**Załącznik numer 8 do OPZ - Wirtualizacja Cloud SDN Zarządzanie**

# Informacje wstępne

### W podmiotach o numerach porządkowych 1, 4, 5, 6, 7, 8, 9, 10, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 23, 60 Zamawiający dysponuje infrastrukturą konieczną do zaadoptowania na potrzeby Projektu (zestawienie posiadanej infrastruktury zawarte jest w osobnym załączniku do OPZ). W każdym z tych podmiotów Zamawiający dysponuje licencjami „VMware vCenter Server 6 Essentials” i „VMware vSphere Essentials Plus”. Spełnienie wymagań opisanych jak dla części lokalnej, będzie wymagało upgrade’u, lub wymiany tych licencji. Jeśli w związku z wymianą licencji oprogramowania wirtualizacyjnego wystąpi konieczność zmigrowania ustawień istniejącego środowiska i wirtualnych maszyn, to Wykonawca wykona migrację konfiguracji całego istniejącego środowiska łącznie z migracją maszyn wirtualnych na nową platformę.

### W podmiotach 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58 Zamawiający nie dysponuje infrastrukturą i wymaga dostarczenia nowych licencji odpowiednich do oferowanego sprzętu i spełniających wymagania jak dla części lokalnej.

### W lokalizacji 60 dla nowo dostarczonego sprzętu Zamawiający wymaga dostarczenia nowych licencji odpowiednich do oferowanego sprzętu i spełniających wymagania jak dla części regionalnej.

# Wirtualizacja zasobów sprzętowych – część lokalna

## Wymagania podstawowe

### Warstwa wirtualizacyjna musi być zainstalowania bezpośrednio na sprzęcie fizycznym bez dodatkowych pośredniczących systemów operacyjnych.

### Rozwiązanie musi zapewnić możliwość obsługi wielu instancji systemów operacyjnych na jednym serwerze fizycznym oraz na klastrze serwerów fizycznych.

### Oprogramowanie wirtualizacyjne musi być dostarczone z licencjami obsługującymi wszystkie fizyczne procesory dostępne w dostarczonych fizycznych serwerach bez względu na liczbę rdzeni dostępnych w procesorach.

### Oprogramowanie do wirtualizacji musi zapewnić możliwość wykonywania kopii migawkowych instancji wirtualnych systemów operacyjnych na potrzeby tworzenia kopii zapasowych bez przerywania ich pracy z możliwością wskazania konieczności zachowania stanu pamięci pracującej maszyny wirtualnej.

### Rozwiązanie musi zapewniać mechanizm bezpiecznego, bezprzerwowego i automatycznego uaktualniania warstwy wirtualizacyjnej (wliczając zarówno poprawki bezpieczeństwa jak i zmianę jej wersji) bez potrzeby wyłączania wirtualnych maszyn.

### Rozwiązanie musi posiadać co najmniej 2 niezależne mechanizmy wzajemnej komunikacji między serwerami oraz z serwerem zarządzającym, gwarantujące właściwe działanie mechanizmów wysokiej dostępności na wypadek izolacji sieciowej serwerów fizycznych lub partycjonowania sieci.

### Decyzja o próbie przywrócenia funkcjonalności maszyny wirtualnej w przypadku awarii lub niedostępności serwera fizycznego powinna być podejmowana automatycznie, jednak musi istnieć możliwość określenia przez administratora czasu po jakim taka decyzja jest wykonywana.

### Rozwiązanie musi zapewnić mechanizm do bezpiecznej automatycznej kopii zapasowej i odtwarzania wskazanych maszyn wirtualnych i ich zasobów dyskowych.

### Oprogramowanie do wirtualizacji musi umożliwić wykonywanie kopii zapasowych instancji systemów operacyjnych oraz ich odtworzenia w możliwie najkrótszym czasie.

### Rozwiązanie musi posiadać wbudowany interfejs programistyczny (API) zapewniający pełną integrację zewnętrznych rozwiązań wykonywania kopii zapasowych z istniejącymi mechanizmami warstwy wirtualizacyjnej.

### Rozwiązanie musi umożliwiać konfigurację wysokiej dostępności (HA) dla każdego swojego komponentu w celu unikania awarii pojedynczego elementu.

### Rozwiązanie musi zapewniać mechanizm migracji wskazanych maszyn wirtualnych w obrębie klastra serwerów fizycznych bez konieczności wyłączania wirtualnych maszyn.

### System musi posiadać funkcjonalność wirtualnego przełącznika (virtual switch) umożliwiającego tworzenie sieci wirtualnej w obszarze hosta i pozwalającego połączyć maszyny wirtualne w obszarze jednego hosta, a także na zewnątrz sieci fizycznej. Pojedynczy przełącznik wirtualny powinien mieć możliwość konfiguracji do 4000 portów.

### Pojedynczy wirtualny przełącznik musi posiadać możliwość przyłączania do niego co najmniej dwóch fizycznych kart sieciowych, aby zapewnić bezpieczeństwo połączenia ethernetowego w razie awarii karty sieciowej.

### Oprogramowanie do wirtualizacji musi obsługiwać przełączenie ścieżek LAN (bez utraty komunikacji) w przypadku awarii jednej ze ścieżek.

### Wirtualne przełączniki muszą obsługiwać wirtualne sieci lokalne (VLAN).

### Rozwiązanie musi umożliwiać wykorzystanie technologii 10GbE w tym agregację połączeń fizycznych.

### Rozwiązanie musi umożliwiać rozbudowę infrastruktury o nowe usługi bez spadku wydajności i dostępności usług uprzednio uruchomionych.

### Oprogramowanie zarządzające musi posiadać możliwość przydzielania i konfiguracji uprawnień z możliwością integracji z usługami katalogowymi (w tym - z uwagi na wykorzystywanie przez Zamawiającego - Microsoft Active Directory, Open LDAP).

### Rozwiązanie musi zapewnić możliwość zdefiniowania alertów informujących o przekroczeniu wartości progowych.

## Wymagania dotyczące hostów fizycznych

### Oprogramowanie do wirtualizacji zainstalowane na serwerze fizycznym musi potrafić obsłużyć i wykorzystać wszystkie dostępne procesory fizyczne niezależnie od liczby rdzeni oraz do 12TB pamięci fizycznej RAM.

### System musi mieć możliwość uruchamiania fizycznych serwerów z centralnie przygotowanego obrazu poprzez protokół PXE.

## Wymagania dotyczące maszyn wirtualnych

### Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych z maksymalną liczbą co najmniej 128 wirtualnych procesorów (vCPU).

### Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych z możliwością przydzielenia do 4TB pamięci operacyjnej RAM.

### Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych, z których każda może mieć do 10 wirtualnych kart sieciowych.

### Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych z których każda może mieć do 60 wirtualnych dysków.

### Rozwiązanie musi umożliwiać (łącznie dla wszystkich maszyn wirtualnych) przydzielenie większej ilości pamięci RAM dla maszyn wirtualnych niż fizyczne zasoby RAM serwera.

### Rozwiązanie musi umożliwiać przydzielenie większej ilości zasobów obliczeniowych (CPU) dla maszyn wirtualnych niż fizyczne zasoby procesorowe serwera.

### Rozwiązanie musi umożliwiać udostępnienie maszynie wirtualnej większej ilości zasobów dyskowych niż jest fizycznie zarezerwowane na zasobach dyskowych.

### Oprogramowanie do wirtualizacji musi zapewniać możliwość stworzenia dysku maszyny wirtualnej o wielkości co najmniej 62 TB.

### Czas planowanego przestoju usług związanych z koniecznością prac serwisowych (np. rekonfiguracja serwerów, macierzy, switchy) musi być ograniczony do minimum. Konieczna jest możliwość przenoszenia maszyn wirtualnych pomiędzy serwerami fizycznymi bez przerywania pracy usług.

### Rozwiązanie musi mieć możliwość przenoszenia maszyn wirtualnych w czasie ich pracy pomiędzy serwerami fizycznymi.

### Musi zostać zapewniona odpowiednia redundancja i taki mechanizm wysokiej dostępności (HA), aby w przypadku awarii lub niedostępności serwera fizycznego, wybrane przez administratora i przypisane do niedostępnego serwera wirtualne maszyny zostały automatycznie uruchomione na innych serwerach z zainstalowanym oprogramowaniem wirtualizacyjnym.

### W przypadku awarii lub niedostępności serwera fizycznego, po ustabilizowaniu środowiska, maszyny wirtualne uruchomione w wyniku awarii na pozostałych serwerach fizycznych muszą mieć dostęp do wszystkich swoich dysków i danych dostępnych przed awarią.

### Oprogramowanie do wirtualizacji musi zapewnić możliwość klonowania maszyn wirtualnych wraz z ich pełną konfiguracją i danymi.

### Rozwiązanie musi zapewniać możliwość dodawania zasobów w czasie pracy maszyny wirtualnej, w szczególności w zakresie ilości procesorów, pamięci operacyjnej i przestrzeni dyskowej.

### System musi umożliwiać udostępnianie pojedynczego urządzenia fizycznego jako logicznie separowane wirtualne urządzenie dedykowane dla poszczególnych maszyn wirtualnych.

### Musi zostać zapewniona odpowiednia redundancja i nadmiarowość zasobów tak by w przypadku awarii np. serwera fizycznego usługi na nim świadczone zostały automatycznie przełączone na inne serwery infrastruktury.

### Rozwiązanie musi umożliwiać łatwe i szybkie ponowne uruchomienie systemów/usług w przypadku awarii poszczególnych elementów infrastruktury bez utraty danych.

### Rozwiązanie musi zapewnić bezpieczeństwo danych mimo poważnego uszkodzenia lub utraty sprzętu lub oprogramowania.

### Dostarczone oprogramowanie musi zapewniać możliwość wirtualizacji dla wszystkich dostarczonych w ramach postępowania serwerów.

### System musi wspierać mechanizmy zaawansowanego uwierzytelniania do systemu operacyjnego wirtualnej maszyny za pomocą technologii Smart Card Reader.

# Wirtualizacja zasobów sprzętowych – część regionalna

## Wymagania jak dla części lokalnej

### Oprogramowanie związane z wirtualizacją zasobów sprzętowych musi spełniać wszystkie wymagania jak dla części lokalnej oraz wymagania dodatkowe opisane poniżej.

## Dodatkowe wymagania

### Rozwiązanie musi zapewnić mechanizm automatycznego równoważenia obciążenia CPU/MEM hostów fizycznych pracujących jako platforma dla infrastruktury wirtualnej.

### Rozwiązanie musi zapewniać mechanizm przenoszenia wirtualnych dysków twardych maszyn wirtualnych pomiędzy różnymi zasobami dyskowymi w czasie pracy maszyn wirtualnych, bez konieczności ich wyłączania.

### Rozwiązanie musi umożliwiać utworzenie jednorodnego, wirtualnego przełącznika sieciowego, rozproszonego na wszystkie hosty platformy wirtualizacyjnej. Przełącznik taki musi zapewniać możliwość konfiguracji parametrów sieciowych maszyny wirtualnej z granulacją na poziomie portu tego przełącznika. Pojedyncza maszyna wirtualna musi mieć możliwość wykorzystania jednego lub wielu portów przełącznika z niezależną od siebie konfiguracją.

### System musi mieć wbudowany mechanizm kontrolowania i monitorowania ruchu sieciowego oraz ustalania priorytetów w zależności od jego rodzaju na poziomie konkretnych maszyn wirtualnych.

### Rozwiązanie powinno posiadać proaktywnie działający mechanizm, który wymigruje wirtualne maszyny po wykryciu potencjalnego problemu z serwerem fizycznym, zanim on ulegnie awarii.

### Oprogramowanie do wirtualizacji musi obsługiwać przełączenie ścieżek SAN (bez utraty komunikacji) w przypadku awarii jednej ze ścieżek.

### System musi mieć możliwość grupowania pamięci masowych o podobnych parametrach w grupy i przydzielania ich do wirtualnych maszyn zgodnie z ustaloną przez administratora polityką.

### System musi mieć możliwość równoważenia obciążenia i zajętości pamięci masowych wraz z możliwością przenoszenia plików wirtualnych maszyn z bardziej zajętych na mniej zajęte przestrzenie dyskowe lub/i z przestrzeni dyskowych bardziej obciążonych operacjami I/O na mniej obciążone.

### System musi umożliwiać uruchamianie kontenerów w wirtualnych maszynach.

### System musi zapewniać mechanizm weryfikujący integralność komponentów systemowych i plików hosta wirtualizującego i wirtualnej maszyny podczas ich uruchamiania (ochrona systemu hypervisor i OS wirtualnej maszyny na wypadek sfałszowania lub podmiany).

### Rozwiązanie musi umożliwiać wykorzystanie technologii 10GbE w tym agregację połączeń fizycznych do minimalizacji czasu przenoszenia maszyny wirtualnej pomiędzy serwerami fizycznymi.

### Rozwiązanie musi zapewnić możliwość bieżącego monitorowania wykorzystania zasobów fizycznych infrastruktury wirtualnej (np. wykorzystanie procesorów, pamięci RAM, wykorzystanie przestrzeni na dyskach/wolumenach) oraz przechowywać i wyświetlać dane co najmniej sprzed roku.

### Rozwiązanie musi mieć możliwość przenoszenia maszyn wirtualnych w czasie ich pracy pomiędzy serwerami fizycznymi, pamięciami masowymi niezależnie od dostępności współdzielonej przestrzeni dyskowej, różnymi rodzajami wirtualnych przełączników sieciowych.

### Rozwiązanie musi umożliwiać konfiguracje trybu wysokiej dostępności HA dla każdego swojego komponentu w celu uniknięcia awarii pojedynczego elementu.

### Oprogramowanie do wirtualizacji musi być wspierane przez producenta oferowanego rozwiązania do wirtualizacji sieci oraz chmury prywatnej.

### Platforma będzie w stanie zbierać informacje na temat wydajności pod kątem zarządzania pojemnością.

### Platforma musi przewidywać trendy związane z pojemnością środowiska wirtualizacji.

### Platforma musi posiadać moduł odpowiedzialny za analizę środowiska pod kątem optymalizacji wykorzystania zasobów (CPU, RAM, HDD).

### Platforma będzie w stanie tworzyć personalizowane zbiory (możliwość grupowania obiektów w logiczne zbiory), dla których będzie istniała możliwość informowania o alertach, pojemności, ryzykach zgromadzonych w zbiorze obiektach. Obiekty mogą pochodzić z różnych Data Center objętych tym rozwiązaniem.

### Platforma będzie w stanie monitorować dostarczoną infrastrukturę wirtualizacji.

### Platforma w obrębie monitorowania będzie posiadała rozwiązanie generowania alertów na podstawie szeregu anomalii i symptomów, a nie pojedynczych monitorowanych metryk.

### Platforma będzie alarmowała o wykryciu sytuacji nietypowych (np. odmienne od typowego zwiększone obciążenie elementu platformy wirtualnej).

### Możliwość uruchamiania automatycznych zadań (w tym modyfikujących parametry maszyn wirtualnych) w zależności od aktualnych alarmów, ostrzeżeń, powiadomień, obciążenia.

### Możliwość dowolnego konfigurowania alertów w środowisku dla różnych grup odbiorców (także z użyciem alertów stworzonych we własnym zakresie).

### Platforma będzie dostarczała informacji na temat rekomendowanych działań mających na celu utrzymanie środowiska wirtualizacji w sprawności.

### Platforma będzie w stanie dostarczać analizę głównego problemu oraz rekomendacji z nimi związanych.

### Platforma powinna umożliwiać integrację z zewnętrznym kolektorem logów i zdarzeń.

### System musi wizualizować online obciążenie środowiska wirtualnego wraz z tzw. funkcjonalnością „drill down”.

### System musi posiadać funkcjonalność dashboardów.

### System powinien automatycznie tworzyć linie bazowe określające typowe zachowanie elementów systemu w danym czasie.

### System będzie miał zaimplementowane mechanizmy planowania pojemności środowiska.

### System powinien dokonywać predykcji wykorzystania zasobów maszyn fizycznych na podstawie analiz zebranych danych.

### System powinien umożliwiać przeglądanie linii trendu monitorowanych parametrów.

### System musi umożliwiać tworzenie raportów pojemnościowych dla monitorowanego środowiska, zarówno dla urządzeń fizycznych jak i wirtualnych.

### System musi umożliwiać monitorowanie w czasie rzeczywistym.

### System musi zbierać oraz prezentować w formie wykresów oraz tabelaryczno-tekstowej zbiorczo oraz osobno dla każdego OS aktualne i historyczne dane dotyczące utylizacji CPU, RAM, HDD oraz interfejsów sieciowych.

### System musi umożliwiać przeglądanie wszystkich zbieranych statystyk w dowolnie wybranym zakresie czasu w postaci wykresów.

### System powinien umożliwiać szczegółowe monitorowanie komponentów serwerów fizycznych (CPU, sieć, RAM, przestrzeń dyskowa).

### System musi wskazywać „wąskie gardła” a także umożliwiać definiowanie progów wydajności i pojemności w celu identyfikacji przypadków wąskich gardeł.

### Oprogramowanie musi automatycznie przeszukiwać składy danych w celu identyfikacji nadmiarowo przyznanych zasobów (CPU, RAM, HDD).

### System powinien pozwalać na odczyt wyświetlanych alarmów w środowisku wirtualnym.

### System powinien umożliwiać definiowanie alertów związanych z: zarządzaniem pojemnością, zarządzeniem wydajnością, anomaliami w środowisku, zarządzaniem dostępnością.

### System musi mieć możliwość realizacji funkcji automatycznego lub półautomatycznego równoważenia obciążenia serwerów fizycznych w obrębie klastra logicznego.

## Wirtualizacja warstwy sieciowej (SDN)

### Rozwiązaniem do wirtualizacji warstwy sieciowej należy objąć wszystkie urządzenia i systemy dostarczane dla części regionalnej.

### Rozwiązanie musi zapewnić bezpieczeństwo transmisji danych (filtracja pakietów) na poziomie hypervisora/wirtulanego interfejsu sieciowego (vNIC), 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.

### Rozwiązanie musi posiadać funkcję rozproszonego, stanowego firewall'a instalowanego w/na poziomie jądra wirtualizatora (Hypervisor) serwerów umożliwiający tworzenie polityk bezpieczeństwa w warstwach 2-4 modelu OSI. Nie dopuszcza się stosowania filtracji typu "reflexive".

### 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.

### Rozwiązanie musi umożliwiać wykorzystanie dynamicznych obiektów do tworzenia reguł polityk bezpieczeństwa.

### Rozwiązanie powinno umożliwiać natywną integrację z produktami firm trzecich oferującymi rozwiązania typu antywirus/antymalware w postaci bezagentowej, tj. instalowane na wirtualizatorze serwerów, ale poza wirtualną maszyną.

### Rozwiązanie powinno umożliwiać natywną integrację z produktami firm trzecich oferującymi rozwiązania typu Next Generation Firewall warstwy 7.

### Rozwiązanie musi umożliwiać przekierowanie wybranego ruchu L2 do systemów firm trzecich z obszaru bezpieczeństwa.

### Rozwiązanie musi zabezpieczać środowisko wirtualne przed nieautoryzowaną zmianą adresu IP wirtualnej maszyny, poprzez zablokowanie ruchu z i do wirtualnej maszyny po zmianie jej adresu IP.

### Oferowane rozwiązanie musi zapewnić funkcjonalność rozkładania/równoważenia ruchu – tj. load balancing działającą do warstwy 7 modelu ISO OSI.

### Rozwiązanie musi zapewniać następujące mechanizmy przywiązania sesji: adres źródłowy, cookie, SSL ID oraz JSessionID.

### W ramach inspekcji warstwy 7 rozwiązanie musi oferować funkcję blokowania URL.

### Rozwiązanie musi oferować możliwość wstrzykiwania nagłówka XFF (X-Fowarder-For).

### Funkcja Wirtualny Load Balancer musi być realizowana i w pełni zintegrowana z platformą do wirtualizacji sieci.

### Dostarczone oprogramowanie musi oferować możliwość budowy sieci komunikacyjnych (IP) oparciu o środowiska wirtualne.

### Oferowane oprogramowanie musi zapewniać funkcjonalność tworzenia wirtualnych sieci w sposób niezależny od topologii sieci fizycznej i używanych w obrębie tej sieci w protokołów sieciowych.

### Rozwiązanie musi posiadać funkcję rozproszonego, wirtualnego przełącznika instalowanego w jądrze wirtualizatora serwerów (Hypervisor), umożliwiający tworzenie logicznych segmentów sieci L2. Wirtualny przełącznik musi być wspierany bezpośrednio przez producenta wirtualizatora serwerów.

### Rozwiązanie musi posiadać funkcję rozproszonego, wirtualnego routera instalowanego w jądrze wirtualizatora serwerów (Hypervisor), zapewniającego funkcję bramy domyślnej dla środowiska maszyn wirtualnych. Brama domyślna musi działać w trybie rozproszonym. Przełączanie pakietów L3 musi odbywać się w obrębie fizycznego serwera, bez wynoszenia ruchu do fizycznych przełączników.

### Rozwiązanie musi posiadać możliwość kreowania segmentów sieci przy użyciu technologii VXLAN.

### Oferowane oprogramowanie musi zapewnić funkcjonalność łączenia (bridging) środowiska zwirtualizowanego opartego o technologię VXLAN oraz niezwirtualizowanego zdefiniowanego za pomocą technologii VLAN-ów.

### Oferowane oprogramowanie musi zapewnić funkcjonalność wirtualnego routera wspierającego protokoły BGP i OSPF.

### Rozwiązanie musi posiadać funkcję łączenia/bridge segmentów sieci L2 VLAN i VXLAN poprzez zastosowanie wirtualnej bramy/bridge.

### Rozwiązanie musi umożliwiać funkcję translacji adresów IP zarówno dla ruchu wychodzącego ze środowiska wirtualnego (SNAT) jak i przychodzącego (DNAT).

### Rozwiązanie musi posiadać funkcję serwera DHCP w celu dynamicznego nadawania adresów IP dla środowiska zwirtualizowanego.

### Oferowane oprogramowanie musi udostępniać funkcjonalność zarządzania poprzez ustandaryzowany interfejs tj. API.

### Oferowane rozwiązanie musi posiadać pełną wymaganą funkcjonalność zarówno funkcji bezpieczeństwa oraz funkcji sieciowych.

## Chmura prywatna

### Rozwiązaniem umożliwiającym budowę chmury prywatnej należy objąć wszystkie urządzenia i systemy dostarczane dla części regionalnej.

### Dostarczone licencje i oprogramowanie Chmury muszą umożliwiać zbudowanie chmury prywatnej.

### Licencje na oprogramowanie Chmury muszą być dopasowane do oferowanych zasobów sprzętowych i aplikacyjnych.

### Oprogramowanie Chmurowe musi umożliwiać zarządzanie zasobami obsługiwanej przez nie infrastruktury przetwarzania i przechowywania danych (części regionalnej) zorganizowanych w spójny katalog usług.

### Oprogramowanie realizujące funkcje chmury prywatnej musi umożliwiać dostarczenie infrastruktury jako usługi (ang. Infrasructure as a Service - IaaS).

### Oprogramowanie realizujące funkcje chmury prywatnej musi zawierać zestaw narzędzi do budowy i zarządzania prywatną chmurą obliczeniowa w formie IaaS (ang. Infrastructure as a Service).

### Funkcje wirtualizacji serwerów fizycznych musi realizować dostarczona w ramach tego przetargu platforma wirtualizacji zasobów sprzętowych części regionalnej.

### Oprogramowanie Chmurowe musi zostać zintegrowane, korzystać z oferowanych funkcjonalności i poprawnie współpracować z dostarczonym środowiskiem fizycznym, systemem wirtualizacji infrastruktury oraz systemem wirtualizacji warstwy sieciowej.

### Oprogramowanie Chmurowe musi mieć architekturę modułową.

### Oprogramowanie Chmurowe musi spełniać wymagania bez konieczności uzupełniania go o pisany samodzielnie przez Zamawiającego kod wykonywalny. Wszelkie dostosowania niezbędne do realizacji Chmury Prywatnej muszą zostać wykonane w ramach niniejszego zamówienia oraz udokumentowane.

### Oprogramowanie Chmurowe musi zapewniać zdefiniowanie wielu środowisk klienckich.

### Oprogramowanie Chmurowe musi zapewniać separację poszczególnych udostępnionych środowisk klienckich, w szczególności uniemożliwiać dostęp do obiektów zdefiniowanych w innych środowiskach klienckich.

### Oprogramowanie Chmurowe musi umożliwiać użytkownikom końcowym samodzielne zarządzanie zasobami przydzielonymi do środowiska klienckiego.

### Oprogramowanie Chmurowe musi posiadać mechanizm uwierzytelniania i autoryzacji zapewniający poufność i integralność danych i konfiguracji.

### Oprogramowanie Chmurowe musi umożliwiać uwierzytelnianie użytkowników zarówno w oparciu o konta domenowe jak i tworzone lokalnie w ramach Oprogramowania Chmurowego.

### Oprogramowanie Chmurowe musi umożliwiać definiowanie ról i przypisywanie im zdefiniowanych uprawnień (agregację uprawnień).

### Oprogramowanie Chmurowe musi umożliwiać delegowanie użytkownikom ról i uprawnień.

### Oprogramowanie Chmurowe musi umożliwiać nadanie uprawnień do poszczególnych zasobów, obszarów funkcjonalnych oraz zdefiniowanych operacji na obiektach.

### Oprogramowanie Chmurowe musi umożliwiać dynamiczną skalowalność i elastyczny przydział Zasobów, a w szczególności dodanie dodatkowych zasobów i dowolną ich dystrybucję pomiędzy wydzielonymi środowiskami klienckimi, z zachowaniem ciągłości działania środowiska.

### Udostępnianie zasobów w modelu IaaS powinno odbywać się automatycznie w zakresie zdefiniowanych przez Administratora zasobów do (tj. do udostępnienia zasobów nie jest konieczna ingerencja służb technicznych Zamawiającego oraz nie jest konieczna „ręczna” zmiana konfiguracji urządzeń i oprogramowania z wykorzystaniem natywnych interfejsów takich jak CLI (np. SSH), lub innych interfejsów systemów zarządzania dedykowanych do konfiguracji manualnej.

### Zautomatyzowane procesy dostarczania Zasobów muszą wykonywać się na podstawie zadanych przez Użytkownika końcowego parametrów, bez konieczności jego ingerencji w sam proces.

### Oprogramowanie Chmurowe musi zapewnić mechanizmy zarządzania cyklem życia dostarczanych Zasobów.

### Oprogramowanie Chmurowe musi pozwalać na definiowanie wzorców systemowych z zestandaryzowanymi zestawami parametrów instancji. Definicja wzorca systemowego musi uwzględniać parametry takie jak CPU, RAM, przestrzeń dyskowa, adresy IPv4 i IPv6, VLAN, sieci prywatne.

### Oprogramowanie Chmurowe musi umożliwiać udostępnianie użytkownikom zdefiniowanych Wzorców systemowych i aplikacyjnych w postaci Katalogu usług.

### Oprogramowanie chmurowe musi zapewniać portal administratora w postaci aplikacji webowej dla Administratorów umożliwiający zarządzanie w zakresie kluczowych funkcjonalności udostępnianych Administratorowi (w tym zarządzanie Użytkownikami, zarządzanie uprawnieniami i rolami, zarządzanie Katalogiem usług, zarządzanie Zasobami itp).

### Oprogramowanie chmurowe musi zapewniać portal użytkownika w postaci aplikacji webowej dla użytkowników umożliwiający zarządzanie w zakresie udostępnionych mu zasobów.

### Oprogramowanie chmurowe musi być dostępne bezprzerwowo nawet w przypadku braku dostępności jednego z Centrów Przetwarzania Danych.

### W przypadku awarii/niedostępności jednego z Centrów Przetwarzania Danych Oprogramowanie chmurowe musi zapewnić realizację opisanych funkcjonalności i realizować swoje funkcje na pozostałych do dyspozycji urządzeniach.

# Zarządzanie platformą wirtualizacji

## Wymagania podstawowe

### Oprogramowanie zarządzające platformami wirtualizacji musi zostać zainstalowane centralnie w części regionalnej w obu Centrach Przetwarzania Danych.

### Oprogramowanie zarządzające musi zostać uruchomione w formie gwarantującej możliwość zarządzania całym środowiskiem wirtualizacji (wszystkimi elementami lokalnymi oraz regionalnymi).

### Oprogramowanie zarządzające musi być dostępne bezprzerwowo nawet w przypadku braku dostępności jednego z Centrów Przetwarzania Danych.

### Rozwiązanie musi zapewniać natywne mechanizmy wysokiej dostępności HA w niezawodnej architekturze dla wszystkich składowych komponentów centralnej konsoli graficznej zarządzającej platformą wirtualną.

### Rozwiązanie musi posiadać centralną konsolę graficzną do zarządzania maszynami wirtualnymi i do konfigurowania innych funkcjonalności.

### Centralna konsola graficzna musi mieć możliwość działania zarówno jako aplikacja na maszynie fizycznej jak i wirtualnej.

### Konsola graficzna musi być dostępna poprzez przeglądarkę internetową (obsługa co najmniej Internet Explorer i Firefox).

### Usługa dostępu przez przeglądarkę do konsoli graficznej musi być skalowalna w przypadku wystąpienia zapotrzebowania na dużą liczbę jednoczesnych dostępów administracyjnych do środowiska.

### Rozwiązanie musi zapewniać zdalny i lokalny dostęp administracyjny do wszystkich serwerów fizycznych poprzez protokół SSH, z możliwością nadawania uprawnień do takiego dostępu nazwanym użytkownikom bez konieczności wykorzystania konta root.

### Rozwiązanie musi umożliwiać integrację z rozwiązaniami antywirusowymi firm trzecich w zakresie skanowania maszyn wirtualnych z poziomu warstwy wirtualizacji.

### Zarządzanie wszystkimi hostami (lokalnymi oraz regionalnymi) musi być realizowane z centralnego punktu z oprogramowania do zarządzania platformą wirtualizacji.

### Oprogramowanie zarządzające musi umożliwiać logiczne wydzielenie poszczególnych zasobów fizycznych na wyłączny użytek poszczególnych podmiotów oraz selektywne nadawanie praw dostępu do tej wydzielonej infrastruktury dla nazwanych użytkowników/administratorów.

### Logicznie wydzielone zasoby fizyczne na wyłączny użytek poszczególnych podmiotów powinny być zorganizowane w formie klastra wysokiej dostępności maszyn wirtualnych uruchomionych w ramach tego klastra (lokalny klaster HA).

### W przypadku wystąpienia awarii połączenia sieciowego lokalnego klastra HA do centralnej konsoli zarządzającej, mechanizm zapewniający wysoką dostępność maszyn wirtualnych (HA) nie może przestać działać.

### W przypadku wystąpienia awarii połączenia sieciowego lokalnego klastra HA do centralnej konsoli zarządzającej, każdy z hostów wchodzących w skład tego klastra powinien pozwolić zalogować się do jego konsoli zarządzania i umożliwiać zarządzanie jego ustawieniami oraz maszynami wirtualnymi obecnymi na tym hoście wraz z dostępem do konsoli graficznej maszyny wirtualnej.

# Wymagania dodatkowe

### Architektura rozwiązania musi przewidywać jego pracę w trybie ciągłym 24 godziny na dobę przez 7 dni w tygodniu przez 365 dni w roku, czyli prace serwisowe na pojedynczych elementach infrastruktury nie mogą wpływać na funkcjonalność całej platformy.

### Oprogramowanie musi być w wersji oficjalnej i produkcyjnej. Niedopuszczalne jest dostarczenie w wersji typu Alpha, Beta, Community Preview lub innej, która wyklucza jej wykorzystanie produkcyjne.

### Wszystkie dostarczone licencje na oprogramowanie muszą być bezterminowe.

### Architektura musi umożliwiać dalszą jej rozbudowę bez konieczności przebudowy dostarczonych i wdrożonych elementów.

### Architektura musi zapewniać możliwość wprowadzania zmian w konfiguracji oprogramowania i infrastrukturze z zachowaniem ciągłości pracy całego systemu.