Collegium Da Vinci
ul. Gen. Tadeusza Kutrzeby 10
61-719 Poznań
61 271 10 10 / info@cdv.pl
cdv.pl

Załącznik nr 1 do zapytania ofertowego nr 29/Z092 z dnia 11.08.2023 r.
Szczegółowy opis przedmiotu zamówienia

Przedmiot zamówienia: Dostarczenie kompletnego rozwiązania do obsługi klastra wysokiej dostępności składającego się z 2 serwerów oraz macierzy dyskowej wraz z wymaganym oprogramowaniem do jego obsługi.

1. Specyfikacja

Część 1:
Przedmiotem zamówienia jest dostarczenie kompletnego rozwiązania do obsługi klastra wysokiej dostępności składającego się z 2 serwerów oraz macierzy dyskowej (specyfikacja urządzeń w dalszej części dokumentu) wraz z wymaganym oprogramowaniem do jego obsługi w najnowszej, dostępnej wersji.
Ze względu na infrastrukturę zamawiającego najbardziej preferowane jest dostarczenie oprogramowania z rodziny Microsoft, tj:

- Windows Serwer 2022 Standard pokrywający wszystkie rdzenia procesora umożliwiając uruchomienie w ramach licencji do 4 maszyn wirtualnych z rodziny Windows Server na każdym z serwerów wraz z pakietem Software Assurance (wsparcie techniczne producenta) na okres 3 lat w polskiej wersji językowej lub produkt równoważny dla instytucji edukacyjnych.
- SQL Server 2022 Standard możliwego do uruchomienia na wszystkich rdzeniach serwera wraz z pakiem Software Assurance (wsparcie techniczne producenta) na okres 3 lat lub produkt równoważny dla instytucji edukacyjnej wraz z 30 licencjami dostępowymi dla użytkownika (tzw. User CAL).
- 250 licencji dostępowych do systemu Windows Server 2022 w wersji na urządzenie.
- pakietów subskrypcji Microsoft 365 A5 dla pracowników instytucji edukacyjnych na okres 12 miesięcy od daty dostawy. Zamówienie obejmuje 120 licencji/subskrypcji na użytkownika (lub równoważne) w formie SaaS w modelu licencjonowania CSP (Cloud Solution Provider). Zamawiający dopuszcza oferowanie produktów równoważnych spełniających wymagania funkcjonalne dotyczące zamówienia opisane szczegółowo w następnej części dokumentu.

SPECYFIKACJA SZCZEGÓŁOWA:

1. OPROGRAMOWANIE WINDOWS SERVER 2022 STANDARD – OPIS RÓWNOWAŻNOŚCI:

- Współpraca z procesorami o architekturze x64.
- Instalacja i użytkowanie aplikacji 32-bit. i 64-bit. na dostarczonym systemie operacyjnym.
- Możliwość budowania klastrów składających się z 64 węzłów.
- Pojedyncza licencja musi obsłużyć serwer fizyczny wyposażony w 2 procesory oraz 16 rdzeni.
- Praca w roli klienta domeny Microsoft Active Directory.
- Możliwość uruchomienia roli kontrolera domeny Microsoft Active Directory na poziomie Windows Server 2022.
- Możliwość federowania klastrów typu failover w zespół klastrów (Cluster Set) z możliwością przenoszenia maszyn wirtualnych wewnątrz zespołu.
- Możliwość uruchomienia roli klienta i serwera czasu (NTP).
- Możliwość uruchomienia roli serwera plików z uwierzytelnianiem i autoryzacją dostępu w domenie Microsoft Active Directory.
- Możliwość uruchomienia roli serwera wydruku z uwierzytelnieniem i autoryzacją dostępu w domenie Microsoft Active Directory.
- Możliwość uruchomienia roli serwera stron WWW.
- W ramach dostarczonej licencji zawarte prawo do użytkowania i dostęp do oprogramowania oferowanego przez producenta systemu operacyjnego umożliwiającego wirtualizowanie zasobów sprzętowych serwera.

Collegium Da Vinci
ul. Gen. Tadeusza Kutrzeby 10
61-719 Poznań
61 271 10 10 / info@cdv.pl
cdv.pl

- W ramach dostarczonych licencji zawarte prawo do instalacji i użytkowania systemu operacyjnego na co najmniej czterech maszynach wirtualnych na każdym z 2 serwerów.
- W ramach dostarczonej licencji zawarte prawo do pobierania poprawek systemu operacyjnego.
- Wszystkie wymienione w tabeli parametry, role, funkcje, itp. systemu operacyjnego objęte są dostarczoną licencją (licencjami) i zawarte w dostarczonej wersji oprogramowania (nie wymagają ponoszenia przez Zamawiającego dodatkowych kosztów).
- Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.
- Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy.
- Wbudowane wsparcie instalacji i pracy na wolumenach, które:
    - pozwalają na zmianę rozmiaru w czasie pracy systemu,
    - umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,
    - umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów,
    - umożliwiają zdefiniowanie list kontroli dostępu (ACL).
- Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.
- Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.
- Możliwość uruchamiania aplikacji internetowych wykorzystujących technologię ASP.NET.
- Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.
- Możliwość wykorzystania standardu http/2.
- Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.
- Dostępne dwa rodzaje graficznego interfejsu użytkownika:
    - klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,
    - dotykowy umożliwiający sterowanie dotykiem na monitorach dotykowych.
- Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe.
- Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji.
- Mechanizmy logowania w oparciu o:
    - login i hasło,
    - karty z certyfikatami (smartcard),
    - wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM).
- 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.
- Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).
- Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.
- Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa.
- Dostępny, pochodzący od producenta systemu serwis zarządzania polityką dostępu do informacji w dokumentach (Digital Rights Management).

Collegium Da Vinci
ul. Gen. Tadeusza Kutrzeby 10
61-719 Poznań
61 271 10 10 / info@cdv.pl
cdv.pl

- Wsparcie dla środowisk Java i .NET Framework 4.x i wyższych - możliwość uruchomienia aplikacji działających we wskazanych środowiskach.
- Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:
    - Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC.
    - 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:
        - Podłączenie do domeny w trybie offline - bez dostępnego połączenia sieciowego z domeną, o Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika - na przykład typu certyfikatu użytego do logowania,
        - Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza.
        - Bezpieczny mechanizm dołączania do domeny uprawnionych użytkowników prywatnych urządzeń mobilnych opartych o iOS i Windows.
    - Zdalna dystrybucja oprogramowania na stacje robocze.
    - Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej z możliwością dostępu minimum 65 tys. Użytkowników.
    - Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:
        - Dystrybucję certyfikatów poprzez http, o Konsolidację CA dla wielu lasów domeny,
        - Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen,
        - Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509.
    - Szyfrowanie plików i folderów.
    - Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec)
    - Szyfrowanie sieci wirtualnych pomiędzy maszynami wirtualnymi
    - Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów
    - Serwis udostępniania stron WWW
    - Wsparcie dla protokołu IP w wersji 6 (IPv6).
    - Wsparcie dla algorytmów Suite B (RFC 4869).
    - Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows.
    - Wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie do 1000 aktywnych środowisk wirtualnych systemów operacyjnych.
    - Możliwość migracji maszyn wirtualnych między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci.
    - Możliwość przenoszenia maszyn wirtualnych pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności.
    - Mechanizmy wirtualizacji mające wsparcie dla:
        - dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych, o możliwość obsługi ramek typu jumbo frames dla maszyn wirtualnych
        - nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra, o możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API. o możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw.

Collegium Da Vinci
ul. Gen. Tadeusza Kutrzeby 10
61-719 Poznań
61 271 10 10 / info@cdv.pl
cdv.pl

trunk mode) możliwość tworzenia wirtualnych maszyn chronionych, separowanych od środowiska systemu operacyjnego.
- Możliwość uruchamiania kontenerów bazujących na Windows i Linux na tym samym hoście kontenerów.
- Wsparcie dla rozwiązania Kubernetes.
- 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.
- Wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath).
- Mechanizmy deduplikacji i kompresji na wolumenach do 64 TB.
- Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego.
- Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.
- Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF
- Mechanizm konfiguracji połączenia VPN do platformy Azure.
- Wbudowany mechanizm wykrywania ataków na poziomie pamięci RAM i jądra systemu.
- Mechanizmy pozwalające na blokadę dostępu nieznanych procesów do chronionych katalogów.
- Zorganizowany system szkoleń i materiały edukacyjne w języku polskim.
- Możliwość instalacji i poprawnej pracy Systemu Bazodanowego (Microsoft SQL Server Standard).
- W przypadku zaproponowania licencji równoważnych Wykonawca przeprowadzi na własny koszt instalację, konfigurację i integrację dostarczonego produktu. Wykonawca przeprowadzi migrację wszelkich danych i konfiguracji zapewniając identyczne funkcjonowanie całego środowiska w stosunku do aktualnego środowiska. Przerwa w działaniu aktualnie eksploatowanego środowiska produkcyjnego nie może wynieść więcej niż 7 godzin. Dodatkowo w przypadku błędnego działania środowiska po instalacji licencji równoważnych, Wykonawca zobowiązany będzie na własny koszt przywrócić środowisko do stanu poprawnego funkcjonowania, a w przypadku braku takiej możliwości do stanu pierwotnego oraz dostarczenia innego rozwiązania spełniającego wymagania określone w zapytaniu ofertowym.
- Ponadto zastosowanie rozwiązania równoważnego nie może ograniczyć funkcjonalności posiadanego systemu przez Zamawiającego i nie może powodować konieczności ponoszenia dodatkowych kosztów dla Zamawiającego.

- Możliwość dokupienia wsparcia technicznego producenta na okres co najmniej 3 lat umożliwiający darmową aktualizację systemu do nowszej wersji.

2. Microsoft SQL Server Standard 2022 – OPIS RÓWNOWAŻNOŚCI:

- Licencje dla instytucji edukacyjnej
- Licencje muszą być licencjami bezterminowymi
- Licencje muszą być swobodnie przenoszone pomiędzy serwerami
- Licencje muszą zapewniać możliwość korzystania z wcześniejszych wersji zamawianego oprogramowania i korzystania z kopii zamiennych
- Oferowane licencje muszą być fabrycznie nowe, zakupione w autoryzowanym kanale dystrybucji producenta – nie dopuszcza się licencji pochodzących z rynku wtórnego,
- Zamawiający wymaga, aby dostarczone licencje posiadały stosowne atrybuty legalności, np. z tzw. naklejkami GML (Genuine Microsoft Label) lub naklejkami COA (Certificate of Authenticity) lub inną formą uwiarygodnienia oryginalności wymaganą przez producenta oprogramowania. Zamawiający na każdym etapie realizacji niniejszego zamówienia zastrzega sobie prawo sprawdzenia, czy dostarczone licencje są oryginalne i legalne.

Collegium Da Vinci
ul. Gen. Tadeusza Kutrzeby 10
61-719 Poznań
61 271 10 10 / info@cdv.pl
cdv.pl

System bazodanowy (SBD) licencjonowany na rdzenie procesora musi spełniać poniższe wymagania poprzez wbudowane mechanizmy:

- 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.
- 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.
- 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.
- Dedykowana sesja administracyjna - SBD musi pozwalać na zdalne połączenie sesji administratora systemu bazy danych w sposób niezależny od normalnych sesji klientów.
- 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.
- Możliwość automatycznej aktualizacji systemu - SBD musi umożliwiać automatyczne ściąganie i instalację wszelkich poprawek producenta oprogramowania (redukowania zagrożeń powodowanych przez znane luki w zabezpieczeniach oprogramowania).
- 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).
- Możliwość dodawania procesorów wirtualnych bez restartu SBD. SBD powinien umożliwiać dodanie procesora wirtualnego do systemu, bez konieczności restartu silnika bazy danych.
- 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.
- SBD musi umożliwiać tworzenie klastrów niezawodnościowych. Powinien również umożliwiać tworzenie klastrów niezawodnościowych, których węzły znajdują się w różnych podsieciach komputerowych.
- Wysoka dostępność - SBD musi posiadać mechanizm pozwalający na replikację 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);
    - replikacja danych w trybie synchronicznym lub asynchronicznym;
    - SBD musi umożliwiać replikację danych z ośrodka podstawowego, do co najmniej 8 lokalizacji zapasowych;
    - SBD musi umożliwiać replikację danych z ośrodka podstawowego, do co najmniej 4 lokalizacji zapasowych w trybie synchronicznym;
    - 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 replikacji 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 między 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);

Collegium Da Vinci
ul. Gen. Tadeusza Kutrzeby 10
61-719 Poznań
61 271 10 10 / info@cdv.pl
cdv.pl

  - 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).
- 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.
- 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.
- 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.
- 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. Szyfrowanie danych musi też obejmować szyfrowanie kolumn i komórek w bazie (Column/Cell-level Encryption) Zaszyfrowanie lub odszyfrowanie danych nie powinno powodować przerwy w dostępie do danych. Kopia bezpieczeństwa szyfrowanej bazy także powinna być automatycznie zaszyfrowana.
- Możliwość szyfrowania ruchu sieciowego z i do SBD (TLS encrypted connections).
- 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.
- 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.
- 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.
- System SBD musi łączyć w sobie cechy bazy przechowywanej w pamięci RAM (IMDB) oraz tradycyjnej bazy danych (RDBMS) przechowywanej na dyskach.
- System SBD musi zapewniać w ramach tej samej bazy danych możliwość umieszczenia wybranych tabel w pamięci RAM serwera, a pozostałych tabel w tradycyjnej postaci (na dysku).
- SBD musi posiadać możliwość korzystania w procedurach jednocześnie z tabel przechowywanych w pamięci RAM oraz tabel przechowywanych na dyskach.
- System SBD musi zapewniać wersjonowanie wierszy w tabelach przechowywanych w pamięci RAM.
- 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 podczasich tworzenia oraz składają się z instrukcji procesora, które nie wymagają dalszych kompilacji lub interpretacji.

Collegium Da Vinci
ul. Gen. Tadeusza Kutrzeby 10
61-719 Poznań
61 271 10 10 / info@cdv.pl
cdv.pl

- 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.
- Możliwość efektywnego przechowywania dużych obiektów binarnych większych niż 20 MBSBD 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).
- 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.
- Partycjonowanie danych (tabel i indeksów) - 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).
- 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 debugowania.
- 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.
- Raportowanie zależności między obiektami - SBD musi udostępniać informacje o wzajemnych zależnościach między obiektami bazy danych.
- 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.
- 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 rozłącznie 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).
- Wbudowany system analityczny powinien posiadać narzędzie do rejestracji i śledzenia zapytań wykonywanych do baz analitycznych.

Collegium Da Vinci
ul. Gen. Tadeusza Kutrzeby 10
61-719 Poznań
61 271 10 10 / info@cdv.pl
cdv.pl

- 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).
- Wbudowany system analityczny powinien obsługiwać wielojęzyczność (tworzenie obiektów wielowymiarowych w wielu językach – w zależności od ustawień na komputerze klienta).
- Wbudowany system analityczny powinien udostępniać mechanizm zapisu danych przez użytkownika do kostek wielowymiarowych.
- 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.
- Wbudowany system analityczny powinien umożliwiać użytkownikom tworzenie analiz InMemory, 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.
- 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.
- 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).
- 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.
- 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).
- 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.
- Środowisko raportowania powinno być osadzone i administrowane z wykorzystaniem mechanizmu Web Serwisów (Web Services).
- Wymagane jest generowanie raportów w formatach: XML, PDF, Microsoft Excel, Microsoft Word, HTML, TIFF, PowerPoint.
- 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.
- Wbudowany system raportowania powinien posiadać rozszerzalną architekturę oraz otwarte interfejsy do osadzania raportów oraz do integrowania rozwiązania z różnorodnymi środowiskami IT.
- SBD musi mieć wbudowane mechanizmy umożliwiające wirtualizację danych (czyli przetwarzanie zapytań na danych niezależnie od miejsca przechowywania tych danych). W ramach wirtualizacji danych powinny być obsługiwane m.in. następujące platformy przechowywania danych źródłowych: MongoDB, Oracle, Teradata, Microsoft SQL Server, Hadoop, Azure Blob Storage.

Collegium Da Vinci
ul. Gen. Tadeusza Kutrzeby 10
61-719 Poznań
61 271 10 10 / info@cdv.pl
cdv.pl

- SBD musi mieć możliwość budowy klastrów obliczeniowych dedykowanych do przetwarzania dużych zbiorów danych (big data, data lake) w oparciu o technologie SQL, Spark i HDFS. SBD musi umożliwiać odpytywanie danych z wielu źródeł, składowanie dużych zbiorów danych w HDFS, skalowanie wydajnościowe klastrów obliczeniowych wykorzystujące konteneryzację.
- SBD musi posiadać pełne wsparcie kodowania znaków UTF-8.
- SBD musi umożliwiać wdrażanie i zarządzanie certyfikatami SSL\TLS.
- SDB musi umożliwiać nadawanie granularnych ról i uprawnień w zakresie całej instancji serwera bazodanowego, pojedynczych baz danych, pojedynczych obiektów w bazie danych (np. tabel, widoków) oraz pojedynczych wierszy (tzw. Row-Level Security).

3. Licencje dostępowe Device CAL 2022 do Windows Server Standard 2022 – 250 licencji:

- dla 250 urządzeń
- bez terminu wygaśnięcia
- z możliwością przenoszenia
- używane w celu dostępu do systemu Windows Server 2022 lub starszego
- Zamawiający wymaga, aby oferowane licencje były fabrycznie nowe, nieużywane oraz nieaktywowane nigdy wcześniej na innym urządzenia – nie dopuszcza się licencji pochodzących z rynku wtórnego,
- Zamawiający wymaga, aby dostarczone licencje posiadały stosowne atrybuty legalności, np. z tzw. naklejkami GML (Genuine Microsoft Label) lub naklejkami COA (Certificate of Authenticity) lub inną formą uwiarygodnienia oryginalności wymaganą przez producenta oprogramowania. Zamawiający na każdym etapie realizacji niniejszego zamówienia zastrzega sobie prawo sprawdzenia, czy dostarczone licencje są oryginalne i legalne.

4. Microsoft 365 A5 (subskrypcja na użytkownika) – opis równoważności:

Subskrypcja powszechnie dostępnej, standardowej usługi hostowanej (on-line) typu COTS (Commercial Of-The-Shelf) ma uprawniać użytkowników posiadających subskrypcję do wykorzystania usług on-line – usługi zarządzania tożsamością użytkowników i uwierzytelniania, portalu wewnętrznego, poczty elektronicznej, narzędzi wiadomości błyskawicznych, konferencji głosowych i video, repozytorium dokumentów, wewnętrznego serwisu społecznościowego oraz edycji dokumentów biurowych on-line (dalej Usługi). Ponadto musi zawierać subskrypcję pakietu biurowego.
Wymagania dotyczące usługi hostowanej:

- Wszystkie elementy Usługi muszą pozwalać na dostęp użytkowników na zasadzie niezaprzeczalnego uwierzytelnienia wykorzystującego mechanizm logowania pozwalający na autoryzację użytkowników w usłudze poprzez wbudowaną usługę zarządzania tożsamością użytkowników
- Wbudowana usługa zarządzania tożsamością użytkowników musi umożliwiać realizację pojedynczego logowania (single sign-on) dla użytkowników logujących się do własnej usługi katalogowej Active Directory.
- Dostępność portalu administracyjnego do zarządzania Usługą oraz zasadami grup.
- Wbudowane mechanizmy ochrony informacji z mechanizmami śledzenia wycieków informacji z poczty elektronicznej i przechowywanych plików.
- Ochrona danych w systemie poczty elektronicznej przed złośliwym oprogramowaniem i wirusami oraz atakami typu zero-day.
- Gwarantowana dostępność usług platformy na poziomie 99,9%.
- Zastosowanie w Platformie powszechnie uznanych i rozpowszechnionych standardów przemysłowych, pozwalających na potencjalne wykorzystanie różnych technologii i rozwiązań w ramach jednej platformy, w szczególności:
    - ISO 27001, ISO 27002, ISO 27017, ISO 27018
    - UK G-Cloud

Collegium Da Vinci
ul. Gen. Tadeusza Kutrzeby 10
61-719 Poznań
61 271 10 10 / info@cdv.pl
cdv.pl

  - SOC 1, SOC 2
  - Open Authentication Standard – OAuth
- Dostępność mechanizmów pełnej rozliczalności działań użytkowników w usługach platformy.
- Dostępność na żądanie wyników aktualnych audytów, w tym audytów bezpieczeństwa, dla usług i centrów przetwarzania danych oferujących te usługi i audytów związanych z certyfikatami ISO.
- Dostępność mechanizmów monitorowania zachowań użytkowników usługi oraz prób dostępu do przetwarzanych/składowanych w usłudze danych Zamawiającego.
- Możliwość realizacji uwierzytelnienia za pomocą modelu pojedynczego logowania (single sign-on) na bazie własnej usługi katalogowej Active Directory.
- Dostępność mechanizmu uwierzytelnienia wieloskładnikowego.
- Dostępność logów informujących o wszystkich zdarzeniach uwierzytelnienia do usług i danych Zamawiającego, zakończonych powodzeniem lub niepowodzeniem oraz prób uwierzytelnienia przy pomocy tożsamości będących na listach „wykradzione".
- Dostępność raportów odnośnie logów z urządzeń potencjalnie zainfekowanych, z sieci botnetowych.
- Wbudowane w platformę mechanizmy zabezpieczające przez atakami DDoS.
- Przynajmniej dwa równorzędne ośrodki przetwarzania danych, odległe od siebie o co najmniej 100 km.
- W okresie obowiązywania subskrypcji Usługa będzie przechowywać dane i umożliwiać uprawnione przetwarzanie danych, które pozostają wyłączną własnością Zamawiającego. Po zakończeniu okresu subskrypcji, w przypadku podjęcia decyzji o braku jej kontynuacji, Usługa będzie przechowywać dane Zamawiającego, które zostały w niej zapisane, na koncie o ograniczonej funkcjonalności przez 90 dni od daty wygaśnięcia lub wypowiedzenia subskrypcji w celu umożliwienia ich odzyskania. Po upływie tego 90-dniowego okresu przechowywania konto związane z subskrypcją Usługi zostanie wyłączone a dane Zamawiającego zostaną usunięte.
- Dostęp do Usługi musi być możliwy z dowolnego urządzenia klasy PC, tabletu lub telefonu wyposażonego w system operacyjny Linux, Windows lub Apple OS.
- Subskrypcja ma uprawniać użytkownika do instalacji pakietu biurowego na minimum 5 urządzeniach klienckich.
- Subskrypcja Usługi musi umożliwiać zmianę jej przypisania do innego użytkownika będącego pracownikiem Zamawiającego.
- Centra przetwarzania świadczące Usługę muszą znajdować się na terenie Europejskiego Obszaru Gospodarczego.
- Usługa musi odpowiadać wymaganiom prawa Europejskiego w zakresie ochrony danych osobowych w tym realizować zapisy Decyzji Komisji Europejskiej z dnia 5 lutego 2010 r. w sprawie standardowych klauzul umownych.
- Usługa musi zapewniać szyfrowanie danych przesyłanych za pomocą sieci publicznych.
- Usługa ma zapewniać usunięcie danych Zamawiającego po zakończeniu okresu jej subskrypcji.
- Zobowiązania umowne potwierdzające zgodność z rozp. RODO i potwierdzające rolę operatora usługi jako współprzetwarzającego dane.
- Zobowiązanie umowne o pozostawieniu całkowitej własności przetwarzanych/składowanych w usłudze danych po stronie Zamawiającego.
- Mechanizmy pozwalające na realizację wymagań rozliczalności i monitorowania użytkowników i usług.
- Gwarancja braku dostępu do danych Zamawiającego na Platformie, z wyłączeniem działań serwisowych wymagających każdorazowo zgody zamawiającego i wykonywanych wyłącznie przez uprawnione osoby z organizacji dostawcy Platformy.

Usługa poczty elektronicznej on-line musi spełniać następujące wymagania:

- Usługa musi umożliwiać:
  - obsługę poczty elektronicznej,
  - zarządzanie czasem,

Collegium Da Vinci
ul. Gen. Tadeusza Kutrzeby 10
61-719 Poznań
61 271 10 10 / info@cdv.pl
cdv.pl

  - zarządzania zasobami
  - zarządzanie kontaktami i komunikacją.
- Usługa musi dostarczać kompleksową funkcjonalność zdefiniowaną w opisie oraz narzędzia administracyjne:
  - Zarządzania użytkownikami poczty,
  - Wsparcia migracji z innych systemów poczty,
  - Wsparcia zakładania kont użytkowników na podstawie profili własnych usług katalogowych,
  - Wsparcia integracji własnej usługi katalogowej (Active Directory) z usługą hostowana poczty.

Dostęp do usługi hostowanej systemu pocztowego musi być możliwy przy pomocy:
- Posiadanego oprogramowania Outlook,
- Przeglądarki (Web Access),
- Urządzeń mobilnych.

Wymagane cechy usługi to:
- Skrzynki pocztowe dla każdego użytkownika o pojemności minimum 40 GB,
- Standardowy i łatwy sposób obsługi poczty elektronicznej,
- Obsługa najnowszych funkcji Outlook, w tym tryb konwersacji, czy znajdowanie wolnych zasobów w kalendarzach, porównywanie i nakładanie kalendarzy, zaawansowane wyszukiwanie i filtrowanie wiadomości, wsparcie dla Internet Explorer, Firefox i Safari,
- Współdziałanie z innymi produktami takimi jak portal wielofunkcyjny czy serwer komunikacji wielokanałowej, a co za tym idzie uwspólnianie w obrębie wszystkich produktów statusu obecności, dostępu do profilu (opisu) użytkownika, wymianę informacji z kalendarzy.
- Bezpieczny dostęp z każdego miejsca, w którym jest dostępny internet

Usługa poczty elektronicznej on-line musi się opierać o serwery poczty elektronicznej charakteryzujące się następującymi cechami, bez konieczności użycia rozwiązań firm trzecich:
- Funkcjonalność podstawowa:
  - Odbieranie i wysyłanie poczty elektronicznej do adresatów wewnętrznych oraz zewnętrznych
  - Mechanizmy powiadomień o dostarczeniu i przeczytaniu wiadomości przez adresata Tworzenie i zarządzanie osobistymi kalendarzami, listami kontaktów, zadaniami, notatkami
  - Zarządzanie strukturą i zawartością skrzynki pocztowej samodzielnie przez użytkownika końcowego, w tym: organizacja hierarchii folderów, kategoryzacja treści, nadawanie ważności, flagowanie elementów do wykonania wraz z przypisaniem terminu i przypomnienia
  - Wsparcie dla zastosowania podpisu cyfrowego i szyfrowania wiadomości.

- Funkcjonalność wspierająca pracę grupową:
  - Możliwość przypisania różnych akcji dla adresata wysyłanej wiadomości, np. do wykonania czy do przeczytania w określonym terminie.
  - Możliwość określenia terminu wygaśnięcia wiadomości
  - Udostępnianie kalendarzy osobistych do wglądu i edycji innym użytkownikom, z możliwością definiowania poziomów dostępu
  - Podgląd stanu dostępności innych użytkowników w oparciu o ich kalendarze
  - Mechanizm planowania spotkań z możliwością zapraszania wymaganych i opcjonalnych uczestników oraz zasobów (np. sala, rzutnik), wraz z podglądem ich dostępności, raportowaniem akceptacji bądź odrzucenia zaproszeń, możliwością proponowania alternatywnych terminów spotkania przez osoby zaproszone
  - Mechanizm prostego delegowania zadań do innych pracowników, wraz ze śledzeniem statusu ich wykonania Tworzenie i zarządzanie współdzielonymi repozytoriami kontaktów, kalendarzy, zadań
  - Obsługa list i grup dystrybucyjnych.
  - Dostęp ze skrzynki do poczty elektronicznej, poczty głosowej i wiadomości błyskawicznych.

Collegium Da Vinci
ul. Gen. Tadeusza Kutrzeby 10
61-719 Poznań
61 271 10 10 / info@cdv.pl
cdv.pl

- Możliwość informowania zewnętrznych partnerów biznesowych o dostępności lub niedostępności, co umożliwia szybkie i wygodne ustalane harmonogramu.
- Możliwość wyboru poziomu szczegółowości udostępnianych informacji o dostępności.
- Widok rozmowy, który ułatwia nawigację w skrzynce odbiorczej, automatycznie organizując wątki wiadomości w oparciu o przebieg rozmowy między stronami.
- Funkcja informująca użytkowników przed kliknięciem przycisku wysyłania o szczegółach wiadomości, które mogą spowodować jej niedostarczenie lub wysłanie pod niewłaściwy adres, obejmująca przypadkowe wysłanie poufnych informacji do odbiorców zewnętrznych, wysyłanie wiadomości do dużych grup dystrybucyjnych lub odbiorców, którzy pozostawili informacje o nieobecności.
- Transkrypcja tekstowa wiadomości głosowej, pozwalająca użytkownikom na szybkie priorytetyzowanie wiadomości bez potrzeby odsłuchiwania pliku dźwiękowego.
- Możliwość uruchomienia osobistego automatycznego asystenta poczty głosowej. Telefoniczny dostęp do całej skrzynki odbiorczej – w tym poczty elektronicznej, kalendarza i listy kontaktów
- Udostępnienie użytkownikom możliwości aktualizacji danych kontaktowych i śledzenia odbierania wiadomości e-mail bez potrzeby informatyków

- Funkcjonalność wspierająca zarządzanie informacją w systemie pocztowym:
  - Centralne zarządzanie cyklem życia informacji przechowywanych w systemie pocztowym, w tym śledzenie i rejestrowanie ich przepływu, wygaszanie po zdefiniowanym okresie czasu, archiwizacja
  - Definiowanie kwot na rozmiar skrzynek pocztowych użytkowników, z możliwością ustawiania progu ostrzegawczego poniżej górnego limitu.
  - Możliwość definiowania różnych limitów dla różnych grup użytkowników.
  - Możliwość wprowadzenia modelu kontroli dostępu, który umożliwia nadanie specjalistom uprawnień do wykonywania określonych zadań – na przykład pracownikom odpowiedzialnym za zgodność z uregulowaniami uprawnień do przeszukiwania wielu skrzynek pocztowych – bez przyznawania pełnych uprawnień administracyjnych.
  - Możliwość przeniesienia lokalnych archiwów skrzynki pocztowej z komputera na serwer, co pozwala na wydajne zarządzanie i ujawnianie prawne.
  - Możliwość łatwiejszej klasyfikacji wiadomości e-mail dzięki definiowanym centralnie zasadom zachowywania, które można zastosować do poszczególnych wiadomości lub folderów.
  - Możliwość wyszukiwania w wielu skrzynkach pocztowych poprzez interfejs przeglądarkowy i funkcja kontroli dostępu w oparciu o role, która umożliwia przeprowadzanie ukierunkowanych wyszukiwań przez pracowników działu HR lub osoby odpowiedzialne za zgodność z uregulowaniami.
  - Integracja z usługami zarządzania dostępem do treści (ADRMS) pozwalająca na automatyczne stosowanie ochrony za pomocą zarządzania prawami do informacji (IRM) w celu ograniczenia dostępu do informacji zawartych w wiadomości i możliwości ich wykorzystania, niezależnie od miejsca nadania.
  - Odbieranie wiadomości zabezpieczonych funkcją IRM przez partnerów i klientów oraz odpowiadanie na nie – nawet, jeśli nie dysponują oni usługami ADRMS.
  - Przeglądanie wiadomości wysyłanych na grupy dystrybucyjne przez osoby nimi zarządzające i blokowanie lub dopuszczanie transmisji.
  - Możliwość korzystania z łatwego w użyciu interfejsu internetowego w celu wykonywania często spotykanych zadań związanych z pomocą techniczną.

Pakiet biurowy on-line musi spełniać następujące wymagania:

- Wymagania odnośnie interfejsu użytkownika:
  - Pełna polska wersja językowa interfejsu użytkownika,
  - Prostota i intuicyjność obsługi, pozwalająca na pracę osobom nieposiadającym umiejętności technicznych.

Collegium Da Vinci
ul. Gen. Tadeusza Kutrzeby 10
61-719 Poznań
61 271 10 10 / info@cdv.pl
cdv.pl

- Oprogramowanie musi umożliwiać tworzenie i edycję dokumentów elektronicznych w ustalonym formacie, który spełnia następujące warunki:
    - posiada kompletny i publicznie dostępny opis formatu,
    - ma zdefiniowany układ informacji w postaci XML zgodnie z Tabelą B1 załącznika 2 Rozporządzenia w sprawie minimalnych wymagań dla systemów teleinformatycznych (Dz.U.05.212.1766).
- Pakiet biurowy on-line musi zawierać:
    - Edytor tekstów,
    - Arkusz kalkulacyjny,
    - Narzędzie do przygotowywania i prowadzenia prezentacji
    - Narzędzie do tworzenia notatek przy pomocy klawiatury lub notatek odręcznych.

- Edytor tekstów musi umożliwiać:
    - Edycję i formatowanie tekstu w języku polskim wraz z obsługą języka polskiego w zakresie sprawdzania pisowni i poprawności gramatycznej oraz funkcjonalnością słownika wyrazów bliskoznacznych i autokorekty
    - Wstawianie oraz formatowanie tabel
    - Wstawianie oraz formatowanie obiektów graficznych
    - Wstawianie wykresów i tabel z arkusza kalkulacyjnego
    - Automatyczne numerowanie rozdziałów, punktów, akapitów, tabel i rysunków
    - Automatyczne tworzenie spisów treści
    - Formatowanie nagłówków i stopek stron
    - Sprawdzanie pisowni w języku polskim
    - Śledzenie zmian wprowadzonych przez użytkowników
    - Określenie układu strony (pionowa/pozioma)
    - Wydruk dokumentów
    - Pracę na dokumentach utworzonych przy pomocy poprzednich wersji Microsoft Word z zapewnieniem konwersji wszystkich elementów i atrybutów dokumentu
    - Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji.

- Arkusz kalkulacyjny musi umożliwiać:
    - Tworzenie raportów tabelarycznych,
    - Tworzenie wykresów liniowych (wraz linią trendu), słupkowych, kołowych,
    - Tworzenie arkuszy kalkulacyjnych zawierających teksty, dane liczbowe oraz formuły przeprowadzające operacje matematyczne, logiczne, tekstowe, statystyczne oraz operacje na danych finansowych i na miarach czasu,
    - Wyszukiwanie i zamianę danych,
    - Wykonywanie analiz danych przy użyciu formatowania warunkowego,
    - Nazywanie komórek arkusza i odwoływanie się w formułach po takiej nazwie,
    - Formatowanie czasu, daty i wartości finansowych z polskim formatem,
    - Zapis wielu arkuszy kalkulacyjnych w jednym pliku,
    - Zachowanie pełnej zgodności z formatami plików utworzonych za pomocą oprogramowania Microsoft Excel we wcześniejszych wersjach, z uwzględnieniem poprawnej realizacji użytych w nich funkcji specjalnych i makropoleceń,
    - Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji.

- Narzędzie do przygotowywania i prowadzenia prezentacji musi umożliwiać tworzenie prezentacji, które będą posiadały funkcje:
    - Prezentowanie przy użyciu projektora multimedialnego,
    - Drukowanie w formacie umożliwiającym robienie notatek,

Collegium Da Vinci
ul. Gen. Tadeusza Kutrzeby 10
61-719 Poznań
61 271 10 10 / info@cdv.pl
cdv.pl

- Zapisanie jako prezentacja tylko do odczytu,
- Nagrywanie narracji i dołączanie jej do prezentacji,
- Opatrywanie slajdów notatkami dla prezentera,
- Umieszczanie i formatowanie tekstów, obiektów graficznych, tabel, nagrań dźwiękowych i wideo,
- Umieszczanie tabel i wykresów pochodzących z arkusza kalkulacyjnego,
- Odświeżenie wykresu znajdującego się w prezentacji po zmianie danych w źródłowym arkuszu kalkulacyjnym,
- Możliwość tworzenia animacji obiektów i całych slajdów,
- Prowadzenie prezentacji w trybie prezentera, gdzie slajdy są widoczne na jednym monitorze lub projektorze, a na drugim widoczne są slajdy i notatki prezentera,
- Pełna zgodność z formatami plików utworzonych za pomocą oprogramowania MS PowerPoint w starszych wersjach.

Repozytorium dokumentów musi zapewnić usługę przestrzeni dyskowej o pojemności minimum 1 TB dla każdego użytkownika. Repozytorium musi umożliwiać użytkownikom pakietów biurowych na:

- traktowanie go, jako własnego dysku,
- synchronizację zawartości wybranego folderu ze stacji roboczej do repozytorium przypisanego danemu użytkownikowi na bazie niezaprzeczalnego uwierzytelnienia,
- synchronizację zawartości repozytorium z wieloma urządzeniami w ramach uprawnień użytkownika,
- właściciela repozytorium.

Aplikacja do centralnego zarządzania infrastrukturą zamawiającego pozwalająca na co najmniej:

- instalację systemu operacyjnego w trybie nienadzorowanym,
- zdalną instalację oprogramowania,
- tworzenia pakietów sterowników,
- tworzenia kolekcji urządzeń,
- zdalną aktualizację systemów operacyjnych,
- możliwość zdalnej komunikacji obejmującą zarówno połączenia wideo jak i transfer plików,
- możliwość wykonywania skryptów na urządzeniach końcowych,
- tworzenie raportów.

5. SPECYFIKACJA SERWERY- 2 szt.:

Parametr	Charakterystyka (wymagania minimalne)
Obudowa	Obudowa Rack o wysokości max 1U wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych oraz organizatorem do kabli. Obudowa z możliwością wyposażenia w kartę umożliwiającą dostęp bezpośredni poprzez urządzenia mobilne - serwer musi posiadać możliwość konfiguracji oraz monitoringu najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej min. (Android/ Apple iOS) przy użyciu jednego z protokołów BLE/ WIFI.
Płyta główna	Płyta główna z możliwością zainstalowania do dwóch procesorów. Obsługa procesorów 32 rdzeniowych. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym.
Chipset	Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych.
Procesor	Zainstalowane dwa procesory min. 16-rdzeniowy, min. 2.5GHz, klasy x86 dedykowane do pracy z zaoferowanym serwerem umożliwiające osiągnięcie wyniku min. 328 w teście SPECrate2017_int_base, dostępnym na stronie www.spec.org dla konfiguracji dwuprocesorowej.

Collegium Da Vinci
ul. Gen. Tadeusza Kutrzeby 10
61-719 Poznań
61 271 10 10 / info@cdv.pl
cdv.pl

RAM	Minimum 512GB DDR5 RDIMM 4800MT/s, na płycie głównej powinno znajdować się minimum 16 slotów przeznaczonych do instalacji pamięci. Płyta główna powinna obsługiwać do 1TB pamięci RAM.
Funkcjonalność pamięci RAM	Demand Scrubing, Patrol Scrubing, Permanent Fault Detection
Gniazda PCI	- minimum trzy sloty PCIe generacji 4
Interfejsy sieciowe/FC/SAS	Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT oraz 2 interfejsy sieciowe 25Gb Ethernet w standardzie SFP28 (porty nie mogą być osiągnięte poprzez karty w slotach PCIe) Dodatkowa czteroportowa karta SAS HBA 12Gb
Dyski twarde	Zainstalowane dwa dyski M.2 NVMe SSDs o pojemności min. 480GB Hot-Plug z możliwością konfiguracji RAID 1.
Wbudowane porty	4 x USB z czego nie mniej niż 1x USB 3.0, 2x VGA
Video	Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1920x1200
Zasilacze	Redundantne, Hot-Plug min. 800W każdy.
Bezpieczeństwo	• Zatrzask 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. • Moduł 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 • kontrola stanu BIOS pod kątem naruszenia integralności oprogramowania • możliwość wykorzystania tokenu lub aplikacji SecurID do uwierzytelniania wielkoskładnikowego przy logowaniu do karty zarządzającej
Diagnostyka	Serwer wyposażony w panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS'u, zasilaniu oraz temperaturze.
Karta Zarządzania	Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca: • zdalny dostęp do graficznego interfejsu Web karty zarządzającej; • zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera); • Dostosowanie zarządzania temperaturą i przepływem powietrza w serwerze • monitorowanie przepływu powietrza na bieżąco • możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer; • Przesyłanie danych telemetrycznych w czasie rzeczywistym • szyfrowane SSL • wsparcie dla IPv6; • wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish; • możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer; • integracja z Active Directory; • wsparcie dla dynamic DNS;

Collegium Da Vinci
ul. Gen. Tadeusza Kutrzeby 10
61-719 Poznań
61 271 10 10 / info@cdv.pl
cdv.pl

	• wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej. • możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera • możliwość zarządzania do 100 serwerów bezpośrednio z konsoli karty zarządzającej pojedynczego serwera • możliwość obsługi przez sześciu użytkowników jednocześnie; • możliwość podmontowania zdalnych wirtualnych napędów; • wirtualną konsolę z dostępem do myszy, klawiatury; • Wirtualny schowek ułatwiający korzystanie z konsoli zdalnej • Automatyczna rejestracja certyfikatów (ACE) • możliwość wysyłania danych do zewnętrznych narzędzi analitycznych jak Splunk, ElasticSearch, Grafana. • Logowanie połączenia przez port szeregowy • Informacje SMART z lokalnych urządzeń dyskowych • Wykrywanie nieaktywnych serwerów •
Oprogramowanie do zarządzania	Możliwość zainstalowania oprogramowania producenta do zarządzania, spełniającego 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

Collegium Da Vinci
ul. Gen. Tadeusza Kutrzeby 10
61-719 Poznań
61 271 10 10 / info@cdv.pl
cdv.pl

	• 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 modularnych 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.
Certyfikaty	Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015, ISO-50001 oraz ISO-14001 Serwer musi posiadać deklaracja CE. 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 Dyrektywy WEEE 2002/96/EC. 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.** Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Microsoft Windows Server 2019, Microsoft Windows Server 2022.
Dokumentacja użytkownika	Zamawiający wymaga dokumentacji w języku polskim lub angielskim. Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.
Warunki gwarancji	3 lata gwarancji producenta Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 9/5 następującymi kanałami: telefonicznie oraz przez Internet. Certyfikowany Technik wykonawcy / producenta z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) ma rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym (NBD) od otrzymania zgłoszenia / zakończenia

Collegium Da Vinci
ul. Gen. Tadeusza Kutrzeby 10
61-719 Poznań
61 271 10 10 / info@cdv.pl
cdv.pl

	diagnostyki. Naprawa ma się odbywać w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę. Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania producenta, w tym także sprzedanego oprogramowania. Zgłoszenie przyjęte jest potwierdzane przez zespół pomocy technicznej (mail/telefon / portal) przez nadanie unikalnego numeru zgłoszenia pozwalającego na identyfikację zgłoszenia w trakcie realizacji naprawy i po jej zakończeniu. Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji serwera. Zamawiający oczekuje nieodpłatnego udostępnienia narzędzi serwisowych i procesów wsparcia umożliwiających: Wykrywanie usterek sprzętowych z predykcją awarii. Automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych. **UWAGA:** • **Firma serwisująca musi posiadać ISO 9001:2015 oraz ISO-27001 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty.** • **Wymagane dołączenie do oferty oświadczenia Producenta potwierdzające, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta.**

6. SPECYFIKACJA MACIERZ – 1 szt.:

Element konfiguracji/cecha/ funkcjonalność	Wymagania minimalne
Typ obudowy	Macierz musi być przystosowana do montażu w szafie rack 19”, o wysokość maksymalnie 2U.
Przestrzeń dyskowa	Macierz musi posiadać minimum 24 dyski SSD SAS o pojemności min. 960GB każdy.
Możliwość rozbudowy	Macierz musi umożliwiać rozbudowę (bez wymiany kontrolerów macierzy), do co najmniej 276 dysków twardych.
Obsługa dysków	Macierz musi mieć możliwość obsługiwania dysków SSD, SAS i Nearline SAS. Macierz musi umożliwiać mieszanie napędów dyskowych SSD, SAS i NL SAS w obrębie pojedynczej półki dyskowej. Macierz musi obsługiwać dyski 2,5” jak również 3,5”.
Sposób zabezpieczenia danych	Macierz musi obsługiwać mechanizmy RAID zgodne z RAID0, RAID1, RAID10, RAID5, RAID6 oraz RAID z tzw. rozproszoną wolną pojemnością, realizowane sprzętowo za pomocą dedykowanego układu, z możliwością dowolnej ich kombinacji w obrębie oferowanej macierzy i z wykorzystaniem wszystkich dysków (tzw. wide-striping). Macierz musi umożliwiać definiowanie globalnych dysków spare oraz dedykowanie dysków spare do konkretnych grup RAID. Macierz musi również oferować możliwość zdefiniowania grup dyskowych z tzw. rozproszoną wolną pojemnością, która nie wykorzystuje tradycyjnych dysków zapasowych (integracja dysków zapasowych i nieaktywnych do zwiększenia dostępności i wydajności macierzy, zwiększenie szybkości odbudowy macierzy na wypadek awarii dysku). Macierz musi umożliwiać obsługę dysków różnej pojemności w ramach grupy dysków.

Collegium Da Vinci
ul. Gen. Tadeusza Kutrzeby 10
61-719 Poznań
61 271 10 10 / info@cdv.pl
cdv.pl

Tryb pracy kontrolerów macierzowych	Macierz musi posiadać minimum 2 kontrolery macierzowe pracujące w trybie active-active i udostępniające jednocześnie dane blokowe. Wszystkie kontrolery muszą komunikować się między sobą bez stosowania dodatkowych przełączników lub koncentratorów.
Pamięć cache	Macierz musi posiadać minimum sumarycznie 32 GB pamięci cache. Pamięć cache musi być zbudowana w oparciu o wydajną pamięć typu RAM. Pamięć zapisu musi być mirrorowana (kopie lustrzane) pomiędzy kontrolerami dyskowymi. Dane niezapisane na dyskach (np. zawartość pamięci kontrolera) muszą zostać zabezpieczone w przypadku awarii zasilania za pomocą podtrzymania bateryjnego lub z zastosowaniem innej technologii przez okres minimum 5 lat.
Rozbudowa pamięci cache	Macierz musi umożliwiać zwiększenie pojemności pamięci cache dla odczytów do minimum 8 TB z wykorzystaniem dysków SSD lub kart pamięci flash. Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć wraz z rozwiązaniem.
Interfejsy	Macierz musi posiadać, co najmniej 8 portów SAS 12Gb (4 porty na kontroler) Należy dostarczyć min. 4 kable SAS do połączenia macierzy z oferowanymi serwerami o długości min. 2m.
Zarządzanie	Zarządzanie macierzą musi być możliwe z poziomu interfejsu graficznego i interfejsu znakowego. Zarządzanie macierzą musi odbywać się bezpośrednio na kontrolerach macierzy z poziomu przeglądarki internetowej.
Zarządzanie grupami dyskowymi oraz dyskami logicznymi	Macierz musi umożliwiać zdefiniowanie, co najmniej 500 wolumenów logicznych w ramach oferowanej macierzy dyskowej. Musi istnieć możliwość rozłożenia pojedynczego wolumenu logicznego na wszystkie dyski fizyczne macierzy (tzw. wide-striping), bez konieczności łączenia wielu różnych dysków logicznych w jeden większy. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia.
Thin Provisioning	Macierz musi umożliwiać udostępnianie zasobów dyskowych do serwerów w trybie tradycyjnym, jak i w trybie typu Thin Provisioning. Macierz musi umożliwiać odzyskiwanie przestrzeni dyskowych po usuniętych danych w ramach wolumenów typu Thin. Proces odzyskiwania danych musi być automatyczny bez konieczności uruchamiania dodatkowych procesów na kontrolerach macierzowych (wymagana obsługa standardu T10 SCSI UNMAP). Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia.
Tiering	Macierz musi posiadać funkcjonalność Tiering między dyskami SSD i SAS i między dyskami SAS i NL SAS. Tiering musi obejmować wszystkie woluminy w danej puli dyskowej. Dyski SSD mogą być wykorzystane zarówno do uzyskania pojemności w warstwie wydajności lub na potrzeby zwiększenia pamięci podręcznej odczytu w celu przyspieszenia operacji losowego odczytu z jednej lub wielu warstw napędów mechanicznych.
Wewnętrzne kopie migawkowe	Macierz musi umożliwiać dokonywania na żądanie tzw. migawkowej kopii danych (snapshot, point-in-time) w ramach macierzy za pomocą wewnętrznych kontrolerów macierzowych. Kopia migawkowa wykonuje się bez alokowania dodatkowej przestrzeni dyskowej na potrzeby kopii. Zajmowanie dodatkowej przestrzeni dyskowej następuje w momencie zmiany danych na dysku źródłowym lub na jego kopii. Macierz musi wspierać minimum 512 kopii migawkowych. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia.
Wewnętrzne kopie pełne	Macierz musi umożliwiać dokonywanie na żądanie pełnej fizycznej kopii danych (clone) w ramach macierzy za pomocą wewnętrznych kontrolerów macierzowych.

Collegium Da Vinci
ul. Gen. Tadeusza Kutrzeby 10
61-719 Poznań
61 271 10 10 / info@cdv.pl
cdv.pl

	Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia.
Migracja danych w obrębie macierzy	Macierz dyskowa musi umożliwiać migrację danych bez przerywania do nich dostępu pomiędzy różnymi warstwami technologii dyskowych na poziomie części wolumenów logicznych (ang. Sub-LUN). Zmiany te muszą się odbywać wewnętrznymi mechanizmami macierzy. Funkcjonalność musi umożliwiać zdefiniowanie zasobu LUN, który fizycznie będzie znajdował się na min. 3 typach dysków obsługiwanych przez macierz, a jego części będą realokowane na podstawie analizy ruchu w sposób automatyczny i transparentny (bez przerywania dostępu do danych) dla korzystających z tego wolumenu hostów. Zmiany te muszą się odbywać wewnętrznymi mechanizmami macierzy. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności dostarczanego urządzenia.
Podłączanie zewnętrznych systemów operacyjnych	Macierz musi umożliwiać jednoczesne podłączenie wielu serwerów w trybie wysokiej dostępności (co najmniej dwoma ścieżkami). Macierz musi wspierać podłączenie następujących systemów operacyjnych: Windows, RHEL, SLES, Vmware, Citrix. Dla wymienionych systemów operacyjnych należy dostarczyć oprogramowanie do przełączania ścieżek i równoważenia obciążenia poszczególnych ścieżek. Wymagane jest oprogramowanie dla nielimitowanej liczby serwerów. Dopuszcza się rozwiązania bazujące na natywnych możliwościach systemów operacyjnych. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla maksymalnej liczby serwerów obsługiwanych przez oferowane urządzenie.
Redundancja	Macierz nie może posiadać pojedynczego punktu awarii, który powodowałby brak dostępu do danych. Musi być zapewniona pełna redundancja komponentów, w szczególności zdublowanie kontrolerów, zasilaczy i wentylatorów. Macierz musi umożliwiać wymianę elementów systemu w trybie „hot-swap", a w szczególności takich, jak: dyski, kontrolery, zasilacze, wentylatory. Macierz musi mieć możliwość zasilania z dwu niezależnych źródeł zasilania – odporność na zanik zasilania jednej fazy lub awarię jednego z zasilaczy macierzy. Zasilacze użyte w macierzy powinny posiadać certyfikat sprawności zasilacza minimum 80+ Gold.
Dodatkowe wymagania	Oferowany system dyskowy musi się składać z pojedynczej macierzy dyskowej. Niedopuszczalna jest realizacja zamówienia poprzez dostarczenie wielu macierzy dyskowych. Za pojedynczą macierz nie uznaje się rozwiązania opartego o wiele macierzy dyskowych (par kontrolerów macierzowych) połączonych przełącznikami SAN lub tzw. wirtualizatorem sieci SAN czy wirtualizatorem macierzy dyskowych. Możliwość ograniczania poboru zasilania przez dyski, które nie obsługują operacji we/wy, poprzez ich zatrzymanie.
Standardy bezpieczeństwa	Urządzenie musi spełniać następujące standardy bezpieczeństwa: EN 62368-1 (European Union), IEC 60950-1 (International)
Inne	Urządzenia muszą być zakupione w oficjalnym kanale dystrybucyjnym producenta. Na żądanie Zamawiającego, Wykonawca musi przedstawić oświadczenie producenta oferowanego serwera, potwierdzające pochodzenie urządzenia z oficjalnego kanału dystrybucyjnego producenta. Wymagane są dokumenty poświadczające, że sprzęt jest produkowany zgodnie z normami ISO 9001 oraz ISO 14001. Deklaracja zgodności CE.
Warunki gwarancji	3 lata gwarancji producenta Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie, przez Internet oraz z wykorzystaniem aplikacji.

Collegium Da Vinci
ul. Gen. Tadeusza Kutrzeby 10
61-719 Poznań
61 271 10 10 / info@cdv.pl
cdv.pl

	Zamawiający oczekuje rozpoczęcia diagnostyki telefonicznej / internetowej już w momencie dokonania zgłoszenia. Certyfikowany Technik wykonawcy / producenta z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) ma rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym (NBD) od otrzymania zgłoszenia / zakończenia diagnostyki. Naprawa ma się odbywać w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę. Zamawiający oczekuje bezpośredniego dostępu do wykwalifikowanej kadry inżynierów technicznych a w przypadku konieczności eskalacji zgłoszenia serwisowego wyznaczonego Kierownika Eskalacji po stronie wykonawcy. Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania producenta, w tym także sprzedanego oprogramowania. Zgłoszenie przyjęte jest potwierdzane przez zespół pomocy technicznej (mail/telefon / aplikacja / portal) przez nadanie unikalnego numeru zgłoszenia pozwalającego na identyfikację zgłoszenia w trakcie realizacji naprawy i po jej zakończeniu. Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy. Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji urządzenia. Zamawiający oczekuje nieodpłatnego udostępnienia narzędzi serwisowych i procesów wsparcia umożliwiających: Wykrywanie usterek sprzętowych z predykcją awarii. Automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych. Możliwość rozszerzenia gwarancji przez producenta do 7 lat. **UWAGA:** • **Firma serwisująca musi posiadać ISO 9001:2015 oraz ISO-27001 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty**. • **Wymagane dołączenie do oferty oświadczenia Producenta potwierdzające, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta.**

2. Terminy realizacji przedmiotu zamówienia:
Część 1: dostarczenie zamówienia maksymalnie do 21 dni kalendarzowych od daty podpisania umowy.

3. Warunki ogólne:

a) Przedmiotowy sprzęt wraz z oprogramowaniem powinien być fabrycznie nowy i pochodzić z oficjalnej dystrybucji producenta.

b) Integralną część przedmiotu zamówienia stanowi dostarczenie przedmiotowego sprzętu do siedziby Zamawiającego: **ul. gen. Tadeusza Kutrzeby 10, 61-719 Poznań**.

c) Opisane w pkt. 2 termin realizacji zamówienia wyznacza graniczną (najpóźniejszą dopuszczalną przez Zamawiającego) datę dostarczenia całości przedmiotowego zamówienia do siedziby Zamawiającego.

d) Wyłoniony Oferent jest zobowiązany do stałego kontaktu z koordynatorem zamówienia wyznaczonym przez Zamawiającego w celu ustalenia szczegółów dostarczenia oraz odebrania zamówienia w siedzibie CDV.