

ZAPYTANIE O WYCENĘ DO OSZACOWANIA WARTOŚCI ZAMÓWIENIA

Ministerstwo planuje uruchomić postępowanie przetargowe o udzielenie zamówienia publicznego na zakup klastra serwerów wirtualizacji oraz licencji baz danych i systemów operacyjnych

Uprzejmie prosimy o wycenę, poniżej opisanych minimalnych wymagań stanowiących przedmiot planowanego do wszczęcia postępowania przetargowego.

Zamówienie zostanie podzielone na trzy części:

1. Część I, tj. dostawa klastra serwerów wirtualizacji wraz ze wsparciem na 36 miesięcy
2. Część II, tj. dostawa licencji oprogramowania wirtualizacji dla dostarczanego klastra ze wsparciem na 36 miesięcy.
3. Część III, tj. dostawa licencji baz danych i systemów operacyjnych

Zamawiający zamierza podzielić zamówienie na części. Tym samym Zamawiający dopuszcza składanie ofert częściowych, tj. Wykonawca może złożyć ofertę na jedną, dwie lub trzy części zamówienia.

Część IZakres zamówienia

Lp.	Produkt	Liczba sztuk
1	<u>Serwer klastra wirtualizacji wraz ze wsparciem na 36 miesięcy.</u>	4
2	<u>Usługa wdrożenia oraz instruktażu</u>	1

Część IIZakres zamówienia

Lp.	Produkt	Rodzaj licencjonowania	Liczba produktów
1	Licencja oprogramowania wirtualizacji dla dostarczanego klastra ze wsparciem na 36 miesięcy	Subskrypcja	64 core fizyczne

Część IIIZakres zamówienia

Lp.	Numer katalogowy	Produkt	Rodzaj licencjonowania	Liczba produktów
1	9EA-00271	Win Server DC Core ALng LSA 16L z Software Assurance ważnym od dostarczenia do 30.06.2028 r.	Nieograniczona w czasie	4
2	7JQ-00341	SQL Server Enterprise Core ALng LSA 2L) z Software Assurance od dostarczenia do 30.06.2028 r.	Nieograniczona w czasie	32

I. PRZEDMIOT ZAMÓWIENIA

Przedmiotem Zamówienia, jest zakup klastra serwerów wirtualizacji oraz licencji baz danych i systemów operacyjnych..

zamówienia obejmuje:

Część I, tj. dostawa klastra serwerów wirtualizacji wraz ze wsparciem na 36 miesięcy, w tym:

1. Dostawę klastra wirtualizacji, tj. elementów infrastruktury przeznaczonych do uruchomienia klastra wraz ze wsparciem producenta na okres 36 miesięcy
2. wdrożenie dostarczonych elementów, w tym:
 - a) instalację dostarczonych urządzeń i subskrypcji oprogramowania,
 - b) konfigurację, uruchomienie i testowanie, w tym dodatkowych elementów,
 - c) wykonanie dokumentacji technicznej i eksploatacyjnej,
 - d) przeprowadzenie instruktażu dla administratorów Systemu.

Część II, tj. dostawa Licencja oprogramowania wirtualizacji dla dostarczanego klastra ze wsparciem na 36 miesięcy, w tym:

1. dostawa licencji wirtualizacji

Część III, tj. dostawa licencji baz danych i systemów operacyjnych, w tym"

2. dostawa licencji Microsoft Windows Datacenter wraz z Software Assurance
3. dostawa licencji Microsoft SQL Server Enterprise wraz z Software Assurance

II. TERMIN REALIZACJI ZAMÓWIENIA

Przedmiot zamówienia zostanie zrealizowany w terminie maksymalnie **do 40 dni** od daty podpisania przez strony umowy **(termin realizacji do uzupełnienia przez Wykonawcę w Formularzu Ofertowym)**.

Realizacja przedmiotu zamówienia obejmować będzie dostawę zakup klastra serwerów baz danych wraz z niezbędnymi licencjami technologicznymi dla Ministerstwa Rozwoju i Technologii do centrum przetwarzania na terenie Polski wskazanego przez Zamawiającego.

III. MINIMALNE WYMAGANIA DOTYCZĄCE REALIZACJI PRZEDMIOTU ZAMÓWIENIA

1. Zaoferowane urządzenia oraz oprogramowanie nie może być przeznaczone przez producenta do wycofania z produkcji lub sprzedaży.
2. Wszystkie elementy dostarczone z urządzeniami, będą pochodziły od jednego producenta. Stosowane elementy muszą być wspierane przez producenta urządzeń i być objęte możliwością analizy potencjalnych błędów w trakcie potencjalnych zgłoszeń serwisowych. Muszą pochodzić z autoryzowanego kanału sprzedaży producentów Urządzeń na rynek polski lub Unii Europejskiej
3. Zaoferowane urządzenia muszą być fabrycznie nowe przeznaczone do sprzedaży na rynku europejskim (zgodnie z ustawą z dnia 30.08.2002 r. o systemie oceny zgodności (Dz.U. z 2004 r., nr 204, poz. 2087 j.t. z późn. zm.) i z wydanymi na jej podstawie rozporządzeniami), wyprodukowane nie wcześniej niż 6 miesięcy przed datą dostarczenia oraz objęte wymaganą przez Zamawiającego gwarancją w Polsce. Zamawiający nie dopuszcza produktów „odnawianych” (ang. Refurbished). Zaoferowane urządzenia, oprogramowanie sterujące połączeniami oraz aplikacje zarządzające muszą pochodzić od tego samego producenta. Zamawiający wymaga, aby dostarczony System pochodził z oficjalnego kanału dystrybucyjnego danego producenta, a serwis gwarancyjny był autoryzowany przez producenta urządzeń i oprogramowania oraz świadczony przez producenta lub autoryzowanych partnerów w centrach serwisowych na terenie Unii Europejskiej.
4. Zamawiający wymaga, aby zaoferowane urządzenia były dostępne i serwisowane przez Producenta oraz nie będą przez niego przewidziane do wycofania ze sprzedaży i wsparcia (ogłoszone tzw. dokumenty End-of-Sale lub End-of-Life lub równoważne) – na dzień składania oferty.

IV. MINIMALNE WYMAGANIA TECHNICZNE I FUNKCJONALNE KLASTRA WIRTUALIZACJI

1. Klaster wirtualizacji musi składać się z minimum 4 serwerów fizycznych.
2. Każdy z serwerów musi być wyposażony w 2 procesory x86 wyposażony w 8 rdzeni fizycznych i z bazowym taktowaniem minimum 4 Ghz i osiągające w testach SPECrate2017_int_base wynik nie gorszy niż 205 punktów, dla testu oferowanego modelu serwera z 2 procesorami
3. Obudowa Rack o wysokości max. 2U z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych z organizerem do kabli.

4. Płyta główna z możliwością zainstalowania dwóch procesorów. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym.
5. Chipset dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych
6. RAM Min. 1TB DDR5 RDIMM 6400MT/s w modułach pamięci o pojemności min. 64GB każdy. Na płycie głównej powinno znajdować się minimum 32 slotów przeznaczonych do instalacji pamięci. Płyta główna powinna obsługiwać do 8TB pamięci RAM.
7. Zabezpieczenia pamięci RAM: Demand Scrubbing, Patrol Scrubbing, Permanent Fault Detection
8. Gniazda PCIe - minimum dwa sloty PCIe x16 generacji 5 i dwa sloty OCP.
9. Interfejsy sieciowe/FC/SAS: Dwa interfejsy sieciowe 25Gb Ethernet ze złączami SFP28 i cztery interfejsy sieciowe 1Gb Ethernet ze złączami Base-T nie zajmujące slotów PCIe.
Dodatkowo zainstalowane:
 - jedna karta dwuportowa 25Gb Ethernet ze złączami SFP28.
 - jedna karta dwuportowa FC 32Gb/s
10. Dyski twarde:

Zainstalowany 1 x 1.6TB NVMe E3s, DWPD min. 3.

Zainstalowane dwa dyski hot-swap M.2 NVMe o pojemności min. 480GB z możliwością konfiguracji RAID 1.
11. Kontroler RAID: Sprzętowy kontroler dyskowy z pojemnością cache 8GB, możliwe konfiguracje poziomów RAID: 0,1,5,6,10,50,60, non-RAID (JBOD). Obsługa najnowszego standardu transmisji danych w technologii PCIe generacji 5, umożliwiającego pełne wykorzystanie wydajności nośników NVMe.
12. Wbudowane porty min. port USB 2.0 oraz dwa porty USB 3.1, port VGA,
13. Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1600x900
14. Wentylatory Redundantne Hot-Plug
15. Zasilacze Min. dwa zasilacze Hot-Plug min. 1500W Titanium.
16. Bezpieczeństwo:
 - Zatrask górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych. Możliwość wyłączenia w BIOS funkcji przycisku zasilania. BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła
 - Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą TPM 2.0 Możliwość dynamicznego włączania i wyłączania portów USB na obudowie – bez potrzeby restartu serwera Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem. Wbudowany w serwer mechanizm pozwalający na weryfikację niezmienności konfiguracji sprzętowej serwera od momentu produkcji do dostawy do docelowej lokalizacji. Mechanizm ma również pozwalać na kontrolę otwarcia urządzenia w trakcie transportu, niezależnie od stanu zasilania.
17. Karta Zarządzania:
 - Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowane port RJ-45 Gigabit Ethernet umożliwiające:
 - zdalny dostęp do graficznego interfejsu Web karty zarządzającej
 - szyfrowane połączenie (TLS) oraz autentykację i autoryzację użytkownika
 - możliwość podmontowania zdalnych wirtualnych napędów
 - wirtualną konsolę z dostępem do myszy, klawiatury
 - wsparcie dla IPv6
 - wsparcie dla SNMP; IPMI2.0, VLAN tagging, SSH
 - możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer, dane historyczne powinny być dostępne przez min. 7 dni wstecz.
 - możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer
 - integracja z Active Directory
 - możliwość obsługi przez ośmiu administratorów jednocześnie
 - Wsparcie dla automatycznej rejestracji DNS
 - wsparcie dla LLDP
 - wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej
 - możliwość podłączenia lokalnego za pomocą interfejsu USB-C na froncie serwera, który pozwala na bezpośredni dostęp interfejsu karty zarządzającej (zarówno UI w przeglądarce, jak i konsolę RACADM czy API Redfish) bez potrzeby połączenia sieciowego
 - Monitorowanie zużycia dysków SSD
 - możliwość monitorowania z jednej konsoli min. 100 serwerami fizycznymi,

- Automatyczne zgłaszanie alertów do centrum serwisowego producenta
- Automatyczne update firmware dla wszystkich komponentów serwera
- Możliwość przywrócenia poprzednich wersji firmware
- Możliwość eksportu eksportu/importu konfiguracji (ustawienie karty zarządzającej, BIOSu, kart sieciowych, HBA oraz konfiguracji kontrolera RAID) serwera do pliku XML lub JSON
- Możliwość zaimportowania ustawień, poprzez bezpośrednie podłączenie plików konfiguracyjnych
- Automatyczne tworzenie kopii ustawień serwera w oparciu o harmonogram.
- Możliwość wykrywania odchyłań konfiguracji na poziomie konfiguracji UEFI oraz wersji firmware serwera

18. Oprogramowanie do zarządzania.

Zainstalowane oprogramowanie producenta serwera do zarządzania, spełniające poniższe wymagania:

- Wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych
- integracja z Active Directory
- Możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta
- Wsparcie dla protokołów SNMP, IPMI, Linux SSH, Redfish
- Możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram
- Szczegółowy opis wykrytych systemów oraz ich komponentów
- Możliwość eksportu raportu do CSV, HTML, XLS, PDF
- Możliwość tworzenia własnych raportów w oparciu o wszystkie informacje zawarte w inwentarzu.
- Grupowanie urządzeń w oparciu o kryteria użytkownika
- Tworzenie automatycznie grup urządzeń w oparciu o dowolny element konfiguracji serwera np. Nazwa, lokalizacja, system operacyjny, obsadzenie slotów PCIe, pozostałego czasu gwarancji
- Możliwość uruchamiania narzędzi zarządzających w poszczególnych urządzeniach
- Szybki podgląd stanu środowiska
- Podsumowanie stanu dla każdego urządzenia
- Szczegółowy status urządzenia/elementu/komponentu
- Generowanie alertów przy zmianie stanu urządzenia.
- Filtry raportów umożliwiające podgląd najważniejszych zdarzeń
- Integracja z service desk producenta dostarczonej platformy sprzętowej
- Możliwość przejęcia zdalnego pulpitu
- Możliwość podmontowania wirtualnego napędu
- Kreator umożliwiający dostosowanie akcji dla wybranych alertów
- Możliwość importu plików MIB
- Przesyłanie alertów „as-is” do innych konsol firm trzecich
- Możliwość definiowania ról administratorów
- Możliwość zdalnej aktualizacji oprogramowania wewnętrznego serwerów
- Aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania)
- Możliwość instalacji oprogramowania wewnętrznego bez potrzeby instalacji agenta
- Możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów
- Moduł raportujący pozwalający na wygenerowanie następujących informacji: nr seryjne sprzętu, konfiguracja poszczególnych urządzeń, wersje oprogramowania wewnętrznego, obsadzenie slotów PCI i gniazd pamięci, informację o maszynach wirtualnych, aktualne informacje o stanie i poziomie gwarancji, adresy IP kart sieciowych, występujących alertów, MAC adresów kart sieciowych, stanie poszczególnych komponentów serwera.
- Możliwość tworzenia sprzętowej konfiguracji bazowej i na jej podstawie weryfikacji środowiska w celu wykrycia rozbieżności.
- Wdrażanie serwerów, rozwiązań modułarnych oraz przełączników sieciowych w oparciu o profile
- Możliwość migracji ustawień serwera wraz z wirtualnymi adresami sieciowymi (MAC, WWN, IQN) między urządzeniami.
- Tworzenie gotowych paczek informacji umożliwiających zdiagnozowanie awarii urządzenia przez serwis producenta.

- Zdalne uruchamianie diagnostyki serwera.
- Dedykowana aplikacja na urządzenia mobilne integrująca się z wyżej opisanymi oprogramowaniem zarządzającym.
- Oprogramowanie dostarczane jako wirtualny appliance dla KVM, ESXi i Hyper-V.

19. Normy Środowiskowe:

Oferowane produkty muszą zawierać informacje dotyczące ponownego użycia i recyklingu, nie mogą zawierać farb i powłok na dużych plastikowych częściach, których nie da się poddać recyklingowi lub ponownie użyć. Wszystkie produkty zawierające podzespoły elektroniczne oraz niebezpieczne składniki powinny być bezpiecznie i łatwo identyfikowalne oraz usuwalne. Usunięcie materiałów i komponentów powinno odbywać się zgodnie z wymogami rozporządzenia nr 1272/2008WE. Produkty muszą składać się z co najmniej w 65% ze składników wielokrotnego użytku/zdatnych do recyklingu. We wszystkich produktach części tworzyw sztucznych większe niż 25-gramowe powinny zawierać nie więcej niż śladowe ilości środków zmniejszających palność sklasyfikowanych w dyrektywie RE 67/548/EEC. Potwierdzeniem spełnienia powyższego wymogu jest wydruk ze strony internetowej www.epeat.net potwierdzający spełnienie normy co najmniej Epeat Silver według normy wprowadzonej w 2019 roku - Wykonawca złoży dokument potwierdzający spełnianie wymogu. Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia producenta serwera

20. Certyfikaty:

- Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015 oraz ISO-14001.
- Serwer musi posiadać deklarację CE. Urządzenia wyprodukowane są przez producenta, zgodnie z normą PN-EN ISO 50001 lub oświadczenie producenta o stosowaniu w fabrykach polityki zarządzania energią, która jest zgodna z obowiązującymi przepisami na terenie Unii Europejskiej.
- Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Microsoft Windows 2022 x64, Microsoft Windows 2025.

V. MINIMALNE WYMAGANIA TECHNICZNE I FUNKCJONALNE OPROGRAMOWANIA WIRTUALIZACJI

1. Wszystkie licencje zaoferowanego oprogramowania do wirtualizacji muszą być licencjami subskrypcyjnymi, tj. licencja na określony czas w formularzu technicznym wraz ze wsparciem technicznym do tych licencji świadczonym przez producenta zaoferowanego oprogramowania. Ilość licencji musi uwzględniać parametry serwerów do wirtualizacji (4 serwerów dwuprocesorowych z procesorami szesnasto-rdzeniowymi).
2. Wszystkie wymagane poniżej komponenty/moduły muszą pochodzić od jednego producenta oprogramowania.
3. Licencje zaoferowanego oprogramowania muszą być zaoferowane w formie „per core” fizyczny procesora fizycznego.
4. Zaoferowane oprogramowanie musi być instalowane bezpośrednio na sprzęcie fizycznym i nie może być ono częścią innego systemu operacyjnego.
5. Zaoferowane oprogramowanie musi być instalowane bezpośrednio na sprzęcie fizycznym i nie może być ono częścią innego systemu operacyjnego.
6. W zaoferowanym oprogramowaniu warstwa wirtualizacji nie może dla własnych celów alokować więcej niż 700MB pamięci operacyjnej RAM serwera fizycznego
7. Zaoferowane oprogramowanie do wirtualizacji zainstalowane na serwerze fizycznym musi potrafić obsłużyć i wykorzystać procesory fizyczne tego serwera wyposażone w 768 logicznych wątków, 24TB pamięci fizycznej RAM tego serwera oraz 16 procesorów fizycznych tego serwera.
8. Zaoferowane oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych z ilością od 1 do 768 procesorów wirtualnych
9. Zaoferowane oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych z możliwością przydzielenia do 24 TB pamięci operacyjnej RAM.
10. Zaoferowane oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych z możliwością przydzielenia od 1 do 10 wirtualnych kart sieciowych dla każdej z nich. Dodatkowo, oprogramowanie musi posiadać możliwość utworzenia maszyny wirtualnej bez przydzielonej wirtualnej karty sieciowej.

11. Zaoferowane oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych, z których każda może mieć 32 porty szeregowo, 3 porty równoległe i 20 urządzeń USB.
12. Zaoferowane oprogramowanie musi wspierać minimum następujące systemy operacyjne: Windows Server 2012/2016/2019/2022, Windows 8/10/11, RHEL 6/7/8/9, SLES 12/15, Debian 10/11, CentOS 7/8, Ubuntu 16/18/20/22, Photon OS 2/3/4, Oracle Linux 6/7/8/9, FreeBSD 12/13.
13. W celu osiągnięcia maksymalnego współczynnika konsolidacji, zaoferowane oprogramowanie musi umożliwiać przydzielenie łącznie większej ilości pamięci RAM dla maszyn wirtualnych niż fizyczne zasoby RAM serwera, na którym maszyny te są posadowione.
14. Rozwiązanie musi umożliwiać udostępnienie maszynie wirtualnej większej ilości zasobów dyskowych niż jest fizycznie dostępne na zasobach dyskowych
15. Zaoferowane oprogramowanie musi umożliwiać integrację z rozwiązaniami antywirusowymi firm trzecich w zakresie skanowania maszyn wirtualnych z poziomu warstwy wirtualizacji bez ingerencji w systemy operacyjne maszyn wirtualnych (bezagentowość).
16. Zaoferowane oprogramowanie 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”
17. Zaoferowane oprogramowanie do wirtualizacji musi zapewnić możliwość powielania maszyn wirtualnych wraz z ich pełną konfiguracją i danymi
18. Zaoferowane oprogramowanie do wirtualizacji musi zapewnić możliwość wykonywania kopii migawkowych instancji systemów operacyjnych na potrzeby tworzenia kopii zapasowych bez przerywania ich pracy z możliwością konieczności zachowania stanu pamięci pracującej maszyny wirtualnej.
19. Konsola zarządzająca zaoferowanego oprogramowania musi posiadać możliwość przydzielania i konfiguracji uprawnień z możliwością integracji z usługami katalogowymi, minimalnie z: Microsoft Active Directory i Open LDAP oraz umożliwiać federacyjne zarządzanie tożsamością w oparciu o Microsoft Active Directory Federation Services (ADFS).
20. Zaoferowane oprogramowanie musi zapewniać możliwość dodawania zasobów w czasie pracy maszyny wirtualnej, w szczególności w zakresie ilości procesorów, pamięci operacyjnej i przestrzeni dyskowej
21. Zaoferowane oprogramowanie musi posiadać funkcjonalność tworzenia wirtualnego przełącznika (virtual switch) umożliwiającego tworzenie sieci wirtualnej w obszarze hosta (hypervisora wirtualizacyjnego) i pozwalającego połączyć tym przełącznikiem maszyny wirtualne w obszarze jednego hosta, a także na zewnątrz sieci fizycznej. Pojedynczy przełącznik wirtualny powinien mieć możliwość konfiguracji aż do 4096 portów
22. Pojedynczy wirtualny przełącznik w zaoferowanym oprogramowaniu, w celu zapewnienia bezpieczeństwa połączenia ethernetowego w razie awarii fizycznej karty sieciowej, musi posiadać możliwość przyłączania do niego minimum dwóch fizycznych kart sieciowych
23. Wirtualne przełączniki w zaoferowanym oprogramowaniu muszą posiadać funkcjonalność obsługi wirtualnych sieci lokalnych (VLAN)
24. Zaoferowane oprogramowanie musi umożliwiać wykorzystanie technologii przepustowości sieci komputerowych do 200GbE poprzez agregację połączeń fizycznych do minimalizacji czasu przenoszenia maszyny wirtualnej pomiędzy serwerami fizycznymi
25. Zaoferowane oprogramowanie do wirtualizacji musi obsługiwać przełączenie ścieżek LAN (bez utraty komunikacji) w przypadku awarii jednej ze ścieżek
26. Zaoferowane oprogramowanie musi zapewnić możliwość zdefiniowania alertów informujących o przekroczeniu wartości progowych
27. Zaoferowane oprogramowanie, w przypadku działania pod zarządcą klastra VMware vCenter, 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. Replikacja musi gwarantować współczynnik RPO (ang. Recovery Point Objective) na poziomie minimum 5 minut
28. Zaoferowane oprogramowanie do wirtualizacji musi obsługiwać przełączenie ścieżek SAN (bez utraty komunikacji) w przypadku awarii jednej ze ścieżek
29. Zaoferowane oprogramowanie, w przypadku działania pod zarządcą klastra VMware vCenter, musi mieć możliwość przenoszenia maszyn wirtualnych pomiędzy serwerami fizycznymi bez przerywania pracy usług na przenoszonych maszynach wirtualnych. Wymaga się wsparcia natywnego szyfrowania ruchu sieciowego dla maszyn wirtualnych podczas ich przenoszenia między serwerami fizycznymi
30. Zaoferowane oprogramowanie, w przypadku działania pod zarządcą klastra VMware vCenter oraz w środowisku z więcej niż pojedynczym wirtualizatorem, musi umożliwiać automatyczne, ponowne uruchomienie maszyn wirtualnych w przypadku awarii jednego z

- wirtualizatorów na kolejnym, działającym w tym samym klastrze wirtualizatorze (funkcjonalność HA) (ang. High Availability)
31. Zaoferowane oprogramowanie, w przypadku działania pod zarządcą klastra VMware vCenter w środowisku z minimalnie dwoma wirtualizatorami oraz w przypadku potrzeby wgrania aktualizacji do warstwy wirtualizacji, musi posiadać możliwość w przypadku wywołania startu aktualizacji, automatycznego przeniesienia bezprzerwowego działających maszyn wirtualnych do innego wirtualizatora nie objętego aktualizacją, przed rozpoczęciem samej aktualizacji
 32. Zaoferowane oprogramowanie musi posiadać co najmniej 2 niezależne mechanizmy wzajemnej komunikacji między serwerami z zainstalowanym wirtualizatorem oraz z serwerem zarządzającym, gwarantujące właściwe działanie mechanizmów wysokiej dostępności na wypadek izolacji sieciowej serwerów fizycznych lub partycjonowania sieci
 33. Zaoferowane oprogramowanie, w przypadku działania pod zarządcą klastra VMware vCenter, w środowisku z minimum dwoma wirtualizatorami, musi zapewniać pracę bez przestojów dla wybranych maszyn wirtualnych (o maksymalnie dwóch procesorach wirtualnych), niezależnie od systemu operacyjnego oraz aplikacji, podczas awarii wirtualizatora, bez utraty danych i dostępności danych na maszynach wirtualnych objętych ochroną
 34. Zaoferowane oprogramowanie do wirtualizacji musi zapewniać możliwość stworzenia dysku maszyny wirtualnej o wielkości 62 TB
 35. Zaoferowane oprogramowanie musi posiadać wbudowany interfejs programistyczny (API) zapewniający pełną integrację zewnętrznych rozwiązań wykonywania kopii zapasowych z istniejącymi mechanizmami warstwy wirtualizacyjnej
 36. Producent zaoferowanego oprogramowania do wirtualizacji musi wspierać rozwiązania do automatyzacji procesów oraz wirtualizacji sieci (SDN, ang. Software Defined Network).
 37. Zaoferowane oprogramowanie musi wspierać mechanizmy zaawansowanego uwierzytelniania do systemu operacyjnego wirtualnej maszyny za pomocą technologii Smart Card Reader
 38. Zaoferowane oprogramowanie musi wspierać TPM 2.0. Minimalne wymaganie Zamawiającego dla TPM oznacza, że TPM zapewnia mechanizm gwarantujący, że serwer fizyczny, na którym zainstalowane jest zaoferowane oprogramowanie, uruchomił się z włączoną opcją Secure Boot. Po potwierdzeniu, że Secure Boot jest włączone, system gwarantuje, poprzez weryfikację podpisu cyfrowego, że hypervisor uruchomił się w niezmienionej formie
 39. Wirtualizator w zaoferowanym oprogramowaniu musi mieć możliwość włączenia funkcji "Microsoft virtualization-based security", tzw. Microsoft VBS dla systemów operacyjnych maszyn wirtualnych opartych o system operacyjny Microsoft Windows 10, Microsoft Windows Server 2016 oraz Microsoft Windows Server 2019
 40. Zaoferowane oprogramowanie musi posiadać certyfikację FIPS-140-2 min. dla modułu jądra wirtualizatora odpowiedzialnego za szyfrowanie danych
 41. Zaoferowane oprogramowanie musi posiadać funkcjonalność wirtualnego TPM 2.0 dla maszyn wirtualnych z zainstalowanym Microsoft Windows 10 oraz Microsoft Windows 2016. Zamawiający wymaga, aby z punktu widzenia maszyny wirtualnej z systemem operacyjnym Microsoft Windows 10 lub Microsoft Windows 2016 wirtualny TPM widziany był jako standardowy TPM, gdzie można przechowywać bezpiecznie wrażliwe dane np. certyfikaty. Zawartość wirtualnego TPM musi być przechowywana w pliku przynależnym do maszyny wirtualnej oraz musi być szyfrowana.
 42. Zaoferowane oprogramowanie musi posiadać funkcjonalność szybkiego uruchamiania wirtualizatora po przeprowadzonym procesie jego aktualizacji. Zamawiający wymaga, aby w procesie aktualizacji wirtualizatora, jeśli wymagany jest jego restart, funkcjonalność szybkiego uruchamiania powodowała eliminację czasochłonnej fazy inicjalizacji serwera fizycznego
 43. Zaoferowane oprogramowanie, w przypadku działania pod zarządcą klastra, musi posiadać możliwość aktualizacji i kontroli wersji oprogramowania do wirtualizacji w ramach klastra serwerów z poziomu centralnej konsoli zarządzającej. Dodatkowo centralna konsola zarządzająca musi posiadać funkcjonalność aktualizacji firmware komponentów serwera fizycznego (dyski, kontrolery, karty sieciowe) z poziomu konsoli zarządzającej wirtualizatora. Konsola zarządzająca musi mieć możliwość automatycznej weryfikacji, czy zainstalowane komponenty serwera posiadają rekomendowaną wersję sterowników i firmware, eliminując ryzyko pracy na nieaktualnych wersjach. Taka funkcjonalność powinna być dostępna dla minimum dwóch producentów serwerów obecnych na rynku
 44. Zaoferowane oprogramowanie musi posiadać wsparcie dla natywnych dysków 4K
 45. Zaoferowane oprogramowanie musi wspierać protokół precyzyjnej synchronizacji czasu PTP (ang. Precision Time Protocol)
 46. Zaoferowane oprogramowanie, w przypadku działania pod zarządcą klastra, musi posiadać mechanizm, który ogranicza dostęp do indywidualnego zarządzania warstwą wirtualizacji

- na serwerach fizycznych w ramach klastra serwerów w celu utwardzenia/hardening (maksymalnego zwiększenia bezpieczeństwa dostępu) systemu wirtualizacji.
47. Zaoferowane oprogramowanie musi mieć funkcjonalność migracji w trybie rzeczywistym dysków działających maszyn wirtualnych z jednego podsystemu dyskowego do innego bez konieczności przerywania pracy maszyny wirtualnej, której dysk jest migrowany
 48. Zaoferowane oprogramowanie obejmuje walidację FIPS, a także zaktualizowane przewodniki audytów.
 49. Zaoferowane oprogramowanie musi mieć możliwość utworzenia, poprzez API, maszyny wirtualnej jako tzw. Instant Clone poprzez klonowanie działającej maszyny wirtualnej w wyniku którego powstanie nowa działająca maszyna wirtualna identyczna z klonowaną. Nowa maszyna wirtualna musi powstawać w pamięci operacyjnej wirtualizatora
 50. Zaoferowane oprogramowanie, w przypadku działania pod zarządcą klastra, musi mieć możliwość monitorowania i wyświetlania za pomocą grafu w konsoli bieżącego poboru energii elektrycznej dla hosta wirtualizacyjnego oraz dla maszyn wirtualnych na nim posadowionych
 51. Ilość instancji zaoferowanego oprogramowania do zarządzania klastrem wirtualizacyjnym musi być równa liczbie fizycznych core zaoferowanych w oprogramowaniu do wirtualizacji mocy obliczeniowej
 52. Zaoferowane oprogramowanie musi posiadać konsolę graficzną do zarządzania maszynami wirtualnymi i do konfigurowania innych funkcjonalności. min: zasobów dyskowych oraz zasobów sieci komputerowej. Konsola graficzna powinna działać jako zainstalowana aplikacja na maszynie wirtualnej. Dodatkowo wymaga się, aby maszyna z aplikacją była wstępnie skonfigurowana i dostępna jako tzw. virtual appliance. Instalacja w/w virtual appliance nie może wiązać się z potrzebą dostawy dodatkowego oprogramowania takiego jak np. system operacyjny lub baza danych.
 53. Zaoferowane oprogramowanie musi posiadać wbudowany serwer ściany ogniowej (ang. firewall) dający możliwość konfiguracji blokady lub akceptacji ruchu pomiędzy konsolą zarządzającą a serwerami oraz serwerami wirtualnymi na nich posadowionymi, przy założeniu blokowania całego ruchu a nie poszczególnych portów
 54. Zaoferowane oprogramowanie musi mieć możliwość konfiguracji uwierzytelniania użytkowników logujących się do niego w oparciu o minimum: domenę Microsoft Active Directory, Microsoft Active Directory over LDAP oraz Open LDAP.
 55. Zaoferowane oprogramowanie musi posiadać konsolę graficzną, która musi być dostępna poprzez dedykowanego klienta (za pomocą przeglądarek minimum Mozilla Firefox oraz Chrome) lub poprzez konsolę graficzną, która zbudowana jest z wykorzystaniem języka HTML5
 56. Zaoferowane oprogramowanie musi posiadać funkcjonalność zcentralizowanego zarządzania hostami VMware vSphere.
 57. Zaoferowane oprogramowanie musi posiadać natywne mechanizmy do wykonywania kopii zapasowej swojej konfiguracji. Dodatkowo wymaga się możliwości ustawienia harmonogramu wykonywania kopii zapasowej. Wymaga się aby kopie zapasowe wspierały protokoły: FTPS, HTTPS, SCP, FTP oraz http.
 58. Zaoferowane oprogramowanie, poprzez rozszerzenie o dodatkową licencję oferowaną przez tego samego producenta musi posiadać wbudowaną funkcjonalność zarządzania wirtualną przestrzenią dyskową SDS (ang. Software Defined Storage).
 59. Zaoferowane oprogramowanie musi posiadać interfejs graficzny do prowadzenia prac administracyjnych w zakresie swojej konfiguracji oraz monitoringu (możliwość monitorowania obciążenia min. vCPU, vRAM, vHDD, sieci, bazy danych). Interfejs graficzny powinien być wykonany w standardzie HTML5
 60. Zaoferowane oprogramowanie zawiera możliwość automatyzacji instalacji wielu konsoli zarządzania poprzez użycie schematów konfiguracji.
 61. Zaoferowane oprogramowanie umożliwia aktualizowanie wielu wirtualizatorów równocześnie.
 62. Rozwiązanie musi pozwalać na wykorzystanie łącz o szybkości do 100 GbE do bezawaryjnego przenoszenia maszyn wirtualnych między wirtualizatorami.
 63. Rozwiązanie musi zapewniać natywne mechanizmy wysokiej dostępności HA (ang. High Availability) w niezawodnej architekturze Active-Passive-Witness dla wszystkich składowych komponentów centralnej konsoli graficznej zarządzającej platformą wirtualną.
 64. Zaoferowane oprogramowanie zapewnia podstawowe funkcje serwera zarządzania kluczami (KMS), które upraszcza włączenie szyfrowania i zaawansowanych funkcji bezpieczeństwa.
 65. Zaoferowane oprogramowanie, w przypadku zarządzania serwerami opartymi o VMware vSphere, musi prezentować poziom zbalansowania mocy obliczeniowej w klastrze opartym o w/w wirtualizatory.

66. Dostęp przez przeglądarkę do konsoli graficznej w zaoferowanym oprogramowaniu musi być skalowalny tj. powinien umożliwiać rozdzielenie komponentów na wiele instancji w przypadku zapotrzebowania na dużą liczbę jednoczesnych dostępów administracyjnych do środowiska.

VI. MINIMALNE WYMAGANIA TECHNICZNE I FUNKCJONALNE DLA OPROGRAMOWANIA WINDOWS SERVER DATACENTER

1. Dla każdego z serwerów wirtualizacji należy dostarczyć wieczystą licencję typu Gov dla systemu operacyjnego Microsoft Windows Server Datacenter 2022 z możliwością przeniesienia licencji na inny serwer tego samego producenta.
2. Licencje na serwerowy system operacyjny muszą uprawniać do uruchamiania serwerowego systemu operacyjnego w środowisku fizycznym i nielimitowanej liczbie wirtualnych środowisk serwerowego systemu operacyjnego za pomocą wbudowanych mechanizmów wirtualizacji.
3. Dodatkowo musi pozwalać na uruchamianie wirtualnych środowisk serwerowego systemu operacyjnego w usłudze hostowanej platformy producenta serwerowego systemu operacyjnego.
4. Oferowane Produkty muszą być produktami standardowymi – powszechnie dostępnymi na rynku (typu Commercial off-the-shelf - COTS).
5. Zamawiający nie dopuszcza zaoferowania licencji w modelu CSP.
6. Licencja musi być z Software Assurance ważnym do 30.06.2028 r. Serwerowy system operacyjny musi posiadać następujące, wbudowane cechy:
 - a. Możliwość wykorzystania 512 logicznych procesorów oraz co najmniej 24 TB pamięci RAM w środowisku fizycznym.
 - b. Możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności do 64TB przez każdy wirtualny serwerowy system operacyjny.
 - c. Możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania 7000 maszyn wirtualnych.
 - d. 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.
 - e. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy.
 - f. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy.
 - g. Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.
 - h. Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading.
 - i. Wbudowane wsparcie instalacji i pracy na wolumenach, które:
 - i. pozwalają na zmianę rozmiaru w czasie pracy systemu,
 - ii. umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym)
 - iii. prosty wgląd w poprzednie wersje plików i folderów,
 - iv. umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów,
 - v. umożliwiają zdefiniowanie list kontroli dostępu (ACL).
 - j. Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.
 - k. Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.
 - l. Możliwość uruchamiania aplikacji internetowych wykorzystujących technologię ASP.NET
 - m. Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.
 - n. Wbudowana zaporę internetową (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.
 - o. Dostępne dwa rodzaje graficznego interfejsu użytkownika:
 - i. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,
 - ii. Dotykowy umożliwiający sterowanie dotykaniem na monitorach dotykowych.
 - p. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe.

- r. Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji.
- s. Mechanizmy logowania w oparciu o:
 - i. Login i hasło,
 - ii. Karty z certyfikatami (smartcard),
 - iii. Wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM),
- t. Możliwość wymuszania wieloelementowej dynamicznej kontroli dostępu dla: określonych grup użytkowników, zastosowanej klasyfikacji danych, centralnych polityk dostępu w sieci, centralnych polityk audytowych oraz narzuconych dla grup użytkowników praw do wykorzystywania szyfrowanych danych.
- u. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).
- v. Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.
- w. Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa.
- x. Pochodzący od producenta systemu serwis zarządzania polityką dostępu do informacji w dokumentach (Digital Rights Management).
- y. Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach.
- z. Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:
 - i. Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC,
 - ii. 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, udział sieciowy), z możliwością wykorzystania następujących funkcji:
 - 1. Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,
 - 2. Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza.
 - 3. Bezpieczny mechanizm dołączania do domeny uprawnionych użytkowników prywatnych urządzeń mobilnych opartych o iOS i Windows 8.1.
 - iii. Zdalna dystrybucja oprogramowania na stacje robocze,
 - iv. Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej,
 - v. Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:
 - 1. Dystrybucję certyfikatów poprzez http,
 - 2. Konsolidację CA dla wielu lasów domeny,
 - 3. Automatyczne rejestrowanie certyfikatów pomiędzy różnymi lasami domen,
 - 4. Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509.
 - vi. Szyfrowanie plików i folderów.
 - vii. Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec).
 - viii. Możliwość tworzenia systemów wysokiej dostępności (klastry typu failover) oraz rozłożenia obciążenia serwerów.
 - ix. Serwis udostępniania stron WWW.
 - x. Wsparcie dla protokołu IP w wersjach 4 oraz 6 (IPv4; IPv6).
 - xi. Wsparcie dla algorytmów Suite B (RFC 4869).
 - xii. Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows.
 - xiii. 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.

- xiv. Mechanizmy wirtualizacji mają zapewnić wsparcie dla:
 1. Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych,
 2. Obsługi ramek typu jumbo frames dla maszyn wirtualnych.
 3. Obsługi 4-KB sektorów dysków
 4. Nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra
 5. Możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API.
 6. Możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk mode)
- aa. Możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta serwerowego systemu operacyjnego umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet.
- bb. Wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath).
- cc. Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego.
- dd. Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji poprzez skrypty.
- ee. Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF.
- ff. Zorganizowany system szkoleń i materiały edukacyjne w języku polskim.

VII. MINIMALNE WYMAGANIA TECHNICZNE I FUNKCJONALNE DLA OPROGRAMOWANIA Baz Danych (SQL Server Enterprise Core ALng LSA 2L) z Software Assurance)

Licencja na System Bazodanowy (SBD) licencjonowany na rdzenie procesora w opcji nadającej się do użycia w jednostkach rządowych.

Oferowane Produkty muszą być produktami standardowymi – powszechnie dostępnymi na rynku (typu Commercial off-the-shelf - COTS).

Zamawiający nie dopuszcza zaoferowania licencji w modelu CSP.

Licencja musi być z Software Assurance ważnym do 30.06.2028 r.

Muszą spełniać poniższe wymagania poprzez wbudowane mechanizmy:

1. 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.
2. Zintegrowane narzędzia graficzne do zarządzania systemem - SBD musi dostarczać zintegrowane narzędzia do zarządzania i konfiguracji wszystkich usług wchodzących w skład systemu (baza relacyjna, usługi analityczne, usługi raportowe, usługi transformacji danych). Narzędzia te muszą udostępniać możliwość tworzenia skryptów zarządzających systemem oraz automatyzacji ich wykonywania.
3. Zarządzanie serwerem za pomocą skryptów - SBD musi udostępniać mechanizm zarządzania systemem za pomocą uruchamianych z linii poleceń skryptów administracyjnych, które pozwolą zautomatyzować rutynowe czynności związane z zarządzaniem serwerem.
4. Dedykowana sesja administracyjna - SBD musi pozwalać na zdalne połączenie sesji administratora systemu bazy danych w sposób niezależny od normalnych sesji klientów.
5. Wykonywanie typowych zadań administracyjnych w trybie on-line - SBD musi umożliwiać wykonywanie typowych zadań administracyjnych (indeksowanie, backup, odtwarzanie danych) bez konieczności przerywania pracy systemu lub przechodzenia w tryb jednoużytkownikowy.
6. Możliwość automatycznej aktualizacji systemu - SBD musi umożliwiać automatyczne ściąganie i instalację wszelkich poprawek producenta oprogramowania (redukowania zagrożeń powodowanych przez znane luki w zabezpieczeniach oprogramowania).
7. Skalowalność systemu - SBD powinien wspierać skalowanie w kontekście wielkości rozwiązania (powinien być dostępny zarówno na platformie wieloserwerowej, jak również średniej wielkości komputerów i urządzeń mobilnych).
8. Możliwość dodawania procesorów bez restartu systemu - SBD powinien umożliwiać dodanie procesora do systemu, bez konieczności restartu silnika bazy danych.

9. Kopie bazy tylko do odczytu - 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 z nich zapytań.
10. Możliwość dodawania pamięci bez restartu systemu - SBD powinien umożliwiać dodanie pamięci do systemu bez konieczności restartu silnika bazy danych.
11. SBD musi umożliwiać tworzenie klastrów niezawodnościowych. Powinien również umożliwiać tworzenie klastrów niezawodnościowych, których węzły znajdują się w różnych podsieciach komputerowych.
12. Wysoka dostępność - SBD musi posiadać mechanizm pozwalający na duplikację bazy danych między wieloma lokalizacjami (podstawowa i zapasowe) przy zachowaniu następujących cech:
 - a. bez specjalnego sprzętu (rozwiązanie tylko programowe oparte o sam SBD),
 - b. niezawodne powielanie danych w czasie rzeczywistym (potwierdzone transakcje bazodanowe),
 - c. duplikacja danych w trybie synchronicznym lub asynchronicznym,
 - d. SBD musi umożliwiać duplikację danych z ośrodka podstawowego, do co najmniej 8 lokalizacji zapasowych,
 - e. 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,
 - f. klienci bazy danych mogą być automatycznie przełączeni do bazy zapasowej w przypadku awarii bazy podstawowej bez zmian w aplikacjach,
 - g. brak limitu odległości między systemami (dopuszczalne są tylko limity w minimalnej wymaganej przepustowości łącza oraz limity wynikające z opóźnień na łączu),
 - h. kompresja danych przesyłanych między serwerem podstawowym i zapasowym (w celu minimalizacji obciążenia sieci),
 - i. system automatycznie naprawia błędy pamięci masowej (w przypadku odkrycia błędu fizycznego odczytu danych z pamięci masowej, poprawny fragment danych jest transferowany z drugiego systemu i korygowany).
13. Replikacja danych i modyfikacja w wielu punktach - 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.
14. Kompresja kopii zapasowych - SBD musi pozwalać na kompresję kopii zapasowej danych (backup) w trakcie jej tworzenia. Powinna to być cecha SBD niezależna od funkcji systemu operacyjnego ani od sprzętowego rozwiązania archiwizacji danych.
15. Możliwość automatycznego szyfrowania kopii bezpieczeństwa bazy danych przy użyciu między innymi certyfikatów lub kluczy asymetrycznych. System szyfrowania powinien wspierać następujące algorytmy szyfrujące: AES 128, AES 192, AES 256, Triple DES. Mechanizm ten nie może wymagać konieczności uprzedniego szyfrowania bazy danych.
16. Możliwość szyfrowania przechowywanych danych - 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. Kopia bezpieczeństwa szyfrowanej bazy także powinna być automatycznie zaszyfrowana.
17. Korzystanie z zewnętrznych urządzeń do przechowywania kluczy szyfrujących - SBD powinien posiadać mechanizm pozwalający na przechowywanie kluczy szyfrujących na urządzeniach zewnętrznych (np. czytniki kart). Rozwiązanie to powinno być otwarte, to znaczy pozwalać na dodawanie w przyszłości obsługi urządzeń nowych, oczywiście pod warunkiem dostarczenia przez producenta urządzenia odpowiednich modułów oprogramowania zgodnych z SBD.
18. Możliwość zastosowania reguł bezpieczeństwa obowiązujących w przedsiębiorstwie - wsparcie dla zdefiniowanej w przedsiębiorstwie polityki bezpieczeństwa (np. automatyczne wymuszanie zmiany haseł użytkowników, zastosowanie mechanizmu

- weryfikacji dostatecznego poziomu komplikacji haseł wprowadzanych przez użytkowników), możliwość zintegrowania uwierzytelniania użytkowników z Active Directory.
19. Możliwość definiowania reguł administracyjnych dla serwera lub grupy serwerów - SBD musi mieć możliwość definiowania reguł wymuszanych przez system i zarządzania nimi. Przykładem takiej reguły jest uniemożliwienie użytkownikom tworzenia obiektów baz danych o zdefiniowanych przez administratora szablonach nazw. Dodatkowo wymagana jest możliwość rejestracji i raportowania niezgodności działającego systemu ze wskazanymi regułami, bez wpływu na jego funkcjonalność.
 20. Ograniczenie użycia zasobów - SBD powinien posiadać wbudowany mechanizm ograniczający wykorzystanie zasobów systemu operacyjnego (% wykorzystania czasu procesora, % wykorzystania pamięci, liczba operacji wejścia/wyjścia podsystemu dyskowego). Reguły definiujące ograniczenia dla użytkowników lub grup użytkowników dotyczące wykorzystania zasobów powinny mieć możliwość użycia w nich logiki zaimplementowanej za pomocą języka programowania (np. używanego w danym SBD języka SQL).
 21. W celu zwiększenia wydajności przetwarzania system bazy danych musi posiadać wbudowaną funkcjonalność pozwalającą na rozszerzenie cache'u przetwarzania w pamięci RAM o dodatkową przestrzeń na dysku SSD.
 22. System bazy danych, w celu zwiększenia wydajności, musi zapewniać możliwość asynchronicznego zatwierdzania transakcji bazodanowych (lazy commit). Włączenie asynchronicznego zatwierdzania transakcji powinno być dostępne zarówno na poziomie wybranej bazy danych, jak również z poziomu kodu pojedynczych procedur/zapytań.
 23. W celu zwiększenia bezpieczeństwa i niezawodności system bazy danych powinien udostępniać komendę pozwalającą użytkownikowi na utrwalenie na dysku wszystkich zatwierdzonych asynchronicznych transakcji (lazy commit).
 24. System SDB musi łączyć w sobie cechy bazy przechowywanej w pamięci RAM (IMDB) oraz tradycyjnej bazy danych (RDBMS) przechowywanej na dyskach.
 25. System SDB musi zapewniać w ramach tej samej bazy danych możliwość umieszczenia wybranych tabel w pamięci RAM serwera, a pozostałych tabel w tradycyjnej postaci (na dysku).
 26. SBD musi posiadać możliwość korzystania w procedurach jednocześnie z tabel przechowywanych w pamięci RAM oraz tabel przechowywanych na dyskach.
 27. System SDB musi zapewniać wersjonowanie wierszy w tabelach przechowywanych w pamięci RAM.
 28. W celu zwiększenia wydajności SBD musi posiadać możliwość tworzenia procedur składowanych w kodzie natywnym, to znaczy takich procedur, które są automatycznie kompilowane do kodu natywnego podczas ich tworzenia oraz składają się z instrukcji procesora, które nie wymagają dalszych kompilacji lub interpretacji.
 29. Rejestrowanie zdarzeń silnika bazy danych w czasie rzeczywistym - SBD musi posiadać możliwość rejestracji zdarzeń na poziomie silnika bazy danych w czasie rzeczywistym w celach diagnostycznych, bez ujemnego wpływu na wydajność rozwiązania, pozwalać na selektywne wybieranie rejestrowanych zdarzeń (rejestrowanie tylko zdarzeń spełniających zdefiniowane warunki filtrujące, np. dotyczących tylko wskazanego obiektu). Wymagana jest rejestracja zdarzeń:
 - a. odczyt/zapis danych na dysku dla zapytań wykonywanych do baz danych (w celu wychwytywania zapytań znacząco obciążających system),
 - b. wykonanie zapytania lub procedury trwające dłużej niż zdefiniowany czas (wychwytywanie długo trwających zapytań lub procedur),
 - c. para zdarzeń zablokowanie/zwolnienie blokady na obiekcie bazy (w celu wychwytywania długotrwałych blokad obiektów bazy).
 30. Możliwość rejestrowania bardzo dużej liczby zdarzeń i analizowania ich z minimalnym opóźnieniem - SBD powinien dostarczać wbudowaną platformę do tworzenia aplikacji typu CEP (Complex Event Processing). Aplikacje takie umożliwiają rejestrowanie bardzo dużej liczby zdarzeń (np. odczytów liczników lub z innych urządzeń pomiarowych, dowolnych zdarzeń występujących z dużą częstotliwością) i reagowanie na nie z minimalnym opóźnieniem. System powinien również udostępniać mechanizmy wysokiej dostępności dla tej usługi.
 31. Zarządzanie pustymi wartościami w bazie danych - SBD musi efektywnie zarządzać pustymi wartościami przechowywanymi w bazie danych (NULL). W szczególności puste wartości wprowadzone do bazy danych powinny zajmować minimalny obszar pamięci.
 32. Definiowanie nowych typów danych - SBD musi umożliwiać definiowanie nowych typów danych wraz z definicją specyficzną 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.
33. Wsparcie dla technologii XML - SBD musi udostępniać mechanizmy składowania i obróbki danych w postaci struktur XML. W szczególności musi:
- udostępniać typ danych do przechowywania kompletnych dokumentów XML w jednym polu tabeli,
 - udostępniać mechanizm walidacji struktur XML-owych względem jednego lub wielu szablonów XSD,
 - udostępniać język zapytań do struktur XML,
 - udostępniać język modyfikacji danych (DML) w strukturach XML (dodawanie, usuwanie i modyfikację zawartości struktur XML),
 - udostępniać możliwość indeksowania struktur XML-owych w celu optymalizacji wykonywania zapytań.
34. Wsparcie dla danych przestrzennych - SBD musi zapewniać wsparcie dla 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:
- zapewniać możliwość wykorzystywania szerokości i długości geograficznej do opisu lokalizacji obiektów,
 - oferować wiele metod, które pozwalają na łatwe operowanie kształtami czy bryłami, testowanie ich wzajemnego ułożenia w układach współrzędnych oraz dokonywanie obliczeń takich wielkości, jak pola figur, odległości do punktu na linii, itp.,
 - obsługa geometrycznych i geograficznych typów danych powinna być dostępna z poziomu języka zapytań do systemu SBD,
 - typy danych geograficznych powinny być konstruowane na podstawie obiektów wektorowych, określonych w formacie Well-Known Text (WKT) lub Well-Known Binary (WKB), (powinny być to m.in. takie typy obiektów jak: lokalizacja (punkt), seria punktów, seria punktów połączonych linią, zestaw wielokątów, itp.).
35. Możliwość efektywnego przechowywania dużych obiektów binarnych - SBD powinien umożliwiać przechowywanie i efektywne zarządzanie dużymi obiektami binarnymi (pliki graficzne, multimedialne, dokumenty, itp.). 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). Dodatkowo dane binarne powinny być dostępne dla użytkowników bazy danych jako standardowa kolumna tabeli (dostęp z poziomu zapytań języka SQL obsługiwanego przez SBD).
36. Możliwość kompresji przechowywanych danych - SBD powinien udostępniać wbudowany mechanizm kompresji zgromadzonych danych w celu osiągnięcia lepszej wydajności przy niezmięnionej konfiguracji sprzętowej. System kompresji powinien umożliwiać również kompresję UNICODE systemem UCS-2.
37. Możliwość rejestracji zmiany w rekordzie danych - SBD powinien pozwalać na rejestrację zmian w danych łącznie z zapamiętaniem stanu pojedynczego rekordu danych sprzed modyfikacji. Rozwiązanie nie powinno ujemnie wpływać na wydajność systemu i powinno być konfigurowalne bez wpływu na istniejące aplikacje korzystające z danych. Rozwiązanie powinno rejestrować także zmiany w definicji struktur danych.
38. Audyt dostępu do danych - 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.
39. Partycjonowanie danych - SBD powinien pozwalać na 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. Dodatkowo powinna być dostępna możliwość szybkiego przesyłania dużych zbiorów danych poprzez mechanizm przełączania partycji (czyli dane przenoszone są z jednej tabeli do drugiej za pomocą operacji na metadanych, a nie przez fizyczne kopiowanie rekordów). Dzięki takiej funkcjonalności możliwe jest przeniesienie dużej liczby rekordów w bardzo krótkim czasie (rzędu sekund). Dodatkowo minimalizowane jest odczuwanie wpływu tej operacji przez użytkowników (minimalny wpływ przenoszenia danych na obciążenie systemu).

40. Wsparcie dla Indeksów kolumnowych - SBD powinien umożliwiać tworzenie indeksów przechowujących dane osobno dla każdej z kolumn tabeli łącząc je następnie w całość. Indeks powinien również wykorzystywać mechanizm kompresji oraz pozwalać na modyfikowanie danych w tabeli, dla której taki indeks utworzono.
41. Indeksowanie podzbioru danych w tabeli - SBD powinien umożliwiać tworzenie indeksów na podzbiorze danych z tabeli określonym poprzez wyrażenie filtrujące.
42. Możliwość tworzenia funkcji i procedur w innych językach programowania - SBD musi umożliwiać tworzenie procedur i funkcji z wykorzystaniem innych języków programowania, 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.
43. Możliwość tworzenia rekursywnych zapytań do bazy danych - SBD musi udostępniać wbudowany mechanizm umożliwiający tworzenie rekursywnych zapytań do bazy danych bez potrzeby pisania specjalnych procedur i wywoływania ich w sposób rekurencyjny.
44. Obsługa błędów w kodzie zapytań - język zapytań i procedur w SBD musi umożliwiać zastosowanie mechanizmu przechwytywania błędów wykonania procedury (na zasadzie bloku instrukcji TRY/CATCH) - tak jak w klasycznych językach programowania.
45. Raportowanie zależności między obiektami - SBD musi udostępniać informacje o wzajemnych zależnościach między obiektami bazy danych.
46. Mechanizm zamrażania planów wykonania zapytań do bazy danych - 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). Mechanizm ten daje możliwość zapewnienia przewidywalnego czasu odpowiedzi na zapytanie po przeniesieniu systemu na inny serwer (środowisko testowe i produkcyjne), migracji do innych wersji SBD, wprowadzeniu zmian sprzętowych serwera.
47. System transformacji danych - 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, pobranie danych z serwera FTP, wysłanie e-maila, łączenie danych z wykorzystaniem logiki rozmytej, poprawa jakości danych wykorzystująca integrację z dedykowanym systemem zarządzania jakością danych oraz jego bazą wiedzy i reguł walidujących. Powinna być także zapewniona możliwość tworzenia własnych transformacji. Środowisko tworzenia transformacji danych powinno udostępniać m.in.:
 - a. mechanizm debuggowania tworzonego rozwiązania,
 - b. mechanizm stawiania „pułapek” (breakpoints),
 - c. mechanizm logowania do pliku wykonywanych przez transformację operacji,
 - d. możliwość wznowienia wykonania transformacji od punktu, w którym przerwano jej wykonanie (np. w wyniku pojawienia się błędu),
 - e. możliwość cofania i ponawiania wprowadzonych przez użytkownika zmian podczas edycji transformacji (funkcja undo/redo)
 - f. mechanizm analizy przetwarzanych danych (możliwość podglądu rekordów przetwarzanych w strumieniu danych oraz tworzenia statystyk, np. histogram wartości w przetwarzanych kolumnach tabeli),
 - g. mechanizm automatyzacji publikowania utworzonych transformacji na serwerze bazy danych (w szczególności tworzenia wersji instalacyjnej pozwalającej automatyzować proces publikacji na wielu serwerach),
 - h. mechanizm tworzenia parametrów zarówno na poziomie poszczególnych pakietów, jak też na poziomie całego projektu, parametry powinny umożliwiać uruchamianie pakietów podrzędnych i przesyłanie do nich wartości parametrów z pakietu nadrzędnego,
 - i. mechanizm mapowania kolumn wykorzystujący ich nazwę i typ danych do automatycznego przemapowania kolumn w sytuacji podmiiany źródła danych,
 - j. możliwość integracji z transakcjami bazy danych SBD, także rozproszonymi bez potrzeby pisania kodu.
48. Wbudowany system analityczny - SBD musi posiadać moduł pozwalający na tworzenie rozwiązań służących do analizy danych wielowymiarowych (hurtownia danych).

System powinien umożliwiać pracę w dwóch trybach: wielowymiarowym (tworzenie kostek wielowymiarowych), tabelarycznym (wykorzystującym technologię in-memory BI). 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. Przykład: wymiar Lokalizacja Geograficzna. Atrybuty: miasto, gmina, województwo. Hierarchia: Województwo->Gmina.

49. Wbudowany system 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 - wyliczone gotowe agregacje rozłączenie w stosunku do danych źródłowych, ROLAP - agregacje wyliczane w trakcie zapytania z danych źródłowych). Pojedyncza baza analityczna musi mieć możliwość mieszania modeli składowania, np. dane bieżące ROLAP, historyczne - MOLAP w sposób przezroczysty dla wykonywanych zapytań. System powinien pozwalać na integrację z relacyjną bazą danych -wymagana jest możliwość uruchomienia procesu wyliczenia agregacji zainicjowana poprzez dodanie rekordu do tabeli w relacyjnej bazy danych. Dodatkowo powinna być dostępna możliwość drążenia danych z kostki do poziomu rekordów szczegółowych z bazy relacyjnych (drill to detail).
50. Wbudowany system analityczny musi pozwalać na dodanie akcji przypisanych do elementów kostek wielowymiarowych (np. pozwalających na przejście użytkownika do raportów kontekstowych lub stron www powiązanych z przeglądaniem obszarem kostki).
51. Narzędzia do zarządzania jakością danych - SBD powinien mieć wbudowane mechanizmy do zarządzania jakością danych w organizacji. W ramach tych funkcji powinien:
 - a. udostępniać funkcje do profilowania danych (analiza i raporty dotyczące jakości danych),
 - b. udostępniać funkcje do deduplikacji danych,
 - c. określać stopień poprawności wartości atrybutu i w przypadku błędnej wartości sugerować wartość poprawną do akceptacji przez użytkownika,
 - d. umożliwiać definiowanie osobnych reguł czyszczenia dla wybranych domen (typów atrybutów),
 - e. 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),
 - f. pozwalać na ręczną korektę nieprawidłowych danych w dedykowanej aplikacji (bez konieczności programowania),
 - g. 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,
 - h. przechowywać reguły walidujące i oceniające jakość danych w dedykowanej bazie danych (bazie wiedzy),
 - i. umożliwiać uzupełnianie i rozszerzanie bazy wiedzy o dane referencyjne pochodzące z systemów zewnętrznych,
 - j. 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,
 - k. 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).
52. Możliwość zarządzania centralnymi słownikami danych - SBD powinien dostarczać narzędzia do przechowywania i zarządzania centralnym słownikiem danych (Master Data Management - MDM). System MDM powinien:
 - a. udostępniać narzędzia do wprowadzania, modyfikacji i wyszukiwania danych w słownikach,
 - b. umożliwiać wersjonowanie danych (śledzenie zmian wprowadzonych przez użytkowników z możliwością ich cofnięcia do wybranej wersji),
 - c. udostępniać mechanizm tworzenia i uruchamiania reguł walidujących poprawność danych w słownikach,
 - d. udostępniać narzędzia do administracji i kontroli uprawnień dostępu do danych w MDM,
 - e. udostępniać zestaw bibliotek (API programistyczne) z funkcjonalnościami MDM do wykorzystania w aplikacjach użytkownika,
 - f. umożliwiać eksport danych zgromadzonych w systemie MDM,

- g. umożliwiać zarządzanie danymi podstawowymi z poziomu programu Microsoft Excel.
53. Wbudowany system analityczny powinien posiadać narzędzie do rejestracji i śledzenia zapytań wykonywanych do baz analitycznych.
 54. Wbudowany system analityczny musi umożliwiać rejestrowanie zapytań wykonywanych przez użytkowników, a następnie umożliwiać na podstawie zgromadzonych informacji na automatyczną optymalizację wydajności systemu (np. automatyczne projektowanie agregacji pozwalające na przyspieszenie wykonywania najczęściej wykonywanych zapytań do bazy danych).
 55. Wbudowany system analityczny powinien obsługiwać wielojęzyczność (tworzenie obiektów wielowymiarowych w wielu językach - w zależności od ustawień na komputerze klienta).
 56. Wbudowany system analityczny powinien udostępniać mechanizm zapisu danych przez użytkownika do kostek wielowymiarowych.
 57. Wbudowany system analityczny powinien umożliwiać tworzenie perspektyw na bazie wielowymiarowej pozwalających ograniczyć widok dla użytkownika tylko do pewnego podzbioru obiektów dostępnych w całej bazie danych.
 58. Wbudowany system 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.
 59. Wbudowany system analityczny powinien udostępniać dedykowany język do tworzenia logiki biznesowej w modelu. Język ten powinien m.in. obsługiwać relacje utworzone między tabelami, mechanizmy time intelligence (operacje na datach i okresach) oraz zapewniać mechanizmy kontroli bezpieczeństwa i dostępu do danych na poziomie poszczególnych wierszy.
 60. Wbudowany system analityczny powinien dostarczać kreatory modelowania złożonych procesów biznesowych, pozwalających w prosty sposób niezaawansowanym użytkownikom implementować złożone problemy analizy biznesowej w modelu analitycznym, czyniąc programowanie projektów BI przystępnym dla większej liczby osób i organizacji.
 61. Wsparcie dla optymalizacji zapytań z modelu gwiazdy (fakty-wymiary) - SBD powinien udostępniać mechanizmy optymalizacji zapytań w modelu gwiazdy (tabela faktów łączona z tabelami wymiarów). Zapytania te często wykorzystywane są w hurtowniach danych i analizach wielowymiarowych. Ze względu na dużą liczbę danych wykorzystywanych w tego typu zapytaniach metody optymalizacji tego typu zapytań pozwalają znacząco zwiększyć wydajność przy tworzeniu rozwiązań hurtowni danych i wielowymiarowych struktur analitycznych (OLAP).
 62. Wsparcie dla zapytań aktualizujących tabele faktów w modelach wielowymiarowych - 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.
 63. Aktywne buforowanie danych Proactive caching - SBD powinien udostępniać mechanizm odświeżania danych w strukturach wielowymiarowych, który wykrywa zmiany w systemach źródłowych i na bieżąco aktualizuje bazę wielowymiarową.
 64. Wbudowany system analityczny powinien zapewniać mechanizmy dynamicznego security (każdy z użytkowników modelu powinien widzieć tylko swoje dane).
 65. Wbudowany system analityczny powinien mieć wbudowaną funkcję importu tabelarycznych modeli danych wykorzystujących technologię in-memory BI i przygotowanych w aplikacji Microsoft Excel. Podczas procesu importu na serwerze model powinien być odtwarzany w postaci bazy danych.
 66. Wbudowany system analityczny powinien umożliwiać zasilanie modelu tabelarycznego m.in. z następujących systemów źródłowych: bazy relacyjne, bazy wielowymiarowe, modele tabelaryczne, zbiory danych przechowywane w usługach chmury publicznej, pliki płaskie, inne raporty udostępniane w formacie Atom 1.0.
 67. Wbudowany system analityczny powinien umożliwiać działanie modelu tabelarycznego w dwóch trybach - z użyciem buforowania (możliwe opóźnienie, ale większa wydajność) oraz bez użycia buforowania (zapytania użytkowników końcowych korzystających z modelu są przesyłane bezpośrednio do źródłowej bazy relacyjnej i zwracają najbardziej aktualną wersję danych).
 68. Wbudowany system analityczny musi udostępniać rozwiązania Data Mining, m.in.: algorytmy reguł związków (Association Rules), szeregów czasowych (Time Series), drzew regresji (Regression Trees), sieci neuronowych (Neural Nets oraz Naive Bayes).

- Dodatkowo system powinien udostępniać narzędzia do wizualizacji danych z modelu Data Mining oraz język zapytań do odpytywania tych modeli.
69. System analityczny powinien pozwalać na dodawanie własnych algorytmów oraz modułów wizualizacji modeli Data Mining.
 70. Tworzenie głównych wskaźników wydajności KPI (Key Performance Indicators) - 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.
 71. System raportowania - SBD musi posiadać możliwość definiowania i generowania raportów. Narzędzie do tworzenia raportów powinno pozwalać na ich graficzną definicję. Raporty powinny być udostępniane przez system protokołem HTTP (dostęp klienta za pomocą przeglądarki), bez konieczności stosowania dodatkowego oprogramowania po stronie serwera. Dodatkowo system raportowania powinien obsługiwać:
 - a. raporty parametryzowane,
 - b. cache raportów (generacja raportów bez dostępu do źródła danych),
 - c. cache raportów parametryzowanych (generacja raportów bez dostępu do źródła danych, z różnymi wartościami parametrów),
 - d. współdzielenie predefiniowanych zapytań do źródeł danych,
 - e. wizualizację danych analitycznych na mapach geograficznych (w tym import map w formacie ESRI Shape File),
 - f. możliwość opublikowania elementu raportu (wykresu, tabeli) we współdzielonej bibliotece, z której mogą korzystać inni użytkownicy tworzący nowy raport,
 - g. możliwość wizualizacji wskaźników KPI,
 - h. możliwość wizualizacji danych w postaci obiektów sparkline.
 72. Środowisko raportowania powinno być osadzone i administrowane z wykorzystaniem mechanizmu Web Serwisów (Web Services).
 73. Wymagane jest generowanie raportów w formatach: XML, PDF, Microsoft Excel, Microsoft Word, HTML, TIFF. Dodatkowo raporty powinny być eksportowane w formacie Atom data feeds, które można będzie wykorzystać jako źródło danych w innych aplikacjach.
 74. 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), mechanizmy zabezpieczeń dostępu do raportów.
 75. SBD musi umożliwiać wysyłkę raportów drogą mailową w wybranym formacie (subskrypcja) do dynamicznej listy odbiorców (pobieranej z bazy danych np. zapytaniem SQL).
 76. Wbudowany system raportowania powinien posiadać rozszerzalną architekturę oraz otwarte interfejsy do osadzania raportów oraz do integrowania rozwiązania z różnorodnymi środowiskami IT.
 77. Narzędzia do tworzenia raportów ad-hoc - SBD powinien udostępniać narzędzia do tworzenia raportów ad-hoc przez niezawansowanych 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.

VIII. MINIMALNE WYMAGANIA w ZAKRESIE WDROŻENIA SYSTEMU WRAZ Z PRZEPROWADZENIEM INSTRUKTAŻU

1. Dostarczenie i instalacja platformy wirtualizacji będzie realizowana we wskazanej lokalizacji. Sprzęt będący przedmiotem niniejszego zamówienia zostanie dostarczony do lokalizacji wskazanej przez Zamawiającego.
2. Dostarczenie platformy obejmuje dostawę wszelkich wymaganych do działania platformy oprogramowania oraz licencji/subskrypcji.
3. Konfigurację i uruchomienie urządzeń/elementów platformy wirtualizującej w środowisku Zamawiającego w terminie do 60 dni od podpisania umowy.
4. Wykonawca przeprowadzi instalację i konfigurację wszystkich elementów dostarczonej platformy wymaganej przez Zamawiającego.

5. Wszelkie prace konfiguracyjne muszą uwzględniać dobre praktyki i rekomendacje eksploatacyjne publikowane przez producenta dostarczonej infrastruktury sprzętowej oraz programowej.
6. Wdrożony klaster wirtualizacyjny musi być skonfigurowany tak, aby był w pełni funkcjonalny we wszystkich czterech aspektach: serwerowym, dyskowym, sieciowym i zarządzania.
7. Przed rozpoczęciem prac należy ustalić plan adresacji sieci IP. Ustalenia te będą prowadzone z wyznaczonym do tego celu pracownikiem/pracownikami Zamawiającego.
8. Zamawiający zapewni przestrzeń min. 15U w szafie RACK 19", zasilanie gwarantowane wraz z niezbędną ilością gniazd w listwach zasilających.
9. Zamawiający zapewni niezbędną ilość portów w standardzie 1000BASE-T na potrzeby zarządzania dostarczonym środowiskiem.
10. Prace wdrożeniowe klastra wirtualizacyjnego będą polegały w szczególności na:
 - a. montażu i podłączeniu fizycznym sprzętu w serwerowni (szafa RACK wskazana przez zamawiającego),
 - b. podłączeniu zasilania oraz sieci management,
 - c. aktualizacji oprogramowania układowego i jego komponentów wszystkich dostarczonych komponentów,
 - d. konfiguracji macierzy dyskowej, przełączników sieciowych,
 - e. konfiguracji systemu backupu Zamawiającego
 - f. hardeningu urządzeń oraz wdrażanego oprogramowania według najlepszych praktyk producenta,
 - g. niezbędnej rekonfiguracji istniejącej infrastruktury informatycznej (VLANY, routing, polityki firewalla, wpisy DNS),
 - h. aktywacji zakupionego oprogramowania oraz wszelkich subskrypcji i serwisów producenta,
 - i. konfiguracji oraz uruchomieniu klastra wirtualizacyjnego, opartego o dostarczane oprogramowanie wirtualizacyjne.
11. Wykonaniu testów akceptacyjnych (niezawodnościowe oraz funkcjonalne) oraz opracowaniu i przedstawieniu Raportu z testów Wykonanie dokumentacji powykonawczej wszystkich wdrożonych elementów.
12. Dokumentacja powykonawcza, musi w szczególności zawierać następujące elementy:
 - a. architektury logicznej,
 - b. architektury fizycznej,
 - c. architektury sieciowej,
 - d. konfiguracji klastra wirtualizacyjnego, zasobów dyskowych i sieci,
 - e. zestawienie wersji firmware zainstalowanych na dostarczonych urządzeniach,
 - f. zestawienie zakupionego i aktywowanego oprogramowania,
 - g. specyfikacja techniczna dostarczonego sprzętu,
 - h. schemat rozmieszczenia zainstalowanych urządzeń w szafach RACK i fizycznymi połączeniami między nimi,
 - i. tabele wykorzystanych adresów IP
 - j. zebrane informacje na temat obsługi wsparcia dostarczonych urządzeń, adresy url, nazwy kont do logowania, numery telefonów, adresy e-mail
13. Przeprowadzenie instruktażu
14. Wykonawca przeprowadzi instruktaż dla administratorów wskazanych przez Zamawiającego:
 - a) Instruktaż zostanie przeprowadzony w terminie uzgodnionym z Zamawiającym (jednak nie później niż 10 dni od daty wdrożenia), w jego siedzibie, tj. Plac Trzech Krzyży 3/5, 00-507 Warszawa.
Instruktaż powinien obejmować:
 - b) omówienie dostarczonego sprzętu i oprogramowania (parametry, funkcjonalności),
 - c) omówienie przeprowadzonych prac instalacyjno-konfiguracyjnych,
 - d) omówienie i weryfikację przygotowanych i dostarczonych procedur,
 - e) omówienie scenariuszy w przypadku wystąpienia błędów/awarii.

Przed ustalonym terminem instruktażu Wykonawca prześle Zamawiającemu zakres tematyczny/programu instruktażu. Zamawiający będzie miał prawo do weryfikacji

IX. MINIMALNE WYMAGANIA W ZAKRESIE GWARANCJI

Gwarancja dla oferowanych urządzeń i oprogramowania musi spełniać niżej opisane wymagania:

1. Minimalny okres gwarancji na urządzenia i oprogramowanie wskazany w Formularzu Oferowym
2. Zamawiający wymaga, aby usługa gwarancyjna na wszystkie dostarczone w ramach zamówienia sprzęt była, przez cały okres jej trwania, świadczona na podstawie wykupionego wsparcia producenta dostarczonych urządzeń, to jest by zapewniona była naprawa lub wymiana urządzeń lub ich części, na części nowe i oryginalne, zgodnie z metodyką i zaleceniami producenta dostarczanego urządzeń i był jego autoryzowanym dostawcą.
3. Wszystkie urządzenia dostarczone i zastosowane przez Wykonawcę będą pochodziły z autoryzowanego kanału sprzedaży producentów Urządzeń na rynek polski lub Unii Europejskiej. Spełnienie powyższego wymogu zostanie potwierdzone oświadczeniem producenta Urządzeń lub jego polskiego przedstawicielstwa, które Wykonawca zobowiązuje się dostarczyć Zamawiającemu najpóźniej w dniu dostawy oferowanych Urządzeń.
4. Gwarancja będzie liczona od daty odbioru przedmiotu umowy i oparta na gwarancji producentów rozwiązania. Serwis gwarancyjny świadczony ma być w miejscu instalacji Sprzętów.
5. Gwarancja ma być świadczona w reżimie 8x5xNBD. Czas naprawy Awarii liczony jest od czasu przesłania zgłoszenia o awarii do Wykonawcy zgodnie z procedurą przyjmowania zgłoszeń serwisowych.
6. Zamawiający dopuszcza świadczenie serwisu dla dostarczonych urządzeń poprzez zastosowanie zamienników wskazanych przez producenta tylko i wyłącznie w przypadku, gdy takiego wsparcia u producenta nie da się wykupić (np. produkty zostały wycofane przez producenta bez możliwości świadczenia serwisu).
7. W przypadku, gdy w okresie gwarancyjnym nastąpi trzykrotna naprawa wadliwego podzespołu Wykonawca niezwłocznie tj. w terminie nie dłuższym niż 14 dni liczonych od dnia zgłoszenia awarii, dokona jego wymiany na sprzęt nowy, wolny od wad. Na czas potrzebny do wymiany podzespołu wykonawca dostarczy element zastępczy o parametrach tożsamy z podzespołem uszkodzonym. Zamawiający oczekuje, iż w wypadku konieczności wymiany urządzenia, dyski na których zapisane są dane nieulotne wymienianego urządzenia pozostaną w siedzibie Zamawiającego.
8. Zamawiający otrzyma dostęp do pomocy technicznej Wykonawcy (telefon, e-mail lub www) w zakresie rozwiązywania problemów związanych z bieżącą eksploatacją dostarczonych urządzeń w godzinach pracy Zamawiającego.
9. Zamawiający zastrzega sobie prawo do dodawania nowych modułów oraz wymiany zainstalowanych modułów samodzielnie lub z pomocą Wykonawcy, w zakresie przewidzianym przez producenta Urządzenia, bez utraty gwarancji na zakupione Urządzenia. Zamawiający będzie dokonywał wymiany modułów samodzielnie po wcześniejszym uzgodnieniu z Wykonawcą. W przypadku nieprawidłowego lub niezgodnego z zaleceniami Wykonawcy i producenta Urządzenia dodania modułów lub wymiany zainstalowanych modułów przez Zamawiającego Wykonawca nie jest obciążony gwarancją i rękojmią w tym zakresie.
10. W okresie gwarancji Wykonawca w ramach otrzymanego wynagrodzenia udostępni Zamawiającemu możliwość wielokrotnego uaktualniania całego dostarczonego Oprogramowania do najnowszych wersji oferowanych przez producenta (włączając tzw. firmware) oraz pache i programy korekcji błędów, a także dostęp do usług wsparcia technicznego producenta właściwy dla danego Urządzenia lub Oprogramowania. W przypadku, gdy dostęp taki wymaga podania nazwy użytkownika, hasła lub numeru seryjnego Wykonawca dostarczy Zamawiającemu ww. przed podpisaniem protokołu odbioru Urządzeń.
11. W przypadku konieczności naprawy Urządzenia lub Oprogramowania poza Lokalizacją, Wykonawca pokrywa koszty transportu i ponosi ryzyko uszkodzenia lub przypadkowej utraty urządzenia lub oprogramowania Standardowego w przypadku konieczności naprawy poza siedzibą Zamawiającego.

12. Na okres przedłużającej się naprawy Wykonawca może stosować procedury zastępcze. Czas trwania procedur zastępczych nie może być dłuższy niż 45 dni kalendarzowe od chwili zgłoszenia awarii.
13. Przez usunięcie Awarii należy rozumieć przywrócenie pierwotnej funkcjonalności Systemu we wszystkich modułach i zaprzestanie stosowania w bieżącej prac rezerwowego Urządzenia i/lub procedur zastępczych.
14. Po usunięciu każdej Awarii, Wykonawca zobowiązuje się do doprowadzenia całego systemu do stanu integralnej całości w rozumieniu poprawnego działania wszystkich zainstalowanych komponentów.
15. W ramach gwarancji Zamawiający będzie miał prawo przez okres wskazany w formularzu ofertowym do:
 - a) pobierania i instalowania nowych wersji oprogramowania dla każdego elementu wchodzącego w skład oferty
 - b) Dostępu do bazy wiedzy oraz dokumentacji dostarczonych elementów
 - c) Dostępu do powiadomień/ogłoszeń/alarmów w zakresie dostarczonych elementów
 - d) Zgłaszania nieograniczonej liczby awarii systemu w trybie 24x365x7 za pomocą dedykowanego portalu i/lub zgłoszenia telefonicznego,
 - e) Wymiany uszkodzonych/wadliwych dostarczonych elementów w trybie NDB (Next-Business Day),
16. Czasy reakcji/naprawy na zgłoszenie będą na poziomie:
 - a) 1 godzina/8 godzin - błąd krytyczny – tj. przerwa w działaniu usług w środowisku produkcyjnym, brak dostępnego obejścia problemu,
 - b) 2 godziny/2 dni - błędy wysokie – tj. problem z poprawnym działaniem usługi znacząco utrudniający realizację procesów biznesowych, brak dostępnego obejścia problemu,
 - c) 4 godziny/7 dni - błędy średnie - tj. problem z poprawnym działaniem usługi, utrudnienie realizacji procesów biznesowych, dostępne obejście problemu,
 - d) 8 godzin/14 dni - błędy niskie – tj. problem z poprawnym działaniem usługi, brak wpływu na realizację procesów biznesowych.
17. Wykonawca do dostarczonych urządzeń, będących przedmiotem zamówienia, dołączy karty gwarancyjne zawierające numer seryjny, termin i warunki ważności gwarancji, adresy i numery telefonów punktów serwisowych świadczących usługi gwarancyjne.
18. Wykonawca w terminie 7 dni od zawarcia Umowy dostarczy Zamawiającemu procedury zgłaszania i obsługi Awarii wraz z listą osób upoważnionych do kontaktów, wykazem adresów poczty elektronicznej i nr telefonów.
19. Wykonawca, najpóźniej w dniu zawarcia Umowy, przedstawi do akceptacji Zamawiającemu listę osób uprawnionych do wykonywania czynności serwisowych.
20. W okresie gwarancji Wykonawca ponosi odpowiedzialność za poprawne funkcjonowanie urządzeń i oprogramowania stanowiącego przedmiot zamówienia, z zastrzeżeniem, że Wykonawca nie ponosi odpowiedzialności za uszkodzenia urządzeń i oprogramowania powstałych z wyłącznej winy Zamawiającego lub osób trzecich działających w jego imieniu.
21. Wymagany tryb zgłaszania wszelkich awarii, wad i błędów. Zgłoszenie następuje w drodze pisemnej mailem na adres podany przez Wykonawcę lub za pośrednictwem telefonicznego zgłaszania awarii, wad i błędów dotyczących sprzętu i oprogramowania w dni robocze w godzinach 8:00-17:00.
22. Zamawiający wymaga obsługi zgłoszeń w języku polskim.