**Załącznik nr 1 do Szacowania**

**SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA**

1. Wstęp  
   Niniejszy dokument stanowi szczegółowy opis przedmiotu zamówienia na zakup Sprzętu i Oprogramowania na potrzeby realizacji Umowy dotacji celowej nr 2/DC/D/2025
   1. Zastosowane skróty i pojęcia

|  |  |
| --- | --- |
| **Skrót/pojęcie** | **Opis skrótu/pojęcia** |
| **Dokumentacja** | oznacza dokumenty, specyfikacje, karty gwarancyjne (warunki świadczenia gwarancji) Sprzętu, instrukcje dotyczące Sprzętu i Oprogramowania dołączone przez Wykonawcę; w szczególności mogą to być instrukcje/dokumenty opracowane przez producenta Sprzętu, producenta lub Licencjodawcę Oprogramowania, Wykonawcę dotyczące montażu Sprzętu, instalacji Oprogramowania, obsługi i eksploatacji Sprzętu i Oprogramowania, konserwacji Sprzętu i inne (jeżeli występują); sposobu prawidłowego działania Oprogramowania, sposobu aktualizowania Oprogramowania, uprawnienia do korzystania z aktualizacji i innych ulepszeń Oprogramowania i inne, jeśli występują Dokumentacja powinna być sporządzona w języku polskim lub angielskim. |
| **Oprogramowanie lub System** | oznacza oprogramowanie zaoferowane przez Wykonawcę, spełniające wszystkie wymagania opisane w SOPZ, wraz z odpowiednią Dokumentacją na potrzeby celu Umowy, które może być wykorzystywane zgodnie z Warunkami Licencyjnymi; za Oprogramowanie uznaje się także każdą jego wersję lub odpowiednie zmiany Oprogramowania wprowadzone w kolejnych aktualizacjach Oprogramowania |
| **Sprzęt** | Oznacza Sprzęt wymagany i dostarczony przez wykonawcę do realizacji instalacji dostarczonego Oprogramowania. |
| **OPD1** | Oznacza podstawową lokalizację serwerowni Zamawiającego na terenie Warszawy. |
| **OPD2** | Oznacza zapasową lokalizację serwerowni Zamawiającego na terenie Warszawy. |
| **Umowa** | umowa zawarta w wyniku rozstrzygnięcia postępowania o udzielenie niniejszego zamówienia publicznego. |
| **Infrastruktura Zamawiającego** | Infrastruktura sieciowo, serwerowa w OPD1 i OPD2 |
| **Awaria** | Awarią należy rozumieć stan techniczny lub operacyjny Sprzętu, który powoduje całkowitą niemożność korzystania ze Sprzęty lub jego kluczowych funkcji, co uniemożliwia realizację zadań objętych jego przeznaczeniem. Awaria wymaga podjęcia natychmiastowych działań naprawczych. Przykłady awarii obejmują: całkowite uszkodzenie systemu, brak dostępu do kluczowych funkcjonalności lub przerwanie podstawowych procesów operacyjnych. |
| **Usterka** | Usterką należy rozumieć stan techniczny lub operacyjny Sprzętu, który nie powoduje całkowitej niemożności korzystania z Sprzętu, lecz w istotny sposób ogranicza jego funkcjonalność, komfort użytkowania lub wydajność. Przykłady usterek obejmują: obniżoną wydajność, problemy z niektórymi funkcjonalnościami, czy drobne błędy techniczne niezakłócające podstawowego działania. |

1. **Informacje ogólne:**
   1. Wszystkie wymagania i parametry, w tym techniczne, funkcjonalne i wydajnościowe zawarte w niniejszym dokumencie mają charakter obligatoryjny i Wykonawca zobowiązany jest do ich spełnienia w ramach oferowanego rozwiązania. Wykonawca jest zobowiązany do takiego doboru urządzeń, który zapewni efektywność energetyczną oferowanego rozwiązania i optymalizację ponoszonych przez Zamawiającego kosztów utrzymania rozwiązania.
   2. Wszystkie podane wymagania i parametry musza być spełnione łącznie. Wszystkie wymagania podane w niniejszym dokumencie muszą być spełnione dla dowolnej wielkości obciążenia lub ruchu, chyba że w opisie danej funkcjonalności podano inaczej.
   3. W przypadku wymienienia wielu wymagań, konieczne jest spełniania wszystkich z nich (np. umieszczenie wygania „Urządzenie musi obsługiwać multicast IPv4 (IGMPv2/3, PIM SM, SSM, MSDP)” oznacza konieczność obsługi przez urządzenie wszystkich wymienionych protokołów).
   4. Wykonawca jest proszony o dobór odpowiedniego Sprzętu i Oprogramowania do realizacji zapotrzebowania Zamawiającego.
   5. Zamawiający wskazuje nazwy producentów infrastruktury, którą posiada, w celu zapewnienia zgodności oraz możliwości jej rozbudowy z oferowanym Sprzętem. Poniżej przedstawiono specyfikację infrastruktury, która powinna być brana pod uwagę przy składaniu ofert.
2. **Przedmiot zamówienia:**

Grupa 1 – Dostawa sprzętu i Oprogramowania do budowy środowiska. Kompletna oferta, na dostarczenie infrastruktury i oprogramowania (wraz z jego instalacją) do zbudowania klastrów.

|  |  |  |  |
| --- | --- | --- | --- |
| **Przedmiot zamówienia** | **Zamówienie podstawowe (szt)** | **Zamówienie opcjonalne (niegwarantowane) szt.** | **Uwagi** |
| **Serwer typ1 wraz z wyposażeniem - zgodny ze specyfikacją szczegółową** | **5** |  | **Gwarancja 5 lat** |
| **Serwer typ1 wraz z wyposażeniem i rozszerzeniem oprogramowania do budowy chmury prywatnej zgodne ze specyfikacją szczegółową** |  | **3** | **Gwarancja 5 lat** |
| **Oprogramowanie do budowy chmury prywatnej zgodne ze szczegółową specyfikacją** | **1 szt** |  | **Oprogramowanie musi obsługiwać serwery zakupione w ramach zamówienia podstawowego. Licencje na 5 lat.** |

1. **Grupa1 – Infrastruktura** 
   1. Serwery
      1. Wszystkie elementy serwera muszą być zintegrowane przez producenta i dostarczone przez Wykonawcę wraz z dokumentacją producenta i posiadać numery części występujące w dokumentacji producenta jako numery części przeznaczone do danego modelu;
      2. Serwery muszą pochodzić z jednej linii produkcyjnej, zapewniając uproszczony proces aktualizacji i rozbudowy infrastruktury;
      3. Pojedynczy serwer powinien zapewnić następujące wartosći:
         1. CPU – 48 Core;
         2. RAM – 768GB;
         3. Przestrzeń na dane – 45TB RAW;
         4. Kable 3m DAC 25GB SFP+ – 2 szt
      4. Serwery muszą być zgodne z dostarczonym oprogramowaniem do wirtualizacji mocy obliczeniowej i komponentem SDS. Model serwera i jego elementy muszą być umieszczone na oficjalnej stronie producenta oprogramowania do wirtualizacji (Compute i SDS);
      5. Obudowa serwera typu RACK 19" o wysokości nie przekraczającej 1U wraz z zestawem do zamontowania w szafie teleinformatycznej 19", o głębokości 80-100 cm i prowadzeniem dla kabli, umożliwiającym pełne wysunięcie obudowy na szynach;
      6. Serwery wyposażone w panel LCD lub LED umieszczony na froncie urządzenia, umożliwiający wyświetlenie informacji o stanie serwera, zasilania oraz temperatury lub za pomocą dedykowanego oprogramowania do zarządzania serwerami;
      7. Płyta główna musi posiadać następujące cechy:
         1. posiadać dwa fizyczne gniazda do obsługi procesorów 64 bitowych wyspecyfikowanych w następnych punktach;
         2. posiadać chipset dedykowany do pracy w konfiguracjach 2 procesorowych, obsługujący opisane procesory;
         3. posiadać co najmniej 24 slotów do obsługi pamięci DDR4, pracującej z częstotliwością min. 2666 MHz;
         4. posiadać możliwość obsługi co najmniej 1024 GB pamięci RAM;
      8. Możliwość instalacji minimum dziesięciu dysków SSD lub NVMe w formie 2.5” SFF lub E3.S wymiennych dla serwerów o wysokości 1U;
      9. Zainstalowany kontroler macierzy RAID zgodny z dostarczonym Oprogramowaniem Komponentu SDS (jeśli taki jest wymagany);
      10. Minimum 3 slotów PCI Express (w tym min. 2 sloty PCI Express x16 generacji 3) dla serwera o wysokości 1U;
      11. Zintegrowana karta graficzna o rozdzielczości minimum 1920 x 1080;
      12. Możliwość instalacji modułu TPM 2.0;
      13. Wyposażony w 2 identyczne procesory, każdy z procesorów o następujących minimalnych parametrach:
          1. architektura 64 bitowa;
          2. przy częstotliwości taktowania zegara min. 2.6 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: 30 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 dla zaoferowanego modelu serwera minimum 275 punktów.
      14. Wyposażony w pamięć RAM o następujących parametrach:
          1. kości DDR4 co najmniej 2666 MHz RDIMM;
          2. zainstalowane kości o pojemności min. 32GB;
          3. zainstalowane minimum 384 GB pamięci RAM dla jednego procesora w każdym serwerze;
          4. obsadzone nie więcej niż połowa dostępnych slotów na moduły pamięci RAM;
          5. posiadać co najmniej dwadzieścia cztery sloty na moduły pamięci RAM;
          6. możliwość rozbudowy do co najmniej 1024 GB pamięci RAM;
          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) lub równoważne mechanizmy, które zapewniają korekcję błędów pamięci RAM na poziomie pojedynczego chipu DRAM – takie jak Advanced Memory Device Correction (AMDC) lub inne mechanizmy RAS (Reliability, Availability, Serviceability) zapewniające porównywalny poziom niezawodności i dostępności.
      15. Wyposażony w dyski twarde o następujących parametrach:
      16. Dyski systemowe (dla ESXi / systemu operacyjnego) Wymaganie
          1. Minimum 2 dyski SSD lub moduł BOSS (Boot Optimized Storage Solution) RAID-1 – zgodnie z profilem ESA ReadyNode producenta.
          2. Złącze SATA, SAS lub NVMe – zależnie od rozwiązania producenta serwera.
          3. Pojemność co najmniej 480 GB na dysk (lub zgodnie z profilem ReadyNode).
          4. Minimalna trwałość: 1 DWPD, zgodnie ze specyfikacją producenta.
          5. Odczyt/zapis sekwencyjny: odpowiednio powyżej 500 MB/s i 450 MB/s.
          6. Odczyt losowy: min. 70 000 IOPS
          7. Zapis losowy: min. 30 000 IOPS.
          8. Obsługa RAID-1 (sprzętowa lub programowa) dla partycji systemowej.
      17. Minimum 8 dysków NVMe, zgodnie z profilem ESA ReadyNode;
          1. zainstalowane dyski:
             1. muszą być certyfikowane jako kompatybilne z VMware vSAN ESA;
             2. Dyski muszą być częścią konfiguracji ESA ReadyNode zatwierdzonej przez VMware/Broadcom;
             3. Trwałość: ≥1 DWPD przez 5 lat (NVMe Enterprise Class), zgodna z wymaganiami vSAN ESA;
             4. Wymienione dyski pozostają u zamawiającego.
      18. Wymagane są następujące parametry dysków twardych:
          1. Serwery wyposażone w dyski typu NVMe:
             1. Sekwencyjny odczyt/zapis: co najmniej 5000 MB/s / 4000 MB/s. ;
             2. Odczyt losowy: minimum 1 000 000 IOPS (4K random read). ;
             3. Zapis losowy: minimum 180 000 IOPS (4K random write).
      19. Minimalna ilość zasobów musi zapewniać co najmniej 5% bufora wydajnościowego zgodnie z najlepszymi praktykami VMware ESA,
      20. Wyposażone w interfejsy sieciowe LAN:
          1. min. 1 port Gigabit Ethernet 1000Base-T;
          2. min. 2x2 porty 25 Gigabit Ethernet w formie gniazd SFP28 na płycie głównej lub/i karcie PCIe;
      21. Karty sieciowe muszą wspierać budowę sieci programowej SDN dla zastosowanego protokołu enkapsulacji;
      22. Wyposażone w minimum 1 interfejs sieciowy na potrzeby zarządzania Gigabit Ethernet 1000Base-T dedykowany dla zarządzania;
      23. Zgodność ze standardem UEFI Secure Boot weryfikującym podpisy kryptograficzne sterowników UEFI przed uruchomieniem systemu operacyjnego;
      24. Wbudowana bezpieczna pamięć chroniąca wrażliwe dane, takie jak poświadczenia użytkownika oraz klucze prywatne dla certyfikatów SSL;
      25. Wyposażone w następujące inne interfejsy:
          1. minimum 2 bezpośrednio udostępnione zewnętrzne porty USB 3.0;
          2. minimum 1 bezpośrednio udostępniony port VGA DB15 lub HDMI lub DisplayPort;
          3. Wyposażone w moduł zdalnego zarządzania (konsoli) umożliwiający:
             1. zdalne włączenie, wyłączenie i restart serwera;
             2. wykorzystanie zdalnej, graficznej konsoli obsługującej 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 w wersji 1 i 2;
             10. monitorowanie stanu zasilaczy, wentylatorów, dysków, temperatury, wielkości poboru energii;
             11. rozwiązanie sprzętowe, niezależne od CPU i od działających systemów operacyjnych;
             12. aktualizacja firmware-u modułu (karty) zarządzania zdalnego bez konieczności restartu serwera;
             13. definiowanie wielu użytkowników z możliwością uwierzytelniania w LDAP, Active Directory;
             14. wysyłanie powiadomień syslog do zewnętrznych serwerów np. SIEM;
             15. rejestrowanie działań administratora w oparciu o log;
      26. Zasilanie, chłodzenie:
          1. minimum dwa jednakowe zasilacze dostosowane do napięcia przemiennego 230V 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;
          3. dołączone kable zasilające pozwalające na podłączenie wszystkich zasilaczy do standardowych gniazd zasilających oraz gniazd typu IEC;
      27. Posiadanie deklaracji zgodności CE lub równoważne potwierdzające, że produkt może być wprowadzony do obrotu lub oddany do użytkowania na terenie unii Europejskiej;
      28. Zgodność ze standardem UEFI Secure Boot weryfikującym podpisy kryptograficzne sterowników UEFI przed uruchomieniem systemu operacyjnego;
      29. Informowanie o zmianie konfiguracji serwera.
      30. Wykonawca udziela gwarancji na Sprzęt i Oprogramowanie Sprzętowe na zasadach określonych poniżej:
2. Wykonawca bezpośrednio lub poprzez autoryzowany serwis producenta w ramach gwarancji zapewni usunięcie Awarii i Usterek Sprzętu lub zapewni ich wymianę na nowy, wolny od wad.
3. Opis procedur zgłaszania i procedowania zgłoszeń musi być dostępny na oficjalnej stronie internetowej producenta Sprzętu.
4. Wykonawca zapewni system zgłoszeń serwisowych. Zgłoszenia naprawy będą przyjmowane w języku polskim w tzw. trybie 24x7x365 (bez przerw, przez całą dobę, we wszystkie dni w roku) przez dedykowany serwis internetowy producenta. Wykonawca zapewni założenie kont użytkowników dla pracowników Zamawiającego lub osób wskazanych przez Zamawiającego, upoważnionych do dokonywania zgłoszeń.
5. Przyjmowanie zgłoszeń, o których mowa powyżej, odbywa się we wszystkie dni w roku w godzinach 0:00 – 23:59.
6. Proces obsługi zgłoszeń musi zapewniać ciągłość komunikacji i jej poufność na poszczególnych etapach procesowania zgłoszenia. Nie dopuszcza się obsługi zgłoszeń przez firmy trzecie lub w systemach informatycznych nie zarządzanych przez producenta lub jego autoryzowany serwis.
7. Wszystkie zgłoszenia gwarancyjne muszą być obsłużone, a naprawa dokonana w terminie:
8. Awaria – najpóźniej następnego Dnia Roboczego od zgłoszenia,
9. Usterka – w terminie do 4 Dni Roboczych od zgłoszenia.
10. Czas naprawy uznaje się za zachowany, jeżeli w tym terminie Wykonawca zapewni rozwiązanie tymczasowe na czas przedłużającej się naprawy lub zapewni, zainstaluje i skonfiguruje Sprzęt zastępczy.
11. Jeżeli wada (Awaria, Usterka) Sprzętu jest tego rodzaju, że wymaga instalacji update Oprogramowania, czas naprawy Awarii/Usterki rozpoczyna swój bieg z chwilą oficjalnego opublikowania przez producenta update’u (aktualizacji) tego Oprogramowania; z zastrzeżeniem, że Wykonawca zobowiązany jest zapewnić Zamawiającemu – bez zbędnej zwłoki, w miarę możliwości technicznych Wykonawcy - rozwiązanie zastępcze w zakresie tej wady (Awarii Usterki) celem zneutralizowania wynikających z niej uciążliwości na okres do momentu zapewnienia przez producenta przedmiotowego update’u (aktualizacji) Oprogramowania.
12. Gwarancja obejmuje możliwość wielokrotnego uaktualniania oprogramowania urządzeń do wersji i dokumentacji technicznej dotyczącej tej wersji, dla której producent umożliwia zgłaszanie Awarii i Usterek i zapewnia ich naprawę, w tym najnowszych dostępnych aktualizacji usuwających wykryte błędy krytyczne lub eliminujących krytyczne podatności bezpieczeństwa. Gwarancja zapewnia też dostęp do narzędzia producenta pozwalającego na automatyczne zbieranie danych o statusie i działaniu produktów objętych usługą.
13. Wykonawca zapewni ciągłość gwarancji w wypadku zawieszenia lub zakończenia działalności swojego przedsiębiorstwa w czasie, na który została udzielona gwarancja.
14. W wypadku zapewnienia gwarancji przez podmiot trzeci, w tym producenta lub jego autoryzowany serwis, Wykonawca odpowiedzialny jest za zapewnienie takiej gwarancji na warunkach nie gorszych niż wynikające z Umowy i SOPZ.
15. Zamawiający może dokonać rozbudowy posiadanej infrastruktury sprzętowej, aplikacyjnej oraz teleinformatycznej bez utraty uprawnień wynikających z gwarancji na dostarczony Sprzęt w ramach realizacji Umowy, z zastrzeżeniem, że rozbudowa została dokonana zgodnie z zaleceniami / wytycznymi producenta.
16. Naprawa lub diagnoza mogą być realizowane w formie zdalnego wsparcia przez pracownika Wykonawcy lub autoryzowanego serwisu producenta pod warunkiem zastosowania środków zdalnego dostępu i bezpieczeństwa zaakceptowanych lub wskazanych przez Zamawiającego.
17. Serwis gwarancyjny świadczony będzie w Siedzibie Zamawiającego lub w innym miejscu wskazanym przez Zamawiającego na terenie Warszawy, w obecności przedstawiciela Zamawiającego.
18. Wykonawca zobowiązuje się do tego, że serwis gwarancyjny będzie realizowany przez producenta lub autoryzowany serwis producenta;
19. Gwarancja nie może ograniczać praw Zamawiającego do dysponowania zakupionym Sprzętem w razie sprzedaży lub innej formy przekazania Sprzętu gwarancja przechodzi na nowego właściciela.
20. Zgłoszenie przez Zamawiającego przed upływem terminu gwarancji, podlega realizacji na zasadach opisanych w powyżej.
21. W trakcie obowiązywania Umowy Wykonawca odpowiada za prawidłową realizację wymagań Zamawiającego dotyczących gwarancji.
22. Uprawnienia wynikające z udzielonej gwarancji nie wyłączają możliwości dochodzenia przez Zamawiającego uprawnień z rękojmi za wady.
23. Czas obowiązywania rękojmi liczony jest od daty odbioru potwierdzonego Protokołem Odbioru jakościowego.
24. Wykonawca ponosi wszelkie koszty związane z wykonaniem obowiązków wynikających z udzielonej gwarancji.
    1. **Oprogramowanie do budowy chmury prywatanej – szczegółowa specyfikacja**
       1. Oprogramowanie do utworzenia i użytkowania platformy chmury prywatnej, będące rozbudową istniejącej infrastruktury VMware, musi zawierać wszystkie poniżej wymienione komponenty/moduły. Dodatkowo, wszystkie komponenty muszą pochodzić od jednego producenta oprogramowania. Cały zaoferowany pakiet oprogramowania do budowania chmury prywatnej musi składać się z następujących komponentów:

* Do wirtualizacji mocy obliczeniowej.
* Do zarządzania klastrami wirtualizacyjnymi.
* Do instalacji i zarządzania komponentami chmury prywatnej.
* Do monitorowania i zarządzania pojemnością chmury prywatnej.
* Do automatyzacji.
* Do zbierania, korelowania i analizowania logów.
* Do tworzenia platformy konteneryzacyjnej opartej na Kubernetes.
* Do tworzenia sieci wirtualnych.
* Do monitorowania i analizowania sieci oraz polityk firewall w sieciach wirtualnych i fizycznych.
* Do wirtualizacji przestrzeni dyskowych.
* Do zaawansowanej migracji maszyn wirtualnych lub systemów operacyjnych z fizycznych serwerów.
* Do portalu samoobsługowego do automatycznego tworzenia maszyn wirtualnych z bazami danych MySQL i PostgreSQL na dostarczanym module do wirtualizacji mocy obliczeniowej.
  + 1. **Ogólne wymagania dotyczące wirtualizacji**
       1. Licencjonowanie: Oprogramowanie musi umożliwiać licencjonowanie na rdzeń fizycznego procesora lub na cały procesor, aby zapewnić zgodność licencyjną dla całej infrastruktury dostarczonej przez Wykonawcę
       2. Instalacja i alokacja zasobów: Oprogramowanie musi być instalowane bezpośrednio na sprzęcie fizycznym, nie będąc częścią innego systemu operacyjnego. Warstwa wirtualizacji nie może alokować więcej niż 3GB pamięci RAM serwera fizycznego.
       3. Obsługa sprzętu: Oprogramowanie musi obsługiwać serwery z 768 logicznymi wątkami, 12TB pamięci RAM i 8 fizycznymi procesorami. Możliwość konfiguracji maszyn wirtualnych z 768 procesorami wirtualnymi, do 12TB RAM oraz do 8 wirtualnych kart sieciowych.
       4. Kompatybilność systemów operacyjnych: Oprogramowanie musi wspierać różne systemy operacyjne, w tym różne wersje Windows, Linux i FreeBSD.
       5. Funkcje i zarządzanie: Możliwość nad przydzielania pamięci RAM oraz zasobów dyskowych. Integracja z rozwiązaniami antywirusowymi firm trzecich. Zdalny i lokalny dostęp administracyjny z możliwością nadawania uprawnień użytkownikom.
       6. Kopie zapasowe i migawki: Funkcje powielania maszyn wirtualnych, tworzenia migawkowych kopii zapasowych oraz zdalnego zarządzania zasobami.
       7. Sieci i przełączniki wirtualne: Tworzenie wirtualnych przełączników z obsługą VLAN, agregacją połączeń fizycznych i wsparciem dla sieci 200GbE.Przełączanie ścieżek LAN i SAN bez utraty komunikacji. Możliwość migracji dysków maszyn wirtualnych między podsystemami dyskowymi bez przerywania ich pracy.
       8. Zarządzanie i monitorowanie: Integracja z katalogami użytkowników (AD, LDAP), federacyjne zarządzanie tożsamością (ADFS). Możliwość dodawania zasobów w czasie pracy maszyn wirtualnych. Mechanizmy alertów o przekroczeniu wartości progowych. Centralne zarządzanie aktualizacjami i konfiguracją serwerów oraz monitorowanie zużycia zasobów.
       9. Bezpieczeństwo i zgodność: Wsparcie dla TPM 2.0, Microsoft VBS, FIPS 140 2. Funkcjonalność wirtualnego TPM 2.0. Ochrona danych wrażliwych i wspieranie mechanizmów zaawansowanego uwierzytelniania.
       10. Integracja i automatyzacja: Wsparcie dla API do integracji zewnętrznych rozwiązań backupowych i SDN. Możliwość tworzenia kontenerów i klastrów Kubernetes bezpośrednio na hiperwizorze.
       11. Wydajność i skalowalność: Obsługa migracji maszyn wirtualnych w czasie rzeczywistym. Automatyczne równoważenie obciążenia zasobów fizycznych. Wsparcie dla technologii RDMA, Persistent Memory i DPU.
       12. Zarządzanie ryzykiem i audyt: Wbudowane mechanizmy audytu i walidacji FIPS. Automatyczna weryfikacja wpływu aktualizacji na komponenty klastra.
       13. Dodatkowe wymagania: Wsparcie dla natywnych dysków 4K i precyzyjnej synchronizacji czasu (PTP). Granularna kontrola nad konfiguracją sieciową maszyn wirtualnych. Możliwość eksportu konfiguracji centralnej konsoli zarządzającej przez API.
    2. **Wymagania dotyczące zarządzania klastrami wirtualizacyjnymi**
       1. Skalowalność Oprogramowania: Oprogramowanie do zarządzania klastrem wirtualizacyjnym musi umożliwiać dynamiczne dostosowywanie liczby instancji do liczby fizycznych rdzeni używanych w wirtualizowanych środowiskach obliczeniowych.
       2. Konsola graficzna: Zaoferowane oprogramowanie musi posiadać konsolę graficzną do zarządzania maszynami wirtualnymi i konfigurowania innych funkcjonalności, takich jak zasoby dyskowe oraz zasoby sieci komputerowej. Konsola graficzna powinna działać jako zainstalowana aplikacja na maszynie wirtualnej i być dostępna jako tzw. virtual appliance. Instalacja virtual appliance nie może wymagać dostawy dodatkowego oprogramowania, takiego jak system operacyjny lub baza danych.
       3. Wbudowany serwer ściany ogniowej: Zaoferowane oprogramowanie musi posiadać wbudowany serwer ściany ogniowej (firewall) z możliwością konfiguracji blokady lub akceptacji ruchu między konsolą zarządzającą a serwerami oraz serwerami wirtualnymi, z założeniem blokowania całego ruchu, a nie poszczególnych portów.
       4. Uwierzytelnianie użytkowników: Oprogramowanie musi umożliwiać konfigurację uwierzytelniania użytkowników logujących się do niego na podstawie minimum: domeny Microsoft Active Directory, Microsoft Active Directory over LDAP oraz Open LDAP.
       5. Dostępność konsoli graficznej: Oprogramowanie musi posiadać konsolę graficzną, dostępną poprzez dedykowanego klienta (za pomocą przeglądarek minimum Mozilla Firefox oraz Chrome) lub poprzez konsolę graficzną zbudowaną w HTML5.
       6. Zarządzanie Hostami VMware vSphere: Oprogramowanie musi posiadać funkcjonalność zcentralizowanego zarządzania hostami opartymi na VMware vSphere które posiada w rozbudowywanej infrastrukturze Zamawiający.
       7. Kopie zapasowe: Oprogramowanie musi posiadać natywne mechanizmy do wykonywania kopii zapasowej swojej konfiguracji, z możliwością ustawienia harmonogramu. Kopie zapasowe muszą wspierać protokoły: FTPS, HTTPS, SCP, FTP oraz HTTP.
       8. Zarządzanie wirtualną przestrzenią dyskową SDS: Oprogramowanie musi posiadać wbudowaną funkcjonalność zarządzania wirtualną przestrzenią dyskową SDS (Software Defined Storage) poprzez rozszerzenie o dodatkową licencję oferowaną przez tego samego producenta.
       9. Interfejs Graficzny: Oprogramowanie musi posiadać interfejs graficzny do prowadzenia prac administracyjnych oraz monitoringu (monitorowanie obciążenia min. vCPU, vRAM, vHDD, sieci, bazy danych), wykonany w standardzie HTML5.
       10. Automatyzacja Instalacji Konsol Zarządzania: Oprogramowanie musi umożliwiać automatyzację instalacji wielu konsoli zarządzania poprzez użycie schematów konfiguracji.
       11. Aktualizacje Wirtualizatorów: Oprogramowanie musi umożliwiać aktualizowanie wielu wirtualizatorów równocześnie.
       12. Przenoszenie Maszyn Wirtualnych: Rozwiązanie musi pozwalać na wykorzystanie łącz o szybkości do 100 GbE do bezawaryjnego przenoszenia maszyn wirtualnych między wirtualizatorami.
       13. Mechanizmy Wysokiej Dostępności HA: Rozwiązanie musi zapewniać natywne mechanizmy wysokiej dostępności HA w niezawodnej architekturze Active Passive Witness dla wszystkich komponentów centralnej konsoli graficznej zarządzającej platformą wirtualną.
       14. Serwer Zarządzania Kluczami (KMS): Oprogramowanie musi zapewniać podstawowe funkcje serwera zarządzania kluczami (KMS), upraszczające włączenie szyfrowania i zaawansowanych funkcji bezpieczeństwa.
       15. Balansowanie Mocy Obliczeniowej: Oprogramowanie, w przypadku zarządzania serwerami opartymi o VMware vSphere, musi prezentować poziom zbalansowania mocy obliczeniowej w klastrze opartym na tych wirtualizatorach. skalowalność dostępu przez przeglądarkę: Dostęp przez przeglądarkę do konsoli graficznej w zaoferowanym oprogramowaniu musi być skalowalny, tj. powinien umożliwiać rozdzielenie komponentów na wiele instancji w przypadku dużego zapotrzebowania na jednoczesne dostępy administracyjne do środowiska.
    3. **W zakresie dodatkowej konsoli/oprogramowania do instalacji i zarządzania komponentami chmury prywatnej Zamawiający wymaga:** 
       1. Centralna konsola zarządzająca: Oprogramowanie musi posiadać centralną konsolę umożliwiającą automatyczną instalację i/lub konfigurację oprogramowania do wirtualizacji serwerów fizycznych, macierzy dyskowej typu SDS (ang. Software Defined Storage) na serwerach, oraz wirtualizacji sieci typu SDN (ang. Software Defined Network) wraz z mechanizmami bezpieczeństwa. Konsola musi także umożliwiać aktualizację wszystkich powyższych komponentów oprogramowania.
       2. Automatyzacja i uproszczenie wdrażania: O programowanie musi oferować narzędzia automatyzujące i upraszczające proces wdrażania stosu oprogramowania infrastrukturalnego, w tym wirtualizacji serwerów x86, wirtualizacji sieci oraz tworzenia macierzy dyskowej typu SDS. Musi to obejmować zautomatyzowaną instalację oprogramowania, tworzenie klastrów obliczeniowych (w tym Kubernetes) oraz dedykowanego klastra zarządzającego całością platformy.
       3. Mechanizmy aktualizacji:Oprogramowanie musi mieć mechanizmy do aktualizacji całego stosu oprogramowania wirtualizującego oraz możliwość definiowania harmonogramu i zakresu tych aktualizacji. Aktualizacje powinny być dostępne w trybie online (poprzez portal z poprawkami) i offline (poprzez wcześniejsze wgranie poprawek do repozytorium).
       4. Wsparcie dla konfiguracji sprzętowych: Oprogramowanie musi posiadać na oficjalnej stronie producenta listę wspieranych i certyfikowanych konfiguracji serwerów sprzętowych. Wymagane jest wsparcie dla co najmniej 3 niezależnych producentów sprzętu serwerowego.
       5. Automatyczna instalacja i aktualizacja komponentów:Oprogramowanie musi automatycznie instalować i aktualizować komponenty środowiska wirtualnego, w tym wirtualizację mocy obliczeniowej, wirtualizację przestrzeni dyskowej, wirtualizację sieci komputerowej, moduł zarządzania i optymalizacji pojemności, oraz moduł gromadzenia logów z infrastruktury.
       6. Zarządzanie hasłami:Oprogramowanie musi wspierać zarządzanie hasłami dla komponentów, takich jak wirtualizacja mocy obliczeniowej, przestrzeni dyskowej i sieci komputerowej. Powinno dostarczyć co najmniej 3 metody zmiany haseł, takie jak automatyczne generowanie haseł, zmiana na własne hasło oraz możliwość integracji z menedżerem haseł przez API. Dodatkowo, oprogramowanie powinno zapewniać automatyczną rotację haseł.
       7. Zarządzanie certyfikatami SSL:Oprogramowanie musi umożliwiać zarządzanie certyfikatami SSL z centralnej konsoli dla całego stosu oprogramowania wirtualizującego.
       8. Kopie zapasowe konfiguracji: Oprogramowanie musi zapewniać możliwość wykonywania kopii zapasowych konfiguracji całego stosu oprogramowania wirtualizującego oraz definiowania harmonogramu tych kopii zapasowych.
       9. Integracja z systemami monitorującymi:Oprogramowanie musi integrować i automatyzować warstwę oprogramowania monitorującego oraz zbierającego logi, w tym kontrolować aktualizacje tego oprogramowania.
    4. **Wymagania dotyczące monitorowania i zarządzania pojemnością chmury prywatnej**
       1. Zamawiający wymaga, aby oferowane oprogramowanie do zarządzania pojemnością chmury prywatnej spełniało następujące kryteria:
       2. Licencjonowanie: Oprogramowanie musi mieć możliwość licencjonowania na rdzeń fizycznego procesora lub procesora w celu zapewnienia licencjonowania dla całości dostarczonej infrastruktury przez Wykonawcę
       3. Monitorowanie wydajności: Musi zapewniać informacje o wydajności środowiska wirtualnego w celu zarządzania pojemnością.
       4. Przewidywanie trendów: Powinno przewidywać trendy pojemności za pomocą inteligentnych algorytmów, zwłaszcza dla środowiska opartego na VMware vSphere.
       5. Optymalizacja zasobów: Musi analizować środowisko wirtualne pod kątem optymalizacji wykorzystania CPU, RAM i zasobów dyskowych.
       6. Grupowanie obiektów: Powinno umożliwiać tworzenie unikalnych zbiorów obiektów odpowiadających funkcjom Datacenter, z możliwością monitorowania alertów, pojemności i ryzyk.
       7. Tworzenie scenariuszy: Musi umożliwiać tworzenie scenariuszy "co, jeśli" dotyczących dodawania maszyn wirtualnych, z analizą średniego obciążenia oraz skoków obciążenia.
       8. Analiza pojemności: Powinno posiadać funkcjonalność zapisywania i przechowywania różnych scenariuszy "co by było, gdyby" oraz wpływać na prognozowanie analizy pojemności.
       9. Definiowanie poziomu konsolidacji: Musi definiować poziom konsolidacji/wirtualizacji w celu poprawnej predykcji pojemności w przyszłości.
       10. Monitorowanie VMware: Powinno monitorować infrastrukturę opartą o VMware vSphere oraz VMware vSAN, generując alerty na podstawie korelacji wykrytych anomalii i symptomów.
       11. Rekomendacje: Musi dostarczać informacje o rekomendowanych działaniach zapewniających prawidłowe działanie środowiska VMware vSphere.
       12. Integracja z zewnętrznymi systemami: Powinno mieć wbudowane komponenty integracyjne dla zewnętrznych kolektorów logów i zdarzeń oraz funkcjonalność monitorowania zgodności z najlepszymi praktykami bezpieczeństwa.
       13. Baza wiedzy: Powinno zawierać bazę wiedzy eksperckiej jako źródło dobrych praktyk i sugestii.
       14. Wizualizacja danych: Musi wizualizować obciążenie środowiska wirtualnego online z możliwością "drill down" oraz posiadać graficzne dashboardy.
       15. Mapy graficzne: Powinno oferować aktywne mapy graficzne elementów środowiska wirtualnego.
       16. Predykcja zasobów: Musi dokonywać automatycznej predykcji wykorzystania zasobów na podstawie zebranych danych.
       17. Raportowanie: Powinno umożliwiać przeglądanie linii trendu monitorowanych parametrów i tworzenie raportów pojemnościowych.
       18. Monitorowanie w czasie rzeczywistym: Musi umożliwiać monitorowanie środowisk w czasie rzeczywistym z maksymalnym opóźnieniem 5 minut.
       19. Szczegółowe statystyki: Powinno umożliwiać przeglądanie wszystkich zbieranych statystyk w wybranym zakresie czasu z minimalnym zapisywaniem metryk co 5 minut na 10 lat.
       20. Monitorowanie fizycznych serwerów: Musi umożliwiać szczegółowe monitorowanie komponentów fizycznych serwerów.
       21. Definiowanie progów: Powinno pozwalać na definiowanie progów wydajności i pojemności dla identyfikacji wąskich gardeł.
       22. Zarządzanie maszynami wirtualnymi: Powinno umożliwiać zarządzanie maszynami wirtualnymi, w tym kasowanie, snapshoty, włączanie i wyłączanie.
       23. Analiza nadmiarowości: Musi automatycznie analizować dane w celu wykrywania nadmiarowości i niedoborów zasobów.
       24. Automatyczne alarmowanie: Powinno automatycznie alarmować w sytuacjach nietypowych.
       25. Elastyczne przypisywanie alertów: Musi umożliwiać przypisywanie alertów różnym grupom odbiorców.
       26. Porady eksperckie: Powinno pozwalać na odczyt alarmów wraz z powiązanymi poradami eksperckimi.
       27. Definiowanie alertów: Musi umożliwiać definiowanie alertów związanych z zarządzaniem pojemnością, wydajnością, anomaliami i dostępnością.
       28. Predefiniowane raporty: Musi umożliwiać generowanie gotowych raportów o stanie środowiska.
       29. Dashboardy: Musi posiadać gotowe pulpity kierownicze (dashboardy) z możliwością automatycznej analizy danych za pomocą uczenia maszynowego.
       30. Wsparcie dla zdalnych kolektorów: Powinno wspierać kolektory do zdalnego zbierania danych w sieciach o słabej wydajności.
       31. Obsługa dużych danych: Powinno obsługiwać do 0,5 mln obiektów na klaster z 50 mln metryk.
       32. Dodatkowe adaptery: Musi posiadać możliwość zastosowania adapterów integrujących z systemami firm trzecich.
       33. Wysoka dostępność: Powinno umożliwiać konfigurację trybu wysokiej dostępności dla każdego komponentu.
       34. Zmiana parametrów: Musi umożliwiać zmianę parametrów maszyn wirtualnych oraz odkładanie w czasie tych zmian.
       35. Integracja z systemami zewnętrznymi: Powinno monitorować urządzenia firm trzecich, takie jak macierze dyskowe i urządzenia sieciowe.
       36. Zrównoważony rozwój: Powinno wykazywać zrównoważony rozwój poprzez redukcję śladu węglowego.
       37. Monitorowanie aplikacji: Powinno monitorować aplikacje, serwery aplikacyjne i bazy danych firm trzecich.
       38. Integracja z APM: Musi integrować się z zewnętrznymi rozwiązaniami APM, takimi jak AppDynamics, Datadog, New Relic, VMware Tanzu Observability, czy DynaTrace.
       39. Monitorowanie systemów operacyjnych: Musi monitorować systemy operacyjne serwerów wirtualnych bez udziału agentów oraz za pomocą zainstalowanego agenta
       40. Integracja VMware Aria Automation.
       41. Paczki monitorujące: Powinno posiadać paczki do monitorowania dla produktów VMware Aria Orchestrator, VMware SDDC, VMware Aria Automation.
       42. Scenariusze pojemnościowe: Musi tworzyć scenariusze pojemnościowe dla CPU, RAM i przestrzeni dyskowej, uwzględniając dodawanie nowych serwerów, elementów VMware vSAN oraz migracje do chmur publicznych.
       43. Super metryki: Powinno umożliwiać matematyczne wyliczanie wartości super metryk na podstawie innych monitorowanych metryk.
       44. Wykrywanie usług: Musi wykrywać usługi uruchomione na maszynach wirtualnych i budować relacje między nimi.
       45. Automatyczne działania: Powinno wykonywać automatyczne działania naprawcze na podstawie uruchomionych alarmów.
       46. Monitorowanie urządzeń firm trzecich: Musi monitorować urządzenia firm trzecich za pomocą paczek monitorujących.
       47. Monitorowanie aplikacji i serwerów: Powinno monitorować aplikacje, serwery aplikacyjne oraz bazy danych firm trzecich za pomocą paczek monitorujących.
       48. Monitorowanie zmian: Musi monitorować zmiany na poziomie systemów operacyjnych.
       49. Paczki dla Multi Cloud: Powinno posiadać paczki do monitorowania platform Multi Cloud, takich jak AWS, Microsoft Azure, Google Cloud
       50. Obsługa API: Musi umożliwiać odczyt i zapis wszystkich metryk poprzez otwarte API REST.
       51. Przyjazny interfejs: Powinno oferować interfejs użytkownika w języku polskim oraz angielskim.
    5. **Wymagania dotyczące automatyzacji chmury prywatnej**
       1. Zamawiający wymaga, aby oferowane oprogramowanie do automatyzacji chmury prywatnej spełniało następujące kryteria:
       2. Licencjonowanie: Oprogramowanie musi mieć możliwość licencjonowania na rdzeń fizycznego procesora lub procesora w celu zapewnienia licencjonowania dla całości dostarczonej infrastruktury przez Wykonawcę
       3. Zarządzanie cyklem życia: Musi zapewniać automatyczne zarządzanie pełnym cyklem życia zasobów IT (maszyn wirtualnych, kontenerów, serwerów fizycznych).
       4. Integracja z rozwiązaniami chmurowymi: Powinno umożliwiać integrację z chmurami publicznymi, takimi jak AWS, Microsoft Azure oraz Google Cloud Platform.
       5. Automatyzacja infrastruktury: Musi automatyzować infrastrukturę fizyczną i wirtualną, zapewniając funkcjonalność zarządzania środowiskiem VMware vSphere.
       6. Zarządzanie siecią: Powinno automatyzować zarządzanie siecią, w tym konfigurację VLAN ów, load balancerów oraz firewalli.
       7. Współpraca z systemami ITSM: Musi współpracować z systemami ITSM, takimi jak ServiceNow, umożliwiając automatyzację procesów zarządzania incydentami i zmianami.
       8. Definiowanie polityk: Powinno umożliwiać definiowanie polityk automatyzacji dla zasobów IT, w tym polityk zarządzania pojemnością i dostępnością.
       9. Monitorowanie zgodności: Musi monitorować zgodność z politykami bezpieczeństwa i zgodności.
       10. Integracja z narzędziami DevOps: Powinno integrować się z narzędziami DevOps, takimi jak GitLab oraz Kubernetes.
       11. Obsługa API: Powinno oferować otwarte API REST do integracji z innymi systemami.
       12. Interfejs użytkownika: Powinno oferować przyjazny interfejs użytkownika w języku polskim oraz angielskim.
    6. **Wymagania dotyczące zbierania, korelowania i analizowania logowania:** 
       1. Licencjonowanie: Oprogramowanie musi mieć możliwość licencjonowania na rdzeń fizycznego procesora lub procesora w celu zapewnienia licencjonowania dla całości dostarczonej infrastruktury przez Wykonawcę
       2. Centralne gromadzenie i analiza logów: Oprogramowanie musi umożliwiać centralne gromadzenie i analizę logów z urządzeń fizycznych wykorzystujących technologię „Syslog”.
       3. Integracja z oprogramowaniem monitorującym: Oprogramowanie musi integrować się z oprogramowaniem do monitorowania, umożliwiając uzyskanie natychmiastowego dostępu do logów konkretnego urządzenia fizycznego z poziomu konsoli użytkownika.
       4. Personalizacja i wizualizacja logów: Oprogramowanie musi umożliwiać personalizację i wizualizację logów w postaci wykresów liniowych, kołowych oraz słupkowych.
       5. Integracja z oprogramowaniem do zarządzania klastrem: Oprogramowanie musi w pełni integrować się z oprogramowaniem do zarządzania klastrem wirtualizacyjnym.
       6. Wbudowana baza wiedzy: Oprogramowanie musi posiadać wbudowaną bazę wiedzy dotyczącą logów oraz zdarzeń dla platformy wirtualizacyjnej VMware.
       7. Udostępnianie raportów: Oprogramowanie musi umożliwiać udostępnianie raportów za pomocą URL kierującego do systemu logowania wysyłanego do odbiorcy.
       8. Korelacja zdarzeń i graficzna prezentacja: Oprogramowanie musi umożliwiać łatwą korelację wybranych zdarzeń w infrastrukturze fizycznej/wirtualnej oraz ich graficzną prezentację.
       9. Personalizacja interfejsu graficznego:Oprogramowanie musi posiadać możliwość personalizacji interfejsu graficznego w zależności od użytkownika/operatora.
       10. Przeszukiwanie logów:Oprogramowanie musi umożliwiać łatwe i szybkie przeszukiwanie logów w oparciu o zdefiniowane przez użytkownika kryteria.
       11. Analiza logów z różnych urządzeń: Oprogramowanie musi posiadać funkcjonalność implementacji dedykowanych modułów do analizy logów innych urządzeń fizycznych, takich jak macierze dyskowe i przełączniki LAN.
       12. Efektywna analiza logów: Oprogramowanie musi posiadać mechanizmy efektywnej analizy wszystkich rodzajów logów, w tym logów aplikacji, sieciowych, plików konfiguracyjnych, danych wydajnościowych, zrzutów awaryjnych oraz logów „nieustrukturyzowanych”.
       13. Definiowanie struktury logów: Oprogramowanie musi umożliwiać definiowanie struktury dla logów nieustrukturyzowanych.
       14. Raportowanie utylizacji klastra: Oprogramowanie musi mieć możliwość raportowania utylizacji klastra wytworzonego na potrzeby przyjmowania dużych obciążeń EPS oraz przedstawiania tego zużycia w postaci grafów.
       15. Zabezpieczenie kanału wysyłania logów: Oprogramowanie musi dawać możliwość zabezpieczenia kanału wysyłania logów na zewnątrz za pomocą SSL.
       16. Granularna aktualizacja agentów: Oprogramowanie musi mieć możliwość granularnej aktualizacji pojedynczych agentów zainstalowanych na systemach operacyjnych.
       17. Rozłączność uprawnień:W oprogramowaniu uprawnienia do interfejsu prezentacji i analizy logów muszą być rozłączne z uprawnieniami do infrastruktury, z której zbierane są logi.
       18. Generowanie i eksportowanie raportów: Oprogramowanie musi umożliwiać generowanie i eksportowanie dowolnych raportów związanych z zarejestrowanymi zdarzeniami i logami oraz tworzenie raportów wysyłanych zgodnie z zdefiniowanymi parametrami czasowymi.
       19. Tworzenie klastra: Oprogramowanie musi umożliwiać stworzenie klastra składającego się z co najmniej 8 węzłów, z których każdy ma wydajność 5 000 EPS, co sumarycznie daje 40 000 EPS oraz 20 TB przestrzeni dyskowej.
       20. Wsparcie dla transformacji logów: Oprogramowanie musi wspierać transformację logów, w tym filtrowanie, przekazywanie do innych systemów i maskowanie logów.
       21. Logowanie zdarzeń z Kubernetes: Oprogramowanie musi posiadać możliwość logowania zdarzeń z platformy Kubernetes za pomocą agenta fluentd.
       22. Określanie czasu retencji danych: Oprogramowanie musi mieć możliwość określania czasu retencji danych i archiwizacji logów na zewnętrznej macierzy dyskowej, z możliwością granularnego ustawiania retencji dla różnych typów logów.
       23. Instalacja agentów na systemach operacyjnych:Oprogramowanie musi mieć możliwość instalacji agentów na systemach operacyjnych Windows i Linux w celu zbierania logów oraz umożliwiać granularną aktualizację poszczególnych agentów.
    7. Oto przekształcone wymagania dotyczące tworzenia platformy konteneryzacyjnej opartej na Kubernetes w formie specyfikacji:
       1. **Wymagania dotyczące tworzenia platformy konteneryzacyjnej opartej na Kubernetes:**
       2. Certyfikacja przez CNCF: Oprogramowanie musi być certyfikowane przez Cloud Native Computing Foundation (CNCF) w ramach programu certyfikacji zgodności z oprogramowaniem Kubernetes. Link do strony CNCF: [CNCF Software Conformance] (<https://www.cncf.io/certification/software> conformance/).
       3. Licencjonowanie oprogramowania: Oprogramowanie musi mieć możliwość licencjonowania na rdzeń fizycznego procesora lub procesora w celu zapewnienia licencjonowania dla całości dostarczonej infrastruktury przez Wykonawcę
       4. Definiowanie limitów zasobów systemowych: Platforma musi umożliwiać deklaratywne definiowanie limitów zasobów systemowych, takich jak pamięć RAM i moc procesora, dostępnych dla projektu (grupy obiektów tj. wiele klastrów Kubernetes, maszyn wirtualnych), jak i dla poszczególnych kontenerów aplikacji.
       5. Automatyczne tworzenie i zarządzanie klastrami: Platforma musi umożliwiać automatyczne stworzenie i zarządzanie co najmniej 100 klastrami Kubernetes, bez ograniczeń wynikających z licencji i wsparcia technicznego.
       6. Wielozadaniowość: Platforma musi umożliwiać uruchamianie wielu aplikacji równocześnie na współdzielonych zasobach sprzętowych, umożliwiając budowanie aplikacji pracujących w oparciu o maszyny wirtualne oraz mikro serwisy.
       7. Zarządzanie infrastrukturą: Platforma do automatycznego tworzenia i zarządzania klastrami Kubernetes musi posiadać narzędzia do zarządzania infrastrukturą poprzez Cluster API, w tym automatyczne tworzenie klastrów, modyfikowanie ilości węzłów i ich wielkości (moc CPU, pojemność RAM, pojemność dyskowa), usuwanie klastrów oraz aktualizowanie do nowszej wersji.
       8. Środowisko wykonawcze kontenera: Platforma musi zapewniać środowisko wykonawcze kontenera umożliwiające interakcję z wtyczkami sieciowymi (CNI) i pamięcią masową (CSI).
       9. Oprogramowanie sieciowe: Platforma musi posiadać możliwość wyboru co najmniej dwóch różnych rodzajów oprogramowania sieciowego w ramach automatycznego tworzenia klastra Kubernetes przez interfejs CNI. Platforma musi wspierać integrację z zewnętrznymi rozwiązaniami klasy SDN (Software Defined Network), umożliwiając tworzenie polityk bezpieczeństwa z poziomu SDN.
       10. Trwałe zasoby pamięci: Platforma musi umożliwiać realizowanie trwałych zasobów na kompatybilnej pamięci masowej poprzez zintegrowaną wtyczkę CSI, co najmniej w trybie pojedynczego odczytu.
       11. Praca w środowiskach zamkniętych: Platforma do tworzenia i zarządzania klastrami Kubernetes musi umożliwiać pracę w środowiskach zamkniętych (air gapped environments).
       12. Przesyłanie logów: Platforma musi umożliwiać przesyłanie logów do zewnętrznych systemów logowania.
       13. Budowanie i uruchamianie aplikacji: Platforma musi umożliwiać budowanie i uruchamianie aplikacji stanowych i bezstanowych na bazie orkiestratora Kubernetes, który musi posiadać wsparcie producenta oprogramowania.
       14. Izolacja aplikacji: Platforma musi umożliwiać izolację aplikacji przy użyciu technologii kontenerów, umożliwiając uruchamianie wielu odizolowanych aplikacji na jednej instancji systemu operacyjnego z dostępem do ograniczonych zasobów systemowych, takich jak pamięć RAM, moc procesora i system plików.
       15. Przekazywanie danych do systemu SIEM: Platforma powinna zapewniać przekazywanie danych do systemu SIEM.
       16. Zarządzanie w chmurze prywatnej: Platforma musi mieć możliwość uruchomienia i zarządzania w chmurze prywatnej opartej o wirtualizator VMware vSphere w wersji 7 lub nowszej. Który posiada Zamawiający.
    8. **Wymagania dotyczące tworzenia i zarządzania sieciami wirtualnymi:**
       1. Budowa sieci IP: Oprogramowanie musi umożliwiać tworzenie sieci IP w środowisku wirtualnym na bazie zaoferowanego wirtualizatora mocy obliczeniowej.
       2. Niezależność od topologii fizycznej: Oprogramowanie musi pozwalać na tworzenie wirtualnych sieci niezależnie od topologii sieci fizycznej i używanych protokołów.
       3. Wirtualny przełącznik: Musi mieć funkcję tworzenia wirtualnego przełącznika L2 w jądrze wirtualizatora, wspieranego przez producenta platformy wirtualizacyjnej.
       4. Wirtualny router: Musi posiadać funkcję tworzenia wirtualnego routera w jądrze Hypervisora, działającego jako rozproszona brama domyślna dla środowiska serwerów wirtualnych, bez potrzeby wynoszenia ruchu do fizycznych przełączników.
       5. Segmenty sieci wirtualnej: Musi wspierać tworzenie segmentów sieci przy użyciu technologii GENEVE lub równoważnej.
       6. Łączenie środowisk: Musi umożliwiać łączenie zwirtualizowanego środowiska GENEVE z niezwirtualizowanym środowiskiem VLAN.
       7. Wsparcie protokołów routingu: Musi wspierać OSPFv2, BGP, BFD.
       8. Translacja adresów IP: Musi obsługiwać SNAT i DNAT.
       9. Serwer DHCP: Musi dynamicznie nadawać adresy IP.
       10. REST API: Musi umożliwiać automatyzację wdrażania lub modyfikacji konfiguracji poprzez REST API.
       11. Aktualizacje: Aktualizacje powinny odbywać się przez portal umożliwiający planowanie, uruchamianie, przegląd elementów systemu oraz sprawdzanie konsystencji działania przed i po aktualizacji.
       12. Wsparcie JSON: Musi obsługiwać pliki danych JSON.
       13. Zabezpieczenie przed nieautoryzowanymi zmianami IP: Musi blokować ruch w przypadku nieautoryzowanej zmiany adresu IP wirtualnej maszyny.
       14. Tunelowanie IPSeC: Musi umożliwiać terminowanie tuneli IPSeC site to site z uwierzytelnieniem za pomocą klucza współdzielonego lub certyfikatu.
       15. Integracja z antywirusami: Musi natywnie integrować się z rozwiązaniami antywirus/antymalware bezagentowo.
       16. Integracja z Next Generation Firewall: Musi wspierać integrację z minimum trzema produktami Next Generation Firewall w warstwie 7 ISO OSI.
       17. Przekierowanie ruchu: Musi umożliwiać przekierowanie ruchu warstwy 2 do rozwiązań firm trzecich z obszaru bezpieczeństwa.
       18. Wsparcie VRF: Musi wspierać mechanizm VRF w wirtualizacji sieci.
       19. Analiza przepływów sieciowych: Musi analizować przepływy sieciowe, w tym IPFIX, w warstwie wirtualizacji opartej na VMware vSphere.
       20. Raporty przepływów: Musi tworzyć raporty przepływów z informacjami o adresach IP i portach TCP/UDP dla środowiska wirtualnego.
       21. Kolektor ruchu sieciowego: Musi mieć kolektor ruchu sieciowego do analizy.
       22. Wizualizacja ścieżki logicznej: Musi wizualizować ścieżkę logiczną i przejścia między maszynami wirtualnymi w topologii logicznej.
       23. Zarządzanie wieloma instancjami: Musi umożliwiać zarządzanie minimum trzema lokalnymi instancjami oprogramowania.
       24. Wsparcie procesu troubleshooting: Musi mieć moduł wsparcia procesu poszukiwania błędów.
    9. **Wymagania dotyczące monitorowania i analizowania sieci oraz polityk firewall w sieciach wirtualnych i fizycznych:**
       1. Analiza przepływów sieciowych: Musi analizować przepływy sieciowe, w tym IPFIX, w warstwie sieciowej VMware vSphere oraz dla urządzeń posiadanych przez Zamawiającego (minimum Netflow).
       2. Raporty przepływów: Musi tworzyć raporty z informacją o adresach IP oraz portach TCP/UDP dla środowiska wirtualnego, przedstawiające ruch między konkretnymi maszynami wirtualnymi.
       3. Wbudowany kolektor: Musi mieć wbudowany kolektor ruchu sieciowego do analizy.
       4. Rekomendacje dla reguł firewall: Musi generować rekomendacje dla reguł firewall na bazie zebranych przepływów.
       5. Wizualizacja ścieżki logicznej: Musi wizualizować ścieżki logiczne i przejścia między maszynami wirtualnymi oraz komponentami sieciowymi w topologii logicznej i fizycznej, uwzględniając przełączniki, routery, firewalle i komponenty wirtualne.
       6. Wizualizacja przepływów: Musi wizualizować przepływy między sieciami wirtualnymi, podsieciami, aplikacjami oraz grupami bezpieczeństwa.
       7. Informowanie o maskowanych regułach: Musi informować o regułach firewall, które są maskowane przez inne reguły w kolejce analizy.
       8. Wizualizacja aplikacji: Musi wizualizować działające aplikacje oraz zależności między maszynami wirtualnymi, a także ruch zewnętrzny, wraz z glokalizacją zapytań.
       9. API: Musi posiadać API umożliwiające automatyzowanie wdrażania lub modyfikację konfiguracji.
       10. Backup i odtworzenie konfiguracji: Musi posiadać funkcję tworzenia kopii zapasowej i odtwarzania konfiguracji.
       11. Analiza przepływów w chmurze: Musi zapewniać widoczność przepływów dla maszyn wirtualnych w przynajmniej jednej usłudze chmury publicznej (np. AWS, Microsoft Azure).
       12. Moduł analityczny: Musi posiadać moduł analityczny wykrywający przekroczenia progów ruchu sieciowego powiązanego z maszynami wirtualnymi.
       13. Informowanie o źródłach ruchu: Musi informować o źródłach generujących największy ruch sieciowy.
       14. Troubleshooting: Musi posiadać moduł wsparcia procesu poszukiwania błędów.
       15. Automatyczne odkrywanie infrastruktury: Musi wspierać proces automatycznego odkrywania infrastruktury sieciowej i mapowania ruchu sieciowego aplikacji.
       16. Mapa urządzeń sieciowych: Musi wspierać mapę urządzeń sieciowych.
       17. Widoczność przepływów w Kubernetes: Musi wizualizować przepływy sieciowe do klastrów kontenerów działających na Kubernetes.
       18. Widoczność BGP EVPN: Musi zapewniać widoczność infrastruktury BGP EVPN (min. Arista– underlay oraz overlay).
       19. Zarządzanie retencją danych: Musi mieć funkcję konfigurowania i zarządzania okresem retencji gromadzonych danych.
       20. Zgodność ze standardem PCI: Musi analizować i przedstawiać wyniki analizy ruchu sieciowego zgodnie ze standardem bezpieczeństwa PCI (Payment Card Industry).
    10. **Specyfikacja Wymagań w Zakresie Wirtualizacji Przestrzeni Dyskowych**
        1. Współdzielona Przestrzeń Dyskowa: Oprogramowanie musi umożliwiać budowę współdzielonej przestrzeni dyskowej opartej na wewnętrznych dyskach serwerów fizycznych.
        2. Licencjonowanie i Funkcjonalność: Licencje na oprogramowanie muszą być licencjonowane w sposób elastyczny, umożliwiający dostosowanie do potrzeb Zamawiającego. Proponowane licencje powinny być oparte na ilości używanych przestrzeni dyskowej oraz liczbie rdzeni fizycznych serwerów.
        3. Obsługa Dysków SSD i HDD: System musi wspierać konfiguracje hybrydowe (SSD i HDD) oraz all flash (SSD SAS/SATA/NVMe). Musi wspierać konfiguracje z wyłącznie dyskami NVMe.
        4. Cache’owanie Operacji : Musi zapewniać optymalizację wydajności poprzez wbudowaną funkcjonalność cache’owania operacji zapisu i odczytu.
        5. Rezerwacja Cache: Musi posiadać funkcjonalność rezerwacji części dysku „cache” dla poszczególnych maszyn wirtualnych.
        6. Wsparcie dla NVMe: Musi wspierać technologie NVMe i cache’owanie operacji zapisu z wykorzystaniem dysków NVMe. Powinno pozwalać na wsparcie dla cache o rozmiarze do 1.6TB per grupa dyskowa.
        7. Hot Plug dla NVMe : Musi wspierać hot plug dla dodawania i wyjmowania dysków NVMe na minimum dwóch producentów serwerów.
        8. Aktualizacje i Monitoring: Oprogramowanie musi umożliwiać aktualizację i kontrolę wersji oprogramowania do wirtualizacji pamięci masowej oraz komponentów serwera (dyski, kontrolery, karty sieciowe) z poziomu centralnej konsoli zarządzającej.
        9. Skalowalność : Musi umożliwiać zmniejszanie lub zwiększanie przestrzeni dyskowej (dysków lub serwerów) bez przestoju dla maszyn wirtualnych.
        10. Integracja z Warstwą Wirtualizacji: Musi być zintegrowane z warstwą wirtualizacji bez potrzeby dodatkowych komponentów.
        11. Obsługa Dysków Wirtualnych : Musi wspierać dyski wirtualne do rozmiaru 62TB.
        12. Bezpieczeństwo i Redundancja Musi zapewniać mechanizmy zabezpieczania danych na wypadek awarii sprzętowej w ramach lokalizacji lub szafy rack. Musi umożliwiać szyfrowanie przestrzeni dyskowej przydzielonej do serwerów wirtualnych.
        13. Wsparcie dla NFS i SMB:Musi posiadać funkcjonalność uruchomienia usług NFS (wersja 3 oraz 4.1) z poziomu centralnej konsoli zarządzającej klastrem wirtualizacyjnym.
        14. Automatyzacja i Integracja: Musi posiadać interfejs API umożliwiający automatyzowanie wdrażania lub modyfikacji konfiguracji systemu. Musi wspierać tworzenie i konfigurowanie polityk niezawodnościowych, wydajnościowych i pojemnościowych przypisanych z granulacją na poziomie dysków maszyn wirtualnych.
        15. Wsparcie dla protokółu RDMA : Musi pozwalać na wykorzystanie protokołu RDMA.
        16. Szyfrowanie i Klucze Szyfrujące :Musi wspierać natywnego dostawcę kluczy szyfrujących oraz zewnętrznych dostawców.
        17. Wsparcie dla SHA256 : Musi wspierać szyfrowanie na poziomie SHA256.
        18. Dedykacja i Kompresja : Musi umożliwiać włączanie/wyłączanie deduplikacji i kompresji na żądanie.
        19. Erasure Coding : Musi zapewniać mechanizmy optymalizacji wykorzystania przestrzeni dyskowych (erasure coding) dla RAID 5 i RAID 6.
        20. Wsparcie dla Kubernetes CSI Driver: Musi współpracować z Kubernetes CSI driver (Container Storage Interface) dla automatycznego zarządzania zasobami NFS.
        21. Obsługa Maszyn Wirtualnych: Musi umożliwiać działanie w klastrze o ilości minimum 500 maszyn wirtualnych.
        22. Zarządzanie Środowiskiem: Musi wspierać monitoring i zarządzanie całym środowiskiem wirtualizacji obliczeniowej i przestrzeni dyskowej z jednego panelu zarządzającego.
        23. Kompaktowość i Efektywność: Powinno pozwalać na efektywne wykorzystanie przestrzeni dyskowej przy zachowaniu wysokiej dostępności i wydajności operacji I/O.
    11. Zaawansowana Migracja Maszyn Wirtualnych i Systemów Operacyjnych do Chmury Publicznej
        1. Migracja Masowa: Oprogramowanie musi umożliwiać równoczesną migrację wielu maszyn wirtualnych z wykorzystaniem protokołów replikacji danych, zarówno między lokalnym oprogramowaniem wirtualizacyjnym, jak i chmurą publiczną.
        2. Migracja Pojedynczych Maszyn Wirtualnych Bez Przestojów: Oprogramowanie musi oferować możliwość przenoszenia pojedynczych maszyn wirtualnych pomiędzy lokalnym środowiskiem wirtualizacyjnym a chmurą publiczną bez przerywania ich działania.
        3. Migracja Wyłączonych Maszyn Wirtualnych: Funkcjonalność przenoszenia wyłączonych maszyn wirtualnych przy użyciu protokołu NFC między lokalnym oprogramowaniem wirtualizacyjnym a chmurą publiczną musi być zapewniona.
        4. Migracja z Replikacją i Bez Przestojów: Oprogramowanie musi umożliwiać migrację maszyn wirtualnych z użyciem protokołu replikacji oraz bez przerywania ich działania pomiędzy lokalnym oprogramowaniem wirtualizacyjnym a chmurą publiczną.
        5. Migracja Systemów Operacyjnych: Oprogramowanie musi wspierać migrację systemów operacyjnych (Windows, Linux) z serwerów fizycznych do lokalnego oprogramowania wirtualizacyjnego oraz chmury publicznej.
        6. Optymalizacja WAN: Oprogramowanie musi posiadać funkcjonalność optymalizacji wykorzystania sieci WAN, minimalizując opóźnienia i zwiększając przepustowość podczas migracji maszyn wirtualnych.
        7. Bezpieczeństwo Transmisji Danych: Oprogramowanie musi zapewniać kryptografię dla ruchu sieciowego podczas migracji maszyn wirtualnych, gwarantując bezpieczeństwo transmisji danych.
        8. Migracja Bez Zmiany Adresów IP: Oprogramowanie musi umożliwiać migrację maszyn wirtualnych pomiędzy lokalnym środowiskiem wirtualizacyjnym a chmurą publiczną bez konieczności zmiany adresów IP.
        9. Wsparcie dla Starszych Wersji vSphere: Oprogramowanie musi wspierać migrację maszyn wirtualnych dla starszych wersji oprogramowania do wirtualizacji vSphere.
        10. Rozszerzenie Centrum Danych: Oprogramowanie musi umożliwiać rozszerzenie istniejącego centrum danych opartego na lokalnym oprogramowaniu do wirtualizacji do środowiska wirtualizatora w chmurze publicznej.
        11. Ochrona Przed Katastrofami (DR): Oprogramowanie musi oferować funkcjonalność ochrony przed katastrofami, zapewniając ciągłość działania oraz integralność danych w przypadku awarii centrum danych.
    12. **Portal samoobsługowy do automatycznego tworzenia maszyn wirtualnych z bazami danych**
        1. Tworzenie Maszyn Wirtualnych z Bazą Danych: Oprogramowanie musi umożliwiać tworzenie maszyn wirtualnych z bazą danych MySQL lub Postgres, z możliwością dostosowania zasobów obliczeniowych (pamięć wirtualna, procesory) w zależności od uprawnień użytkownika.
        2. Skalowanie Instancji Maszyn Wirtualnych: Oprogramowanie musi umożliwiać skalowanie maszyn wirtualnych z bazą danych MySQL lub Postgres (skalowanie w górę, skalowanie w dół, rozszerzenie dysku) w zależności od zapotrzebowania.
        3. Aktualizacje Maszyn Wirtualnych: Oprogramowanie musi umożliwiać planowanie i przeprowadzanie aktualizacji maszyn wirtualnych z bazą danych MySQL lub Postgres, w tym instalację poprawek i aktualizacji systemu operacyjnego, na żądanie lub według harmonogramu.
        4. Kopie Zapasowe i Odzyskiwanie Danych: Oprogramowanie musi umożliwiać tworzenie kopii zapasowych, dzienników transakcji oraz odzyskiwanie do punktu w czasie dla baz danych MySQL lub Postgres, na żądanie lub według harmonogramu.
        5. Replikacja Danych: Oprogramowanie musi wspierać tworzenie replikacji (zimna/gorąca lub repliki do odczytu) w zarządzanych strefach.
        6. Monitorowanie Systemu: Oprogramowanie musi umożliwiać monitorowanie silnika bazy danych (MySQL i Postgres), infrastruktury vSphere oraz sieci wirtualnej.
        7. Interfejs Graficzny: Oprogramowanie musi posiadać interfejs graficzny w HTML5, działający jako portal samoobsługowy.
    13. **Serwis gwarancyjny dla oprogramowania chmury prywatnej**
        1. Jednoźródłowa Obsługa Zgłoszeń: Serwis gwarancyjny musi być świadczony przez jedną organizację na każdym etapie procesu zgłoszenia serwisowego. Przekazywanie zgłoszeń pomiędzy różnymi podmiotami oraz wykupienie serwisu gwarancyjnego u partnerów OEM są niedopuszczalne. Serwis ten musi być częścią licencji w ramach subskrypcji.
        2. Poufność i Systemy Obsługi: Komunikacja podczas obsługi zgłoszeń serwisowych musi być poufna. Zgłoszenia nie mogą być przetwarzane w systemach informatycznych niezależnych od producenta oprogramowania.
        3. Dostępność Wsparcia: Zgłaszanie problemów musi być możliwe 24 godziny na dobę, 7 dni w tygodniu (7/24).
        4. Priorytetyzacja i Reakcja   
           Priorytet 1 (Severity 1) : Czas reakcji do 30 minut, obsługa 24/7, z zasadą „follow the sun”.  
           Priorytet 2 (Severity 2) : Czas reakcji do 2 godzin, obsługa w ciągu 10 godzin dziennie przez 5 dni w tygodniu.  
           Priorytet 3 (Severity 3) : Czas reakcji do 4 godzin, obsługa w ciągu 10 godzin dziennie przez 5 dni w tygodniu.

Priorytet 4 (Severity 4) : Czas reakcji do 1 dnia roboczego, obsługa w ciągu 10 godzin dziennie przez 5 dni w tygodniu.

* + - 1. Dostęp do materiałów i narzędzi: Użytkownik musi mieć dostęp do dokumentacji technicznej, bazy wiedzy, poprawek, uaktualnień oraz portalu internetowego umożliwiającego zarządzanie licencjami i zgłaszanie problemów. Portal serwisowy musi umożliwiać zgłaszanie problemów bez limitu ilości zgłoszeń.
      2. Monitorowanie i Analiza: Dostęp do narzędzi do automatycznego zbierania danych o statusie i działaniu produktów, takich jak wirtualizacja mocy obliczeniowej, sieci komputerowej i przestrzeni dyskowej. Możliwość instalacji narzędzia w formie wirtualnego appliance do automatycznego przesyłania zaszyfrowanych danych (TLS minimum 1.2) oraz otrzymywania wyników analizy i rekomendacji na portalu internetowym.
      3. Automatyzacja i Wsparcie Logów: Narzędzie musi automatycznie zbierać i przesyłać pliki dziennika logów związane z wirtualizacją mocy obliczeniowej, sieci komputerowej i przestrzeni dyskowej w ramach zgłoszeń serwisowych.
  1. **Serwer wraz z rozszerzeniem oprogramowania do chmury prywatnej – specyfikacja szczegółowa**

3.1 Serwer spełnia wszystkie wymagania wymienione dla serwera typ 1 wraz z wyposażeniem.

3.2 Rozszerzenie oprogramowania do budowy chmury prywatnej ma umożliwiać stosowanie wszystkich funkcjonalności oprogramowania do budowy chmury prywatnej, opisane w specyfikacji szczegółowej w odniesieniu do kupowanego serwera.

3.2 Rozszerzenie oprogramowania do budowy chmury prywatnej umożliwia wykorzystanie wszystkich zasobów dostarczanego serwera, a w szczególności. pamięci RAM, przestrzeni dyskowej i rdzeni procesora.