Załącznik nr 1 do SIWZ

numer sprawy: 32/BP/SMUP/POWER/PN/2020

**Opis Przedmiotu Zamówienia – zmieniony w dniu 4-06-2020 r.**

Przedmiotem zamówienia jest dostawa oraz wdrożenie uniwersalnej infrastruktury sprzętowo-systemowej w Centrum Przetwarzania Danych w Głównym Urzędzie Statystycznym i dostawa bezterminowych licencji oprogramowania systemowego, narzędziowego oraz bazodanowego dla CPD GUS na potrzeby projektu „System Monitorowania Usług Publicznych – wdrożenie SMUP”, realizowanego w ramach Programu Operacyjnego Wiedza Edukacja Rozwój 2014-2020.

Zamówienie publiczne składa się z dwóch części:

**Część I**

Dostawa oraz wdrożenie uniwersalnej infrastruktury sprzętowo-systemowej w Centrum Przetwarzania Danych w Głównym Urzędzie Statystycznym na potrzeby projektu „System Monitorowania Usług Publicznych – wdrożenie SMUP” realizowanego w ramach Programu Operacyjnego Wiedza Edukacja Rozwój 2014-2020.

**Część II**

Dostawa bezterminowych licencji oprogramowania systemowego narzędziowego oraz bazodanowego dla Centrum Przetwarzania Danych w Głównym Urzędzie Statystycznym na potrzeby projektu „System Monitorowania Usług Publicznych – wdrożenie SMUP” realizowanego w ramach Programu Operacyjnego Wiedza Edukacja Rozwój 2014-2020.

**Część I**

**W ramach Części I, Wykonawca zrealizuje 3 zadania:**

1. Zadanie I - Dostawa oraz wdrożenie wyspecyfikowanego sprzętu oraz dostawa dodatkowych elementów infrastruktury sprzętowej w tym kabli, jeśli będą niezbędne do prawidłowego wdrożenia.
2. Zadanie II - Dostawa oraz wdrożenie oprogramowania do wirtualizacji.
3. Zadanie III - Dostawa oraz wdrożenie oprogramowania do backupu z wykorzystaniem urządzenia do backupu dyskowego z deduplikacją.
4. **Wspólne uwarunkowania dla zadań oraz opis posiadanego przez Zamawiającego środowiska**

Prace wdrożeniowe i konfiguracyjne będą realizowane w Centrum Przetwarzania Danych GUS w Warszawie – Al. Niepodległości 208.

Z uwagi na fakt, iż prace wdrożeniowe i rekonfiguracyjne będą prowadzone na działającym środowisku sprzętowo–systemowo–aplikacyjnym, wymagane jest zachowanie ciągłości działania tego środowiska oraz minimalizacja przestojów.

W Centrum Przetwarzania Danych Zamawiający posiada środowisko serwerowe oparte na systemach operacyjnych MS Windows Server stanowiących platformę systemową dla następujących komponentów infrastruktury informatycznej:

* Systemu usług katalogowych bazującego na Microsoft Active Directory w wersji Windows 2012 R2 o funkcjonalności lasu i domeny na poziomie wersji Windows Server 2008 R2.
* Modułu monitorowania wydajności oraz dostępności aplikacji i usług zbudowanego na bazie systemu Microsoft System Center Operations Manager 2012 R2.
* Modułu zarządzania konfiguracją dla serwerów stworzonego w oparciu o oprogramowanie Microsoft System Center Configuration Manager 2012 R2.
* Systemu poczty Microsoft Exchange 2010 Sp3.
* Środowisk do wirtualizacji serwerów bazujących na oprogramowaniu VMware vCenter 5.1
* Serwerów bazodanowych z oprogramowaniem Microsoft SQL Server 2008 Enterprise oraz 2012 Enterprise.
1. Opis posiadanej infrastruktury sprzętowej

Infrastruktura sprzętowa w Centrum Przetwarzania Danych kształtowała się w latach 2008-2014, w miarę realizacji kolejnych funkcjonalnych projektów SISP.

Zasoby serwerowe w Centrum Przetwarzania Danych zostały poszerzone o serwery blade HPE rozmieszczone w infrastrukturach blade HP C7000 oraz serwery blade IBM Flex System rozmieszczone w infrastrukturach blade IBM Flex System Enterprise Chassis.

Zamawiający posiada dostępowe przełączniki sieciowe Cisco Nexus N9K-C9336C-FX2-B wyposażone we wkładki QSFP 40GBASE-SR4.

Skonsolidowane środowisko sprzętowe pamięci masowych zostało oparte na bazie macierzy dyskowych SAN HP EVA 4400, SAN HP EVA 8100, SAN HP EVA 8400, SAN NetApp3240 i IBM Storwize V7000.

W czwartym kwartale 2019 roku zasoby Centrum Przetwarzania Danych w budynku GUS powiększyły się o poniższe zasoby:

* infrastruktury serwerowo-sieciowe HPE Synergy12000 Frame;
* serwery HPE SY 480 Gen10 dwu procesorowe (20,16 i 8 rdzeniowe) interfejsami sieciowymi 25GbE
* półki dyskowe SAS umieszczane w infrastrukturze serwerowo-sieciowej HPE Synergy z dyskami SSD Mixed Used (DWPD˃=3) o pojemności 6,4 TB;
* urządzenie do backupu dyskowego z deduplikacją HPE StoreOnce 5250;
* macierz dyskową HPE 3PAR StoreServ 8000.
1. Opis obecnego środowiska zwirtualizowanego

W Centrum Przetwarzania Danych w budynku GUS oprócz środowiska serwerów fizycznych znajdują się trzy współpracujące ze sobą środowiska wirtualizacyjne Vmware, dwa produkcyjne i jedno zarządzające, z oprogramowaniem VMware vSphere w wersji 5.1. Łącznie działa tam 50 hostów fizycznych.

W czwartym kwartale 2019 do Centrum Przetwarzania Danych w budynku GUS zakupiono oprogramowanie wirtualizacyjne VMware Cloud Foundation Advanced (na nowe serwery HPE SY) z funkcjami NSX i vSAN. Nowa infrastruktura zwirtualizowana powinna umożliwiać integrację z infrastrukturą istniejącą, w szczególności przenoszenie istniejących maszyn wirtualnych z obecnej infrastruktury do nowej. Do backupowania zasobów środowiska wirtualnego na zewnętrzne zasoby dyskowe zakupiono oprogramowania Veeam Enterprise Plus 9.5.

1. **Szczegółowa specyfikacja i opisy zadań do realizacji przez Wykonawcę.**
2. **Zadanie I - Dostawa oraz wdrożenie wyspecyfikowanego sprzętu oraz dostawa dodatkowych elementów infrastruktury sprzętowej w tym kabli, jeśli będą niezbędne do prawidłowego wdrożenia.**

W ramach Zadania I Wykonawca dostarczy do siedziby Głównego Urzędu Statystycznego,
w terminie uzgodnionym z Zamawiającym, z zastrzeżeniem dochowania terminu realizacji Umowy, urządzenia w ilościach wyspecyfikowanych w Tabeli 1 zgodnych z opisem w Tabelach 2-7,
a następnie wykona wdrożenie tego sprzętu.

Zamawiający wymaga dostarczenie sprzętu wraz ze standardową, dołączaną przez producenta danego urządzenia dokumentacją techniczną w języku polskim lub angielskim oraz instrukcją obsługi, która powinna być w języku polskim.

Zamawiający wymaga dostarczenia sprzętu:

* fabrycznie nowego, nie używanego w innych środowiskach ani projektach,
* wyprodukowanego nie wcześniej niż 6 miesięcy przed dostawą do Zamawiającego,
* pochodzącego z autoryzowanego kanału sprzedaży producentów zaoferowanych urządzeń,
* nieprzeznaczonego, w dniu składania ofert, przez producenta do wycofania z produkcji,
* współpracującego z siecią energetyczną o parametrach: 230 V ± 10%, 50 Hz, jednofazowo i wyposażonego w przewody zasilające,
* objętego okresem gwarancyjnym,
* posiadającego najnowszą dostępną w dniu składania ofert wersję oprogramowania.

Wykonawca w treści złożonej oferty oświadczy, że Urządzenia dostarczone Zamawiającemu będą spełniały powyższe wymagania.

**Tabela 1. Zbiorcza specyfikacja ilościowa sprzętu dostarczanego w Zadaniu I:**

|  |  |  |
| --- | --- | --- |
| Typ sprzętu | Ilość szt. | Numer tabeli |
| Infrastruktura serwerowo-sieciowa | 1 | Tabela 2(tabele 2.1,2.2) |
| Serwer typ 1 (2 procesory po 20 rdzeni)  | 4 | Tabela 3 |
| Serwer typ 2 (2 procesory po 8 rdzeni)  | 2 | Tabela 4 |
| Serwer typ 3 (2 procesory po 16 rdzeni) | 1 | Tabela 5 |
| Urządzenie do backupu dyskowego z deduplikacją | 1 | Tabela 6 |
| Szafa rack | 2 | Tabela 7 |

Zamawiający wymaga dostarczenia infrastruktury serwerowo-sieciowej wyspecyfikowanej w Tabeli 2, urządzenia do backupu dyskowego z deduplikacją wyspecyfikowanego w Tabeli 6, serwerów zgodnych ze specyfikacją zapisaną w Tabelach 3, 4 i 5, przy czym procesory serwerów opisanych w Tabeli 3 powinny być wyłącznie dwudziestordzeniowe, procesory serwerów opisanych w Tabeli 4 powinny być wyłącznie ośmiordzeniowe, natomiast procesory serwerów opisanych w Tabeli 5 powinny być wyłącznie szesnastordzeniowe.

Wymaganie jest konieczne ze względu na licencjonowanie oprogramowania.

Serwery opisane w Tabelach 3, 4 i 5 będą docelowo umieszczone w infrastrukturze serwerowo-sieciowej opisanej w Tabeli 2 zgodnie z projektem uzgodnionym z Zamawiającym.

Zamawiający wymaga dostarczenia dodatkowych elementów infrastruktury sprzętowej w tym wkładek do interfejsów oraz kabli jeśli będą niezbędne do prawidłowego i efektywnego podłączenie dostarczonego sprzętu do infrastruktury sieci LAN i SAN Zamawiającego.

**Tabela 2.** **Infrastruktura serwerowo-sieciowa**

**Tabela 2.1 Wymagania podstawowe**

|  |  |  |
| --- | --- | --- |
| **Lp.** | **Parametr** | **Wymagania minimalne** |
| 1. | Typ infrastruktury serwerowo-sieciowej | Przystosowana do montażu w szafie typu rack 19”, składająca się z jednej lub większej liczby obudów, umożliwiająca instalację minimum 24 serwerów kasetowych dwuprocesorowych z procesorami Intel Xeon Cascade Lake bez konieczności rozbudowy o kolejne elementy sprzętowe. Pojedyncza obudowa wchodząca w skład infrastruktury o wysokości maksymalnej 10U.Infrastruktura obsługująca pasmo 40GbE i 100GbE oraz 32Gb FC. |
| 2. | Moduły komunikacyjne LAN | Wyposażona w minimum dwa niezależne moduły komunikacyjne 100GbE. Urządzenia umożliwiające agregację połączeń LAN/FCoE (Fibre Channel over Ethernet) w infrastrukturze i umożliwiające wyprowadzenie sygnałów LAN i FC/FCoE ze wszystkich serwerów z zachowaniem redundancji połączeń. Awaria dowolnego z zainstalowanych modułów nie może powodować utraty komunikacji dla żadnego z serwerów z siecią LAN. Każdy moduł posiadający minimum 12 portów o sumarycznym pasmie min. 400Gb.Co najmniej 2 z tych portów muszą pracować jako Ethernet 10GbE/40GbE/25GbE/100GbE oraz zamiennie mogą zostać rozszyte na minimum 2 porty 16Gb FC.Aktywne wszystkie porty w każdym module.Dla każdego z dostarczonych modułów należy dostarczyć: minimum 2 wkładki 100 Gb QSFP28 MPO SR4 100m.Sumarycznie z infrastrukturą wymagane jest dostarczenie minimum 6 wkładek 100 Gb QSFP28 MPO SR4 100m.Ponadto Wykonawca dostarczy do posiadanych przez Zamawiającego przełączników sieciowych Cisco Nexus N9K-C9336C-FX2-B 6 (sześć) wkładek 100Gb QSPF (kompatybilnych czyli nie powodujących utraty gwarancji producenta na te przełączniki) oraz kable umożliwiające włączenie urządzeń do infrastruktury sieciowej Zamawiającego. |
| 3. | Moduły Pamięci Masowej | W ramach infrastruktury należy dostarczyć min. 2 półki dyskowe SAS lub 2 macierze dyskowe FC (dopuszcza się zastosowanie macierzy zewnętrznej), każda umożliwiająca instalację min. 16 dysków 2,5 cala SAS/SATA/SSD. Półki mają być włożone w obudowy na serwery. Z dwoma półkami lub dwoma macierzami należy dostarczyć min. 32 dyski o sumarycznej pojemności min. 204TB Parametry podstawowe dysków :SAS, 12Gb, SSD Mixed Used (parametr DWPD >=3)Z oferowanymi półkami lub macierzami należy dostarczyć wszystkie niezbędne elementy typu przełączniki, kontrolery FC lub SAS w serwerach oraz odpowiednie kable umożliwiające w każdej obudowie na serwery podłączenie i udostępnienie zasobów dyskowych do co najmniej 6 serwerów blade. W celu zapewnienia redundancji wymagane są przynajmniej 2 przełączniki SAS lub FC. |
| 4. | Dodatkowa funkcjonalność modułów LAN | Zainstalowane moduły LAN/FC/FCoE w każdej obudowie z funkcjonalnością przydzielania adresów MAC i WWN predefiniowanych przez producenta rozwiązania kasetowego dla poszczególnych wnęk na serwery. Przydzielenie adresów powodujące zastąpienie fizycznych adresów kart konwergentnych lub Ethernet na serwerze. Musi istnieć także możliwość przenoszenia przydzielonych adresów pomiędzy wnękami w obudowie. Funkcjonalność ta może być realizowana zarówno poprzez moduły LAN w infrastrukturze jak i poprzez dodatkowe oprogramowanie producenta serwerów. Dodatkowo dla sieci LAN musi istnieć możliwość stworzenia niezależnych połączeń VLAN tak, aby między wydzielonymi sieciami nie było komunikacji. Musi istnieć możliwość określenia pasma przepustowości pojedynczego portu LAN na serwerze od 500Mb/s do min.25Gb/s, z dokładnością do 500Mb. Każdy moduł pozwalający na podział fizycznego portu w serwerze na 4 niezależne interfejsy logiczne z regulowaną szerokością pasma i oddzielnymi adresami MAC.  |
| 5. | Moduły komunikacyjne SAN FC | Każda z obudów wchodzących w skład infrastruktury wyposażona w min. 2 moduły SAN FC min. 32Gb, posiadające odpowiednią aktywną liczbę portów zewnętrznych FC zapewniających sumaryczną przepustowość w FullDuplex: 192Gb/s dla portów 8Gb/s, 384Gb/s dla portów 16 Gb/s, 768Gb/s dla portów 32Gb/s. Moduły zapewniające redundantne wyprowadzenie z każdego serwera zainstalowanego w obudowie pasma 2x32Gb FC (przy zastosowaniu dedykowanej dwuportowej karty FC). Awaria dowolnego z modułów SAN FC 32Gb nie może powodować utraty komunikacji serwera z siecią SAN FC. Każdy moduł SAN FC wyposażony w min. 8 wkładek SFP+ FC 32Gb SW. |
| 6. | Chłodzenie | Każda obudowa wyposażona w komplet redundantnych wentylatorów (typ hot plug, czyli możliwość wymiany podczas pracy urządzenia) zapewniających chłodzenie dla maksymalnej liczby serwerów i urządzeń I/O zainstalowanych w obudowie. Wentylatory niezależne od zasilaczy, wymiana wentylatora (wentylatorów) nie może powodować konieczności wyjęcia zasilacza (zasilaczy). |
| 7. | Zasilanie | Każda obudowa wyposażona w komplet zasilaczy redundantnych typu Hot Plug. System zasilania musi pracować w trybie redundancji N+N lub N+1, wymagane ciągłe dostarczenie mocy niezbędnej do zasilenia maksymalnej liczby serwerów i urządzeń I/O zainstalowanych w ­obudowie. Procesory serwerów winny pracować z nominalną, maksymalną częstotliwością.Obudowa przystosowana do zasilania jednofazowego. |
| 8. | Moduły zarządzające | Dwa redundantne, sprzętowe moduły zarządzające, moduły typu Hot Plug, umożliwiający podłączenie klawiatury, myszy i monitora. Moduły muszą zarządzać chłodzeniem i zasilaniem, a także dokonywać inwentaryzacji sprzętu w infrastrukturze. Muszą komunikować się z modułami zarządzającymi serwerów po dedykowanych łączach min.1GbE, niezależnych od kart sieciowych serwera.Nawet awaria wszystkich modułów komunikacyjnych LAN i SAN FC nie może powodować utraty dostępu do modułu zarządzania każdego z serwerów, czyli musi być możliwe m.in. przejęcie konsoli graficznej każdego z serwerów. |
| **Tabela 2.2 Wymagania dla systemu zarządzania infrastrukturą serwerowo-sieciową** |
| 1. | Zarządzanie  | Zarządzanie w oparciu o jednolite oprogramowanie, czyli z jednego panelu o jednym adresie IP.Oprogramowanie musi w sposób graficzny wizualizować stan poszczególnych elementów infrastruktury (stan normalnej pracy, ostrzeżenia, awarie). Musi istnieć możliwość modyfikacji panelu głównego aplikacji poprzez zmianę kategorii systemów, dla których prezentowany jest stan zdrowia/status. Na przykład musi istnieć możliwość zawężenia prezentacji stanu zdrowia tylko do serwerów kasetowych. |
| 2. | Serwery zarządzające  | Dwa dodatkowe serwery lub moduły zarządzające zainstalowane w oferowanej obudowie, ale niezajmujące żadnego z 24 slotów na serwery w infrastrukturze. Oprogramowanie zarządzające działające na tych serwerach lub modułach musi pracować w trybie wysokiej dostępności HA (High Availability). Awaria dowolnego z serwerów lub modułów nie może powodować przestoju w pracy oprogramowania zarządzającego ani utraty jakichkolwiek danych. Parametry serwerów lub modułów zarządzających, spełniające minimalne wymagania wydajnościowe podane przez producenta oprogramowania zarządzającego na publicznie dostępnych stronach. Wymagane wszystkie potrzebne licencje na systemy operacyjne i ewentualnie wirtualizator, potrzebne do uruchomienia oprogramowania zarządzającego. Jeżeli zapewnienie wysokiej dostępności dla systemu zarządzania wymaga dostarczenia współdzielonej macierzy, to taka macierz musi być częścią oferowanego rozwiązania i musi to być macierz niezależna od innych wyspecyfikowanych macierzy czy zasobów dyskowych.  |
| 3. | Podstawowe funkcje zarządzania | * zdalne włączanie/wyłączanie/restart niezależnie dla każdego serwera;
* bezagentowe zarządzanie i monitorowanie stanu urządzeń;
* pojedynczy interfejs zapewniający widoki, podsumowanie szczegółowych informacji o sprzęcie i oprogramowaniu układowym zainstalowanym na serwerach;
* zebrane dane muszą być udostępniane poprzez interfejs REST API oraz interfejs graficzny użytkownika;
* zarządzanie uprawnieniami użytkowników poprzez definiowanie ról.
 |
| 4. | Sposób zarządzania | Dostęp do aplikacji zarządzającej z serwera zarządzającego lub dowolnego innego miejsca poprzez przeglądarkę internetową (połączenie szyfrowane SSL/TLS) bez konieczności instalowania dodatkowego oprogramowania producenta serwera. |
| 5. | Liczba jednoczesnych sesji zarządzania | W danym momencie musi być niezależny, równoległy dostęp do konsol tekstowych i graficznych wszystkich serwerów. |
| 6. | Zdalna identyfikacja | Zdalna identyfikacja fizycznego serwera i obudowy za pomocą sygnalizatora optycznego. |
| 7. | Konfiguracja sprzętowa serwera | Zautomatyzowana konfiguracja sprzętowa każdego serwera kasetowego za pomocą profili. |
| 8. | Dodatkowe cechy oprogramowania do zarządzania | * konfiguracja środowiska serwerów kasetowych w oparciu o logiczne profile serwerowe obejmujące konfigurację serwera w zakresie sieci LAN i SAN (zonning, wolumeny) wraz z możliwością migracji pomiędzy wieloma obudowami lub serwerami. W zakres logicznego profilu serwerowego muszą wchodzić następujące parametry: adres MAC, adres WWN, sekwencja bootowania systemu, sposób konfiguracji adapterów NIC i HBA, ustawienia BIOS, wersja oprogramowania układowego i sterowników (dla Windows, VMware i Red Hat);
* Ustawienia BIOS pozwalające na minimum:

-włączenie/wyłączenie funkcji hyper threading w procesorach Intel;-włączenie/wyłączenie rdzeni procesora;-włączenie/wyłącznie funkcji wirtualizacyjnych;-zmiana ustawień poziomu poboru prądu;- ustawienia trybu turbo boost w procesorach Intel;- ustawienia trybu zabezpieczenia pamięci RAM; * zdalna aktualizacja oprogramowania układowego serwerów kasetowych, obudów, modułów LAN zainstalowanych w obudowie kasetowej;
* monitorowanie utylizacji serwera: procesorów, zasilania, temperatury;
* prezentacja w postaci graficznej logicznych i fizycznych połączeń pomiędzy serwerami kasetowymi, obudowami na serwery kasetowe, profilami serwerów i modułami interconnect oraz dyskami (wolumenami logicznymi) zaprezentowanymi z macierzy FC.
* integracja z narzędziami jak VMware vCenter oraz Microsoft System Center przez specjalną wtyczkę (np. dodatkowe zakładki) w tych aplikacjach, rozszerzającą możliwości zarządzania o warstwę sprzętową
* wbudowane raporty dotyczące użycia zasobów jak również zarejestrowanych zdarzeń z możliwością eksportu do plików w formacie xls, lub csv lub PDF;
* wbudowany system automatycznego wysyłania zgłoszeń do serwisu producenta w razie wystąpienia awarii dowolnego komponentu sprzętowego serwerów i obudów zarządzanych przez aplikację;
* aplikacja musi posiadać interfejs REST API, przez który możliwa jest integracja z narzędziami firm trzecich w tym środowiska opisywanego w dalszej części jako Platforma
 |
| 9. | Licencje | Licencje na powyższą funkcjonalność na wszystkie oferowane serwery. |

**Tabela 3.** **Serwer typ1 – 4 szt.**

**Opis minimalnych wymagań dla serwera do instalacji w infrastrukturze serwerowo-sieciowej**

|  |  |  |
| --- | --- | --- |
| **Lp.** | **Parametr** | **Wymagania minimalne** |
| 1. | Procesory (ilość i typ)  | 2 procesory, każdy min. dwudziestordzeniowy, klasy x86-64bit, dla których serwer osiąga wynik nie mniejszy niż 223 punktów w teście SPECrate2017\_int\_base, dla oferowanego modelu serwera w konfiguracji dwuprocesorowej. Wynik testu musi być potwierdzony przez organizację SPEC i opublikowany na jej oficjalnej stronie internetowej ([www.spec.org](http://www.spec.org)). |
| 2. | Pamięć RAM  | 1.5TB RDIMM DDR4 w modułach min. 64GB. Serwer posiadający minimum 24 sloty na pamięć. |
| 3. | Interfejsy sieciowe | Minimum 2 Interfejsy sieciowe min. 50GbE lub 4 interfejsy 25GbE (CNA, wspierające FCoE – funkcjonalność w standardzie), z możliwością podzielenia każdego interfejsu na min. 3 interfejsy sieciowe (posiadające własne adresy MAC oraz będące widoczne z poziomu systemu operacyjnego, jako fizyczne karty sieciowe) i kartę FC/FCoE o przepustowości min. 16Gb ( posiadającą własny adres WWN). Podział musi być niezależny od zainstalowanego na serwerze systemu operacyjnego/platformy wirtualizacyjnejDedykowana karta FC lub FCoE min. 2 portowe, 32Gb FC do podłączenia do zewnętrznej macierzy dyskowej FC.Dedykowany kontroler SAS 12G lub FC min.32Gb lub przełącznik FC znajdujący się w obudowie do podłączenia dysków z modułów pamięci masowych (opisanych w punkcie Moduły Pamięci Masowej) |
| 4. | Kontroler dyskowy | Sprzętowy kontroler do dysków wewnętrznych z 1GB pamięci cache podtrzymywanej bateryjnie. |
| 5. | Dyski twarde | Min. 2 wnęki przygotowane do instalacji dysków twardych typu hot plug. Zainstalowane dwa dyski hot-plug SSD, każdy o pojemności min. 240GB Mixed Use (DWPD>=3). |
| 6. | Sloty PCI-E | Trzy sloty PCIe 3.0, |
| 7. | Porty | 1 x USB 3.0 (wewnętrzny) lub 1x port na kartę SD |
| 8. | Wsparcie dla systemów operacyjnych i systemów wirtualizacyjnych | Microsoft Windows Server 2012 R2, 2016 , 2019Red Hat Enterprise Linux (RHEL) 7 i 8SUSE Linux Enterprise Server (SLES) 12 i 15VMware 6.5 Update 3 i 6.7. |
| 9. | Zarządzanie serwerem | Serwer musi być wyposażony w kartę zdalnego zarządzania (konsoli) pozwalającej na: - włączenie, wyłączenie i restart serwera;- podgląd logów sprzętowych serwera i karty;- przejęcie zdalnej pełnej konsoli tekstowej i graficznej serwera niezależnie od jego stanu (także podczas startu, restartu OS); - zdalne podłączenie wirtualnych napędów CD/DVD/ISO i FDD; - integrację z Active Directory;- powiadamianie o zdarzeniach za pomocą email’a;- nagrywanie zdalnych sesji graficznych i ich późniejsze odtwarzanie;- wysyłanie zdarzeń do zdalnego serwera syslog;- współdzielenie jednej zdalnej konsoli graficznej przez 5 użytkowników;- wspierane i obsługiwane SSH, TLS- wspierane i obsługiwane zarządzanie RESTfull- zarządzanie poborem energii przez serwer – historia poboru energii.Rozwiązanie sprzętowe, niezależne od systemów operacyjnych, zintegrowane z płytą główną.  |
| 10. | Inne | Serwer fabrycznie nowy, wyprodukowany nie wcześniej niż 6 miesięcy przed datą dostarczenia do Zamawiającego i pochodzić z oficjalnego kanału dystrybucyjnego producenta. Zamawiający zastrzega sobie, aby Wykonawca na żądanie Zamawiającego przedłożył oświadczenie Producenta oferowanego sprzętu, w języku polskim, potwierdzające pochodzenie sprzętu z autoryzowanego kanału sprzedaży. |

**Tabela 4. Serwer typ2 – 2 szt.**

**Opis minimalnych wymagań dla serwera do instalacji w infrastrukturze serwerowo-sieciowej**

|  |  |  |
| --- | --- | --- |
| **Lp.** | **Parametr** | **Wymagania minimalne** |
| 1. | Procesory (ilość i typ)  | 2 procesory, każdy maksymalnie ośmiordzeniowy, klasy x86-64bit, dla których serwer osiąga wynik nie mniejszy niż 107 punktów w teście SPECrate2017\_int\_base, dla oferowanego modelu serwera w konfiguracji dwuprocesorowej. Wynik testu musi być potwierdzony przez organizację SPEC i opublikowany na jej oficjalnej stronie internetowej ([www.spec.org](http://www.spec.org)). |
| 2. | Pamięć RAM  | 1.5TB RDIMM DDR4 w modułach min. 64GB. Serwer posiadający minimum 24 sloty na pamięć. |
| 3. | Interfejsy sieciowe | Minimum 2 Interfejsy sieciowe min. 50GbE lub 4 interfejsy 25GbE (CNA, wspierające FCoE – funkcjonalność w standardzie), z możliwością podzielenia każdego interfejsu na min. 3 interfejsy sieciowe (posiadające własne adresy MAC oraz będące widoczne z poziomu systemu operacyjnego, jako fizyczne karty sieciowe) i kartę FC/FCoE o przepustowości min. 16Gb ( posiadającą własny adres WWN). Podział musi być niezależny od zainstalowanego na serwerze systemu operacyjnego/platformy wirtualizacyjnejDedykowana karta FC lub FCoE min. 2 portowe, 32Gb FC do podłączenia do zewnętrznej macierzy dyskowej FC.Dedykowany kontroler SAS 12G lub FC min.32Gb lub przełącznik FC znajdujący się w obudowie do podłączenia dysków z modułów pamięci masowych (opisanych w punkcie Moduły Pamięci Masowej) |
| 4. | Kontroler dyskowy | Sprzętowy kontroler do dysków wewnętrznych z 1GB pamięci cache podtrzymywanej bateryjnie. |
| 5. | Dyski twarde  | Min. 2 wnęki przygotowane do instalacji dysków twardych typu hot plug. Zainstalowane dwa dyski hot-plug SSD, każdy o pojemności min. 240GB Mixed Use (DWPD>=3). |
| 6. | Sloty PCI-E | Trzy sloty PCIe 3.0, |
| 7. | Porty | 1 x USB 3.0 (wewnętrzny) lub 1 x port na kartę SD |
| 8. | Wsparcie dla systemów operacyjnych i systemów wirtualizacyjnych | Microsoft Windows Server 2012 R2, 2016 , 2019Red Hat Enterprise Linux (RHEL) 7 i 8SUSE Linux Enterprise Server (SLES) 12 i 15VMware 6.5 Update 3 i 6.7. |
| 9. | Zarządzanie serwerem | Serwer musi być wyposażony w kartę zdalnego zarządzania (konsoli) pozwalającej na: - włączenie, wyłączenie i restart serwera;- podgląd logów sprzętowych serwera i karty;- przejęcie zdalnej pełnej konsoli tekstowej i graficznej serwera niezależnie od jego stanu (także podczas startu, restartu OS); - zdalne podłączenie wirtualnych napędów CD/DVD/ISO i FDD; - integrację z Active Directory;- powiadamianie o zdarzeniach za pomocą email’a;- nagrywanie zdalnych sesji graficznych i ich późniejsze odtwarzanie;- wysyłanie zdarzeń do zdalnego serwera syslog;- współdzielenie jednej zdalnej konsoli graficznej przez  5 użytkowników;- wspierane i obsługiwane SSH, TLS- wspierane i obsługiwane zarządzanie RESTfull- zarządzanie poborem energii przez serwer – historia poboru energii.Rozwiązanie sprzętowe, niezależne od systemów operacyjnych, zintegrowane z płytą główną.  |
| 10. | Inne | Serwer fabrycznie nowy, wyprodukowany nie wcześniej niż 6 miesięcy przed datą dostarczenia do Zamawiającego i pochodzić z oficjalnego kanału dystrybucyjnego producenta. Zamawiający zastrzega sobie, aby Wykonawca na żądanie Zamawiającego przedłożył oświadczenie Producenta oferowanego sprzętu, w języku polskim, potwierdzające pochodzenie sprzętu z autoryzowanego kanału sprzedaży. |

**Tabela 5. Serwer typ 3 - 1 szt.**

**Opis minimalnych wymagań dla serwera do instalacji w infrastrukturze serwerowo-sieciowej**

|  |  |  |
| --- | --- | --- |
| **Lp.** | **Parametr** | **Wymagania minimalne** |
| 1. | Procesory (ilość i typ)  | 2 procesory, każdy min. szesnastordzeniowy, klasy x86-64bit, dla których serwer osiąga wynik nie mniejszy niż 174 punktów w teście SPECrate2017\_int\_base, dla oferowanego modelu serwera w konfiguracji dwuprocesorowej. Wynik testu musi być potwierdzony przez organizację SPEC i opublikowany na jej oficjalnej stronie internetowej ([www.spec.org](http://www.spec.org)). |
| 2. | Pamięć RAM  | 64GB RDIMM DDR4 w modułach min. 16GB. Serwer posiadający minimum 24 sloty na pamięć. |
| 3. | Interfejsy sieciowe | Minimum 2 Interfejsy sieciowe min. 50GbE lub 4 interfejsy 25GbE (CNA, wspierające FCoE – funkcjonalność w standardzie), z możliwością podzielenia każdego interfejsu na min. 3 interfejsy sieciowe (posiadające własne adresy MAC oraz będące widoczne z poziomu systemu operacyjnego, jako fizyczne karty sieciowe) i kartę FC/FCoE o przepustowości min. 16Gb ( posiadającą własny adres WWN). Podział musi być niezależny od zainstalowanego na serwerze systemu operacyjnego/platformy wirtualizacyjnejDedykowana karta FC lub FCoE min. 2 portowe, 32Gb FC do podłączenia do zewnętrznej macierzy dyskowej FC.Dedykowany kontroler SAS 12G lub FC min. 32Gb lub przełącznik FC znajdujący się w obudowie do podłączenia dysków z modułów Storage (opisanych w punkcie Moduły Storage) |
| 4. | Kontroler dyskowy | Sprzętowy kontroler do dysków wewnętrznych z 1GB pamięci cache podtrzymywanej bateryjnie. |
| 5. | Dyski twarde | Min. 2 wnęki przygotowane do instalacji dysków twardych typu hot plug. Zainstalowane dwa dyski hot-plug SSD, każdy 480GB Mixed Use (DWPD>=3) |
| 6. | Sloty PCI-E | Trzy sloty PCIe 3.0, |
| 7. | Porty | 1 x USB 3.0 (wewnętrzny) lub 1x port na kartę SD |
| 8. | Wsparcie dla systemów operacyjnych i systemów wirtualizacyjnych | Microsoft Windows Server 2012 R2, 2016 , 2019Red Hat Enterprise Linux (RHEL) 7 i 8SUSE Linux Enterprise Server (SLES) 12 i 15VMware 6.5 Update 3 i 6.7. |
| 9. | Zarządzanie serwerem | Serwer musi być wyposażony w kartę zdalnego zarządzania (konsoli) pozwalającej na: - włączenie, wyłączenie i restart serwera;- podgląd logów sprzętowych serwera i karty;- przejęcie zdalnej pełnej konsoli tekstowej i graficznej serwera niezależnie od jego stanu (także podczas startu, restartu OS); - zdalne podłączenie wirtualnych napędów CD/DVD/ISO i FDD; - integrację z Active Directory;- powiadamianie o zdarzeniach za pomocą email’a;- nagrywanie zdalnych sesji graficznych i ich późniejsze odtwarzanie;- wysyłanie zdarzeń do zdalnego serwera syslog;- współdzielenie jednej zdalnej konsoli graficznej przez 5 użytkowników;- wspierane i obsługiwane SSH, TLS- wspierane i obsługiwane zarządzanie RESTfull- zarządzanie poborem energii przez serwer – historia poboru energii.Rozwiązanie sprzętowe, niezależne od systemów operacyjnych, zintegrowane z płytą główną.  |
| 10. | Inne | Serwer fabrycznie nowy, wyprodukowany nie wcześniej niż 6 miesięcy przed datą dostarczenia do Zamawiającego i pochodzić z oficjalnego kanału dystrybucyjnego producenta. Zamawiający zastrzega sobie, aby Wykonawca na żądanie Zamawiającego przedłożył oświadczenie Producenta oferowanego sprzętu, w języku polskim, potwierdzające pochodzenie sprzętu z autoryzowanego kanału sprzedaży. |

**Tabela 6. Urządzenie do backupu dyskowego z deduplikacją – 1 szt.**

**Opis minimalnych wymagań**

|  |  |  |
| --- | --- | --- |
| L.p. | Cecha | Wymagania minimalne |
| 1. | Definicja | Urządzenie musi być kompletnym rozwiązaniem sprzętowym typu „appliance”. Nie dopuszcza się rozwiązania zbudowanego z niezależnych komponentów sprzętowo-programowych. Urządzenie powinno być oficjalnie dostępne w ofercie producentów przed ukazaniem się niniejszego postępowania. |
| 2. | Typ obudowy | Urządzenie musi być przystosowane do montażu w szafie rack 19”. Wymagania dotyczące szafy rack zawiera Tabela 7.  |
| 3. | Przestrzeń dyskowa | Urządzenie musi oferować minimum 90 TiB (108TB) przestrzeni użytkowej dla danych (bez deduplikacji).  |
|  4. | Bezpieczeństwo danych | Dane przechowywane w obrębie podsystemu dyskowego urządzenia muszą być chronione za pomocą technologii RAID-6.Urządzenie musi posiadać zapasowe dyski spare, które będą automatycznie włączane do grup RAID w przypadku awarii jednego z dysków produkcyjnych. Urządzenie musi posiadać co najmniej 1 dysk hot-spare na każde 12 dysków produkcyjnych.Urządzenie musi weryfikować ewentualne przekłamanie danych w wyniku działań systemu plików / mechanizmów RAID zaimplementowanych w urządzeniu. Wymaga się, aby urządzenie sprawdzało sumy kontrolne zapisywanych fragmentów danych po przejściu danych przez system plików / mechanizmy RAID. Urządzenie musi automatycznie rozpoznawać i naprawiać błędy w locie. |
| 5. | Możliwość rozbudowy | Urządzenie musi umożliwiać rozbudowę pojemności użytkowej dla danych (bez deduplikacji) do co najmniej 180TiB (216TB) bez uwzględniania mechanizmów protekcji. Rozbudowa pojemności nie może wymuszać rozbudowy lub wymiany kontrolerów urządzenia – rozbudowa musi odbywać się jedynie poprzez instalację nowych dysków i/lub półek dyskowych. |
| 6. | Interfejsy do hostów | Urządzenie musi posiadać minimum:* 4 porty FC minimum 16Gb/s z możliwością obsługi każdym portem FC protokołów VTL oraz deduplikacji na źródle,
* 4 porty Ethernet minimum 10Gb/s SFP z możliwością obsługi każdym portem Ethernet protokołów CIFS i NFS oraz deduplikacji na źródle.

Do zarządzania musi posiadać minimum 2 porty Ethernet 1 Gb/s z możliwością obsługi każdym portem Ethernet protokołów CIFS i NFS oraz deduplikacji na źródle. |
| 7. | Wydajność | Urządzenie musi osiągać w maksymalnej konfiguracji zagregowaną wydajność backupu protokołami CIFS / NFS / VTL co najmniej 17 TB/h (dane podawane przez producenta) oraz co najmniej 31 TB/h z wykorzystaniem deduplikacji na źródle (dane podawane przez producenta), a także zagregowaną wydajność odtwarzania protokołami CIFS / NFS / VTL co najmniej 17 TB/h (dane podawane przez producenta).Urządzenie nie może zmniejszać swojej wydajności w czasie przybywania kolejnych danych.Urządzenie musi pozwalać na jednoczesną obsługę minimum 500 strumieni (zapis danych, odczyt danych, replikacja danych). |
| 8. | Sposób udostępniania zasobów | Urządzenie musi umożliwiać jednoczesny dostęp do całej pojemności urządzenia wszystkimi poniższymi protokołami:* CIFS, NFS i deduplikacja na źródle (OST/Boost/Catalyst) dla interfejsów Ethernet,
* VTL i deduplikacja na źródle (OST/Boost/Catalyst) dla interfejsów FC.

Urządzenie musi posiadać obsługę mechanizmów deduplikacji dla danych otrzymywanych wszystkimi protokołami (CIFS, NFS, VTL, deduplikacja na źródle) przechowywanych w obrębie urządzenia.Oferowane urządzenie musi mieć możliwość emulacji napędów taśmowych LTO oraz emulacji bibliotek taśmowych. Urządzenie musi umożliwiać przyporządkowanie do pojedynczej biblioteki taśmowej minimum 64 napędów oraz 16 000 slotów na taśmy.Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia. |
| 9. | Partycjonowanie | Urządzenie musi umożliwiać podział na minimum 60 partycji logicznych w taki sposób, aby każdy z podłączonych systemów backupowych mógł pracować na osobnym urządzeniu logicznym. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia. |
| 10. | Deduplikacja danych | Urządzenie musi deduplikować dane inline przed zapisem na nośnik dyskowy. Technologia deduplikacji musi wykorzystywać algorytm bazujący na zmiennym, dynamicznym bloku. Algorytm ten musi samoczynnie i automatycznie dopasowywać się do otrzymywanego strumienia danych. Oznacza to, że urządzenie musi dzielić otrzymany pojedynczy strumień danych na bloki o różnej długości. Proces deduplikacji musi odbywać się inline – w pamięci urządzenia, przed zapisem danych na nośnik dyskowy. Rozwiązanie nie może w żadnej fazie korzystać (w całości lub częściowo) z dodatkowego bufora na składowanie danych w postaci oryginalnej (niezdeduplikowanej).Wszystkie unikalne, zdeduplikowane bloki przed zapisaniem na dysk muszą być kompresowane.Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia. |
| 11. | Replikacja danych | Urządzenie musi umożliwiać replikację danych do drugiego urządzenia. Replikacja musi się odbywać w trybie asynchronicznym. Transmitowane muszą być tylko te fragmenty danych (bloki), które nie znajdują się na docelowym urządzeniu. W przypadku wykorzystania portów Ethernet do replikacji urządzenie musi umożliwiać przyjmowanie backupów, odtwarzanie danych, przyjmowanie strumienia replikacji, wysyłanie strumienia replikacji tymi samymi portami.Musi istnieć możliwość ograniczenia pasma używanego do replikacji między dwoma urządzeniami.Zarządzanie całym procesem kopiowania danych oraz wszystkimi kopiami musi być możliwy z poziomu oprogramowania backupowego. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia. |
| 12. | Szyfrowanie danych | Urządzenie musi mieć zaimplementowaną funkcjonalność wewnętrznego mechanizmu szyfrowania danych AES-256 realizowaną na poziomie urządzenia przy pomocy certyfikowanego algorytmu zgodnego ze standardem FIPS 140-2 Level 1. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, dostarczenie ich nie jest aktualnie wymagane. |
| 13. | Usuwanie przeterminowanych danych | Urządzenie musi automatycznie usuwać przeterminowane dane (bloki danych nienależące do backupów o aktualnej retencji) w procesie czyszczenia. Proces usuwania przeterminowanych danych (czyszczenia) nie może uniemożliwiać pracy procesów backupu i odtwarzania danych.  |
| 14. | Sposób zarządzania | Urządzenie musi mieć możliwość zarządzania poprzez interfejs graficzny dostępny z przeglądarki internetowej. Oprogramowanie do zarządzania musi rezydować na oferowanym na urządzeniu deduplikacyjnym.Urządzenie musi umożliwiać ustawienie powiadomień administratora o problemach w urządzeniu za pomocą poczty elektronicznej. |
| 15. | Kompatybilność | Urządzenie musi wspierać (wymagane formalne wsparcie producenta urządzenia) co najmniej następujące aplikacje backupujące bezpośrednio na oferowane urządzenie: Veeam, Commvault, Veritas NetBackup, Micro Focus Data Protector, IBM Spectrum Protect, Microsoft SQL, Oracle RMAN i SAP HANA.W przypadku przyjmowania backupów od aplikacji: Veeam, Commvault, Veritas NetBackup, Micro Focus Data Protector, Microsoft SQL, Oracle RMAN i SAP HANA urządzenie musi umożliwiać deduplikację na źródle i przesłanie tylko nowych, unikalnych bloków danych poprzez sieć FC i Ethernet. |
| 16. | Redundancja | Redundantne zasilacze i wentylatory. |
| 17. | Dodatkowe wymagania | Wszystkie opisane funkcje urządzenia mają być dostępne w urządzeniu na dzień składania ofert i być udokumentowane w dostępnej dokumentacji technicznej. |

**Tabela 7. Szafa rack - 2 szt.**

|  |  |  |
| --- | --- | --- |
| **Lp.**  | **Opis wymagania / Element** | **Wymaganie / Wymagany parametr** |
| 1. | Wymiary szafy RACK 19” | Szafa RACK 19” zapewniająca 42U wewnętrznego miejsce do instalacji urządzeń. Wysokość max 202cm, szerokość szafy 80cm (min 79cm) , głębokość szafy min. 115cm./max.131cm |
| 2. | Wyposażenie szafy RACK 19” | Szafa wyposażona w:* drzwi przednie perforowane (perforacja min. 80%), wyposażone w zamek
* drzwi tylne, dzielone, wyposażone w zamek
* ściany boczne (prawa i lewa strona) zamykane na zamek.
* zaślepki montowane bez użycia narzędzi z przodu szafy, pozwalające na zamaskowanie miejsca o wysokości 30U; wysokość pojedynczej zaślepki max 1U
* elementy stabilizujące
* elementy do uziemienia
* zestaw pierścieni/uchwytów typu D
* 4 x listwa PDU min. 7.3kVA, każda obsługująca napięcie 220-240V, z podłączeniem IEC-309 32A 1 fazowe, z 36 gniazdami wyjściowymi C13 i 6 gniazd wyjściowych C19
 |
| 3. |  Standardy przemysłowe dla szafy RACK19” | Szafa RACK 19” zgodna ze standardami:* EIA-310
* WEEE
* RoHS compliant
* UL/CES Certification
 |
| 4. | Inne  | Możliwość instalacji sprzętu o wadze 1360kg (obciążenie statyczne). Dopuszczalne obciążenie podczas przemieszczania/przesuwania szafy 1360kg ( obciążenie dynamiczne) bez użycia dodatkowych środków technicznych (wózek, platforma itp.) |

**W ramach wdrożenia dostarczonego sprzętu Wykonawca:**

1. Przygotuje szczegółowy **Projekt techniczny** realizacji wdrożenia dostarczonego sprzętu, uwzględniający dobre praktyki i rekomendacje eksploatacyjne publikowane przez producenta dostarczonej infrastruktury sprzętowej, który powinien zawierać co najmniej schematy połączeń sieci SAN, LAN i elektrycznej, koncepcję instalacji i konfiguracji sprzętu, konfigurację urządzeń, konfigurację zasobów dyskowych, schematy szaf rack z rozmieszczonymi urządzeniami i fizycznymi połączeniami miedzy nimi, procedury testowe potwierdzające zgodność dostarczonego rozwiązania z wymaganiami OPZ oraz procedury odbiorcze dostarczonego i uruchomionego rozwiązania sprzętowego i narzędziowego.
2. Wykona instalację infrastruktury serwerowo-sieciowej oraz serwerów w szafie rack opisanej w Tabeli 7, dokona wszystkich połączeń energetycznych i logicznych FC, Ethernet oraz dokona konfiguracji dostarczonych urządzeń zgodnie z zaleceniami Zamawiającego.
3. Rozprowadzi okablowanie logiczne LAN/SAN oraz kable energetyczne w serwerowniach oraz odpowiednio w miejscach i w sposób wskazany przez Zamawiającego wewnątrz szaf rack, gdzie kable będą spięte w wiązki i przymocowane do elementów konstrukcyjnych szaf.
4. Podłączy szafy rack do wskazanych przez Zamawiającego miejscach w rozdzielnicach elektrycznych.
5. Zainstaluje i skonfiguruje system zarządzania dostarczonej infrastruktury sprzętowej w zakresie wymaganym przez OPZ.
6. Wykona aktualizację oprogramowania układowego (firmware) do najnowszych wersji, zgodnie z bieżącymi zaleceniami producenta sprzętu.
7. Wykona konfigurację automatycznej usługi powiadamiania serwisu producenta sprzętu o zaistniałych awariach/zdarzeniach serwisowych.
8. Wykona konfigurację urządzeń sieciowych LAN/SAN dostarczonej infrastruktury zgodnie z Projektem technicznym.
9. Wykona niezbędną rekonfigurację istniejącej infrastruktury informatycznej Zamawiającego w związku z implementacją nowego sprzętu.
10. Zainstaluje urządzenie do backupu dyskowego z deduplikacją w szafie rack opisanej w Tabeli 7, dokona wszystkich niezbędnych połączeń energetycznych i logicznych FC, Ethernet oraz dokona niezbędnej konfiguracji.
11. Przeprowadzi testy środowiska sprzętowego oraz utworzy raporty z testów.
12. Opracuje **Dokumentację powykonawczą**, która powinna zawierać:
13. Specyfikację techniczną dostarczonego sprzętu,
14. Charakterystykę instalacyjną w tym:
* Lokalizację szaf rack w pomieszczeniu serwerowni
* Schemat rozmieszczenia zainstalowanych urządzeń w szafach rack
* Szacunkowy ciężar szaf rack z zainstalowanymi urządzeniami
* Wymagania energetyczne dla poszczególnych szaf rack
* Schemat podłączeń energetycznych
* Schemat podłączenia sieciowego (FC i Ethernet) do sieci produkcyjnej LAN i SAN zaoferowanego sprzętu w zakresie niezbędnym do uruchomienia zaoferowanego rozwiązania.
1. Dokumentacja powykonawcza dotycząca zainstalowanego sprzętu, zostanie przekazana Zamawiającemu najpóźniej w dniu podpisania Protokołu odbioru Zadania I, w formie papierowej w 2 egzemplarzach oraz w formie elektronicznej na pendrive, w postaci plików do edycji i PDF.
2. **Zadanie II - Dostawa oraz wdrożenie oprogramowania do wirtualizacji.**

Przedmiotem tego zadania jest dostawa oraz wdrożenie oprogramowania do budowy środowiska zwirtualizowanego, dla wskazanej infrastruktury, umożliwiającego wirtualizację serwerów, zasobów dyskowych i sieci.

Wymaganymi elementami zamówienia są:

1. Pakiet VMware Cloud Foundation Advanced lub oprogramowanie równoważne zawierające funkcjonalność tego pakietu (licencjonowanie na procesor) – dla 6 sztuk dwu procesorowych serwerów fizycznych,
2. Oprogramowanie VMware vCenter Server lub oprogramowanie równoważne zawierające funkcjonalność tego oprogramowania (licencjonowanie na instancję) – 1 sztuka,
3. 5 letni okres gwarancji zapewniającej możliwość wprowadzania wszelkich poprawek i nowych wersji, które powstaną w tym okresie na całe dostarczone oprogramowanie,

Ze względu na spójność środowiska i zapewnienie niezawodności platformy wirtualizacyjnej oraz uniknięcie zagrożeń mogących powstać na styku produktów różnych producentów całe oprogramowanie wirtualizacyjne musi być kompatybilne i ściśle ze sobą współpracować. Dostarczone oprogramowanie musi być w wersji najnowszej na dzień złożenia oferty, z uwzględnieniem specyfiki sprzętu Zamawiającego.

Licencjonowanie musi uwzględniać prawo do bezpłatnej instalacji udostępnianych przez producenta oprogramowania uaktualnień i poprawek krytycznych i opcjonalnych do zakupionej wersji oprogramowania. W ramach umowy Wykonawca ma zapewnić udzielanie uprawnień na witrynie producenta oprogramowania wskazanym przez Zamawiającego osobom (pracownikom Zamawiającego) do pobierania kodu zamówionego oprogramowania i kluczy licencyjnych.

**W ramach wdrożenia dostarczonego oprogramowania do wirtualizacji Wykonawca powinien:**

Wykonać instalację i konfigurację oprogramowania do budowy środowiska zwirtualizowanego (hiperkonwergentnego), dla wskazanej infrastruktury, umożliwiającego wirtualizację serwerów, zasobów dyskowych i sieci. Wdrożona infrastruktura zwirtualizowana musi być skonfigurowana i w pełni funkcjonalna we wszystkich trzech aspektach: serwerowym, dyskowym i sieciowym.

Podczas wdrożenia wirtualizowana infrastruktura sprzętowa będzie się znajdować w jednej szafie rack ale musi być przewidziana możliwość przenoszenia niektórych zasobów do innych szaf rack w ramach tego samego Centrum Przetwarzania Danych. Infrastruktura będzie składać się z 6 serwerów fizycznych dwu procesorowych dostarczonych w Zadaniu I i opisanych w Tabeli 3 i 4. Podsystem dyskowy podlegający wirtualizacji będzie składać się z dysków SSD o łącznej pojemności ponad 200 TB.

W ramach prac wdrożeniowych Wykonawca:

1. Przygotuje szczegółowy **Projekt techniczny** realizacji, uwzględniający dobre praktyki i rekomendacje eksploatacyjne publikowane przez producenta dostarczanego oprogramowania oraz zawierający opis konfiguracji środowiska.
2. Wykona instalację i konfigurację wszystkich elementów oprogramowania wymaganych przez Zamawiającego.
3. Skonfiguruje wdrożoną infrastrukturę zwirtualizowaną i uruchomi aby była w pełni funkcjonalna we wszystkich czterech aspektach: serwerowym, dyskowym, sieciowym i zarządzania, zgodnie z Projektem technicznym w tym:
	1. Podłączenie wskazanych przez Zamawiającego vLAN do hostów
	2. Utworzenie i podłączenie zasobów dyskowych do hostów
	3. Utworzenie i podłączenie datastore z macierzy dyskowej
	4. Podłączenie wskazanych przez Zamawiającego zasobów dyskowych (LUN) z obecnie istniejącej infrastruktury
4. Wykona testy akceptacyjne (niezawodnościowe oraz funkcjonalne) oraz opracuje i przedstawi Raport z testów.
5. Opracuje **Dokumentację powykonawczą** zawierającą opis wdrożonej konfiguracji (konfigurację poszczególnych serwerów, modułów, komponentów i usług) oraz procedury administracyjne i eksploatacyjne (w tym procedury awaryjnego odtwarzania funkcjonalności systemu, procedury bieżącego monitoringu oraz utrzymania i aktualizacji systemu) w zakresie uzgodnionym z Zamawiającym.
6. Dokumentacja powykonawcza wdrożonego oprogramowania do wirtualizacji, zostanie przekazana Zamawiającemu najpóźniej w dniu podpisania Protokołu odbioru Zadania II, w formie papierowej w 2 egzemplarzach oraz w formie elektronicznej na pendrive, w postaci plików do edycji i PDF.

**Warunki równoważności dla elementów pakietu VMware Cloud Foundation oraz VMware vCenter Server są następujące:**

1. **W zakresie wirtualizacji serwerów i zarządzania środowiskiem serwerów wirtualnych**
2. Warstwa wirtualizacji nie może dla własnych celów alokować więcej niż 200MB pamięci operacyjnej RAM serwera fizycznego.
3. Oprogramowanie do wirtualizacji zainstalowane na serwerze fizycznym musi potrafić obsłużyć i wykorzystać procesory fizyczne wyposażone w 576 logicznych wątków oraz do 12TB pamięci fizycznej RAM.
4. Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych 1-128 procesorowych.
5. Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych z możliwością przydzielenia do 6 TB pamięci operacyjnej RAM.
6. Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych, z których każda może mieć 1-10 wirtualnych kart sieciowych.
7. Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych, z których każda może mieć 32 porty szeregowe i 3 porty równoległe.
8. Rozwiązanie musi wspierać następujące systemy operacyjne: Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows Server 2016, Windows Server 2019, Windows 7, Windows 8, Windows 10, SLES 12, SLES 11, REHL 7, RHEL 6, Debian, CentOS, FreeBSD, Ubuntu, Mac OS X, Oracle Linux.
9. Rozwiązanie musi umożliwiać przydzielenie większej ilości pamięci RAM dla maszyn wirtualnych niż fizyczne zasoby RAM serwera w celu osiągnięcia maksymalnego współczynnika konsolidacji.
10. Rozwiązanie musi umożliwiać udostępnienie maszynie wirtualnej większej ilości zasobów dyskowych niż jest fizycznie zarezerwowane na zasobach dyskowych.
11. Rozwiązanie musi umożliwiać integrację z rozwiązaniami antywirusowymi firm trzecich w zakresie skanowania maszyn wirtualnych z poziomu warstwy wirtualizacji.
12. 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.
13. Oprogramowanie do wirtualizacji musi zapewnić możliwość klonowania systemów operacyjnych wraz z ich pełną konfiguracją i danymi.
14. Oprogramowanie do wirtualizacji musi zapewnić możliwość wykonywania kopii migawkowych instancji systemów operacyjnych na potrzeby tworzenia kopii zapasowych bez przerywania ich pracy z możliwością wskazania konieczności zachowania stanu pamięci pracującej maszyny wirtualnej.
15. Oprogramowanie zarządzające musi posiadać możliwość przydzielania i konfiguracji uprawnień z możliwością integracji z usługami katalogowymi, w szczególności: Microsoft Active Directory, Open LDAP.
16. Rozwiązanie musi zapewniać możliwość dodawania zasobów w czasie pracy maszyny wirtualnej, w szczególności w zakresie ilości procesorów, pamięci operacyjnej i przestrzeni dyskowej.
17. Oprogramowanie do wirtualizacji musi mieć możliwość uruchamiania fizycznych serwerów z centralnie przygotowanego obrazu poprzez protokół PXE.
18. Oprogramowanie do wirtualizacji musi umożliwiać udostępnianie pojedynczego urządzenia fizycznego (PCIe) jako logicznie separowane wirtualne urządzenia dedykowane dla poszczególnych maszyn wirtualnych.
19. Oprogramowanie do wirtualizacji musi posiadać funkcjonalność wirtualnego przełącznika (virtual switch) umożliwiającego tworzenie sieci wirtualnej w obszarze hosta i pozwalającego połączyć maszyny wirtualne w obszarze jednego hosta, a także na zewnątrz sieci fizycznej. Pojedynczy przełącznik wirtualny powinien mieć możliwość konfiguracji do 4000 portów.
20. Pojedynczy wirtualny przełącznik musi posiadać możliwość przyłączania do niego dwóch i więcej fizycznych kart sieciowych, aby zapewnić bezpieczeństwo połączenia ethernet’owego w razie awarii karty sieciowej.
21. Wirtualne przełączniki muszą obsługiwać wirtualne sieci lokalne (VLAN).
22. Rozwiązanie musi zapewniać możliwość konfigurowania polityk separacji sieci w warstwie trzeciej, tak aby zapewnić oddzielne grupy wzajemnej komunikacji pomiędzy maszynami wirtualnymi.
23. Rozwiązanie musi umożliwiać wykorzystanie technologii 10GbE, w tym agregację połączeń fizycznych do minimalizacji czasu przenoszenia maszyny wirtualnej pomiędzy serwerami fizycznymi.
24. Oprogramowanie do wirtualizacji musi obsługiwać przełączenie ścieżek LAN (bez utraty komunikacji) w przypadku awarii jednej ze ścieżek.
25. Rozwiązanie musi zapewnić możliwość zdefiniowania alertów informujących o przekroczeniu wartości progowych.
26. Rozwiązanie musi zapewniać możliwość replikacji maszyn wirtualnych z dowolnej pamięci masowej w tym z dysków wewnętrznych serwerów fizycznych na dowolną pamięć masową w tym samym lub oddalonym ośrodku przetwarzania.
27. Rozwiązanie replikujące musi gwarantować współczynnik RPO na poziomie nie większym niż 5 minut.
28. Czas planowanego przestoju usług związany z koniecznością prac serwisowych (np. rekonfiguracja serwerów, macierzy, switch’y) musi być ograniczony do minimum. Konieczna jest możliwość przenoszenia maszyn wirtualnych pomiędzy serwerami fizycznymi bez przerywania pracy usług.
29. Rozwiązanie musi posiadać natywne mechanizmy szyfrowania podczas przenoszenia maszyn wirtualnych w czasie ich pracy pomiędzy serwerami fizycznymi.
30. 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.
31. Rozwiązanie musi umożliwiać łatwe i szybkie ponowne uruchomienie systemów/usług w przypadku awarii poszczególnych elementów infrastruktury bez utraty danych.
32. Rozwiązanie musi zapewnić bezpieczeństwo danych mimo poważnego uszkodzenia lub utraty sprzętu lub oprogramowania.
33. Rozwiązanie musi zapewniać mechanizm bezpiecznego, bezprzerwowego i automatycznego uaktualniania warstwy wirtualizacyjnej, wliczając w to zarówno poprawki bezpieczeństwa, jak i zmianę jej wersji bez potrzeby wyłączania wirtualnych maszyn.
34. 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.
35. 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.
36. Rozwiązanie musi zapewniać pracę bez przestojów dla wybranych maszyn wirtualnych (o maksymalnie czterech procesorach wirtualnych), niezależnie od systemu operacyjnego oraz aplikacji, podczas awarii serwerów fizycznych, bez utraty danych i dostępności danych podczas awarii serwerów fizycznych.
37. Oprogramowanie do wirtualizacji musi obsługiwać przełączenie ścieżek SAN (bez utraty komunikacji) w przypadku awarii jednej ze ścieżek.
38. Oprogramowanie do wirtualizacji musi zapewniać możliwość stworzenia dysku maszyny wirtualnej o wielkości do 60 TB.
39. Rozwiązanie musi posiadać wbudowany interfejs programistyczny (API) zapewniający pełną integrację zewnętrznych rozwiązań wykonywania kopii zapasowych z istniejącymi mechanizmami warstwy wirtualizacyjnej.
40. Rozwiązanie musi umożliwiać konfigurację wysokiej dostępności (HA) dla każdego swojego komponentu w celu unikania awarii pojedynczego elementu.
41. Oprogramowanie do wirtualizacji musi być wspierane przez producenta oferowanego rozwiązania do automatyzacji procesów (Automatyzacja) oraz wirtualizacji sieci (SDN) na wszystkich poziomach wsparcia (L1-L3). Wsparcie musi odbywać się poprzez jednorodny kanał serwisowy (jeden numer telefonów dla wszystkich zgłoszeń, jeden portal www, pozwalający zarządzać licencjami i zgłaszać zlecenia serwisowe).
42. Oprogramowanie do wirtualizacji musi wspierać mechanizmy zaawansowanego uwierzytelniania do systemu operacyjnego wirtualnej maszyny za pomocą technologii Smart Card Reader.
43. Wirtualizator musi wspierać TPM 2.0. Oznacza to min. że TPM zapewnia mechanizm gwarantujący, że serwer fizyczny uruchomił się z włączoną opcją Secure Boot. Po potwierdzeniu, że Secure Boot jest włączone, rozwiązanie gwarantuje, że wirtualizator uruchomił się w prawidłowej, niezmienionej formie poprzez weryfikację podpisu cyfrowego.
44. Wirtualizator musi mieć możliwość włączenia funkcji “Microsoft virtualization-based security”, tzw. Microsoft VBS dla systemów operacyjnych maszyn wirtualnych opartych o system operacyjny min. Windows 10 oraz min. Windows Server 2016.
45. Rozwiązanie musi posiadać certyfikację FIPS-140-2 min. dla modułu jądra wirtualizatora odpowiedzialnego za szyfrowanie danych.
46. Wirtualizator musi posiadać funkcjonalność wirtualnego TPM 2.0 dla maszyn wirtualnych Windows 10 oraz Windows 2016. Oznacza to, że z punktu widzenia maszyny wirtualnej z systemem operacyjnym Windows 10 lub Windows 2016 wirtualny TPM widziany jest jako standardowy TPM, gdzie można przechowywać bezpiecznie wrażliwe dane np. certyfikaty. Zawartość wirtualnego TPM przechowywana jest w pliku przynależnym do maszyny wirtualnej oraz musi być szyfrowana. Wirtualizator musi posiadać rolę administratora odpowiedzialnego za zarządzanie kluczami szyfrującymi. Rola ta powinna być odseparowana od roli administratora wirtualizatora. Oznacza, to, że tylko administrator odpowiedziany za szyfrowanie ma dostęp do kluczy szyfrujących oraz może zarządzać procesem szyfrowania w obrębie wirtualizatora.
47. Rozwiązanie musi posiadać funkcjonalność szybkiego uruchamiania wirtualizatora po przeprowadzonym procesie jego aktualizacji. Taka funkcjonalność powoduje, że w procesie aktualizacji wirtualizatora, jeśli wymagany jest jego restart, eliminowana jest czasochłonna faza inicjalizacji serwera fizycznego – następuje skrócenia czasu wymaganego do ponownego uruchomienia serwera fizycznego podczas operacji aktualizacji.
48. Dostarczone oprogramowanie musi zapewniać możliwość wirtualizacji dla wszystkich serwerów dostarczonych w ramach postępowania.
49. Rozwiązanie musi posiadać wsparcie dla natywnych dysków 4K.
50. Rozwiązanie wirtualizatora musi posiadać mechanizmy proaktywnej wysokiej dostępności. Oznacza, to, że jeśli serwer fizyczny posiada funkcję przekazania do wirtualizatora informacji o stanie serwera, to wirtualizator na podstawie tych danych jest w stanie proaktywnie przenieść wszystkie maszyny wirtualne na inne, prawidłowo działające serwery fizyczne w klastrze, zanim dojdzie do całkowitej awarii serwera fizycznego.
51. Rozwiązanie musi umożliwiać automatyczne równoważenie obciążenia CPU/MEM serwerów fizycznych pracujących jako platforma dla infrastruktury wirtualnej.
52. Oprogramowanie do wirtualizacji musi zapewniać mechanizm pozwalający tworzyć profil (szablon konfiguracji) wybranego serwera, a następnie wymuszać ten profil/konfigurację na innych serwerach lub sprawdzać zgodność konfiguracji pomiędzy zdefiniowanym wcześniej profilem a wskazanym serwerem fizycznym.
53. Rozwiązanie musi umożliwiać utworzenie jednorodnego, wirtualnego przełącznika sieciowego, rozproszonego na wszystkie serwery fizyczne platformy wirtualizacyjnej. Przełącznik taki musi zapewniać możliwość konfiguracji parametrów sieciowych maszyny wirtualnej z granulacją na poziomie portu tego przełącznika. Pojedyncza maszyna wirtualna musi mieć możliwość wykorzystania jednego lub wielu portów przełącznika z niezależną od siebie konfiguracją.
54. Przełącznik rozproszony musi współpracować z protokołem NetFlow.
55. Platforma wirtualizacji powinna w ramach przełącznika sieciowego zapewniać możliwość integracji z produktami (przełącznikami wirtualnymi) firm trzecich, tak aby umożliwić granularną delegację zadań w zakresie zarządzania konfiguracją sieci do zespołów sieciowych.
56. Przełącznik rozproszony musi umożliwiać funkcjonalność duplikowania ruchu sieciowego dowolnego jego portu wirtualnego na inny port.
57. Przełącznik musi mieć wbudowane mechanizmy składowania kopii konfiguracji, przywracania tej kopii, a także mechanizmy automatycznie zapobiegające niewłaściwej konfiguracji sieciowej, które w całości lub w części mogą eliminować błędy ludzkie i utratę łączności sieciowej.
58. Rozwiązanie musi mieć wbudowany mechanizm kontrolowania i monitorowania ruchu sieciowego oraz ustalania priorytetów w zależności od jego rodzaju, na poziomie konkretnych maszyn wirtualnych.
59. Rozwiązanie musi zapewnić możliwość bieżącego monitorowania wykorzystania zasobów fizycznych infrastruktury wirtualnej (np. procesorów, pamięci RAM, przestrzeni na dyskach/wolumenach) oraz przechowywać i wyświetlać dane sprzed roku.
60. 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 oraz pomiędzy różnymi Centrami Przetwarzania Danych.
61. Rozwiązanie musi mieć możliwość przenoszenia maszyn wirtualnych w czasie ich pracy pomiędzy różnymi Centralnymi Konsolami Zarządzającymi platformy wirtualnej na daleką odległość min. 150 km.
62. Rozwiązanie powinno posiadać proaktywnie działający mechanizm, który przemigruje wirtualne maszyny po wykryciu potencjalnego problemu z serwerem fizycznym, zanim on ulegnie awarii.
63. Rozwiązanie musi mieć wbudowany mechanizm kontrolowania i monitorowania ruchu do pamięci masowych oraz ustalania priorytetów dostępu do nich na poziomie konkretnych wirtualnych maszyn.
64. Rozwiązanie musi mieć możliwość grupowania pamięci masowych o podobnych parametrach w grupy i przydzielania ich do wirtualnych maszyn zgodnie z ustaloną przez administratora polityką.
65. Rozwiązanie musi mieć możliwość równoważenia obciążenia i zajętości pamięci masowych wraz z pełną automatyką i przenoszeniem plików wirtualnych maszyn z bardziej zajętych na mniej zajęte przestrzenie dyskowe lub/i z przestrzeni dyskowych bardziej obciążonych operacjami I/O na mniej obciążone.
66. Rozwiązanie jako funkcja wirtualizatora (jądra) musi umożliwiać szyfrowanie wirtualnych maszyn oraz szyfrowanie maszyny wirtualnej podczas przenoszenia bez przerywania jej pracy na innych host lub zasób dyskowy.
67. Rozwiązanie 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).
68. Rozwiązanie musi umożliwiać uruchamianie kontenerów zbudowanych w topologii Docker Image w wirtualnych maszynach.
69. Rozwiązanie musi umożliwiać instalowanie, uruchamianie i zarządzanie aplikacjami Big Data oraz Hadoop z poziomu platformy wirtualizującej.
70. Rozwiązanie musi wspierać technologię rozproszonego udostępniania procesora graficznego Nvidia Grid vGPU do maszyn wirtualnych.
71. Wirtualizator musi wspierać tzw. rozwiązanie trwałej, nieulotnej pamięć (Persistent Memory) zbliżonej do szybkości pamięci DRAM. W ten sposób wirtualizator może udostępnić dla maszyn wirtualnych dyski, które wspierają taką funkcjonalność - ultraszybką pamięć masową zbliżoną do pamięci DRAM.
72. Wirtualizator musi wspierać protokół Remote Direct memory Access (RDMA) poprzez konwergentny Ethernet, lub RoCE (“rocky”) v2, Fiber Channel over Ethernet (FCoE) adapter, i iSCSI rozszerzenie dla RDMA (iSER).
73. Rozwiązanie musi posiadać centralną konsolę graficzną do zarządzania maszynami wirtualnymi i do konfigurowania innych funkcjonalności oraz monitoringu (możliwość monitorowania obciążenia min. vCPU, vRAM, vHDD, sieci, bazy danych). Centralna konsola graficzna powinna działać jako gotowa, wstępnie skonfigurowana maszyna wirtualna (tzw. virtual appliance).
74. Konsola graficzna musi być dostępna poprzez dedykowanego klienta (za pomocą przeglądarek, minimum IE i Firefox) lub poprzez konsolę graficzną, która zbudowana jest z wykorzystaniem standardu HTML5.
75. Dostęp przez przeglądarkę do konsoli graficznej musi być skalowalny tj. powinien umożliwiać rozdzielenie komponentów na wiele instancji w przypadku zapotrzebowania na dużą liczbę jednoczesnych dostępów administracyjnych do środowiska.
76. Rozwiązanie musi zapewniać natywne mechanizmy HA w niezawodnej architekturze Active-Passive-Witness dla wszystkich składowych komponentów centralnej konsoli graficznej zarządzającej platformą wirtualną.
77. Rozwiązanie musi posiadać natywne mechanizmy do wykonywania kopii zapasowej swojej konfiguracji. Dodatkowo musi być możliwość ustawienia harmonogramu wykonywania kopii zapasowej.
78. **W zakresie wirtualizacji zasobów dyskowych**
	1. Oferowane rozwiązanie musi umożliwiać zbudowanie wspólnej przestrzeni dyskowej w oparciu o dyski wewnętrzne serwerów fizycznych. Wymagane wsparcie dla konfiguracji sprzętowej serwera opartej o dyski SSD i HDD oraz dla konfiguracji serwera opartej wyłącznie o dyski SSD.
	2. Rozwiązanie musi zapewniać możliwość optymalizacji wydajności poprzez wbudowaną funkcjonalność „cache’owania” operacji odczytu/zapisu (Read/Write IO) po stronie serwerów fizycznych.
	3. Rozwiązanie musi posiadać możliwość budowania własnych schematów konfiguracji dyskowej dla przestrzeni akcelerującej operacje Read/Write (cache) oraz dla przestrzeni budującej pojemność. Wymagana jest możliwość zmiany konfiguracji zarówno pod kątem dostępności, wydajności jak i pojemności "w locie".
	4. Rozwiązanie musi być zintegrowane z warstwą wirtualizacji w sposób bezpośredni, niewymagający instalacji/konfiguracji dodatkowych komponentów sprzętowych oraz dodatkowego oprogramowania/dodatkowych maszyn wirtualnych.
	5. Konfiguracja, zarządzanie i monitoring ww. przestrzeni dyskowej muszą być zintegrowane z konsolą zarządzającą platformą wirtualizacyjną.
	6. Narzut definiowany jako moc procesora i zużycie pamięci RAM fizycznego serwera podczas działania rozwiązania tj. podczas udostępniania zasobów dyskowych dla min. 50 maszyn wirtualnych, gdzie każda korzysta z min. 400GB przestrzeni dyskowej i generująca min. 800 IO/sek, nie może być większy niż 10% zasobów fizycznego serwera dostarczonego w ramach postępowania. W przypadku braku oficjalnych testów na stronie producenta rozwiązania Zamawiający zastrzega sobie prawo do przeprowadzenia testów wydajności na etapie analizy ofert oraz odbiorów rozwiązania.
	7. Rozwiązanie musi zapewniać możliwość budowy wspólnej wysoko-wydajnej i wysoko-dostępnej przestrzeni dyskowej z wykorzystaniem dysków wewnętrznych udostępnianych przez minimalnie 2 serwery fizyczne, oraz umożliwiać rozbudowę w ramach jednej logicznej puli do minimum 64 serwerów fizycznych.
	8. Rozwiązanie musi zapewniać obsługiwanie dysków wirtualnych maszyn do rozmiaru min. 60TB.
	9. Rozwiązanie musi zapewniać wysoką dostępność oraz odporność na awarie usług uruchomionych na serwerach z zainstalowanym oprogramowaniem do udostępniana przestrzeni dyskowej. Wysoka dostępność musi być realizowana w oparciu o wbudowane mechanizmy oprogramowania i nie dopuszcza się stosowania produktów firm trzecich lub dedykowanych komponentów sprzętowych aby zapewnić ciągłość działania w przypadku awarii komponentów takich jak: serwer fizyczny i jego komponenty takie jak: dysk cache’ujący, dysk pojemnościowy.
	10. Rozwiązanie nie może w żaden sposób ograniczać funkcjonalności platformy wirtualizacyjnej zarówno w warstwie mechanizmów niezawodnościowych, wydajnościowo-optymalizacyjnych jak i zarządzania.
	11. Rozwiązanie musi posiadać konfigurowalne mechanizmy zabezpieczania danych na wypadek niedostępności danych lub awarii sprzętowej w taki sposób, aby zabezpieczane dane można było rozlokować na min. poniższych poziomach: między różnymi lokalizacjami, między różnymi centami przetwarzania danych, między różnymi szafami rack/chassis.
	12. Rozwiązanie musi zapewniać wsparcie dla rozwiązań sprzętowych różnych producentów i posiadać oficjalną stronę producenta na której znajduje się lista wspieranych lub rekomendowanych konfiguracji. Rozwiązanie nie może wprowadzać ograniczenia, aby na etapie rozbudowy przestrzeni dyskowej wymagana była rozbudowa jedynie o serwery producenta wykorzystane na etapie przed rozbudową. W przypadku rozbudowy o kolejne serwery rozwiązanie nie może wprowadzać wymogu, aby w dostarczanych serwerach wymagana była instalacja komponentów sprzętowych oferowanych tylko przez jednego dostawcę/producenta (np. dyski, adaptery, specjalizowane karty i kontrolery).
	13. Rozwiązanie musi zapewniać możliwość rozbudowy i skalowania zarówno mocy obliczeniowej, pojemności przestrzeni cache, jak i pojemności przestrzeni dyskowej.
	14. Rozwiązanie musi zapewniać możliwość rozbudowy oferowanej przestrzeni dyskowej (dodanie pojedynczego dysku, dodanie serwera/serwerów fizycznych) w sposób niewymagający przestoju i przerwy w dostępie do działających usług wirtualnych.
	15. Rozwiązanie musi zapewniać możliwość ochrony danych przed utratą ich integralności (np.: sfałszowaniem) za pomocą weryfikacji sum kontrolnych.
	16. Rozwiązanie musi umożliwiać utworzenie wysokodostępnego klastra przestrzeni dyskowej w scenariuszu dla tzw. oddziału zdalnego, zbudowanego w oparciu o min. 2 serwery fizyczne i min. dwie lokalizacje. Architektura systemu musi mieć możliwość dołączania kolejnych lokalizacji oddziałów zdalnych w ilości min. 6.
	17. Rozwiązanie nie może wymagać instalacji dodatkowych komponentów i maszyn wirtualnych na serwerach wykorzystywanych do udostępniania przestrzeni dyskowych.
	18. W ramach rozwiązania musi zostać dostarczony wirtualizator (Hypervisor) posiadający wbudowane mechanizmy typu Multi-Processor Fault Tolerance.
	19. W ramach rozwiązania musi zostać dostarczony wirtualizator (Hypervisor) pracujący niezależnie od systemów operacyjnych jakie wspiera.
	20. Rozwiązanie musi posiadać na oficjalnej stronie producenta listę wspieranych i certyfikowanych konfiguracji serwerowych. Wymagane jest wsparcie dla min. 4 niezależnych producentów sprzętu serwerowego dostępnego na rynku Unii Europejskiej.
	21. Oprogramowanie do wirtualizacji podsystemu dyskowego (SDS) musi być wspierane przez producenta oferowanego rozwiązania do automatyzacji procesów (Automatyzacja), wirtualizacji serwerów (Hypervisor) oraz wirtualizacji sieci IP (SDN) na wszystkich poziomach wsparcia (L1-L3). Wsparcie musi odbywać się poprzez jednorodny kanał serwisowy (jeden numer telefonów dla wszystkich zgłoszeń, jeden portal www pozwalający zarządzać licencjami i zgłaszać zlecenia serwisowe).
	22. Oprogramowanie musi zapewniać natywną integrację (bez skryptów i/lub pluginów) z obecnie używanym przez Zamawiającego systemem zarządzania wirtualnym środowiskiem VMware – Vcenter.
	23. Rozwiązanie musi zapewniać możliwość zmniejszania przestrzeni dyskowej (odjęcie pojedynczego dysku, odjęcie serwera/serwerów fizycznych) w sposób niewymagający przestoju i przerwy w dostępie do działających usług wirtualnych.
	24. Rozwiązanie musi posiadać możliwość udostępniania swojej przestrzeni dyskowej również dla fizycznych systemów operacyjnych w oparciu o technologię iSCSI i umożliwiać zarządzanie dostępnością, pojemnością i wydajnością w locie.
	25. Rozwiązanie musi posiadać interfejs API umożliwiający automatyzowanie wdrażania/modyfikacji konfiguracji systemu.
	26. Rozwiązanie musi współdzielić zasób dyskowy dla platformy wirtualizacyjnej oraz musi umożliwiać wykorzystanie ww. przestrzeni dyskowej przez serwery fizyczne nie posiadające dysków wewnętrznych.
	27. Rozwiązanie musi zapewniać możliwość tworzenia i konfigurowania polityk niezawodnościowych, wydajnościowych i pojemnościowych przypisanych do maszyn wirtualnych tak, aby można było określić min.: liczbę serwerów fizycznych, które mogą ulec awarii jednocześnie, liczbę operacji I/O, użycie funkcji thin-provisioning.
	28. Rozwiązanie musi mieć możliwość skonfigurowania dedupikacji i kompresji przy zapisie danych na dysk/grupę pojemnościową (składowanie danych).
	29. Rozwiązanie powinno wspierać mechanizmy optymalizacji wykorzystania przestrzeni dyskowych. Wymagane wsparcie dla technologii deduplikacji oraz technologii implementującej RAID5 i RAID6 za pomocą oprogramowania.
	30. Rozwiązanie musi umożliwiać utworzenie jednej przestrzeni dyskowej jako „rozciągniętego klastra geograficznego” realizującego scenariusze Disaster Recovery/Disaster Avoidance, zbudowanego w oparciu o dyski wewnętrzne serwerów fizycznych umieszczonych w dwóch różnych lokalizacjach fizycznych, gwarantując tym samym dostępność danych na wypadek awarii całego pojedynczego Data Center oraz dowolnego elementu w dowolnej lokalizacji.
	31. Rozwiązanie musi umożliwiać szyfrowanie wirtualnych maszyn zlokalizowanych w zbudowanym w oparciu o rozwiązanie zasobie dyskowym oraz musi umożliwiać szyfrowanie maszyny wirtualnej bez przerywania jej pracy podczas przenoszenia na inny host lub zasób dyskowy.
79. **W zakresie wirtualizacji sieci**
80. Dostarczone oprogramowanie musi oferować możliwość budowy sieci komunikacyjnych (IP) w oparciu o środowiska wirtualne
81. Oprogramowanie musi zapewniać funkcjonalność tworzenia wirtualnych sieci w sposób niezależny od topologii sieci fizycznej i używanych w obrębie tej sieci protokołów sieciowych
82. Rozwiązanie realizujące usługi wirtualnych sieci musi być zarządzane przez narzędzie zarządzające warstwą wirtualną serwerów. Wyklucza się używanie skryptów lub plugin’ów nie wspieranych przez dostawcę platformy wirtualizatora serwerów
83. 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
84. 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
85. Rozwiązanie musi posiadać możliwość kreowania segmentów sieci przy użyciu technologii VXLAN
86. Oprogramowanie musi zapewnić funkcjonalność łączenia (bridging) środowiska zwirtualizowanego opartego o technologię VXLAN oraz niezwirtualizowanego zdefiniowanego za pomocą technologii VLAN-ów
87. Oprogramowanie musi zapewnić funkcjonalność wirtualnego routera wspierającego protokoły OSPF i BGP. Routing statyczny oraz BGP musi być możliwy poprzez tunel GRE
88. Rozwiązanie musi posiadać funkcję łączenia (bridge) segmentów sieci L2 VLAN i VXLAN poprzez zastosowanie wirtualnej bramy (bridge)
89. Rozwiązanie musi umożliwiać funkcję translacji adresów IP zarówno dla ruchu wychodzącego ze środowiska wirtualnego (SNAT) jak i przychodzącego (DNAT)
90. Rozwiązanie musi posiadać funkcję serwera DHCP w celu dynamicznego nadawania adresów IP dla środowiska zwirtualizowanego
91. Rozwiązanie musi posiadać pełną wymaganą funkcjonalność zarówno funkcji bezpieczeństwa jak i funkcji sieciowych w ramach jednego produktu i być gotowe do instalacji i konfiguracji z wykorzystaniem GUI
92. Oprogramowanie musi udostępniać funkcjonalność zarządzania poprzez ustandaryzowany interfejs tj. API
93. Zmiana konfiguracji sieciowej musi odbywać się poprzez narzędzia zarządzające dostępne dla środowiska wirtualizacyjnego serwerów
94. Aktualizacje oprogramowania powinny odbywać się poprzez zintegrowany portal służący do ich planowania i uruchamiania. Portal musi umożliwiać przegląd wszystkich elementów systemu pod kątem ich aktualnej oraz przygotowanej do aktualizacji wersji. Portal musi oferować wskaźniki postępu aktualizacji, umożliwiać tworzenie planów aktualizacji oraz zapewniać mechanizmy sprawdzenia spójności działania systemu przed oraz po aktualizacji
95. Oprogramowanie powinno zapewniać wsparcie dla wykorzystania plików danych JSON oraz XML
96. Oprogramowanie musi zapewnić bezpieczeństwo transmisji danych (filtracja pakietów) na poziomie hypervisora/wirtualnego 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
97. 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". Wymagana jest możliwość definiowania reguł dla warstwy 7 modelu OSI dla wybranych aplikacji w celu zapewnienia kontroli przepływu danych oraz planowania mikro-segmentacji.
98. Musi zostać zapewniona możliwość tworzenia reguł firewalla w trybie stateless dla różnych grup wirtualnych maszyn.
99. Oprogramowanie musi zapewniać możliwość tworzenia granularnych polityk bezpieczeństwa na poziomie wirtualnego portu maszyny wirtualnej, włączając ruch pomiędzy wirtualnymi maszynami w ramach tego samego segmentu sieci i na tym samym fizycznym serwerze
100. Rozwiązanie musi umożliwiać wykorzystanie dynamicznych obiektów do tworzenia reguł polityk bezpieczeństwa. Wymagane min.: nazwa maszyny wirtualnej, nazwa przełącznika wirtualnego, nazwa grupy maszyn wirtualnych, system operacyjny wirtualnej maszyny
101. Oprogramowanie realizujące usługę rozproszonego firewalla musi być zarządzane przez narzędzie zarządzające warstwą wirtualną serwerów. Wyklucza się używanie skryptów lub pluginów nie wspieranych przez dostawcę platformy wirtualizatora serwerów
102. 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
103. Rozwiązanie musi oferować w ramach platformy, funkcjonalność bezpiecznego, zdalnego i szyfrowanego dostępu użytkowników dla minimum następujących systemów operacyjnych : Windows 7 i wyższe, Mac OS oraz Linux, przy użyciu technologii SSL VPN
104. Rozwiązanie musi oferować w ramach platformy, możliwość terminowania tuneli IPSec site-to-site z metodą authentykacji współdzielonego klucza (pre shared key) lub certyfikatu
105. Rozwiązanie musi umożliwiać natywną integrację z produktami firm trzecich oferującymi rozwiązania typu Next Generation Firewall warstwy 7, m.in. integracja z systemem do zarządzania Next Generation Firewall
106. Rozwiązanie musi umożliwiać przekierowanie wybranego ruchu L2 do rozwiązań firm trzecich z obszaru bezpieczeństwa
107. Oferowane oprogramowanie musi zapewnić funkcjonalność rozkładania/równoważenia ruchu – tj. load balancing działającą do warstwy 7 modelu ISO OSI:
	1. Rozwiązanie musi zapewniać następujące mechanizmy przywiązania sesji: adres źródłowy, cookie, SSL ID oraz JSessionID
	2. W ramach inspekcji warstwy 7 rozwiązanie musi oferować funkcję blokowania i modyfikacji URL
	3. Rozwiązanie musi oferować możliwość wstrzykiwania nagłówka XFF (X-Fowarder-For)
108. Funkcja Wirtualny Load Balancer musi być realizowana i w pełni zintegrowana z platformą do wirtualizacji sieci
109. Rozwiązanie typu Identity Firewall musi zapewniać integrację z Active Direcory z obsługą selektywnej synchronizacji
110. Rozwiązanie musi posiadać funkcję łączenia (bridge) segmentów sieci L2 VLAN i VXLAN poprzez zastosowanie fizycznego przełącznika firm trzecich
111. Rozwiązanie musi zapewniać mechanizm wspomagający planowanie tworzenia grup oraz polityk bezpieczeństwa
112. Rozwiązanie musi oferować funkcjonalność typu Identity Firewall umożliwiające obsługę sesji użytkowników na pulpitach wirtualnych (VDI) oraz serwerach aplikacji (RDSH) współdzielących pojedynczy adres IP
113. Rozwiązanie musi oferować funkcjonalność identyfikacji aplikacji, np. MySQL, http, DNS, DHCP, Active Directory, TLS, itp. na poziomie sieciowym OSI warstw 5-7, a następnie móc wykorzystać tę informację w rozproszonym firewall w celu kontroli dostępu nie tylko na poziomie adresów IP oraz portów, ale również w połączeniu adresów IP, portów oraz zidentyfikowanej aplikacji
114. Rozwiązanie musi mieć możliwość analizowania przepływów sieciowych (w tym IPFIX) opartych o wirtualizację VMware vSphere
115. Rozwiązanie musi mieć możliwość tworzenia raportów przepływów z informacją uwzględniającą adresy IP oraz porty TCP/UDP dla środowiska wirtualnego oraz fizycznego
116. Rozwiązanie musi mieć możliwość wykorzystania wbudowanego kolektora w celach dalszej analizy ruchu
117. Rozwiązanie musi mieć możliwość tworzenia automatycznych rekomendacji reguł firewalla na bazie zebranych informacji o przepływach
118. Rozwiązanie musi mieć możliwość wizualizacji ścieżki logicznej i przejść w relacji vm-vm, wskazanie komponentów sieciowych w topologii logicznej i fizycznej (przełączników, routerów, firewalli) oraz połączeń między nimi z uwzględnieniem komponentów wirtualnych
119. Rozwiązanie musi mieć możliwość wizualizacji przepływów pomiędzy maszynami wirtualnymi i/lub środowiskiem fizycznym pogrupowanych ze względu na sieci wirtualne, podsieci, aplikacje, grupy bezpieczeństwa
120. Rozwiązanie musi mieć możliwość informowania o tym, jakie reguły firewalla wirtualnego są aktualnie zaaplikowane i aktywne
121. Rozwiązanie musi mieć możliwość informowania o maskowanych regułach firewalla, czyli regułach, które nie są wykorzystywane ze względu na reguły położone wyżej
122. Rozwiązanie musi mieć możliwość wizualizacji połączeń maszyn wirtualnych do zasobów dyskowych, połączenia do hosta i wyjścia na zewnątrz do sieci fizycznej
123. Rozwiązanie do analizy przepływów sieciowych musi posiadać funkcjonalność API
124. **Zadanie III - Dostawa oraz wdrożenie oprogramowania do backupu z wykorzystaniem urządzenia do backupu dyskowego z deduplikacją**

Przedmiotem tego zadania jest dostawa oraz wdrożenie oprogramowania do wykonywania backupu i odzyskiwania danych środowiska wirtualnego z wykorzystaniem urządzenia do backupu dyskowego z deduplikacją opisanego w Zadaniu I w Tabeli 6 oraz z uwzględnieniem oprogramowania wirtualizacyjnego dostarczonego w ramach Zadania II.

Wymaganymi elementami zamówienia są:

1. Oprogramowanie do wykonywania backupu i odzyskiwania danych dla 6 serwerów fizycznych dwu procesorowych dostarczonych w Zadaniu I i opisanych w Tabeli 3 i 4 oraz podsystemu dyskowego składającego się z dysków SSD o łącznej pojemności ponad 200 TB,
2. 5 letni okres gwarancji zapewniającej możliwość wprowadzania wszelkich poprawek i nowych wersji, które powstaną w tym okresie na całe dostarczone oprogramowanie

**W ramach wdrożenia oprogramowania do backupu i budowy środowiska z wykorzystaniem urządzenia do backupu dyskowego z deduplikacją Wykonawca powinien:**

Wykonać instalację i konfigurację oprogramowania do wykonywania backupu i odzyskiwania danych środowiska wirtualnego z wykorzystaniem urządzenia do backupu dyskowego z deduplikacją opisanego w Zadaniu I w Tabeli 6 z uwzględnieniem oprogramowania wirtualizacyjnego dostarczonego w ramach Zadania II.

Infrastruktura sprzętowa, która będzie korzystała z dostarczonego oprogramowania backupowego będzie się znajdować w jednej szafie rack. Infrastruktura będzie składać się z 6 serwerów fizycznych dwu procesorowych dostarczonych w Zadaniu I i opisanych w Tabeli 3 i 4 oraz urządzenia do deduplikacji dostarczonego w Zadaniu I i opisanego w Tabeli 6. Podsystem dyskowy podlegający wykonywaniu kopii zapasowych ma łączną pojemność ponad 200 TB.

Wdrożona infrastruktura środowiska backupowego dla tej infrastruktury musi być skonfigurowana i w pełni funkcjonalna.

W ramach prac wdrożeniowych Wykonawca:

1. Przygotuje szczegółowy **Projekt techniczny** realizacji, uwzględniający dobre praktyki i rekomendacje eksploatacyjne publikowane przez producenta dostarczanego oprogramowania.
2. Dokona weryfikacji:
* środowiska fizycznego/wirtualnego pod wymagania wdrożenia,
* przydzielonej przestrzeni dyskowej przeznaczonej na wdrożenie,
* dostępu do zewnętrznej bazy danych MS SQL oraz połączeń sieciowych
1. Przygotuje systemy pod wdrożenie (maszyny z komponentami serwerowymi dostarczonego oprogramowania oraz maszyny robocze)
2. Wykona instalację i konfigurację wszystkich niezbędnych elementów oprogramowania wymaganych przez Zamawiającego.
3. Skonfiguruje repozytoria kopii zapasowych na zasobach utworzonych na dedykowanej macierzy dyskowej z wykorzystaniem deduplikatora sprzętowego
4. Skonfiguruje zadania wykonywania kopii zapasowych zgodnie z wymaganiami Zamawiającego
5. Wykona testy akceptacyjne (niezawodnościowe oraz funkcjonalne) oraz opracuje i przedstawi Raport z testów.
6. Opracuje **Dokumentację powykonawczą** zawierającą opis wdrożonej konfiguracji oraz procedury administracyjne i eksploatacyjne wykonywania i odtwarzania kopii zapasowych środowiska zarówno na macierz jak i deduplikator oraz odtwarzanie z kopii w zakresie uzgodnionym z Zamawiającym w tym:
* odtworzenie pojedynczych danych plikowych z wykonanych kopii zapasowych
* odtworzenie pełnych maszyn wirtualnych, w tym serwerów SQL
* procedura odtworzenia hosta wirtualizacyjnego w przypadku jego całkowitej awarii: odtworzenie hosta wirtualizacyjnego wraz z działającymi na nim wirtualnymi maszynami
* procedura w razie całkowitej awarii: odtworzenie danych i środowiska na podstawie repliki kopii zapasowych.
1. Dokumentacja powykonawcza wdrożonego oprogramowania do backupu, zostanie przekazana Zamawiającemu najpóźniej w dniu podpisania Protokołu odbioru Zadania III, w formie papierowej w 2 egzemplarzach oraz w formie elektronicznej na pendrive, w postaci plików do edycji i PDF.

**Wymagania dla oprogramowania**

1. **Wymagania ogólne**
2. Oprogramowanie musi współpracować co najmniej z infrastrukturą wirtualizacyjną VMware w wersji 5.x, 6.x oraz Microsoft Hyper-V 2012 R2, 2016 i 2019. Wszystkie funkcjonalności opisane w tej specyfikacji muszą być dostępne na wszystkich wspieranych platformach wirtualizacyjnych, chyba, że wyszczególniono inaczej.
3. Oprogramowanie musi współpracować z hostami zarządzanymi przez VMware vCenter oraz pojedynczymi hostami.
4. Oprogramowanie musi współpracować z hostami zarządzanymi przez System Center Virtual Machine Manager, klastrami hostów oraz pojedynczymi hostami.
5. Oprogramowanie musi zapewniać tworzenie kopii zapasowych wszystkich systemów operacyjnych maszyn wirtualnych, wspieranych przez vSphere i Hyper-V.
6. **Wymagania podstawowe**
7. Oprogramowanie musi być licencjonowanie w modelu “per-CPU”. Wszystkie wymienione poniżej funkcjonalności muszą być zapewnione w tej licencji. Jakiekolwiek dodatkowe licencjonowanie (per zabezpieczony TB, dodatkowo płatna deduplikacja) nie jest dozwolone.
8. Oprogramowanie musi umożliwiać wykorzystanie dowolnej platformy serwerowej i dyskowej.
9. Oprogramowanie musi tworzyć “samowystarczalne” archiwa do odzyskania których nie wymagana jest osobna baza danych z metadanymi deduplikowanych bloków.
10. Oprogramowanie musi mieć mechanizmy deduplikacji i kompresji w celu zmniejszenia wielkości archiwów. Włączenie tych mechanizmów nie może skutkować utratą jakichkolwiek funkcjonalności wymienionych w tej specyfikacji.
11. Oprogramowanie musi zapewniać warstwę abstrakcji nad poszczególnymi urządzeniami pamięci masowej, pozwalając utworzyć jedną wirtualną pulę pamięci na kopie zapasowe. Wymagane jest wsparcie dla nieograniczonej liczby pamięci masowych w takiej puli.
12. Oprogramowanie nie może przechowywać danych o deduplikacji w centralnej bazie. Utrata bazy danych używanej przez oprogramowanie nie może prowadzić do utraty możliwości odtworzenia backupu. Metadane deduplikacji muszą być przechowywane w plikach backupu.
13. Oprogramowanie nie może instalować żadnych stałych agentów wymagających wdrożenia
czy upgradowania wewnątrz maszyny wirtualnej dla jakichkolwiek funkcjonalności backupu lub odtwarzania.
14. Oprogramowanie musi zapewniać backup jednoprzebiegowy - nawet w przypadku wymagania granularnego odtworzenia.
15. Oprogramowanie musi zapewniać mechanizmy informowania o wykonaniu/błędzie zadania poprzez email lub SNMP. W środowisku VMware musi mieć możliwość aktualizacji pola „notatki” na wirtualnej maszynie.
16. Oprogramowanie musi mieć możliwość uruchamiania dowolnych skryptów przed i po zadaniu backupowym lub przed i po wykonaniu zadania snapshota w środowisku VMware.
17. Oprogramowanie musi oferować portal samoobłsugowy, umożliwiający odtwarzanie użytkownikom wirtualnych maszyn, obiektów MS Exchange i baz danych MS SQL (w tym odtwarzanie point-in-time).
18. Oprogramowanie musi zapewniać możliwość delegacji uprawnień do odtwarzania na portalu.
19. Oprogramowanie musi mieć możliwość integracji z innymi systemami poprzez wbudowane RESTful API.
20. Oprogramowanie musi mieć wbudowane mechanizmy backupu konfiguracji w celu prostego odtworzenia systemu po całkowitej reinstalacji.
21. Oprogramowanie musi mieć wbudowane mechanizmy szyfrowania zarówno plików
z backupami jak i transmisji sieciowej. Włączenie szyfrowania nie może skutkować utratą jakiejkolwiek funkcjonalności wymienionej w tej specyfikacji.
22. Oprogramowanie musi oferować zarządzanie kluczami szyfrowania w przypadku utraty podstawowego klucza.
23. Oprogramowanie musi wspierać backup maszyn wirtualnych używających współdzielonych dysków VHDX na Hyper-V (shared VHDX).
24. Oprogramowanie musi posiadać architekturę klient/serwer z możliwością instalacji wielu instancji konsoli administracyjnych.
25. **Wymagania dotyczące wykonywania kopii zapasowych**
26. Oprogramowanie musi wykorzystywać mechanizmy Change Block Tracking na wszystkich wspieranych platformach wirtualizacyjnych. Mechanizmy muszą być certyfikowane przez dostawcę platformy wirtualizacyjnej.
27. Oprogramowanie musi oferować możliwość sterowania obciążeniem storage'u produkcyjnego tak aby nie przekraczane były skonfigurowane przez administratora backupu poziomy latencji. Funkcjonalność ta musi być dostępna na wszystkich wspieranych platformach wirtualizacyjnych.
28. Oprogramowanie musi oferować powyższy mechanizm z dokładnością do datastore’u.
29. Oprogramowanie musi automatycznie wykrywać i usuwać snapshoty-sieroty (orphaned snapshots), które mogą zakłócić poprawne wykonanie backupu. Proces ten nie może wymagać interakcji administratora.
30. Oprogramowanie musi wspierać kopiowanie backupów na taśmy wraz z pełnym śledzeniem wirtualnych maszyn.
31. Oprogramowanie musi mieć możliwość kopiowania backupów do lokalizacji zdalnej.
32. Oprogramowanie musi mieć możliwość tworzenia retencji GFS (Grandfather-Father-Son).
33. Oprogramowanie musi umieć korzystać z protokołu Catalyst w przypadku gdy repozytorium backupów jest umiejscowione na oferowanym urządzeniu. Funkcjonalność powinna wspierać łącze sieciowe Ethernet lub FC SAN.
34. Oprogramowanie musi mieć możliwość kopiowania backupów oraz replikacji wirtualnych maszyn do zdalnej lokalizacji z wykorzystaniem wbudowanej akceleracji WAN.
35. Oprogramowanie musi mieć możliwość replikacji włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere, pomiędzy hostami ESXi, włączając asynchroniczną replikacją ciągłą. Dodatkowo oprogramowanie musi mieć możliwość użycia plików kopii zapasowych jako źródła replikacji.
36. Oprogramowanie musi umożliwiać przechowywanie punktów przywracania dla replik.
37. Oprogramowanie musi umożliwiać wykorzystanie istniejących w infrastrukturze wirtualnych maszyn jako źródła do dalszej replikacji (replica seeding).
38. Oprogramowanie musi wykorzystywać wszystkie oferowane przez hypervisor tryby transportu (sieć, hot-add, LAN Free-SAN).
39. Oprogramowanie musi dawać możliwość tworzenia backupów ad-hoc z konsoli jak i z klienta webowego vSphere.
40. Oprogramowanie musi przetwarzać wiele wirtualnych dysków jednocześnie (parallel processing).
41. **Wymagania dotyczące odtwarzania danych i systemów z kopii zapasowych.**
42. Oprogramowanie musi umożliwić uruchomienie wielu maszyn wirtualnych bezpośrednio
ze zdeduplikowanego i skompresowanego pliku backupu, z dowolnego punktu przywracania, bez potrzeby kopiowania jej na storage produkcyjny. Funkcjonalność musi być oferowana niezależnie od rodzaju storage’u użytego do przechowywania kopii zapasowych. Dla środowiska vSphere powinien być wykorzystany wbudowany w oprogramowanie serwer NFS. Dla Hyper-V powinna być zapewniona taka sama funkcjonalność realizowana wewnętrznymi mechanizmami oprogramowania.
43. Oprogramowanie musi pozwalać na migrację on-line tak uruchomionych maszyn na storage produkcyjny. Migracja powinna odbywać się mechanizmami wbudowanymi w hypervisor. Jeżeli licencja na hypervisor nie posiada takich funkcjonalności - oprogramowanie musi realizować taką migrację swoimi mechanizmami.
44. Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny, plików konfiguracji i dysków.
45. Oprogramowanie musi umożliwić odtworzenie plików na dowolną maszynę, lub na serwer produkcyjny bez potrzeby użycia agenta instalowanego wewnątrz wirtualnej maszyny. Funkcjonalność ta nie powinna być ograniczona wielkością i liczbą przywracanych plików.
46. Oprogramowanie musi mieć możliwość odtworzenia plików przy pomocy VMware VIX API
47. Oprogramowanie musi wspierać odtwarzanie plików z następujących systemów plików:
48. Linux
* ext3, ext4, JFS, XFS, Btrfs,
1. BSD
* UFS, UFS2
1. Solaris
* UFS, ZFS
1. Windows
* NTFS, FAT, FAT32, ReFS
1. Oprogramowanie musi wspierać przywracanie plików z partycji Linux LVM oraz Windows Storage Space.
2. Oprogramowanie musi umożliwiać szybkie granularne odtwarzanie obiektów aplikacji
bez użycia jakiegokolwiek agenta zainstalowanego wewnątrz maszyny wirtualnej.
3. Oprogramowanie musi wspierać granularne odtwarzanie dowolnych obiektów i dowolnych atrybutów Active Directory włączając hasło, obiekty Group Policy, partycja konfiguracji AD, rekordy DNS zintegrowane z AD.
4. Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Exchange 2010 i nowszych (dowolny obiekt w tym obiekty w folderze "Permanently Deleted Objects"),
5. Oprogramowanie musi wspierać granularne odtwarzanie Microsoft SQL 2012 i nowsze włączając bazy danych z opcją odtwarzania point-in-time, tabele, schemat.
6. Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Sharepoint 2010 i nowsze. Opcja odtworzenia elementów, witryn, uprawnień.
7. Oprogramowanie musi wspierać granularne odtwarzanie baz danych Oracle z opcją odtwarzanie point-in-time. Funkcjonalność ta musi być dostępna dla baz uruchomionych
w środowiskach Windows oraz Linux bez konieczności pełnego odtworzenia wirtualnej maszyny ani jej uruchomienia.
8. Oprogramowanie musi indeksować pliki Windows i Linux w celu szybkiego wyszukiwania plików w plikach backupowych.
9. Oprogramowanie musi używać mechanizmów VSS wbudowanych w system operacyjny Microsoft Windows.
10. Oprogramowanie musi wspierać także specyficzne metody odtwarzania w tym "reverse CBT" oraz odtwarzanie z wykorzystaniem sieci SAN.
11. **Weryfikacja poprawności kopii zapasowych**
12. Oprogramowanie musi dawać możliwość stworzenia laboratorium (izolowanego środowiska) dla vSphere i Hyper-V, używając wirtualnych maszyn uruchamianych bezpośrednio z plików backupu. Dla VMware’a oprogramowanie musi pozwalać na uruchomienie takiego środowiska bezpośrednio ze snapshotów macierzowych stworzonych na wspieranych urządzeniach.
13. Oprogramowanie musi umożliwiać weryfikację odtwarzalności wielu wirtualnych maszyn jednocześnie z dowolnego backupu według własnego harmonogramu w izolowanym środowisku. Testy powinny uwzględniać możliwość uruchomienia dowolnego skryptu testującego również aplikację uruchomioną na wirtualnej maszynie. Testy muszą być przeprowadzone bez interakcji z administratorem
14. **Warunki potwierdzenia realizacji dla 3 zadań:**
15. **Odbiór Projektu Technicznego i Dokumentacji powykonawczej**
	1. Potwierdzeniem realizacji danego Zadania będzie Protokół odbioru Zadania podpisany z wynikiem pozytywnym
	2. **Wspólny Projekt techniczny** dotyczący realizacji wszystkich Zadań, opisujący szczegółową konfigurację urządzeń i oprogramowania niezbędnego do realizacji wdrożenia, uwzględniający szczegółowe projekty techniczne Zadań I –III, podlegał będzie procedurze odbioru, na następujących warunkach:
16. Wykonawca przekaże Zamawiającemu wspólny Projekt techniczny, nie później niż 30 dni od dnia zawarcia Umowy,
17. Zamawiający w terminie nie dłuższym niż 5 dni od dnia dostarczenia wspólnego Projektu technicznego, poinformuje Wykonawcę o jego akceptacji lub o konieczności wprowadzenia zmian,
18. wszystkie uwagi do wspólnego Projektu technicznego zgłoszone przez Zamawiającego zostaną wprowadzone przez Wykonawcę, w terminie nie dłuższym niż 3 dni od dnia ich otrzymania,
19. Zamawiający w terminie 3 dni od dnia powtórnego dostarczenia przez Wykonawcę poprawionego wspólnego Projektu technicznego, poinformuje Wykonawcę o jego akceptacji lub konieczności wprowadzenia zmian,
20. Zamawiający zastrzega sobie prawo do trzykrotnego zgłoszenia zmian we wspólnym Projekcie technicznym,
21. komunikacja pomiędzy Zamawiającym a Wykonawcą w zakresie akceptacji wspólnego Projektu technicznego, odbywać się będzie drogą mailową na adres poczty elektronicznej Wykonawcy wskazany w Umowie,
22. zatwierdzony wspólny Projekt techniczny zostanie przekazany Zamawiającemu najpóźniej w dniu podpisania Protokołu odbioru projektu, w formie papierowej w 2 egzemplarzach oraz w formie elektronicznej na pendrive, w postaci plików do edycji i PDF,
23. potwierdzeniem odbioru Projektu technicznego będzie Protokół odbioru projektu podpisany z wynikiem pozytywnym przez osoby odpowiedzialne za realizację Umowy ze strony Wykonawcy i Zamawiającego;
	1. Dokumentacja Powykonawcza przygotowana dla każdego Zadania, opisująca szczegółowo konfigurację wdrożonego rozwiązania, podlegała będzie procedurze odbioru na poniższych zasadach:
		1. Wykonawca przekaże Zamawiającemu do akceptacji Dokumentację powykonawczą, niepóźniej niż na 15 dni przez terminem zakończenia realizacji poszczególnych Zadań,
		2. Zamawiający, w terminie nie dłuższym niż 3 dni od dnia dostarczenia przez Wykonawcę Dokumentacji powykonawczej, poinformuje Wykonawcę o jej akceptacji lub konieczności wprowadzenia zmian,
		3. wszystkie uwagi do Dokumentacji powykonawczej zgłoszone przez Zamawiającego zostaną wprowadzone przez Wykonawcę, w terminie nie dłuższym niż 2 dni od dnia ich otrzymania,
		4. Zamawiający, w terminie 2 dni od dnia powtórnego dostarczenia przez Wykonawcę poprawionej Dokumentacji powykonawczej, poinformuje Wykonawcę o jej akceptacji lub konieczności wprowadzenia zmian,
		5. Zamawiający zastrzega sobie prawo do dwukrotnego zgłoszenia zmian w Dokumentacji powykonawczej,
		6. komunikacja pomiędzy Zamawiającym a Wykonawcą, w zakresie akceptacji Dokumentacji powykonawczej, odbywać się będzie drogą mailową na adres poczty elektronicznej Wykonawcy i Zamawiającego,
		7. zatwierdzona Dokumentacja powykonawcza zostanie przekazana Zamawiającemu najpóźniej niż w dniu podpisania Protokołu odbioru poszczególnych Zadań, w formie papierowej w 2 egzemplarzach oraz w formie elektronicznej na pendrive, w postaci plików do edycji i PDF,
		8. potwierdzeniem odbioru zaakceptowanej przez Zamawiającego poszczególnych Zadań podpisany z wynikiem pozytywnym przez osoby odpowiedzialne za realizację Umowy ze strony Wykonawcy i Zamawiającego.
24. **Odbiór dostawy urządzeń dostarczonych w ramach Zadania I**
25. Odbiór ilościowy dostarczonych elementów zamówienia sprzętowego będzie się odbywał w obecności przedstawiciela Zamawiającego i Wykonawcy.
26. Wykonawca przygotuje zestawienie dostarczonego sprzętu z zaznaczeniem typu urządzenia, numerów fabrycznych i ilości.
27. Warunkiem przyjęcia dostarczonych urządzeń, jest sprawdzenie ich przez uprawnionego przedstawiciela Zamawiającego, w zakresie zgodności ze złożoną przez Wykonawcę Ofertą oraz warunkami Umowy. Sprawdzeniu podlegać będzie w szczególności: ilość dostarczonych urządzeń oraz czas (godziny) wykonania dostawy, który powinien uwzględniać wymagania klauzuli środowiskowej. Do każdej dostawy Wykonawca dołączy oświadczenie, potwierdzające, że dostarczone Urządzenia są zgodne z wymaganiami określonymi przez Zamawiającego w Opisie przedmiotu zamówienia oraz Ofertą Wykonawcy,
28. Potwierdzeniem wykonania każdej z dostaw Urządzeń, będzie Protokół odbioru dostawy podpisany przez Strony z wynikiem pozytywnym,
29. **Odbiór dostawy oprogramowania**

1) odbiorowi podlega całość oprogramowania określonego dla Zadania II i Zadania III,

2) odbiór oprogramowania nastąpi na podstawie dostarczonych elektronicznie przez Wykonawcę dokumentów licencyjnych wystawionych na Zamawiającego,

3) warunkiem przyjęcia dostarczonego oprogramowania, jest jego sprawdzenie przez uprawnionego przedstawiciela Zamawiającego, w zakresie zgodności ze złożoną przez Wykonawcę Ofertą oraz warunkami Umowy. Do każdej dostawy Wykonawca dołączy oświadczenie, potwierdzające, że dostarczone oprogramowanie jest zgodne z wymaganiami określonymi przez Zamawiającego w Opisie przedmiotu zamówienia oraz Ofertą Wykonawcy,

4) potwierdzeniem wykonania każdej z dostaw oprogramowania, będzie Protokół odbioru dostawy podpisany przez Strony z wynikiem pozytywnym,

1. **Warunki gwarancji**
2. Wszystkie oferowane elementy dostawy tj. urządzenia oraz oprogramowanie muszą być objęte minimum pięcioletnią gwarancją.
3. Gwarancja obejmuje zaoferowane w Zadaniu I urządzenia: infrastrukturę serwerowo-sieciową opisaną w Tabeli 2, serwery opisane w Tabelach 3, 4 i 5 oraz urządzenie do backupu dyskowego z deduplikacją opisane w Tabeli 6. Gwarancja będzie obejmować wszystkie komponenty oferowanych urządzeń - uszkodzone dyski twarde pozostają własnością Zamawiającego.
4. Gwarancja dotyczy oprogramowania do wirtualizacji opisanego w Zadaniu II oraz oprogramowania do backupu opisanego w Zadaniu III.
5. Warunki udzielonej gwarancji będą zgodne z wymaganiami Zamawiającego, z zastrzeżeniem, że nie mogą być gorsze niż warunki gwarancji producenta(ów) urządzeń i oprogramowania.
6. Udzielona przez Wykonawcę gwarancja nie wyłącza prawa Zamawiającego do gwarancji udzielonych przez producentów urządzeń i oprogramowania, dostarczonych w ramach realizacji przedmiotu zamówienia.
7. W okresie gwarancji dotyczącej zaoferowanych urządzeń Wykonawca:
8. zapewni koordynatora obsługi gwarancyjnej, z którym będą prowadzone wszelkie bieżące uzgodnienia w zakresie realizacji napraw gwarancyjnych i przeglądów,
9. wykona cykliczne przeglądy urządzeń nie rzadziej niż co 12 miesięcy, przy czym pierwszy i ostatni przegląd powinny być przeprowadzone odpowiednio w pierwszym i ostatnim roku obowiązywania gwarancji,
10. zapewni Zmawiającemu 100 godzin bezpłatnych konsultacji technicznych dotyczących zaoferowanych urządzeń w siedzibie Zamawiającego,
11. udzielać będzie konsultacji zdalnych (np. e-mail, telefon) dotyczących rozwiązywania problemów występujących podczas obsługi lub funkcjonowania urządzeń.
12. zapewni realizację serwisu gwarancyjnego w języku polskim
13. Warunki świadczenia gwarancji dotyczącej zaoferowanych urządzeń:
	1. gwarancja będzie świadczona w miejscu instalacji,
	2. zgłaszanie Awarii lub problemów technicznych przyjmowane będą w trybie 24x7, usunięcie Awarii i przywrócenie pełnej funkcjonalności Urządzenia wykazującego awarię, zostanie wykonane w terminie 24 godzin od zgłoszenia Awarii, z zastrzeżeniem, że w przypadku gdy termin usunięcia Awarii przypadać będzie na dzień ustawowo wolny od pracy, usunięcie awarii nastąpi w następnym dniu roboczym przypadającym bezpośrednio po dniu ustawowo wolnym od pracy,
	3. w celu świadczenia gwarancji wykonawca uruchomi kanał kontaktowy w formie elektronicznej przez stronę www lub za pomocą poczty elektronicznej lub telefonicznej, umożlwiający zgłaszanie Awarii,
	4. wszystkie zgłoszenia muszą być obsługiwane zgodnie z wymaganym czasem reakcji,
	5. diagnoza problemu wliczana jest w wymagany czas naprawy,
	6. serwis gwarancyjny musi być realizowany przez Wykonawcę w języku polskim,
	7. przez Awarię rozumie się wadę urządzenia, zdarzenie, w wyniku, którego uszkodzeniu uległ jeden (lub więcej) element urządzenia, ograniczający jego wydajność i funkcjonalność i uniemożliwiający Zamawiającemu korzystanie z urządzenia zgodnie z jego Specyfikacją Techniczną lub Instrukcją użytkowania,
	8. czas reakcji (rozumiany jako maksymalny czas, jaki może upłynąć pomiędzy zgłoszeniem Awarii, a reakcją Serwisu) na podjęcie działań diagnostycznych przez Wykonawcę i kontakt ze zgłaszającym nie może przekroczyć 4 godzin od momentu gwarancyjnego zgłoszenia Awarii przez Zamawiającego, jeżeli do zgłoszenia doszło do godziny 16:00 dnia roboczego. W przypadku gwarancyjnego zgłoszenia Awarii po godzinie 16:00 lub w dzień ustawowo wolny od pracy, podjęcie działań diagnostycznych przez Wykonawcę i kontakt ze zgłaszającym nastąpi następnego dnia roboczego w godzinach od 8:00 do 12:00,
	9. w przypadku gdy nie będzie możliwe usunięcie Awarii urządzenia, w miejscu i terminie określonym w pkt.7 ppkt2), wykonawca zobowiązany będzie dostarczyć na czas jego naprawy wolne od wad urządzenie zastępcze, o parametrach technicznych nie gorszych niż parametry urządzania wykazującego Awarię,
	10. w przypadku, jeżeli Awaria urządzenia nie zostanie usunięta w terminie 30 dni od dnia jej zgłoszenia przez Zamawiającego oraz w przypadku ponownego wystąpienia awarii urządzenia po wykonaniu dwóch napraw dotyczących tego samego elementu (zespołu), Wykonawca zobowiązany będzie do wymiany urządzenia na nowe, o parametrach nie gorszych niż urządzenie podlegające wymianie,
	11. wszelkie koszty związane z naprawami gwarancyjnymi, usuwaniem Awarii, włączając w to koszt części i transportu z i do siedziby Zamawiającego ponosi Wykonawca,
	12. usunięcie Awarii, będzie każdorazowo potwierdzone Protokołem wykonania naprawy, którego wzór stanowi załącznik do umowy,
	13. w przypadku, gdy w urządzeniach, dokonana zostanie istotna naprawa lub gdy nastąpi jego wymiana na nowe, okres gwarancji na to urządzenie zostaje wydłużony o czas diagnozy i wykonania naprawy urządzenia lub o czas wymiany wadliwie działającego elementu urządzenia na nowe lub całego urządzenia na nowe, z zastrzeżeniem, że przez istotną naprawę rozumie się naprawę urządzenia lub naprawę elementu urządzenia, mającego istotne znaczenie dla funkcjonowania urządzenia jako całości, którego wada zmniejsza użyteczność całego urządzenia; Naprawa może być oceniona jako istotna w przypadku nagromadzenia się drobnych napraw, w przypadku, gdy nakład pracy niezbędny do usunięcia wady nie jest duży ale bez usunięcia tej wady użyteczność urządzenia jako całości byłaby zmniejszona oraz w przypadku wielokrotnej naprawy lub wymiany tego samego elementu urządzenia, wykazującego wady w działaniu,
	14. w przypadku stwierdzenia niezgodności w sposobie realizacji przez Wykonawcę zobowiązań gwarancyjnych, Zamawiający zastrzega sobie prawo do naliczenia kar umownych i potrącenia ich z Zabezpieczenia należytego wykonania umowy, z zastrzeżeniem, że może to nastąpić po zakończeniu okresu realizacji umowy,
	15. w przypadku, jeżeli Wykonawca nie wywiązuje się ze zobowiązań wynikających z gwarancji, Zamawiający może dokonać czynności naprawy we własnym zakresie lub zlecić jej wykonanie osobie trzeciej, a kosztami obciążyć Wykonawcę z wykorzystaniem kwoty zabezpieczenia należytego wykonania umowy, z zastrzeżeniem, że może to nastąpić po zakończeniu okresu realizacji umowy,
	16. Zamawiający ma prawo dokonywania rozbudowy urządzeń, zgodnie z dokumentacją techniczną, przez wykwalifikowanych pracowników, a także prawo do przemieszczenia zainstalowanych urządzeń bez utraty gwarancji. Wykonawca nie ponosi odpowiedzialności za uszkodzenia mechaniczne przedmiotu zamówienia powstałe z winy pracowników Zamawiającego.
14. Warunki świadczenia gwarancji dotyczącej zaoferowanego oprogramowania:
15. W okresie gwarancji Wykonawca musi zapewnić dostęp do bazy wiedzy, aktualnych wersji oraz krytycznych poprawek producentów komponentów związanych z bezpieczeństwem i stabilnością działania oprogramowania w całym czasie trwania gwarancji, poprzez wskazanie i udostępnienie odpowiednich stron www.
16. W ramach gwarancji Wykonawca zapewni wsparcie techniczne inżyniera Wykonawcy w sytuacji krytycznej zagrażającej stabilnej pracy oprogramowania, w formie konsultacji zdalnych (np. e-mail, telefon) lub w miejscu instalacji.
17. W ramach gwarancji Wykonawca zapewni wsparcie techniczne inżyniera Wykonawcy w czasie wykonywania przez Zamawiającego planowanych instalacji poprawek, uaktualnień lub nowych wersji oprogramowania w formie konsultacji zdalnych (np. e-mail, telefon), lub w miejscu instalacji.
18. W ramach gwarancji Wykonawca zapewni wsparcie techniczne inżyniera Wykonawcy, w tym zdalną diagnozę, w przypadku wystąpienia nieprzewidzianych problemów z oprogramowaniem oraz zapewni rozwiązywanie bieżących problemów technicznych związanych z funkcjonowaniem oprogramowania, w formie konsultacji zdalnych (np. e-mail, telefon), lub w miejscu instalacji.
19. W ramach gwarancji Wykonawca zapewni 100 godzin bezpłatnych konsultacji w zakresie eksploatacji, konfiguracji oraz funkcjonalności oprogramowania w formie konsultacji zdalnych (np. e-mail, telefon), lub w miejscu instalacji.

**Część II**

**W ramach realizacji Części II** Wykonawca dostarczy bezterminowe licencje oprogramowania systemowego narzędziowego oraz bazodanowego dla Centrum Przetwarzania Danych w Głównym Urzędzie Statystycznym na potrzeby projektu „System Monitorowania Usług Publicznych – wdrożenie SMUP” realizowanego w ramach Programu Operacyjnego Wiedza Edukacja Rozwój 2014-2020, wyszczególnionego w Tabeli 1.

**Tabela 1 -** Zestawienie oprogramowania objętego zamówieniem

|  |  |  |  |
| --- | --- | --- | --- |
| **Pozycja OPZ(sekcja)** | **Typ oprogramowania** | **Metoda licencjonowania** | **Liczba elementów1) objętych licencjonowaniem** |
| **A** | Serwerowy system operacyjny dla środowisk o wysokim stopniu wirtualizacji  | Na rdzeń procesora*(per core)* | 192 |
| **B** | Serwerowy system operacyjny na serwery fizyczne. | Na rdzeń procesora*(per core)* | 32 |
| **C** | Pakiet produktów narzędziowych do zarządzania i monitorowania serwerów oraz zarządzania wirtualizacją serwerów dedykowany dla środowisk o wysokim stopniu wirtualizacji | Na rdzeń procesora*(per core)* | 192 |
| **D** | Pakiet Management Pack do monitorowania środowiska wirtualnego dla pakietu opisanego w sekcji C | Na procesor*(per socket)* | 12 |
| **E** | System bazodanowy dla nieograniczonej liczby użytkowników | Na rdzeń procesora*(per core)* | 32 |

1) procesorów/rdzeni/ wszystkie wyszczególnione elementy muszą być objęte licencjonowaniem

# Opis środowiska Zamawiającego

W Ośrodkach Przetwarzania Danych Zamawiający posiada środowisko serwerowe z zainstalowanym systemem operacyjnym MS Windows Server 2008 R2 i MS Windows Server 2012 R2, stanowiącym platformę systemową dla różnych komponentów infrastruktury informatycznej w tym:

* 1. Systemu usług katalogowych bazującego na MS Active Directory w wersji Windows Server 2012 R2 o funkcjonalności lasu i domeny na poziomie wersji Windows Server 2008 R2;
	2. Modułu monitorowania wydajności oraz dostępności aplikacji i usług zbudowanego na bazie systemu MS System Center Operations Manager 2012 R2;
	3. Modułu zarządzania konfiguracją dla serwerów stworzonego w oparciu o oprogramowanie MS System Center Configuration Manager 2012 R2;
	4. Systemu poczty korporacyjnej MS Exchange 2010 Sp3;
	5. Systemu komunikacji korporacyjnej MS Lync 2013;
	6. Środowisk MS Sharepoint 2013;
	7. Środowisk do wirtualizacji serwerów bazujących na oprogramowaniu VMware vCenter 5.1 oraz Hyper-V wraz MS System Center Virtual Machine Manager 2012 R2;
	8. Serwerów bazodanowych z oprogramowaniem MS SQL Server 2008 Enterprise, MS SQL Server 2012 Enterprise oraz MS SQL Server 2019 Enterprise ;

# Wymagania ogólne w zakresie licencji:

1. Licencje muszą pozwalać na swobodne przenoszenie pomiędzy stacjami roboczymi i/lub serwerami (np. w przypadku wymiany sprzętu) oraz możliwość sublicencjonowania dla jednostek służb statystyki publicznej.
2. Licencje na zamawiane oprogramowanie muszą być bezterminowe.
3. Licencje muszą obejmować najnowszą (najwyższą) wersję oprogramowania, dostępną na dzień złożenia oferty.
4. Z uwagi na szeroki zakres funkcjonalny planowanego wdrożenia na bazie zamawianego oprogramowania oraz konieczności minimalizacji kosztów związanych z wdrożeniem, szkoleniami i eksploatacją systemów, Zamawiający wymaga aby zaoferowane licencje, umożliwiały wykorzystanie wspólnych i jednolitych procedur masowej instalacji, uaktualniania, zarządzania i monitorowania.
5. Wymagane jest zapewnienie możliwości korzystania z wcześniejszych wersji zamawianego oprogramowania (umożliwia downgrading) i korzystania z kopii zamiennych (możliwość kopiowania oprogramowania na wiele urządzeń przy wykorzystaniu jednego standardowego obrazu uzyskanego z nośników dostępnych w programach licencji grupowych), z prawem do wielokrotnego użycia jednego obrazu dysku w procesie instalacji i tworzenia kopii zapasowych.
6. W ramach umowy Wykonawca jest zobowiązany zapewnić udzielanie uprawnień na witrynie producenta danego oprogramowania wskazanym przez Zamawiającego osobom (pracownikom Zamawiającego) do pobierania kodu zamówionego oprogramowania i kluczy licencyjnych.
7. Wymagane jest udostępnienie podstawowych informacji na temat instalacji i użytkowania oprogramowania na witrynie producenta.

# Specyfikacja techniczno-eksploatacyjna wraz z cechami użytkowymi przedmiotu zamówienia

# Serwerowy system operacyjny dla środowisk o wysokim stopniu wirtualizacji (SSOW)

1. Przedmiotem zamówienia jest dostawa serwerowego systemu operacyjnego dla środowisk
o wysokim stopniu wirtualizacji, w celu uzupełnienia stanu posiadanego oprogramowania.
2. Wskazane w opisie nazwy produktów odnoszą się do posiadanego i wykorzystywanego przez jednostki organizacyjne służb statystyki publicznej oprogramowania, a zachowanie parametrów określonych jako równoważne jest konieczne do zachowania kompatybilności i spójności środowiska. Zamawiający oczekuje ofert spełniających wymagania minimalne określone poniżej.
3. Zamawiający posiada licencje:
4. Windows Server 2008 R2 Datacenter,
5. Windows Server 2012 R2 Datacenter,
6. Windows Server 2019 Datacenter.
7. Oprogramowanie musi być dostarczone w najwyższej (najnowszej) wersji, na moment złożenia oferty przez Wykonawcę.
8. Dopuszcza się zaoferowanie produktów równoważnych do produktów wymienionych w pkt. 3.
9. Oferowany przez Wykonawcę Produkt, musi spełniać wszystkie warunki wymienione poniżej i posiadać następujące, wbudowane cechy:
	* 1. Możliwość uruchomienia oprogramowania serwerowego firm trzecich dedykowanego na system Windows Serwer 2012R2 lub nowszy.
		2. Możliwość wykorzystania co najmniej 2 logicznych procesorów oraz co najmniej 4 GB pamięci RAM w środowisku fizycznym.
		3. Możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności do 64TB przez każdy wirtualny serwerowy system operacyjny.
		4. Możliwość budowania klastrów składających się z 16 węzłów, z możliwością uruchamiania do 2000 maszyn wirtualnych.
		5. Możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci.
		6. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy.
		7. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy.
		8. Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.
		9. Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading.
		10. Wbudowane wsparcie instalacji i pracy na wolumenach, które:
10. pozwalają na zmianę rozmiaru w czasie pracy systemu,
11. umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,
12. umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów,
13. umożliwiają zdefiniowanie list kontroli dostępu (ACL).
	* 1. Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.
		2. Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez instytucję lub firmę upoważnioną do wydawania certyfikatu bezpieczeństwa danych. Za równoważny Zamawiający uzna certyfikat potwierdzający bezpieczeństwo danych.
		3. Możliwość uruchamiania aplikacji internetowych wykorzystujących technologię ASP.NET.
		4. Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.
		5. Graficzny interfejs użytkownika.
		6. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).
		7. Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.
		8. Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa.
		9. Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:
14. Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC,
15. Usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe) z możliwością wykorzystania następujących funkcji:
	1. Podłączenie SSOW do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną,
	2. Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,
	3. Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza,
16. Zdalna dystrybucja oprogramowania na stacje robocze,
17. Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej,
18. Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego umożliwiające:
19. Dystrybucję certyfikatów poprzez http,
20. Konsolidację CA dla wielu lasów domen,
21. Automatyczne rejestrowanie certyfikatów pomiędzy różnymi lasami domen.
22. Szyfrowanie plików i folderów,
23. Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec),
24. Możliwość tworzenia systemów wysokiej dostępności (klastry typu failover) oraz rozłożenia obciążenia serwerów,
25. Serwis udostępniania stron WWW,
26. Wsparcie dla protokołu IP w wersji 6 (IPv6),
27. Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows, posiadanymi przez Zamawiającego,
28. Wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie do 1000 aktywnych środowisk wirtualnych systemów operacyjnych. Wirtualne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności.
	* 1. Możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet.
		2. Wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath).
		3. Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego.
		4. Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.
		5. Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF.
29. Oprogramowanie równoważne musi być kompatybilne i w sposób niezakłócony współdziałać ze sprzętem i oprogramowaniem funkcjonującym u Zamawiającego.
30. Oprogramowanie równoważne nie może zakłócić pracy środowiska systemowo-programowego Zamawiającego.
31. Oprogramowanie równoważne musi w pełni współpracować z systemami już eksploatowanymi u Zamawiającego.
32. Oprogramowanie równoważne musi zapewniać pełną, równoległą współpracę i pełną funkcjonalną zamienność produktu z produktami stosowanymi przez Zamawiającego.
33. Produkt równoważny, oferowany przez Wykonawcę, musi spełniać wszystkie warunki wymienione poniżej:
34. Warunki licencji w każdym aspekcie licencjonowania są nie gorsze niż licencja produktu określonego w punkcie 2) tzn. licencja na oprogramowanie musi być przypisana do liczby rdzeni każdego procesora fizycznego na serwerze. Pozostałe parametry serwera np. ilość pamięci RAM nie mogą mieć wpływu na liczbę wymaganych licencji. Licencja musi uprawniać do uruchamiania serwerowego systemu operacyjnego (SSOW) w środowisku fizycznym i nielimitowanej liczby wirtualnych środowisk serwerowego systemu operacyjnego za pomocą wbudowanych mechanizmów wirtualizacji.
35. Nabycie licencji oprogramowania równoważnego pozwala na legalne używanie posiadanych przez Zamawiającego licencji oprogramowania w tym na serwerowy system operacyjny maszyn wirtualnych.
36. Ważność licencji na serwer fizyczny i serwerowy system operacyjny maszyn wirtualnych nie jest ograniczona czasowo.
37. Funkcjonalność oprogramowania równoważnego nie może być gorsza od funkcjonalności oprogramowania wykorzystywanego przez Zamawiającego, przy czym pod pojęciem funkcjonalności Zamawiający rozumie zbiór funkcji oprogramowania określających zakres jego wykorzystania z wyłączeniem wyglądu interfejsu, opisanych w pkt. 6.

# Serwerowy system operacyjny na serwery fizyczne (SSO)

1. Przedmiotem zamówienia jest dostawa serwerowego systemu operacyjnego na serwery fizyczne.
2. Oprogramowanie musi być dostarczone w najwyższej (najnowszej) wersji, na moment złożenia oferty przez Wykonawcę.
3. Wskazane w opisie nazwy produktów odnoszą się do posiadanego i wykorzystywanego przez jednostki organizacyjne służb statystyki publicznej oprogramowania, a zachowanie parametrów określonych jako równoważne jest konieczne do zachowania kompatybilności i spójności środowiska. Zamawiający oczekuje ofert spełniających wymagania minimalne określone poniżej.
4. Zgodnie z opisem środowiska Zamawiającego pkt. II.1. jako serwerowy system operacyjny, wykorzystywany jest:
	1. Windows Server 2012 R2,
	2. Windows Server 2008R2.
5. Oferowany produkt, przez wykonawcę musi spełniać wszystkie warunki poniżej:
	1. Licencja na oprogramowanie musi być przypisana do liczby rdzeni każdego procesora fizycznego na serwerze. Pozostałe parametry serwera np. ilość pamięci RAM nie mogą mieć wpływu na liczbę wymaganych licencji. Licencja musi uprawniać do uruchamiania serwerowego systemu operacyjnego (SSO) w środowisku fizycznym.
	2. Ważność licencji na serwer fizyczny i serwerowy system operacyjny maszyn wirtualnych nie jest ograniczona czasowo.
	3. Serwerowy system operacyjny (SSO) musi posiadać następujące, wbudowane cechy:
		1. Możliwość uruchomienia oprogramowania serwerowego firm trzecich dedykowanego na system Windows Serwer 2012R2 lub nowszy
		2. Możliwość wykorzystania co najmniej 2 logicznych procesorów oraz co najmniej 4 GB pamięci RAM w środowisku fizycznym.
		3. Możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności do 64TB przez każdy wirtualny serwerowy system operacyjny.
		4. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy.
		5. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy.
		6. Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.
		7. Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading.
		8. Wbudowane wsparcie instalacji i pracy na wolumenach, które:
6. pozwalają na zmianę rozmiaru w czasie pracy systemu,
7. umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,
8. umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów,
9. umożliwiają zdefiniowanie list kontroli dostępu (ACL).
	* 1. Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.
		2. Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez instytucję lub firmę upoważnioną do wydawania certyfikatu bezpieczeństwa danych. Za równoważny Zamawiający uzna certyfikat potwierdzający bezpieczeństwo danych.
		3. Możliwość uruchamiania aplikacji internetowych wykorzystujących technologię ASP.NET.
		4. Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.
		5. Graficzny interfejs użytkownika.
		6. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).
		7. Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.
		8. Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa.
		9. Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:
10. Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC,
11. Usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe) z możliwością wykorzystania następujących funkcji:
	1. Podłączenie SSO do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną,
	2. Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,
	3. Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza.
12. Zdalna dystrybucja oprogramowania na stacje robocze,
13. Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej,
14. Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego umożliwiające:
15. Dystrybucję certyfikatów poprzez http,
16. Konsolidację CA dla wielu lasów domen,
17. Automatyczne rejestrowanie certyfikatów pomiędzy różnymi lasami domen.
18. Szyfrowanie plików i folderów,
19. Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec),
20. Możliwość tworzenia systemów wysokiej dostępności (klastry typu failover) oraz rozłożenia obciążenia serwerów,
21. Serwis udostępniania stron WWW,
22. Wsparcie dla protokołu IP w wersji 6 (IPv6),
23. Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows, posiadanymi przez Zamawiającego,
24. Wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie do 1000 aktywnych środowisk wirtualnych systemów operacyjnych. Wirtualne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności.
	1. Możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet.
	2. Wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath).
	3. Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego.
	4. Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.
	5. Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF.
25. Oprogramowanie równoważne musi być kompatybilne i w sposób niezakłócony współdziałać ze sprzętem i oprogramowaniem funkcjonującym u Zamawiającego.
26. Oprogramowanie równoważne nie może zakłócić pracy środowiska systemowo-programowego Zamawiającego.
27. Oprogramowanie równoważne musi w pełni współpracować z systemami już eksploatowanymi u Zamawiającego.
28. Oprogramowanie równoważne musi zapewniać pełną, równoległą współpracę i pełną funkcjonalną zamienność produktu z produktami stosowanymi przez Zamawiającego.

# Pakiet produktów narzędziowych do zarządzania i monitorowania serwerów oraz zarządzania wirtualizacją serwerów dedykowany dla środowisk o wysokim stopniu wirtualizacji.

1. Przedmiotem zamówienia jest dostawa pakietu produktów narzędziowych do zarządzania i monitorowania serwerów oraz zarządzania wirtualizacją serwerów, dedykowany dla środowisk o wysokim stopniu wirtualizacji, w celu uzupełnienia stanu posiadanego oprogramowania.
2. Wskazane w opisie nazwy produktów odnoszą się do posiadanego i wykorzystywanego przez jednostki organizacyjne służb Statystyki Publicznej oprogramowania, a zachowanie parametrów określonych jako równoważne jest konieczne do zachowania kompatybilności i spójności środowiska. Zamawiający oczekuje ofert spełniających wymagania minimalne, nie gorsze w stosunku do minimalnych określonych poniżej.
3. Zamawiający posiada licencje:
	1. System Center 2012 R2 Datacenter Edition,
	2. System Center 2012 R2 Standard Edition.
4. Oprogramowanie musi być dostarczone w najwyższej (najnowszej) wersji, na moment złożenia oferty przez Wykonawcę.
5. Licencje muszą pozwalać na pobieranie nowych wersji oprogramowania zamawianego systemu w okresie trzech lat.
6. Dopuszcza się zaoferowanie produktów równoważnych do produktów wymienionych
w pkt 3.1)1).
7. Oferowany przez Wykonawcę produkt musi posiadać wszystkie funkcje zawarte w opisanych poniżej modułach:
8. System zarządzania infrastrukturą i oprogramowaniem,
9. System zarządzania komponentami,
10. System zarządzania środowiskami wirtualnym,
11. System tworzenia kopii zapasowych,
12. System automatyzacji zarządzania środowisk IT,
13. System zarządzania incydentami i problemami,
14. Ochrona antymalware.

|  |
| --- |
| **System zarządzania infrastrukturą i oprogramowaniem** |
| System zarządzania infrastrukturą i oprogramowaniem musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji. 1. Inwentaryzacja i zarządzanie zasobami:
	1. Inwentaryzacja zasobów serwera powinna się odbywać w określonych przez administratora systemu interwałach czasowych. System powinien mieć możliwość odrębnego planowania inwentaryzacji sprzętu i oprogramowania.
	2. Inwentaryzacja sprzętu powinna się odbywać przez pobieranie informacji z interfejsu WMI, komponent inwentaryzacyjny powinien mieć możliwość konfiguracji w celu ustalenia informacji, o jakich podzespołach będą przekazywane do systemu.
	3. Inwentaryzacja oprogramowania powinna skanować zasoby dyskowe przekazując dane o znalezionych plikach do systemu w celu identyfikacji oprogramowania oraz celów wyszukiwania i gromadzenia informacji o szczególnych typach plików (np. pliki multimedialne: wav, mp3, avi, xvid, itp…)
	4. System powinien posiadać własną bazę dostępnego na rynku komercyjnego oprogramowania, pozwalającą na identyfikację zainstalowanego i użytkowanego oprogramowania.
	5. System powinien dawać możliwość aktualizacji tej bazy przy pomocy konsoli administratora oraz automatycznie przez aktualizacje ze stron producenta.
	6. Informacje inwentaryzacyjne powinny być przesyłane przy pomocy plików różnicowych w celu ograniczenia ruchu z agenta do serwera.
2. Użytkowane oprogramowanie – pomiar wykorzystania
3. System powinien mieć możliwość zliczania uruchomionego programowania w celu śledzenia wykorzystania.
4. Reguły dotyczące monitorowanego oprogramowania powinny być tworzone automatycznie przez skanowanie oprogramowania uruchamianego.
5. System powinien dostarczać funkcje dystrybucji oprogramowania, dystrybucja i zarządzania aktualizacjami, instalacja/aktualizacja systemów operacyjnych.
6. System powinien umożliwiać dystrybucją oprogramowania w trybie wymaganym, opcjonalnym lub na prośbę użytkownika.
7. System powinien dawać możliwość integracji dostępnych zadań dystrybucji (pakietów instalacyjnych) z obsługą oprogramowania systemów Windows (dostępne do instalacji pakiety powinny się pojawiać w Panelu Sterowania w sekcji Dodaj/Usuń Programy, w części Dodaj Nowe Programy).
8. System powinien posiadać narzędzia pozwalające na przeskanowanie serwerów pod kątem zainstalowanych poprawek dla systemów operacyjnych Windows oraz dostarczać narzędzia dla innych producentów oprogramowania (ISVs) w celu przygotowania reguł skanujących i zestawów poprawek.
9. System powinien posiadać możliwość instalacji wielu poprawek jednocześnie bez konieczności restartu komputera w trakcie instalacji kolejnych poprawek.
10. System powinien udostępniać informacje o aktualizacjach systemów operacyjnych Windows dostępnych na stronach producenta (Windows Update) oraz informacje o postępie instalacji tych aktualizacji na serwerach (również w postaci raportów).
11. System powinien również umożliwiać skanowanie i inwentaryzację poprawek, które były już instalowane wcześniej niezależnie od źródła dystrybucji.
12. System powinien umożliwiać instalację lub aktualizację systemu operacyjnego ze zdefiniowanego wcześniej obrazu, wraz z przeniesieniem danych użytkownika (profil).
13. Przy przenoszeniu danych użytkownika, powinny one na czas migracji być składowane w specjalnym, chronionym (zaszyfrowanym) zasobie.
14. System powinien zawierać wszystkie narzędzia do sporządzenia, modyfikacji i dystrybucji obrazów na dowolny komputer, również taki, na którym nie ma żadnego systemu operacyjnego (bare metal).
15. System powinien być zintegrowany z oprogramowaniem antywirusowym i być zarządzany przy pomocy jednej wspólnej konsoli do zarządzania.
16. Definiowanie i sprawdzanie standardu serwera:
17. System powinien posiadać komponenty umożliwiające zdefiniowanie i okresowe sprawdzanie standardu serwera, standard ten powinien być określony zestawem reguł sprawdzających definiowanych z poziomu konsoli administracyjnej.
18. Reguły powinny sprawdzać następujące elementy systemy komputerowego:
19. stan usługi (Windows Service),
20. obecność poprawek (Hotfix),
21. WMI,
22. system plików,
23. Active Directory,
24. SQL (query),
25. IIS Metabase.
26. Dla reguł sprawdzających system powinien dawać możliwość wprowadzenia wartości poprawnej, która byłaby wymuszana w przypadku odstępstwa lub wygenerowania alertu administracyjnego w sytuacji, kiedy naprawa nie jest możliwa.
27. Raportowanie, prezentacja danych:
	1. System powinien posiadać komponent raportujący oparty o technologie webową (wydzielony portal z raportami) i/lub wykorzystujący mechanizmy raportujące dostarczane wraz z silnikami bazodanowymi, np. SQL Reporting Services.
	2. System powinien posiadać predefiniowane raport w następujących kategoriach:
28. sprzęt (inwentaryzacja),
29. oprogramowanie (inwentaryzacja),
30. oprogramowanie (wykorzystanie),
31. oprogramowanie (aktualizacje, w tym system operacyjny).
	1. System powinien umożliwiać budowanie stron z raportami w postaci tablic (dashboard), na których może znajdować się więcej niż jeden raport.
	2. System powinien posiadać konsolę administratora, w postaci programu do zainstalowania na stacjach roboczych, obsługującą wszystkie funkcje systemu.
	3. Konsola powinna zapewnić dostęp do wszystkich opcji konfiguracyjnych systemu (poza opcjami dostępnymi w procesie instalacji i wstępnej konfiguracji), w tym:
32. konfigurację granic systemu zarządzania,
33. konfigurację komponentów systemu zarządzania,
34. konfigurację metod wykrywania serwerów, użytkowników i grup,
35. konfigurację metod instalacji klienta,
36. konfiguracje komponentów klienta,
37. grupowanie serwerów (statyczne, dynamiczne na podstawie zinwentaryzowanych parametrów),
38. konfiguracje zadań dystrybucji, pakietów instalacyjnych, itp…,
39. konfigurację reguł wykorzystania oprogramowania,
40. konfigurację zapytań (query) do bazy danych systemu,
41. konfiguracje raportów,
42. podgląd zdarzeń oraz zdrowia komponentów systemu.
	1. Analiza działania systemu, logi, komponenty
43. Konsola systemu powinna dawać dostęp do podstawowych logów obrazujących pracę poszczególnych komponentów, wraz z oznaczaniem stanu (OK, Warning, Error) w przypadku znalezienia zdarzeń wskazujących na problemy.
44. Konsola systemu powinna umożliwiać podgląd na stan poszczególnych usług wraz z podstawowymi informacjami o stanie usługi, np. ilość wykorzystywanego miejsca na dysku twardym.
 |
| **System zarządzania komponentami** |
| System zarządzania komponentami musi udostępniać funkcje pozwalające na budowę bezpiecznych i skalowalnych mechanizmów zarządzania komponentami IT spełniając następujące wymagania: 1. Architektura
2. System zarządzania komponentami powinien składać się z:
3. Serwera Zarządzającego, który jest punktem centralnym do zarządzanie grupą (pulą) serwerów i komunikowania się z bazą danych. Po otwarciu konsoli serwera możliwe jest podłączenie się do grupy zarządzającej. W zależności od wielkości środowiska komputerowego, grupa zarządzania może zawierać jeden lub wiele serwerów połączonych w pule zasobów.
4. Bazy Operacyjnej przechowującej informacje o zarządzanych elementach, która zawiera wszystkie dane konfiguracyjne dla zarządzanej grupy serwerów i przechowuje wszystkie dane związane z monitorowaniem. Baza Operacyjna zachowuje dane krótkoterminowe, domyślnie 7 dni.
5. Baza Hurtowej przechowującej dane do analiz historycznych, definiuje granicę czasową do retencji danych historycznych.
6. System musi mieć możliwość tworzenia konfiguracji wysokiej dostępności (klaster typu fail-over).
7. System musi pozwalać na zarządzanie platformami wirtualizacyjnymi, co najmniej trzech różnych dostawców.
8. Serwery zarządzające muszą mieć możliwość publikowania informacji o uruchomionych komponentach w usługach katalogowych, informacje te powinny być odstępne dla klientów systemu w celu automatycznej konfiguracji.
9. Możliwość budowania struktury wielopoziomowej (tiers) w celu separacji pewnych grup komputerów/usług.
10. System uprawnień musi być oparty o role (role based security), użytkownicy i grupy użytkowników w poszczególnych rolach powinny być pobierane z usług katalogowych.
11. Możliwość definiowania użytkowników do wykonywania poszczególnych zadań na klientach i serwerze zarządzającym, w tym zdefiniowany użytkownik domyślny.
12. Uwierzytelnianie klientów na serwerze zarządzającym przy pomocy certyfikatów w standardzie X.509, z możliwością odrzucania połączeń od klientów niezaakceptowanych.
13. Kanał komunikacyjny pomiędzy klientami a serwerem zarządzającym powinien być szyfrowany.
14. Możliwość budowania systemu w oparciu o łącza publiczne - Internet (bez konieczności wydzielania kanałów VPN).
15. Wsparcie dla protokołu IPv6.
16. System powinien udostępniać funkcje autodiagnostyczne, w tym: monitorowanie stanu klientów, możliwość automatycznego lub administracyjnego restartu klienta, możliwość reinstalacji klienta,
17. Pulpit nawigacyjny HTML5.
18. Audyt zdarzeń bezpieczeństwa

System musi udostępniać komponenty i funkcje pozwalające na zbudowanie systemu zbierającego zdarzenia związane z bezpieczeństwem monitorowanych systemów i gwarantować: * 1. przekazywanie zdarzeń z podległych klientów w czasie „prawie” rzeczywistym (dopuszczalne opóźnienia mogą pochodzić z medium transportowego – sieć, oraz komponentów zapisujących i odczytujących),
	2. niskie obciążenie sieci poprzez schematyzację parametrów zdarzeń przed wysłaniem, definicja schematu powinna być definiowana w pliku XML z możliwością dodawania i modyfikacji,
	3. obsługę co najmniej 2500 zdarzeń/sek w trybie ciągłym i 100000 zdarzeń/sek w trybie „burst” – chwilowy wzrost ilości zdarzeń, jeden kolektor zdarzeń powinien obsługiwać, co najmniej 100 kontrolerów domen (lub innych systemów autentykacji i usług katalogowych) lub 1000 serwerów.
1. Konfiguracja i monitorowanie
2. System musi umożliwiać zbudowanie jednorodnego środowiska monitorującego, korzystając z takich samych zasad do monitorowania różnych komponentów, a w tym:
3. monitorowane obiekty powinny być grupowane (klasy) w oparciu o atrybuty, które można wykryć na klientach systemu w celu autokonfiguracji systemu. Powinny być wykrywane - co najmniej, atrybuty pobierane z:
	* 1. rejestru,
		2. WMI,
		3. OLEDB,
		4. LDAP,
		5. skrypty (uruchamiane w celu wykrycia atrybutów obiektu).
4. W definicjach klas powinny być również odzwierciedlone zależności pomiędzy nimi.
5. Na podstawie wykrytych atrybutów system powinien dokonywać autokonfiguracji klientów, przez wysłanie odpowiadającego wykrytym obiektom zestawu monitorów, reguł, skryptów, zadań, itp…
6. Wszystkie klasy obiektów, monitory, reguły, skrypty, zadania, itp... elementy służące konfiguracji systemu muszą być grupowane i dostarczane w postaci zestawów monitorujących, system powinien posiadać w standardzie zestawy monitorujące, co najmniej dla:
7. Windows Server 2012,
8. Windows Server 2012 R2,
9. Windows Server 2016,
10. Windows Server 2019,
11. Active Directory,
12. Exchange,
13. Microsoft SharePoint,
14. Microsoft SharePoint Services,
15. Microsoft SharePoint Foundation,
16. SQL,
17. Information Worker (Office, IExplorer, Outlook, itp…),
18. IIS,
19. Linux/Unix (Red Hat Enterprise Linux, SUSE Linux Enterprise Server 15, Linux RPM (Oracle i Centos), Linux DPKG (Debian 9 i Ubuntu 18), Solaris, AIX, openSUSE przestępny 15, SUSE 12 PPC),
20. Usług i zasobów infrastruktury zlokalizowanej w Chmurze Publicznej np. Azure/AWS/Google,
21. Apache Tomcat 7, Apache Tomcat 8, Apache Tomcat 9,
22. Red Hat JBoss 4, 5, 6, 7, serwera aplikacji Wildfly 8/9/10/11/12/13/14, JBoss JBoss JBoss Red Hat JBoss EAP 6, Red Hat JBoss EAP 7,
23. Oracle WebLogic 10gR3, Oracle WebLogic 11, WebLogic 12cR1, WebLogic 12cR2.
24. System powinien posiadać możliwość monitorowania za pomocą agenta lub bez niego.
25. System musi pozwalać na wykrycie oraz monitorowanie urządzeń sieciowych (routery, przełączniki sieciowe, itp.) za pomocą SNMP v1, v2c oraz v3. System monitorowania w szczególności powinien mieć możliwość zbierania następujących informacji:
26. interfejsy sieciowe,
27. porty,
28. sieci wirtualne (VLAN),
29. grupy Hot Standby Router Protocol (HSRP).
30. System zarządzania musi mieć możliwość czerpania informacji z następujących źródeł danych:
31. SNMP (trap, probe),
32. WMI Performance Counters,
33. Log Files (text, text CSV),
34. Windows Events (logi systemowe),
35. Windows Services,
36. Windows Performance Counters (perflib),
37. WMI Events,
38. Scripts (wyniki skryptów, np.: WSH, JSH),
39. Unix/Linux Service,
40. Unix/Linux Log.
41. Na podstawie uzyskanych informacji monitor powinien aktualizować status komponentu, powinna być możliwość łączenia i agregowania statusu wielu monitorów.
42. Tworzenie reguł
43. W systemie zarządzania powinna mieć możliwość czerpania informacji z następujących źródeł danych:
	1. Event based (text, text CSV, NT Event Log, SNMP Event, SNMP Trap, syslog, WMI Event),
	2. Performance based (SNMP performance, WMI performance, Windows performance),
	3. Probe based (scripts: event, performance).
44. System musi umożliwiać przekazywanie zebranych przez reguły informacji do bazy danych w celu ich późniejszego wykorzystania w systemie, np. raporty dotyczące wydajności komponentów, alarmy mówiące o przekroczeniu wartości progowych czy wystąpieniu niepożądanego zdarzenia.
45. Reguły zbierające dane wydajnościowe muszą mieć możliwość ustawiania tolerancji na zmiany, w celu ograniczenia ilości nieistotnych danych przechowywanych w systemie bazodanowym. Tolerancja powinna mieć, co najmniej dwie możliwości:
	1. na ilość takich samych próbek o takiej samej wartości
	2. na procentową zmianę od ostatniej wartości próbki.
46. Monitory sprawdzające dane wydajnościowe w celu wyszukiwania wartości progowych muszą mieć możliwość – oprócz ustawiania progów statycznych, „uczenia” się monitorowanego parametru w zakresie przebiegu bazowego „baseline” w zadanym okresie czasu.
47. System musi umożliwiać blokowanie modyfikacji zestawów monitorujących, oraz definiowanie wyjątków na grupy komponentów lub konkretne komponenty w celu ich odmiennej konfiguracji.
48. System powinien posiadać narzędzia do konfiguracji monitorów dla aplikacji i usług, w tym:
	1. ASP .Net Application,
	2. ASP .Net Web Service,
	3. OLE DB,
	4. TCP Port,
	5. Web Application,
	6. Windows Service,
	7. Unix/Linux Service,
	8. Process Monitoring.

Narzędzia te powinny pozwalać na zbudowanie zestawu predefiniowanych monitorów dla wybranej aplikacji i przyporządkowanie ich do wykrytej/działającej aplikacji 1. System musi posiadać narzędzia do budowania modeli aplikacji rozproszonych (składających się z wielu wykrytych obiektów), pozwalając na agregację stanu aplikacji oraz zagnieżdżanie aplikacji.
2. Z każdym elementem monitorującym (monitor, reguła, alarm, itp…) powinna być skojarzona baza wiedzy, zawierająca informacje o potencjalnych przyczynach problemów oraz możliwościach jego rozwiązania (w tym możliwość uruchamiania zadań diagnostycznych z poziomu).
3. System musi zbierać informacje udostępniane przez systemy operacyjne Windows o przyczynach krytycznych błędów (crash) udostępnianych potem do celów analitycznych.
4. System musi umożliwiać budowanie obiektów SLO (Service Level Object) służących przedstawianiu informacji dotyczących zdefiniowanych poziomów SLA (Service Level Agreement) przynajmniej dla monitora (dostępność) i licznika wydajności (z agregacją dla wartości – min, max, avg).
5. Przechowywanie i dostęp do informacji
	1. Wszystkie informacje operacyjne (zdarzenia, liczniki wydajności, informacje o obiektach, alarmy, itp…) powinny być przechowywane w bazie danych operacyjnych.
	2. System musi mieć co najmniej jedną bazę danych z przeznaczeniem na hurtownię danych do celów historycznych i raportowych. Zdarzenia powinny być umieszczane w obu bazach jednocześnie, aby raporty mogłyby być generowane w oparciu o najświeższe dane.
	3. System musi mieć osobną bazę danych, do której będą zbierane informacje na temat zdarzeń security z możliwością ustawienia innych uprawnień dostępu do danych tam zawartych (tylko audytorzy).
	4. System powinien mieć zintegrowany silnik raportujący niewymagający do tworzenia raportów używania produktów firm trzecich. Produkty takie mogą być wykorzystanie w celu rozszerzenia tej funkcjonalności.
	5. System powinien mieć możliwość generowania raportów na życzenie oraz tworzenie zadań zaplanowanych.
	6. System powinien umożliwiać eksport stworzonych raportów przynajmniej do następujących formatów:
		1. XML,
		2. CSV,
		3. TIFF,
		4. PDF,
		5. XLS,
		6. Web archive.
6. Konsola systemu zarządzania
7. Konsola systemu musi umożliwiać pełny zdalny dostęp do serwerów zarządzających dając dostęp do zasobów zgodnych z rolą użytkownika korzystającego z konsoli.
8. System powinien udostępniać dwa rodzaje konsoli:
9. w postaci programu do zainstalowania na stacjach roboczych, obsługującą wszystkie funkcje systemu (konsola zdalna),
10. w postaci web’owej dla dostępu do podstawowych komponentów monitorujących z dowolnej stacji roboczej (konsola webowa).
11. Konsola zdalna powinna umożliwiać definiowanie każdemu użytkownikowi własnych widoków, co najmniej w kategoriach:
	1. Alerts,
	2. Events,
	3. State,
	4. Performance,
	5. Diagram,
	6. Task Status,
	7. Web Page (dla użytkowników, którzy potrzebują podglądu tylko wybranych elementów systemu).
12. Konsola musi umożliwiać budowanie widoków tablicowych (dashboard) w celu prezentacji różnych widoków na tym samym ekranie.
13. Widoki powinny mieć możliwość filtrowania informacji, jakie się na nich znajdą (po typie, ważności, typach obiektów, itp…), sortowania oraz grupowania podobnych informacji, wraz z możliwością definiowania kolumn, jakie mają się znaleźć na widokach „kolumnowych”.
14. Z każdym widokiem (obiektem w tym widoku) powinno być skojarzone menu kontekstowe, z najczęstszymi operacjami dla danego typu widoku/obiektu.
15. Konsola musi zapewnić dostęp do wszystkich opcji konfiguracyjnych systemu (poza opcjami dostępnymi w procesie instalacji i wstępnej konfiguracji), w tym:
	1. opcji definiowania ról użytkowników,
	2. opcji definiowania widoków,
	3. opcji definiowania i generowania raportów,
	4. opcji definiowania powiadomień,
	5. opcji tworzenia, konfiguracji i modyfikacji zestawów monitorujących,
	6. opcji instalacji/deinstalacji klienta.
16. Konsola musi pozwalać na pokazywanie obiektów SLO (Service Level Object) i raportów SLA (Service Level Agreement) bez potrzeby posiadania konsoli i dostepu do samego systemu monitorującego, na potrzeby użytkowników biznesowych (właścicieli procesu biznesowego).
17. Wymagania dodatkowe

System musi dostarczać API lub inny system (web service, connector) z publicznie dostępną dokumentacją pozwalający m.in. na: 1. budowanie konektorów do innych systemów, np. help-desk w celu przekazywania zdarzeń czy alarmów (dwukierunkowo),
2. wykonywanie operacji w systemie z poziomu linii poleceń,
3. podłączenie rozwiązań firm trzecich pozwalających na monitorowanie w jednolity sposób systemów informatycznych niewspieranych natywnie przez system zarządzania,
4. podłączenie do aplikacji biurowych pozwalające na integrację statycznych modeli (np. diagramów Visio) z monitorowanymi obiektami, pozwalające na wyświetlanie ich stanu na diagramie.
 |
| **System zarządzania środowiskami wirtualnym** |
| System zarządzania środowiskami wirtualnymi musi posiadać następujące cechy: 1. Architektura
	1. System zarządzania środowiskiem wirtualnym powinien składać się z:
		1. serwera zarządzającego,
		2. relacyjnej bazy danych przechowującej informacje o zarządzanych elementach,
		3. konsoli, instalowanej na komputerach operatorów,
		4. portalu self-service (konsoli webowej) dla operatorów „departamentowych”,
		5. biblioteki, przechowującej komponenty niezbędne do budowy maszyn wirtualnych,
		6. agenta instalowanego na zarządzanych hostach wirtualizacyjnych,
		7. „konektora” do systemu monitorującego pracę hostów i maszyn wirtualnych.
	2. System musi mieć możliwość tworzenia konfiguracji wysokiej dostępności (klaster typu fail-over).
	3. System musi pozwalać na zarządzanie platformami wirtualizacyjnymi co najmniej trzech różnych dostawców.
2. Interfejs użytkownika
	1. Konsola musi umożliwiać wykonywanie codziennych zadań związanych z zarządzaniem maszynami wirtualnymi w sposób jak najbardziej intuicyjny.
	2. Konsola musi umożliwiać grupowanie hostów i nadawanie uprawnień poszczególnym operatorom do grup hostów.
	3. Widoki hostów i maszyn wirtualnych powinny mieć możliwość zakładania filtrów, pokazując tylko odfiltrowane elementy, np.
	4. maszyny wyłączone, maszyny z systemem operacyjnym X, itp...
	5. Widok szczegółowy elementu w przypadku maszyny wirtualnej musi pokazywać stan, ilość alokowanej pamięci i dysku twardego, system operacyjny, platformę wirtualizacyjną, stan ostatniego zadania, oraz wykres utylizacji procesora i podgląd na pulpit.
	6. Konsola musi posiadać odrębny widok z historią wszystkich zadań oraz statusem zakończenia poszczególnych etapów i całych zadań.
3. Scenariusze i zadania
	1. Tworzenie maszyn wirtualnych – system musi umożliwiać stworzenie maszyny wirtualnej w co najmniej dwóch trybach:
		1. Ad hoc – gdzie wszystkie elementy są wybierane przez operatora podczas tworzenia maszyny,
		2. Nadzorowany – gdzie operator tworzy maszynę korzystając z gotowego wzorca (template), a wzorzec składa się z przynajmniej 3-ech elementów składowych:
4. profilu sprzętowego,
5. profilu systemu operacyjnego,
6. przygotowanych dysków twardych,
	1. Predefiniowane elementy muszą być przechowywane w bibliotece systemu zarządzania.
	2. System musi umożliwiać przenoszenie maszyny wirtualnej pomiędzy zarządzanymi hostami:
	3. w trybie migracji „on-line” – bez przerywania pracy,
	4. w trybie migracji „off-line – z zapisem stanu maszyny
	5. System musi umożliwiać automatyczne, równomierne rozłożenie obciążenia pomiędzy zarządzanymi hostami.
	6. System musi umożliwiać wyłączenie hosta, gdy jego zasoby nie są konieczne do pracy, w celu oszczędności energii. System powinien również umożliwiać ponowne włączenie takiego hosta.
	7. System musi umożliwiać przełączenie wybranego hosta w tryb „maintenance” w przypadku wystąpienia awarii lub w celu przeprowadzenia planowanych prac serwisowych. Uruchomienie tego trybu musi skutkować migracją maszyn na inne hosty lub zapisaniem ich stanu.
	8. System musi posiadać możliwość konwersji maszyny fizycznej do wirtualnej.
	9. System misi posiadać (bez potrzeby instalowania dodatkowego oprogramowania) - możliwość wykrycia maszyny fizycznej w sieci i instalacje na niej systemu operacyjnego wraz z platformą do wirtualizacji.
7. Wymagania dodatkowe
8. System musi informować operatora o potrzebie migracji maszyn, jeśli wystąpią nieprawidłowe zdarzenia na hoście lub w innych maszynach wirtualnych mające wpływ na ich pracę, np. awarie sprzętu, nadmierna utylizacja współdzielonych zasobów przez jedną maszynę.
9. System musi dawać operatorowi możliwość implementacji w/w migracji w sposób automatyczne bez potrzeby każdorazowego potwierdzania.
10. System musi kreować raporty z działania zarządzanego środowiska, w tym:
	1. utylizacja poszczególnych hostów,
	2. trend w utylizacji hostów,
	3. alokacja zasobów na centra kosztów,
	4. utylizacja poszczególnych maszyn wirtualnych,
	5. komputery-kandydaci do wirtualizacji.
11. System musi umożliwiać skorzystanie z szablonów:
	1. wirtualnych maszyn,
	2. usług,
	3. oraz profili dla:
	4. aplikacji,
	5. serwera SQL,
	6. hosta,
	7. sprzętu,
	8. systemu operacyjnego gościa.
12. System musi umożliwiać tworzenie chmur prywatnych na podstawie dostępnych zasobów (hosty, sieci, przestrzeń dyskowa, biblioteki zasobów).
13. System musi posiadać możliwość przygotowania i instalacji zwirtualizowanej aplikacji serwerowej.
14. System musi pozwalać na skalowalność wirtualnego środowiska aplikacji (poprzez automatyczne dodanie wirtualnej maszyny z aplikacją).
 |
| **System tworzenia kopii zapasowych** |
| System tworzenia i odtwarzania kopii zapasowych danych (backup) musi spełniać następujące wymagania: 1. Architektura:
	1. System musi składać się z serwera zarządzającego kopiami zapasowymi i agentami kopii zapasowych.
	2. System musi posiadać agentów kopii zapasowych instalowanych na komputerach zdalnych.
	3. System musi posiadać konsolę administracyjną instalowaną lokalnie na komputerach użytkowników zarządzających systemem.
	4. System musi posiadać własną bazę danych (niewymagającą dodatkowych zakupów).
2. Wykonywanie kopii zapasowych:
	1. System kopii zapasowych musi wykorzystywać mechanizm migawkowych kopii – VSS (Volume ShadowCopy Service).
	2. System kopii zapasowych musi posiadać możliwości zapisu danych na:
		1. na puli magazynowej złożonej z dysków twardych,
		2. na napędach I bibliotekach taśmowych,
		3. podłączonych zdalnie zasobach chmurowych.
	3. System kopii zapasowych musi umożliwiać zdefiniowanie ochrony zasobów krótkoterminowej, długoterminowej i online (chmura). Oznacza to, iż krótkookresowe kopie mogą być tworzone w puli magazynowej, a długookresowe na napędach i bibliotekach taśmowych.
	4. System kopii zapasowych powinien wykonywać zapis na napędach dyskowych i zasobach chmurowych w postaci repliki danych produkcyjnych (pierwszy backup) a następnie odkładanie tylko zmienionych partii danych.
	5. System kopii zapasowych powinien wykonywać zapis na napędach i bibliotekach taśmowych w postaci pełnego backupu na chwilę wykonywania zadania.
	6. System kopii zapasowych musi umożliwiać synchronizację przechowywanych kopii zapasowych (kopie różnicowe) z produkcyjnymi transakcyjnymi bazami danych na poziomie poniżej 30 minut. Kopie te muszą być tworzone w ciągu godzin pracy, w niezauważalny dla użytkowników końcowych sposób.
	7. System kopii zapasowych musi umożliwiać odtworzenie dowolnego 30 minutowego kwantu czasu dla krytycznych systemów, takich jak bazy danych.
	8. System kopii zapasowych musi umożliwiać rozwiązanie automatycznego przenoszenia chronionych danych do zdalnej lokalizacji (nadrzędny serwer kopii zapasowych), wykorzystując przy tym mechanizm regulacji przepustowości.
	9. System powinien umożliwiać skonfigurowanie okresu przechowywania danych (retention) dla poszczególnych typów ochrony:
3. Krótkoterminowe: Pule dyskowe – do 448 dni,
4. Online: Zasoby chmurowe – do 3360 dni,
5. Krótkoterminowe: Taśmy – do 12 tygodni iv. Długoterminowe: Taśmy – do 99 lat.
6. Odzyskiwanie danych:
7. System kopii zapasowych musi umożliwiać odzyskanie chronionych zasobów plikowych użytkownika na jego komputerze z poziomu zakładki „Poprzednie wersje”.
8. System kopii zapasowych musi umożliwiać odtworzenie danych do:
	1. lokalizacji oryginalnej,
	2. lokalizacji alternatywnej,
	3. w przypadku nadrzędnego serwera kopii zapasowych (w centrum zapasowym) do podrzędnego serwera kopii zapasowych.
9. Agent kopii zapasowej
10. Agent powinien posiadać możliwość współpracy z komponentami VSC.
11. Agent powinien posiadać możliwość sterowania pasmem a w szczególności określenia godzin „biznesowych” oraz wykorzystywanego pasma w i poza godzinami „biznesowymi”.
12. Agent powinien rozpoznawać podstawowe aplikacje i systemy wykorzystywane w środowisku zamawiającego i automatycznie dodawać wszystkie wymagane pliki do puli chronionej, w tym:
	1. System operacyjny Windows (w tym pliki, system state i BMR).
	2. Maszyny wirtualne na platformie Hyper-V.
	3. Bazy danych MS SQL iv. Sharepoint v. Exchange.
13. Konsola administracyjna:
14. Konsola powinna umożliwiać tworzenie określonych harmonogramów wykonywania kopii zapasowych na chronionych agentach.
15. Konsola powinna umożliwiać grupowanie chronionych zasobów ze względu na typy chronionych zasobów.
16. Zarządzanie agentami i zadaniami kopii zapasowych powinno być możliwe również za pomocą linii poleceń.
17. Konsola powinna posiadać mechanizm kontrolowania wykonywanych zadań kopii zapasowych.
18. Konsola powinna posiadać mechanizm notyfikacji administratorów odnośnie zdarzeń w systemie kopii zapasowych.
19. Konsola powinna posiadać wbudowany system raportujący (m.in. raporty dotyczące zużycia puli magazynowej, wykonania kopii zapasowych, itp.).
 |
| **System automatyzacji zarządzania środowisk IT** |
| System automatyzacji zarządzania środowisk IT musi udostępniać środowisko standaryzujące i automatyzujące zarządzanie procesami w systemach IT na bazie najlepszych praktyk. 1. Architektura:
	1. System musi posiadać graficzną konsolę dla administratorów (autorów) pozwalającą w łatwy sposób (bez znajomości języków programowania) tworzenie przebiegów procesów (runbooks) przy pomocy gotowych elementów aktywności.
	2. System musi posiadać tester przebiegów pozwalający na sprawdzenie poprawności wykonywania stworzonego przez administratora (autora) pokazując informacje o wykonaniu poszczególnych kroków, informacje wchodzące i wychodzące z poszczególnych kroków, możliwość ustawiania pułapek (breakpoints) oraz wykonywania krok po kroku.
	3. System musi posiadać serwer zarządzający i własną bazę danych, w której przechowywane są informacje o stworzonych przebiegach procesów oraz ich stanie.
	4. System musi posiadać serwery wykonawcze, które realizują przebiegi procesów zdefiniowane przez administratorów (autorów).
	5. System powinien posiadać konsolę webową pozwalającą na podgląd zdefiniowanych przebiegów procesów, ich stanu, informacji historycznych o wykonanych przebiegach oraz pozwalająca na uruchamianie przebiegów procesów na żądanie.
	6. System powinien posiadać własną bazę danych (niewymagającą dodatkowych zakupów).
2. Tworzenie przebiegów:
3. Do tworzenia przebiegów procesów powinny być gotowe zestawy aktywności, które przy pomocy graficznego środowiska pracy (konsola administratora) autor może łączyć w gotowe przebiegi.
4. Zestawy aktywności powinny być dostarczane do systemu w postaci pakietów, zawierających gotowe przygotowane aktywności dla zadanego obszaru.
5. System powinien posiadać podstawowy (wbudowany) zestaw aktywności w następujących obszarach:
	* 1. System:
6. Run Program,
7. Run .Net Script,
8. End Process,
9. Start/Stop Service,
10. Restart System,
11. Save Event Log,
12. Query WMI,
13. Run SSH Command,
14. Get SNMP Variable,
15. Monitor SNMP Trap,
16. Send SNMP Trap,
17. Set SNMP Variable.
	* 1. Planowanie:
			1. Monitor Date/Time,
			2. Check Schedule.
		2. Monitorowanie:
18. Monitor Event Log,
19. Monitor Service,
20. Get Service Status,
21. Monitor Process,
22. Get Process Status,
23. Monitor Computer/IP Status,
24. Monitor Disk Space,
25. Get Disk Space Status,
26. Monitor Internet Application,
27. Get Internet Application Status,
28. Monitor WMI.
	* 1. Zarządzanie plikami:
29. Compress File,
30. Copy File,
31. Create Folder,
32. Decompress File,
33. Delete File,
34. Delete Folder,
35. Get File Status,
36. Monitor File,
37. Monitor Folder,
38. Move File,
39. Move Folder,
40. PGP Decrypt File,
41. PGP Encrypt File,
42. Print File,
43. Rename File.
	* 1. E-mail:
44. Send E-mail.
	* 1. Powiadomienia:
45. Send Event Log Message,
46. Send Syslog Message,
47. Send Platform Event.
	* 1. Narzędzia:
48. Apply XSLT,
49. Query XML,
50. Map Published Data,
51. Compare Values,
52. Write Web Page,
53. Read Text Log,
54. Write to Database,
55. Query Database,
56. Monitor Counter,
57. Get Counter Value,
58. Modify Counter,
59. Invoke Web Services,
60. Format Date/Time,
61. Generate Random Text,
62. Map Network Path,
63. Disconnect Network Path,
64. Get Dial-up Status,
65. Connect/Disconnect Dial-up.
	* 1. Zarządzanie plikami tekstowymi:
66. Append Line,
67. Delete Line,
68. Find Text,
69. Get Lines,
70. Insert Line,
71. Read Line.
	* 1. Kontrola przepływów (runbooks):
72. Invoke Runbook,
73. Initialize Data,
74. Junction,
75. Return Data.
76. System powinien posiadać również inne zestawy aktywności, które mogą być zaimportowane na życzenie administratora (autora) w celu zarządzania procesami na innych systemach posiadanych przez zamawiającego, w tym:
77. Active Directory,
78. Exchange Admin,
79. Exchange Users iv. FTP Integration,
80. HP iLO and OA,
81. HP Operations Manager,
82. HP Service Manager,
83. IBM Tivoli Netcool/OMNIbus,
84. Representational State Transfer (REST),
85. Sharepoint,
86. Microsoft Azure,
87. VMware vSphere,
88. System Center.
89. Serwer zarządzający i baza danych:
90. Serwer zarządzający powinien organizować jednoczesny dostęp konsoli graficznych administratorów i zapewniać funkcje Check- In/Check-Out dla poszczególnych przebiegów uniemożliwiając jednoczesne zmiany tego samego przebiegu przez dwóch użytkowników.
91. Serwer zarządzający powinien zapewniać dostęp - na zdefiniowanym przez autora poziomie, dla poszczególnych przebiegów oraz zestawów przebiegów (całe katalogi).
92. Baza danych systemu powinna przechowywać:
	1. Definicje przebiegów procesów,
	2. Stan uruchomionych przebiegów,
	3. Informacje statusowe (logs),
	4. Dane konfiguracyjne systemu.
 |
| **System zarządzania incydentami i problemami** |
| System zarządzania incydentami i problemami musi zapewniać zintegrowane środowisko pozwalające na uruchomienie usług wsparcia (service-desk) u zamawiającego.1. Architektura:
2. System musi posiadać serwer zarządzający odpowiedzialny za wykonywanie wszystkich zadań związanych z obsługą incydentów, problemów, zmian, zleceń, użytkowników, itp… zapewniając jednocześnie wymuszenie odpowiednich uprawnień.
3. System musi posiadać zintegrowany komponent CMDB (Configuration Management Database).
4. System musi posiadać zintegrowany moduł bazy wiedzy (Knowledge Management).
5. System musi posiadać graficzną konsolę użytkownika instalowana lokalnie na komputerach pracowników wsparcia.
6. System musi posiadać komponent hurtowni danych, odpowiedzialny za agregację i przechowywanie danych historycznych i przygotowywanie raportów.
7. System musi posiadać własną bazę danych (niewymagającą dodatkowych zakupów).
8. System musi posiadać konsolę webową umożliwiającą pracownikom zgłaszanie incydentów/problemów technicznych oraz zapotrzebowania na zasoby IT.
9. Procesy wsparcia:
10. System musi posiadać przygotowanie i dostępne po instalacji następujące procesy:
	1. Zarządzanie incydentami,
	2. Zarządzanie problemami,
	3. Zarządzanie zmianą.
11. W zakresie zarządzania incydentami i problemami system powinien posiadać:
	1. Przygotowane formatki do wprowadzania incydentów przez pracowników wsparcia, formatka powinna umożliwiać wprowadzenie, co najmniej następujących danych:
12. Narażony użytkownik,
13. Alternatywna metoda kontaktu,
14. Tytuł,
15. Opis,
16. Kategoria,
17. Pilność,
18. Wpływ,
19. Źródło,
20. Grupa pomocy technicznej,
21. Przypisany,
22. Podstawowy właściciel,
23. Uwzględnione usługi,
24. Narażone elementy,
25. Dziennik akcji (komentarz).
26. Komponent
27. Baza danych CMDB powinna mieć domyślnie skonfigurowane podstawowe klasy obiektów wraz z atrybutami i relacje pomiędzy nimi, w tym:
28. Użytkownik:
29. Komputer
30. System musi posiadać gotowe konektory do innych skojarzonych systemów pozwalające na automatyczną i planowana aktualizację odpowiednich rekordów w CMDB, a w szczególności:
31. Konektor do systemu zarządzania infrastrukturą i oprogramowaniem,
32. Konektor do systemu zarządzania komponentami,
33. Konektor do systemu zarządzania środowiskami wirtualnym,
34. Konektor do systemu automatyzacji zarządzania środowisk IT,
35. Konektor do usługi katalogowej Active Directory.
36. System musi mieć postać zintegrowanej platformy pozwalającej poprzez wbudowane i definiowane mechanizmy w ramach przyjętej metodyki (np. MOF czy ITIL) na zarządzanie incydentami i problemami oraz zarządzanie zmianą.
37. System powinien posiadać bazę wiedzy (CMDB) automatycznie zasilaną z takich systemów jak: usługa katalogowa, system monitorujący, system do zarządzania desktopami.
38. System musi udostępniać narzędzia efektywnego zarządzania dostępnością usług, umożliwiających dostarczenie użytkownikom systemów SLA na wymaganym poziomie.
39. System, poprzez integrację z systemami zarządzania i monitorowania musi zapewniać:
	1. Optymalizację procesów i ich prawidłową realizację poprzez predefiniowane scenariusze, zgodne z najlepszymi praktykami i założoną metodyką,
	2. Redukcję czasu rozwiązywania problemów z działaniem systemów poprzez zapewnienie dotarcia właściwej, zagregowanej informacji do odpowiedniego poziomu linii wsparcia,
	3. Automatyczne generowanie opisu problemów na bazie alarmów i kojarzenie zdarzeń w różnych komponentach systemu,
	4. Wspomaganie procesów podejmowania decyzji poprzez integrację informacji i logikę ich powiązania,
	5. Planowanie działań prewencyjnych poprzez kolekcjonowanie informacji o zachowaniach systemu w przypadku incydentów,
	6. Raportowanie pozwalające na analizy w zakresie usprawnień systemu oraz usprawnień procesów ich opieki serwisowej,
	7. Tworzenie baz wiedzy na temat rozwiązywania problemów,
	8. Automatyzację działań w przypadku znanych i opisanych problemów.
	9. Wykrywanie odchyleń od założonych standardów ustalonych dla systemu.
 |
| **Ochrona antymalware** |
| Oprogramowanie antymalware musi spełniać następujące wymagania: 1. Ochrona przed zagrożeniami typu wirusy, robaki, Trojany, rootkity, ataki typu phishing czy exploity zero-day.
2. Centralne zarządzanie ochroną serwerów poprzez konsolę System zarządzania infrastrukturą i oprogramowaniem.
3. Centralne zarządzanie politykami ochrony.
4. Automatyzacja wdrożenia i wymiany dotychczasowych agentów ochrony.
5. Mechanizmy wspomagające masową instalację.
6. Pakiet ma wykorzystywać platformę skanowania, dzięki której dostawcy zabezpieczeń stosować mogą technologię „minifiltrów”, skanujących w czasie rzeczywistym w poszukiwaniu złośliwego oprogramowania. Dzięki użyciu technologii minifiltrów, system ma wykrywać wirusy, oprogramowanie szpiegowskie i inne pliki przed ich uruchomieniem, dając dzięki temu wydajną ochronę przed wieloma zagrożeniami, a jednocześnie minimalizując zaangażowanie użytkownika końcowego.
7. Aparat ochrony przed złośliwym oprogramowaniem ma używać zaawansowanych technologii wykrywania, takich jak analiza statyczna, emulacja, heurystyka i tunelowanie w celu identyfikacji złośliwego oprogramowania i ochrony systemu. Ponieważ zagrożenia stają się coraz bardziej złożone, ważne jest, aby zapewnić nie tylko oczyszczenie systemu, ale również poprawne jego funkcjonowanie po usunięciu złośliwego oprogramowania. Aparat ochrony przed złośliwym oprogramowaniem w systemie ma zawierać zaawansowane technologie oczyszczania, pomagające przywrócić poprawny stan systemu po usunięciu złośliwego oprogramowania.
8. Generowanie alertów dla ważnych zdarzeń, takich jak atak złośliwego oprogramowania czy niepowodzenie próby usunięcia zagrożenia.
9. Tworzenie szczegółowych raportów zabezpieczeń systemów IT o określonych priorytetach, dzięki którym użytkownik może wykrywać i kontrolować zagrożenia lub słabe punkty zabezpieczeń. Raporty mają obejmować nie tylko takie informacje, jak ilość ataków wirusów, ale wszystkie aspekty infrastruktury IT, które mogą wpłynąć na
10. bezpieczeństwo firmy (np. ilość komputerów z wygasającymi hasłami, ilość maszyn, na których jest zainstalowane konto „gościa”, itd.).
11. Pakiet ma umożliwiać zdefiniowanie jednej zasady konfigurującej technologie antyszpiegowskie, antywirusowe i technologie monitorowania stanu jednego lub wielu chronionych komputerów. Zasady obejmują również ustawienia poziomów alertów, które można konfigurować, aby określić rodzaje alertów i zdarzeń generowanych przez różne grupy chronionych komputerów oraz warunki ich zgłaszania.
12. System ochrony musi być zoptymalizowany pod kątem konfiguracji ustawień agenta zabezpieczeń przy użyciu Zasad Grupy usługi katalogowej oraz dystrybucji aktualizacji definicji.
 |

1. Oferowany produkt równoważny musi spełniać wszystkie warunki poniżej:
	1. Warunki licencji w każdym aspekcie licencjonowania są nie gorsze niż licencja produktu określonego w punkcie 3.1). tzn. licencja na oprogramowanie musi być przypisana do liczby rdzeni każdego procesora fizycznego na serwerze. Pozostałe parametry serwera np. ilość pamięci RAM nie mogą mieć wpływu na liczbę wymaganych licencji.
	2. Nabycie licencji oprogramowania równoważnego pozwala na legalne używanie posiadanych przez Zamawiającego licencji oprogramowania.
	3. Ważność licencji na serwery fizyczne i wirtualne nie jest ograniczona czasowo.
	4. Funkcjonalność oprogramowania równoważnego nie może być gorsza od funkcjonalności oprogramowania wykorzystywanego przez Zamawiającego, przy czym pod pojęciem funkcjonalności Zamawiający rozumie zbiór funkcji oprogramowania określających zakres jego wykorzystania z wyłączeniem wyglądu interfejsu, opisanych w pkt. 7.

# Pakiet Management Pack do monitorowania środowiska wirtualnego dla pakietu opisanego w sekcji C

1. Przedmiotem zamówienia jest dostawa Pakiet Management Pack do monitorowania środowiska wirtualnego dla pakietu opisanego w sekcji C, w celu uzupełnienia stanu posiadanego oprogramowania
2. Wskazane w opisie nazwy produktów odnoszą się do posiadanego i wykorzystywanego przez jednostki organizacyjne służb Statystyki Publicznej oprogramowania, a zachowanie parametrów określonych jako równoważne jest konieczne do zachowania kompatybilności i spójności środowiska. Zamawiający oczekuje ofert spełniających wymagania minimalne określone poniżej.
3. Zamawiający posiada licencje: Veeam Management Pack for System Center v. 6.5.0.1549
4. Oprogramowanie musi być dostarczone w najwyższej (najnowszej) wersji, na moment złożenia oferty przez Wykonawcę.
5. Licencje muszą pozwalać na pobieranie nowych wersji oprogramowania systemu w okresie pięciu lat.
6. Dopuszcza się zaoferowanie produktów równoważnych do produktów wymienionych w pkt 3.
7. Oferowany przez Wykonawcę produkt musi posiadać wszystkie wymienione cechy:
8. Management Pack musi być zgodny i całkowicie integrować się z Microsoft System Center Operations Manager.
9. Management Pack musi zapewnić monitorowanie przez Microsoft System Center Operations Manager środowiska opartego o VMware ESXi 5.x i 6.x zarówno w wersji płatnej jak i pojedynczych hostów pracujących w oparciu o edycję darmową.
10. Management Pack musi zapewnić monitorowanie przez Microsoft System Center Operations Manager środowiska opartego o Windows Server Hyper-V 2012 R2, 2016, 2019,
11. Management Pack musi korzystać z wbudowanych w infrastrukturę VMware mechanizów monitorowania (VMware API) i nie może instalować na infrastrukturze żadnych agentów.
12. Dla środowiska Hyper-V Management Pack musi móc się zintegrować i skorzystać
z agentów Microsoft System Center Operations Managera.
13. Management Pack musi być certyfikowany przez VMware (certyfikat VMware Ready) oraz przez Microsoft (pakiet umieszczony na Microsoft System Center Marketplace).
14. Management Pack musi zapewnić możliwość monitorowania i raportowania o problemach wszystkich elementów infrastruktury VMware takich jak vCenter Server, klastry, hosty, wirtualne maszyny, wirtualne switche, podsystem dyskowy, hardware.
15. Management Pack musi zapewnić możliwość monitorowania i raportowania o problemach wszystkich elementów infrastruktury Hyper-V takich jak System Center Virtual Machine Manager, klastry, hosty, wirtualne maszyny, wirtualne switche, podsystemy dyskowe.
16. Dane przesyłane podczas monitoringu muszą być zaszyfrowane i przesyłane przy pomocy protokołu HTTPS.
17. Management Pack musi zawierać wbudowane łącza do bazy wiedzy VMware oraz
Hyper-V skorelowane z obsługiwanymi alertami i wydarzeniami.
18. Management Pack musi mieć możliwość integracji z Microsoft System Center Virtual Machine Manager.
19. Managment Pack musi zapewniać możliwość monitorowania i raportowania szczegółowych parametrów infrastruktury Veeam Backup&Replication.
20. Produkt równoważny musi spełniać wszystkie warunki poniżej:
	1. Warunki licencji w każdym aspekcie licencjonowania są nie gorsze niż licencja produktu określonego w punkcie 3 tzn. licencja na oprogramowanie musi być przypisana do liczby procesorów fizycznych na serwerze fizycznym. Pozostałe parametry serwera np. ilość pamięci RAM nie mogą mieć wpływu na liczbę wymaganych licencji.
	2. Nabycie licencji oprogramowania równoważnego pozwala na legalne używanie posiadanych przez Zamawiającego licencji oprogramowania.
	3. Ważność licencji nie jest ograniczona czasowo.
21. Przez produkt równoważny rozumie się taki, który w sposób poprawny współpracuje z posiadanym przez Zamawiającego oprogramowaniem, a jego zastosowanie nie wymaga żadnych nakładów, po stronie Zamawiającego, związanych z dostosowaniem systemów i aplikacji Zamawiającego do produktu równoważnego oraz posiada wszelkie funkcjonalności zamawianego oprogramowania, opisane w pkt. 7.

# System bazodanowy dla nieograniczonej liczby użytkowników (SBD)

1. Przedmiotem zamówienia jest dostawa systemu bazodanowy dla nieograniczonej liczby użytkowników, w celu uzupełnienia stanu posiadanego oprogramowania.
2. Wskazane w opisie nazwy produktów odnoszą się do posiadanego i wykorzystywanego przez jednostki organizacyjne służb statystyki publicznej oprogramowania, a zachowanie parametrów określonych jako równoważne jest konieczne do zachowania kompatybilności i spójności środowiska. Zamawiający oczekuje ofert spełniających wymagania minimalne określone poniżej.
3. Zamawiający posiada licencje:
	1. Microsoft SQL Server 2008 Enterprise
	2. Microsoft SQL Server 2012 Enterprise
	3. Microsoft SQL Server 2012 Developer
	4. Microsoft SQL Server 2019 Enterprise
4. Oprogramowanie musi być dostarczone w najwyższej (najnowszej) wersji, na moment złożenia oferty przez Wykonawcę.
5. Wymagania ogólne w zakresie licencji:
	1. Licencje muszą pozwalać na przenoszenie pomiędzy serwerami fizycznymi jak również hostami farmy serwerów wirtualnych.
	2. Licencjonowanie musi uwzględniać dostarczanie przez producenta oprogramowania poprawek krytycznych i opcjonalnych do zakupionej wersji oprogramowania i prawo do bezpłatnej ich instalacji w okresie przynajmniej 5 lat.
	3. Wymagane jest zapewnienie możliwości korzystania z wcześniejszych wersji zamawianego oprogramowania i korzystania z kopii zamiennych (możliwość kopiowania oprogramowania na wiele urządzeń przy wykorzystaniu jednego standardowego obrazu uzyskanego z nośników dostępnych w programach licencji grupowych), z prawem do wielokrotnego użycia jednego obrazu dysku w procesie instalacji i tworzenia kopii zapasowych.
	4. W ramach umowy Wykonawca ma zapewnić udzielanie uprawnień na witrynie producenta oprogramowania wskazanym przez Zamawiającego osobom (pracownikom Zamawiającego) do pobierania zamówionego oprogramowania i kluczy licencyjnych.
6. Oferowany przez Wykonawcę produkt musi spełniać wszystkie warunki poniżej:
7. Możliwość wykorzystania SBD jako silnika relacyjnej bazy danych, analitycznej wielowymiarowej bazy danych, platformy bazodanowej dla wielu aplikacji. Powinien zawierać serwer raportów, narzędzia do definiowania raportów, wykonywania analiz biznesowych, tworzenia procesów ETL, tworzenia obiektów bazodanowych, realizacji zapytań do baz danych, analizy sposobu wykonania zapytania przez system bazodanowy.
8. Dostarczone oprogramowanie systemu bazodanowego powinno umożliwić przenoszenie struktur baz danych i danych z funkcjonującego obecnie środowiska bazodanowego do środowiska zbudowanego przy wykorzystaniu dostarczonego oprogramowania systemu bazodanowego.
9. Wykorzystywane w centrach przetwarzania Statystyki publicznej aplikacje, komunikujące się z bazami danych Microsoft SQL Server 2012, powinny bez wprowadzania zmian w kodzie aplikacji komunikować się z bazami danych dostarczonego oprogramowania systemu bazodanowego.
10. Bazy danych dostarczonego oprogramowania systemu bazodanowego powinny móc stanowić źródła danych dla: raportów Reporting Services, baz analitycznych, pakietów ETL, skryptów bazodanowych tworzonych i utrzymywanych w obecnym środowisku.
11. SBD nie powinien ograniczać wykorzystania liczby procesorów/rdzeni oraz pamięci RAM serwera.
12. Zarządzanie, konfigurowanie i monitorowanie wszystkich usług/modułów środowiska bazy danych powinno być zrealizowane w oparciu o dostarczone narzędzia graficzne. Narzędzia te muszą udostępniać możliwość automatyzacji wykonywania zadań związanych z zarządzaniem, konfigurowaniem i monitorowaniem wszystkich usług/modułów środowiska bazy danych.
13. SBD musi udostępniać graficzne narzędzia do diagnozowania wydajności bazy danych. SBD musi również udostępniać graficzne narzędzia do strojenia wydajności bazy danych z funkcją śledzenia wykonywanych zapytań SQL.
14. SBD musi udostępniać mechanizm zarządzania systemem za pomocą uruchamianych z linii poleceń skryptów administracyjnych, które pozwolą zautomatyzować rutynowe czynności związane z zarządzaniem serwerem.
15. SBD musi pozwalać na zdalne połączenie sesji administratora systemu bazy danych w sposób niezależny od normalnych sesji klientów.
16. SBD musi umożliwiać wykonywanie typowych zadań administracyjnych (indeksowanie, backup) bez konieczności przerywania pracy systemu lub przechodzenia w tryb jednoużytkownikowy.
17. SBD powinien umożliwiać tworzenie w dowolnym momencie kopii bazy danych tylko do odczytu zawierającej stan bazy z bieżącego momentu czasu. Wiele takich kopii może być równolegle użytkowanych w celu wykonywania do nich zapytań.
18. SBD musi umożliwiać tworzenie klastrów niezawodnościowych. Powinien również umożliwiać tworzenie klastrów niezawodnościowych, których węzły znajdują się w różnych podsieciach komputerowych SBD musi posiadać mechanizm pozwalający na duplikację bazy danych między wieloma lokalizacjami (podstawowa i zapasowe) przy zachowaniu następujących cech: - bez specjalnego sprzętu (rozwiązanie tylko programowe oparte o sam SBD), - niezawodne powielanie danych w czasie rzeczywistym (potwierdzone transakcje bazodanowe), - duplikacja danych w trybie synchronicznym lub asynchronicznym, - SBD musi umożliwiać duplikację danych z ośrodka podstawowego, do co najmniej 8 lokalizacji zapasowych, - w celu zwiększenia skalowalności i wydajności systemu SBD musi umożliwiać korzystanie z kopii baz w lokalizacjach zapasowych w trybie tylko do odczytu (raportowanie, tworzenie backupów itp.) bez przerywania działania mechanizmu duplikacji danych z ośrodka podstawowego, - klienci bazy danych mogą być automatycznie przełączeni do bazy zapasowej w przypadku awarii bazy podstawowej bez zmian w aplikacjach, - brak limitu odległości miedzy systemami (dopuszczalne są tylko limity w minimalnej wymaganej przepustowości łącza oraz limity wynikające z opóźnień na łączu), - kompresja danych przesyłanych między serwerem podstawowym i zapasowym (w celu minimalizacji obciążenie sieci).
19. SBD musi umożliwiać zapewnienie wysokiej dostępności zarówno poszczególnych baz danych, jak i całych instancji SBD, pozwalającej na utrzymanie ciągłości świadczonych usług bez konieczności zmiany konfiguracji połączeń aplikacji klienckich sięgających do baz danych.
20. SBD powinien pozwalać na transakcyjną replikację wybranych danych z bazy danych między wieloma węzłami. Dodanie lub usunięcie węzła nie powinno wpływać na funkcjonowanie i spójność systemu replikacji, ani nie powinno przerywać procesu replikacji. Dane mogą w takim schemacie replikacji być modyfikowane w dowolnym węźle (ale tylko w jednym węźle w danym momencie). System powinien zawierać narzędzie do nadzorowania i wizualizacji topologii oraz stanu procesu replikacji. Dodatkowo SBD powinien umożliwiać kompresję przesyłanych danych między serwerami uczestniczącymi w replikacji, aby minimalizować obciążenie łączy sieciowych.
21. SBD musi pozwalać na kompresję kopii zapasowej bazy danych w trakcie jej tworzenia. Powinna to być cecha SBD niezależna od funkcji systemu operacyjnego ani od sprzętowego rozwiązania archiwizacji danych.
22. SBD musi pozwalać na szyfrowanie przechowywanych danych. Szyfrowanie musi być cechą SBD i nie może wymagać jakichkolwiek zmian w aplikacjach korzystających z danych. Zaszyfrowanie lub odszyfrowanie danych nie powinno powodować przerwy w dostępie do danych. SBD powinien także dostarczać możliwość szyfrowania danych podczas tworzenia kopii bezpieczeństwa przy użyciu między innymi certyfikatów lub kluczy asymetrycznych.
23. SBD musi posiadać możliwość rejestracji zdarzeń na poziomie silnika bazy danych w czasie rzeczywistym w celach diagnostycznych, pozwalać na selektywne wybieranie rejestrowanych zdarzeń.
24. SBD powinien posiadać wbudowany mechanizm ograniczający wykorzystanie zasobów systemu operacyjnego (% wykorzystania czasu procesora, % wykorzystania pamięci).
25. W celu zwiększenia wydajności przetwarzania SBD musi posiadać wbudowaną funkcjonalność pozwalającą na rozszerzenie cache-u przetwarzania w pamięci RAM o dodatkową przestrzeń na dysku SSD.
26. SBD musi umożliwiać tworzenie procedur składowanych, które mogą być udostępnione i wywoływane jako WebServices.
27. SBD musi umożliwiać definiowanie nowych typów danych wraz z definicją specyficznej dla tych typów danych logiki operacji. Jeśli np. zdefiniujemy typ do przechowywania danych hierarchicznych, to obiekty tego typu powinny udostępnić operacje dostępu do “potomków” obiektu, “rodzica” itp. Logika operacji nowego typu danych powinna być implementowana w zaproponowanym przez Dostawcę języku programowania. Nowe typy danych nie mogą być ograniczone wyłącznie do okrojenia typów wbudowanych lub ich kombinacji.
28. SBD musi udostępniać mechanizmy składowania i obróbki danych w postaci struktur XML. (wsparcie dla technologii XML) W szczególności musi:
29. udostępniać typ danych do przechowywania kompletnych dokumentów XML w jednym polu tabeli,
30. udostępniać mechanizm walidacji struktur XML-owych względem jednego lub wielu szablonów XSD,
31. udostępniać język zapytań do struktur XML,
32. udostępniać język modyfikacji danych (DML) w strukturach XML (dodawanie, usuwanie i modyfikację zawartości struktur XML),
33. udostępniać możliwość indeksowania struktur XML-owych w celu optymalizacji wykonywania zapytań.
34. SBD musi zapewniać wsparcie dla danych przestrzennych (geometrycznych i geograficznych typów danych) pozwalających w prosty sposób przechowywać i analizować informacje o lokalizacji obiektów, dróg i innych punktów orientacyjnych zlokalizowanych na kuli ziemskiej, a w szczególności:
35. zapewniać możliwość wykorzystywania szerokości i długości geograficznej do opisu lokalizacji obiektów,
36. obsługa geometrycznych i geograficznych typów danych powinna być dostępna z poziomu języka zapytań do systemu SBD.
37. SBD powinien umożliwiać przechowywanie i efektywne zarządzanie dużymi obiektami binarnymi (pliki graficzne, multimedialne, dokumenty). Obiekty te nie powinny być przechowywane w plikach bazy danych, ale w systemie plików . Jednocześnie pliki te powinny być zarządzane przez SBD (kontrola dostępu na podstawie uprawnień nadanych w SBD).
38. SBD powinien udostępniać wbudowany mechanizm kompresji zgromadzonych danych w celu osiągnięcia lepszej wydajności przy niezmienionej konfiguracji sprzętowej. SBD powinien umożliwiać kompresję danych i indeksów.
39. SBD powinien pozwalać na rejestrację zmian w danych włącznie z zapamiętaniem stanu pojedynczego rekordu danych sprzed modyfikacji. Rozwiązanie powinno być konfigurowalne bez wpływu na istniejące aplikacje korzystające z danych. Rozwiązanie powinno rejestrować także zmiany w definicji struktur danych.
40. SBD powinien pozwalać na rejestrację operacji takich jak: logowanie, wylogowanie użytkownika, zmiany w definicji obiektów bazy danych (tabele, procedury), wykonywanie przez wskazanego użytkownika operacji takich jak SELECT, INSERT, UPDATE, DELETE. Rozwiązanie powinno być niezależne od aplikacji, wbudowane w SBD.
41. SBD powinien umożliwiać partycjonowanie danych poprzez podział danych w jednej tabeli między różne fizyczne pamięci masowe zgodnie ze zdefiniowanymi warunkami podziału. Powinien udostępniać mechanizm równoległego (wielowątkowego) dostępu do danych umieszczonych w różnych partycjach.
42. SBD powinien umożliwiać tworzenie indeksów na podzbiorze danych z tabeli określonym poprzez wyrażenie filtrujące.
43. SBD musi umożliwiać tworzenie procedur i funkcji z wykorzystaniem innych języków programowania (np. Java, C#) niż standardowo obsługiwany język zapytań danego SBD. System powinien umożliwiać tworzenie w tych językach m.in. agregujących funkcji użytkownika oraz wyzwalaczy. Dodatkowo powinien udostępniać środowisko do debuggowania.
44. Język zapytań i procedur w SBD musi umożliwiać zastosowanie mechanizmu przechwytywania i obsługi błędów wykonania procedury (na zasadzie bloku instrukcji TRY/CATCH) – tak jak w klasycznych językach programowania.
45. SBD musi udostępniać mechanizm pozwalający na zamrożenie planu wykonania zapytania przez silnik bazy danych (w wyniku takiej operacji zapytanie jest zawsze wykonywane przez silnik bazy danych w ten sam sposób).
46. SBD musi posiadać narzędzie do graficznego projektowania transformacji danych. Narzędzie to powinno pozwalać na przygotowanie definicji transformacji w postaci pliku, które potem mogą być wykonywane automatycznie lub z asystą operatora. Transformacje powinny posiadać możliwość graficznego definiowania zarówno przepływu sterowania (program i warunki logiczne) jak i przepływu strumienia rekordów poddawanych transformacjom. Zestaw standardowych dostępnych transformacji powinien obejmować takie transformacje jak: sortowanie, wyszukiwanie wartości według klucza w tabelach słownikowych, automatyczna obsługa SCD (Slowly Changing Dimension) w zasilaniu hurtowni danych. Powinna być także zapewniona możliwość tworzenia własnych transformacji.
47. SBD powinien umożliwiać integrację danych relacyjnych z nierelacyjnymi źródłami danych, np. Hadoop.
48. SBD musi posiadać moduł pozwalający na tworzenie rozwiązań służących do analizy danych wielowymiarowych (hurtownia danych). Powinno być możliwe tworzenie: wymiarów, miar. Wymiary powinny mieć możliwość określania dodatkowych atrybutów będących dodatkowymi poziomami agregacji. Powinna być możliwość definiowania hierarchii w obrębie wymiaru.
49. Moduł analityczny musi mieć możliwość wyliczania agregacji wartości miar dla zmieniających się elementów (członków) wymiarów i ich atrybutów. Agregacje powinny być składowane w jednym z wybranych modeli (MOLAP, ROLAP). Pojedyncza baza analityczna musi mieć możliwość mieszania modeli składowania.
50. SBD powinien posiadać narzędzia do zarządzania jakością danych w organizacji. W ramach tych funkcji powinien:
	1. udostępniać funkcje do profilowania danych (analiza i raporty dot. jakości danych),
	2. udostępniać funkcje do deduplikacji danych,
	3. określać stopień poprawności wartości atrybutu i w przypadku błędnej wartości sugerować wartość poprawną do akceptacji przez użytkownika,
	4. umożliwiać definiowanie osobnych reguł czyszczenia dla wybranych domen (typów atrybutów),
	5. umożliwiać definiowanie złożonych domen (zestawu kilku atrybutów) oraz ocenę jakości danych na podstawie powiązań między tymi atrybutami (np. weryfikację poprawności danych adresowych złożonych z kodu pocztowego, miasta i ulicy),
	6. pozwalać na ręczną korektę nieprawidłowych danych w dedykowanej aplikacji (bez konieczności programowania),
	7. umożliwiać eksport wyników badania (poprawnych i sugerowanych wartości) do pliku tekstowego lub bazy relacyjnej, eksport powinien obejmować wartości po korekcie oraz ewentualnie te przed korektą,
	8. przechowywać reguły walidujące i oceniające jakość danych w dedykowanej bazie danych (bazie wiedzy),
	9. umożliwiać uzupełnianie i rozszerzanie bazy wiedzy o dane referencyjne pochodzące z systemów zewnętrznych,
	10. zapewniać mechanizmy “uczenia się” bazy wiedzy – czyli w miarę realizacji kolejnych procesów ręcznego czyszczenia danych baza wiedzy powinna umożliwiać gromadzenie tych informacji na potrzeby kolejnych procesów,
	11. umożliwiać wykorzystanie bazy wiedzy w automatycznym procesie czyszczenia danych (powinien integrować się z narzędziami do ekstrakcji, transformacji i ładowania danych, dzięki czemu będzie można wykorzystać te mechanizmy w automatycznym procesie ładowania danych).
51. Możliwość zarządzania centralnymi słownikami danych - SBD powinien dostarczać narzędzia do przechowywania i zarządzania centralnym słownikiem danych (Master Data Management - MDM). System MDM powinien:
52. udostępniać narzędzia do wprowadzania, modyfikacji i wyszukiwania danych w słownikach,
53. umożliwiać wersjonowanie danych (śledzenie zmian wprowadzonych przez użytkowników z możliwością ich cofnięcia do wybranej wersji),
54. udostępniać mechanizm tworzenia i uruchamiania reguł walidujących poprawność danych w słownikach,
55. udostępniać narzędzia do administracji i kontroli uprawnień dostępu do danych w MDM,
56. udostępniać zestaw bibliotek (API programistyczne) z funkcjonalnościami MDM do wykorzystania w aplikacjach użytkownika,
57. umożliwiać eksport danych zgromadzonych w systemie MDM,
58. umożliwiać zarządzanie danymi podstawowymi z poziomu programu Microsoft Excel.
59. Moduł analityczny powinien umożliwiać rejestrowanie zapytań wykonywanych przez użytkowników do baz analitycznych, a następnie umożliwiać na podstawie zgromadzonych informacji automatyczną optymalizację wydajności systemu (np. automatyczne projektowanie agregacji pozwalające na przyspieszenie wykonywania najczęściej wykonywanych zapytań do bazy danych).
60. Moduł analityczny powinien umożliwiać tworzenie perspektyw na bazie wielowymiarowej pozwalających ograniczyć widok dla użytkownika tylko do pewnego podzbioru obiektów dostępnych w całej bazie danych.
61. Moduł analityczny powinien umożliwiać użytkownikom tworzenie analiz In-Memory, czyli przetwarzanie dużej liczby rekordów skompresowanych w pamięci RAM. Powinien umożliwiać tworzenie modeli wykorzystujących tabele pochodzące z wielu niezależnych źródeł danych i łączone między sobą relacjami.
62. Moduł analityczny powinien udostępniać dedykowany język do tworzenia logiki biznesowej w modelu. Język ten powinien m.in. obsługiwać relacje utworzone między tabelami, mechanizmy operacji na datach i okresach, oraz zapewniać mechanizmy kontroli bezpieczeństwa i dostępu do danych na poziomie poszczególnych wierszy.
63. SBD powinien udostępniać mechanizmy optymalizacji zapytań w modelu gwiazdy (tabela faktów łączona z tabelami wymiarów).
64. SBD powinien udostępniać wbudowane mechanizmy pozwalające w łatwy i szybki sposób aktualizować zawartość tabel faktów (wykorzystywanych w modelach wielowymiarowych). Mechanizm ten powinien być dostępny z poziomu zapytań języka SQL obsługiwanego przez silnik bazy danych.
65. Moduł analityczny musi udostępniać rozwiązania Data Mining, m.in.: algorytmy reguł związków, szeregów czasowych, drzew regresji, sieci neuronowych. Dodatkowo system powinien umożliwiać tworzenie własnych algorytmów, udostępniać narzędzia do wizualizacji danych z modelu Data Mining oraz język zapytań do odpytywania tych modeli.
66. SBD musi udostępniać użytkownikom możliwość tworzenia wskaźników KPI (Key Performance Indicators) na podstawie danych zgromadzonych w strukturach wielowymiarowych. W szczególności powinien pozwalać na zdefiniowanie takich elementów, jak: wartość aktualna, cel, trend, symbol graficzny wskaźnika w zależności od stosunku wartości aktualnej do celu. System powinien umożliwiać tworzenie takich wskaźników również w modelach danych wykorzystujących technologię in-memory BI.
67. Moduł raportowania SBD musi posiadać możliwość definiowania i generowania raportów. Narzędzie do tworzenia raportów powinno pozwalać na ich graficzną definicję. Raporty powinny być udostępnianie przez serwer raportów protokołem HTTP (dostęp klienta za pomocą przeglądarki). Dodatkowo system raportowania powinien obsługiwać:
68. raporty parametryzowane,
69. cache raportów i raportów parametryzowanych,
70. współdzielenie predefiniowanych zapytań do źródeł danych,
71. wizualizację danych analitycznych na mapach geograficznych (w tym import map w formacie ESRI Shape File),
72. możliwość opublikowania elementu raportu (wykresu, tabeli) we współdzielonej bibliotece, z której mogą korzystać inni użytkownicy tworzący nowy raport ,
73. możliwość wizualizacji wskaźników KPI,
74. możliwość wizualizacji danych w postaci obiektów sparkline.
75. Wymagane jest generowanie raportów w formatach: XML, PDF, Microsoft Excel, Microsoft Word, HTML, TIFF, CSV. Dodatkowo raporty powinny być eksportowane w formacie Atom data feeds, które można będzie wykorzystać jako źródło danych w innych aplikacjach.
76. SBD musi umożliwiać rozbudowę mechanizmów raportowania m.in. o dodatkowe formaty eksportu danych, obsługę nowych źródeł danych dla raportów, funkcje i algorytmy wykorzystywane podczas generowania raportu (np. nowe funkcje agregujące).
77. SBD musi umożliwiać wysyłkę raportów drogą mailową w formacie wybranym spośród udostępnianych formatów (subskrypcja) do dynamicznej listy odbiorców (pobieranej z bazy danych np. zapytaniem SQL).
78. SBD powinien udostępniać narzędzia do tworzenia raportów ad-hoc przez niezaawansowanych użytkowników. Tworzenie raportów powinno odbywać się w środowisku graficznym. Użytkownicy powinni mieć możliwość na publikowanie stworzonych raportów na serwerze w celu udostępnienia ich szerszemu gronu osób.
79. Oferowany produkt równoważny musi spełniać wszystkie warunki poniżej:
80. Warunki licencji w każdym aspekcie licencjonowania są nie gorsze niż licencja produktu określonego w punkcie 3.2 tzn. licencja na oprogramowanie musi być przypisana do liczby rdzeni każdego procesora fizycznego na serwerze. Pozostałe parametry serwera np. ilość pamięci RAM nie mogą mieć wpływu na liczbę wymaganych licencji.
81. Nabycie licencji oprogramowania równoważnego pozwala na legalne używanie posiadanych przez Zamawiającego licencji oprogramowania.
82. Ważność licencji na serwery fizyczne i wirtualne nie jest ograniczona czasowo.
83. Funkcjonalność oprogramowania równoważnego nie może być gorsza od funkcjonalności oprogramowania wykorzystywanego przez Zamawiającego, przy czym pod pojęciem funkcjonalności Zamawiający rozumie zbiór funkcji oprogramowania określających zakres jego wykorzystania z wyłączeniem wyglądu interfejsu, opisanych w pkt. 6.