełniającego poniższe funkcjonalności:

1. rozwiązanie musi integrować zasoby mocy obliczeniowej (CPU, pamięć operacyjna) i pamięć masową;
2. rozwiązanie musi być zbudowane w oparciu o węzły serwerowe x86 integrujące procesory, pamięć operacyjną i pamięć masową opartą o dyski HDD, SSD, NVMe;
3. architektura rozwiązania musi zapewniać rozbudowę i skalowanie zarówno mocy obliczeniowej pamięci RAM, pojemności przestrzeni cache, jak i pojemności przestrzeni dyskowej;
4. serwery muszą być maksymalnie dwuprocesorowe, aby ograniczyć spadek wydajności w wyniku awarii jednego z węzłów;
5. architektura musi zapewniać ciągłość i pełną funkcjonalność działania w wypadku awarii lub całkowitej niedostępności pojedynczego serwera, nadmiarowość min. N+1. Dopuszczalny jest jedynie spadek wydajności w klastrze HCI;
6. architektura musi umożliwiać kontrolowane wyłączenie pojedynczego serwera z klastra poprzez przełączanie go w tryb utrzymaniowy;
7. architektura musi umożliwiać zbudowanie wspólnej przestrzeni dyskowej w oparciu o dyski wewnętrzne serwerów fizycznych. Wymagane jest wsparcie dla konfiguracji sprzętowej serwera opartej o dyski SSD i HDD oraz dla konfiguracji serwera opartej wyłącznie o dyski SSD i NVMe lub NVMe;
8. architektura musi umożliwiać implementację węzłów all-flash (tylko SSD) całkowicie opartych o urządzenia z interfejsem NVMe (tzw. all-NVMe);
9. architektura musi zapewniać implementację wspólnego zasobu pamięci masowej (datastore) w oparciu o cały zbiór serwerów HCI, zapewniając dostęp do danych w taki sam sposób dla każdego serwera HCI wchodzącego w skład klastra;
10. architektura serwerów musi zgodna z wirtualizatorem mocy obliczeniowej oprogramowania SDS i SDN, w tym posiadać możliwość zarządzania i monitorowania z systemu zarządzania (natywnie lub przez moduł typu Plug-in);
11. rozwiązanie musi zapewniać możliwość rozbudowy do co najmniej 32 węzłów w klastrze;
12. rozwiązanie musi posiadać funkcjonalność budowy klastrów rozciągniętych między dwoma węzłami OPD1 i ODP2;
13. rozwiązanie musi być zgodne z co najmniej dwoma systemami wirtualizacji mocy obliczeniowej: VMware vSphere, Microsoft Hyper-V, Linux KVM.

### Serwery HCI - wymagania sprzętowe

Wymagane są serwery charakteryzujące się następującymi parametrami:

1. serwery muszą pochodzić z jednej linii produkcyjnej, zapewniając uproszczony proces aktualizacji i rozbudowy;
2. serwery muszą być zgodne z oferowanym oprogramowaniem do wirtualizacji mocy obliczeniowej i oprogramowaniem do wirtualizacji przestrzeni dyskowej
   1. model serwera i jego składniki muszą być umieszczone na oficjalnej stronie zaoferowanego producenta oprogramowania do wirtualizacji (Compute i SDS);
3. obudowa typu RACK 19" o wysokości nie przekraczającej 2U wraz z zestawem do zamontowania w szafie teleinformatycznej 19", o głębokości 80-100 cm i prowadzeniem dla kabli, umożliwiającym pełne wysunięcie obudowy na szynach;
4. wyposażone w panel LCD lub LED umieszczony na froncie serwera, umożliwiający wyświetlenie informacji o stanie serwera, zasilania oraz temperatury lub za pomocą dedykowanego oprogramowania do zarządzania infrastrukturą serwerową;
5. płyta główna musi posiadać następujące cechy:
   1. być zaprojektowana przez producenta serwera,
   2. dwa fizyczne gniazda do obsługi procesorów 64 bitowych wyspecyfikowanych w następnych punktach,
   3. chipset dedykowany do pracy w konfiguracjach 2 procesorowych, obsługujący opisane procesory,
   4. co najmniej 24 sloty do obsługi pamięci DDR4, pracującej z częstotliwością min. 2666 MHz,
   5. obsługa do 1024 GB pamięci RAM,
6. możliwość instalacji minimum dziesięciu dysków HDD/SSD w formie 2.5” SFF wymiennych od przodu serwera (hot-swap) dla serwerów o wysokości 1U,
7. możliwość instalacji minimum dwudziestu dysków HDD/SSD w formie 2.5” SFF wymiennych od przodu serwera (hot-swap) dla serwerów o wysokości 2U,
8. zajęte nie więcej jak połowa dostępnych slotów na dyski wymienne od przodu serwera,
9. możliwość instalacji/zainstalowany kontrolera macierzy RAID zgodny z dostarczonym oprogramowaniem SDS,
10. możliwość instalacji co najmniej dwóch urządzeń NVMe,
11. minimum 6 slotów PCI Express (w tym min. 2 sloty PCI Express x16 generacji 3) dla serwera o wysokości 2U,
12. minimum 2 gniazda PCI Express x16 generacji 3 dla serwera o wysokości 1U,
13. zintegrowana karta graficzna o rozdzielczości minimum 1900 x 1200,
14. możliwość instalacji modułu TPM,
15. wyposażony w procesory 64 bitowe o minimalnym parametrach:
    1. przy częstotliwość taktowania zegara min.3.0 GHz wyposażony w min. 18 rdzenie,
    2. przy częstotliwość taktowania zegara min.2.0 GHz wyposażony w min. 24 rdzenie,
    3. liczba obsługiwanych kanałów pamięci: 6,
    4. wbudowane w procesor wsparcie dla obsługi standardu PCIe 3.0,
    5. pamięć podręczna procesora cache L3: 20 MB,
    6. zintegrowany kontroler zarządzania pamięcią,
    7. procesor wspierający funkcjonalność dynamicznego i automatycznego zwiększenia wydajności serwera dla aplikacji poprzez zwiększenie częstotliwości rdzenia,
    8. dwa procesory muszą w teście SPEC2017 Int Rate Base publikowanym na stronach spec.org zapewniać osiągnięcie wyniku wydajności serwera minimum 200 punktów;
16. wyposażony w pamięć RAM minimum kości DDR4 2666 MHz RDIMM
    1. zainstalowane kości o pojemności min. 32GB,
    2. zainstalowana pamięć RAM konieczna do zapewnienia wymaganej pojemności klastra zgodnie ze specyfikacją klastrów poniżej,
    3. zainstalowane minimum 220 GB pamięci RAM w OPD1 i ODP2 dla jednego procesora w serwerze,
    4. zainstalowane minimum 140GB pamięci RAM w ROPD dla jednego procesora w serwerze,
    5. obsadzone nie więcej jak połowa dostępnych slotów na moduły pamięci RAM,
    6. możliwość rozbudowy do 1024 GB pamięci RAM w OPD1 i OPD2,
    7. musi posiadać następujące zabezpieczenia pamięci RAM: ECC, Memory Mirroring, Memory demand and patrol scrubbing, Memory Rank Sparing (lub Online Spare), SDDC (lub Fast Fault Tolerance);
17. wyposażony w dyski twarde lub karty pamięci:
    1. zainstalowane nośniki pamięci stałej (SD lub SSD lub M.2) na potrzeby systemu operacyjnego zapewniające pojemność co najmniej 16GB skonfigurowane w RAID 1 (pojemność nie wlicza się do wymaganej pojemności klastra),
    2. zainstalowana odpowiednia kompilacja dysków (HDD, SSD, NVMe) konieczna do zapewnienia wymaganej pojemności klastra zgodnie ze specyfikacją klastrów poniżej,
    3. obsadzone nie więcej jak połowa dostępnych slotów na dyski wymienne,
    4. zainstalowane dyski HDD muszą być dyskami serwerowymi SAS lub SAS-NL o Szybkości obrotowej RPM nie mniej jak 10k (10000),
    5. zainstalowane dyski muszą być wspierane przez producenta rozwiązania HCI w kategorii dysków przeznaczonych pod zastosowania Cache, Capacity,
       1. musza znajdować się na oficjalnej stronie producenta oprogramowania SDS jako dyski dostosowane do zastosowania jako Cache lub Capacity
       2. dyski Cache (typu SSD i NVMe) muszą umożliwiać 3 krotne zapisanie ich pojemności w ciągu dnia przez 5 lat użytkowania dla ROPD
       3. dyski Cache (typu SSD i NVMe) muszą umożliwiać 5 krotne zapisanie ich pojemności w ciągu dnia przez 5 lat użytkowania dla OPD1 i OPD2
       4. dyski Capacity (typu SSD i NVMe) muszą umożliwiać 1 krotne zapisanie ich pojemności w ciągu dnia przez 5 lat użytkowania.
    6. Wymagane są następujące parametry dysków twardych:
       1. Serwery HCI wyposażone wyłącznie w dyski typu NVMe:
          1. Dysk/Dyski Cache muszą spełniać następujące parametry: rozmiar min. 300GB, wydajność min 100 000 zapisów na sekundę
          2. Dysk/Dyski Capacity muszą spełniać następujące parametry: rozmiar min. 9TB, wydajność min. 30 000 zapisów na sekundę
       2. Serwery HCI wyposażone wyłącznie w dyski typu SSD i NVMe:
          1. Dysk/Dyski Cache muszą spełniać następujące parametry: rozmiar min. 900GB, wydajność min 80 000 zapisów na sekundę
          2. Dysk/Dyski Capacity muszą spełniać następujące parametry: rozmiar min. 6TB, wydajność min. 30 000 zapisów na sekundę
       3. Serwery HCI wyposażone wyłącznie w dyski typu HDD/SSD i SSD/NVMe:
          1. Dysk/Dyski Cache muszą spełniać następujące parametry: rozmiar min. 300GB, wydajność min 30 000 zapisów na sekundę
       4. Dysk/Dyski Capacity muszą spełniać następujące parametry: rozmiar min. 2TB, wydajność min. 200 zapisów na sekundę,
    7. współczynnik pojemność dysków Cache do pojemności dysków Capacity musi być zgodny z dobrymi praktykami producenta oprogramowania i nie może być mniejszy jak:
       1. 10% Cache dla rozwiązań hybrydowych dyski HDD i SSD/NVMe
       2. 3% Cache dla rozwiązań bez dysków HDD,
18. wyposażony w interfejsy sieciowe LAN:
    1. min. 2 porty Gigabit Ethernet 1000Base-T RJ-45
    2. min. 4 porty 10 Gigabit Ethernet w formie gniazd SFP+ na płycie głównej lub karcie PCIe
19. wyposażony w min. 1 interfejs sieciowy na potrzeby zarządzania RJ-45 10/100/1000 dedykowany dla zarządzania;
20. wyposażony w następujące inne interfejsy:
    1. min. 2 bezpośrednio udostępnione zewnętrzne porty USB 3.0,
    2. min. 1 bezpośrednio udostępniony port VGA DB15,
    3. wyposażony w moduł zdalnego zarządzania (konsoli) umożliwiający:
       1. zdalne włączenie, wyłączenie i restart serwera
       2. wykorzystanie zdalnej, graficznej konsoli obsługująca zdalną pracę na serwerze
       3. podgląd logów serwera
       4. przejęcie pełnej konsoli graficznej serwera niezależnie od jego stanu (także podczas startu, restartu OS)
       5. podłączanie wirtualnych napędów CD oraz obrazów instalacyjnych
       6. konfiguracja BIOS
       7. wsparcie dla szyfrowanego połączenia SSL
       8. wsparcie dla SNMP; IPMI2.0, VLAN tagging (zgodnie ze standardem IEEE 802.1q), SSH
       9. wsparcie dla SNMP
       10. monitorowanie stanu zasilaczy, wentylatorów, dysków, temperatury, wielkości poboru energii,
       11. rozwiązanie sprzętowe, niezależne od CPU i od działających systemów operacyjnych,
       12. aktualizacja firmware modułu (karty) zarządzania zdalnego bez konieczności restartu serwera
       13. definiowanie wielu użytkowników z możliwością uwierzytelniania w LDAP, Active Directory, Radius
       14. wysyłanie powiadomień syslog do zewnętrznych serwerów
       15. rejestrowanie działań administratora w oparciu o log;
21. Zasilanie, chłodzenie:
    1. min. dwa jednakowe zasilacze wymienne podczas pracy serwera w konfiguracji redundantnej, zapewniającej zasilanie serwera działającego ze 100% wykorzystaniem zasobów sprzętowych na jednym zasilaczu, hot swap,
    2. redundantne chłodzenie serwera, co najmniej dwa wentylatory, hot swap;
22. Serwer musi posiadać deklarację CE.

### Compute - wirtualizacji mocy obliczeniowej

Zamawiający wymaga dostarczenia oprogramowania spełniającego poniższe funkcjonalności:

1. Oprogramowanie musi być instalowane bezpośrednio na sprzęcie fizycznym i nie może być ono częścią innego systemu operacyjnego;
2. Oprogramowanie musi umożliwiać współdzielenie zasobów obliczeniowych i pamięci masowej dla wielu maszyn wirtualnych;
3. Oprogramowanie musi umożliwiać 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;
4. Oprogramowanie musi dawać możliwość klonowania systemów operacyjnych wraz z ich pełną konfiguracją i danymi;
5. Oprogramowanie musi umożliwiać wykonywanie kopii migawkowych instancji systemów operacyjnych na potrzeby tworzenia kopii;
6. Oprogramowanie musi umożliwiać przenoszenie maszyn wirtualnych w czasie ich pracy pomiędzy serwerami fizycznymi oraz różnymi konsolami do zarządzania wirtualizacją;
7. Oprogramowanie musi umożliwiać ponowne uruchomienie systemów/usług w przypadku awarii poszczególnych elementów infrastruktury bez utraty danych;
8. Oprogramowanie musi umożliwiać bezpieczne, bezprzerwowe i automatyczne uaktualnianie warstwy wirtualizacyjnej, wliczając w to zarówno poprawki bezpieczeństwa jak i zmianę jej wersji, bez potrzeby wyłączania wirtualnych maszyn;
9. Oprogramowanie musi umożliwiać przywrócenie funkcjonalności maszyny wirtualnej w przypadku awarii lub niedostępności serwera fizycznego, powinna ona być podejmowana automatycznie, jednak musi istnieć możliwość określenia przez administratora czasu, po jakim taka decyzja jest wykonywana;
10. Oprogramowanie musi umożliwiać przełączenie ścieżek SAN (bez utraty komunikacji) w przypadku awarii jednej ze ścieżek;
11. Oprogramowanie musi umożliwiać obsługę 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 się w prawidłowej, niezmienionej formie poprzez weryfikację podpisu cyfrowego;
12. Oprogramowanie musi umożliwiać automatyczne równoważenie obciążenia procesora i pamięci RAM serwerów fizycznych pracujących, jako platforma dla infrastruktury wirtualnej;
13. Oprogramowanie musi dawać możliwość rozbudowy do co najmniej 32 węzłów w klastrze;
14. W zaoferowanym oprogramowaniu warstwa wirtualizacji nie może dla własnych celów alokować więcej niż 5GB pamięci operacyjnej RAM serwera fizycznego;
15. Zaoferowane oprogramowanie do wirtualizacji zainstalowane na serwerze fizycznym musi potrafić obsłużyć i wykorzystać procesory fizyczne tego serwera wyposażone w 256 logicznych wątków, 1TB pamięci fizycznej RAM tego serwera oraz 2 procesorów fizycznych tego serwera;
16. Oprogramowanie musi dawać możliwość skonfigurowania maszyn wirtualnych z ilością od 1 do 56 procesorów wirtualnych;
17. Oprogramowanie musi dawać możliwość skonfigurowania maszyn wirtualnych z możliwością przydzielenia do 2 TB pamięci operacyjnej RAM;
18. Oprogramowanie musi dawać możliwość skonfigurowania maszyn wirtualnych z możliwością przydzielenia od 1 do 8 wirtualnych kart sieciowych dla każdej z nich;
19. Oprogramowanie musi dawać możliwość skonfigurowania maszyn wirtualnych, z których każda może mieć 2 porty szeregowe, i 8 urządzeń USB;
20. Oprogramowanie musi dawać możliwość uruchomienia maszyn wirtualnych z systemem operacyjnym: Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows Server 2016, Windows Server 2019, Windows 7, Windows 8, SLES 12, SLES 11, SLES 10, SLES 9, RHEL 8, REHL 7, RHEL 6, RHEL 5, RHEL 4, Debian, CentOS, FreeBSD, Ubuntu, Oracle Linux;
21. W celu osiągnięcia maksymalnego współczynnika konsolidacji, Oprogramowanie musi umożliwiać przydzielenie łącznie większej ilości pamięci RAM dla maszyn wirtualnych niż fizyczne zasoby RAM serwera, na którym maszyny te są posadowione;
22. Rozwiązanie musi umożliwiać udostępnienie maszynie wirtualnej większej ilości zasobów dyskowych niż jest fizycznie dostępne na zasobach dyskowych ;
23. Oprogramowanie musi umożliwiać sprzętowe wsparcie dla wirtualizacji zagnieżdżonej, w szczególności w zakresie możliwości zastosowania przykładowo trybu XP mode w Microsoft Windows 7, a także instalacji wszystkich funkcjonalności, w tym Microsoft Hyper-V pakietu Microsoft Windows Server 2012 na maszynie wirtualnej i oprogramowania GNS3 do wirtualizacji sieci;
24. Oprogramowanie musi umożliwiać integrację z rozwiązaniami antywirusowymi firm trzecich w zakresie skanowania maszyn wirtualnych z poziomu warstwy wirtualizacji bez ingerencji w systemy operacyjne maszyn wirtualnych (bezagentowość);
25. Oprogramowanie musi umożliwiać zdalny i lokalny dostęp administracyjny do wszystkich serwerów fizycznych poprzez protokół SSH;
26. Oprogramowanie musi umożliwiać możliwość powielania maszyn wirtualnych wraz z ich pełną konfiguracją i danymi;
27. Oprogramowanie musi dawać możliwość wykonywania kopii migawkowych instancji systemów operacyjnych na potrzeby tworzenia kopii zapasowych bez przerywania ich pracy z możliwością konieczności zachowania stanu pamięci pracującej maszyny wirtualnej;
28. Konsola zarządzająca zaoferowanego oprogramowania musi posiadać możliwość przydzielania i konfiguracji uprawnień z możliwością integracji z usługami katalogowymi, minimalnie z: Microsoft Active Directory oraz umożliwiać federacyjne zarządzanie tożsamością w oparciu o Active Directory Federation Services (ADFS);
29. Oprogramowanie musi umożliwiać dodawanie zasobów w czasie pracy maszyny wirtualnej, w szczególności w zakresie ilości procesorów, pamięci operacyjnej i przestrzeni dyskowej;
30. Oprogramowanie musi posiadać funkcjonalność tworzenia wirtualnego przełącznika (virtual switch) umożliwiającego tworzenie sieci wirtualnej w obszarze hosta (hypervisora wirtualizacyjnego) i pozwalającego połączyć tym przełącznikiem maszyny wirtualne w obszarze jednego hosta, a także na zewnątrz sieci fizycznej. Pojedynczy przełącznik wirtualny powinien mieć możliwość konfiguracji minimum 3000 portów;
    1. Pojedynczy wirtualny przełącznik w zaoferowanym oprogramowaniu, w celu zapewnienia bezpieczeństwa połączenia ethernetowego w razie awarii fizycznej karty sieciowej, musi posiadać możliwość przyłączania do niego minimum dwóch fizycznych kart sieciowych,
    2. Wirtualne przełączniki w zaoferowanym oprogramowaniu muszą posiadać funkcjonalność obsługi wirtualnych sieci lokalnych (VLAN);
31. Oprogramowanie musi umożliwiać wykorzystanie przepustowości sieci do 20GbE;
32. Oprogramowanie musi obsługiwać przełączenie ścieżek LAN (bez utraty komunikacji) w przypadku awarii jednej ze ścieżek;
33. Oprogramowanie musi zapewnić możliwość zdefiniowania alertów informujących o przekroczeniu wartości progowych;
34. Oprogramowanie musi umożliwiać replikacje maszyn wirtualnych z pamięci masowej SDS między oddalonymi ośrodkami przetwarzania. Replikacja musi gwarantować współczynnik RPO (ang Recovery Point Objective) na poziomie minimum 5 minut
    1. Replikacja danych między OPD musi być szyfrowana
35. Oprogramowanie musi obsługiwać przełączenie ścieżek SAN (bez utraty komunikacji) w przypadku awarii jednej ze ścieżek;
36. Oprogramowanie musi umożliwiać przenoszenia maszyn wirtualnych pomiędzy serwerami fizycznymi bez przerywania pracy usług na przenoszonych maszynach wirtualnych.
    1. Wymaga się wsparcia natywnego szyfrowania ruchu sieciowego dla maszyn wirtualnych podczas ich przenoszenia między ośrodkami danych, serwerami fizycznymi
37. Oprogramowanie musi umożliwiać automatyczne, ponowne uruchomienie maszyn wirtualnych w przypadku awarii jednego z wirtualizatorów na kolejnym, działającym w tym samym klastrze wirtualizatorze (funkcjonalność HA) (ang. high availability);
38. Zaoferowane oprogramowanie minimalnie dwoma wirtualizatorami oraz w przypadku potrzeby wgrania aktualizacji do warstwy wirtualizacji, musi posiadać możliwość w przypadku wywołania startu aktualizacji, automatycznego przeniesienia bezprzerwowego działających maszyn wirtualnych do innego wirtualizatora nie objętego aktualizacją, przed rozpoczęciem samej aktualizacji
39. Oprogramowanie musi posiadać co najmniej 2 niezależne mechanizmy wzajemnej komunikacji między serwerami z zainstalowanym wirtualizatorem oraz z serwerem zarządzającym, gwarantujące właściwe działanie mechanizmów wysokiej dostępności na wypadek izolacji sieciowej serwerów fizycznych lub partycjonowania sieci;
40. Oprogramowanie musi zapewniać możliwość stworzenia dysku maszyny wirtualnej o wielkości 40 TB;
41. Oprogramowanie musi posiadać wbudowany interfejs programistyczny (API), zapewniający pełną integrację zewnętrznych rozwiązań wykonywania kopii zapasowych z istniejącymi mechanizmami warstwy wirtualizacyjnej;
42. Oprogramowanie musi wspierać rozwiązania do automatyzacji procesów;
43. Oprogramowanie musi wspierać TPM 2.0. Minimalne wymaganie Zamawiającego dla TPM oznacza, że TPM zapewnia mechanizm gwarantujący, że serwer fizyczny, na którym zainstalowane jest zaoferowane oprogramowanie, uruchomił się z włączoną opcją Secure Boot. Po potwierdzeniu, że Secure Boot jest włączone, system gwarantuje, poprzez weryfikację podpisu cyfrowego, że hypervisor uruchomił się w niezmienionej formie;
44. Oprogramowanie musi posiadać funkcjonalność wirtualnego TPM 2.0 dla maszyn wirtualnych z zainstalowanym Microsoft Windows 10 oraz Microsoft Windows 2016. Zamawiający wymaga aby z punktu widzenia maszyny wirtualnej z systemem operacyjnym Microsoft Windows 10 lub Microsoft Windows 2016 wirtualny TPM widziany był jako standardowy TPM, gdzie można przechowywać bezpiecznie wrażliwe dane np. certyfikaty. Zawartość wirtualnego TPM musi być przechowywana w pliku przynależnym do maszyny wirtualnej oraz musi być szyfrowana;
45. Oprogramowanie musi posiadać możliwość aktualizacji i kontroli wersji oprogramowania do wirtualizacji w ramach klastra serwerów z poziomu centralnej konsoli zarządzającej.
    1. Konsola zarządzająca musi mieć możliwość automatycznej weryfikacji, czy zainstalowane komponenty serwera posiadają rekomendowaną wersję sterowników i firmware, eliminując ryzyko pracy na nieaktualnych wersjach.
    2. Taka funkcjonalność powinna być dostępna dla minimum trzech producentów serwerów;
46. Oprogramowanie musi posiadać wsparcie dla natywnych dysków 4K;
47. Oprogramowanie musi wspierać protokół precyzyjnej synchronizacji czasu PTP i NTP
48. Oprogramowanie 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;
49. Oprogramowanie musi mieć funkcjonalność migracji w trybie rzeczywistym dysków działających maszyn wirtualnych z jednego podsystemu dyskowego do innego bez konieczności przerywania pracy maszyny wirtualnej, której dysk jest migrowany;
50. Oprogramowanie podczas pracy w klastrze musi umożliwiać automatyczne równoważenie obciążenia wykorzystania procesorów i pamięci RAM serwerów fizycznych pracujących jako platforma dla infrastruktury wirtualnej;
51. Oprogramowanie musi zapewniać mechanizm pozwalający tworzyć profil (szablon konfiguracji) wybranego serwera wirtualizacyjnego (Hypervisora), a następnie wymuszać ten profil/konfigurację na innych serwerach fizycznych lub sprawdzać zgodność konfiguracji pomiędzy zdefiniowanym wcześniej profilem a wskazanym serwerem fizycznym;
52. Oprogramowanie musi umożliwiać utworzenie w nim jednorodnego, wirtualnego przełącznika sieciowego, rozproszonego na wszystkie serwery fizyczne istniejące w tym klastrze.
    1. Przełącznik taki musi zapewniać możliwość konfiguracji parametrów sieciowych maszyny wirtualnej z granulacją na poziomie portu tego przełącznika.
    2. Pojedyncza maszyna wirtualna musi mieć możliwość wykorzystania jednego lub wielu portów przełącznika z niezależną od siebie konfiguracją.
    3. Przełącznik rozproszony musi zapewniać raportowanie przepływów w oparciu o protokół IPFIX
    4. Zaimplementowany w zaoferowanym oprogramowaniu przełącznik rozproszony musi umożliwiać funkcjonalność duplikowania ruchu sieciowego dowolnego jego portu wirtualnego na inny port
    5. Zaimplementowany w zaoferowanym oprogramowaniu przełącznik rozproszony 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;
53. Oprogramowanie musi mieć możliwość uruchamiania fizycznych serwerów z centralnie przygotowanego obrazu poprzez protokół PXE skracając proces budowy i uruchamiania środowiska;
54. Oprogramowanie musi mieć możliwość przenoszenia maszyn wirtualnych w czasie ich pracy pomiędzy serwerami fizycznymi, pamięciami masowymi niezależnie od dostępności współdzielonej przestrzeni dyskowej, oraz pomiędzy dwoma Centrami Przetwarzania Danych;
55. Oprogramowanie musi mieć wbudowany mechanizm kontrolowania i monitorowania ruchu do pamięci masowych oraz ustalania priorytetów dostępu do nich na poziomie konkretnych wirtualnych maszyn;
56. Oprogramowanie 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;
57. Oprogramowanie musi umożliwiać uruchamianie kontenerów zbudowanych w topologii Docker Image w wirtualnych maszynach;
58. Oprogramowanie musi umożliwiać instalowanie, uruchamianie i zarządzanie aplikacjami klasy Big Data oraz Hadoop z poziomu platformy wirtualizującej;
59. Oprogramowanie musi wspierać możliwość eksportu konfiguracji centralnej konsoli zarządzającej przez API;
60. Oprogramowanie musi posiadać możliwość testowania wybranych serwerów (w szczególności tych, na których uruchomione są aplikacje przetwarzające dane wrażliwe i które mają dostęp do kluczy szyfrujących maszyny wirtualne) w celu weryfikacji, czy oprogramowanie jest autentyczne i nie zostało zmodyfikowane. Funkcjonalność ta powinna działać w oparciu o chip TPM 2.0 zainstalowany w serwerze i powinna odbywać się poza centralną konsolą zarządzającą (która sama jest maszyną wirtualną) wyłącznie w oparciu o sprzętowe źródło zaufania (hardware root of trust). Tylko serwery, które przejdą weryfikację, mogą mieć dostęp do kluczy szyfrujących;
61. Centralna konsola zarządzania zapewniająca:
    1. możliwość tworzenia, modyfikowania, usuwania i konfigurowania wirtualnych maszyn
    2. możliwość automatycznego uruchamiania wirtualnych maszyn z przygotowanego szablonu dla wielu lokalizacji jednocześnie
    3. możliwość rezerwacji zasobów dla wybranych grup użytkowników oraz kontroli tych zasobów w obrębie wskazanej grupy użytkowników
    4. możliwość tworzenia wielu logicznych, izolowanych od siebie grup maszyn wirtualnych i określania dla nich zasobów fizycznych
    5. możliwość zarządzania uprawnieniami dla poszczególnych użytkowników w zależności od pełnionej roli, opartej na rolach m.in. administrator, operator, audyt itd..
    6. zarządzanie poprzez ustandaryzowany interfejs API

### SDS wirtualizacji przestrzeni dyskowej

Zamawiający wymaga dostarczenia oprogramowania spełniającego poniższe funkcjonalności:

1. Oprogramowanie musi umożliwiać zbudowanie współdzielonej przestrzeni dyskowej w oparciu o dyski wewnętrzne serwerów fizycznych. System powinien wspierać następujące konfiguracje: hybrydowa w oparciu o dyski SSD i HDD oraz all-flash w oparciu o dyski SSD (SAS/SATA/NVMe).
2. Każdy serwer fizyczny, na którym zostanie zainstalowane zaoferowane oprogramowane, musi dostarczać zarówno moc obliczeniową do klastra (CPU i RAM) jak również przestrzeń dyskową definiowaną programowo (eng. Software Defined Storage). Powyższa funkcjonalność musi dać możliwość utworzenia przestrzeni dyskowej złożonej do 32 hostów.
3. W przypadku potrzeby wykonania rozwiązania, opartego na zaoferowanym oprogramowaniu, posiadającego wyłącznie dyski SSD, oprogramowanie musi zapewniać możliwość optymalizacji wydajności poprzez wbudowaną funkcjonalność „cache’owania” operacji zapisu.
4. W przypadku potrzeby wykonania rozwiązania opartego na zaoferowanym oprogramowaniu, posiadającego dyski mieszane, tj. SSD i HDD, Oprogramowanie musi zapewniać możliwość optymalizacji wydajności poprzez wbudowaną funkcjonalność „cache’owania” operacji zapisu i odczytu.
5. W przypadku potrzeby wykonania rozwiązania opartego na zaoferowanym oprogramowaniu posiadającego dyski mieszane, tj. SSD i HDD, oprogramowanie musi posiadać funkcjonalność rezerwacji, dla poszczególnych maszyn wirtualnych, części dysku „cache” wykonującego funkcję odczytu.
6. Zaoferowane rozwiązanie musi wspierać technologie NVMe i “cache’owanie” operacji zapisu z wykorzystaniem dysków NVMe.
7. Zaoferowane rozwiązanie musi umożliwiać konfigurację serwerów all-NVMe.
8. W przypadku zastosowania dysków NVMe zaoferowanie rozwiązanie musi wspierać ich wymianę w trybie hot-plug dla dodawania i wyjmowania dysków “na gorąco”.
   1. Taka funkcjonalność musi być dostępna dla minimum trzech producentów serwerów
9. Zaoferowane rozwiązanie musi wspierać “cache’owanie” operacji zapisu z wykorzystaniem dysków Intel Optane.
10. Oprogramowanie musi posiadać możliwość aktualizacji i kontroli wersji oprogramowania do wirtualizacji pamięci masowej w ramach klastra serwerów z poziomu centralnej konsoli zarządzającej SDS.
    1. Dodatkowo centralna konsola zarządzająca musi posiadać funkcjonalność aktualizacji firmware komponentów serwera fizycznego (dyski, kontrolery, karty sieciowe) z poziomu konsoli zarządzającej SDS.
    2. Konsola zarządzająca musi mieć możliwość automatycznej weryfikacji, czy zainstalowane komponenty serwera posiadają rekomendowaną wersję sterowników i firmware, eliminując ryzyko pracy na nieaktualnych wersjach.
    3. Taka funkcjonalność powinna być dostępna dla minimum trzech producentów serwerów
11. Oprogramowanie musi zapewniać możliwość zmniejszania lub zwiększenia przestrzeni dyskowej (odjęcie lub dodanie pojedynczego dysku, odjęcie lub dodanie serwera fizycznego) w sposób niewymagający przestoju i przerwy w dostępie do działających na zmienianym środowisku maszyn wirtualnych.
12. Konfiguracja, zarządzanie i monitoring przestrzeni dyskowej, w zaoferowanym oprogramowaniu, muszą być zintegrowane z centralną konsolą zarządzającą platformą wirtualizacyjną Compute
13. Oprogramowanie musi zapewniać możliwość obsługiwania dysków wirtualnych maszyn do rozmiaru min. 40TB.
14. Funkcjonalności zaoferowanego oprogramowania nie może w żaden sposób ograniczać lub niwelować żadnej funkcjonalności platformy wirtualizacyjnej między innymi w warstwie mechanizmów niezawodnościowych, wydajnościowo-optymalizacyjnych jak i zarządzania.
15. Oprogramowanie musi zapewniać funkcjonalność konfigurowalnych mechanizmów zabezpieczania danych na wypadek awarii sprzętowej w ramach lokalizacji lub szafy rack w taki sposób, aby poszczególne kopie dysków maszyny wirtualnej nie były umieszczane na hostach w ramach tej samej szafy rackowej lub w ramach tej samej lokalizacji.
16. Oprogramowanie musi posiadać, na oficjalnej stronie producenta tego oprogramowania, listę wspieranych i certyfikowanych konfiguracji serwerowych. Wymagane jest wsparcie dla min. trzech niezalenych producentów sprzętu serwerowego dostępnego na terenie Unii Europejskiej.
17. Oprogramowanie nie może wprowadzać ograniczenia, aby na etapie rozbudowy przestrzeni dyskowej wymagana była rozbudowa jedynie o serwery fizyczne producenta wykorzystane na etapie przed rozbudową. W przypadku rozbudowy o kolejne serwery fizyczne, wytworzone na podstawie zaoferowanego oprogramowania, rozwiązanie nie może wprowadzać wymogu aby w dostarczanych, kolejnych serwerach fizycznych, wymagana była instalacja komponentów sprzętowych oferowanych tylko przez jednego dostawce/producenta (np. dyski, adaptery, specjalizowane karty i kontrolery).
18. Oprogramowanie musi zapewniać możliwości rozbudowy i skalowania zarówno mocy obliczeniowej, pojemności przestrzeni cache, jak i pojemności przestrzeni dyskowej (w ramach istniejącej infrastruktury serwerów fizycznych) bez konieczności dodawania kolejnych serwerów fizycznych.
19. Oprogramowanie musi zapewniać możliwość rozbudowy oferowanej przestrzeni dyskowej poprzez dodanie pojedynczego dysku lub dodanie jednego lub więcej serwera fizycznego w sposób niewymagający przestoju i przerwy w dostępie do działających usług wirtualnych.
20. Oprogramowanie musi zapewniać możliwość ochrony danych przed utratą ich integralności za pomocą weryfikacji sum kontrolnych. Suma kontrolna musi być liczona w momencie wykonania przez maszynę wirtualną operacji IO write już na poziomie wirtualizatora.
21. Oprogramowanie musi zapewniać możliwość tworzenia i konfigurowania polityk niezawodnościowych, wydajnościowych i pojemnościowych przypisanych z granulacją na poziomie dysków maszyn wirtualnych tak, aby można było określić min.: liczbę serwerów fizycznych, które mogą ulec awarii jednocześnie, liczbę operacji I/O, użycie funkcji thin-provisioning, stripe.
22. Oprogramowanie musi posiadać możliwość udostępniania przestrzeni dyskowej również dla fizycznych systemów operacyjnych w oparciu o technologię iSCSI i umożliwiać zarządzanie dostępnością, pojemnością i wydajnością bez konieczności wyłączania systemów na tej przestrzeni posadowionych („w locie”).
23. Oprogramowanie musi posiadać interfejs API umożliwiający automatyzowanie wdrażania lub modyfikacji konfiguracji Systemu.
24. Oprogramowanie musi mieć możliwość włączania na żądanie i wyłączania na żądanie dostępnej w ramach funkcjonalności zaoferowanego oprogramowania dedupikacji i kompresji.
25. Oprogramowanie musi zapewniać mechanizmy optymalizacji wykorzystania przestrzeni dyskowych (ang. ereasure coding) dla RAID 5 I RAID 6 konfigurowane per dysk maszyny wirtualnej.

### SDN wirtualizacji funkcji sieciowych

Zamawiający wymaga dostarczenia oprogramowania spełniającego poniższe funkcjonalności:

1. Oprogramowanie musi oferować możliwość budowy sieci komunikacyjnych (IP) oparciu o środowiska wirtualne uruchomiona na oprogramowaniu do wirtualizacji mocy obliczeniowej
2. Oprogramowanie musi zapewniać funkcjonalność tworzenia wirtualnych sieci w sposób niezależny od topologii sieci fizycznej i używanych w obrębie tej sieci w protokołów sieciowych
3. Oprogramowanie musi posiadać funkcję rozproszonego, wirtualnego przełącznika zapewniającego przechwytywanie ruchu na poziomie karty sieciowej maszyny wirtualnej bezpośrednio w wirtualizatorze serwerów (Hypervisor), umożliwiając tworzenie logicznych segmentów sieci L2 (min. 5000 segmentów L2).
4. Oprogramowanie musi posiadać funkcję rozproszonego, wirtualnego routera pracującego w wirtualizatorze serwerów (Hypervisor), zapewniającego funkcję bramy domyślnej dla środowiska maszyn wirtualnych. Brama domyślna musi działać w trybie rozproszonym. Przełączanie pakietów w warstwie sieci L3 musi odbywać się w obrębie fizycznego serwera, bez wynoszenia ruchu do fizycznych przełączników (tj. po za środowisko wirtualizacyjne). Wymagana obsługa min. 2000 Routerów-L3 (VRF).
5. Oprogramowanie musi posiadać możliwość kreowania segmentów sieci przy użyciu technologii VXLAN lub GENEVE
6. Oprogramowanie musi zapewnić funkcjonalność łączenia (bridging) środowiska zwirtualizowanego opartego o technologię VXLAN lub GENEVE oraz niezwirtualizowanego zdefiniowanego za pomocą technologii VLAN-ów
7. Oprogramowanie musi zapewnić funkcjonalność wirtualnego routera poprzez zastosowanie protokołu BGP musi zapewniać wymianę informacji o sieciach IPv4 i IPv6 z siecią OSE.
8. Oprogramowanie musi zapewniać funkcję łączenia/bridge segmentów sieci L2 VLAN i VXLAN/GENEVE poprzez zastosowanie wirtualnej bramy/bridge
9. Oprogramowanie musi zapewniać funkcję translacji adresów IP zarówno dla ruchu wychodzącego ze środowiska wirtualnego (SNAT) jak i przychodzącego (DNAT)
10. Oprogramowanie musi posiadać funkcję serwera DHCP w celu dynamicznego nadawania adresów IP dla środowiska zwirtualizowanego
11. Oprogramowanie musi posiadać funkcjonalność API umożliwiającą automatyzowanie wdrażania lub modyfikację konfiguracji
12. Oprogramowanie musi zapewniać bezpieczeństwo transmisji danych (filtracja pakietów) na poziomie wirtualnego interfejsu sieciowego (vNIC) w wirtualizatorze, dla całości transmisji danych (włączając w to transmisję pomiędzy wirtualnymi maszynami w tym samym wirtualnym segmencie sieci) bez wynoszenia ruchu do fizycznych przełączników lub firewalli w warstwie L2-L4 modelu OSI
13. Oprogramowanie musi posiadać funkcję rozproszonego, stanowego firewall'a obsługiwanego bezpośrednio w wirtualizatorze (Hypervisor) serwerów, umożliwiający tworzenie polityk bezpieczeństwa w warstwach 2-4 modelu OSI. Możliwość definiowania reguł do warstwy 7 modelu OSI dla wybranych aplikacji w celu zapewnienia kontroli przepływu danych oraz planowania mikro-segmentacji
14. Oprogramowanie musi zapewniać możliwość tworzenia polityk bezpieczeństwa kontroli ruchu warstwie L2-L4 modelu OSI, na poziomie wirtualnego portu maszyny wirtualnej,
    1. włączając ruch pomiędzy wirtualnymi maszynami w ramach tego samego segmentu sieci VLAN i sieci programowalnej (VXLAN lub GENEVE)
    2. w obrębie (jednego i dwóch) serwerów fizycznych
    3. w obrębie usług ulokowanych w obu lokalizacjach OPD
15. Oprogramowanie musi umożliwiać wykorzystanie dynamicznych obiektów do tworzenia reguł polityk bezpieczeństwa, wymagane min.: nazwa maszyny wirtualnej, nazwa switcha wirtualnego, nazwa grupy maszyn wirtualnych, system operacyjny wirtualnej maszyny
16. Oprogramowanie musi zabezpieczać środowisko wirtualne przed nieautoryzowaną zmianą adresu IP wirtualnej maszyny, poprzez zablokowanie ruchu z i do wirtualnej maszyny po zmianie jej adresu IP
17. Oprogramowanie musi umożliwiać natywną integrację z produktami firm trzecich oferującymi rozwiązania typu antywirus/antymalware w postaci bezagentowej, tj. instalowane na wirtualizatorze serwerów, ale poza wirtualną maszyną, jak również współpracę z narzędziami do analizy zagrożeń typu APT, AV, IPS, NGFW. Musi zapewniać możliwość podejmowania, kreowania automatycznej akcji polegającej na wyizolowania, blokowaniu, ograniczeniu komunikacji z i do podejrzanej maszyny wirtualnej na poziomie wirtulanego interfejsu sieciowego (vNIC) w wirtualizatorze
18. Oprogramowanie musi umożliwiać integrację z produktami firm trzecich oferującymi rozwiązania typu Next Generation Firewall, poprzez przekierowywanie zdefiniowanego ruch sieciowego w warstwach 2-4 modelu OSI do głębokiej analizy do warstwy 7 modelu OSI
19. Oprogramowanie musi zapewniać mechanizm wspomagający planowanie tworzenia grup oraz polityk bezpieczeństwa
20. Oprogramowanie musi zapewniać rozwiązanie typu Firewall tożsamościowa który musi zapewniać integrację z Active Directory z obsługą selektywnej kontroli ruchu w zależności od użytkownika
21. Oprogramowanie musi posiadać możliwość kreowania segmentów sieci rozciągając ich zasięg do drugiej lokalizacji stosującej w sieci podkładowej protokół IP, umożliwiając rozciąganie segmentów sieci L2 i L3 między OPD poprzez sieć IP sieci OSE
22. Oprogramowanie musi umożliwiać wykonywanie automatycznego procesu izolowania zagrożeń w centrum danych, poprzez zastosowanie oprogramowania firm trzecich do analizy zagrożeń typu APT, AV, IPS, NGFW musi istnieć możliwość automatycznej akcji obejmującej wyizolowania komunikacji z i do podejrzanej maszyny VM
23. Oprogramowanie musi zapewniać wydajność dla kontroli ruchu pomiędzy maszynami wirtualnymi VM-VM w warstwie komunikacyjnej L2-L4 w obrębie każdego hosta do poziomu 9Gbps
24. Oprogramowanie musi zapewniać wydajność w komunikacji między siecią podkładową, a siecią nadkładową do poziomu 9Gbps dla każdego punktu
25. Oprogramowanie musi być połączony z siecią OSE poprzez zastosowanie min. 2 połączeń 10Gbps i segmentów L2.
26. Oprogramowanie musi zapewniać wymianę ruchu IP z blokiem CWB OSE, przy zastosowaniu VLANów
27. Oprogramowanie musi wspierać protokół BFD. Umożliwiając szybkie wykrywanie awarii na połączeniu: sieć OSE z siecią SDN. Musi istnieć możliwość skonfigurowania czasu nie dłuższego jak 3 sekundy na wykrycie awarii i poinformowania warstwy kontrolnej SDN i sieci OSE o awarii ścieżki i konieczności zastosowania ścieżki zapasowej
28. Oprogramowanie musi umożliwiać analizę przepływów sieciowych w warstwie L2-L4 modelu OSI dla komunikacji pomiędzy: VM-VM, Kontener - Kontener na jednym i dwóch serwerach, eksport danych telemetrycznych musi odbywać się za pomocą protokołu IPFIX lub NetFlow. Wymagana możliwość zdefiniowania progu dokładności pomiarów dla zbieranych danych z przedziału od 1% do 100%
29. Oprogramowanie musi wspierać środowiska kontenerowe, w tym Kuberneters (K8s) lub Red Hat OpenShift. W zakresie segmentów sieci L2, kontroli ruchu w komunikacji między kontenerami w jednym segmencie L2 na jednym i dwóch serwerach i monitorowania ruchu IP w segmencie L2 modelu OSI.
30. Oprogramowanie musi umożliwiać konfigurację wydzielonych środowisk sieciowych tak zwanych MultiTenant typu Lab, Dev, Produkcja. Wymagane min. 20. Środowiska mogą posiadać tą samą adresację IP, tak zwane lustrzane kopie usług (przedprodukcja i produkcja).
31. Oprogramowanie musi oferować możliwość budowy sieci komunikacyjnych (IP) w oparciu o środowiska wirtualne zbudowane na bazie minimum dwóch wirtualizatorów mocy obliczeniowej.
32. Oprogramowanie musi zapewniać funkcjonalność tworzenia wirtualnych sieci w sposób niezależny od topologii sieci fizycznej i używanych w obrębie tej sieci w protokołów sieciowych
33. Oprogramowanie musi realizować usługi wirtualnych sieci musi być zarządzane przez narzędzie do zarządzania warstwą wirtualizacji SDN.
34. Wykreowane sieci wirtualne w oprogramowaniu SDN muszą widoczne i możliwe do przypisania do maszyn wirtualnych platformie zarządzającego wirtualizacją mocy obliczeniowej serwerów
35. Oprogramowanie musi zapewniać wsparcie dla wykorzystania plików danych JSON oraz XML
36. Oprogramowanie musi zapewnić bezpieczeństwo transmisji danych (filtracja pakietów) na poziomie wirtualnego interfejsu sieciowego (vNIC) w wirtualizatorze, dla całości transmisji danych (włączając w to transmisję pomiędzy wirtualnymi maszynami w tym samym wirtualnym segmencie sieci) bez wynoszenia ruchu do fizycznych przełączników lub firewalli na zewnątrz hypervisora
37. Oprogramowanie musi posiadać funkcję rozproszonego, stanowego firewall'a realizowanego bezpośrednio w serwerze umożliwiającego tworzenie polityk bezpieczeństwa w warstwach 2, 3 i 4 modelu sieciowego OSI. Nie dopuszcza się stosowania filtracji ruchu sieciowego typu "reflexive".
38. Oprogramowanie musi zapewniać możliwość tworzenia reguł firewall’a w trybie bezstanowym (ang. stateless) dla różnych grup wirtualnych serwerów
39. Oprogramowanie musi zapewniać możliwość tworzenia granularnych polityk bezpieczeństwa na poziomie wirtualnego portu maszyny wirtualnej, włączając ruch pomiędzy wirtualnymi maszynami w ramach tego samego segmentu sieci i na tym samym fizycznym serwerze (hoście)
40. Oprogramowanie musi zapewniać możliwość tworzenia granularnych polityk bezpieczeństwa dostępnych do wykorzystania w celu ochrony maszyn wirtualnych oraz serwerów fizycznych (ang. Bare metal) działających pod kontrolą systemu operacyjnego Linux ( Red Hat Enterprise Linux, min. 7.6 ) oraz Microsoft Windows 2016
41. Oprogramowanie do tworzenia reguł polityk bezpieczeństwa, musi umożliwiać wykorzystanie, oprócz parametrów takich jak adres IP, porty i protokoły, dodatkowych obiektów, m in.: nazwa maszyny wirtualnej, nazwa switcha wirtualnego, nazwa grupy maszyn wirtualnych, system operacyjny wirtualnej maszyny
42. Oprogramowanie musi zabezpieczać środowisko wirtualne przed nieautoryzowaną zmianą adresu IP wirtualnej maszyny, poprzez zablokowanie ruchu z i do tej wirtualnej maszyny po zmianie jej adresu IP w sposób nieautoryzowany
43. Oprogramowanie musi posiadać możliwość terminowania tuneli IPSec site-to-site z uwierzytelnieniem za pomocą współdzielonego klucza ( pre shared key ) lub certyfikatu
44. Oprogramowanie musi umożliwiać natywną integrację z produktami firm trzecich oferującymi rozwiązania klasy antywirus/antymalware w postaci bezagentowej. Poprzez bezagentowość Zamawiający rozumie instalacje na poziomie wirtualizatora (hypervisora) serwerów, bez ingerencji w maszynę wirtualną
45. Oprogramowanie musi umożliwiać natywną integrację z minimum dwoma produktami firm trzecich oferującymi rozwiązania typu Next Generation Firewall w warstwie 7 modelu ISO OSI, w celu dodatkowej filtracji i inspekcji ruchu
46. Oprogramowanie musi umożliwiać przekierowanie wybranego ruchu warstwy 2 modelu ISO OSI do rozwiązania firm trzecich z obszaru bezpieczeństwa
47. Oprogramowanie musi posiadać możliwość tworzenia reguł bezpieczeństwa uwzględniających nazwy użytkowników, poprzez integrację z Microsoft Active Directory z obsługą selektywnej synchronizacji
48. Oprogramowanie musi zapewnić funkcjonalność rozkładania/równoważenia ruchu (ang. load balancing) działającą od warstwy 4 do warstwy 7 modelu ISO OSI. Funkcjonalność musi zapewniać następujące mechanizmy utrzymywania sesji (ang. session persistent), m in.: adres źródłowy, cookie, SSL ID oraz SessionID
    1. W ramach inspekcji warstwy 7 modelu ISO OSI funkcjonalność równoważenia ruchu (ang. Load Balancer) musi oferować funkcję blokowania i modyfikacji URL
    2. Rozwiązanie równoważenia ruchu (ang. Load Balancer) w zaoferowanym oprogramowaniu musi posiadać możliwość wstrzykiwania w nagłówek znacznika XFF (X-Fowarder-For)
    3. Funkcja wirtualnego równoważenia ruchu (ang. Load Balancing) musi być zarządzana oraz instalowana w ramach jednego interfejsu graficznego (pojedynczej konsoli) w ramach zaoferowanego oprogramowania
    4. Musi pozwalać na realizację równoważenia obciążenia (ang. Load balancing) w formie scentralizowanej, to znaczy poprzez instalację i procesowanie ruchu na dedykowanym komponencie - na serwerze fizycznym (bare metal) lub maszynie wirtualnej
49. Oprogramowanie musi posiadać funkcjonalność identyfikacji aplikacji, np. MySQL, HTTP, DNS, DHCP, Active Directory, TLS, itp. na poziomie sieciowym modelu ISO OSI w warstwach 5, 6 i 7, a następnie móc wykorzystać wynik identyfikacji w rozproszonym, wewnętrznym firewall w celu kontroli dostępu nie tylko na poziomie adresów IP oraz portów, ale również w połączeniu adresów IP, portów oraz zidentyfikowanej aplikacji

### Skalowanie Klastrów obliczeniowych Komponent HCI

Zamawiający wymaga spełnienia poniższych wymagań:

1. Wymagania określone w tabeli są wymaganiami minimalnymi i należy je traktować jako pojemność infrastruktury sprzętowej.
2. Aby zmaksymalizować możliwości przenoszenia mocy i zminimalizować koszty serwisowania, klastry muszą być zbudowane w oparciu o nie więcej niż:
   1. trzy modele serwerów jednego producenta,
   2. dwa typy procesorów jednego producenta,
   3. dwa typy kości pamięci jednego producenta,
   4. sześć typów dysków twardych (typu HDD, SSD, NVMe).
3. Wymagana jest nadmiarowość N+1 niezależnie dla serwerów z procesorami o częstotliwości taktowania 2Ghz oraz 3Ghz.
4. Tabela prezentuje minimalne obligatoryjne parametry infrastruktury w centralnych węzłach OPD1 i OPD2
   1. vCPU – oznacza fizyczne rdzenie procesora
   2. vRAM - oznacza fizyczną pamięć RAM
   3. SSD, NVMe - oznacza fizyczną pamięć dyskową
      1. Wymagane jest zastosowanie jednej technologii typu SSD lub NVMe jako dyski Cache, i stosowanie w ODP1 i OPD2
      2. Wymagane jest zastosowanie jednej technologii typu SSD lub NVMe jako dyski Capacity i stosowanie w ODP1 i OPD2
      3. Nie jest dozwolone mieszanie różnej pojemności dysków Capacity w serwerze HCI
      4. Nie jest dozwolone mieszanie różnej pojemności dysków Cache w serwerze HCI
      5. Zastosowane dyski Capacity muszą być jednego producenta
      6. Zastosowane dyski Cache muszą być jednego producenta
   4. wymagane są minimum 3 klastry obliczeniowe
      1. zarządzanie i monitorowanie dostarczonego środowiska
      2. produkcyjne systemy Zamawiającego
      3. przedprodukcyjne systemy Zamawiającego
      4. Klastry urządzeń mogą składać się z serwerów 1U i 2U, wyposażone w jeden lub dwoma procesory
   5. wymagany jest minimum jeden klaster zbudowany w oparciu o wyłącznie pamięć NVMe dedykowany do wymagających systemów.
   6. wymagane jest środowisko testowe w lokalizacji ODP1 umożliwiającego testowanie usług i cykliczne odtwarzanie systemów z kopii zapasowych

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Identyfikator  klastra | Suma serwerów  1CPU /("lub") 2CPU | Suma fizyczne rdzenie Procesora | Fizyczne rdzenie procesora o zegarze 3Ghz | Ilość vRAM (GB) | Przestrzeń dyskowa  Capacity  **SSD lub NVMe** (TB) | Przestrzeń  dyskowa  Cache **SSD lub NVMe** (TB) | Liczba serwerów tylko **NVMe (**powierzchnia **Capacity TB)** |
| OPD1 Warszawa | 52/26 | 1240 | 144 | 12 | 1572 | 46 | 4 (72) |
| OPD2 Poznań | 52/26 | 1240 | 144 | 12 | 1572 | 46 | 4 (72) |
| OPD1 Warszawa „środowisko testowe” | 10/5 | 130 | 72 | 3 | 180 | 6 | 0 |

1. Tabela prezentuje minimalne obligatoryjne parametry infrastruktury w regionalnych węzłach, szesnastu ROPD
   1. vCPU – oznacza fizyczne rdzenie procesora
   2. vRAM - oznacza fizyczną pamięć RAM
   3. HDD, SSD, NVMe - oznacza fizyczną pamięć dyskową
      1. Wymagane jest zastosowanie jednej technologii typu SSD lub NVMe jako dyski Cache i stosowanie we wszystkich szesnastu lokalizacjach ROPD
      2. Wymagane jest zastosowanie jednej technologii typu HDD/SSD/NVMe jako dyski Capacity i stosowanie we wszystkich szesnastu lokalizacjach ROPD
      3. Nie jest dozwolone mieszanie różnej pojemności dysków Capacity w serwerze HCI
      4. Nie jest dozwolone mieszanie różnej pojemności dysków Cache w serwerze HCI
      5. Zastosowane dyski Capacity muszą być jednego producenta
      6. Zastosowane dyski Cache muszą być jednego producenta
      7. Podane w tabeli wartości dla „Pojemność Netto pamięci masowej **HDD /SSD /NVMe** (TB)” oznacza dostępną sumaryczną pojemność użytkową w lokalizacji, możliwą do przypisania dla wirtualnych maszyn, wymagana przestrzeń musi posiadać min. jedną kopię danych, a dane muszą znajdować się na min. dwóch serwerach
      8. Klastry urządzeń mogą składać się z serwerów 1U i 2U, wyposażone w jeden lub dwoma procesory
         1. nie dozwolone jest stosowanie w jednej lokalizacji serwerów jedno i dwu procesorowych taktowanych tym samym zegarem.
   4. wymagany jest minimum 1 klaster obliczeniowy
      1. zapewniający zasoby dla systemu SWG Zamawiającego w oparciu o procesory min. 2Ghz i 3Ghz
      2. Klaster urządzeń nie może składać się z więcej jak 16 urządzeń

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Identyfikator klastra | Suma serwerów 1CPU /("lub") 2CPU | Suma fizyczne rdzenie Procesora | Liczba serwerów z  1CPU /("lub") 2CPU  **z zegarem 3GHz** | Fizyczne rdzenie Procesora 3GHz | Ilość vRAM (GB) | Pojemność **Netto** pamięci Capacity masowej **HDD /SSD /NVMe** (TB) | Pojemność pamięci cache **SSD/NVMe** (GB) |
| MAZOWIECKIE | 33/17 | 528 | 28/12 | 352 | 4500 | 80 | 9900 |
| ŚLĄSKIE | 11/6 | 176 | 3/2 | 80 | 1600 | 8 | 3300 |
| MAŁOPOLSKIE | 8/4 | 128 | 4/2 | 64 | 1100 | 7 | 2400 |
| WIELKOPOLSKIE | 22/11 | 336 | 18/9 | 272 | 3500 | 80 | 6300 |
| PODKARPACKIE | 7/4 | 104 | 4/2 | 56 | 900 | 7 | 1950 |
| LUBELSKIE | 7/4 | 104 | 4/2 | 56 | 900 | 7 | 1950 |
| DOLNOŚLĄSKIE | 7/4 | 104 | 4/2 | 56 | 900 | 7 | 1950 |
| ŁÓDZKIE | 7/4 | 104 | 4/2 | 56 | 900 | 7 | 1950 |
| POMORSKIE | 7/4 | 104 | 4/2 | 56 | 900 | 7 | 1950 |
| KUJAWSKO-POMORSKIE | 7/4 | 104 | 4/2 | 56 | 900 | 7 | 1950 |
| ZACHODNIOPOMORSKIE | 7/4 | 104 | 4/2 | 56 | 900 | 7 | 1950 |
| WARMIŃSKO-MAZURSKIE | 5/4 | 80 | 3/2 | 48 | 700 | 5 | 1500 |
| ŚWIĘTOKRZYSKIE | 5/4 | 80 | 3/2 | 48 | 700 | 5 | 1500 |
| PODLASKIE | 5/4 | 80 | 3/2 | 48 | 700 | 5 | 1500 |
| OPOLSKIE | 5/4 | 80 | 3/2 | 48 | 700 | 5 | 1500 |
| LUBUSKIE | 5/4 | 80 | 3/2 | 48 | 700 | 5 | 1500 |

### Moduł orkiestracji, zarządzania i administracji

Zamawiający wymaga dostarczenia oprogramowania spełniającego poniższe funkcjonalności:

1. Oprogramowanie musi uzyskiwać informacje na temat wydajności środowiska wirtualnego pod kątem zarządzania pojemnością
2. Oprogramowanie musi za pomocą wbudowanych inteligentnych algorytmów przewidywać trendy związane z pojemnością środowiska wirtualnego w centralnych lokalizacjach OPD1 i OPD2
   1. Oprogramowanie musi posiadać funkcjonalność dającą możliwość analizy środowiska wirtualnego pod kątem optymalizacji wykorzystania zasobów (CPU, RAM, zasoby dyskowe)
   2. Oprogramowanie musi mieć możliwość tworzenia unikalnego zbioru obiektów korespondujących funkcjami z obiektami Datacenter, tzn. musi być możliwe grupowanie obiektów w logiczne zbiory, dla których będzie istniała możliwość informowania o alertach, pojemności, ryzykach zgromadzonych w zbiorze obiektów.
   3. Oprogramowanie musi mieć możliwość tworzenia unikalnego/dedykowanego profilu pojemności, tzn. będzie możliwe grupowanie obiektów z Data Center w logiczne zbiory dla których będzie istniała możliwość informowania o alertach, pojemności, ryzykach zgromadzonych w zbiorze obiektów.
   4. Oprogramowanie musi mieć funkcjonalność tworzenia scenariuszy predykcyjnego obliczania pojemności 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 musi odnosić się zarówno do średniego obciążenia środowiska, jak również do tzw. skoków obciążenia
3. Oprogramowanie musi monitorować infrastrukturę opartą o rozwiązania Compute i SDS
   1. obrębie monitorowania, będzie posiadało rozwiązanie generowania alertów na podstawie korelacji wykrytych w środowisku wirtualnym anomalii i symptomów.
4. Oprogramowanie musi posiadać funkcjonalność dostarczania informacji na temat rekomendowanych przez producenta środowiska działań, mających na celu prawidłowe działanie środowiska
5. Oprogramowanie musi posiadać wbudowane komponenty integracyjne obsługujące zewnętrzne kolektory logów i zdarzeń
6. Oprogramowanie musi posiadać funkcjonalność monitorowania i alertowania na temat zgodności serwerów z najlepszymi praktykami bezpieczeństwa oraz DISA (Defence Information Systems Agency), ISO, CIS (center of internet security), PCI (Payment Card Industry).
7. Oprogramowanie musi posiadać bazę wiedzy eksperckiej, która będzie używana przez administratorów, jako źródło dobrych praktyk, sugestii, opisu typowych problemów i błędów związanych ze środowiskiem zwirtualizowanym
8. Oprogramowanie musi wizualizować w trybie online obciążenie środowiska wirtualnego
9. Oprogramowanie musi posiadać funkcjonalność graficznej prezentacji wyników (ang. dashboard)
10. Oprogramowanie musi posiadać funkcjonalność aktywnych map graficznych ukazujących elementy lub całe środowisko wirtualne bez konieczności korzystania z usługi wsparcia technicznego producenta do ich dodatkowego wytwarzania podczas używania oprogramowania
11. Oprogramowanie musi dokonywać automatycznej predykcji wykorzystania zasobów maszyn fizycznych na podstawie analiz zebranych danych oraz planów uruchomienia kolejnych serwerów wirtualnych
12. Oprogramowanie musi umożliwiać przeglądanie linii trendu monitorowanych parametrów
13. Oprogramowanie musi umożliwiać tworzenie raportów pojemnościowych dla monitorowanego środowiska, zarówno dla urządzeń wirtualnych jak i fizycznych, związanych z wirtualizatorem opartym o rozwiązanie VMware vSphere oraz fizycznymi zasobami dyskowymi poza środowiskiem wirtualnym
14. Oprogramowanie musi umożliwiać monitorowanie środowisk w czasie rzeczywistym (przeglądane informacje powinny ukazywać się w trybie rzeczywistym – dopuszczane jest maksymalne opóźnienie nie większe niż 5 minut)
15. Oprogramowanie musi pozyskiwać oraz prezentować, w formie wykresów oraz tabelaryczno-tekstowej, zbiorczo oraz osobno, dla każdego systemu operacyjnego, aktualne i historyczne dane dotyczące utylizacji CPU, RAM, zasobów dyskowych oraz interfejsów sieciowych
16. Oprogramowanie musi umożliwiać przeglądanie wszystkich zbieranych statystyk w okresie 6 miesięcy w postaci wykresów
17. Oprogramowanie musi umożliwiać szczegółowe monitorowanie komponentów serwerów fizycznych (CPU, Ethernet, RAM, zasoby dyskowe)
18. Oprogramowanie musi umożliwiać definiowanie progów wydajności i pojemności w celu identyfikacji przypadków wąskich gardeł
19. Oprogramowanie musi posiadać funkcjonalność zmiany parametrów maszyn wirtualnych, minimum CPU i RAM, za pomocą wygenerowanego zadania. Dodatkowo, wymagana jest funkcjonalność odkładania w czasie w/w zadania, po wygenerowaniu określonym czasie.
20. Oprogramowanie musi posiadać możliwość kasowania, wykonywania kopii migawkowych (ang. snapshot), włączania oraz wyłączania maszyn wirtualnych posadowionych na monitorowanym środowisku wirtualnym
21. Oprogramowanie musi automatycznie przeszukiwać i analizować zebrane dane w celu wynajdywania nadmiarowości oraz niedoborów przyznanych zasobów (CPU, RAM, HDD) w monitorowanym środowisku
22. Oprogramowanie musi posiadać funkcjonalność automatycznego alarmowania w sytuacji nietypowych (system monitoringu obserwuje i analizuje zachowanie platformy wirtualnej, na tej podstawie podnosi alarmy o minimum nie normalnym w tym dniu zwiększonym obciążeniu elementu platformy wirtualnej)
23. Oprogramowanie musi posiadać możliwość dowolnego przypisywania powiadamiania o alertach w środowisku dla różnych grup odbiorców (także z użyciem alertów stworzonych we własnym zakresie przez użytkownika)
24. Oprogramowanie musi pozwalać na odczyt wyświetlanych alarmów dotyczących monitorowanego środowiska wirtualnego wraz z powiązanymi z nimi poradami eksperckim
25. Oprogramowanie musi umożliwiać definiowanie alertów związanych z: zarządzaniem pojemnością, zarządzaniem wydajnością, anomaliami w środowisku, zarządzaniu dostępnością dla monitorowanego środowiska
26. Oprogramowanie musi mieć posiadać funkcjonalność przypisania alertu do administratora/operatora rozwiązującego problem
27. Oprogramowanie musi mieć możliwość realizacji funkcji półautomatycznego równoważenia obciążenia serwerów fizycznych w obrębie klastra wirtualizacyjnego
28. Oprogramowanie musi mieć możliwość generowania gotowych, predefiniowanych raportów o stanie środowiska monitorowanego
29. Oprogramowanie musi posiadać funkcjonalność gotowego pulpitu kierowniczego (ang. dashboard) za pomocą którego administrator będzie posiadał gotowe trzy kolumny z następującymi informacjami:
    1. Zdarzenia jakie wystąpiły w zadanym okresie czasu dla analizowanego problemu, min. dla: wirtualnych maszyn, sieci wirtualnej, wirtualnej przestrzeni dyskowej
    2. Anomalie, jakie wystąpiły w zadanym okresie czasu dla analizowanego problemu
    3. Zmiany w konfiguracji monitorowanej infrastruktury jakie wystąpiły w zadanym okresie czasu dla analizowanego problemu
    4. Analiza danych ukazująca powyższe wyniki prezentowane w dashboard musi odbywać się automatycznie poprzez mechanizmy uczenia się maszynowego zaoferowanego oprogramowania do monitorowania na podstawie zakresu czasowego definiowanego przez użytkownika tego Dashboard. Dodatkowo użytkownik musi mieć możliwość definiowania, dla którego obiektu, np. wybranej maszyny wirtualnej należy przeprowadzić analizę, a następnie wyświetlić jej wyniki.
30. Oprogramowanie musi posiadać możliwość zastosowania dodatkowych adapterów umożliwiających integrację z systemami firm trzecich monitorującymi infrastrukturę
31. Oprogramowanie musi posiadać możliwość zastosowania dodatkowych paczek monitorujących dla rozwiązań firm trzecich
32. Oprogramowanie musi wykrywać usługi uruchomione na monitorowanych maszynach wirtualnych, a następnie budować relacje lub zależności między usługami z różnych maszyn wirtualnych na podstawie komunikacja sieciowej
33. Oprogramowanie musi posiadać możliwość, po uruchomieniu alarmu, wykonywać na podstawie tego alarmu, automatyczne działania dotyczących akcji naprawczych
34. Oprogramowanie musi posiadać funkcjonalność monitorowania aplikacji, serwerów aplikacyjnych oraz baz danych firm trzecich, m.in. baz danych Oracle DB, Microsoft SQL, MySQL, Oracle Weblogic, IBM WebSphere za pomocą specjalnie przygotowanych paczek (ang. management packs) firm trzecich
35. Oprogramowanie musi mieć możliwość monitorowania zmian na poziomie systemów operacyjnych w tym konfiguracji tych systemów oraz procesu zarządzania aktualizacjami (ang. patch management)
36. Oprogramowanie musi mieć gotowe paczki (ang. management packs) do monitorowania platform typu Multi-Cloud, tj. OCHK, AWS (Amazon Web Services) , Microsoft Azure, OpenStack i rozwiązań kontenerowych, tj. Kubernetes
37. Interfejs graficzny musi być dostępny bezpiecznie poprzez przeglądarkę internetową zabezpieczony SSL
38. Oprogramowanie musi posiadać zestaw wbudowanych procesów/czynności automatyzacji dostarczania usług wraz z możliwością ich edycji, zmiany konfiguracji i tworzenia nowych „kroków” w procesie cyklu życia konkretnej usługi
39. Oprogramowanie musi informować o statusie usługi w czasie rzeczywistym np. (usługa zaakceptowana, zakolejkowana, odrzucona, w trakcie akceptacji itp.) dodatkowo rozwiązanie musi mieć możliwość wysłania informacji poprzez pocztę elektroniczną o zmianie statusu usługi
40. Oprogramowanie musi umożliwiać provisioning do dostawców chmur publicznych: OpenStack, OVH, AWS, Azure, OCHK
41. Oprogramowanie musi realizować model: "Projektuj usługę raz, wdrażaj gdziekolwiek"
42. Oprogramowanie musi umożliwiać rezerwację zasobów fizycznych dla wybranych grup użytkowników, oraz pełną kontrolę tych zasobów w obrębie wskazanej grupy użytkowników
43. Oprogramowanie musi mieć możliwość tworzenia wielu logicznych, izolowanych od siebie grup maszyn wirtualnych, określania dla nich zasobów fizycznych, grup użytkowników, wzorców usług a także procesów tworzenia, zarzadzania cyklem życia usług
44. Oprogramowanie musi umożliwiać tworzenie nowych usług wraz z określeniem ilości i rodzaju zasobów dostępnych dla danej usługi zarówno na etapie tworzenia jak i późniejszej rekonfiguracji danej usługi
45. Oprogramowanie musi posiadać jedno narzędzie do projektowania usługi opartej na OS, aplikacjach, usług sieciowych tj.: Load Balancing, Routing, Switching oraz tworzenia reguł bezpieczeństwa w locie podczas provisioningu - w sieciowym aspekcie rozwiązanie musi mieć wsparcie dla mikrosegmentacji tj. filtrowania ruchu pomiędzy dowolnymi maszynami wirtualnymi również w obrębie tej samej sieci
46. Oprogramowanie musi posiadać interfejs typu „drag-drop” przeznaczony do tworzenia dowolnej aplikacji na podstawie utworzonych wcześniej komponentów, aplikacji, systemów, sieci i polityk bezpieczeństwa oraz innych skryptów pomocnych w automatyzacji
47. Oprogramowanie musi umożliwiać graficzną edycję przebiegu procesu realizacji usług, definiowanie poszczególnych kroków oraz ich danych wejściowych i wyjściowych. Przebiegi procesów mogą być sekwencyjne lub składać się z wielu sekwencji zadań realizowanych równocześnie, musi istnieć możliwość testowania zdefiniowanych procesów realizacji usług przy użyciu debugger-a, który pozwala analizować postęp procesu krok po kroku ze śledzeniem przekazywanych danych
48. Rozwiązanie musi umożliwiać export/import zdefiniowanych procesów realizacji usług do/z pliku
49. Oprogramowanie musi umożliwiać integrację z Active Directory
50. Oprogramowanie musi posiadać możliwość granularnego zarządzania uprawnieniami dla poszczególnych użytkowników w zależności od pełnionej roli, opartego na rolach: np.: Tenant Admin, Service Architect, Network Architect, Application Architect
51. Oprogramowanie musi służące do automatyzacji musi standaryzować wdrażanie usług IT oraz eliminować w ten sposób błędy czynnika ludzkiego
52. Oprogramowanie musi dostarczać mechanizmy monitorowania statusów zdarzeń, notyfikacji o tych zdarzeniach, umożliwiać śledzenie i kontrolę zmian w konfiguracji wszystkich usług, za pomocą min. portalu Self-Service i powiadomień e-mail
53. Oprogramowanie musi udostępniać funkcjonalność zarządzania poprzez ustandaryzowany interfejs tj. API
54. Oprogramowanie musi wspierać możliwość wcześniejszego i automatycznego przetestowania wpływu jej aktualizacji na pozostałe podłączone do niej komponenty klastra oraz uruchomione na nim funkcjonalności. Musi również wspierać proces aktualizacji całego klastra poprzez automatyczne raportowanie kolejności aktualizacji podłączonych do niej komponentów i rekomendowanej ich wersji
55. Oprogramowanie musi zapewniać konsolę graficzną w przeglądarce internetowej, za pomocą której istnieje możliwość prowadzenie procesu automatycznego instalowania i konfigurowania następujących modułów:
    1. Wirtualizacja mocy obliczeniowej i pamięci
    2. Wirtualizacji funkcji sieciowych
56. Oprogramowanie musi zostać uruchomione w obu OPD jednocześnie, pracując w modelu nadmiarowym, proces przywrócenia funkcjonalności usługi w przypadku awarii OPD nie może przekroczyć 15 minut.

### Monitorowanie i eksploatacja środowiska

Zamawiający wymaga dostarczenia oprogramowania spełniającego poniższe funkcjonalności:

1. Oprogramowanie musi zapewniać możliwość centralnego gromadzenia i analizy wszystkich logów z urządzeń fizycznych wykorzystujących technologię „Syslog”
2. Oprogramowanie musi umożliwiać personalizację i wizualizację logów w postaci wykresów minimum: liniowych, kołowych
3. Oprogramowanie musi być zgodne z dostarczoną warstwą wirtualizacji i zarządzania mocą obliczeniową i obejmować nadzorem wymienione środowisko,
4. Oprogramowanie musi zapewniać monitorowanie urządzeń typu „Real Time”
5. Oprogramowanie musi posiadać wbudowaną bazę wiedzy dotycząca logów oraz zdarzeń dla dostarczonej platformy wirtualizacyjnej
6. Oprogramowanie musi posiadać możliwość udostępniania raportów za pomocą URL kierującego do systemu logowania wysyłanego do odbiorcy
7. Oprogramowanie musi umożliwiać korelację zdarzeń w infrastrukturze fizycznej i wirtualnej oraz ich graficzną prezentację
8. Oprogramowanie musi posiadać możliwość personalizacji interfejsu graficznego w zależności od użytkownika/operatora
9. Oprogramowanie musi umożliwiać przeszukiwanie logów w oparciu o zdefiniowane przez użytkownika kryteria
10. Oprogramowanie musi posiadać funkcjonalność implementacji dedykowanych modułów do analizy logów innych urządzeń fizycznych np. macierzy dyskowych, przełączników LAN, itp., tak aby analiza i korelacja wszystkich wiadomości systemowych mogła odbywać się z jednej konsoli zarządzającej
11. Oprogramowanie musi posiadać mechanizmy efektywnej analizy wszystkich rodzajów logów, takich jak np. logi aplikacji, logi sieciowe, pliki konfiguracyjne, informacje, dane wydajnościowe, zrzuty awaryjne itp., a także logów nieustrukturyzowanych
12. Oprogramowanie musi umożliwiać definiowanie struktury dla logów nieustrukturyzowanych
13. W zaoferowanym oprogramowaniu uprawnienia do interfejsu prezentacji i analizy logów muszą dopuszczać rozłączność z uprawnieniami do infrastruktury, z której zbierane są logi
14. Oprogramowanie musi umożliwiać generowanie i eksportowanie dowolnych raportów związanych z zarejestrowanymi zdarzeniami i logami
15. Oprogramowanie musi zapewniać możliwość stworzenie klastra składającego się co najmniej 4 węzłów, z którego każdy ma wydajność 15 000 EPS (ang. Events Per Second), co sumarycznie daje 60 000 EPS
16. Oprogramowanie musi posiadać możliwość logowania zdarzeń z platformy Kubernetes dla zaoferowanego oprogramowania do wirtualizacji
17. Oprogramowanie musi mieć możliwość określania czasu retencji danych, tzn. Administrator w konsoli graficznej do zarządzania platformą do zbierania i korelacji logów musi mieć możliwość określenia czasu po jakim zebrane logi będą archiwizowane (eksportowane) na zewnętrznej macierzy dyskowej po protokole NFS. Dodatkowo wymaga się aby retencja mogła być ustawiana granularnie, tj. np. inny czas retencji dla logów z urządzeń klasy firewall a inny czas retencji dla logów z wirtualizatora.
18. Oprogramowanie musi mieć możliwość analizowania przepływów sieciowych (w tym IPFIX) w warstwie sieciowej wirtualizacji opartej o rozwiązanie SDN
19. Oprogramowanie musi mieć możliwość tworzenia raportów przepływów z informacją uwzględniającą adresy IP oraz porty TCP/UDP dla środowiska wirtualnego. Poprzez raporty przepływów Zamawiający rozumie informację o ruchu sieciowym z konkretnej maszyny wirtualnej do innej konkretnej maszyny wirtualnej
20. Oprogramowanie musi mieć możliwość generowania rekomendacji dla reguł serwerów klasy ściana ogniowa na bazie zebranych wcześniej informacji o przepływach
21. Oprogramowanie musi mieć możliwość wizualizacji (przedstawienia w postaci graficznej) ścieżki logicznej i przejść w relacji maszyna wirtualna do maszyny wirtualnej, wskazania komponentów sieciowych w topologii logicznej i fizycznej uwzględniając przełączniki, routery, firewall’e oraz połączenia między nimi z uwzględnieniem komponentów wirtualnych (minimum host i maszyna wirtualna)
22. Oprogramowanie musi mieć możliwość wizualizacji w formie graficznej przepływów pomiędzy minimum sieciami wirtualnymi, podsieciami, aplikacjami oraz grupami bezpieczeństwa
23. Oprogramowanie musi mieć możliwość informowania o maskowanych regułach firewalla, czyli regułach, które nie są wykorzystywane ze względu na reguły, które w ciągu analizy ruchu znajdują się w kolejce analizy je poprzedzają
24. Oprogramowanie musi mieć możliwość automatycznego wykrycia aplikacji działających w sieci klienta oraz wizualizacji zależności zarówno, pomiędzy maszynami wirtualnymi należącymi do tej aplikacji jak i ruchem zewnętrznym, wychodzącym i wchodzącym do maszyn wirtualnych odpowiedzialnych za tę aplikacje
25. Oprogramowanie musi posiadać funkcjonalność API umożliwiającą automatyzowanie wdrażania lub modyfikację konfiguracji
26. Oprogramowanie musi posiadać główną konsole do automatycznej instalacji i konfiguracji oprogramowania do wirtualizacji serwerów fizycznych, macierzy dyskowej typu SDS (ang. software defined storage) na serwerach, wirtualizacji sieci typu SDN (ang. software defined network) wraz z mechanizmami bezpieczeństwa.
27. Oprogramowanie musi być w stanie instalować i aktualizować powyższe komponenty oprogramowania (pkt. od 6.3.2 do 6.3.4).
28. Oprogramowanie musi posiadać narzędzia automatyzujące i upraszczające proces wdrażania stosu oprogramowania infrastrukturalnego do wirtualizacji serwerów x86, wirtualizacji sieci oraz tworzenia macierzy dyskowej typu SDS poprzez zautomatyzowaną instalację oprogramowania, tworzenie klastrów obliczeniowych (w tym klastry obliczeniowe dla środowisk typu mikro usług - klastry Kubernetes)
29. Oprogramowanie musi posiadać mechanizmy aktualizacji całego oprogramowania zainstalowanego w oparciu definiowane harmonogramy i zakresy tych aktualizacji
30. Oprogramowanie musi posiadać, na oficjalnej stronie producenta listę wspieranych i certyfikowanych konfiguracji serwerów sprzętowych. Wymagane jest wsparcie dla min. pięciu niezależnych producentów sprzętu serwerowego x86
31. Oprogramowanie musi posiadać funkcjonalność analizy i monitorowania przepływu danych dla aplikacji
    1. możliwość monitorowania przepływu danych (network flow) pomiędzy usługami opartymi o maszyny wirtualne
    2. możliwość wskazania usług, które charakteryzują się najwyższym poziomem generowanego ruchu (top talkers) w oparciu o co najmniej:
       1. ilość przepływów
       2. wolumen ruchu
    3. identyfikacja sytuacji nietypowych, statystycznie odbiegających od standardowego wzorca pracy (tzw. outliers), np. przepływy o nietypowo dużym lub małym wolumenie danych w ramach danej aplikacji
    4. możliwość przeszukiwania bazy wiedzy, z dokładnością do nazw maszyn VM, adresów IP, ilości przepływów, wolumenu ruchu, etykiet/tagów itp.
32. Oprogramowanie musi obsługiwać minimum 2000 elementów końcowych (maszyn wirtualnych).
33. Oprogramowanie musi zostać uruchomione w obu OPD1 i OPD2 jednocześnie, pracując w modelu nadmiarowym, proces przywrócenia funkcjonalności usługi w przypadku awarii OPD nie może przekroczyć 15minut

### Chmura Publiczna

Zamawiający wymaga dostarczenia oprogramowania spełniającego poniższe wymagania na możliwość integracji:

1. Oprogramowanie musi umożliwiać rozbudowę środowiska o zasoby chmury publicznej
2. Oprogramowanie musi umożliwiać wykorzystanie zasobów publicznych do realizacji takich zadań jak: laboratorium, testowanie nowych rozwiązań, pre-prod, składowanie nagrań materiałów wideo z sesji zdalnych i innych.
3. Rozwiązanie ma zapewniać elastyczność, poprzez możliwość zastosowania gotowych komponentów, które można wykorzystywać przez systemy Zamawiającego – np. analiza obrazu i wideo celem kategoryzacji.
4. Rozwiązanie musi umożliwiać pozyskanie następujących zasobów publicznych
   1. Infrastruktura publicznego węzła obliczeniowego:
      1. Pojedynczy klaster, składający się z 3 serwerów, każdy o parametrach:
         1. 2 procesory, 18 rdzeni (fizycznych) każdy, wydajność 1 procesora nie mniej niż 15000 w testach CPU Mark (dostępnych na stronie <https://www.cpubenchmark.net>)
         2. 512 GB RAM
         3. Dyski SSD o łącznej pojemności co najmniej 15 TB
         4. Interfejsy sieciowe o przepustowości co najmniej 25 Gbps
         5. Możliwość dynamicznej rozbudowy do co najmniej 5 klastrów, każdy składający się z co najmniej 12 serwerów.
   2. Połączenie pomiędzy węzłami centralnymi (OPD1 i OPD2) a węzłem chmurowym
      1. Dedykowane łącze, o przepustowości minimum 10 Gbps, z możliwością rozbudowy do minimum 40 Gbps. Komunikacja nieprzechodząca przez Internet.
      2. Wsparcie dla IPv4 oraz IPv6.
      3. Wsparcie dla BGP
      4. Wsparcie dla połączeń szyfrowanych
   3. Zamawiający szacuje poziom przesyłanych danych miesięcznie na poziomie:
      1. Z infrastruktury OPD do węzła chmurowego do 5 TB
      2. Z węzła chmurowego do infrastruktury OPD do 5 TB
5. Wymaga jest integracja oprogramowania wirtualizacyjnego w chmury publicznej z oprogramowaniem Compute wirtualizacja mocy obliczeniowego dla węzłów centralnych (OPD1 i OPD2).
   1. Kompatybilność musi w szczególności obejmować:
      1. Praca w architekturze redundantnej. Replikacja pomiędzy węzłami OPD a węzłem chmurowym, zarówno na poziomie storage jak i maszyn wirtualnych.
      2. Architektura rozwiązania umożliwia przełączenie przetwarzania pomiędzy węzłami OPD a węzłem chmurowym, w tym ma możliwość bezprzerwowej migracji maszyn wirtualnych pomiędzy węzłami OPD a węzłem chmurowym.
      3. Rozwiązanie infrastruktury węzła chmurowego posiada funkcjonalność, która pozwala na zautomatyzowany failover oraz failback infrastruktury maszyn wirtualnych w przypadku wystąpienia awarii jednego z głównych OPD.
      4. Architektura rozwiązania informatycznego węzła chmurowego umożliwia tworzenie klastra wysokiej dostępności (HA) pomiędzy OPD a węzłem chmurowym oraz pozwala na wdrożenie mechanizmu niezawodności (DR) pomiędzy OPD a węzłem chmurowym.
      5. Możliwość uruchomienia w węźle chmurowym elementów środowiska OPD1 i OPD2, zapisanych jako kopie zapasowe maszyn wirtualnych wraz z ich konfiguracją i obrazami.
6. Możliwość wykorzystywania zasobów i funkcjonalności zlokalizowany w publicznie dostępnej infrastrukturze chmurowej, tak aby z poziomu węzła chmurowego możliwe było wykorzystanie udostępnianych przez tę chmurę usług zarządzanych (typu PaaS, SaaS). Chmura publiczna może udostępniać poniższe usługi:
   * 1. CDN
     2. Storage obiektowy
     3. AI/ML
     4. Kontenery
     5. Big data
     6. Zarządzane bazy danych (relacyjne i nierelacyjne)

## Komponent Macierz obiektowa

Zamawiający wymaga rozwiązania dostarczającego funkcjonalność:

1. Usługi/Aplikacje umieszczone w OPD1 mogą użytkować danych obiektowych w lokalizacji OPD1, a awaryjnie uzyskiwać dostęp do tych samych danych w innej lokalizacji OPD2 lub OPD3
2. Usługi/Aplikacje umieszczone w OPD2 mogą użytkować danych obiektowych w lokalizacji OPD2, a awaryjnie uzyskiwać dostęp do tych samych danych w innej lokalizacji OPD2 lub OPD3
3. Zaoferowane rozwiązanie musi umożliwiać rozbudowę do co najmniej 20 PB przestrzeni użytkowej w każdym z trzech ośrodków
4. Zaoferowane rozwiązanie musi składając się z trzech identycznych systemów obiektowych, rozmieszczonych w trzech centralnych ośrodkach przetwarzania danych OPD (OPD1, OPD2, OPD3)

### Architektura i wymagania funkcjonalne

Zamawiający wymaga dostarczenia rozwiązania spełniającego poniższe funkcjonalności:

1. Zaoferowane rozwiązanie musi zapewniać min. 1 PB przestrzeni użytkowej pamięci obiektowej zainstalowanej w każdym z trzech ośrodków (system odporny na awarie jednego ośrodka ODP1 lub OPD2). Jako przestrzeń użytkową należy rozumieć przestrzeń bez uwzględnienia jakichkolwiek mechanizmów redukcji danych na dostarczonej pojemności takich jak kompresja, deduplikacja, ThinProvisioning ale po realizacji zabezpieczenia RAID i odliczeniu rezerwy na przestrzeń zapasową
2. Oprogramowanie musi umożliwiać rozbudowę do co najmniej 20 PB przestrzeni użytkowej w każdym z trzech ośrodków
3. Architektura musi składając się z trzech identycznych systemów obiektowych, rozmieszczonych w trzech centralnych ośrodkach przetwarzania danych OPD (OPD1, OPD2 i OPD3)
   1. wymagana praca w klastrze active- active -passive lub active-active-active.
   2. wymagana replikacja danych miedzy pomiędzy trzema centralnymi ośrodkami przetwarzania danych OPD (OPD1, OPD2 i OPD3) w sposób asynchroniczny lub synchroniczny.
   3. wszystkie trzy lokalizacje w celu zapewnienia odpowiedniej niezawodności mają posiadać te same dane
   4. należy uwzględnić występujące na łączu WAN (sieci IP/MPLS OSE) opóźnienie, które w normalnym stanie pracy wynosi <= 8ms, opóźnienie i jitter może ulec zmianie przy obciążeniu/awarii sieci
4. Zaoferowane rozwiązanie musi dane w obiektowym magazynie danych składować na napędach dyskowych, nie dopuszcza się rozwiązań zbudowanych w oparciu o napędy taśmowe
5. Oprogramowanie musi powiadać wbudowane mechanizmy przechowywania zarówno danych, jak i metadanych (informacji opisujących dane). Nie dopuszcza się wykorzystania rozwiązań plikowych (NAS) jako warstwę przechowywania w systemie składowania danych.
6. Oprogramowanie musi powiadać wbudowane mechanizmy protekcji danych, które gwarantują odczyt wszystkich składowanych danych w przypadku awarii pojedynczego, losowego komponentu architektury (dysku, karty sieciowej, serwera itp.)
7. Oprogramowanie musi posiadać elastyczny mechanizm replikacji i Erasure Coding, umożliwiające określanie nadmiarowości i schematów kodowania danych per partycja
8. Oprogramowanie musi zapewniać funkcjonalność gwarantującą niezmienność składowanych w nim obiektów, między innymi poprzez wykorzystanie wbudowanej technologii WORM (Write Once Read Many) zapisz raz, odczyt wielkokrotny.
9. Oprogramowanie musi posiadać własne wbudowane mechanizmy weryfikacji sum kontrolnych składowanych obiektów
10. Oprogramowanie musi posiadać wbudowane mechanizmy redukcji danych, w tym co najmniej kompresję danych
11. Oprogramowanie musi posiadać wbudowany mechanizm indeksowania i wyszukiwania metadanych. Musi istnieć możliwość wyszukiwania w oparciu o wewnętrzną wyszukiwarkę oraz interfejs API pozwalający na integrację silnika wyszukiwania z własną aplikacją
12. Oprogramowanie musi posiadać wbudowane mechanizmy umożliwiające replikację składowanych danych pomiędzy różnymi lokalizacjami z wykorzystaniem sieci LAN/WAN. Zastosowanie niniejszego mechanizmu musi również spełniać wymagania replikacji metadanych, uprawnień oraz niezmienności danych tzn. awaria urządzenia w lokalizacji podstawowej nie może eliminować gwarancji niezmienności danych na platformie zdalnej
    1. replikacja musi być możliwa zarówno w trybie Active/Passive lub Active/Active
    2. replikacja powinna być możliwa pomiędzy co najmniej 3 ośrodkami
    3. możliwość szyfrowania składowanych danych
    4. pojemność rozwiązania musi zostać uzyskana w oparciu o dyski o pojemności minimum 4TB
13. Oprogramowanie musi posiadać możliwość mieszania różnych rozmiarów dysków (4, 6, 8, 10 TB itd.) w tym samym klastrze
14. Oprogramowanie musi i dostarczone urządzenia stanowiące całościowe rozwiązanie muszą być redundantne
    1. architektura musi zapewniać odporność na wystąpienie pojedynczego punktu awarii w obrębie poszczególnych grup elementów, co najmniej: interfejsów dostępowych serwerów, zasilaczy, wentylatorów, dysków. Odporność na awarię oznacza, że dostęp do funkcjonalności oraz do składowanych na nim danych musi być realizowany bez przerywania pracy, zapewniając możliwość odczytu wszystkich składowanych danych oraz wykonywania zapisów na urządzenie nawet w przypadku awarii lub wymiany pojedynczego elementu urządzenia z ww. grup urządzeń.
15. Oprogramowanie musi zapewniać odporność na awarię dowolnego z trzech ośrodków tzn. w przypadku całkowitego zniszczenia infrastruktury oferowanego rozwiązania w jednym z ośrodków wszystkie dane powinny być dostępne umożliwiając kontynuację pracy aplikacji;
    1. po usunięciu awarii dane powinny zostać automatycznie zsynchronizowane pomiędzy trzema ośrodkami
16. Oprogramowanie musi zapewniać odporność na utratę dowolnego serwera/urządzenia składującego dane - awaria taka nie może skutkować utratą danych ani niedostępnością systemu
    1. po usunięciu awarii serwera/urządzenia dane powinny zostać automatycznie zsynchronizowane pomiędzy serwerami/urządzeniami
17. Oprogramowanie musi zapewniać wydajność odbudowy w przypadku awarii węzła, urządzenia/serwera, dysku na poziomie nie więcej niż 30min / 25TB
18. Oprogramowanie musi zapewniać bezprzerwową aktualizacje oprogramowania, wymianę serwera, rozszerzenie pojemności nie wymagające zatrzymywania pracy rozwiązania i bez przerywania dostępu do danych.
19. Oprogramowanie musi zapewniać możliwość definiowania różnych poziomów retencji przechowywania danych, gwarantujących brak możliwości skasowania danych przed upływem zdefiniowanego czasu.
20. Oprogramowanie musi zapewniać wykorzystania co najmniej 30 atrybutów metadanych dla pojedynczego obiektu.
21. Oprogramowanie musi zapewniać wykorzystania do 3mld obiektów o wielkości 25KB.
22. Oprogramowanie musi zapewniać rozwiązanie posiadało możliwość zdefiniowania co najmniej 1000 logicznych partycji oraz co najmniej 1000 przestrzeni nazw. Musi istnieć możliwość mapowania i wykorzystania różnych przestrzeni nazw dla różnych aplikacji, w taki sposób, aby dla każdej z tych aplikacji możliwe było definiowanie różnych i niezależnych parametrów i kryteriów składowania danych, w tym co najmniej: retencji, wersjonowania, indeksowania i replikacji.
23. Oprogramowanie musi zapewniać możliwość szyfrowania składowanych obiektów algorytmem AES-256
24. Oprogramowanie musi zapewniać możliwość integracji z aplikacjami za pomocą co najmniej następujących protokołów i interfejsów: http, HTTPS, S3, REST API, NFS v3. Jeżeli wykorzystanie któregokolwiek z wymienionych protokołów i interfejsów wymaga zastosowania dodatkowej licencji lub oprogramowania, to należy je dostarczyć wraz z rozwiązaniem. Wszystkie protokoły muszą być dostępne równocześnie
25. Oprogramowanie musi zapewniać architekturę rozwiązania zapewniającą dostępność interfejsów dostępowych i dyskowych w każdym węźle klastra
26. Oprogramowanie musi zapewniać automatyczne ponowne rozkładanie danych po dodaniu nowego serwera w klastrze
27. Oprogramowanie musi zapewniać brak limitu rozmiaru obiektu lub plików
28. Oprogramowanie musi zapewniać skalowalność do co najmniej 2100 obiektów
29. Oprogramowanie musi i urządzenia muszą zapewniać wydajność w obrębie węzła, dla interfejsów S3/NFS odczyt/zapis obiektów/plików o małych rozmiarach (30KB) z prędkością nie mniejszą niż 200 MBps oraz nie mniejszą niż 1000 MBps w przypadku obiektów/plików o dużych rozmiarach (powyżej 10MB)
30. Oprogramowanie musi zapewniać centralny interfejs zarządzający całym systemem, lokalnymi użytkownikami i przyznawanie uprawnień dostępu w oparciu o role
    1. możliwość zarządzania co najmniej poprzez graficzny interfejs użytkownika oraz poprzez API.
    2. możliwość tworzenia logicznie odseparowanych obszarów tzw. „multi-tenancy”. Wymagana jest możliwość rozdzielnego administrowania (np.: przypisywanie użytkowników, tworzenie praw dostępu, monitorowanie wykorzystania) tak tworzonymi obszarami
    3. widok topologii - stan środowiska z uwzględnieniem stref, serwerów i szczegółów węzłów
    4. możliwość wykorzystania platformy sprzętowej co najmniej trzech niezależnych producentów

### Wymagania sprzętowe

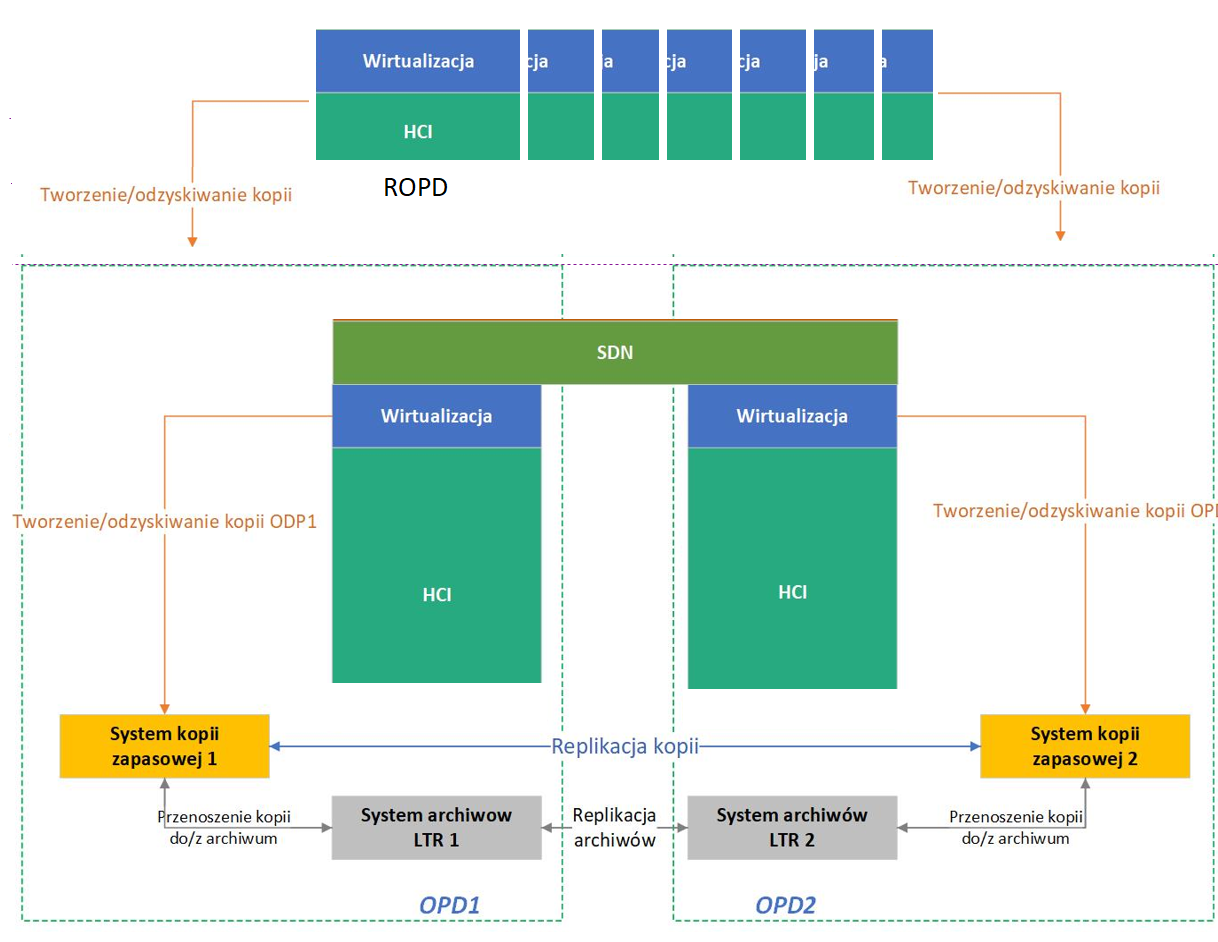
1. Dostarczane urządzenia muszą być dedykowaną platformą wyłącznie do oprogramowania macierzy obiektowej i zarządzania nią. Urządzenia nie mogą stanowić elementu innego Komponentu ani być wykorzystywane w innym celu niż dedykowany.
2. Urządzenia muszą być zgodne z oferowanym oprogramowaniem macierzy obiektowej
   1. model urządzeń/serwery i jego składniki muszą być umieszczone na oficjalnej stronie producenta oprogramowania jako odpowiadające wymaganiom oprogramowania
3. Specyfikacja urządzeń
   1. obudowa typu RACK 19" wraz z zestawem do zamontowania w szafie teleinformatycznej 19", o głębokości 80-100cm i prowadzeniem dla kabli, umożliwiającym pełne wysunięcie obudowy na szynach.
   2. wyposażone w panel LCD lub LED umieszczony na froncie serwera, umożliwiający wyświetlenie informacji o stanie serwera, zasilania oraz temperatury lub za pomocą dedykowanego oprogramowania do zarządzania infrastrukturą serwerową
   3. płyta główna zaprojektowana przez producenta serwera
   4. zintegrowana karta graficzna o rozdzielczości minimum 1900 x 1200
   5. wyposażony w procesory 64 bitowe o minimalnym parametrach:
      1. wbudowane w procesor wsparcie dla obsługi standardu PCIe 3.0
      2. zintegrowany kontroler zarządzania pamięcią
   6. wyposażony w pamięć RAM minimum kości DDR4 2666 MHz RDIMM
   7. wyposażony w interfejsy sieciowe LAN:
      1. min. 2 porty Gigabit Ethernet 1000Base-T
      2. min. 4 porty 10 Gigabit Ethernet w formie gniazd SFP+ na płycie głównej lub karcie PCIe
   8. wyposażony w min. 1 interfejs sieciowy na potrzeby zarządzania RJ-45 10/100/1000 dedykowany dla zarządzania;
   9. wyposażony w następujące inne interfejsy:
      1. min. 2 bezpośrednio udostępnione zewnętrzne porty USB 3.0
      2. min. 1 bezpośrednio udostępniony port VGA DB15
      3. wyposażony w moduł zdalnego zarządzania (konsoli) umożliwiający:
         1. zdalne włączenie, wyłączenie i restart urządzenia
         2. podgląd logów serwera
         3. wsparcie dla SNMP
         4. monitorowanie stanu zasilaczy, wentylatorów, dysków, temperatury, wielkości poboru energii,
         5. definiowanie wielu użytkowników z możliwością uwierzytelniania w LDAP, Active Directory, Radius
         6. wysyłanie powiadomień syslog do zewnętrznych serwerów
         7. rejestrowanie działań administratora w oparciu o log
   10. Zasilanie, chłodzenie:
       1. min. dwa jednakowe zasilacze wymienne podczas pracy serwera w konfiguracji redundantnej, zapewniającej zasilanie serwera działającego ze 100% wykorzystaniem zasobów sprzętowych na jednym zasilaczu, hot swap
       2. redundantne chłodzenie serwera, co najmniej dwa wentylatory, hot swap
   11. Serwer musi posiadać deklarację CE.
4. W przypadku awarii któregokolwiek z dysków dyski twarde pozostają własnością Zamawiającego.

## Komponent kopii zapasowych i archiwów

### Założenia, architektura i wymagania funkcjonalne środowiska kopii zapasowych

1. Należy dostarczyć komercyjne rozwiązanie wykonywania kopii zapasowych i odzyskiwania maszyn wirtualnych, które będzie wykorzystywane w ramach dostarczonej infrastruktury Compute i SDS.
2. Oprogramowanie musi zapisywać kopie i przywracać stan maszyn wirtualnych za pomocą kopii migawkowych (tzw. snapshotów).
3. Oprogramowanie nie może wnikać w to, co dzieje się w logice aplikacyjnej wewnątrz uruchomionych maszyn wirtualnych. Wymaga się zabezpieczania dodatkowo mechanizmami „tradycyjnych" backupów agentowych, w sytuacjach gdy aplikacja zabezpieczana wymaga agenta, który w odpowiedni sposób wyda komendy z żądaniami zrzutu danych, dzięki czemu zachowana będzie konsystencja (kompletność) i poprawność danych zrzucanych z działającej aplikacji np. bazy danych typu SQL/Oracle itp.
4. Pod pojęciami archiwizacja danych lub archiwa rozumieć należy długoterminowe przechowywanie kopii zapasowych zgodnie z polityką retencji opisaną w dalszej części dokumentu.
   1. Należy założyć, że dane zapisane w kopiach zapasowych o statusie archiwalnym będą znacznie rzadziej wykorzystywane (odzyskiwane) w porównaniu do kopii zapasowych o krótkiej retencji tj. mniej niż 30 dni od wykonania kopii danych.
5. Zmawiający wymaga aby wszystkie dane w centralnych OPD1 i OPD2 były przechowywane i archiwizowane w następującym modelu:
   1. Codzienna kopia środowiska chmury – 7 dni (7 kopii)
   2. Tygodniowa kopia środowiska chmury – 4 tygodnie (4 kopie)
   3. Miesięczna kopia środowiska chmury – 12 miesięcy (12 kopii)
   4. Roczna kopia środowiska chmury – 2 lata (1 kopia)
6. Przyjęto także, że wszystkie dane w szesnastu ROPD będą archiwizowane w następującym modelu:
   1. Codzienna kopia wirtualnych maszyn – 7 dni (7 kopii)
   2. Tygodniowa kopia wirtualnych maszyn – 2 tygodnie (2 kopie)
7. Oprogramowanie musi umożliwiać określenie RPO (Recovery Point Objective) i RTO (Recovery Time Objective) dla zabezpieczanych danych.
8. Wykonawca stworzy odpowiednie środowisko testowe celem cyklicznych weryfikacji możliwości i poprawności odtwarzania danych z kopii zapasowych i archiwów w OPD1.
   1. Utworzone środowisko testowe musi być tożsame pod kątem funkcjonalnym ze środowiskiem produkcyjnego. Składać się będzie serwerów HCI w OPD1.
9. Oprogramowanie musi być dedykowane dla infrastruktury wirtualnej i wykorzystywać istniejące w niej mechanizmy związane z wykonywaniem kopii zapasowych i odtwarzania, uwzględniając standardy charakterystyczne dla obszaru wirtualizacji.
10. Licencjonowane rozwiązania muszą umożliwiać rozbudowę i pozwalać w policzalny sposób planować rozbudowę środowiska i związane z tym inwestycje.
    1. Rozwiązanie musi reprezentować architekturę trójwarstwową (serwer zarządzający, serwer medialny oraz klient),
11. System do tworzenia kopii zapasowych musi być zgodny z platformą wirtualizacyjną dostarczaną w ramach przedmiotu zamówienia, minimalizować nakłady pracy potrzebne do konfiguracji i obsługi środowiska.
    1. System musi zapewniać uproszczenie codziennych czynności poprzez automatyzację, bez utraty funkcjonalności.
    2. System musi raportować stan wykonywanych zadań
12. W każdym z dwóch centralnych OPD1 i OPD2 musi być zaimplementowane rozwiązanie do tworzenia kopii zapasowych (Komponent Kopie zapasowe i archiwum) odpowiedzialny za tworzenie kopii zapasowych z tej samej lokalizacji
    1. w OPD1 tworzone są kopie zapasowe i zapisywane w OPD1,
    2. w OPD2 tworzone są kopie zapasowe i zapisywane w OPD2,
    3. w szesnastu ROPD tworzone są kopie zapasowe do centralnych OPD1 i OPD2
13. Wzajemna replikacja kopii zapasowych miedzy oboma OPD zapewnia drugą kopię pierwotnej kopii zapasowej i możliwość odzyskania w drugiej lokalizacji.
14. Okno potrzebne na wykonywanie kopii zapasowej oraz replikacji zawiera się pomiędzy godziną 22:00 a 6:00 rano.
15. Oprogramowanie musi zostać skonfigurowane w formie zapewniającej nadmiarowość gwarantującą ciągłość działania w obrębie każdego OPD1 i OPD2 w razie awarii elementów kopii zapasowych/archiwum w obrębie danego OPD.
16. System kopii zapasowych ma zapewniać mechanizmy wysokiej dostępności na wypadek pełnej awarii jednego z OPD, poprzez replikację kompletu krótkoterminowych kopii zapasowych do drugiego OPD na zasadach: OPD1 replikuje kopie zapasowe do OPD2, a OPD2 replikuje kopie zapasowe do OPD1.
17. Systemy kopii zapasowych w obu OPD będą przechowywać krótkoterminowo kopie środowisk produkcyjnych na własnych dedykowanych zasobach dyskowych, a następnie w ramach zautomatyzowanych polityk retencji przenosić kopie wymagające długoterminowego składowania na dedykowane zasoby archiwów LTR z zachowaniem deduplikacji i kompresji.
18. Zakłada się, że archiwa LTR będą znacznie mniej obciążone względem kopii zapasowych, jednak z racji gromadzenia danych w dłuższym czasie muszą zapewniać większe pojemności i rozbudowę w miarę przyrostu danych w archiwach.
19. Archiwum LTR będzie zapewniać odporność na awarię i mechanizmy HA w obrębie każdego OPD poprzez nadmiarowość komponentów oraz w obrębie OPD1 i OPD2 objętych kopiami zapasowymi poprzez replikację zasobów archiwalnych między OPD1 i OPD2 tj. długoterminowe archiwa z OPD1 będą replikowane do analogicznego rozwiązania w OPD2 oraz odwrotnie archiwa z OPD2 będą replikowane do OPD1.
20. Proces archiwizowania kopii zapasowych z systemu kopii zapasowych do systemu archiwów LTR powinien być zautomatyzowany i zgodny ze zdefiniowanymi politykami obrotu danych w OSE.
21. W celu optymalizacji wykorzystania zasobów i rozłożenia procesów w czasie dopuszcza się wykonywanie archiwizowania kopii zapasowych w godzinach roboczych (przenoszenie kopii zapasowych krótkiego przechowywania do systemu archiwów LTR w obrębie tego samego OPD).

Poniższy diagram przedstawia topologię Komponentu Kopii zapasowych/archiwów względem OPD1 i OPD2:



1. Ze względów bezpieczeństwa oraz wydajności wymagane jest, aby infrastruktura tworzenia, przetwarzania i przechowywania kopii zapasowych była niezależna fizycznie od zasobów dyskowych, obliczeniowych i wirtualizacyjnych Compute i SDS.
2. Oprogramowanie nie może preferować platformy sprzętowej, nie może być profilowane pod konkretnego dostawcę sprzętu serwerowego oraz pamięci masowych. Niedopuszczalne jest aby funkcjonalności związane z zabezpieczaniem danych były w jakikolwiek sposób związane czy zależne od konkretnego typu czy producenta urządzenia.
3. Jeśli system korzysta z bazy danych to wszelkie potrzebne licencje muszą być dostarczone i stanowić całość oferty, z tym iż licencje dla silnika bazodanowego muszą pozwalać na zainstalowanie go na dostarczonych serwerach fizycznych (minimum 2xCPU po 8 core), klastrze active-passive czy serwerze wirtualnym.
4. Licencje muszą pozwalać na stworzenie dla serwera zarządzającego rozwiązania wysokodostępnego z czasem przełączenia nie dłuższym niż 15 minut. Jeśli do stworzenia takowego rozwiązania potrzebne są licencje replikacyjne, klastrowe, współdzielona przestrzeń dyskowa, to muszą zostać zaoferowane. Licencje muszą pozwalać na skonfigurowanie serwerów zarządzających oraz ich replikację dla co najmniej dwóch lokalizacji,
5. Oprogramowanie musi zapewnić interfejs graficzny do zarządzania i instalacji.
6. Oprogramowanie musi umożliwiać zdalne instalowanie i odinstalowywanie klienta systemu z centralnego serwera dla systemów Windows, Linux i Unix – musi być to możliwe z jednego serwera pełniącego rolę cache dla wszystkich binarii klienckich
7. Oprogramowanie musi umożliwiać funkcjonalność odtwarzania po awarii konfiguracji serwera zarządzającego tworzeniem kopii bezpieczeństwa i archiwów.
8. Oprogramowanie musi umożliwiać nieodwracalne kasowanie danych – funkcjonalność ta musi być częścią oprogramowania
9. Dla dowolnego transferu danych z klienta musi istnieć możliwość definiowania/ograniczania pasma dla transferu danych
   1. funkcjonalność ta musi być dostępna także przy włączonej deduplikacji na kliencie
10. Oprogramowanie musi pozwalać na składowanie danych na zewnętrznych zasobach dyskowych celem przechowywania długoterminowego.
11. Oprogramowanie musi pozwalać na zarządzanie całością działania systemu (kopii zapasowych, archiwum) z jednej konsoli administracyjnej oraz także z konsoli webowej
12. Oprogramowanie musi umożliwiać stosowanie Agentów posiadających funkcjonalność komunikowania się poprzez jeden port TCP/IP, celem zabezpieczenia komunikacji z środowisk typu DMZ
13. Oprogramowanie musi realizować automatyczne tunelowanie komunikacji TCP/IP pomiędzy agentami systemu – jeśli agent systemu wykryje ograniczenia w komunikacji, wtedy automatycznie zestawia połączenie tunelowe
14. Oprogramowanie musi realizować wykonywanie kopii zapasowych z ROPD stosując mechanizm szyfrowania przesyłanych danych.
15. Oprogramowanie musi umożliwiać konfigurację, którymi kartami sieciowymi ma przebiegać komunikacja i transfer danych, wybór interfejsu musi odbywać się co najmniej poprzez subnet, zakres IP
16. Oprogramowanie musi zapewniać przechowywanie jedynie unikalnych bloków danych tzw. deduplikacja. Funkcjonalność ta musi działać na poziomie blokowym i być wykonywana online podczas procesu tworzenia kopii danych.
    1. Deduplikacja musi być realizowana poprzez oprogramowanie systemu na dowolnym sprzęcie czy to w warstwie serwera systemu czy klienta.
    2. Pojedynczy serwer systemu musi umożliwiać przechowywanie danych po deduplikacji minimum do 50 TB (rozbudowa do tej wielkości może nastąpić tylko poprzez dodanie dodatkowych dysków czy macierzy dyskowej).
17. Włączenie funkcjonalności deduplikacji na kliencie musi być możliwe dla różnych systemów operacyjnych: Windows, Linux, Unix i
18. Oprogramowanie musi zapewniać deduplikację globalną, co oznacza iż niezależnie z jakich klientów dane będą deduplikowane (serwery fizyczne, hosty wirtualne, bazy i aplikację) – deduplikacja musi opierać się na jednej centralnej bazie dedupplikacyjnej
19. Deduplikacja blokowa musi obejmować dane nie tylko backupowane ale i archiwizowane
20. Oprogramowanie musi zapewniać wykonywanie kopii w post procesie do drugiej lokalizacji przesyłając jedynie unikalne bloki danych (dla dowolnych danych: czy to z procesu backupu czy archiwizacji). A więc replikacja danych do innej lokalizacji musi być wykonywana na danych po deduplikacji i funkcjonalność ta musi być realizowana i zarządzana z poziomu systemu skracając czas i pasmo wykorzystywane na łączu WAN
21. Proces przesyłania danych (replikacji) na inny serwer systemu celem tworzenia dodatkowej kopii danych nie może być zależny od warstwy sprzętowej, a więc dowolny producent serwera, dowolny producent macierzy/półki dyskowej
22. Zainstalowana baza deduplikacyjna musi zostać zrealizowana w układzie wysokiej dostępności (minimum na dwóch serwerach) w taki sposób, aby awaria pojedynczego serwera nie powodowała utraty możliwości deduplikacji i odtwarzania danych
23. Oprogramowanie musi zapewniać odtwarzanie zdeduplikowanych danych nawet w momencie, gdy baza deduplikacyjna jest niedostępna.
24. Oprogramowanie musi zapewniać dostęp zintegrowany z usługą katalogową, minimum to Active Directory – pojedyncze logowanie: użytkownik po zalogowaniu do domeny AD, nie potrzebuje wykonywać następnego logowania aby zarządzać systemem poprzez konsolę administracyjną
25. Oprogramowanie musi zapewniać elastyczne delegowanie uprawnień oraz audytowanie działań użytkowników z tym, że delegowanie uprawnień musi pozwalać na przydział uprawnień per serwer czy grupa serwerów, przydział uprawnień musi pozwalać na definiowanie uprawnień dla grup użytkowników z domeny AD.
26. Komunikacja pomiędzy agentem a serwerem systemu musi opierać się na certyfikatach
27. Oprogramowanie musi zapewniać funkcjonalność blokowania danych do odczytu dla administratora, to znaczy, że administrator systemu nawet mając pełne uprawnienia nie może odtworzyć danych, jeśli nie jest ich właścicielem,
28. Oprogramowanie musi zapewniać skonfigurowanie mechanizmu podwójnej autentyfikacji administratora – do uruchomienia konsoli administracyjnej systemu potrzebne jest nie tylko logowanie, ale i dodatkowy tymczasowy kod wysyłany do administratora np. poprzez mail
29. Oprogramowanie musi umożliwiać szyfrowanie danych pozwalać na wybór algorytmu (minimum dwa algorytmy: Blowfish, AES) także dla danych deduplikowanych na kliencie systemu.
    1. Możliwość szyfrowania musi pozwalać na elastyczny wybór miejsca szyfrowania: szyfrowanie danych na kliencie, szyfrowanie danych na serwerze backupowym i szyfrowanie tylko transmisji pomiędzy klientem backupowym a serwerem
30. Oprogramowanie musi pozwalać na integrację z zewnętrznymi repozytoriami do przechowywania kluczy szyfrującym – minimum dla: Safenet, Amazon Web Services (AWS) key management service, Microsoft Azure Key Vault
31. Oprogramowanie musi mieć wbudowane mechanizmy zabezpieczające przed złośliwym oprogramowaniem (ang. ransomware), minimum to:
    1. Zabezpieczenie ścieżek dostępu do danych składowanych (kopii backupowych) na dyskach – tylko procesy systemu mogą zapisywać i modyfikować dane
    2. Monitorowanie nietypowych aktywności na serwerach
    3. Monitorowanie dużych aktywności na serwerach plikowych i desktopach, monitorowanie musi odbywać się nie rzadziej, niż co 5 minut i każdy niestandardowy wynik jest automatycznie wysyłany w postaci alertu lub notyfikacji
    4. System musi posiadać rozbudowany system powiadamiania o zdarzeniach poprzez email.
    5. System musi automatycznie wysyłać informacje o alertach, zdarzeniach oraz informacjach audytowych do syslog serwera
32. Oprogramowanie musi pozwalać na automatyczne monitorowanie stanu systemu poprzez wiadomości SMS na urządzeniach mobilnych i telefonach
33. Oprogramowanie musi posiadać rozbudowany system raportowania dla administratorów, minimalny zestaw dostępnych raportów to:
    1. Raport zmian/wzrostu środowiska systemu
    2. Raport wykorzystania licencji
    3. Raport wykonanych zadań backupowych
34. Oprogramowanie musi pozwalać automatyczne na wysyłanie dowolnych raportów do wybranych użytkowników poprzez mail
35. Oprogramowanie musi pozwalać na automatyczne zapisywanie raportów w formacie minimum: PDF, HTML i CSV
36. Oprogramowanie musi pozwalać na definiowanie alertów per zadanie backupowe lub zadanie odtwarzania danych przy spełnieniu minimum kryteriów:
    1. Czas zadania dłuższy niż zadany
    2. Ilość danych większa niż ….
    3. Ilość danych mniejsza niż ….
    4. Liczba nie zbackupowanych plików większa niż
    5. Liczba nie zbackupowanych plików większa niż …%
    6. Wielkość backupowanych danych większa niż …
    7. Notyfikacje alertów muszą być wysyłane minimum poprzez mail.
    8. Raport spełnienia wymogów SLA dla parametrów:
       1. Ilości dodatkowych kopii backupowych
       2. RTO
       3. RPO
37. Oprogramowanie musi zapewniać możliwość monitorowania, raportowania, szczegółowego rozliczania i analizy błędów dla środowiska kopii zapasowej Zamawiającego. Wymagana jest dostępność następujących raportów min.:
    1. Podsumowanie zadań backupowych (liczba backupów udanych, nieudanych, aktywnych, łączny rozmiar zbackupowanych danych)
    2. Podsumowanie zadań odtworzeniowych (liczba odtworzeń udanych, nieudanych, aktywnych, łączny rozmiar odtworzonych danych)
    3. Zbiorcze zestawienie zabezpieczanych serwerów, które w sposób ciągły (wielokrotnie) mają problem z backupami
    4. Poziom SLA (procentowa liczba udanych backupów) w odniesieniu do poziomu założonego
    5. Mierzenie poziomu SLA dla poszczególnych zabezpieczanych serwerów przy uwzględnieniu założonego okna backupowego.
    6. Liczba danych backupowanych dziennie.
    7. Liczba zadań backupowych dziennie.
    8. Zużycie zasobów na serwerach backupowych (procesor, pamięć, karty sieciowe LAN).
    9. Zużycie mediów backupowych.
    10. Aktualna konfiguracja systemu kopii zapasowych.
    11. Historia zmian konfiguracji systemu kopii zapasowych.
38. Oprogramowanie musi zapewniać funkcjonalność wznawiania zadań backupowych.
39. Oprogramowanie musi zapewniać funkcjonalność równoległego wykonywania kopii danych backupowanych – inline copy (tego samego zestawu danych pojedynczego klienta) na minimum dwa docelowe urządzenia przechowywania danych.
40. Oprogramowanie musi zapewniać funkcjonalność wykonywania zadania backupu wieloma równoległymi strumieniami – tzw. multistreaming. Polega ona na tym iż agent systemu równolegle czyta różne obszary danych i bez pośredniczenia dysków automatycznie wysyła je do serwera, który zapisuje te dane albo na dyski. Funkcjonalność ta musi być dostępna dla backup plikowy, bazodanowy
41. Funkcjonalność multistreamingu musi być dostępna dla deduplikacji na kliencie
42. Rozwiązanie musi posiadać możliwość wykonywania backupu pełnego, przyrostowego, różnicowego oraz syntetycznego.
43. Oprogramowanie musi oferować funkcjonalność backupu blokowego, polegającego na tym, iż agent buduje własną bazę zmian bloków danych, przez co kopia zapasowa przyrostowa nie wymaga odczytu całych plików tylko zmienionych bloków wielokrotnie przyspieszając procesowanie kopii zapasowej. Funkcjonalność ta musi być dostępna dla kopii zapasowych danych plikowych.
44. Oprogramowanie musi umożliwiać tworzenie zadań backupowych w oparciu o kalendarz.
45. Oprogramowanie musi posiadać zintegrowane w systemie mechanizmy indeksowania pełnokontekstowego i wyszukiwania danych. Indeksowaniu powinny podlegać dane kopii zapasowych i archiwizowane.
46. Oprogramowanie musi realizować funkcjonalność weryfikacji wykonanych kopii.
47. Oprogramowanie musi umożliwiać wykorzystanie funkcjonalności Bare Metal Restore dla odtwarzania systemu po awarii, wsparcie musi być dostępne dla systemów:
    1. Windows
    2. Linux: Debian/Oracle Linux/RHEL/CentOs/SuSe/Ubuntu
48. Oprogramowanie musi umożliwiać opcjonalnie obsługę składowania danych w chmurze, m.in. Azure, Amazon, Google Cloud
49. Oprogramowanie musi umożliwiać odtwarzanie danych plikowych pomiędzy systemami operacyjnymi np. odtwarzanie danych plikowych Linux na systemie Windows
50. Oprogramowanie musi pozwalać na odtwarzanie tylko samych uprawnień do plików
51. Oprogramowanie musi umożliwiać odtwarzanie zasobów plikowych bez praw dostępu (tzw. ACL)
52. Oprogramowanie musi umożliwiać odtwarzanie backupów plikowych poprzez udostepnienia CIFS lub NFS, a więc dostęp do zbackupowanych danych widocznych jako udostępnione przez sieć zasoby CIFS/NFS
53. Oprogramowanie musi posiadać wbudowany mechanizm tworzenia kopii otwartych plików na platformie Windows i Linux
54. Oprogramowanie musi zapewniać wykonanie kopii na systemach klasy Windows, Linux i Unix
    1. wsparcie dla środowisk Windows, minimum: Windows Serwer 2008, Windows Serwer 2016, Windows Serwer 2019
    2. wsparcie dla środowisk Linux, minimum: RHEL, SuSe, Debian, Fedora, Oracle Linux, Red Flag Linux, Ubuntu, Slackware
    3. wsparcie dla środowisk Unix, minimum: FreeBSD, HP-UX,
55. Oprogramowanie musi umożliwiać realizację kopii zapasowych dla czołowych rozwiązań wirtualizacyjnych i kontenerowych: VMware, Hyper-V, Citrix Xen, RHEV, OracleVM, Docker, OpenStack, Huawei FusionCompute, Nutanix Acropolis, OpenShift, to znaczy musi posiadać możliwość wykonania kopii zapasowej całej maszyny wirtualnej bez konieczności instalowania agenta wewnątrz maszyny.
56. Oprogramowanie musi umożliwiać w przypadku kopii pliku maszyny wirtualnej granularne odtwarzanie pojedynczych plików.
57. Oprogramowanie musi zapewniać automatyczne wykrywanie i dodawanie do polityki backupu nowych maszyn wirtualnych.
58. Oprogramowanie musi umożliwiać odzyskanie i uruchomienie maszyn wirtualnych z kopii zapasowej bez oczekiwania na pełne przywrócenie maszyny wirtualnej.
59. Oprogramowanie musi umożliwiać konwersję zbackupowanego serwera Windows i Linux do maszyny wirtualnej w środowisku minimum do dwóch wirtualizatorów
60. Oprogramowanie musi umożliwiać wykonanie kopii na gorąco bazy danych MySQL, Postgress, Oracle, Informix na dowolnej platformie systemu operacyjnego (Windows/Linux/Unix) poprzez dedykowanego agenta bazodanowego, transfer danych musi odbywać się bez pośredniczenia dysków, a więc transfer danych z agenta bazodanowego bezpośrednio do serwera backupowego celem zapisu na dany nośnik.
61. Oprogramowanie musi umożliwiać wykonanie kopii na gorąco bazy danych MS SQL, Oracle, MySQL, Postgress, DB2, Informix konfiguracja agenta nie może powodować konieczności tworzenia skryptów uruchamianych po stronie klienta niezależnie czy jest to serwer fizyczny czy wirtualny.
    1. Odtwarzanie danych z backupu bazodanowego (MS SQL, Oracle, MySQL, Postgress, DB2, Informix) musi odbywać się poprzez konsolę administracyjną bez konieczności konfigurowania skryptów
    2. Konfiguracja agentów backupowych dla: MS SQL, Oracle, mySQL musi odbywać się poprzez interfejs graficzny, jakakolwiek modyfikacja zasobów do backupu (np. dodanie nowej bazy) nie może powodować konieczności modyfikacji skryptów czy to dla backupów planowanych czy wykonywanych na żądanie
62. Oprogramowanie musi umożliwiać wykonanie kopii na gorąco Active Directory, a następnie odzyskanie pojedynczych obiektów AD wraz z hasłami użytkowników
63. Oprogramowanie musi umożliwiać odtwarzanie backupu wykonywanego online dedykowanym agentem do pliku, celem późniejszego odtwarzania bez udziały systemu. Funkcjonalność ta musi być dostępna minimum dla MS SQL, Oracle
64. Oprogramowanie musi umożliwiać backup online dla minimum MS SQL Server 2016/2014/2012/2008/2005
65. Oprogramowanie musi zapewniać dedykowanego agenta bazodanowego dla backupu MS SQL na platformie Linux: Ubuntu, SuSe, RHEL
66. Sposób licencjonowania musi opierać się na ilości danych podlegających zabezpieczeniu bez ograniczeń co do ilości:
    1. serwerów/hostów – dla serwerów fizycznych
    2. maszyn wirtualnych lub fizycznych CPU wirtualizatorów - dla środowisk wirtualnych
    3. ilości lokalizacji systemu backupowego
    4. replikacji danych po backupie
    5. wielkości storage przeznaczonego na składowanie danych
67. Dla środowiska wirtualnego i fizycznego zaoferowane licencje muszą pozwalać na backup nieograniczonej ilości aplikacji dedykowanym agentem zainstalowanym wewnątrz serwera wirtualnego czy fizycznego
68. Zaoferowane licencje nie mogą ograniczać wielkości przestrzeni do składowania danych czy replikowania ich do innych lokalizacji. Jakakolwiek rozbudowa przestrzeni dyskowej czy to w siedzibie podstawowej czy innej nie może wymagać zakupu jakichkolwiek licencji dla systemu
69. Oferowana licencja oraz architektura musi pozwalać na kopie zapasowe danych na nielimitowana ilość nośników.
70. Oferowana licencja musi pozwalać na replikację danych po deduplikacji pomiędzy lokalizacjami OSP1 i OPS2
71. Zaoferowane licencje na rozwiązanie muszą zapewnić backup danych z środowiska o wielkości:
72. środowisko maszyn wirtualnych wraz z aplikacjami i bazami 700 TB
73. środowisko serwerów fizycznych wraz z aplikacjami i bazami 100 TB

### Kopie zapasowe i archiwum –wymagania sprzętowe

1. W każdym z OPD1 i OPD2 musi zostać zainstalowana identyczna architektura sprzętowa pełniąca rolę platformy dla oprogramowania kopii zapasowej i archiwów.
2. Dostarczane urządzenia muszą być dedykowaną platformą wyłącznie do wykonywania kopii zapasowych, archiwum i zarządzania nimi. Urządzenia nie mogą stanowić elementu innego Komponentu ani być wykorzystywane w innym celu niż dedykowany.
3. Musi zostać zapewniona wysoka dostępność oraz balansowanie ruchem/obciążeniem i agregacją wydajności zapisu/odczytu kopii zapasowych
4. Urządzenia muszą być zgodne z oferowanym oprogramowaniem realizacji kopii zapasowych i archiwum
   1. model urządzeń/serwery i jego składniki muszą być umieszczone na oficjalnej stronie producenta oprogramowania jako odpowiadające wymaganiom oprogramowania
5. specyfikacja urządzeń
   1. obudowa typu RACK 19" wraz z zestawem do zamontowania w szafie teleinformatycznej 19", o głębokości 80-100cm i prowadzeniem dla kabli, umożliwiającym pełne wysunięcie obudowy na szynach.
   2. wyposażone w panel LCD lub LED umieszczony na froncie serwera, umożliwiający wyświetlenie informacji o stanie serwera, zasilania oraz temperatury lub za pomocą dedykowanego oprogramowania do zarządzania infrastrukturą serwerową
   3. płyta główna zaprojektowana przez producenta serwera
   4. zintegrowana karta graficzna o rozdzielczości minimum 1900 x 1200
   5. wyposażony w procesory 64 bitowe o minimalnym parametrach:
      1. wbudowane w procesor wsparcie dla obsługi standardu PCIe 3.0
      2. zintegrowany kontroler zarządzania pamięcią
   6. wyposażony w pamięć RAM minimum kości DDR4 2666 MHz RDIMM
   7. wyposażony w interfejsy sieciowe LAN:
      1. min. 2 porty Gigabit Ethernet 1000Base-T
      2. min. 4 porty 10 Gigabit Ethernet w formie gniazd SFP+ na płycie głównej lub karcie PCIe
   8. wyposażony w min. 1 interfejs sieciowy na potrzeby zarządzania RJ-45 10/100/1000 dedykowany dla zarządzania;
   9. wyposażony w następujące inne interfejsy:
      1. min. 2 bezpośrednio udostępnione zewnętrzne porty USB 3.0
      2. min. 1 bezpośrednio udostępniony port VGA DB15
      3. wyposażony w moduł zdalnego zarządzania (konsoli) umożliwiający:
         1. zdalne włączenie, wyłączenie i restart urządzenia
         2. podgląd logów serwera
         3. wsparcie dla SNMP
         4. monitorowanie stanu zasilaczy, wentylatorów, dysków, temperatury, wielkości poboru energii,
         5. definiowanie wielu użytkowników z możliwością uwierzytelniania w LDAP, Active Directory, RADIUS
         6. wysyłanie powiadomień syslog do zewnętrznych serwerów
         7. rejestrowanie działań administratora w oparciu o log
   10. Zasilanie, chłodzenie:
       1. min. dwa jednakowe zasilacze wymienne podczas pracy serwera w konfiguracji redundantnej, zapewniającej zasilanie serwera działającego ze 100% wykorzystaniem zasobów sprzętowych na jednym zasilaczu, hot swap
       2. redundantne chłodzenie serwera, co najmniej dwa wentylatory, hot swap
   11. Serwer musi posiadać deklarację CE.
6. W przypadku awarii któregokolwiek z dysków dyski twarde pozostają własnością Zamawiającego
7. Zduplikowane i skompresowane dane przechowywane w obrębie podsystemu dyskowego urządzeń muszą być chronione za pomocą technologii np. RAID 6 lub alternatywnej, zapewniającej nie mniejszy poziom zabezpieczenia, w celu maksymalizacji poziomu bezpieczeństwa przechowywanych danych.
8. Wymagane jest dostarczenie urządzeń i licencji pozwalających na gromadzenie archiwalnych kopii zapasowych w OPS1 i OPS2 (z deduplikacją i kompresją) min. do ich pojemności użytkowej tj. w każdy OPD po 500TB.
   1. Dostarczone urządzenia muszą oferować przestrzeń min. 500TB (1TB=1000GB) netto (powierzchni użytkowej na której będą zapisywane archiwalne kopie zapasowe) bez uwzględniania redukcji danych (deduplikacji i/lub kompresji) oraz już po uwzględnieniu wszelkich mechanizmów zabezpieczenia danych (RAID, przestrzeń na bazę danych, system operacyjny itp.). Wymagana jest skalowalność do minimum 2PB netto.
9. Wymagane jest dostarczenie urządzeń i licencji, pozwalających na wykonywanie kopii zapasowych w OPS1 i OPS2 (z deduplikacją i kompresją) min. do ich pojemności użytkowej tj. każdy OPS po 120TB.
   1. Musi istnieć możliwość rozbudowy do 170TB pojemności użytkowej
10. Dostarczone urządzenia i elementy składowe tj. procesory, pamięci RAM, kontrolery RAID, dyski, zasilacze oraz inne muszą być tak wyskalowane, aby zapewnić opisaną w części serwerów kopii zapasowych wydajność dla komponentów programowych w tym i archiwów zgodnie z zaleceniami producentów tych platform
    1. Aby w razie ewentualnej rozbudowy zasobów dyskowych (pojemności użytkowej dysków dla kopii zapasowych) nie była konieczna wymiana lub rozbudowa podzespołów sprzętowych w klastrze oferowanych serwerów.

## Wymagania wdrożeniowe

Wymagania w zakresie prac wdrożeniowych realizowanych przez Wykonawcę w ramach przedmiotu zamówienia:

1. Wykonanie szczegółowego projektu architektury infrastruktury obliczeniowej (Projekt Techniczny Infrastruktury HLD, i LLD) i uzyskanie zgody Zamawiającego na realizację
2. Dostarczenie sprzętu do wyznaczonych przez Zamawiającego Kolokacji
3. Zamontowanie i uruchomienie sprzętu w wyznaczonych szafach serwerowych
4. Konfiguracja Systemu i Komponentów
5. Podłączenie Systemu do infrastruktury OSE w OPD i ROPD do posiadanych przez Zamawiającego przełączników QFX Juniper zgodnie z projektem
6. Instalacja platformy wirtualizacyjnej wraz z niezbędnymi (wymaganymi) modułami
7. Instalacja platformy wirtualizacji sieci SDN wraz z niezbędnymi (wymaganymi) modułami
8. Instalacja systemu kopii zapasowych i przechowywania archiwum wraz z niezbędnymi (wymaganymi) modułami
9. Instalacja systemu pamięci obiektowej wraz z niezbędnymi (wymaganymi) modułami
10. Uruchomienie i konfiguracja na potrzeby OSE platformy wirtualizacyjnej wraz z niezbędnymi (wymaganymi) modułami
11. Uruchomienie i konfiguracja na potrzeby OSE platformy wirtualizacji sieci SDN wraz z niezbędnymi (wymaganymi) modułami
12. Uruchomienie i konfiguracja na potrzeby OSE systemu kopii zapasowych i przechowywania archiwum
13. Uruchomienie i konfiguracja na potrzeby OSE pamięci obiektowej
14. Integracja systemów kopii zapasowych i przechowywania archiwum z platformą wirtualizacyjną
15. Integracja pamięci obiektowej z siecią OSE
16. Konfiguracja monitorowania i zarządzania infrastrukturą obliczeniową
17. Przeprowadzenie testów i audytu konfiguracji sprzętu i platformy
18. Integracja z siecią OSE infrastruktury obliczeniowej zgodnie z Projektem Technicznym HLD
19. Przeprowadzenie instruktaży dla pracowników Zamawiającego, zgodnie z wymaganiami opisanymi w załączniku "Zakres Instruktaży"
20. Dostosowanie architektury Systemu do przedstawionych przez Zamawiającego założeń bezpieczeństwa opartych na elementach CWB. Zamawiający dostosuje system CWB do tych założeń.
21. Opracowanie podłączenia sieci SDN do sieci OSE w zakresie kontroli ruchu północ-południe i wschód-zachód
22. Opracowanie szczegółowego planuj kontroli ruchu do i z całego Systemu, obejmującego urządzenia i oprogramowanie zarządzające
23. Przeprowadzenie testów odbiorczych Systemu
24. Opracowanie szczegółowej dokumentacji Systemu stanu docelowego

### Zakres testów weryfikacyjnych

Wymagania w zakresie realizacji testów odbiorczych realizowanych przez Wykonawcę w ramach przedmiotu zamówienia, weryfikowanych przez Zamawiającego (testy przygotowuje Wykonawca):

1. Test dostępności danych w klastrze SDS-HCI.
   1. Odporność na Awarie klastra: wyłączenie jednego serwera.
   2. Awaria klastra: wyłączenie dwóch serwerów.
2. Test dostępności danych w klastrze SDS-HCI.
   1. Odporność na Awarie dysku: wyjęcie jednego dysku.
3. Test auto przełączanie VM w klastrze niezawodnościowym Compute-SDS HCI.
   1. Odporność na awarię serwera w klastrze: wyłączenie jednego serwera z usługami (VM), weryfikacja automatycznego przywrócenia dostępności usługi (VM) na inny serwer
4. Test automatycznego przełączania usługi w przypadku awarii OPD (usługa składająca się 3 maszyn VM) między OPD (z OPD 1 do OPD2).
   1. Scenariusz testu: Awaria klastra z usługami (3xVM)
   2. Weryfikacja procesu przywracania dostępności usługi w drugim OPD, obejmujący proces uruchomienia (3xVM), zapewnienia sieci i rutingu: test dostępności usługi IP w sieci OSE udostępnionej z drugiego OPD.
   3. Weryfikacja czasu przywrócenia usługi w drugim OPD, nie więcej jak 1 godzina dla wymaganego testu
5. Test mikro-segmentacji VM w środowisku wirtualnym.
   1. Opis testu weryfikacja kontroli ruchu L3-L4 w jednym segmencie L2 dla ruchu IP między VM – VM
   2. Test wykonany dla dwóch VM pracujących na jednym serwerze
   3. Test wykonany dla dwóch VM pracujących na dwóch serwerach
6. Test wydajności w komunikacji VM-VM w raz z mikro segmentacją
   1. Uruchomiona kontrolą ruchu IP L3-L4 weryfikacja między VM
7. Test przepływności między VM-VM, weryfikacja wydajności na poziomie do 9Gbps dla komunikacji TCP/IP
8. Test backupu w środowisku OPD i ROPD.
   1. Wykonanie i otworzenie backupu w OPD i ROPD
9. Test wydajności zapis/odczyt z macierzy obiektowej
10. Testy funkcjonalne macierzy obiektowej:
    1. Uruchamianie i zatrzymywanie urządzeń.
    2. Symulacja awarii pojedynczego węzła.
    3. Symulacja awarii pojedynczego portu LAN.
    4. Symulacja awarii pojedynczego dysku.
    5. Symulacja awarii jednego z zasilaczy w węźle.
    6. Test Wydajności Odczyt i Zapis dla S3 i NFS
11. Test przełączania klastra macierzy obiektowej i dostępności danych
    1. Wyłączenie macierzy obiektowej w węźle OPD1, aktywne macierze obiektowe w węzłach OPD2 i OPD3
    2. Wyłączenie macierzy obiektowej w węźle OPD2, aktywne macierze obiektowe w węzłach OPD1 i OPD3
    3. Wyłączenie macierzy obiektowej w węźle OPD3, aktywne macierze obiektowe w węzłach OPD1 i OPD2
12. Testy środowiskowe całości rozwiązania obejmują:
13. Symulacja awarii jednego z torów zasilania dla zasilaczy w urządzeniach.
14. Symulacja awarii sieci LAN poprzez wyłączenie portów komunikacyjnych LAN
15. Awaria całego ośrodka ODP (Wyłączenie urządzeń)
16. Awaria całego ośrodka ROPD (Wyłączenie urządzeń)
17. Skasowanie usług w OPD i ROPD i odtworzenie z ostatniej Kopii zapasowej

### Zakres dokumentacji powdrożeniowej

Wymagania w zakresie dokumentacji dostarczonej przez Wykonawcę w ramach przedmiotu zamówienia:

1. Dostarczenie dokumentacji poszczególnych modułów i dokumentacji rozwiązań technologicznych, w postaci papierowej, elektronicznej lub dostępu do zasobów elektronicznych producenta na stronie WWW przez okres gwarancji.
2. Dokumentacja powykonawcza całego Systemu w zakresie administracji, procedur eksploatacyjnych i awaryjnych.
3. Konfiguracja elementów infrastruktury. Konfiguracja musi obejmować wszystkie elementy wdrożone, zainstalowane w ramach budowy Systemu. Przykładowy zestaw wymaganych danych konfiguracyjnych:
   1. model urządzenia, parametry sprzętowe (np. kontrolery, półki dyskowe, dyski, switche, wkładki, itp.), konfigurację macierzy (grupy dyskowe, zasoby dyskowe, itp.), sposób podłączenia do infrastruktury Zamawiającego.
   2. Schemat infrastruktury wraz z opisem.
   3. Licencje dla dostarczonych elementów infrastruktury.
   4. Informacje o ograniczeniach technologicznych (ilość dysków, rozmiar cache, itp.) dostarczonych elementów infrastruktury
   5. Raport z przeprowadzonych testów.
   6. Procedury utrzymaniowe dla poszczególnych komponentów.
   7. Procedury aktualizacji oprogramowania wbudowanego.
   8. Procedury zgłaszania problemów do serwisu.
4. Opisanie modeli udostępniania usług do sieci wew. OSE i zew. Internet przy zastosowaniu posiadanego bloku CWB (NGFirewall Data Center-FortiGate, LB/WAF-F5 Networks)
5. Opisanie procedur i modelu planowanych przełączeń w zakresie dostępności usług w obu OPD1-2.
6. Opracowanie założeń i procedur do kontroli ruchu wschód-zachód (SDN) i północ-południe dla NGFW z zakresie udostępniania i budowy usług w Systemie

### Zakres instruktaży

Wymaganie jest przeprowadzenie przez Wykonawcę instruktaży w zakresie:

1. Dostarczonego i wdrożonego Systemu
   1. Omówienie komponentów rozwiązania
   2. Omówienie funkcjonalności rozwiązania
   3. Min. 3 dni
   4. Do 10 osób
2. Komponentu Platforma wirtualizacyjna HCI
   1. Omówienie komponentów HCI
   2. Omówienie funkcjonalności HCI
   3. Praktyczne zadania w formie ćwiczeń z typowych zadań administracyjnych min.:
      1. Konfiguracja elementów HCI
      2. Migracja maszyn wirtualnych
      3. Aktualizacja oprogramowania HCI
      4. Monitorowania zasobów HCI
   4. Min. 5 dni
   5. Do 5 osób
3. Komponentu SDN
   1. Omówienie komponentu SDN
   2. Omówienie funkcjonalności SDN
   3. Praktyczne zadania w formie ćwiczeń z typowych zadań administracyjnych min.:
      1. Konfiguracja elementów SDN
      2. Mikrosegmentacja
      3. Monitorowanie SDN
   4. Projektowanie usług w SDN
   5. Zaawansowana diagnostyka
   6. Min. 3 x 5 dni
   7. Do 5 osób
4. Komponentu zabezpieczania ciągłości działania centrów danych
   1. omówienie architektury z wysoką dostępnością usług w centrach danych
   2. omówienie funkcjonalności oprogramowania
   3. omówienie sposób przywracania centrów danych po awarii
   4. Praktyczne zadania w formie ćwiczeń z typowych zadań administracyjnych
   5. Min. 2 dni
   6. Do 5 osób
5. Komponentu Orkiestracji i Automatyzacji
   1. Omówienie komponentów Orkiestracji i Automatyzacji
   2. Omówienie funkcjonalności Orkiestracji i Automatyzacji
   3. Omówienie zaawansowanych możliwości oprogramowania
   4. Praktyczne zadania w formie ćwiczeń z typowych zadań administracyjnych
   5. Min. 2 x 5 dni
   6. Do 5 osób
6. Komponentu kopii zapasowych i archiwum
   1. Omówienie komponentu systemu kopii zapasowych i archiwum
   2. Omówienie funkcjonalności systemu kopii zapasowych i archiwum
   3. Praktyczne zadania w formie ćwiczeń z typowych zadań administracyjnych
   4. Min. 2 x 5 dni
   5. Do 5 osób
7. Komponentu Macierz obiektowa
   1. Omówienie komponentu Macierz obiektowa
   2. Omówienie funkcjonalności Komponentu Macierz obiektowa
   3. Praktyczne zadania w formie ćwiczeń z typowych zadań administracyjnych
   4. Min. 5 dni
   5. Do 5 osób
8. Komponentu Monitorowania systemu
   1. Omówienie Komponentu Monitorowania Systemu
   2. Omówienie funkcjonalności Komponentu Monitorowania Systemu
   3. Praktyczne zadania w formie ćwiczeń z typowych zadań administracyjnych
      1. Monitorowania infrastruktury
      2. Diagnostyka problemów
   4. Min. 2 dni
   5. Do 15 osób

Ogólne wymagania na instruktaży:

1. Harmonogram oraz zakres poszczególnych instruktaży będzie uzgadniany i akceptowany przez Zamawiającego
2. Jeden dzień instruktażu obejmuje 8 godzin nauki (w tym przerwa obiadowa)
3. Sale szkoleniowe wyposażone będą w niezbędny sprzęt, w tym komputery dla uczestników do ćwiczeń praktycznych
4. Materiały w języku polskim lub angielskim
5. W przypadku instruktażu poza Warszawą, wykonawca pokrywa koszty transportu, zakwaterowania i wyżywienia pracowników Zamawiającego

W trakcie instruktaży Wykonawca zapewnia posiłki na swój koszt

### Gwarancja

Wymagania gwarancyjne:

1. Całość dostarczonego sprzętu i oprogramowania musi być objęta gwarancją przez okres minimum 60 miesięcy.
2. Oprogramowanie musi być dostarczone ze wsparciem technicznym na nie
   1. Zamawiający będzie mógł otrzymywać i używać aktualizacji dostarczonego oprogramowania w ramach otrzymanej wersji, przez okres umowy
3. Czas reakcji na zgłoszony problem (rozumiany jako podjęcie działań diagnostycznych i kontakt ze zgłaszającym) nie może przekroczyć 4 godzin. Usunięcie usterki (naprawa lub wymiana wadliwego podzespołu lub urządzenia) ma zostać wykonana w przeciągu 1 dnia od momentu zgłoszenia usterki.
4. Wykonawca ma obowiązek przyjmowania zgłoszeń serwisowych przez telefon (w godzinach pracy Zamawiającego), fax, e-mail lub WWW (przez całą dobę).
5. Wykonawca ma udostępnić pojedynczy punkt przyjmowania zgłoszeń serwisowych dla wszystkich oferowanych Komponentów Systemu.
6. W przypadku sprzętu, dla którego jest wymagany dłuższy czas naprawy, Zamawiający dopuszcza podstawienie na czas naprawy sprzętu o nie gorszych parametrach funkcjonalnych. Naprawa w takim przypadku nie może przekroczyć 5 dni od momentu zgłoszenia usterki.
7. wykonywanie przez Zamawiającego nieograniczonej ilości zgłoszeń serwisowych
8. możliwość zapotrzebowania przez Zamawiającego wsparcia zdalnego
9. dostęp dla Zamawiającego do materiałów producenta oprogramowania, do którego oferowane jest przedmiotowe wsparcie, takich jak: techniczna dokumentacja, internetowa baza wiedzy, forum internetowe
10. dostęp dla Zamawiającego do poprawek i uaktualnień oprogramowania objętego usługą wsparcia serwisowego
11. Usługa wsparcia serwisowego musi spełniać poniższe cechy w zakresie mocy obliczeniowej:
    1. dostęp do portalu internetowego umożliwiającego zarządzanie posiadanymi przez Zamawiającego licencjami, utworzenie zgłoszenia serwisowego oraz generowania kluczy licencyjnych do różnych wersji numerycznych posiadanego oprogramowania
    2. Dostęp dla Zamawiającego do autoryzowanego przez producenta oprogramowania narzędzia pozwalającego na automatyczne zbieranie danych o statusie i działaniu produktów o funkcjonalnościach minimum: wirtualizacji mocy obliczeniowej, wirtualizacji sieci komputerowej oraz wirtualizacji przestrzeni dyskowej
    3. Umożliwienie Zamawiającemu instalacji narzędzia w formie wirtualnego appliance, które ma możliwość przesyłania zaszyfrowanych (TLS minimum 1.2) danych o konfiguracji, logach i wydajności, dla funkcjonalności minimum: wirtualizacji mocy obliczeniowej, wirtualizacji sieci komputerowej oraz wirtualizacji przestrzeni dyskowej, w trybie automatycznym do narzędzi analitycznych producenta oprogramowania. W rezultacie analizy przekazywanych informacji Zamawiający otrzyma możliwe do odczytu na portalu internetowym, wyniki analizy wraz z rekomendacjami do wykonania w celu poprawy funkcjonowania posiadanego środowiska opartego na oprogramowaniu, do którego wsparcia dotyczy przedmiotowe postępowanie przetargowe.
    4. umożliwienie Zamawiającemu używania asystenta logów odpowiadającego za eliminację czasochłonnego procesu ręcznego gromadzenia i przesyłania plików dziennika logów w ramach zgłoszeń serwisowych, poprzez automatyczne wysyłanie logów serwisowych, dla funkcjonalności minimum: wirtualizacji mocy obliczeniowej, wirtualizacji sieci komputerowej oraz wirtualizacji przestrzeni dyskowej, w przypadku utworzenia wcześniej zgłoszeń serwisowych
12. Wykonawca zapewni zdalne wsparcie techniczne (poprzez platformę współpracy (typu Skype/Webex/TeamViewer), telefon lub e-mail) w zakresie rozwiązywania problemów z konfiguracją i użytkowaniem oprogramowania.

### Okres stabilizacji Systemu

W Okresie Stabilizacji zostanie zweryfikowana poprawność działania dostarczonego i uruchomionego Systemu w zakresie:

1. stabilnej pracy Systemu,
2. zgodności z wymaganiami Zamawiającego,
3. usuwania Problemów i wprowadzania niezbędnych korekt

Zakres i zadania Wykonawcy w Okresie Stabilizacji:

1. okres stabilizacji będzie trwał do 4 miesięcy, z możliwością skrócenia do 3 miesięcy w przypadku jeżeli w okresie 2 tygodni przed zakończeniem trzymiesięcznego okresu nie wystąpią żadne poważne awarie,
2. jeden inżynier dostępny przez 8 godzin dziennie, w dni robocze zdalnie lub lokalnie w zależności o potrzeb
3. analiza i sprawdzanie pracy Systemu
4. testowanie i weryfikacja poszczególnych elementów Systemu
5. usuwanie Problemów, zgodnie z poziomem świadczenia usług w okresie Gwarancji
6. poprawa konfiguracji Systemu
7. zmiana w konfiguracji Systemu
8. aktualizacja Dokumentacji
9. udzielanie Zamawiającemu szczegółowych informacji na temat działania Systemu
10. zadania muszą być planowane i akceptowane przez Zamawiającego
11. raportowanie wdrożonych zmian, zaistniałych problemów i innych elementów mających wpływ na działanie Systemu
12. wsparcie merytoryczne i techniczne w procesie planowania i migracji usług do dostarczonego Systemu
13. wsparcie techniczne i merytoryczne przy wykonywaniu testu przełączania usług między OPD1 i OPD2. Planowane jest minimum jedno wykonanie testu weryfikującego poprawność pracy Systemu i ciągłości świadczenia usług

### Okres utrzymania

W Okresie utrzymania, trwającym 6 miesięcy od zakończenia okresu stabilizacji, świadczone będzie doraźne wsparcie dla administratorów w sposób zdalny, w zakresie:

1. min. 8 godzin tygodniowo,
2. minimum jeden inżynier świadczący zdalne wsparcie
3. wsparcie administratorów przy analizie pracy Systemu
4. wsparcie administratorów przy diagnostyce elementów Systemu
5. wsparcie administratorów przy usuwaniu Problemów, zgodnie z poziomem świadczenia usług w okresie Gwarancji
6. wsparcie administratorów przy zmianach konfiguracji Systemu
7. raportowanie zrealizowanych zadań w ramach wsparcia w okresie utrzymania, w cyklu miesięcznym
8. wsparcie techniczne i merytoryczne przy wykonywaniu testu przełączania usług między OPD1 i OPD2. Planowane jest minimum jedno testowe wykonane przełączenie usług weryfikującego poprawność pracy Systemu i ciągłości świadczenia usług