



BIURO INFORMATYKI I ŁĄCZNOŚCI
KOMENDA GŁÓWNA PAŃSTWOWEJ STRAŻY POŻARNEJ

OPZ – Załącznik nr 1 Zakup licencji

www.it.straz.gov.pl



Nr sprawy: BF-IV.2370.26.2024
 Załącznik nr 1 do SWZ/ nr 1 do umowy

Spis treści

WYMAGANIA OGÓLNE:.....	4
DOSTAWA OPROGRAMOWANIA.....	5
TYTUŁ WYMAGANIA: SQL.01.2024 - SKALOWALNOŚĆ ZASOBÓW SYSTEMOWYCH	7
TYTUŁ WYMAGANIA: SQL.02.2024 - WYSOKA DOSTĘPNOŚĆ I ODZYSKIWANIE PO AWARII	8
TYTUŁ WYMAGANIA: SQL.03.2024 - GRUPY WYSOKIEJ DOSTĘPNOŚCI (ALWAYS ON)	9
TYTUŁ WYMAGANIA: SQL.04.2024 - INSTANCJE KLASTRA AWARYJNEGO (FAILOVER CLUSTER INSTANCES)	9
TYTUŁ WYMAGANIA: SQL.05.2024 - KOMPRESJA DANYCH.....	10
TYTUŁ WYMAGANIA: SQL.06.2024 - TRANSPARENTNE SZYFROWANIE DANYCH (TDE)	10
TYTUŁ WYMAGANIA: SQL.07.2024 - ZAWSZE SZYFROWANE DANE (ALWAYS ENCRYPTED).....	11
TYTUŁ WYMAGANIA: SQL.08.2024 - ZABEZPIECZENIA NA POZIOMIE WIERSZY (ROW-LEVEL SECURITY).....	12
TYTUŁ WYMAGANIA: SQL.09.2024 - DYNAMICZNE MASKOWANIE DANYCH (DYNAMIC DATA MASKING).....	12
TYTUŁ WYMAGANIA: SQL.10.2024 - AUDYTOWANIE NA POZIOMIE BAZY DANYCH	13
TYTUŁ WYMAGANIA: SQL.11.2024 - PARTYCJONOWANIE TABEL I INDEKSÓW	14
TYTUŁ WYMAGANIA: SQL.12.2024 - IN-MEMORY OLTP	14
TYTUŁ WYMAGANIA: SQL.13.2024 - INDEKSY KOLUMNOWE (COLUMNSTORE INDEXES)	15
TYTUŁ WYMAGANIA: SQL.14.2024 - RÓWNOLEGŁE PRZETWARZANIE ZAPYTAŃ (PARALLEL QUERY PROCESSING)	16
TYTUŁ WYMAGANIA: SQL.15.2024 - MAGAZYN ZAPYTAŃ (QUERY STORE).....	16
TYTUŁ WYMAGANIA: SQL.16.2024 - INTELIGENTNE PRZETWARZANIE ZAPYTAŃ (INTELLIGENT QUERY PROCESSING)	17
TYTUŁ WYMAGANIA: SQL.17.2024 - AUTOMATYCZNE DOSTRAJANIE (AUTOMATIC TUNING)	18
TYTUŁ WYMAGANIA: SQL.18.2024 - ZARZĄDZANIE ZASOBAMI (RESOURCE GOVERNOR).....	18
TYTUŁ WYMAGANIA: SQL.19.2024 - USŁUGI JAKOŚCI DANYCH (DATA QUALITY SERVICES)	19
TYTUŁ WYMAGANIA: SQL.20.2024 - USŁUGI ZARZĄDZANIA DANYMI GŁÓWNYMI (MASTER DATA SERVICES)	20
TYTUŁ WYMAGANIA: SQL.21.2024 - USŁUGI ANALITYCZNE (ANALYSIS SERVICES).....	20
TYTUŁ WYMAGANIA: SQL.22.2024 - USŁUGI RAPORTOWANIA (REPORTING SERVICES).....	21
TYTUŁ WYMAGANIA: SQL.23.2024 - USŁUGI INTEGRACYJNE (INTEGRATION SERVICES).....	22
TYTUŁ WYMAGANIA: SQL.24.2024 - USŁUGI UCZENIA MASZYNOWEGO (MACHINE LEARNING SERVICES).....	23
TYTUŁ WYMAGANIA: SQL.25.2024 - POLYBASE	23
TYTUŁ WYMAGANIA: SQL.26.2024 - ROZSZERZONA BAZA DANYCH (STRETCH DATABASE).....	24
TYTUŁ WYMAGANIA: SQL.27.2024 - TABELE TYMCZASOWE (TEMPORAL TABLES).....	25
TYTUŁ WYMAGANIA: SQL.28.2024 - OBSŁUGA JSON	26
TYTUŁ WYMAGANIA: SQL.29.2024 - OBSŁUGA BAZ GRAFOWYCH (GRAPH DATABASE)	26
TYTUŁ WYMAGANIA: SQL.30.2024 - OBSŁUGA DANYCH PRZESTRZENNYCH (SPATIAL DATA SUPPORT)	27
TYTUŁ WYMAGANIA: SQL.31.2024 - WYSZUKIWANIE PEŁNOTEKSTOWE (FULL-TEXT SEARCH)	28
TYTUŁ WYMAGANIA: SQL.32.2024 - WYSZUKIWANIE SEMANTYCZNE (SEMANTIC SEARCH)	29
TYTUŁ WYMAGANIA: SQL.33.2024 - ŚLEDZENIE ZMIAN DANYCH (CHANGE DATA CAPTURE).....	29
TYTUŁ WYMAGANIA: SQL.34.2024 - ŚLEDZENIE ZMIAN (CHANGE TRACKING).....	30
TYTUŁ WYMAGANIA: SQL.35.2024 - MIGAWKI BAZY DANYCH (DATABASE SNAPSHOTS)	31
TYTUŁ WYMAGANIA: SQL.36.2024 - MIRRORING BAZY DANYCH (DATABASE MIRRORING).....	32
TYTUŁ WYMAGANIA: SQL.37.2024 - LOG SHIPPING (TRANSPORT DZIENNIKA TRANSAKЦИИ)	32
TYTUŁ WYMAGANIA: SQL.38.2024 - REPLIKACJA DANYCH (TRANSAKCYJNA, MERGE, SNAPSHOT).....	33
TYTUŁ WYMAGANIA: SQL.39.2024 - AGENT SQL SERVER (SQL SERVER AGENT)	34
TYTUŁ WYMAGANIA: SQL.40.2024 - POCZTA BAZY DANYCH (DATABASE MAIL)	35
TYTUŁ WYMAGANIA: SQL.41.2024 - SERVICE BROKER	36
TYTUŁ WYMAGANIA: SQL.42.2024 - ROZSZERZONE ZDARZENIA (EXTENDED EVENTS).....	36
TYTUŁ WYMAGANIA: SQL.43.2024 - ZARZĄDZANIE OPARTE NA ZASADACH (POLICY-BASED MANAGEMENT)	37
TYTUŁ WYMAGANIA: SQL.45.2024 - ZARZĄDZANIE ZASOBAMI (RESOURCE GOVERNOR).....	38
TYTUŁ WYMAGANIA: SQL.46.2024 - ROZSZERZENIE PULI BUFORÓW (BUFFER POOL EXTENSION)	39
TYTUŁ WYMAGANIA: SQL.47.2024 - KOMPRESJA KOPII ZAPASOWYCH (BACKUP COMPRESSION)	39
TYTUŁ WYMAGANIA: SQL.48.2024 - REJESTR TRANSAKЦИИ (SQL SERVER LEDGER).....	40
TYTUŁ WYMAGANIA: WDC.1.2024 - OBSŁUGA NIEOGRANICZONEJ LICZBY MASZYN WIRTUALNYCH.....	42
TYTUŁ WYMAGANIA: WDC.2.2024 - WZMOCNIONE ZABEZPIECZENIA SERWERA	42
TYTUŁ WYMAGANIA: WDC.3.2024 - SPRZĘTOWE ZAUFANIE Z TPM 2.0.....	43

Nr sprawy: BF-IV.2370.26.2024
 Załącznik nr 1 do SWZ/ nr 1 do umowy

TYTUŁ WYMAGANIA: WDC.4.2024 - OCHRONA FIRMWARE'U z DRTM i DMA	44
TYTUŁ WYMAGANIA: WDC.5.2024 - BEZPIECZNY ROZRUCH UEFI	44
TYTUŁ WYMAGANIA: WDC.6.2024 - BEZPIECZEŃSTWO OPARTE NA WIRTUALIZACJI (VBS)	45
TYTUŁ WYMAGANIA: WDC.7.2024 - INTEGRALNOŚĆ KODU WYMUSZONA PRZEZ HYPERVISOR (HVCI)	45
TYTUŁ WYMAGANIA: WDC.8.2024 - OCHRONA DANYCH JĄDRA (KDP)	46
TYTUŁ WYMAGANIA: WDC.9.2024 - NATYWNA OBSŁUGA HTTPS I TLS 1.3	47
TYTUŁ WYMAGANIA: WDC.10.2024 - OBSŁUGA DNS-OVER-HTTPS (DoH)	47
TYTUŁ WYMAGANIA: WDC.11.2024 - SZYFROWANIE SMB Z WYKORZYSTANIEM AES-256	48
TYTUŁ WYMAGANIA: WDC.12.2024 - SZYFROWANIE SMB EAST-WEST DLA KOMUNIKACJI WEWNĄTRZ KLASTRA	49
TYTUŁ WYMAGANIA: WDC.13.2024 - SZYFROWANIE SMB DIRECT I RDMA	49
TYTUŁ WYMAGANIA: WDC.14.2024 - OBSŁUGA SERWERÓW z AZURE ARC.....	50
TYTUŁ WYMAGANIA: WDC.15.2024 - WINDOWS ADMIN CENTER z ROZSZERZONYMI FUNKCJAMI ZARZĄDZANIA	51
TYTUŁ WYMAGANIA: WDC.16.2024 - ZMNIEJSZONY ROZMIAR OBRAZÓW KONTENERÓW SYSTEMU	52
TYTUŁ WYMAGANIA: WDC.17.2024 - WSPARCIE DLA AZURE ACTIVE DIRECTORY z GMSA BEZ DOŁĄCZANIA DO DOMENY	53
TYTUŁ WYMAGANIA: WDC.18.2024 - WSPARCIE DLA MICROSOFT DISTRIBUTED TRANSACTION COORDINATOR (MSDTC) w KONTENERACH	53
TYTUŁ WYMAGANIA: WDC.19.2024 - WSPARCIE DLA MICROSOFT MESSAGE QUEUING (MSMQ) w KONTENERACH	54
TYTUŁ WYMAGANIA: WDC.20.2024 - PRZYPISYWANIE PROSTYCH MAGISTRALI DO KONTENERÓW IZOLOWANYCH PROCESOWO	55
TYTUŁ WYMAGANIA: WDC.21.2024 - AKCELERACJA SPRZĘTOWA DIRECTX API w KONTENERACH WINDOWS	56
TYTUŁ WYMAGANIA: WDC.22.2024 - WSPARCIE DLA KONTENERÓW HOST-PROCESS DO KONFIGURACJI WĘZŁÓW	56
TYTUŁ WYMAGANIA: WDC.23.2024 - WSPARCIE DLA IPV6 w KONTENERACH	57
TYTUŁ WYMAGANIA: WDC.24.2024 - SPÓJNA IMPLEMENTACJA POLITYK SIECIOWYCH z CALICO.....	58
TYTUŁ WYMAGANIA: WDC.25.2024 - WSPARCIE DLA PROCESORÓW INTEL ICE LAKE	58
TYTUŁ WYMAGANIA: WDC.26.2024 - CONFIDENTIAL COMPUTING z INTEL SGX	59
TYTUŁ WYMAGANIA: WDC.27.2024 - WSPARCIE DLA 48 TB PAMIĘCI I 2048 RDZENI LOGICZNYCH	60
TYTUŁ WYMAGANIA: WDC.28.2024 - TASK SCHEDULER I HYPER-V MANAGER DLA INSTALACJI SERVER CORE.....	60
TYTUŁ WYMAGANIA: WDC.29.2024 - NESTED VIRTUALIZATION DLA PROCESORÓW AMD	61
TYTUŁ WYMAGANIA: WDC.30.2024 - MICROSOFT EDGE ZAMIAST INTERNET EXPLORER.....	62
TYTUŁ WYMAGANIA: WDC.31.2024 - UDP SEGMENTATION OFFLOAD (USO).....	62
TYTUŁ WYMAGANIA: WDC.32.2024 - UDP RECEIVE SIDE COALESCING (UDP RSC)	63
TYTUŁ WYMAGANIA: WDC.33.2024 - TCP HYSTART++ I RACK	63
TYTUŁ WYMAGANIA: WDC.34.2024 - ULEPSZONE RECEIVE SEGMENT COALESCING (RSC) DLA WIRTUALNYCH PRZEŁĄCZNIKÓW HYPER-V	64
TYTUŁ WYMAGANIA: WDC.35.2024 - SYSTEM INSIGHTS z WYKRYWANIEM ANOMALII DYSKÓW	65
TYTUŁ WYMAGANIA: WDC.36.2024 - AUTOMATYCZNE PRZYWRACANIE PO AWARIACH URUCHAMIANIA	65
TYTUŁ WYMAGANIA: WDC.37.2024 - STORAGE MIGRATION SERVICE z ROZSZERZONYMI MOŻLIWOŚCIAMI.....	66
TYTUŁ WYMAGANIA: WDC.38.2024 - REGULOWANA PRĘDKOŚĆ NAPRAWY PAMIĘCI MASOWEJ	67
TYTUŁ WYMAGANIA: WDC.39.2024 - SZYBSZA NAPRAWA I RESYNCHRONIZACJA PAMIĘCI MASOWEJ	67
TYTUŁ WYMAGANIA: WDC.40.2024 - STORAGE BUS CACHE DLA AUTONOMICZNYCH SERWERÓW	68
TYTUŁ WYMAGANIA: WDC.41.2024 - REFS SNAPSHOTS NA POZIOMIE PLIKÓW	69
TYTUŁ WYMAGANIA: WDC.42.2024 - SMB KOMPRESJA.....	69
TYTUŁ WYMAGANIA: WDC.43.2024 - DŁUŻSZY CYKL WSPARCIA DLA WSZYSTKICH OBRAZÓW KONTENERÓW WINDOWS	70
TYTUŁ WYMAGANIA: WDC.44.2024 - WIRTUALIZOWANA STREFA CZASOWA DLA KONTENERÓW	71
TYTUŁ WYMAGANIA: WDC.45.2024 - SZYBSZA NAPRAWA I RESYNCHRONIZACJA PAMIĘCI MASOWEJ	71
TYTUŁ WYMAGANIA: WDC.46.2024 - STORAGE BUS CACHE DLA AUTONOMICZNYCH SERWERÓW	72
TYTUŁ WYMAGANIA: WDC.47.2024 - REFS SNAPSHOTS NA POZIOMIE PLIKÓW	73
TYTUŁ WYMAGANIA: WDC.48.2024 - HOSTPROCESS KONTENERY DO ZARZĄDZANIA WĘZŁAMI	73
TYTUŁ WYMAGANIA: WDC.49.2024 - AZURE MIGRATE APP CONTAINERIZATION.....	74
TYTUŁ WYMAGANIA: WDC.50.2024 - STORAGE SPACES DIRECT z ULEPSZONYMI FUNKCJAMI	74

Nr sprawy: BF-IV.2370.26.2024
 Załącznik nr 1 do SWZ/ nr 1 do umowy

Nazwa zadania:

„Zakup licencji na oprogramowanie Windows Server 2025 Datacenter, SQL Server Enterprise Edition w celu rozbudowy infrastruktury IT Państwowej Straży Pożarnej, ze szczególnym uwzględnieniem potrzeb związanych z zarządzaniem systemami SWD w czasie prezydencji Polski w Radzie UE.”

Opis przedmiotu zamówienia

Niniejsze zamówienie dotyczy zakupu licencji na oprogramowanie Windows Server 2025 Datacenter oraz SQL Server 2022 Enterprise Core. Zakup licencji ma na celu rozbudowę infrastruktury IT Państwowej Straży Pożarnej (PSP), w szczególności w obszarze systemów wspomaganie decyzji (SWD PSP), które są kluczowe dla operacyjnego zarządzania w czasie prezydencji Polski w Radzie Unii Europejskiej.

Licencje te zostaną wykorzystane m.in. w ramach realizacji projektu "Zaprojektowanie i Uruchomienie Zintegrowanego Kokpitu Operatora dla Systemu Wspomaganie Decyzji Państwowej Straży Pożarnej (SWD PSP)". Zamawiający wymaga dostarczenia licencji na wskazane oprogramowanie, jednak zgodnie z art. 99 ust. 5 ustawy Prawo zamówień publicznych, zamawiający dopuszcza produkty równoważne, które spełnią określone parametry techniczne, funkcjonalne i jakościowe.

Zestawienie produktów referencyjnych i równoważnych

Zamawiający określa wymagania dotyczące produktów referencyjnych lub ich równoważnych odpowiedników. Dopuszczenie produktów równoważnych ma na celu zapewnienie uczciwej konkurencji oraz równego traktowania wykonawców. Produkty równoważne muszą spełniać określone kryteria oceny równoważności, w tym m.in. parametry techniczne, funkcjonalne oraz jakościowe. Produkty te nie muszą być identyczne z produktami referencyjnymi, jednak ich funkcjonalności i parametry muszą być zbliżone, aby zapewnić pełną funkcjonalność systemu.

Tabela 1 - Zestawienie tabelaryczne dla dostawy oprogramowania.

Lp.	Produkty (lub produkty równoważne do podanych poniżej)	Lic./szt.	Core	Part number
1	Windows Server 2025 Datacenter - 16 Core	14	224	DG7GMGF0PWHD-0001
2	SQL Server 2022 Enterprise Core - 2 Core License Pack	13	26	DG7GMGF0M7XV-0003

Wymagania ogólne:

Zamawiający wymaga dostawy licencji na oprogramowanie **Windows Server 2025 Datacenter** oraz **SQL Server 2022 Enterprise Core przy czym licencje nie mogą być dostarczone jako wersje OEM¹**. Oprogramowanie będzie wdrażane w modelu **On-Premise**, co oznacza, że instalacja oraz utrzymanie systemów będą realizowane na zasobach lokalnych Państwowej Straży Pożarnej (PSP).

1. Rozwiązanie On-Premise:

- **Windows Server 2025 Datacenter** oraz **SQL Server 2022 Enterprise Core** zostaną zainstalowane i utrzymywane w środowisku lokalnym PSP, co zapewni pełną kontrolę nad infrastrukturą IT i bezpieczeństwem danych. W tym modelu przetwarzanie wrażliwych danych operacyjnych odbywa się wyłącznie w infrastrukturze Zamawiającego, minimalizując ryzyko ich dostępu przez podmioty trzecie.

2. Elastyczność i skalowalność:

- Zamawiający wymaga, aby rozwiązania były skalowalne, co pozwoli na przyszłą rozbudowę systemu w miarę wzrastających potrzeb operacyjnych. **Windows Server 2025 Datacenter** umożliwia dynamiczne zarządzanie zasobami, takimi jak wirtualizacja czy integracja z innymi systemami używanymi przez PSP.
- **SQL Server 2022 Enterprise Core** musi zapewniać wysoką wydajność i skalowalność w zarządzaniu danymi, co jest kluczowe dla przetwarzania dużych ilości informacji oraz raportowania w czasie rzeczywistym w ramach systemów wspomagania decyzji (SWD).

3. Bezpieczeństwo i zgodność z normami:

- Oprogramowanie musi spełniać najwyższe standardy bezpieczeństwa oraz być zgodne z obowiązującymi przepisami prawa, w tym z normami dotyczącymi ochrony danych osobowych i bezpieczeństwa operacyjnego.
- **Windows Server 2025 Datacenter** i **SQL Server 2022 Enterprise Core** muszą wspierać mechanizmy szyfrowania danych, zabezpieczenia dostępu oraz narzędzia monitorowania aktywności, które umożliwią natychmiastowe wykrycie i neutralizację potencjalnych zagrożeń.
- **Zgodność z istniejącą infrastrukturą:**
- Zamawiane oprogramowanie musi być w pełni zgodne z istniejącą infrastrukturą IT PSP oraz wspierać integrację z używanymi systemami, takimi jak system wspomagania decyzji (SWD). Zamawiający wymaga, aby oferowane licencje umożliwiały rozbudowę systemów bez potrzeby wymiany istniejącego sprzętu czy oprogramowania.

¹ **Definicja OEM:** Oprogramowanie OEM (ang. Original Equipment Manufacturer) to licencja przypisana do konkretnego urządzenia (zazwyczaj komputera lub serwera), zainstalowana fabrycznie przez producenta sprzętu. Tego typu licencje są trwale powiązane z konkretnym urządzeniem i nie mogą być przenoszone na inne urządzenia. W związku z tym licencje OEM są często bardziej ograniczone pod względem wsparcia technicznego oraz możliwości przenoszenia, w przeciwieństwie do pełnych licencji detalicznych.

Nr sprawy: BF-IV.2370.26.2024
Załącznik nr 1 do SWZ/ nr 1 do umowy

Dostawa oprogramowania

Dostawa licencji na oprogramowanie, w tym Windows Server 2025 Datacenter oraz SQL Server 2022 Enterprise Core, dla Komendy Głównej Państwowej Straży Pożarnej, musi spełniać poniższe wymagania:

Produkty standardowe (COTS):

Zamawiający wymaga, aby dostarczane licencje były powszechnie dostępne na rynku komercyjnym (Commercial Off-The-Shelf, COTS) i gotowe do natychmiastowego wdrożenia, bez potrzeby specjalistycznych modyfikacji czy adaptacji. Produkty muszą być w pełni kompatybilne z istniejącą infrastrukturą IT Zamawiającego, zapewniając integrację bez konieczności dodatkowych modyfikacji.

Pochodzenie produktów oraz kwalifikacje Wykonawcy:

Wszystkie licencje muszą pochodzić bezpośrednio od producenta lub jego autoryzowanych dystrybutorów. Wykonawca jest zobowiązany do przedstawienia dowodów na autoryzację do sprzedaży licencji oraz świadczenia usług wsparcia technicznego, zgodnie z wymaganiami producenta. Zamawiający zastrzega sobie prawo do weryfikacji kwalifikacji Wykonawcy, w tym zgodności z obowiązującymi normami prawnymi i technicznymi, a także do potwierdzenia autoryzacji przez producenta.

Możliwość rozszerzeń funkcjonalnych:

Zamawiający dopuszcza dostarczenie produktów o rozszerzonych funkcjonalnościach, pod warunkiem, że dodatkowe opcje przyniosą wartość dodaną i będą w pełni kompatybilne z istniejącymi systemami oraz procesami PSP. Dodatkowe funkcje nie mogą komplikować użytkowania ani utrzymania oprogramowania. Wszystkie dodatkowe funkcjonalności muszą być jasno określone i opisane w ofercie, aby Zamawiający mógł ocenić ich przydatność i wpływ na działalność operacyjną.

Zgodność z RODO:

Wszystkie produkty dostarczane w ramach tego zamówienia muszą być zgodne z Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. (RODO). Oznacza to, że oprogramowanie musi wspierać przetwarzanie, przechowywanie i zarządzanie danymi osobowymi zgodnie z zasadami ochrony danych osobowych, w szczególności w zakresie bezpieczeństwa, audytu i możliwości raportowania incydentów związanych z naruszeniami danych.

Wymogi dla produktów równoważnych i warunki migracji:

Jeśli Wykonawca zaoferuje produkty równoważne, muszą one spełniać następujące kryteria:

- **Wsparcie techniczne:** Wykonawca zobowiązany jest do zapewnienia wsparcia technicznego o jakości co najmniej takiej samej jak wsparcie oferowane przez producenta dla produktów referencyjnych.
- **Warunki licencyjne:** Licencje na produkty równoważne muszą oferować co najmniej te same korzyści dla Zamawiającego, jakie zapewniają produkty referencyjne.

Nr sprawy: BF-IV.2370.26.2024

Załącznik nr 1 do SWZ/ nr 1 do umowy

- **Funkcjonalność:** Wykonawca musi udowodnić, że produkty równoważne posiadają funkcjonalność nie gorszą niż produkty referencyjne.

Migracja na produkty równoważne, jeśli taka zostanie zaoferowana, musi być przeprowadzona w sposób niezakłócający ciągłości działania PSP oraz musi zapewniać pełną operacyjność systemów w czasie migracji. Cały proces migracji nie może trwać dłużej niż 7 dni od momentu podpisania umowy, a jego realizacja musi być zgodna z najwyższymi standardami bezpieczeństwa i wydajności.

Wymagania dotyczące jednolitości produktów równoważnych:

Zamawiający wymaga, aby wszystkie oferowane produkty równoważne pochodziły od jednego producenta. Wymóg ten ma na celu minimalizację kosztów związanych z obsługą wielu rozwiązań od różnych producentów, a także uproszczenie zarządzania, aktualizacji oraz monitorowania produktów. Jednolitość produktów równoważnych zapewni pełną interoperacyjność i spójność w ramach istniejącej infrastruktury IT PSP, minimalizując ryzyko problemów związanych z integracją i zarządzaniem różnorodnymi systemami.



Nr sprawy: BF-IV.2370.26.2024
Załącznik nr 1 do SWZ/ nr 1 do umowy

SQL Server 2022 Enterprise Core - 2 Core License

W ramach niniejszego zamówienia Zamawiający dopuszcza możliwość zaoferowania produktów równoważnych dla licencji SQL Server 2022 Enterprise Core - 2 Core License, pod warunkiem spełnienia przez te produkty określonych wymagań technicznych i funkcjonalnych. Produkty równoważne muszą zapewniać co najmniej taki sam poziom wydajności, funkcjonalności oraz bezpieczeństwa, jakie oferuje SQL Server 2022 Enterprise Core.

Kluczowe kryteria oceny równoważności obejmują:

1. Wydajność i skalowalność: Produkty muszą wspierać przetwarzanie dużych wolumenów danych oraz oferować elastyczne skalowanie na poziomie licencji Core, co pozwala na efektywne dostosowywanie mocy obliczeniowej do aktualnych potrzeb operacyjnych.
2. Bezpieczeństwo danych: Oprogramowanie musi zapewniać zaawansowane mechanizmy ochrony danych, w tym szyfrowanie, zarządzanie dostępem oraz audytowanie, zgodnie z wymogami bezpieczeństwa i przepisami prawa, w tym RODO.
3. Wysoka dostępność: Produkt równoważny powinien oferować funkcje wysokiej dostępności i mechanizmy odtwarzania po awarii, które są kluczowe dla działania krytycznych systemów operacyjnych w Państwowej Straży Pożarnej.
4. Funkcje analityczne i raportowanie: Produkt musi wspierać zaawansowane analizy danych i tworzenie raportów, co jest istotne dla zarządzania operacjami PSP oraz podejmowania decyzji opartych na danych.
5. Licencjonowanie Core: Licencje na produkty równoważne muszą być co najmniej tak samo elastyczne, jak model licencjonowania na rdzeń procesora stosowany w SQL Server 2022 Enterprise Core, zapewniając Zamawiającemu możliwość optymalizacji kosztów i skalowania infrastruktury.

Dopuszczenie produktów równoważnych ma na celu zapewnienie uczciwej konkurencji, jednak Zamawiający zastrzega, że produkty równoważne muszą być w pełni kompatybilne z istniejącą infrastrukturą IT oraz wspierać kluczowe funkcje wymagane dla sprawnego zarządzania danymi w systemach wspomagania decyzji (SWD).

Równoważność:

Poniżej przedstawione są szczegółowe wymagania dotyczące równoważności, które muszą być spełnione przez oferowane produkty lub usługi, aby zostały uznane za równoważne z określonymi w specyfikacji zamówienia.

Tytuł wymagania: SQL.01.2024 - Skalowalność zasobów systemowych

Opis wymagania:

System bazodanowy musi wspierać nieograniczoną liczbę rdzeni procesora oraz pamięci operacyjnej, zapewniając skalowalność i wydajność niezależnie od wielkości infrastruktury.

Nr sprawy: BF-IV.2370.26.2024

Załącznik nr 1 do SWZ/ nr 1 do umowy

Możliwość ta pozwala na optymalne wykorzystanie dostępnych zasobów sprzętowych w celu obsługi intensywnych operacji przetwarzania danych.

Kluczowe aspekty:

- **Skalowalność procesorów:** System musi być zdolny do pracy z dowolną liczbą rdzeni procesora, co umożliwi jego zastosowanie w rozbudowanych środowiskach z dużą liczbą wątków obliczeniowych.
- **Skalowalność pamięci operacyjnej:** System musi obsługiwać dowolną ilość pamięci RAM, co zapewnia płynność działania nawet w przypadku dużych wolumenów danych oraz złożonych zapytań.

Cel:

Zapewnienie maksymalnej elastyczności w wykorzystaniu zasobów sprzętowych, co pozwala na efektywne zarządzanie danymi i operacjami w środowiskach o zróżnicowanych wymaganiach obliczeniowych.

Tytuł wymagania: SQL.02.2024 - Wysoka dostępność i odzyskiwanie po awarii

Opis wymagania:

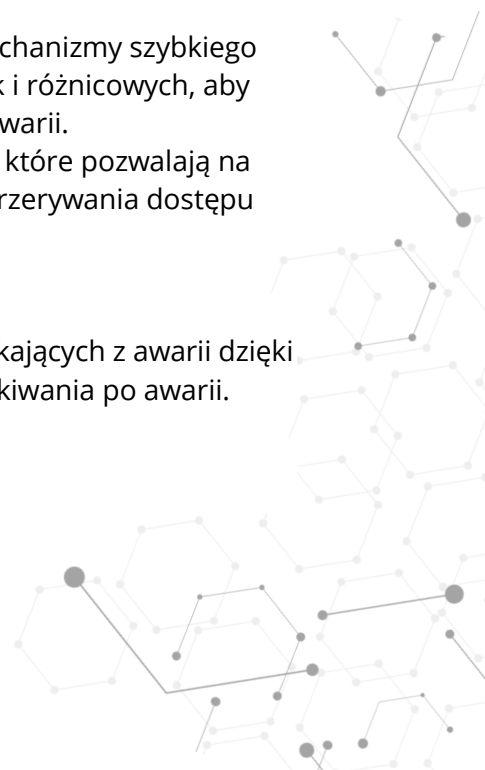
System bazodanowy musi zapewniać zaawansowane funkcje wysokiej dostępności oraz odzyskiwania po awarii, które minimalizują ryzyko przestoju i utraty danych. Te funkcje powinny umożliwiać szybkie przywracanie operacyjności systemu oraz bezprzerwowe działanie w przypadku awarii sprzętowych, sieciowych lub logicznych.

Kluczowe aspekty:

- **Automatyczne przełączanie awaryjne:** System musi wspierać funkcję automatycznego przełączania na zapasowe instancje w przypadku awarii, co zapewnia ciągłość pracy bez zauważalnych przerw dla użytkowników.
- **Replikacja danych w czasie rzeczywistym:** System powinien umożliwiać replikację danych na wielu serwerach w czasie rzeczywistym, co gwarantuje ich aktualność i bezpieczeństwo w razie awarii głównego serwera.
- **Odzyskiwanie danych po awarii:** System musi zapewniać mechanizmy szybkiego odzyskiwania danych z kopii zapasowych, zarówno pełnych, jak i różnicowych, aby zminimalizować czas przywracania pełnej funkcjonalności po awarii.
- **Brak przerw w dostępie:** System musi wspierać mechanizmy, które pozwalają na wykonywanie operacji konserwacyjnych oraz aktualizacji bez przerywania dostępu użytkowników do bazy danych.

Cel:

Zapewnienie ciągłości działania systemu oraz minimalizacja strat wynikających z awarii dzięki zaawansowanym funkcjom wysokiej dostępności i efektywnego odzyskiwania po awarii.



Nr sprawy: BF-IV.2370.26.2024

Załącznik nr 1 do SWZ/ nr 1 do umowy

Tytuł wymagania: SQL.03.2024 - Grupy wysokiej dostępności (Always On)

Opis wymagania:

System bazodanowy musi wspierać funkcję grup wysokiej dostępności, która umożliwia synchronizację i replikację danych między wieloma instancjami baz danych w celu zapewnienia nieprzerwanej dostępności oraz ochrony danych przed awariami. Funkcja ta powinna obsługiwać automatyczne przełączanie na zapasowe instancje oraz replikację w czasie rzeczywistym, zarówno w środowiskach lokalnych, jak i chmurowych.

Kluczowe aspekty:

- **Wielokrotna replika:** System musi umożliwiać tworzenie wielu replik bazy danych, które są synchronizowane w czasie rzeczywistym, zapewniając wysoką dostępność oraz ochronę danych.
- **Automatyczne przełączanie awaryjne:** W przypadku awarii głównej instancji system musi automatycznie przełączać się na jedną z replik zapasowych, minimalizując przerwy w dostępie do bazy danych.
- **Obsługa trybu synchronicznego i asynchronicznego:** System powinien wspierać zarówno synchronizację danych w trybie synchronicznym (dla lokalnych instancji), jak i asynchronicznym (dla instancji rozproszonych geograficznie).
- **Bezprzerwowe kopie zapasowe:** System musi umożliwiać wykonywanie kopii zapasowych z replik zapasowych, co pozwala na zachowanie ciągłości pracy głównej instancji bez jej obciążania.

Cel:

Zapewnienie wysokiej dostępności danych oraz minimalizacja ryzyka utraty danych lub przestojów systemu poprzez wykorzystanie funkcji grup wysokiej dostępności (Always On).

Tytuł wymagania: SQL.04.2024 - Instancje klastra awaryjnego (Failover Cluster Instances)

Opis wymagania:

System bazodanowy musi obsługiwać funkcję instancji klastra awaryjnego, która zapewnia wysoką dostępność poprzez zintegrowanie baz danych z klastrem serwerów. W przypadku awarii jednego węzła, system musi automatycznie przełączać operacje na inny dostępny węzeł, minimalizując przestoje i utratę danych.

Kluczowe aspekty:

- **Automatyczne przełączanie awaryjne:** System musi wspierać automatyczne przełączanie instancji bazodanowej na inny węzeł klastra w przypadku awarii sprzętowej lub logicznej, co zapewnia ciągłość pracy.
- **Współdzielone zasoby:** Klaster awaryjny powinien korzystać z współdzielonych zasobów dyskowych, co umożliwia bezproblemowe przenoszenie danych pomiędzy węzłami podczas przełączania awaryjnego.

Nr sprawy: BF-IV.2370.26.2024

Załącznik nr 1 do SWZ/ nr 1 do umowy

- **Wsparcie dla środowisk lokalnych i chmurowych:** System powinien obsługiwać instancje klastra awaryjnego zarówno w środowiskach fizycznych, jak i wirtualnych, w tym w chmurze, zapewniając elastyczność wdrożeń.
- **Monitorowanie stanu węzłów:** System musi stale monitorować stan węzłów klastra i w razie potrzeby automatycznie inicjować proces przełączania awaryjnego, aby zapewnić nieprzerwane działanie aplikacji.

Cel:

Zabezpieczenie ciągłości operacji poprzez automatyczne przełączanie na inne węzły klastra w przypadku awarii, co minimalizuje przestoje oraz ryzyko utraty danych w kluczowych środowiskach produkcyjnych.

Tytuł wymagania: SQL.05.2024 - Kompresja danych

Opis wymagania:

System bazodanowy musi obsługiwać zaawansowane mechanizmy kompresji danych, które pozwalają na zmniejszenie rozmiaru przechowywanych danych oraz optymalizację wykorzystania przestrzeni dyskowej. Funkcjonalność ta powinna zapewniać zarówno kompresję wierszy, jak i stron danych, co wpływa na zwiększenie wydajności operacji oraz zmniejszenie kosztów przechowywania danych.

Kluczowe aspekty:

- **Kompresja wierszy:** System musi umożliwiać kompresję na poziomie wierszy, co pozwala na zmniejszenie rozmiaru danych bez wpływu na ich integralność i wydajność operacyjną.
- **Kompresja stron:** System powinien obsługiwać kompresję stron, co umożliwia jeszcze większą redukcję przestrzeni dyskowej poprzez kompresję bloków danych na poziomie stron.
- **Bezstratna kompresja:** Mechanizmy kompresji muszą być bezstratne, co oznacza, że dane po dekompresji muszą zachować pełną dokładność i integralność.
- **Optymalizacja operacji I/O:** Kompresja danych powinna wpływać na zmniejszenie liczby operacji wejścia/wyjścia (I/O), co zwiększa wydajność pracy bazy danych, szczególnie przy dużych zbiorach danych.

Cel:

Redukcja rozmiaru przechowywanych danych oraz optymalizacja operacji dyskowych, co przekłada się na obniżenie kosztów związanych z przestrzenią dyskową oraz zwiększenie wydajności przetwarzania danych w systemie.

Tytuł wymagania: SQL.06.2024 - Transparentne szyfrowanie danych (TDE)

Opis wymagania:

System bazodanowy musi obsługiwać funkcję transparentnego szyfrowania danych (TDE), która zapewnia ochronę danych przechowywanych na dyskach przed nieautoryzowanym

Nr sprawy: BF-IV.2370.26.2024

Załącznik nr 1 do SWZ/ nr 1 do umowy

dostępem. Szyfrowanie powinno odbywać się automatycznie na poziomie plików bazy danych, bez wpływu na działanie aplikacji czy operacje użytkowników.

Kluczowe aspekty:

- **Szyfrowanie w locie:** System musi automatycznie szyfrować dane zapisane na dysku oraz odszyfrowywać je podczas odczytu, bez konieczności interakcji ze strony użytkowników lub aplikacji.
- **Ochrona kopii zapasowych:** Funkcja TDE powinna obejmować szyfrowanie nie tylko danych aktywnych, ale również kopii zapasowych i plików dzienników, zapewniając kompleksową ochronę danych.
- **Bezpieczne zarządzanie kluczami szyfrowania:** System musi wspierać bezpieczne zarządzanie kluczami szyfrowania, umożliwiając ich rotację, przechowywanie oraz ochronę przy użyciu dedykowanych modułów bezpieczeństwa (np. HSM).
- **Minimalny wpływ na wydajność:** Implementacja szyfrowania powinna mieć minimalny wpływ na wydajność systemu, zapewniając płynne operacje na danych nawet przy dużych wolumenach.

Cel:

Zabezpieczenie wrażliwych danych przechowywanych w bazie danych przed nieautoryzowanym dostępem dzięki transparentnemu szyfrowaniu, bez wpływu na codzienne operacje i funkcjonowanie aplikacji.

Tytuł wymagania: SQL.07.2024 - Zawsze szyfrowane dane (Always Encrypted)

Opis wymagania:

System bazodanowy musi wspierać funkcję "Zawsze szyfrowane" (Always Encrypted), która zapewnia ochronę danych przechowywanych w bazie danych poprzez szyfrowanie na poziomie kolumn. Funkcja ta pozwala na szyfrowanie danych w spoczynku i podczas ich przetwarzania, zapewniając jednocześnie, że klucze szyfrowania są zarządzane poza bazą danych, co zwiększa bezpieczeństwo i prywatność danych.

Kluczowe aspekty:

- **Szyfrowanie na poziomie kolumn:** System musi umożliwiać szyfrowanie danych na poziomie poszczególnych kolumn tabeli, co zapewnia, że wrażliwe informacje są chronione podczas przechowywania i przetwarzania.
- **Zarządzanie kluczami szyfrowania:** Klucze szyfrowania muszą być zarządzane w bezpieczny sposób, z opcją przechowywania ich w bezpiecznych lokalizacjach zewnętrznych, takich jak moduły sprzętowe bezpieczeństwa (HSM) lub usługi zarządzania kluczami.
- **Bez wpływu na aplikacje:** Funkcja Always Encrypted powinna działać w sposób transparentny dla aplikacji i użytkowników, zapewniając szyfrowanie i deszyfrowanie danych bez potrzeby modyfikowania kodu aplikacji.

Nr sprawy: BF-IV.2370.26.2024

Załącznik nr 1 do SWZ/ nr 1 do umowy

- **Wsparcie dla różnych algorytmów szyfrowania:** System musi oferować wsparcie dla różnych algorytmów szyfrowania, umożliwiając wybór odpowiedniego mechanizmu zabezpieczeń w zależności od wymagań bezpieczeństwa.

Cel:

Ochrona wrażliwych danych poprzez szyfrowanie na poziomie kolumn, zapewniając jednocześnie, że zarządzanie kluczami szyfrowania odbywa się poza bazą danych, co zwiększa bezpieczeństwo i prywatność danych.

Tytuł wymagania: SQL.08.2024 - Zabezpieczenia na poziomie wierszy (Row-level Security)

Opis wymagania:

System bazodanowy musi obsługiwać funkcję zabezpieczeń na poziomie wierszy (Row-level Security), która pozwala na kontrolowanie dostępu do danych na poziomie poszczególnych wierszy w tabeli. Funkcja ta umożliwi tworzenie reguł, które ograniczają widoczność i modyfikowanie danych przez użytkowników na podstawie zdefiniowanych kryteriów, zapewniając wyższy poziom ochrony danych w środowiskach wieloużytkownikowych.

Kluczowe aspekty:

- **Precyzyjna kontrola dostępu:** System musi umożliwiać definiowanie reguł, które ograniczają dostęp użytkowników do określonych wierszy w tabeli, w zależności od ich uprawnień lub ról.
- **Dynamiczne filtrowanie danych:** System powinien dynamicznie filtrować dane na podstawie zasad dostępu bez potrzeby modyfikowania aplikacji, co zapewnia elastyczność i łatwość zarządzania dostępem.
- **Zarządzanie uprawnieniami:** Administratorzy powinni mieć możliwość definiowania i zarządzania politykami dostępu na poziomie wierszy w sposób centralny, zapewniając łatwe wdrożenie reguł w różnych tabelach i bazach danych.
- **Wsparcie dla środowisk wieloużytkownikowych:** Funkcja zabezpieczeń na poziomie wierszy musi być w pełni zgodna ze środowiskami wieloużytkownikowymi, gdzie różne grupy użytkowników mają różny poziom dostępu do tych samych danych.

Cel:

Zapewnienie precyzyjnej kontroli dostępu do danych na poziomie wierszy, co zwiększa bezpieczeństwo i ochronę danych w środowiskach wieloużytkownikowych, umożliwiając ograniczenie widoczności danych zgodnie z politykami organizacji.

Tytuł wymagania: SQL.09.2024 - Dynamiczne maskowanie danych (Dynamic Data Masking)

Opis wymagania:

System bazodanowy musi obsługiwać funkcję dynamicznego maskowania danych, która

Nr sprawy: BF-IV.2370.26.2024

Załącznik nr 1 do SWZ/ nr 1 do umowy

pozwała na ograniczenie widoczności wrażliwych informacji poprzez wyświetlanie danych w zamaskowanej formie dla nieuprawnionych użytkowników. Maskowanie odbywa się w czasie rzeczywistym, bez zmiany rzeczywistych danych przechowywanych w bazie, co zapewnia dodatkową warstwę ochrony.

Kluczowe aspekty:

- **Maskowanie w czasie rzeczywistym:** System musi dynamicznie maskować dane wrażliwe podczas ich odczytu przez nieuprawnionych użytkowników, bez wpływu na integralność i dokładność danych w bazie.
- **Elastyczne reguły maskowania:** Administratorzy powinni mieć możliwość definiowania reguł maskowania dla różnych kolumn, tak aby różne dane mogły być maskowane na różne sposoby (np. pełne zamaskowanie, częściowe ukrycie).
- **Bez wpływu na aplikacje:** Funkcja maskowania powinna działać transparentnie dla aplikacji, bez potrzeby modyfikowania kodu, co pozwala na szybkie wdrożenie w istniejących systemach.
- **Kontrola dostępu:** System musi umożliwiać przypisywanie uprawnień do przeglądania pełnych danych lub ich zamaskowanych wersji w zależności od ról użytkowników.

Cel:

Ochrona wrażliwych danych poprzez ograniczenie dostępu do pełnych informacji dla nieuprawnionych użytkowników dzięki dynamicznemu maskowaniu, bez zmiany danych w bazie i bez konieczności modyfikacji aplikacji.

Tytuł wymagania: SQL.10.2024 - Audytowanie na poziomie bazy danych

Opis wymagania:

System bazodanowy musi obsługiwać zaawansowane funkcje audytowania, które umożliwiają monitorowanie i rejestrowanie wszystkich operacji wykonywanych na poziomie bazy danych. Funkcja audytowania powinna obejmować śledzenie działań użytkowników, zmian w strukturze bazy oraz dostępu do danych, co zapewnia pełną kontrolę i możliwość analizy operacji w celu zapewnienia zgodności z przepisami i standardami bezpieczeństwa.

Kluczowe aspekty:

- **Monitorowanie aktywności użytkowników:** System musi rejestrować operacje wykonywane przez użytkowników, takie jak logowanie, wykonywanie zapytań, modyfikacje danych oraz zmiany uprawnień.
- **Śledzenie zmian strukturalnych:** System powinien audytować wszelkie zmiany w strukturze bazy danych, w tym tworzenie, modyfikowanie i usuwanie tabel, indeksów oraz widoków.
- **Rejestrowanie dostępu do danych:** Funkcja audytowania powinna umożliwiać śledzenie dostępu do danych, zwłaszcza wrażliwych, w celu wykrywania potencjalnych naruszeń bezpieczeństwa.

Nr sprawy: BF-IV.2370.26.2024

Załącznik nr 1 do SWZ/ nr 1 do umowy

- **Konfigurowalne zasady audytowania:** Administratorzy powinni mieć możliwość definiowania elastycznych zasad audytowania, w tym wybierania, które zdarzenia mają być monitorowane i zapisywane.
- **Przechowywanie dzienników audytowych:** System musi zapewniać bezpieczne przechowywanie dzienników audytowych z możliwością ich archiwizacji i analizowania, zgodnie z wymaganiami prawnymi i organizacyjnymi.

Cel:

Zapewnienie pełnej przejrzystości operacji wykonywanych na bazie danych oraz umożliwienie identyfikowania i reagowania na potencjalne naruszenia bezpieczeństwa poprzez kompleksowe audytowanie działań użytkowników i zmian w bazie danych.

Tytuł wymagania: SQL.11.2024 - Partycjonowanie tabel i indeksów

Opis wymagania:

System bazodanowy musi obsługiwać funkcję partycjonowania tabel i indeksów, która umożliwia dzielenie dużych zbiorów danych na mniejsze, bardziej zarządzalne części (partycje). Partycjonowanie powinno poprawiać wydajność operacji na dużych wolumenach danych, umożliwiając optymalizację zapytań oraz zarządzanie danymi na poziomie partycji.

Kluczowe aspekty:

- **Partycjonowanie poziome:** System musi umożliwiać podział tabel na partycje na podstawie wartości w określonych kolumnach (np. zakresów dat), co pozwala na równomierne rozłożenie danych i operacji w różnych segmentach dysku.
- **Partycjonowanie indeksów:** System powinien wspierać partycjonowanie indeksów w sposób spójny z partycjonowaniem tabel, co poprawia wydajność operacji wyszukiwania i przetwarzania danych.
- **Zarządzanie partycjami:** System musi umożliwiać łatwe zarządzanie partycjami, w tym dodawanie, usuwanie oraz przenoszenie partycji bez wpływu na działanie całej tabeli, co zapewnia elastyczność w administrowaniu danymi.
- **Optymalizacja zapytań:** Funkcja partycjonowania musi współpracować z optymalizatorem zapytań, co pozwala na wykonywanie operacji tylko na wybranych partycjach, zwiększając wydajność zapytań dotyczących dużych zbiorów danych.

Cel:

Zwiększenie wydajności i efektywności zarządzania danymi poprzez umożliwienie podziału dużych tabel i indeksów na mniejsze, bardziej zarządzalne części, co pozwala na optymalizację operacji bazodanowych oraz łatwiejsze zarządzanie danymi w środowiskach o dużej skali.

Tytuł wymagania: SQL.12.2024 - In-Memory OLTP

Opis wymagania:

System bazodanowy musi obsługiwać funkcję przetwarzania transakcji w pamięci (In-Memory OLTP), która umożliwia przechowywanie i przetwarzanie danych w pamięci operacyjnej zamiast na dysku. Funkcja ta pozwala na znaczne przyspieszenie operacji przetwarzania

Nr sprawy: BF-IV.2370.26.2024

Załącznik nr 1 do SWZ/ nr 1 do umowy

transakcji (OLTP) poprzez eliminację opóźnień związanych z dostępem do danych na dysku, co zwiększa wydajność i skalowalność systemu.

Kluczowe aspekty:

- **Tabele w pamięci:** System musi umożliwiać tworzenie tabel w pamięci operacyjnej, które są zoptymalizowane pod kątem szybkości dostępu i przetwarzania danych, co przyspiesza transakcje OLTP.
- **Indeksy nieblokujące:** System powinien obsługiwać indeksy w pamięci, które nie powodują blokowania dostępu do danych, co umożliwia jednoczesne wykonywanie wielu operacji na tych samych danych bez spadku wydajności.
- **Kompilacja natywna:** System musi umożliwiać kompilację natywną procedur składowanych w celu optymalizacji przetwarzania danych w pamięci i dalszego przyspieszenia operacji.
- **Integracja z tradycyjnymi tabelami:** System powinien wspierać współpracę między tabelami w pamięci a tradycyjnymi tabelami na dysku, co pozwala na elastyczne zarządzanie danymi w zależności od potrzeb wydajnościowych.

Cel:

Znaczące zwiększenie wydajności przetwarzania transakcji online poprzez eliminację opóźnień związanych z operacjami dyskowymi dzięki przetwarzaniu danych w pamięci operacyjnej. System zapewnia lepszą skalowalność i szybkość działania, szczególnie w intensywnie transakcyjnych środowiskach.

Tytuł wymagania: SQL.13.2024 - Indeksy kolumnowe (Columnstore Indexes)

Opis wymagania:

System bazodanowy musi obsługiwać indeksy kolumnowe, które umożliwiają przechowywanie danych w formie kolumn zamiast wierszy. Indeksy kolumnowe są zoptymalizowane pod kątem zapytań analitycznych (OLAP) i umożliwiają szybsze wykonywanie operacji na dużych zestawach danych, takich jak agregacje i analizy.

Kluczowe aspekty:

- **Przechowywanie danych w kolumnach:** System musi umożliwiać przechowywanie danych w formie kolumn, co pozwala na efektywniejsze kompresowanie danych oraz szybsze przetwarzanie zapytań analitycznych.
- **Kompresja danych:** Indeksy kolumnowe powinny obsługiwać zaawansowane techniki kompresji, które zmniejszają objętość danych przechowywanych na dysku oraz poprawiają wydajność operacji I/O.
- **Wydajność zapytań analitycznych:** System musi optymalizować zapytania analityczne, takie jak agregacje, filtrowanie i sortowanie, poprzez efektywne wykorzystanie indeksów kolumnowych, co znacząco zwiększa wydajność przetwarzania dużych zbiorów danych.

Nr sprawy: BF-IV.2370.26.2024

Załącznik nr 1 do SWZ/ nr 1 do umowy

- **Integracja z tabelami wierszowymi:** System powinien wspierać współpracę między tabelami z indeksami kolumnowymi a tradycyjnymi tabelami wierszowymi, umożliwiając elastyczne zarządzanie danymi i optymalizację zapytań.

Cel:

Zwiększenie wydajności zapytań analitycznych i przetwarzania dużych zbiorów danych poprzez wykorzystanie indeksów kolumnowych, co pozwala na efektywne kompresowanie danych i szybkie wykonywanie operacji analitycznych.

Tytuł wymagania: SQL.14.2024 - Równoległe przetwarzanie zapytań (Parallel Query Processing)

Opis wymagania:

System bazodanowy musi obsługiwać funkcję równoległego przetwarzania zapytań, która umożliwia jednoczesne rozdzielanie i wykonywanie zadań przetwarzania zapytań na wiele rdzeni procesora. Funkcja ta pozwala na przyspieszenie skomplikowanych zapytań oraz operacji na dużych zestawach danych, zwiększając ogólną wydajność systemu.

Kluczowe aspekty:

- **Rozdzielanie zadań:** System musi automatycznie rozdzielać zadania przetwarzania zapytań na wiele rdzeni procesora, co pozwala na równoległe wykonywanie operacji, takich jak filtrowanie, sortowanie i agregacja danych.
- **Optymalizacja zapytań:** System powinien automatycznie analizować zapytania i dobrać odpowiednią liczbę wątków oraz zasobów do równoległego przetwarzania, aby maksymalnie wykorzystać dostępne zasoby sprzętowe.
- **Wsparcie dla zapytań OLAP i OLTP:** System musi wspierać równoległe przetwarzanie zarówno dla zapytań analitycznych (OLAP), jak i transakcyjnych (OLTP), aby zapewnić elastyczność i wydajność w różnych scenariuszach użytkowania.
- **Skalowalność:** Funkcja równoległego przetwarzania powinna skalować się wraz ze wzrostem liczby rdzeni procesora i ilości dostępnej pamięci, co zapewnia optymalną wydajność w środowiskach o dużej skali.

Cel:

Zwiększenie wydajności systemu poprzez równoległe przetwarzanie skomplikowanych zapytań na wielu rdzeniach procesora, co pozwala na szybsze operacje na dużych zestawach danych oraz lepsze wykorzystanie zasobów sprzętowych.

Tytuł wymagania: SQL.15.2024 - Magazyn zapytań (Query Store)

Opis wymagania:

System bazodanowy musi obsługiwać funkcję Magazynu zapytań (Query Store), która rejestruje historię wykonywanych zapytań, ich planów wykonania oraz statystyk wydajności. Magazyn zapytań umożliwia analizowanie zachowań zapytań, identyfikowanie problemów wydajnościowych i optymalizację planów zapytań, co prowadzi do poprawy działania systemu.

Nr sprawy: BF-IV.2370.26.2024
 Załącznik nr 1 do SWZ/ nr 1 do umowy

Kluczowe aspekty:

- **Rejestrowanie zapytań i planów:** System musi automatycznie przechowywać informacje o wykonywanych zapytaniach, planach wykonania oraz ich wydajności, co pozwala na śledzenie historii i analizy zapytań.
- **Analiza zmian w planach zapytań:** Magazyn zapytań powinien umożliwiać analizę zmian w planach zapytań, co pozwala na szybkie wykrywanie degradacji wydajności wynikającej z niewłaściwego optymalizowania zapytań.
- **Stałe monitorowanie wydajności:** System musi umożliwiać stałe monitorowanie wydajności zapytań w czasie rzeczywistym, co pomaga w identyfikacji zapytań, które mogą powodować spowolnienia lub nadmierne obciążenia systemu.
- **Wymuszanie planów wykonania:** Administratorzy powinni mieć możliwość wymuszania określonych planów wykonania zapytań, aby zapewnić stabilną wydajność i uniknąć problemów wynikających z nieefektywnych planów.

Cel:

Poprawa wydajności systemu oraz stabilność zapytań poprzez monitorowanie i optymalizację planów zapytań, a także umożliwienie administratorom szybkiej identyfikacji i rozwiązywania problemów z wydajnością.

Tytuł wymagania: SQL.16.2024 - Inteligentne przetwarzanie zapytań (Intelligent Query Processing)

Opis wymagania:

System bazodanowy musi obsługiwać funkcję inteligentnego przetwarzania zapytań (Intelligent Query Processing), która automatycznie optymalizuje wykonywanie zapytań na podstawie analizy ich charakterystyk i statystyk. Funkcja ta poprawia wydajność bez konieczności modyfikowania kodu aplikacji, umożliwiając lepsze wykorzystanie zasobów i szybsze przetwarzanie danych w różnorodnych scenariuszach.

Kluczowe aspekty:

- **Adaptacyjne plany zapytań:** System musi dynamicznie dostosowywać plany zapytań w czasie ich wykonywania, uwzględniając rzeczywiste statystyki i warunki, co poprawia wydajność zapytań.
- **Ulepszone algorytmy optymalizacji:** Funkcja inteligentnego przetwarzania zapytań powinna wykorzystywać zaawansowane algorytmy, takie jak automatyczne dostrajanie parametrów zapytań, aby zapewnić optymalne plany wykonania.
- **Obsługa dla dużych i złożonych zapytań:** System musi efektywnie radzić sobie z przetwarzaniem dużych, złożonych zapytań, automatycznie optymalizując ich wykonanie poprzez eliminowanie nieefektywnych operacji lub planów.
- **Minimalizacja przestojów i spadków wydajności:** Inteligentne przetwarzanie zapytań powinno automatycznie identyfikować i rozwiązywać problemy wydajnościowe wynikające z nieoptymalnych planów, co minimalizuje konieczność interwencji administratorów.

Nr sprawy: BF-IV.2370.26.2024
 Załącznik nr 1 do SWZ/ nr 1 do umowy

Cel:

Automatyczne zwiększenie wydajności przetwarzania zapytań dzięki zaawansowanej optymalizacji i adaptacji planów zapytań w czasie rzeczywistym, co pozwala na lepsze wykorzystanie zasobów i stabilną wydajność aplikacji bez konieczności ręcznej optymalizacji.

Tytuł wymagania: SQL.17.2024 - Automatyczne dostrajanie (Automatic Tuning)

Opis wymagania:

System bazodanowy musi obsługiwać funkcję automatycznego dostrajania, która automatycznie identyfikuje i rozwiązuje problemy z wydajnością zapytań oraz konfiguracją bazy danych. Funkcja ta monitoruje działanie systemu w czasie rzeczywistym, sugeruje optymalizacje lub samodzielnie wdraża zmiany, takie jak modyfikacja indeksów lub planów zapytań, aby zapewnić optymalną wydajność.

Kluczowe aspekty:

- **Automatyczna rekomendacja indeksów:** System musi analizować wzorce zapytań i automatycznie sugerować tworzenie, usuwanie lub modyfikację indeksów, co poprawia wydajność wyszukiwania i przetwarzania danych.
- **Automatyczne wymuszanie planów zapytań:** System powinien monitorować wydajność zapytań i automatycznie wymuszać optymalne plany wykonania, zapobiegając degradacji wydajności w przypadku nieefektywnych planów.
- **Monitorowanie wydajności w czasie rzeczywistym:** Funkcja automatycznego dostrajania musi stale monitorować działanie systemu i podejmować działania naprawcze, takie jak optymalizacja parametrów zapytań lub zmiany w konfiguracji bazy danych.
- **Historia i analiza optymalizacji:** System powinien przechowywać historię wykonanych działań optymalizacyjnych oraz wyników ich wprowadzenia, umożliwiając administratorom analizę wpływu tych zmian na wydajność.

Cel:

Automatyczne poprawianie wydajności systemu poprzez identyfikację i wdrażanie zmian w konfiguracji, indeksach oraz planach zapytań, co pozwala na minimalizację ręcznej interwencji oraz zapewnia optymalną wydajność bazy danych w sposób ciągły.

Tytuł wymagania: SQL.18.2024 - Zarządzanie zasobami (Resource Governor)

Opis wymagania:

System bazodanowy musi obsługiwać funkcję zarządzania zasobami (Resource Governor), która umożliwia monitorowanie i kontrolowanie alokacji zasobów systemowych, takich jak procesor i pamięć, między różnymi obciążeniami w bazie danych. Funkcja ta pozwala na przypisywanie priorytetów i limitów zasobów do określonych grup użytkowników lub zapytań, co pomaga w zapewnieniu stabilności i wydajności systemu, nawet w przypadku intensywnych operacji.

Nr sprawy: BF-IV.2370.26.2024
 Załącznik nr 1 do SWZ/ nr 1 do umowy

Kluczowe aspekty:

- **Kontrola przydziału zasobów:** System musi umożliwiać definiowanie zasad alokacji procesora, pamięci i innych zasobów systemowych dla różnych obciążeń, takich jak zapytania analityczne (OLAP) czy operacje transakcyjne (OLTP), w celu zminimalizowania ryzyka przeciążenia systemu.
- **Priorytetyzacja obciążeń:** Administratorzy powinni mieć możliwość przypisywania priorytetów dla różnych grup użytkowników lub aplikacji, co pozwala na lepsze zarządzanie zasobami w przypadku konkurujących zadań.
- **Monitorowanie zasobów w czasie rzeczywistym:** System musi zapewniać możliwość monitorowania wykorzystania zasobów przez różne obciążenia w czasie rzeczywistym, umożliwiając dynamiczne dostosowywanie alokacji w zależności od aktualnych potrzeb.
- **Izolacja zasobów:** System powinien wspierać izolację zasobów między różnymi grupami, co zapobiega sytuacjom, w których intensywne zapytania mogą nadmiernie obciążać system i wpływać na wydajność innych operacji.

Cel:

Efektywne zarządzanie zasobami systemowymi, zapewnienie stabilnej wydajności oraz zapobieganie przeciążeniu systemu poprzez przypisywanie limitów i priorytetów dla różnych obciążeń, co pozwala na optymalizację działania bazy danych w środowiskach o zróżnicowanych wymaganiach.

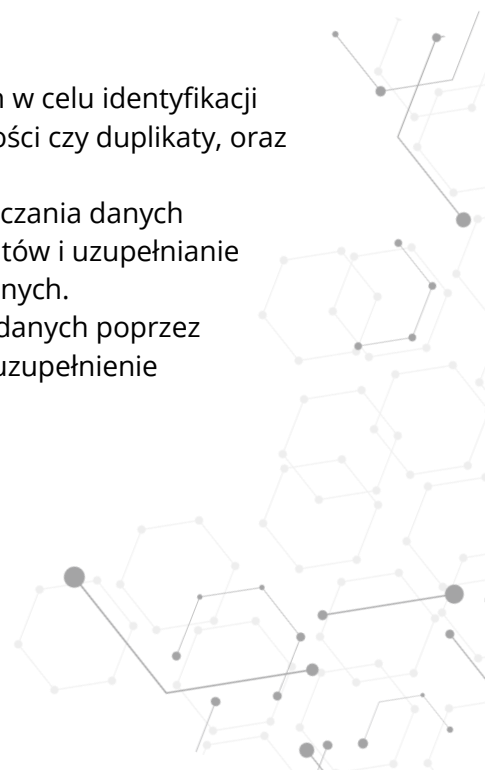
Tytuł wymagania: **SQL.19.2024 - Usługi Jakości Danych (Data Quality Services)**

Opis wymagania:

System bazodanowy musi obsługiwać Usługi Jakości Danych (Data Quality Services), które umożliwiają zarządzanie i poprawę jakości danych poprzez ich profilowanie, oczyszczanie i wzbogacanie. Funkcja ta zapewnia narzędzia do identyfikacji i naprawy problemów z jakością danych, takich jak błędy, duplikaty i niekompletne informacje.

Kluczowe aspekty:

- **Profilowanie danych:** System musi umożliwiać analizę danych w celu identyfikacji problemów, takich jak nieprawidłowe formaty, brakujące wartości czy duplikaty, oraz dostarczać raporty na temat ich jakości.
- **Oczyszczanie danych:** Usługi powinny wspierać proces oczyszczania danych poprzez automatyczne korygowanie błędów, usuwanie duplikatów i uzupełnianie brakujących informacji, co zapewnia poprawność i spójność danych.
- **Wzbogacanie danych:** System musi umożliwiać wzbogacanie danych poprzez integrację z zewnętrznymi źródłami informacji, co pozwala na uzupełnienie brakujących danych i zwiększenie ich wartości.



Nr sprawy: BF-IV.2370.26.2024

Załącznik nr 1 do SWZ/ nr 1 do umowy

- **Zarządzanie regułami jakości:** System powinien oferować możliwość definiowania reguł i polityk jakości danych, które mogą być stosowane do automatycznego monitorowania i poprawiania jakości danych w bazie.

Cel:

Poprawa jakości danych poprzez profilowanie, oczyszczanie i wzbogacanie, co prowadzi do zwiększenia dokładności, spójności i użyteczności danych w systemie oraz wspiera podejmowanie decyzji na podstawie rzetelnych informacji.

Tytuł wymagania: SQL.20.2024 - Usługi Zarządzania Danymi Głównymi (Master Data Services)

Opis wymagania:

System bazodanowy musi obsługiwać Usługi Zarządzania Danymi Głównymi (Master Data Services), które umożliwiają centralne zarządzanie danymi głównymi w organizacji. Funkcja ta pozwala na definiowanie, organizowanie i utrzymywanie kluczowych danych, takich jak informacje o klientach, produktach czy lokalizacjach, zapewniając spójność i integralność danych w różnych systemach i aplikacjach.

Kluczowe aspekty:

- **Centralne zarządzanie danymi głównymi:** System musi umożliwiać tworzenie i utrzymywanie jednego źródła prawdy dla kluczowych danych, co zapewnia ich spójność i zgodność w całej organizacji.
- **Wersjonowanie danych:** System powinien wspierać wersjonowanie danych głównych, co pozwala na śledzenie zmian i zarządzanie różnymi wersjami danych w miarę ich ewolucji.
- **Zarządzanie hierarchiami:** System musi umożliwiać tworzenie i zarządzanie hierarchiami danych głównych, co pozwala na lepszą organizację oraz odniesienie danych do różnych kategorii czy grup.
- **Integracja z innymi systemami:** Usługi Zarządzania Danymi Głównymi powinny wspierać integrację z innymi systemami i aplikacjami w organizacji, zapewniając aktualność i spójność danych w całym środowisku IT.
- **Zarządzanie regułami biznesowymi:** System powinien umożliwiać definiowanie i egzekwowanie reguł biznesowych, które zapewniają zgodność i integralność danych zgodnie z wymaganiami organizacyjnymi.

Cel:

Zapewnienie centralnego zarządzania danymi głównymi w celu utrzymania ich spójności i integralności w całej organizacji, co pozwala na efektywne zarządzanie kluczowymi informacjami i wspiera podejmowanie decyzji opartych na dokładnych danych.

Tytuł wymagania: SQL.21.2024 - Usługi analityczne (Analysis Services)

Opis wymagania:

System bazodanowy musi obsługiwać usługi analityczne, które umożliwiają zaawansowaną

Nr sprawy: BF-IV.2370.26.2024

Załącznik nr 1 do SWZ/ nr 1 do umowy

analizę danych i tworzenie wielowymiarowych modeli analitycznych oraz modeli tabelarycznych. Funkcja ta powinna wspierać proces przetwarzania danych w celu zapewnienia szybkich i złożonych analiz na dużych zbiorach danych, co jest niezbędne do wspierania procesów decyzyjnych w organizacji.

Kluczowe aspekty:

- **Tworzenie modeli wielowymiarowych:** System musi wspierać tworzenie wielowymiarowych kostek OLAP, które umożliwiają zaawansowaną analizę danych według wielu wymiarów, takich jak czas, region, produkt itp.
- **Modele tabelaryczne:** System powinien wspierać modele tabelaryczne, które oferują elastyczną i wydajną analizę danych w środowisku analitycznym przy wykorzystaniu języka DAX.
- **Zaawansowane funkcje agregacji i kalkulacji:** System musi obsługiwać zaawansowane funkcje agregacji oraz kalkulacji, co pozwala na szybkie przetwarzanie dużych ilości danych i dostarczanie wniosków w czasie rzeczywistym.
- **Integracja z narzędziami BI:** Usługi analityczne muszą być w pełni zintegrowane z narzędziami do analizy biznesowej (BI), umożliwiając tworzenie interaktywnych raportów i wizualizacji danych.
- **Zarządzanie wydajnością:** System musi zapewniać optymalizację przetwarzania zapytań analitycznych, co umożliwi szybki dostęp do danych i analizy nawet w przypadku bardzo dużych zbiorów danych.

Cel:

Umożliwienie zaawansowanej analizy danych poprzez tworzenie wielowymiarowych i tabelarycznych modeli, które wspierają złożone analizy biznesowe, agregacje i kalkulacje, pomagając w podejmowaniu szybszych i bardziej świadomych decyzji na podstawie dostępnych danych.

Tytuł wymagania: SQL.22.2024 - Usługi raportowania (Reporting Services)

Opis wymagania:

System bazodanowy musi obsługiwać usługi raportowania, które umożliwiają tworzenie, zarządzanie oraz dostarczanie interaktywnych raportów na podstawie danych przechowywanych w bazie. Usługi raportowania powinny zapewniać szeroki zakres opcji formatowania, umożliwiając generowanie raportów w różnych formatach, a także wsparcie dla automatycznego harmonogramowania i dystrybucji raportów do użytkowników końcowych.

Kluczowe aspekty:

- **Tworzenie raportów:** System musi wspierać tworzenie zaawansowanych raportów z różnymi opcjami formatowania, w tym raporty tabelaryczne, macierzowe, wykresy oraz raporty oparte na elementach wizualnych.

Nr sprawy: BF-IV.2370.26.2024

Załącznik nr 1 do SWZ/ nr 1 do umowy

- **Interaktywne raporty:** Umożliwienie tworzenia interaktywnych raportów, które pozwalają użytkownikom na filtrowanie, sortowanie i eksportowanie danych bezpośrednio z poziomu raportu.
- **Wsparcie dla wielu formatów:** System powinien wspierać generowanie raportów w różnych formatach, takich jak PDF, Excel, CSV, Word i HTML, co umożliwia ich łatwą integrację i udostępnianie.
- **Automatyczne harmonogramowanie:** Usługi raportowania muszą umożliwiać automatyczne harmonogramowanie generowania i dystrybucji raportów na podstawie zdefiniowanych reguł i harmonogramów.
- **Bezpieczeństwo i kontrola dostępu:** System musi zapewniać zarządzanie uprawnieniami dostępu do raportów, co pozwala na kontrolowanie, które raporty mogą być generowane i przeglądane przez poszczególnych użytkowników lub grupy.

Cel:

Zapewnienie elastycznego i zaawansowanego systemu raportowania, który wspiera tworzenie interaktywnych raportów, automatyczne harmonogramowanie i dystrybucję, co umożliwia lepszą wizualizację i analizę danych oraz wspiera procesy decyzyjne w organizacji.

Tytuł wymagania: SQL.23.2024 - Usługi integracyjne (Integration Services)

Opis wymagania:

System bazodanowy musi obsługiwać usługi integracyjne, które umożliwiają efektywne przenoszenie, przekształcanie oraz integrację danych z różnych źródeł do centralnej bazy danych. Funkcja ta powinna zapewniać narzędzia do ekstrakcji, transformacji i ładowania danych (ETL), umożliwiając automatyzację procesów integracyjnych i zapewniając spójność danych w systemie.

Kluczowe aspekty:

- **Procesy ETL:** System musi wspierać kompleksowe procesy ETL (ekstrakcja, transformacja, ładowanie), które umożliwiają pobieranie danych z różnych źródeł, ich przekształcanie oraz ładowanie do centralnej bazy danych lub hurtowni danych.
- **Integracja danych z wielu źródeł:** System powinien obsługiwać integrację danych z różnych źródeł, takich jak bazy danych, pliki, aplikacje i serwisy sieciowe, co zapewnia elastyczność w pozyskiwaniu danych.
- **Automatyzacja przepływów danych:** Usługi integracyjne muszą umożliwiać tworzenie zautomatyzowanych przepływów danych, które mogą być harmonogramowane i monitorowane, co zapewnia regularne i niezawodne zasilanie bazy danych aktualnymi danymi.
- **Transformacja i czyszczenie danych:** System powinien oferować narzędzia do przekształcania danych, takie jak agregacje, filtrowanie, mapowanie oraz czyszczenie, co poprawia jakość i spójność danych przed ich załadowaniem.
- **Monitorowanie i logowanie:** System musi zapewniać możliwość monitorowania procesów ETL oraz rejestrowania informacji o wykonanych operacjach, błędach i wydajności w celu zapewnienia pełnej kontroli nad procesami integracyjnymi.

Nr sprawy: BF-IV.2370.26.2024
 Załącznik nr 1 do SWZ/ nr 1 do umowy

Cel:

Zabezpieczenie wydajnych i niezawodnych procesów integracji danych poprzez zautomatyzowane przepływy ETL, co umożliwia łączenie danych z różnych źródeł, przekształcanie ich i ładowanie do bazy danych, wspierając spójność i dostępność danych w organizacji.

Tytuł wymagania: SQL.24.2024 - Usługi uczenia maszynowego (Machine Learning Services)

Opis wymagania:

System bazodanowy musi obsługiwać usługi uczenia maszynowego, które umożliwiają uruchamianie modeli i skryptów opartych na językach R i Python bezpośrednio w bazie danych. Funkcja ta powinna wspierać przetwarzanie danych, budowanie modeli predykcyjnych oraz analizę danych w czasie rzeczywistym, co pozwala na integrację zaawansowanej analityki z systemami bazodanowymi.

Kluczowe aspekty:

- **Obsługa języków R i Python:** System musi umożliwiać uruchamianie skryptów w językach R i Python bezpośrednio na danych w bazie, co pozwala na wykorzystywanie popularnych bibliotek do uczenia maszynowego i analiz.
- **Budowanie modeli predykcyjnych:** System powinien wspierać tworzenie, trenowanie i wdrażanie modeli uczenia maszynowego bez konieczności przenoszenia danych poza bazę, co minimalizuje czas przetwarzania i zapewnia bezpieczeństwo danych.
- **Wykonywanie modeli w czasie rzeczywistym:** System musi umożliwiać wykonywanie modeli predykcyjnych i skryptów analitycznych w czasie rzeczywistym, co pozwala na bieżące analizowanie danych i wspieranie decyzji operacyjnych.
- **Integracja z istniejącymi danymi:** Usługi uczenia maszynowego muszą być w pełni zintegrowane z bazą danych, co umożliwia łatwe korzystanie z dostępnych danych operacyjnych w modelach analitycznych.
- **Monitorowanie i wersjonowanie modeli:** System powinien wspierać monitorowanie efektywności modeli oraz ich wersjonowanie, co pozwala na zarządzanie cyklem życia modeli uczenia maszynowego i utrzymanie ich aktualności.

Cel:

Zapewnienie zaawansowanej analityki danych poprzez integrację usług uczenia maszynowego bezpośrednio w bazie danych, co umożliwia budowanie modeli predykcyjnych i wykonywanie analiz w czasie rzeczywistym, wspierając procesy decyzyjne w organizacji.

Tytuł wymagania: SQL.25.2024 - PolyBase

Opis wymagania:

System bazodanowy musi obsługiwać funkcję PolyBase, która umożliwia integrację danych przechowywanych w zewnętrznych źródłach, takich jak hurtownie danych, systemy plików Hadoop czy usługi w chmurze, z danymi w bazie. Funkcja ta pozwala na wykonywanie zapytań

Nr sprawy: BF-IV.2370.26.2024

Załącznik nr 1 do SWZ/ nr 1 do umowy

T-SQL na danych pochodzących z różnych źródeł bez konieczności ich przenoszenia, co upraszcza zarządzanie dużymi zbiorami danych i analizę.

Kluczowe aspekty:

- **Dostęp do zewnętrznych źródeł danych:** System musi umożliwiać wykonywanie zapytań na danych z różnych źródeł, takich jak serwery SQL, Hadoop, Azure Blob Storage, Amazon S3 oraz inne systemy zewnętrzne, bez konieczności kopiowania danych do bazy.
- **Użycie zapytań T-SQL:** PolyBase powinien umożliwiać użytkownikom wykonywanie standardowych zapytań T-SQL na danych zewnętrznych, co zapewnia spójność i łatwość integracji w istniejącym środowisku bazodanowym.
- **Zarządzanie dużymi zbiorami danych:** System powinien wspierać przetwarzanie i analizę dużych wolumenów danych z zewnętrznych źródeł, co umożliwia łatwiejsze zarządzanie danymi pochodzącymi z różnych platform.
- **Efektywna integracja danych:** PolyBase musi zapewniać optymalizację przetwarzania zapytań poprzez minimalizowanie ruchu danych między bazą danych a zewnętrznymi źródłami, co zwiększa wydajność i obniża koszty operacyjne.

Cel:

Ułatwienie integracji i analizy danych pochodzących z różnych źródeł zewnętrznych, bez potrzeby ich przenoszenia, co pozwala na bardziej efektywne zarządzanie i analizę danych w złożonych środowiskach danych rozproszonych.

Tytuł wymagania: SQL.26.2024 - Rozszerzona baza danych (Stretch Database)

Opis wymagania:

System bazodanowy musi obsługiwać funkcję rozszerzonej bazy danych (Stretch Database), która umożliwia dynamiczne przenoszenie części danych z lokalnej bazy danych do chmury, bez wpływu na dostępność i wydajność operacji. Funkcja ta pozwala na efektywne zarządzanie przestrzenią dyskową, przechowywanie rzadko używanych danych w chmurze oraz optymalizację kosztów przechowywania, przy jednoczesnym zachowaniu dostępu do danych poprzez zapytania T-SQL.

Kluczowe aspekty:

- **Automatyczne przenoszenie danych:** System musi umożliwiać automatyczne przenoszenie starszych lub mniej używanych danych z lokalnej bazy danych do chmury, co optymalizuje przestrzeń dyskową i koszty przechowywania.
- **Bezproblemowy dostęp do danych:** Użytkownicy muszą mieć możliwość wykonywania zapytań T-SQL na danych zarówno lokalnych, jak i przeniesionych do chmury, bez konieczności modyfikacji aplikacji ani skomplikowanych procedur integracyjnych.
- **Skalowanie przechowywania danych:** Funkcja musi umożliwiać dynamiczne skalowanie zasobów przechowywania w chmurze, co pozwala na elastyczne

Nr sprawy: BF-IV.2370.26.2024

Załącznik nr 1 do SWZ/ nr 1 do umowy

zarządzanie dużymi zbiorami danych bez potrzeby zwiększania lokalnych zasobów sprzętowych.

- **Zarządzanie danymi historycznymi:** Stretch Database powinna wspierać efektywne zarządzanie danymi historycznymi, co pozwala na przenoszenie starszych danych do chmury, podczas gdy bardziej aktualne dane pozostają dostępne lokalnie.
- **Bezpieczeństwo danych w chmurze:** System musi zapewniać pełne bezpieczeństwo danych przeniesionych do chmury, w tym szyfrowanie i kontrolę dostępu, aby spełniać wymagania związane z ochroną danych.

Cel:

Zoptymalizowanie przechowywania danych i kosztów poprzez automatyczne przenoszenie rzadko używanych danych do chmury, przy jednoczesnym zachowaniu ich dostępności i wydajności operacji na tych danych.

Tytuł wymagania: SQL.27.2024 - Tabele tymczasowe (Temporal Tables)

Opis wymagania:

System bazodanowy musi obsługiwać funkcję tabel tymczasowych (Temporal Tables), która umożliwi automatyczne śledzenie i przechowywanie pełnej historii zmian danych w tabelach, pozwalając na łatwe przeglądanie wcześniejszych stanów danych. Funkcja ta zapewnia wgląd w przeszłe wersje danych bez potrzeby skomplikowanego zarządzania wersjami, co wspiera audyt, raportowanie oraz analizę historyczną.

Kluczowe aspekty:

- **Śledzenie zmian danych:** System musi automatycznie rejestrować każdą zmianę w tabelach temporalnych, zapisując poprzednie wersje danych i umożliwiając łatwe przeglądanie ich historii.
- **Przeglądanie danych z przeszłości:** System musi umożliwiać wykonywanie zapytań T-SQL, które pozwalają na analizę danych z dowolnego momentu w przeszłości, bez potrzeby tworzenia złożonych systemów do przechowywania wersji.
- **Zarządzanie danymi historycznymi:** System powinien automatycznie zarządzać danymi historycznymi, zapewniając odpowiednie miejsce do przechowywania danych archiwalnych bez wpływu na bieżącą wydajność.
- **Prosta konfiguracja:** Tabele temporalne muszą być łatwe w konfiguracji, bez potrzeby tworzenia skomplikowanych procedur zarządzania wersjami danych czy manualnego śledzenia zmian.
- **Audyt i zgodność z przepisami:** Funkcja powinna wspierać audyt i zapewniać zgodność z regulacjami prawnymi, które wymagają przechowywania pełnej historii danych, co jest kluczowe w branżach takich jak finanse czy opieka zdrowotna.

Cel:

Umożliwienie automatycznego śledzenia historii zmian danych, co wspiera audyt, analizę historyczną i raportowanie, zapewniając pełny dostęp do danych z przeszłości bez konieczności zarządzania skomplikowanymi mechanizmami archiwizacji.

Nr sprawy: BF-IV.2370.26.2024
 Załącznik nr 1 do SWZ/ nr 1 do umowy

Tytuł wymagania: SQL.28.2024 - Obsługa JSON

Opis wymagania:

System bazodanowy musi obsługiwać natywną obsługę formatu JSON (JavaScript Object Notation), umożliwiając przechowywanie, przetwarzanie i manipulowanie danymi w tym formacie. Funkcja ta powinna zapewniać wsparcie dla operacji takich jak analiza, parsowanie i generowanie dokumentów JSON, co pozwala na łatwą integrację z aplikacjami webowymi i innymi systemami, które korzystają z tego formatu.

Kluczowe aspekty:

- **Przechowywanie danych JSON:** System musi umożliwiać przechowywanie dokumentów JSON w tabelach, co pozwala na elastyczne zarządzanie półstrukturalnymi danymi w bazie.
- **Parsowanie i zapytania JSON:** System musi wspierać funkcje T-SQL do parsowania dokumentów JSON, umożliwiając wykonywanie zapytań na danych JSON, przekształcanie ich w kolumny tabel oraz manipulowanie nimi.
- **Generowanie JSON:** System powinien umożliwiać generowanie danych w formacie JSON z wyników zapytań SQL, co ułatwia ich integrację z aplikacjami wymagającymi tego formatu.
- **Elastyczna struktura danych:** Obsługa JSON pozwala na elastyczne przechowywanie danych o zmiennych schematach, co jest korzystne w przypadku aplikacji wymagających częstych zmian struktury danych.
- **Integracja z aplikacjami webowymi:** System musi wspierać płynną integrację z aplikacjami webowymi i systemami API, które powszechnie wykorzystują format JSON do przesyłania i wymiany danych.

Cel:

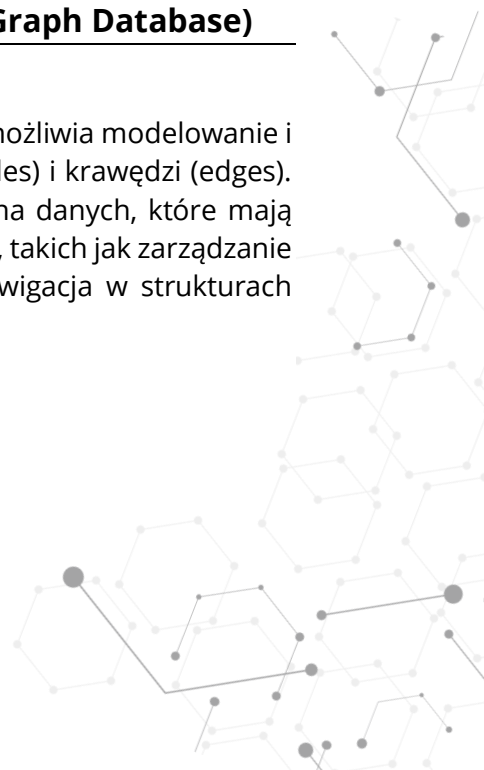
Zapewnienie elastycznego przechowywania i przetwarzania danych w formacie JSON, co umożliwi łatwą integrację z aplikacjami oraz systemami wykorzystującymi ten format, a także wspiera przetwarzanie półstrukturalnych danych w bazie danych.

Tytuł wymagania: SQL.29.2024 - Obsługa baz grafowych (Graph Database)

Opis wymagania:

System bazodanowy musi obsługiwać funkcję baz grafowych, która umożliwia modelowanie i zarządzanie danymi w postaci grafów, składających się z węzłów (nodes) i krawędzi (edges). Funkcja ta pozwala na przechowywanie oraz wykonywanie zapytań na danych, które mają silne relacje między sobą, co jest szczególnie przydatne w przypadkach, takich jak zarządzanie sieciami społecznymi, analizowanie relacji między obiektami lub nawigacja w strukturach hierarchicznych.

Kluczowe aspekty:



Nr sprawy: BF-IV.2370.26.2024

Załącznik nr 1 do SWZ/ nr 1 do umowy

- **Węzły i krawędzie:** System musi umożliwiać tworzenie węzłów, które reprezentują obiekty, oraz krawędzi, które opisują relacje między nimi. Każdy węzeł i krawędź musi mieć możliwość przechowywania dodatkowych atrybutów.
- **Zapytania grafowe:** System powinien wspierać zaawansowane zapytania grafowe, umożliwiające wyszukiwanie i analizę relacji między węzłami, takich jak znajdowanie powiązań, nawigowanie w hierarchiach, analizowanie ścieżek czy wyszukiwanie cykli.
- **Wydajność zapytań grafowych:** Funkcja baz grafowych powinna optymalizować wydajność operacji na dużych zbiorach powiązanych danych, zapewniając efektywne wykonywanie zapytań w sieciach relacji.
- **Zarządzanie złożonymi relacjami:** System musi umożliwiać zarządzanie złożonymi relacjami, w których obiekty mają wiele powiązań, co jest trudne do modelowania w tradycyjnych relacyjnych bazach danych.
- **Integracja z relacyjnym modelem danych:** System powinien wspierać mieszane modele danych, umożliwiając równoczesne korzystanie z relacyjnych i grafowych struktur danych, co pozwala na elastyczne modelowanie różnych typów danych w jednym środowisku.

Cel:

Umożliwienie przechowywania i analizy złożonych relacji między danymi poprzez obsługę grafowych struktur danych, co pozwala na optymalną analizę powiązań i struktur sieciowych w różnych aplikacjach, takich jak sieci społeczne, analizy zależności czy nawigacja hierarchiczna.

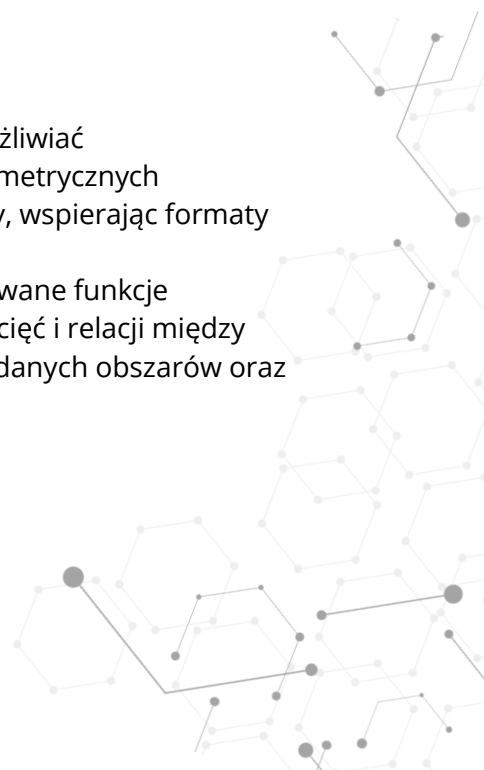
Tytuł wymagania: SQL.30.2024 - Obsługa danych przestrzennych (Spatial Data Support)

Opis wymagania:

System bazodanowy musi obsługiwać dane przestrzenne, umożliwiając przechowywanie, przetwarzanie i analizę danych geograficznych oraz geometrycznych. Funkcja ta powinna wspierać operacje na obiektach przestrzennych, takich jak punkty, linie i wielokąty, co pozwala na wykonywanie zapytań i analiz opartych na lokalizacjach, odległościach oraz relacjach przestrzennych.

Kluczowe aspekty:

- **Przechowywanie danych przestrzennych:** System musi umożliwiać przechowywanie danych geograficznych (Geography) oraz geometrycznych (Geometry), takich jak współrzędne punktów, linie oraz obszary, wspierając formaty zgodne z ogólnymi standardami danych przestrzennych.
- **Operacje przestrzenne:** System powinien wspierać zaawansowane funkcje przestrzenne, takie jak obliczanie odległości, sprawdzanie przecięć i relacji między obiektami przestrzennymi, określanie punktów należących do danych obszarów oraz operacje buforowania i tworzenia stref.



Nr sprawy: BF-IV.2370.26.2024

Załącznik nr 1 do SWZ/ nr 1 do umowy

- **Indeksy przestrzenne:** System musi wspierać indeksowanie danych przestrzennych, co umożliwi optymalizację wydajności zapytań związanych z operacjami przestrzennymi na dużych zbiorach danych.
- **Integracja z mapami i aplikacjami GIS:** System powinien wspierać integrację z narzędziami i systemami GIS (Geographic Information Systems) oraz mapami, umożliwiając wyświetlanie i analizę danych przestrzennych na mapach.
- **Wsparcie dla standardów:** System musi być zgodny z międzynarodowymi standardami dla danych przestrzennych, takimi jak Open Geospatial Consortium (OGC), co zapewnia interoperacyjność z innymi systemami.

Cel:

Umożliwienie przechowywania, przetwarzania i analizowania danych przestrzennych, co wspiera aplikacje bazujące na lokalizacji, takie jak systemy geograficzne, analiza odległości i zależności przestrzennych oraz integracja z aplikacjami GIS i mapami.

Tytuł wymagania: **SQL.31.2024 - Wyszukiwanie pełnotekstowe (Full-Text Search)**

Opis wymagania:

System bazodanowy musi obsługiwać funkcję wyszukiwania pełnotekstowego, która umożliwi szybkie przeszukiwanie dużych zbiorów tekstowych, takich jak dokumenty, opisy i inne dane tekstowe, pod kątem słów kluczowych, fraz oraz wzorców. Funkcja ta powinna wspierać zaawansowane operacje wyszukiwania, takie jak przeszukiwanie wielowyrazowe, sortowanie według trafności oraz wyszukiwanie przybliżone.

Kluczowe aspekty:

- **Indeksowanie pełnotekstowe:** System musi umożliwiać tworzenie indeksów pełnotekstowych, które przyspieszają przetwarzanie zapytań tekstowych, zapewniając szybki dostęp do danych tekstowych nawet w dużych zbiorach.
- **Zaawansowane operacje wyszukiwania:** System powinien wspierać wyszukiwanie przybliżone, wyszukiwanie fraz, wyrażeń wielowyrazowych, z uwzględnieniem operatorów logicznych, takich jak "AND", "OR" czy "NEAR", co pozwala na precyzyjne dopasowanie wyników.
- **Wyniki sortowane według trafności:** System musi umożliwiać sortowanie wyników zapytań na podstawie trafności, uwzględniając częstość występowania słów kluczowych i ich pozycję w przeszukiwanym tekście.
- **Obsługa wielu języków:** System powinien wspierać wyszukiwanie pełnotekstowe w wielu językach, umożliwiając analizę morfologiczną i przetwarzanie różnych form wyrazów w zależności od używanego języka.
- **Zarządzanie dużymi zbiorami danych tekstowych:** System musi efektywnie radzić sobie z przetwarzaniem bardzo dużych zbiorów danych tekstowych, minimalizując wpływ na wydajność innych operacji bazodanowych.

Nr sprawy: BF-IV.2370.26.2024
 Załącznik nr 1 do SWZ/ nr 1 do umowy

Cel:

Zapewnienie szybkiego i precyzyjnego wyszukiwania w dużych zbiorach tekstowych, umożliwiającego przetwarzanie skomplikowanych zapytań tekstowych i sortowanie wyników według trafności, co wspiera aplikacje wymagające zaawansowanego wyszukiwania treści, takie jak systemy zarządzania dokumentami czy portale internetowe.

Tytuł wymagania: SQL.32.2024 - Wyszukiwanie semantyczne (Semantic Search)

Opis wymagania:

System bazodanowy musi obsługiwać funkcję wyszukiwania semantycznego, która umożliwia inteligentne przeszukiwanie danych w sposób uwzględniający znaczenie i kontekst zapytań, a nie tylko dosłowne dopasowanie słów kluczowych. Funkcja ta powinna wspierać analizę znaczenia, relacji między pojęciami oraz rozumienie intencji użytkownika, co pozwala na dostarczanie bardziej trafnych i kontekstualnych wyników wyszukiwania.

Kluczowe aspekty:

- **Analiza semantyczna:** System musi wspierać analizę semantyczną zapytań, co oznacza rozumienie znaczenia słów, fraz oraz relacji między nimi, aby dostarczać wyniki zgodne z intencjami użytkownika.
- **Wyszukiwanie oparte na pojęciach:** System powinien umożliwiać wyszukiwanie oparte na pojęciach, co oznacza, że zapytania mogą być formułowane w naturalnym języku i system będzie rozumieć ich znaczenie oraz powiązane koncepcje.
- **Rozumienie kontekstu:** System musi być zdolny do uwzględniania kontekstu zapytań, takich jak poprzednie wyszukiwania, preferencje użytkownika oraz specyficzne dziedziny tematyczne, aby dostarczać bardziej trafne wyniki.
- **Synonimy i powiązania:** System powinien rozpoznawać synonimy, warianty i powiązania między pojęciami, co pozwala na rozszerzenie wyników wyszukiwania o terminy o podobnym znaczeniu.
- **Ocena i poprawa wyników:** System powinien wspierać mechanizmy oceny trafności wyników wyszukiwania oraz umożliwiać ciągłe doskonalenie algorytmów semantycznych na podstawie feedbacku użytkowników i analizy danych.

Cel:

Umożliwienie zaawansowanego przeszukiwania danych w sposób uwzględniający znaczenie i kontekst zapytań, co poprawia trafność wyników wyszukiwania i dostarcza bardziej relewantne odpowiedzi, wspierając użytkowników w znajdowaniu informacji w sposób bardziej naturalny i zrozumiały.

Tytuł wymagania: SQL.33.2024 - Śledzenie zmian danych (Change Data Capture)

Opis wymagania:

System bazodanowy musi obsługiwać funkcję śledzenia zmian danych (Change Data Capture,

Nr sprawy: BF-IV.2370.26.2024

Załącznik nr 1 do SWZ/ nr 1 do umowy

CDC), która umożliwia rejestrowanie wszelkich zmian w danych zapisanych w tabelach bazy danych, takich jak operacje wstawiania, aktualizacji i usuwania. Funkcja ta pozwala na wydajne śledzenie zmian w czasie rzeczywistym, co jest szczególnie przydatne w scenariuszach replikacji danych, integracji systemów oraz budowy hurtowni danych.

Kluczowe aspekty:

- **Rejestrowanie zmian:** System musi automatycznie rejestrować zmiany w danych, w tym operacje wstawiania, aktualizacji i usuwania, umożliwiając szczegółowe śledzenie historii modyfikacji danych w określonych tabelach.
- **Przechowywanie danych zmienionych:** System powinien przechowywać informacje o zmienionych danych w specjalnych tabelach zmian, co umożliwia dostęp do historii operacji i rekonstrukcję stanu danych z przeszłości.
- **Łatwe odczytywanie zmian:** Funkcja CDC musi udostępniać dane o zmianach w sposób umożliwiający łatwe ich odczytywanie i przetwarzanie w czasie rzeczywistym, np. na potrzeby replikacji danych lub integracji z systemami zewnętrznymi.
- **Integracja z hurtowniami danych:** Śledzenie zmian danych powinno być w pełni zintegrowane z procesami ETL, co ułatwia regularne aktualizowanie hurtowni danych na podstawie bieżących modyfikacji w systemie produkcyjnym.
- **Minimalny wpływ na wydajność:** System musi zapewniać, że śledzenie zmian danych ma minimalny wpływ na wydajność bieżących operacji w bazie danych, przy jednoczesnym zapewnieniu dokładności rejestrowanych danych.

Cel:

Umożliwienie efektywnego śledzenia zmian danych w czasie rzeczywistym w celu integracji, replikacji i aktualizacji danych między systemami, wspierając synchronizację oraz analizy zmian w dużych i dynamicznych środowiskach baz danych.

Tytuł wymagania: SQL.34.2024 - Śledzenie zmian (Change Tracking)

Opis wymagania:

System bazodanowy musi obsługiwać funkcję śledzenia zmian (Change Tracking), która umożliwia identyfikację zmian w danych zapisanych w tabelach, takich jak operacje wstawiania, aktualizacji i usuwania, bez przechowywania pełnej historii tych zmian. Funkcja ta jest lekka i zoptymalizowana do scenariuszy synchronizacji danych oraz aplikacji wymagających informacji o tym, które wiersze zostały zmienione od ostatniego zapytania.

Kluczowe aspekty:

- **Śledzenie wierszy zmienionych:** System musi identyfikować, które wiersze w tabelach zostały zmienione od ostatniej synchronizacji, co umożliwia szybkie wykrywanie modyfikacji bez przechowywania pełnej historii zmian.
- **Brak pełnej historii zmian:** W odróżnieniu od Change Data Capture, funkcja Change Tracking nie musi rejestrować szczegółowych informacji o operacjach na danych ani przechowywać poprzednich wersji danych, co sprawia, że jest bardziej wydajna i lekka.

Nr sprawy: BF-IV.2370.26.2024

Załącznik nr 1 do SWZ/ nr 1 do umowy

- **Szybka synchronizacja danych:** Funkcja ta powinna wspierać scenariusze, w których potrzebna jest szybka synchronizacja danych między systemami lub aplikacjami, identyfikując jedynie zmienione wiersze, co minimalizuje obciążenie systemu.
- **Obsługa zapytań o zmiany:** System musi udostępniać mechanizmy pozwalające aplikacjom na łatwe pobieranie informacji o zmienionych wierszach, aby mogły one zsynchronizować dane lub reagować na te zmiany.
- **Minimalny wpływ na wydajność:** Funkcja śledzenia zmian musi mieć minimalny wpływ na wydajność systemu bazodanowego, co sprawia, że jest optymalna do zastosowań w systemach o wysokiej dynamice danych.

Cel:

Zapewnienie lekkiego mechanizmu śledzenia zmian w danych, umożliwiającego efektywną synchronizację między systemami i aplikacjami, bez przechowywania pełnej historii zmian, co zwiększa wydajność i zmniejsza obciążenie systemu.

Tytuł wymagania: SQL.35.2024 - Migawki bazy danych (Database Snapshots)

Opis wymagania:

System bazodanowy musi obsługiwać funkcję migawek bazy danych, która umożliwia tworzenie statycznych kopii bazy danych w danym momencie, bez konieczności duplikowania całych danych. Migawki bazy danych pozwalają na szybkie przywracanie wcześniejszych wersji danych oraz analizę stanu bazy w określonym czasie, co jest przydatne w scenariuszach testowania, audytu oraz przywracania danych po nieprawidłowych operacjach.

Kluczowe aspekty:

- **Tworzenie natychmiastowych kopii:** System musi umożliwiać szybkie tworzenie migawek bazy danych, które przechowują jedynie zmienione bloki danych, co minimalizuje czas i przestrzeń dyskową potrzebną na ich przechowywanie.
- **Przywracanie bazy danych:** System powinien umożliwiać przywracanie pełnej bazy danych do stanu z momentu utworzenia migawki, co pozwala na szybkie odzyskiwanie danych po nieprawidłowych operacjach lub awariach.
- **Minimalne zużycie zasobów:** Migawki muszą przechowywać tylko zmienione dane, co minimalizuje zużycie przestrzeni dyskowej i zapewnia wysoką efektywność operacyjną, nawet przy dużych bazach danych.
- **Analiza stanu historycznego:** System musi umożliwiać analizę danych z migawek bez wpływu na bieżącą działalność operacyjną, co pozwala na testowanie i audytowanie bez ingerencji w działanie produkcyjne.
- **Bezpieczeństwo operacji:** System powinien zapewniać, że operacje tworzenia i zarządzania migawkami są bezpieczne i nie wpływają na integralność oraz wydajność głównej bazy danych.

Cel:

Zapewnienie szybkiego i efektywnego mechanizmu tworzenia migawek bazy danych, co

Nr sprawy: BF-IV.2370.26.2024

Załącznik nr 1 do SWZ/ nr 1 do umowy umożliwia analizę stanu historycznego, testowanie oraz przywracanie danych bez pełnego duplikowania zasobów, wspierając zarówno bezpieczeństwo, jak i efektywność operacyjną.

Tytuł wymagania: SQL.36.2024 - Mirroring bazy danych (Database Mirroring)

Opis wymagania:

System bazodanowy musi obsługiwać funkcję mirroringu bazy danych, która zapewnia wysoką dostępność i niezawodność poprzez replikację danych w czasie rzeczywistym między główną (primary) a zapasową (mirror) bazą danych. W przypadku awarii głównej bazy danych, system musi umożliwiać automatyczne lub ręczne przełączenie na bazę zapasową, co minimalizuje przestoje i ryzyko utraty danych.

Kluczowe aspekty:

- **Synchronizacja w czasie rzeczywistym:** System musi zapewniać replikację transakcji z głównej bazy danych do bazy zapasowej w czasie rzeczywistym, co umożliwia utrzymanie aktualnych danych w obu instancjach.
- **Tryb synchroniczny i asynchroniczny:** System powinien obsługiwać dwa tryby replikacji: synchroniczny (dla pełnej ochrony danych, minimalizując ryzyko utraty) oraz asynchroniczny (dla większej wydajności i elastyczności w środowiskach rozproszonych).
- **Automatyczne przełączenie awaryjne:** System musi umożliwiać automatyczne przełączanie na bazę zapasową w przypadku awarii głównej bazy danych, co zapewnia ciągłość działania bez potrzeby interwencji administratora (tzw. tryb high-safety with automatic failover).
- **Ręczne przełączanie:** System powinien umożliwiać administratorom ręczne przełączenie między bazami, co pozwala na przeprowadzanie konserwacji lub rozwiązywanie problemów bez przerywania działania aplikacji.
- **Minimalny wpływ na wydajność:** Proces mirroringu powinien mieć minimalny wpływ na wydajność operacyjną głównej bazy danych, zapewniając jednocześnie maksymalną ochronę danych i dostępność.

Cel:

Zapewnienie wysokiej dostępności oraz minimalizacja ryzyka przestojów poprzez replikację i synchronizację danych między główną a zapasową bazą danych. System umożliwia automatyczne lub ręczne przełączenie na bazę zapasową w razie awarii, co gwarantuje ciągłość działania i ochronę przed utratą danych.

Tytuł wymagania: SQL.37.2024 - Log shipping (Transport dziennika transakcji)

Opis wymagania:

System bazodanowy musi obsługiwać funkcję log shipping, która zapewnia wysoką dostępność i odzyskiwanie po awarii poprzez automatyczne kopiowanie, przywracanie i synchronizację dzienników transakcji z głównej bazy danych do jednej lub więcej baz zapasowych (secondary databases). Ta funkcja umożliwia utrzymanie kopii zapasowej bazy

Nr sprawy: BF-IV.2370.26.2024

Załącznik nr 1 do SWZ/ nr 1 do umowy

danych na innej maszynie lub lokalizacji w celu minimalizacji przestoju i zapewnienia ciągłości działania w przypadku awarii.

Kluczowe aspekty:

- **Automatyczne kopiowanie dzienników transakcji:** System musi automatycznie kopiować dzienniki transakcji z głównej bazy danych do bazy zapasowej w zdefiniowanych interwałach czasowych, co zapewnia regularną synchronizację danych.
- **Przywracanie dzienników na bazach zapasowych:** System powinien automatycznie przywracać skopiowane dzienniki transakcji na bazy zapasowe, utrzymując aktualność danych i gotowość do przełączenia w razie awarii.
- **Obsługa wielu baz zapasowych:** System musi wspierać log shipping do wielu baz zapasowych, co zwiększa elastyczność oraz odporność na awarie, umożliwiając redundancję w różnych lokalizacjach.
- **Monitorowanie i alerty:** System powinien zapewniać narzędzia do monitorowania procesu log shipping oraz automatyczne powiadomianie administratorów o ewentualnych problemach, takich jak opóźnienia w kopiowaniu dzienników transakcji.
- **Ręczne przełączenie awaryjne:** W przypadku awarii głównej bazy danych system musi umożliwiać ręczne przełączenie na jedną z baz zapasowych, co pozwala na szybkie wznowienie działalności i minimalizację przestoju.

Cel:

Zapewnienie ciągłości działania oraz ochrony przed utratą danych dzięki automatycznemu kopiowaniu i przywracaniu dzienników transakcji, umożliwiając szybkie przełączenie na bazę zapasową w przypadku awarii głównej bazy danych. Funkcja ta wspiera elastyczność i odporność systemu na awarie w różnych lokalizacjach.

Tytuł wymagania: SQL.38.2024 - Replikacja danych (transakcyjna, merge, snapshot)

Opis wymagania:

System bazodanowy musi obsługiwać funkcję replikacji danych, która umożliwia przesyłanie i synchronizowanie danych między bazami danych w różnych lokalizacjach. Funkcja ta powinna wspierać trzy główne typy replikacji: transakcyjną, merge oraz snapshot, umożliwiając elastyczne dostosowanie do potrzeb systemów o różnych wymaganiach dotyczących synchronizacji i wydajności.

Kluczowe aspekty:

- **Replikacja transakcyjna:** System musi obsługiwać replikację transakcyjną, która umożliwia przesyłanie zmian danych z głównej bazy danych do subskrybentów w czasie rzeczywistym. Ten typ replikacji jest odpowiedni dla systemów wymagających bieżącej synchronizacji i wysokiej dokładności danych.

Nr sprawy: BF-IV.2370.26.2024

Załącznik nr 1 do SWZ/ nr 1 do umowy

- **Replikacja merge:** System powinien wspierać replikację merge, która umożliwia dwukierunkową synchronizację danych między wieloma lokalizacjami, nawet w przypadku przerw w połączeniu. Zmiany wprowadzane w różnych bazach danych są łączone i synchronizowane, co jest idealne dla rozproszonych aplikacji mobilnych lub offline.
- **Replikacja snapshot:** System musi obsługiwać replikację snapshot, która tworzy pełną kopię danych w określonych interwałach czasowych, przysyłając ją do subskrybentów. Ten typ replikacji jest odpowiedni dla środowisk, gdzie pełna aktualizacja danych w regularnych odstępach jest wystarczająca.
- **Zarządzanie konfliktem:** W przypadku replikacji merge system musi mieć możliwość wykrywania i rozwiązywania konfliktów danych, które mogą pojawić się, gdy różne bazy danych jednocześnie zmieniają te same rekordy.
- **Monitorowanie i zarządzanie:** System powinien zapewniać narzędzia do monitorowania stanu replikacji, raportowania błędów oraz dostosowywania ustawień w celu optymalizacji wydajności i niezawodności.

Cel:

Zapewnienie elastycznych i skalowalnych metod synchronizacji danych między bazami danych poprzez obsługę różnych typów replikacji: transakcyjnej (dla bieżących zmian), merge (dla rozproszonych systemów) i snapshot (dla regularnych kopii danych). Funkcja ta wspiera synchronizację, odporność na przerwy oraz skalowalność w złożonych środowiskach rozproszonych.

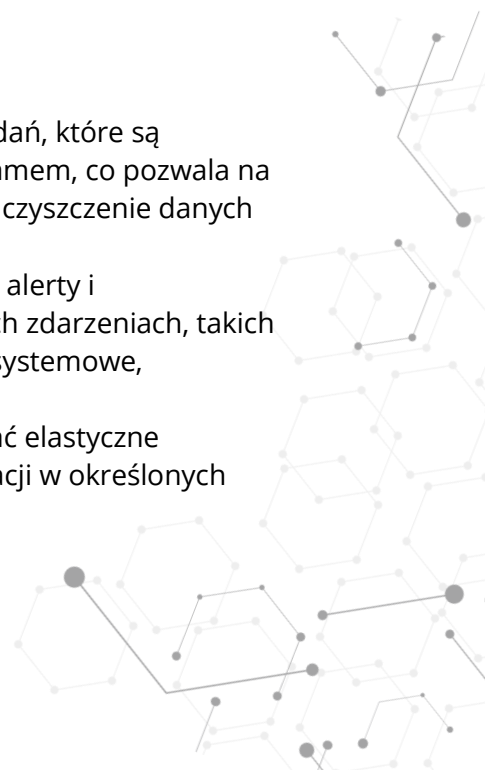
Tytuł wymagania: SQL.39.2024 - Agent SQL Server (SQL Server Agent)

Opis wymagania:

System bazodanowy musi obsługiwać funkcję SQL Server Agent, która umożliwia automatyzację zadań administracyjnych, takich jak uruchamianie skryptów, kopie zapasowe, monitorowanie systemu czy harmonogramowanie operacji na bazie danych. Agent SQL Server pozwala na zarządzanie cyklicznymi zadaniami oraz reagowanie na zdarzenia systemowe, co wspiera efektywność operacyjną i minimalizuje konieczność ręcznej interwencji.

Kluczowe aspekty:

- **Automatyzacja zadań:** System musi umożliwiać tworzenie zadań, które są automatycznie uruchamiane zgodnie z ustalonym harmonogramem, co pozwala na wykonywanie regularnych operacji, takich jak kopie zapasowe, czyszczenie danych czy aktualizacje indeksów.
- **Obsługa alertów i powiadomień:** Agent powinien obsługiwać alerty i powiadomienia, które informują administratorów o określonych zdarzeniach, takich jak niepowodzenie zadania, brak miejsca na dysku czy awarie systemowe, umożliwiając szybką reakcję.
- **Harmonogramowanie zadań:** SQL Server Agent musi wspierać elastyczne harmonogramowanie zadań, umożliwiając wykonywanie operacji w określonych interwałach czasowych lub w reakcji na zdarzenia systemowe.



Nr sprawy: BF-IV.2370.26.2024

Załącznik nr 1 do SWZ/ nr 1 do umowy

- **Zarządzanie zadaniami:** System powinien umożliwiać monitorowanie stanu zadań, ich historię oraz wyniki działania, co pozwala na łatwe zarządzanie operacjami i rozwiązywanie problemów.
- **Bezpieczeństwo:** Agent musi obsługiwać zaawansowane mechanizmy kontroli dostępu, umożliwiając przypisywanie uprawnień do wykonywania i zarządzania zadaniami, co zapewnia odpowiedni poziom bezpieczeństwa w środowiskach wieloużytkownikowych.

Cel:

Umożliwienie automatyzacji zadań administracyjnych i operacyjnych poprzez SQL Server Agent, co zwiększa efektywność zarządzania bazą danych, minimalizuje konieczność ręcznej interwencji oraz wspiera monitorowanie i reagowanie na zdarzenia systemowe w sposób zautomatyzowany.

Tytuł wymagania: SQL.40.2024 - Poczta bazy danych (Database Mail)

Opis wymagania:

System bazodanowy musi obsługiwać funkcję Database Mail, która umożliwia wysyłanie wiadomości e-mail z poziomu bazy danych. Funkcja ta wspiera komunikację o różnych zdarzeniach systemowych, wynikach zadań oraz alertach, a także pozwala na automatyczne powiadamianie administratorów i użytkowników o istotnych informacjach dotyczących stanu i operacji bazy danych.

Kluczowe aspekty:

- **Konfiguracja serwera pocztowego:** System musi umożliwiać konfigurację serwera SMTP (Simple Mail Transfer Protocol), który będzie używany do wysyłania wiadomości e-mail, zapewniając wsparcie dla bezpiecznych połączeń i autoryzacji.
- **Wysyłanie powiadomień:** Database Mail powinien umożliwiać automatyczne wysyłanie powiadomień o zdarzeniach systemowych, takich jak błędy, ostrzeżenia czy zakończenie zadań, co wspiera szybką reakcję i monitorowanie.
- **Obsługa załączników:** System musi umożliwiać dołączanie załączników do wiadomości e-mail, takich jak raporty, pliki dziennika czy wyniki zapytań, co zwiększa funkcjonalność powiadomień.
- **Zarządzanie kontami pocztowymi:** Funkcja ta powinna umożliwiać zarządzanie wieloma kontami e-mail, co pozwala na dostosowanie komunikacji do różnych ról i funkcji w systemie.
- **Monitorowanie i raportowanie:** System powinien zapewniać mechanizmy monitorowania i raportowania statusu wysyłanych wiadomości e-mail, umożliwiając śledzenie dostarczenia, ewentualnych błędów oraz analizę skuteczności komunikacji.

Cel:

Umożliwienie efektywnej komunikacji z administratorami i użytkownikami poprzez automatyczne wysyłanie powiadomień e-mail oraz zarządzanie wiadomościami i załącznikami, co wspiera monitorowanie stanu bazy danych oraz szybkie reagowanie na zdarzenia i problemy.

Nr sprawy: BF-IV.2370.26.2024
 Załącznik nr 1 do SWZ/ nr 1 do umowy

Tytuł wymagania: SQL.41.2024 - Service Broker

Opis wymagania:

System bazodanowy musi obsługiwać funkcję Service Broker, która umożliwia asynchroniczną komunikację i przetwarzanie wiadomości między różnymi komponentami bazy danych. Service Broker wspiera tworzenie rozproszonych i skalowalnych aplikacji, zapewniając bezpieczne, niezawodne i uporządkowane przetwarzanie zadań oraz komunikację między serwerami lub bazami danych.

Kluczowe aspekty:

- **Asynchroniczna komunikacja:** System musi wspierać asynchroniczne przesyłanie wiadomości między różnymi komponentami lub aplikacjami, co pozwala na równoczesne wykonywanie wielu zadań bez blokowania operacji.
- **Przetwarzanie wiadomości:** Service Broker powinien obsługiwać kolejkowanie wiadomości, które umożliwia ich przetwarzanie w uporządkowany sposób, niezależnie od kolejności ich wysyłania i odbierania.
- **Bezpieczeństwo komunikacji:** System musi zapewniać mechanizmy szyfrowania i autoryzacji, aby zagwarantować bezpieczne przesyłanie wiadomości między różnymi bazami danych lub serwerami.
- **Transakcyjność:** Service Broker musi wspierać przetwarzanie wiadomości w sposób transakcyjny, co oznacza, że wiadomości są przetwarzane w ramach transakcji, zapewniając spójność danych oraz możliwość cofania operacji w przypadku błędów.
- **Rozproszona architektura:** System powinien umożliwiać komunikację między bazami danych w rozproszonym środowisku, zarówno w ramach jednego serwera, jak i pomiędzy różnymi serwerami, wspierając skalowanie aplikacji i ich elastyczność.

Cel:

Zapewnienie niezawodnej i bezpiecznej komunikacji między różnymi komponentami i aplikacjami poprzez asynchroniczne przesyłanie wiadomości z wykorzystaniem funkcji Service Broker, co umożliwia budowę skalowalnych i rozproszonych systemów oraz wspiera efektywne przetwarzanie zadań w bazie danych.

Tytuł wymagania: SQL.42.2024 - Rozszerzone zdarzenia (Extended Events)

Opis wymagania:

System bazodanowy musi obsługiwać funkcję rozszerzonych zdarzeń (Extended Events), która umożliwia monitorowanie, analizowanie i diagnozowanie zdarzeń w systemie bazodanowym w sposób wydajny i elastyczny. Extended Events pozwalają na rejestrowanie szczegółowych informacji o zdarzeniach systemowych i operacyjnych, wspierając rozwiązywanie problemów wydajnościowych, monitorowanie aktywności i optymalizację pracy bazy danych.

Kluczowe aspekty:

- **Precyzyjne monitorowanie zdarzeń:** System musi umożliwiać rejestrowanie szerokiego zakresu zdarzeń, takich jak błędy, przeciążenia, blokady, zmiany

Nr sprawy: BF-IV.2370.26.2024

Załącznik nr 1 do SWZ/ nr 1 do umowy

konfiguracji czy aktywność użytkowników, co pozwala na precyzyjne monitorowanie działania bazy danych.

- **Niska ingerencja w wydajność:** Extended Events powinny być zaprojektowane w taki sposób, aby minimalnie wpływać na wydajność systemu podczas monitorowania, umożliwiając ich zastosowanie nawet w środowiskach produkcyjnych.
- **Elastyczne filtrowanie i agregacja danych:** System musi umożliwiać filtrowanie i agregowanie danych zdarzeń w czasie rzeczywistym, co pozwala na szybkie zidentyfikowanie problemów bez konieczności przetwarzania dużych ilości nieistotnych informacji.
- **Analiza danych historycznych:** Extended Events powinny wspierać przechowywanie danych zdarzeń do analizy historycznej, co umożliwia późniejsze badanie incydentów, analizowanie trendów i optymalizację wydajności.
- **Integracja z narzędziami monitorującymi:** System musi wspierać integrację z narzędziami do monitorowania i analizy zdarzeń, co ułatwia zbieranie, przeglądanie i analizowanie wyników w celu szybkiego rozwiązywania problemów.

Cel:

Umożliwienie zaawansowanego monitorowania i diagnozowania zdarzeń w systemie bazodanowym poprzez funkcję Extended Events, co wspiera szybkie rozwiązywanie problemów, analizę wydajności i optymalizację działania bazy danych, minimalizując wpływ na jej pracę.

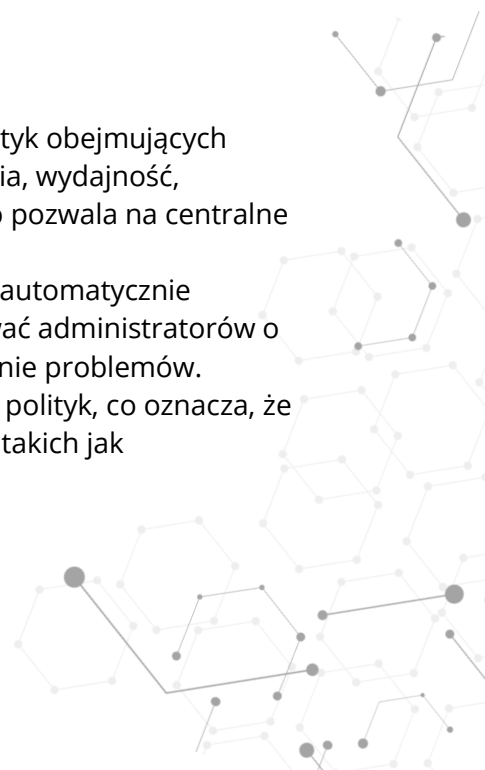
Tytuł wymagania: SQL.43.2024 - Zarządzanie oparte na zasadach (Policy-Based Management)

Opis wymagania:

System bazodanowy musi obsługiwać funkcję zarządzania opartego na zasadach (Policy-Based Management), która umożliwia definiowanie i egzekwowanie zasad dotyczących konfiguracji i operacji na bazie danych. Funkcja ta pozwala na automatyczne monitorowanie zgodności z ustalonymi politykami oraz wymuszanie określonych reguł, co zapewnia spójność i zgodność konfiguracji w całym środowisku bazodanowym.

Kluczowe aspekty:

- **Definiowanie polityk:** System musi umożliwiać tworzenie polityk obejmujących różne aspekty konfiguracji bazy danych, takie jak zabezpieczenia, wydajność, struktura tabel, konfiguracja serwera i zgodność z normami, co pozwala na centralne zarządzanie standardami.
- **Automatyczne monitorowanie zgodności:** System powinien automatycznie monitorować zgodność z zdefiniowanymi zasadami i informować administratorów o niezgodnościach, co umożliwia szybkie wykrywanie i korygowanie problemów.
- **Wymuszanie polityk:** System musi obsługiwać egzekwowanie polityk, co oznacza, że można ustawić automatyczne wymuszanie określonych zasad, takich jak



Nr sprawy: BF-IV.2370.26.2024

Załącznik nr 1 do SWZ/ nr 1 do umowy

ograniczenia na konfigurację serwera lub bazy danych, co minimalizuje ryzyko niezgodności.

- **Ocena i raportowanie:** System powinien umożliwiać cykliczną ocenę zgodności z politykami oraz generowanie raportów dotyczących stanu zgodności, co wspiera zarządzanie zgodnością i umożliwia audyt.
- **Zarządzanie na wielu serwerach:** System musi umożliwiać zarządzanie politykami na wielu instancjach serwera, co zapewnia spójność w dużych, rozproszonych środowiskach bazodanowych.

Cel:

Zarządzanie konfiguracją i operacjami bazy danych poprzez definiowanie i egzekwowanie zasad, co zapewnia zgodność, bezpieczeństwo oraz spójność w całym środowisku bazodanowym. System wspiera automatyczne monitorowanie, wymuszanie polityk oraz raportowanie, minimalizując ryzyko niezgodności i optymalizując zarządzanie bazami danych.

Tytuł wymagania: SQL.45.2024 - Zarządzanie zasobami (Resource Governor)

Opis wymagania:

System bazodanowy musi obsługiwać funkcję zarządzania zasobami (Resource Governor), która umożliwia kontrolowanie i alokację zasobów systemowych, takich jak procesor i pamięć, pomiędzy różnymi obciążeniami w bazie danych. Funkcja ta pozwala na definiowanie polityk zasobów i przydzielanie priorytetów różnym grupom użytkowników lub zapytań, co wspiera optymalizację wydajności oraz stabilność systemu w przypadku konkurujących zadań.

Kluczowe aspekty:

- **Kontrola zasobów CPU i pamięci:** System musi umożliwiać definiowanie limitów zużycia procesora oraz pamięci dla różnych obciążeń, co zapewnia zrównoważoną alokację zasobów między zapytaniami i operacjami.
- **Priorytetyzacja obciążeń:** System powinien wspierać mechanizmy priorytetyzacji, które pozwalają na przypisywanie wyższych lub niższych priorytetów dla określonych grup użytkowników lub typów zapytań, co minimalizuje ryzyko przeciążenia zasobów przez nieoptymalne operacje.
- **Zarządzanie grupami zasobów:** System musi umożliwiać tworzenie i zarządzanie grupami zasobów, które definiują zasady alokacji dla określonych klas obciążeń, takich jak zadania raportowe, operacje OLTP czy procesy ETL.
- **Monitorowanie zasobów w czasie rzeczywistym:** Resource Governor musi zapewniać monitorowanie wykorzystania zasobów systemowych w czasie rzeczywistym, co pozwala administratorom na dynamiczne dostosowywanie limitów oraz identyfikowanie problematycznych obciążeń.
- **Dynamiczne dostosowywanie zasobów:** System powinien wspierać dynamiczne zmiany polityk zarządzania zasobami, co umożliwia elastyczne reagowanie na zmieniające się warunki operacyjne i obciążenia.

Cel:

Optymalizacja wydajności i stabilności systemu poprzez kontrolowanie alokacji zasobów

Nr sprawy: BF-IV.2370.26.2024

Załącznik nr 1 do SWZ/ nr 1 do umowy

procesora i pamięci między różnymi grupami użytkowników i obciążeniami, co zapewnia sprawiedliwy podział zasobów i minimalizuje ryzyko przeciążenia systemu w złożonych środowiskach bazodanowych.

Tytuł wymagania: SQL.46.2024 - Rozszerzenie puli buforów (Buffer Pool Extension)

Opis wymagania:

System bazodanowy musi obsługiwać funkcję rozszerzenia puli buforów (Buffer Pool Extension), która umożliwi rozszerzenie pamięci operacyjnej na szybkie dyski SSD, poprawiając wydajność przetwarzania danych. Funkcja ta pozwala na wykorzystanie pamięci masowej SSD jako dodatkowej przestrzeni dla puli buforów, co zwiększa zdolność systemu do przechowywania danych w pamięci podręcznej, przyspieszając operacje I/O.

Kluczowe aspekty:

- **Wykorzystanie dysków SSD:** System musi umożliwiać wykorzystanie dysków SSD jako rozszerzenie pamięci operacyjnej (RAM) dla puli buforów, co poprawia wydajność operacji I/O bez konieczności zwiększania fizycznej pamięci RAM.
- **Przechowywanie stron danych:** Rozszerzenie puli buforów powinno umożliwiać przechowywanie stron danych, które są najczęściej odczytywane, w szybkim magazynie SSD, co minimalizuje opóźnienia związane z operacjami na dyskach twardych.
- **Zarządzanie dynamiczne:** System musi automatycznie zarządzać buforami rozszerzonymi, zapewniając optymalne wykorzystanie przestrzeni SSD i dynamicznie przenosząc dane między pamięcią RAM a SSD w zależności od potrzeb operacyjnych.
- **Zwiększenie przepustowości I/O:** Funkcja powinna zapewniać znaczną poprawę przepustowości operacji wejścia/wyjścia (I/O) przy dużych obciążeniach, co wspiera lepszą wydajność aplikacji działających na dużych zbiorach danych.
- **Minimalny wpływ na konfigurację:** System powinien umożliwiać łatwą konfigurację rozszerzenia puli buforów bez potrzeby modyfikowania istniejących aplikacji, co zapewnia elastyczność w zarządzaniu zasobami pamięci.

Cel:

Poprawa wydajności systemu poprzez zwiększenie dostępnej pamięci operacyjnej przy wykorzystaniu szybkich dysków SSD jako rozszerzenia puli buforów, co optymalizuje operacje wejścia/wyjścia i przyspiesza przetwarzanie dużych ilości danych w środowiskach o dużych obciążeniach.

Tytuł wymagania: SQL.47.2024 - Kompresja kopii zapasowych (Backup Compression)

Opis wymagania:

System bazodanowy musi obsługiwać funkcję kompresji kopii zapasowych, która umożliwia zmniejszenie rozmiaru plików kopii zapasowych poprzez kompresowanie danych podczas

Nr sprawy: BF-IV.2370.26.2024

Załącznik nr 1 do SWZ/ nr 1 do umowy

tworzenia backupu. Funkcja ta pozwala na oszczędność miejsca na dysku, skrócenie czasu przesyłania kopii zapasowych i redukcję kosztów przechowywania danych, przy jednoczesnym zachowaniu integralności i bezpieczeństwa danych.

Kluczowe aspekty:

- **Zmniejszenie rozmiaru kopii zapasowych:** System musi umożliwiać kompresowanie danych podczas tworzenia kopii zapasowych, co prowadzi do znacznego zmniejszenia rozmiaru plików backupu, redukując wymagania dotyczące przestrzeni dyskowej.
- **Oszczędność miejsca i kosztów:** Kompresja kopii zapasowych powinna przyczyniać się do oszczędności miejsca na dysku, co bezpośrednio obniża koszty związane z długoterminowym przechowywaniem danych.
- **Szybsze tworzenie i przywracanie kopii zapasowych:** Dzięki mniejszemu rozmiarowi plików system musi skracać czas potrzebny na przesyłanie, tworzenie i przywracanie kopii zapasowych, co poprawia wydajność operacyjną, szczególnie w środowiskach o dużych zbiorach danych.
- **Minimalny wpływ na wydajność:** Proces kompresji powinien mieć minimalny wpływ na wydajność systemu, umożliwiając regularne tworzenie kopii zapasowych nawet w intensywnie działających systemach produkcyjnych.
- **Zarządzanie poziomem kompresji:** System powinien umożliwiać administratorom kontrolowanie poziomu kompresji, co pozwala na wybór optymalnego balansu między rozmiarem plików backupu a wydajnością operacji.

Cel:

Zapewnienie efektywnego tworzenia kopii zapasowych dzięki kompresji, co zmniejsza wymagania dotyczące przestrzeni dyskowej, skraca czas tworzenia i przywracania backupów oraz obniża koszty przechowywania danych, bez wpływu na integralność czy dostępność danych.

Tytuł wymagania: SQL.48.2024 - Rejestr transakcji (SQL Server Ledger)

Opis wymagania:

System bazodanowy musi obsługiwać funkcję rejestru transakcji (SQL Server Ledger), która zapewnia niezmienność i przejrzystość danych poprzez rejestrowanie historii transakcji w sposób umożliwiający weryfikację ich integralności. Funkcja ta jest szczególnie przydatna w środowiskach wymagających audytowalności i zgodności z regulacjami, takich jak finanse, zdrowie i administracja publiczna.

Kluczowe aspekty:

- **Rejestr niezmienności:** System musi tworzyć niezmienny rejestr transakcji, który zapisuje każdą zmianę danych, zapewniając, że historia danych jest chroniona przed modyfikacją i możliwa do weryfikacji.
- **Kryptograficzne dowody integralności:** Ledger powinien umożliwiać kryptograficzne zabezpieczenie transakcji, dzięki czemu możliwe jest generowanie

Nr sprawy: BF-IV.2370.26.2024

Załącznik nr 1 do SWZ/ nr 1 do umowy

dowodów, że dane nie zostały zmienione po ich zapisaniu, co zapewnia pełną zgodność z wymaganiami audytowymi.

- **Przejrzystość i weryfikacja:** System powinien umożliwiać audytorom oraz użytkownikom końcowym weryfikowanie integralności danych poprzez analizę historii transakcji, bez konieczności modyfikacji aplikacji.
- **Ochrona przed nieautoryzowanymi zmianami:** SQL Server Ledger powinien chronić dane przed nieautoryzowanymi modyfikacjami, co jest kluczowe w scenariuszach, gdzie bezpieczeństwo danych i ich nienaruszalność są priorytetem.
- **Współpraca z tradycyjnymi danymi:** System musi wspierać funkcję SQL Server Ledger bez wpływu na tradycyjne modele danych i operacje, co zapewnia łatwą integrację z istniejącymi aplikacjami.

Cel:

Zapewnienie pełnej przejrzystości, audytowalności oraz ochrony przed nieautoryzowanymi modyfikacjami danych poprzez funkcję rejestru transakcji (Ledger), która zabezpiecza dane przed manipulacją i umożliwia weryfikację integralności wrażliwych danych w środowiskach o wysokich wymaganiach regulacyjnych.

Windows Server 2025 Datacenter

W ramach niniejszego zamówienia Zamawiający dopuszcza możliwość zaoferowania produktów równoważnych dla licencji **Windows Server 2025 Datacenter**, pod warunkiem, że produkty te spełniają wymagania techniczne i funkcjonalne, które są co najmniej na poziomie oferowanym przez **Windows Server 2025 Datacenter**. Produkty równoważne muszą zapewniać wysoką wydajność, skalowalność oraz bezpieczeństwo, niezbędne do zarządzania infrastrukturą IT Państwowej Straży Pożarnej (PSP).

Kluczowe kryteria oceny równoważności obejmują:

1. **Wydajność i skalowalność:** Produkt musi oferować zaawansowane funkcje skalowania, w tym możliwość obsługi wielu maszyn wirtualnych oraz efektywnego zarządzania zasobami obliczeniowymi, co jest kluczowe dla pracy PSP w środowiskach wielozadaniowych.
2. **Wirtualizacja:** Równoważne rozwiązanie musi wspierać nieograniczoną wirtualizację serwerów, umożliwiając efektywne zarządzanie dużymi infrastrukturami IT i optymalizację wykorzystania zasobów.
3. **Wysoka dostępność:** Produkt musi oferować zaawansowane mechanizmy wysokiej dostępności (HA), takie jak funkcja klastrowania oraz replikacja, zapewniające nieprzerwane działanie systemów krytycznych PSP, nawet w przypadku awarii.
4. **Bezpieczeństwo danych i systemu:** Produkt równoważny musi zawierać zaawansowane mechanizmy ochrony danych, w tym wbudowane narzędzia do szyfrowania, zarządzania tożsamościami oraz kontrolowania dostępu, zgodnie z najwyższymi standardami bezpieczeństwa oraz przepisami, takimi jak RODO.
5. **Zarządzanie i automatyzacja:** Równoważny system musi oferować zaawansowane narzędzia do zarządzania infrastrukturą, w tym mechanizmy automatyzacji zadań administracyjnych i zarządzania zasobami w dużych środowiskach IT.

Nr sprawy: BF-IV.2370.26.2024

Załącznik nr 1 do SWZ/ nr 1 do umowy

6. **Integracja z istniejącymi systemami:** Produkt równoważny musi być w pełni kompatybilny z istniejącą infrastrukturą IT PSP oraz umożliwiać integrację z używanymi rozwiązaniami, takimi jak systemy wspomagania decyzji (SWD) oraz inne krytyczne aplikacje.

Dopuszczenie produktów równoważnych ma na celu zapewnienie uczciwej konkurencji, jednak Zamawiający zastrzega, że oferowane produkty równoważne muszą być w pełni kompatybilne z istniejącą infrastrukturą IT i wspierać kluczowe funkcjonalności niezbędne do zapewnienia ciągłości działania operacyjnego PSP.

Równoważność:

Poniżej przedstawione są szczegółowe wymagania dotyczące równoważności, które muszą być spełnione przez oferowane produkty lub usługi, aby zostały uznane za równoważne z określonymi w specyfikacji zamówienia.

Tytuł wymagania: WDC.1.2024 - Obsługa nieograniczonej liczby maszyn wirtualnych

Opis wymagania:

System operacyjny musi umożliwiać uruchamianie i zarządzanie nieograniczoną liczbą maszyn wirtualnych na danym serwerze fizycznym, bez ograniczeń dotyczących liczby instancji wirtualnych, przy jednoczesnym zapewnieniu optymalnej wydajności i stabilności.

Kluczowe aspekty:

- System powinien wspierać dynamiczne przydzielanie zasobów dla każdej z maszyn wirtualnych w zależności od aktualnych potrzeb operacyjnych.
- Funkcjonalność zarządzania zasobami wirtualnymi musi zapewniać optymalne wykorzystanie procesora, pamięci RAM i pamięci masowej.
- Należy zapewnić możliwość centralnego zarządzania maszynami wirtualnymi oraz ich łatwej migracji między serwerami fizycznymi w ramach infrastruktury.

Cel:

Zwiększenie elastyczności zarządzania środowiskami wirtualnymi, co pozwala na maksymalne wykorzystanie zasobów sprzętowych oraz usprawnia administrowanie wirtualizacją w dużych środowiskach.

Tytuł wymagania: WDC.2.2024 - Wzmocnione zabezpieczenia serwera

Opis wymagania:

System operacyjny musi oferować zaawansowane funkcje zabezpieczeń w celu ochrony przed złośliwym oprogramowaniem oraz atakami na poziomie sprzętu i oprogramowania. Wymagane jest wdrożenie technologii, które integrują zabezpieczenia na poziomie systemu operacyjnego oraz sprzętu serwera.

Nr sprawy: BF-IV.2370.26.2024
 Załącznik nr 1 do SWZ/ nr 1 do umowy

Kluczowe aspekty:

- Wsparcie dla zabezpieczeń opartych na sprzęcie, takich jak ochrona procesora przed atakami na firmware.
- Funkcjonalność bezpiecznego rozruchu, która zapobiega uruchamianiu nieautoryzowanego oprogramowania podczas startu systemu.
- Zabezpieczenia bazujące na izolacji pamięci w celu ochrony krytycznych procesów systemowych przed atakami.
- Mechanizmy umożliwiające wykrywanie i zapobieganie atakom wykorzystującym luki w zabezpieczeniach firmware'u.
- System powinien wspierać integralność kodu w czasie rzeczywistym, aby zapobiegać manipulacjom na poziomie oprogramowania.

Cel:

Zwiększenie odporności serwera na zagrożenia bezpieczeństwa poprzez integrację mechanizmów ochronnych zarówno na poziomie sprzętowym, jak i programowym, co zapewni lepszą ochronę danych i aplikacji działających na serwerze.

Tytuł wymagania: WDC.3.2024 - Sprzętowe zaufanie z TPM 2.0

Opis wymagania:

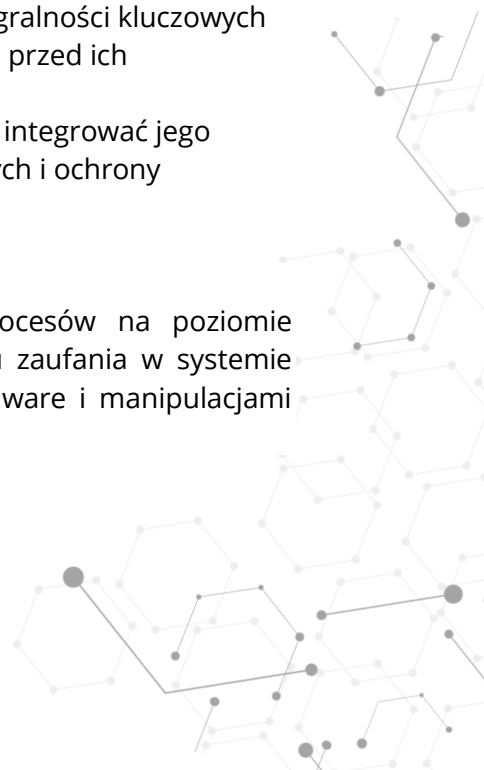
System operacyjny musi wspierać wykorzystanie modułu TPM (Trusted Platform Module) w wersji 2.0 jako sprzętowego źródła zaufania. TPM 2.0 powinien być używany do zapewnienia bezpiecznego przechowywania kluczy kryptograficznych oraz weryfikacji integralności systemu podczas rozruchu.

Kluczowe aspekty:

- System musi umożliwiać wykorzystanie TPM 2.0 do zabezpieczania procesów takich jak szyfrowanie danych i bezpieczny rozruch.
- Wymagana jest integracja funkcji TPM 2.0 z mechanizmami uwierzytelniania systemu, aby zapewnić bezpieczny dostęp do zasobów na poziomie sprzętowym.
- TPM 2.0 powinien wspierać funkcje mierzenia i weryfikacji integralności kluczowych komponentów systemu, takich jak firmware i oprogramowanie przed ich uruchomieniem.
- System powinien automatycznie wykrywać obecność TPM 2.0 i integrować jego funkcjonalności w celu zabezpieczenia operacji kryptograficznych i ochrony tożsamości użytkowników.

Cel:

Zapewnienie najwyższego poziomu bezpieczeństwa danych i procesów na poziomie sprzętowym poprzez zastosowanie modułu TPM 2.0 jako elementu zaufania w systemie operacyjnym, co zwiększa ochronę przed atakami typu rootkit, malware i manipulacjami sprzętowymi.



Nr sprawy: BF-IV.2370.26.2024

Załącznik nr 1 do SWZ/ nr 1 do umowy

Tytuł wymagania: WDC.4.2024 - Ochrona firmware'u z DRTM i DMA

Opis wymagania:

System operacyjny musi zapewniać mechanizmy ochrony firmware'u przy użyciu technologii Dynamic Root of Trust for Measurement (DRTM) oraz ochrony przed nieautoryzowanym dostępem do pamięci przez urządzenia zewnętrzne poprzez zabezpieczenia Direct Memory Access (DMA).

Kluczowe aspekty:

- DRTM: System powinien wspierać funkcję dynamicznego zaufania dla pomiaru (DRTM), która pozwala na weryfikację integralności systemu podczas uruchamiania, zapewniając, że oprogramowanie rozruchowe i firmware nie zostały zmanipulowane.
- DMA: Ochrona przed atakami DMA musi blokować bezpośredni dostęp urządzeń peryferyjnych do pamięci systemowej, co zapobiega nieautoryzowanemu odczytywaniu danych przez urządzenia zewnętrzne.
- System powinien automatycznie inicjować mechanizmy ochrony DMA dla urządzeń podłączanych przez porty PCIe i Thunderbolt, aby minimalizować ryzyko związane z atakami typu „cold boot” i nieautoryzowanym dostępem do danych.
- Obsługa szyfrowania pamięci oraz segmentacji pamięci peryferyjnych, aby uniemożliwić urządzeniom dostępnym przez DMA odczytanie danych systemowych lub aplikacji.

Cel:

Zwiększenie bezpieczeństwa systemu poprzez ochronę firmware'u przed manipulacją oraz zabezpieczenie pamięci przed atakami z urządzeń zewnętrznych, co minimalizuje ryzyko nieautoryzowanego dostępu do krytycznych zasobów systemowych.

Tytuł wymagania: WDC.5.2024 - Bezpieczny rozruch UEFI

Opis wymagania:

System operacyjny musi wspierać funkcję bezpiecznego rozruchu (UEFI Secure Boot), która zapewnia, że podczas uruchamiania systemu uruchamiane są wyłącznie zaufane i autoryzowane komponenty oprogramowania, zapobiegając uruchomieniu złośliwego kodu lub nieautoryzowanego oprogramowania.

Kluczowe aspekty:

- Funkcja UEFI Secure Boot musi weryfikować integralność i autentyczność oprogramowania rozruchowego oraz sterowników przed ich uruchomieniem.
- System powinien blokować uruchamianie niepodpisanego lub zmodyfikowanego kodu, który nie został autoryzowany przez zaufane certyfikaty systemu.
- UEFI Secure Boot musi być w stanie integrować się z infrastrukturą kluczy kryptograficznych, aby umożliwiać dodawanie, usuwanie i zarządzanie zaufanymi certyfikatami.



Nr sprawy: BF-IV.2370.26.2024

Załącznik nr 1 do SWZ/ nr 1 do umowy

- Mechanizmy te powinny automatycznie wykrywać i blokować manipulacje w oprogramowaniu układowym oraz komponentach systemu podczas startu.

Cel:

Zapewnienie bezpiecznego uruchamiania systemu poprzez eliminację ryzyka związanego z wczytywaniem nieautoryzowanego oprogramowania, co zwiększa integralność systemu i chroni go przed złośliwym oprogramowaniem na poziomie rozruchu.

Tytuł wymagania: WDC.6.2024 - Bezpieczeństwo oparte na wirtualizacji (VBS)

Opis wymagania:

System operacyjny musi wspierać funkcję bezpieczeństwa opartą na wirtualizacji (VBS), która wykorzystuje technologię wirtualizacji do izolowania i zabezpieczania krytycznych procesów systemowych oraz danych przed atakami i nieautoryzowanym dostępem.

Kluczowe aspekty:

- **Izolacja wirtualna:** System powinien wykorzystywać wirtualizację do stworzenia bezpiecznych, izolowanych środowisk dla uruchamiania krytycznych procesów systemowych i operacji, takich jak przechowywanie kluczy kryptograficznych oraz procesy uwierzytelniania.
- **Bezpieczne środowiska:** VBS musi umożliwiać tworzenie bezpiecznych środowisk, takich jak Hypervisor-Enforced Code Integrity (HVCI), które chronią przed uruchamianiem złośliwego kodu oraz zapewniają integralność kodu systemowego.
- **Integracja z TPM:** Funkcjonalności VBS powinny współpracować z modułem TPM 2.0, aby dodatkowo zabezpieczyć dane oraz klucze używane w izolowanych środowiskach.
- **Ochrona pamięci:** System powinien zapewniać mechanizmy ochrony pamięci, takie jak Virtualization-based Security (VBS), które chronią przed atakami, które próbują uzyskać dostęp do wrażliwych danych w pamięci systemowej.

Cel:

Zwiększenie poziomu bezpieczeństwa systemu poprzez wykorzystanie technologii wirtualizacji do izolowania krytycznych funkcji i danych, co minimalizuje ryzyko ataków i nieautoryzowanego dostępu, a także chroni integralność systemu operacyjnego.

Tytuł wymagania: WDC.7.2024 - Integralność kodu wymuszona przez hypervisor (HVCI)

Opis wymagania:

System operacyjny musi wspierać funkcję integralności kodu wymuszaną przez hypervisor (HVCI), która wykorzystuje technologię wirtualizacji do zapewnienia, że tylko zaufany i podpisany cyfrowo kod jest wykonywany w systemie. Mechanizm ten chroni system przed uruchamianiem złośliwego lub nieautoryzowanego oprogramowania.

Kluczowe aspekty:

Nr sprawy: BF-IV.2370.26.2024

Załącznik nr 1 do SWZ/ nr 1 do umowy

- **Wymuszona integralność kodu:** HVCI musi zapewniać, że każdy sterownik lub oprogramowanie uruchamiane w systemie jest podpisane cyfrowo i autoryzowane, co zapobiega wprowadzaniu złośliwego kodu.
- **Ochrona przed exploitami:** System musi wykorzystywać HVCI do blokowania exploitów, które próbują modyfikować wrażliwe obszary pamięci, takie jak jądro systemu.
- **Izolacja procesów:** HVCI powinno używać technologii wirtualizacji, aby izolować krytyczne procesy i chronić przed manipulacją z poziomu kodu niskopoziomowego, zwłaszcza w systemach operujących w środowiskach wysokiego ryzyka.
- **Obsługa systemów starszych:** System powinien umożliwiać weryfikację kompatybilności starszych sterowników i oprogramowania z HVCI oraz blokować uruchamianie tych, które nie spełniają standardów bezpieczeństwa.

Cel:

Zapewnienie maksymalnej ochrony systemu operacyjnego poprzez uniemożliwienie uruchamiania nieautoryzowanego i niezweryfikowanego kodu oraz eliminację ryzyka ataków na poziomie jądra systemu i innych krytycznych procesów.

Tytuł wymagania: WDC.8.2024 - Ochrona danych jądra (KDP)

Opis wymagania:

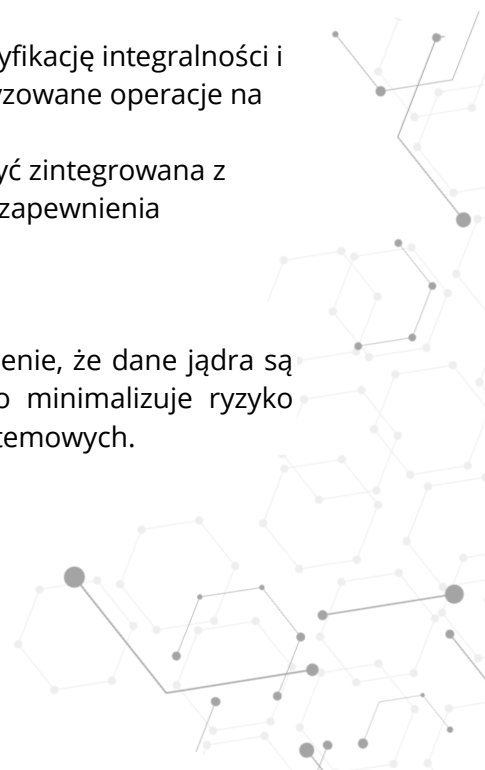
System operacyjny musi wspierać funkcję ochrony danych jądra (Kernel Data Protection, KDP), która zapewnia ochronę integralności i poufności danych używanych przez jądro systemu operacyjnego poprzez mechanizmy zabezpieczeń na poziomie pamięci i procesów.

Kluczowe aspekty:

- **Ochrona pamięci:** KDP musi zapewniać, że dane jądra systemu są zabezpieczone przed nieautoryzowanym dostępem i modyfikacją, w tym przed atakami typu "kernel-level" i próbami przejęcia kontroli nad pamięcią jądra.
- **Izolacja danych:** System powinien stosować mechanizmy izolacji pamięci, które oddzielają dane jądra od innych danych w systemie, w celu zapobiegania manipulacjom i wyciekom informacji.
- **Bezpieczne zarządzanie pamięcią:** KDP musi umożliwiać weryfikację integralności i autoryzację dostępu do pamięci jądra oraz blokować nieautoryzowane operacje na tych danych.
- **Współpraca z HVCI:** Funkcja ochrony danych jądra powinna być zintegrowana z mechanizmami Hypervisor-Based Code Integrity (HVCI) w celu zapewnienia kompleksowej ochrony kodu i danych systemowych.

Cel:

Zwiększenie bezpieczeństwa systemu operacyjnego poprzez zapewnienie, że dane jądra są chronione przed nieautoryzowanym dostępem i manipulacjami, co minimalizuje ryzyko ataków na poziomie jądra systemu i wspiera integralność operacji systemowych.



Nr sprawy: BF-IV.2370.26.2024
Załącznik nr 1 do SWZ/ nr 1 do umowy

Tytuł wymagania: WDC.9.2024 - Natywna obsługa HTTPS i TLS 1.3

Opis wymagania:

System operacyjny musi zapewniać natywną obsługę protokołu HTTPS oraz najnowszej wersji protokołu TLS 1.3 w celu zapewnienia bezpiecznej komunikacji sieciowej poprzez szyfrowanie transmisji danych i ochronę przed atakami, takimi jak podsłuch czy manipulacja danymi.

Kluczowe aspekty:

- **Szyfrowanie TLS 1.3:** System musi wspierać natywnie protokół TLS 1.3, który zapewnia lepsze bezpieczeństwo i wydajność w porównaniu do wcześniejszych wersji, minimalizując czas potrzebny na ustanowienie bezpiecznego połączenia.
- **Zgodność z HTTPS:** Obsługa HTTPS musi być zintegrowana na poziomie systemowym, umożliwiając bezpieczną komunikację pomiędzy klientem a serwerem, eliminując ryzyko wycieku lub manipulacji danymi podczas transmisji.
- **Algorytmy szyfrowania:** TLS 1.3 musi wspierać najnowsze i najsilniejsze algorytmy szyfrowania, takie jak AES-256 i ChaCha20, w celu zapewnienia wysokiego poziomu ochrony danych.
- **Ochrona przed atakami:** System powinien zapewniać mechanizmy ochrony przed atakami typu man-in-the-middle (MITM) oraz downgrade, które mogłyby wpłynąć na jakość szyfrowania lub przechwycić transmisję danych.

Cel:

Zagwarantowanie bezpiecznej komunikacji sieciowej poprzez zastosowanie nowoczesnych protokołów szyfrowania, takich jak TLS 1.3, oraz zapewnienie integralności i poufności danych przesyłanych za pośrednictwem HTTPS. Dzięki temu użytkownicy mogą korzystać z bezpiecznych połączeń bez ryzyka naruszeń bezpieczeństwa.

Tytuł wymagania: WDC.10.2024 - Obsługa DNS-over-HTTPS (DoH)

Opis wymagania:

System operacyjny musi wspierać natywną obsługę protokołu DNS-over-HTTPS (DoH), który zapewnia szyfrowanie zapytań DNS w celu zwiększenia prywatności i bezpieczeństwa komunikacji sieciowej, zapobiegając podsłuchiwaniu i manipulacji zapytaniami DNS przez osoby trzecie.

Kluczowe aspekty:

- **Szyfrowanie zapytań DNS:** System powinien przysyłać wszystkie zapytania DNS poprzez protokół HTTPS, zapewniając ich szyfrowanie i ochronę przed podsłuchiwaniem przez nieautoryzowane podmioty.
- **Ochrona prywatności:** DoH zapewnia prywatność zapytań DNS użytkowników, chroniąc przed śledzeniem i profilowaniem działań w sieci przez dostawców usług internetowych (ISP) lub inne podmioty.

Nr sprawy: BF-IV.2370.26.2024

Załącznik nr 1 do SWZ/ nr 1 do umowy

- **Zgodność z HTTPS:** Zapytania DNS muszą być tunelowane przez połączenia HTTPS, zapewniając ich integralność i bezpieczeństwo w taki sam sposób jak inne dane przesyłane za pomocą protokołu HTTPS.
- **Ochrona przed manipulacją DNS:** DoH musi zabezpieczać zapytania DNS przed atakami typu man-in-the-middle (MITM) oraz przed fałszowaniem odpowiedzi DNS (DNS spoofing).
- **Konfiguracja serwerów DoH:** System powinien umożliwiać administratorom łatwą konfigurację i zarządzanie zaufanymi serwerami DoH, a także dynamiczne przełączanie między nimi w zależności od potrzeb sieciowych.

Cel:

Zwiększenie prywatności i bezpieczeństwa w komunikacji sieciowej poprzez szyfrowanie zapytań DNS, co uniemożliwia ich monitorowanie, przechwytywanie lub manipulowanie. Dzięki temu użytkownicy mogą bezpiecznie i prywatnie korzystać z internetu, minimalizując ryzyko ataków i śledzenia.

Tytuł wymagania: WDC.11.2024 - Szyfrowanie SMB z wykorzystaniem AES-256

Opis wymagania:

System operacyjny musi obsługiwać szyfrowanie protokołu SMB (Server Message Block) z wykorzystaniem algorytmu AES-256, aby zapewnić bezpieczne przesyłanie danych pomiędzy klientami a serwerami, chroniąc je przed nieautoryzowanym dostępem i podsłuchem.

Kluczowe aspekty:

- **Algorytm AES-256:** System musi natywnie wspierać szyfrowanie ruchu SMB przy użyciu algorytmu AES-256, który oferuje wysoki poziom ochrony danych dzięki 256-bitowemu kluczowi szyfrowania.
- **Ochrona transmisji:** Szyfrowanie musi zabezpieczać całą komunikację SMB, w tym pliki, katalogi, metadane oraz inne dane przesyłane pomiędzy klientem a serwerem.
- **Integralność danych:** AES-256 musi zapewniać nie tylko poufność, ale również integralność danych, uniemożliwiając ich modyfikację przez nieautoryzowane podmioty podczas transmisji.
- **Wydajność:** System powinien optymalizować szyfrowanie SMB z AES-256, aby minimalizować wpływ na wydajność sieci, zapewniając jednocześnie wysoki poziom bezpieczeństwa.
- **Obsługa wirtualnych zasobów:** System powinien umożliwiać szyfrowanie SMB w środowiskach wirtualnych oraz w chmurze, zapewniając bezpieczną wymianę danych zarówno w lokalnych sieciach, jak i w zdalnych połączeniach.

Cel:

Zagwarantowanie bezpiecznego przesyłania plików i danych w sieciach lokalnych i rozproszonych przy użyciu szyfrowania SMB z algorytmem AES-256, co chroni wrażliwe informacje przed nieautoryzowanym dostępem i potencjalnymi atakami.

Nr sprawy: BF-IV.2370.26.2024

Załącznik nr 1 do SWZ/ nr 1 do umowy

Tytuł wymagania: WDC.12.2024 - Szyfrowanie SMB East-West dla komunikacji wewnątrz klastra

Opis wymagania:

System operacyjny musi wspierać szyfrowanie protokołu SMB (Server Message Block) dla komunikacji wewnętrznej (East-West) w ramach klastra, zapewniając bezpieczne przesyłanie danych pomiędzy różnymi węzłami w klastrze, chroniąc je przed nieautoryzowanym dostępem i manipulacją.

Kluczowe aspekty:

- **Szyfrowanie komunikacji East-West:** System powinien stosować szyfrowanie dla komunikacji SMB pomiędzy węzłami w klastrze, aby zabezpieczyć dane przesyłane między serwerami, maszynami wirtualnymi oraz innymi komponentami wewnątrz klastra.
- **Algorytmy szyfrowania:** Szyfrowanie powinno być realizowane przy użyciu mocnych algorytmów, takich jak AES-256, aby zapewnić wysoki poziom ochrony danych oraz integralność komunikacji wewnętrznej.
- **Wydajność i skalowalność:** System musi zapewniać, że szyfrowanie SMB East-West nie wpływa negatywnie na wydajność klastra i jest skalowalne, aby sprostać rosnącym potrzebom i obciążeniom sieciowym.
- **Zarządzanie kluczami:** System powinien oferować bezpieczne mechanizmy zarządzania kluczami szyfrowania, w tym ich rotację i aktualizację, aby utrzymać wysoki poziom bezpieczeństwa komunikacji.
- **Integracja z innymi mechanizmami bezpieczeństwa:** Szyfrowanie komunikacji SMB w klastrze powinno być zintegrowane z innymi mechanizmami zabezpieczeń systemu, takimi jak kontrola dostępu i monitorowanie aktywności, w celu zapewnienia kompleksowej ochrony.

Cel:

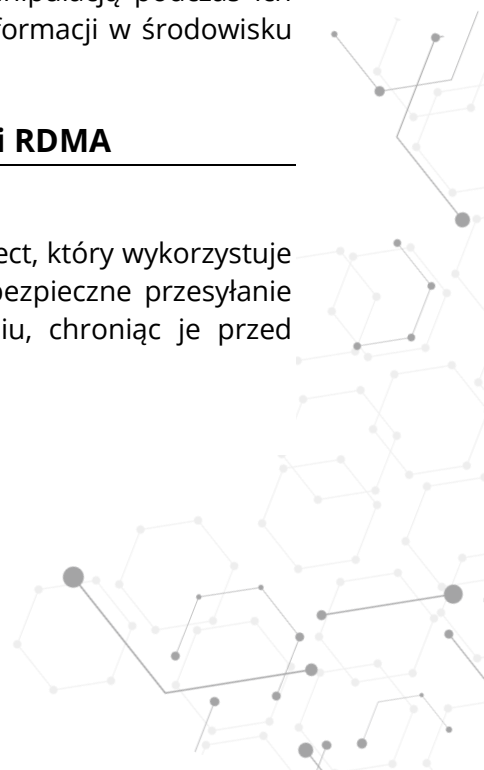
Zabezpieczenie komunikacji wewnątrz klastra poprzez stosowanie szyfrowania SMB East-West, co chroni dane przed nieautoryzowanym dostępem oraz manipulacją podczas ich przesyłania między węzłami, zapewniając integralność i poufność informacji w środowisku rozproszonym.

Tytuł wymagania: WDC.13.2024 - Szyfrowanie SMB Direct i RDMA

Opis wymagania:

System operacyjny musi wspierać szyfrowanie dla protokołu SMB Direct, który wykorzystuje technologię RDMA (Remote Direct Memory Access), aby zapewnić bezpieczne przesyłanie danych z wysoką wydajnością w połączeniach o niskim opóźnieniu, chroniąc je przed nieautoryzowanym dostępem i podsłuchem.

Kluczowe aspekty:



Nr sprawy: BF-IV.2370.26.2024

Załącznik nr 1 do SWZ/ nr 1 do umowy

- **Szyfrowanie SMB Direct:** System musi zapewniać szyfrowanie wszystkich danych przesyłanych za pomocą SMB Direct z wykorzystaniem algorytmów takich jak AES-256, bez wpływu na niskie opóźnienia i wysoką przepustowość charakterystyczną dla RDMA.
- **Obsługa RDMA:** Szyfrowanie danych musi być kompatybilne z różnymi implementacjami RDMA, takimi jak iWARP, InfiniBand i RoCE, zapewniając integralność i poufność danych niezależnie od stosowanej technologii RDMA.
- **Minimalizacja wpływu na wydajność:** Szyfrowanie nie powinno znacząco wpływać na wydajność połączeń RDMA, zachowując wysoką przepustowość i niskie opóźnienia, które są kluczowe dla obciążeń o dużych wymaganiach dotyczących przesyłu danych, takich jak bazy danych czy aplikacje czasu rzeczywistego.
- **Ochrona przed atakami:** System musi zapewniać ochronę przed nieautoryzowanym dostępem do danych przesyłanych za pośrednictwem RDMA, zapobiegając atakom typu man-in-the-middle (MITM) oraz innym zagrożeniom związanym z komunikacją sieciową.
- **Bezpieczne połączenia między serwerami:** Szyfrowanie SMB Direct powinno być szczególnie skoncentrowane na ochronie komunikacji między serwerami w środowiskach klastrów oraz podczas wymiany danych między centrami danych.

Cel:

Zwiększenie bezpieczeństwa danych przesyłanych za pośrednictwem SMB Direct i RDMA poprzez zastosowanie szyfrowania, zapewniając jednocześnie niskie opóźnienia i wysoką wydajność transmisji. Szyfrowanie chroni dane przed nieautoryzowanym dostępem i manipulacją, co jest kluczowe w środowiskach, gdzie wymagana jest szybka i bezpieczna wymiana informacji.

Tytuł wymagania: WDC.14.2024 - Obsługa serwerów z Azure Arc

Opis wymagania:

System operacyjny musi natywnie wspierać integrację z platformą Azure Arc, umożliwiając zarządzanie serwerami fizycznymi i wirtualnymi zarówno w środowiskach lokalnych, jak i chmurowych, przy użyciu jednolitego panelu sterowania i narzędzi zarządzania oferowanych przez Azure.

Kluczowe aspekty:

- **Zarządzanie hybrydowe:** System powinien umożliwiać zarządzanie serwerami w środowiskach lokalnych, multi-cloud oraz edge, z wykorzystaniem narzędzi i usług Azure Arc, zapewniając spójność operacyjną niezależnie od lokalizacji serwerów.
- **Monitorowanie i automatyzacja:** System musi wspierać monitorowanie, zabezpieczanie i automatyzację zarządzania serwerami przez platformę Azure, umożliwiając automatyczne aktualizacje, konfiguracje i wdrożenia polityki bezpieczeństwa.
- **Zarządzanie tożsamościami i dostępem:** Serwery zarządzane przez Azure Arc muszą być integrowane z Azure Active Directory (Azure AD) w celu centralnego



Nr sprawy: BF-IV.2370.26.2024

Załącznik nr 1 do SWZ/ nr 1 do umowy

zarządzania tożsamościami, kontrolą dostępu oraz zapewnienia zgodności z politykami bezpieczeństwa.

- **Rozszerzenie usług Azure:** System powinien umożliwiać wykorzystanie usług Azure, takich jak Azure Security Center, Azure Policy czy Azure Monitor, do monitorowania, zgodności i zabezpieczania serwerów zarządzanych przez Azure Arc.
- **Elastyczność wdrażania:** System musi wspierać zarządzanie zarówno maszynami wirtualnymi, jak i fizycznymi serwerami w różnych środowiskach chmurowych i lokalnych, umożliwiając elastyczne wdrażanie i skalowanie.

Cel:

Zapewnienie jednolitego, scentralizowanego zarządzania serwerami w środowiskach hybrydowych i wielochmurowych poprzez integrację z Azure Arc, co umożliwia efektywne monitorowanie, automatyzację, zabezpieczanie i zarządzanie serwerami w różnych lokalizacjach przy zachowaniu zgodności operacyjnej i bezpieczeństwa.

Tytuł wymagania: WDC.15.2024 - Windows Admin Center z rozszerzonymi funkcjami zarządzania

Opis wymagania:

System operacyjny musi wspierać pełną integrację z Windows Admin Center, oferując rozszerzone funkcje zarządzania serwerami, maszynami wirtualnymi oraz środowiskami chmurowymi, umożliwiając administratorom centralne zarządzanie i monitorowanie zaawansowanych funkcji serwerowych.

Kluczowe aspekty:

- **Zarządzanie serwerami:** Windows Admin Center powinien umożliwiać zaawansowane zarządzanie serwerami lokalnymi i chmurowymi, w tym monitorowanie wydajności, konfigurację systemu, zarządzanie zasobami, aktualizacjami oraz usługami.
- **Zarządzanie maszynami wirtualnymi:** System powinien wspierać zarządzanie maszynami wirtualnymi, w tym tworzenie, migrację, konfigurację zasobów oraz monitorowanie wydajności maszyn wirtualnych poprzez intuicyjny interfejs graficzny Windows Admin Center.
- **Monitorowanie i automatyzacja:** Windows Admin Center musi oferować zaawansowane narzędzia do monitorowania stanu systemu, w tym alerty oparte na progach wydajności, a także umożliwiać automatyzację zadań administracyjnych, takich jak aktualizacje systemu i zarządzanie użytkownikami.
- **Zarządzanie chmurą i hybrydowe:** System powinien integrować się z usługami chmurowymi, takimi jak Azure, oferując administratorom możliwość zarządzania serwerami w środowiskach hybrydowych oraz korzystania z narzędzi takich jak Azure Backup czy Azure Site Recovery.
- **Rozszerzalność:** Windows Admin Center musi wspierać rozszerzenia umożliwiające dodawanie nowych funkcji, takich jak integracja z narzędziami do zarządzania

Nr sprawy: BF-IV.2370.26.2024

Załącznik nr 1 do SWZ/ nr 1 do umowy
 zasobami sieciowymi, monitorowaniem bezpieczeństwa czy kontrolą dostępu,
 pozwalając na dostosowanie systemu do specyficznych potrzeb.

Cel:

Zapewnienie centralnego, zintegrowanego narzędzia do zarządzania serwerami, maszynami wirtualnymi i środowiskami hybrydowymi poprzez Windows Admin Center, które umożliwia monitorowanie, automatyzację i zarządzanie infrastrukturą IT z poziomu jednej platformy, poprawiając efektywność i bezpieczeństwo administracji serwerowej.

Tytuł wymagania: WDC.16.2024 - Zmniejszony rozmiar obrazów kontenerów systemu

Opis wymagania:

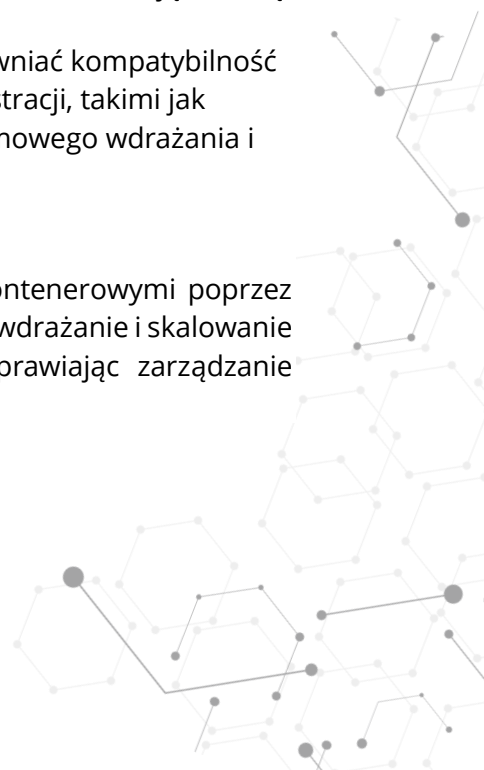
System operacyjny musi wspierać zoptymalizowane obrazy kontenerów Windows o zmniejszonym rozmiarze, co pozwoli na szybsze pobieranie, wdrażanie i uruchamianie aplikacji kontenerowych, a także efektywniejsze zarządzanie zasobami.

Kluczowe aspekty:

- **Redukcja rozmiaru obrazów:** System powinien zapewniać obrazy kontenerów zoptymalizowane pod kątem minimalnego rozmiaru, bez uszczerbku dla funkcjonalności wymaganych do uruchamiania aplikacji w środowisku produkcyjnym.
- **Szybsze wdrażanie:** Mniejsze obrazy kontenerów powinny umożliwiać szybsze pobieranie, instalowanie i uruchamianie kontenerów, co poprawi czas reakcji na zmiany w infrastrukturze i ułatwi skalowanie aplikacji.
- **Optymalizacja zasobów:** System musi wspierać optymalne zarządzanie zasobami pamięci i procesora podczas pracy kontenerów, co pozwala na uruchamianie większej liczby kontenerów na tej samej infrastrukturze, minimalizując koszty operacyjne.
- **Wersje obrazów minimalnych:** Powinny być dostępne obrazy minimalne dla aplikacji, które nie wymagają pełnego środowiska systemowego, umożliwiając dalszą redukcję zasobów potrzebnych do uruchomienia kontenerów.
- **Zgodność z narzędziami orkiestracji:** System powinien zapewniać kompatybilność zoptymalizowanych obrazów kontenerów z platformami orkiestracji, takimi jak Kubernetes czy Docker Swarm, w celu zapewnienia bezproblemowego wdrażania i zarządzania.

Cel:

Zwiększenie wydajności i elastyczności w zarządzaniu aplikacjami kontenerowymi poprzez zmniejszenie rozmiaru obrazów kontenerów Windows, co przyspiesza wdrażanie i skalowanie aplikacji, jednocześnie zmniejszając wymagania zasobów oraz poprawiając zarządzanie infrastrukturą.



Nr sprawy: BF-IV.2370.26.2024

Załącznik nr 1 do SWZ/ nr 1 do umowy

Tytuł wymagania: WDC.17.2024 - Wsparcie dla Azure Active Directory z gMSA bez dołączania do domeny

Opis wymagania:

System operacyjny musi wspierać zarządzane konta usług grupowych (gMSA) w integracji z Azure Active Directory (Azure AD) bez konieczności dołączania serwera do tradycyjnej domeny Active Directory. Rozwiązanie to ma umożliwiać bezpieczne uwierzytelnianie i zarządzanie kontami usług w środowiskach hybrydowych i chmurowych.

Kluczowe aspekty:

- **gMSA z Azure AD:** System powinien wspierać zarządzane konta usług grupowych (gMSA) skonfigurowane z Azure AD, co pozwoli na bezpieczne zarządzanie tożsamościami usług bez potrzeby dołączania do domeny Active Directory.
- **Uwierzytelnianie usług:** gMSA powinny umożliwiać aplikacjom i usługom działającym na serwerach w środowisku Azure AD bezpieczne uwierzytelnianie przy wykorzystaniu zarządzanych haseł, eliminując konieczność ręcznego zarządzania poświadczeniami.
- **Środowiska hybrydowe i chmurowe:** Funkcjonalność ta powinna być szczególnie przydatna w środowiskach hybrydowych oraz chmurowych, gdzie pełne dołączenie serwerów do lokalnej domeny Active Directory nie jest wymagane lub pożądane.
- **Bezpieczeństwo i rotacja haseł:** System musi zapewniać automatyczną rotację i bezpieczne przechowywanie haseł dla kont gMSA, zapewniając bezpieczeństwo poświadczeń oraz zgodność z najlepszymi praktykami w zakresie zarządzania tożsamościami.
- **Zarządzanie z Azure AD:** Administratorzy powinni mieć możliwość zarządzania i monitorowania gMSA bezpośrednio z poziomu Azure AD, integrując zarządzanie tożsamościami z innymi usługami chmurowymi Microsoft.

Cel:

Umożliwienie bezpiecznego zarządzania kontami usług w środowiskach opartych na Azure AD bez konieczności dołączania serwerów do tradycyjnej domeny Active Directory, co ułatwia wdrażanie i zarządzanie aplikacjami w chmurze i środowiskach hybrydowych, minimalizując ryzyko związane z ręcznym zarządzaniem poświadczeniami.

Tytuł wymagania: WDC.18.2024 - Wsparcie dla Microsoft Distributed Transaction Coordinator (MSDTC) w kontenerach

Opis wymagania:

System operacyjny musi wspierać uruchamianie Microsoft Distributed Transaction Coordinator (MSDTC) w środowisku kontenerowym, umożliwiając rozproszone transakcje między aplikacjami działającymi w kontenerach oraz między kontenerami a zewnętrznymi źródłami danych, takimi jak bazy danych i usługi.

Kluczowe aspekty:

Nr sprawy: BF-IV.2370.26.2024

Załącznik nr 1 do SWZ/ nr 1 do umowy

- **Obsługa rozproszonych transakcji:** System musi wspierać pełną funkcjonalność MSDTC w kontenerach, pozwalając na zarządzanie transakcjami rozproszonymi, które obejmują wiele komponentów, takich jak serwery baz danych, aplikacje i inne zasoby sieciowe.
- **Zgodność z kontenerami:** MSDTC musi być zoptymalizowany do pracy w kontenerach, zapewniając wydajność i niezawodność nawet w dynamicznie skalowanych środowiskach kontenerowych.
- **Integracja z zewnętrznymi źródłami danych:** System powinien umożliwiać kontenerom korzystanie z MSDTC do koordynowania transakcji między różnymi bazami danych (np. SQL Server, Oracle) oraz innymi usługami dostępnymi w sieci.
- **Wysoka dostępność:** System musi wspierać mechanizmy zapewniające wysoką dostępność i skalowalność MSDTC w środowiskach kontenerowych, umożliwiając równoczesne zarządzanie wieloma transakcjami przy minimalnych opóźnieniach.
- **Bezpieczeństwo transakcji:** Funkcje MSDTC w kontenerach muszą być zabezpieczone przed nieautoryzowanym dostępem, a dane związane z transakcjami muszą być chronione za pomocą odpowiednich mechanizmów szyfrowania oraz zarządzania tożsamościami.

Cel:

Zapewnienie wsparcia dla MSDTC w środowiskach kontenerowych, umożliwiając aplikacjom uruchamianym w kontenerach realizację rozproszonych transakcji z innymi usługami i bazami danych, co zwiększa elastyczność i skalowalność nowoczesnych aplikacji korzystających z kontenerów.

Tytuł wymagania: WDC.19.2024 - Wsparcie dla Microsoft Message Queuing (MSMQ) w kontenerach

Opis wymagania:

System operacyjny musi wspierać uruchamianie Microsoft Message Queuing (MSMQ) w środowisku kontenerowym, umożliwiając zarządzanie i przetwarzanie wiadomości w rozproszonych aplikacjach kontenerowych oraz zapewniając integralność i niezawodność systemów kolejkowania wiadomości.

Kluczowe aspekty:

- **Obsługa MSMQ w kontenerach:** System musi umożliwiać instalację i uruchamianie usług MSMQ w kontenerach, zapewniając pełną funkcjonalność kolejkowania wiadomości, jak w tradycyjnych środowiskach serwerowych.
- **Kompatybilność z aplikacjami:** MSMQ powinno być kompatybilne z aplikacjami działającymi w kontenerach, umożliwiając komunikację między kontenerami oraz między kontenerami a innymi komponentami systemu, takimi jak bazy danych i usługi zewnętrzne.
- **Wydajność i skalowalność:** System musi zapewniać odpowiednią wydajność i skalowalność MSMQ w środowiskach kontenerowych, pozwalając na efektywne zarządzanie dużymi wolumenami wiadomości oraz elastyczne skalowanie aplikacji.

Nr sprawy: BF-IV.2370.26.2024

Załącznik nr 1 do SWZ/ nr 1 do umowy

- **Zarządzanie i monitorowanie:** Kontenery powinny wspierać mechanizmy zarządzania i monitorowania MSMQ, w tym dostęp do logów, metryk wydajności oraz narzędzi do diagnozowania problemów związanych z przesyłaniem wiadomości.
- **Bezpieczeństwo:** System musi zapewniać odpowiednie mechanizmy zabezpieczeń dla MSMQ działającego w kontenerach, w tym szyfrowanie wiadomości i kontrolę dostępu, aby chronić dane i komunikację przed nieautoryzowanym dostępem.

Cel:

Umożliwienie skutecznego zarządzania komunikacją opartą na kolejkach wiadomości w środowiskach kontenerowych poprzez wsparcie dla Microsoft Message Queuing (MSMQ), co pozwala na integrację i skalowanie aplikacji kontenerowych oraz zapewnia niezawodność i bezpieczeństwo systemów kolejkowania wiadomości.

Tytuł wymagania: WDC.20.2024 - Przypisywanie prostych magistrali do kontenerów izolowanych procesowo

Opis wymagania:

System operacyjny musi wspierać przypisywanie prostych magistrali (np. PCIe, USB) do kontenerów izolowanych procesowo, umożliwiając bezpośredni dostęp do sprzętu przez aplikacje działające w kontenerach, przy jednoczesnym zachowaniu wysokiego poziomu bezpieczeństwa i izolacji procesów.

Kluczowe aspekty:

- **Bezpośredni dostęp do magistrali:** System powinien umożliwiać przypisywanie prostych magistrali sprzętowych, takich jak PCIe czy USB, do kontenerów izolowanych procesowo, zapewniając dostęp do urządzeń fizycznych, takich jak karty sieciowe, urządzenia magazynujące czy inne peryferia.
- **Izolacja procesowa:** Kontenery muszą być izolowane procesowo, co zapewnia, że dostęp do sprzętu przez kontener nie wpływa na inne procesy działające na tym samym serwerze, minimalizując ryzyko kolizji lub naruszeń bezpieczeństwa.
- **Bezpieczeństwo:** System powinien wdrożyć mechanizmy bezpieczeństwa, które uniemożliwiają nieautoryzowane procesy w kontenerze na dostęp do magistrali i chronią dane przesyłane przez przypisane urządzenia przed nieautoryzowanym dostępem.
- **Wydajność:** Kontenery izolowane procesowo muszą zapewniać wydajność zbliżoną do natywnego dostępu do urządzeń sprzętowych, co jest kluczowe dla aplikacji wymagających wysokiej przepustowości lub niskich opóźnień.
- **Zarządzanie sprzętem:** System musi umożliwiać łatwe przypisywanie i zwalnianie magistrali sprzętowych do i z kontenerów, wspierając dynamiczne zmiany konfiguracji i skalowanie aplikacji bez przerywania ich działania.

Cel:

Zapewnienie elastyczności i wydajności w aplikacjach kontenerowych, które wymagają bezpośredniego dostępu do sprzętu, poprzez wsparcie przypisywania prostych magistrali do

Nr sprawy: BF-IV.2370.26.2024

Załącznik nr 1 do SWZ/ nr 1 do umowy

kontenerów izolowanych procesowo. Dzięki temu aplikacje działające w kontenerach mogą bezpiecznie korzystać z urządzeń sprzętowych, przy zachowaniu izolacji procesów i wysokiego poziomu bezpieczeństwa.

Tytuł wymagania: WDC.21.2024 - Akceleracja sprzętowa DirectX API w kontenerach Windows

Opis wymagania:

System operacyjny musi zapewniać wsparcie dla akceleracji sprzętowej API DirectX w środowisku kontenerowym, umożliwiając aplikacjom uruchamianym w kontenerach Windows wykorzystanie zasobów graficznych hosta, takich jak GPU, do renderowania grafiki oraz przetwarzania zadań związanych z obliczeniami graficznymi.

Kluczowe aspekty:

- **Dostęp do GPU:** Kontenery muszą mieć możliwość uzyskania bezpośredniego dostępu do zasobów GPU hosta w celu wykorzystania akceleracji sprzętowej w zadaniach graficznych, takich jak rendering 3D, wideo czy obliczenia GPGPU.
- **Obsługa DirectX API:** System musi wspierać pełne funkcje DirectX API w kontenerach, umożliwiając uruchamianie aplikacji zależnych od DirectX, takich jak gry, aplikacje CAD czy symulacje naukowe.
- **Optymalizacja wydajności:** Wsparcie dla DirectX w kontenerach powinno zapewniać wydajność zbliżoną do natywnego uruchamiania aplikacji na hostach fizycznych.
- **Zabezpieczenia:** Dostęp do zasobów GPU musi być izolowany i kontrolowany w taki sposób, aby zabezpieczyć kontenery przed dostępem do zasobów graficznych innych aplikacji.

Cel:

Umożliwienie aplikacjom kontenerowym wykorzystania akceleracji sprzętowej DirectX w środowisku Windows w celu poprawy wydajności grafiki i obliczeń graficznych, co jest szczególnie istotne dla aplikacji graficznie intensywne.

Tytuł wymagania: WDC.22.2024 - Wsparcie dla kontenerów host-process do konfiguracji węzłów

Opis wymagania:

System operacyjny musi zapewniać wsparcie dla kontenerów typu host-process, umożliwiając bezpośredni dostęp do zasobów systemowych hosta w celu wykonywania operacji na poziomie węzła, takich jak konfiguracja systemowa, instalacja oprogramowania czy monitorowanie infrastruktury.

Kluczowe aspekty:

Nr sprawy: BF-IV.2370.26.2024

Załącznik nr 1 do SWZ/ nr 1 do umowy

- **Dostęp do zasobów hosta:** Kontenery host-process muszą mieć dostęp do przestrzeni użytkownika i systemu operacyjnego hosta, umożliwiając zarządzanie konfiguracją węzła, co jest kluczowe dla zadań administracyjnych.
- **Bezpieczeństwo i izolacja:** Chociaż kontenery host-process mają większy dostęp do systemu, system musi zapewniać odpowiednie mechanizmy izolacji i kontroli dostępu, aby zapobiec nieautoryzowanym modyfikacjom i zwiększyć bezpieczeństwo.
- **Zarządzanie węzłami:** Kontenery host-process powinny umożliwiać wykonywanie zadań związanych z administracją węzła, takich jak aktualizacje, konfiguracja sieci, instalacja agentów monitorujących, bez potrzeby korzystania z pełnych maszyn wirtualnych.
- **Kompatybilność z narzędziami orkiestracji:** Kontenery tego typu muszą być w pełni kompatybilne z narzędziami zarządzania węzłami w systemach orkiestracji, takich jak Kubernetes.

Cel:

Umożliwienie bardziej elastycznego i wydajnego zarządzania konfiguracją węzłów w środowiskach kontenerowych poprzez wykorzystanie kontenerów host-process, które mogą bezpośrednio wykonywać operacje na poziomie systemu operacyjnego hosta.

Tytuł wymagania: WDC.23.2024 - Wsparcie dla IPv6 w kontenerach

Opis wymagania:

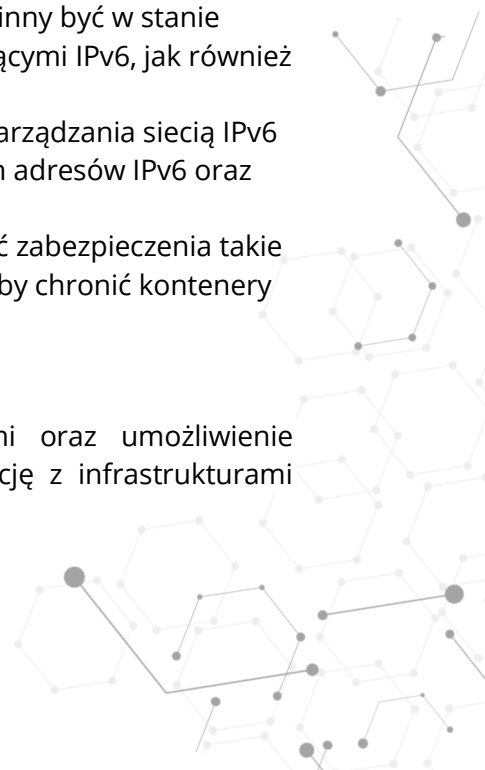
System operacyjny musi wspierać pełną obsługę protokołu IPv6 w kontenerach, umożliwiając aplikacjom kontenerowym korzystanie z adresacji IPv6, zarówno wewnątrz węzła, jak i w komunikacji międzywęzłowej oraz z zewnętrznymi sieciami.

Kluczowe aspekty:

- **Adresacja IPv6:** System musi umożliwiać przypisywanie adresów IPv6 do kontenerów, zapewniając zgodność z nowoczesnymi sieciami opartymi na tym protokole oraz obsługując zarówno lokalną, jak i globalną komunikację sieciową.
- **Kompatybilność z istniejącą infrastrukturą:** Kontenery powinny być w stanie komunikować się z innymi systemami i urządzeniami obsługującymi IPv6, jak również z zasobami w chmurze oraz w środowiskach hybrydowych.
- **Zarządzanie siecią:** System powinien wspierać narzędzia do zarządzania siecią IPv6 w kontenerach, w tym konfigurację statycznych i dynamicznych adresów IPv6 oraz rozwiązywanie nazw DNS w kontekście IPv6.
- **Bezpieczeństwo i izolacja:** Wsparcie dla IPv6 musi obejmować zabezpieczenia takie jak filtrowanie ruchu, firewalle oraz polityki kontroli dostępu, aby chronić kontenery przed zagrożeniami związanymi z komunikacją sieciową IPv6.

Cel:

Zapewnienie zgodności z nowoczesnymi protokołami sieciowymi oraz umożliwienie kontenerom obsługi ruchu IPv6, co pozwala na łatwiejszą integrację z infrastrukturami



Nr sprawy: BF-IV.2370.26.2024

Załącznik nr 1 do SWZ/ nr 1 do umowy

sieciowymi i chmurowymi opartymi na IPv6 oraz zwiększa skalowalność i elastyczność rozwiązań sieciowych.

Tytuł wymagania: WDC.24.2024 - Spójna implementacja polityk sieciowych z Calico

Opis wymagania:

System operacyjny musi zapewniać pełną integrację z narzędziami do zarządzania politykami sieciowymi, takimi jak Calico, umożliwiając definiowanie, egzekwowanie i monitorowanie polityk sieciowych w środowiskach kontenerowych, aby zapewnić spójność konfiguracji oraz bezpieczeństwo ruchu sieciowego.

Kluczowe aspekty:

- **Integracja z Calico:** System musi wspierać Calico jako rozwiązanie do zarządzania politykami sieciowymi, w tym filtrowanie ruchu, kontrolę dostępu oraz wdrażanie polityk bezpieczeństwa w kontenerach.
- **Spójność polityk:** Polityki sieciowe wdrażane przez Calico muszą być spójne w całej infrastrukturze, niezależnie od tego, czy kontenery działają lokalnie, w chmurze czy w środowiskach hybrydowych.
- **Zarządzanie ruchem sieciowym:** System powinien umożliwiać granularne zarządzanie ruchem sieciowym pomiędzy kontenerami oraz innymi komponentami systemu, zapewniając pełną widoczność i kontrolę nad przepływem danych.
- **Bezpieczeństwo i izolacja:** Polityki sieciowe muszą zapewniać izolację kontenerów, ochronę przed atakami sieciowymi oraz możliwość blokowania nieautoryzowanego ruchu zgodnie z zasadami bezpieczeństwa organizacji.

Cel:

Zapewnienie spójnej i bezpiecznej implementacji polityk sieciowych w środowiskach kontenerowych za pomocą narzędzia Calico, co zwiększa bezpieczeństwo i kontrolę nad ruchem sieciowym, jednocześnie ułatwiając zarządzanie siecią w skalowalnych środowiskach.

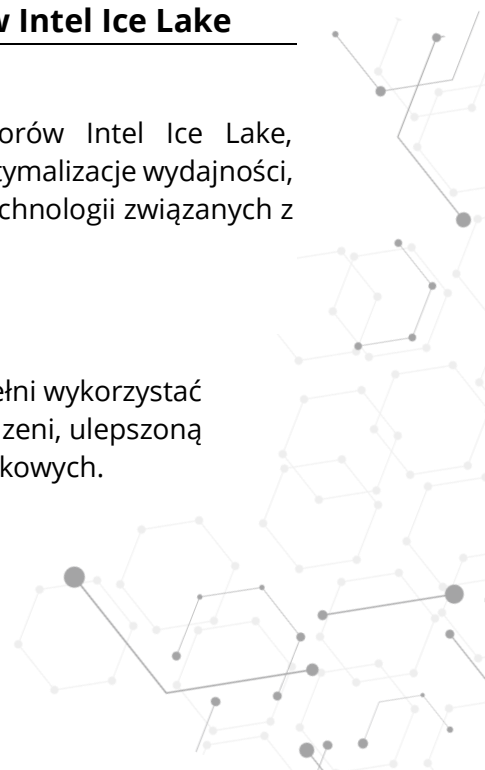
Tytuł wymagania: WDC.25.2024 - Wsparcie dla procesorów Intel Ice Lake

Opis wymagania:

System operacyjny musi zapewniać pełne wsparcie dla procesorów Intel Ice Lake, umożliwiając wykorzystanie ich zaawansowanych funkcji, takich jak optymalizacje wydajności, obsługa większej liczby rdzeni oraz wsparcie dla nowych instrukcji i technologii związanych z bezpieczeństwem.

Kluczowe aspekty:

- **Zoptymalizowana wydajność:** System musi być w stanie w pełni wykorzystać architekturę procesorów Intel Ice Lake, w tym większą liczbę rdzeni, ulepszoną przepustowość pamięci oraz optymalizacje dla zadań wielowątkowych.



Nr sprawy: BF-IV.2370.26.2024

Załącznik nr 1 do SWZ/ nr 1 do umowy

- **Wsparcie dla AVX-512:** System powinien obsługiwać instrukcje AVX-512 oferowane przez procesory Ice Lake, co jest kluczowe dla zadań wymagających wysokiej wydajności obliczeniowej, takich jak przetwarzanie danych, sztuczna inteligencja oraz analityka.
- **Technologie związane z bezpieczeństwem:** System musi wspierać zaawansowane technologie bezpieczeństwa wprowadzone w procesorach Ice Lake, takie jak Intel Control-Flow Enforcement Technology (CET) oraz Intel Total Memory Encryption (TME).
- **Efektywne zarządzanie energią:** System musi umożliwiać zarządzanie funkcjami oszczędzania energii w procesorach Ice Lake, minimalizując zużycie energii bez wpływu na wydajność.

Cel:

Zapewnienie pełnego wsparcia dla najnowszych procesorów Intel Ice Lake, aby umożliwić użytkownikom korzystanie z ich zaawansowanych funkcji wydajnościowych i bezpieczeństwa, co pozwala na optymalizację pracy serwerów oraz aplikacji wymagających dużej mocy obliczeniowej.

Tytuł wymagania: WDC.26.2024 - Confidential computing z Intel SGX

Opis wymagania:

System operacyjny musi wspierać funkcje confidential computing oparte na technologii Intel SGX (Software Guard Extensions), zapewniając bezpieczne uruchamianie aplikacji oraz ochronę danych w izolowanych enklawach sprzętowych, co chroni przed atakami na poziomie sprzętu i systemu.

Kluczowe aspekty:

- **Izolacja danych w enklawach:** System musi umożliwiać uruchamianie aplikacji w izolowanych enklawach sprzętowych przy użyciu Intel SGX, zapewniając ochronę danych oraz kodu aplikacji przed nieautoryzowanym dostępem nawet w przypadku naruszenia bezpieczeństwa systemu.
- **Ochrona poufnych danych:** Technologia Intel SGX powinna być wykorzystywana do ochrony poufnych danych, takich jak klucze kryptograficzne, dane finansowe czy medyczne, zapewniając ich bezpieczeństwo nawet podczas przetwarzania.
- **Wsparcie dla aplikacji chmurowych:** System powinien umożliwiać zastosowanie Intel SGX w środowiskach chmurowych, wspierając confidential computing w aplikacjach, które przetwarzają wrażliwe dane w chmurze.
- **Bezpieczeństwo na poziomie sprzętowym:** Intel SGX musi zapewniać ochronę na poziomie sprzętu przed atakami typu side-channel oraz innymi zagrożeniami, które mogą próbować uzyskać dostęp do danych podczas ich przetwarzania.

Cel:

Zabezpieczenie wrażliwych danych i aplikacji poprzez wykorzystanie technologii confidential computing z Intel SGX, co pozwala na izolację i ochronę danych w dedykowanych enklawach

Nr sprawy: BF-IV.2370.26.2024

Załącznik nr 1 do SWZ/ nr 1 do umowy

sprzętowych, zwiększając poziom bezpieczeństwa w środowiskach lokalnych oraz chmurowych.

Tytuł wymagania: WDC.27.2024 - Wsparcie dla 48 TB pamięci i 2048 rdzeni logicznych

Opis wymagania:

System operacyjny musi obsługiwać konfiguracje serwerowe z maksymalnie 48 TB pamięci RAM oraz 2048 rdzeniami logicznymi, umożliwiając zarządzanie dużymi obciążeniami oraz wdrażanie zasobożernych aplikacji w środowiskach o wysokiej skali.

Kluczowe aspekty:

- **Obsługa dużych konfiguracji sprzętowych:** System musi zapewniać pełne wsparcie dla serwerów z pamięcią RAM do 48 TB oraz procesorów o łącznej liczbie 2048 rdzeni logicznych, co pozwala na wydajną pracę w środowiskach intensywnie wykorzystujących zasoby.
- **Zoptymalizowane zarządzanie pamięcią:** System powinien posiadać funkcje optymalizujące wykorzystanie pamięci w tak dużych konfiguracjach, w tym mechanizmy zarządzania pamięcią wirtualną oraz dynamiczne alokowanie zasobów.
- **Wydajność wieloprotocowa:** System musi być zoptymalizowany do obsługi procesorów z dużą liczbą rdzeni logicznych, zapewniając optymalne rozłożenie obciążenia i minimalizację opóźnień w przetwarzaniu zadań.
- **Zastosowania wielkoskalowe:** Funkcjonalności te powinny wspierać wdrożenia dla baz danych, maszyn wirtualnych oraz innych zasobożernych aplikacji wykorzystywanych w dużych środowiskach korporacyjnych i centrach danych.

Cel:

Zapewnienie wsparcia dla zaawansowanych konfiguracji serwerowych, umożliwiających obsługę bardzo dużych obciążeń, co jest kluczowe dla nowoczesnych centrów danych i rozwiązań chmurowych.

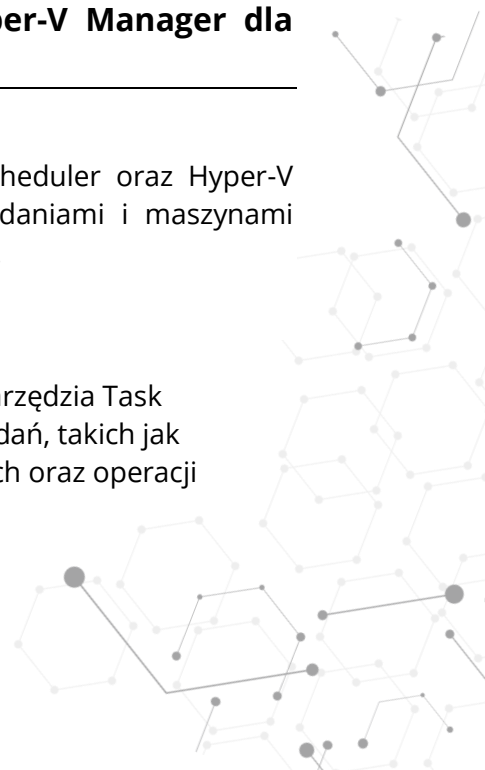
Tytuł wymagania: WDC.28.2024 - Task Scheduler i Hyper-V Manager dla instalacji Server Core

Opis wymagania:

System operacyjny musi zapewniać wsparcie dla narzędzi Task Scheduler oraz Hyper-V Manager w instalacjach Server Core, umożliwiając zarządzanie zadaniami i maszynami wirtualnymi w wersjach systemu o minimalnym interfejsie graficznym.

Kluczowe aspekty:

- **Task Scheduler:** System powinien umożliwiać korzystanie z narzędzia Task Scheduler na Server Core do zarządzania harmonogramem zadań, takich jak automatyczne uruchamianie skryptów, zadań administracyjnych oraz operacji systemowych.



Nr sprawy: BF-IV.2370.26.2024

Załącznik nr 1 do SWZ/ nr 1 do umowy

- **Hyper-V Manager:** Instalacje Server Core muszą wspierać Hyper-V Manager do zarządzania maszynami wirtualnymi, ich konfiguracją, uruchamianiem, zatrzymywaniem oraz migracją w środowisku wirtualizacyjnym.
- **Minimalny interfejs:** Narzędzia te muszą być dostępne w wersji dostosowanej do środowiska bez graficznego interfejsu użytkownika (GUI), zapewniając wydajność i oszczędność zasobów Server Core.
- **Zdalne zarządzanie:** System powinien wspierać zdalne zarządzanie tymi narzędziami, umożliwiając administratorom pracę z nimi z poziomu innych systemów lub za pomocą PowerShell.

Cel:

Zapewnienie administratorom możliwości zarządzania zadaniami oraz maszynami wirtualnymi w środowiskach Server Core, co zwiększa elastyczność i wydajność instalacji bez pełnego GUI, jednocześnie pozwalając na efektywne zarządzanie serwerami.

Tytuł wymagania: WDC.29.2024 - Nested virtualization dla procesorów AMD

Opis wymagania:

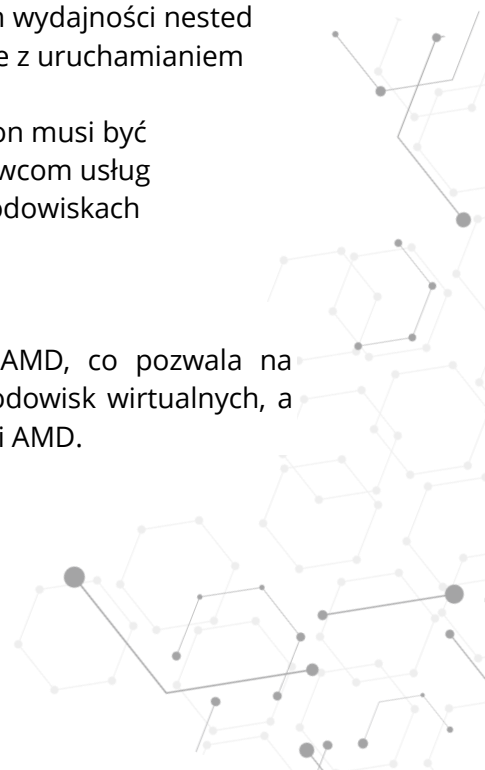
System operacyjny musi wspierać funkcję nested virtualization (wirtualizacji zagnieżdżonej) dla procesorów AMD, umożliwiając uruchamianie maszyn wirtualnych wewnątrz innych maszyn wirtualnych, co pozwala na większą elastyczność w środowiskach testowych i chmurowych.

Kluczowe aspekty:

- **Wsparcie dla AMD:** System musi wspierać nested virtualization na procesorach AMD, zapewniając funkcjonalność podobną do tej dostępnej na procesorach Intel, co umożliwi uruchamianie wielu warstw wirtualizacji.
- **Zarządzanie maszynami wirtualnymi:** Nested virtualization musi umożliwiać efektywne zarządzanie maszynami wirtualnymi wewnątrz innych VM, co jest kluczowe dla środowisk testowych, rozwoju oprogramowania, a także infrastruktury jako usługi (IaaS).
- **Wydajność:** System powinien być zoptymalizowany pod kątem wydajności nested virtualization, minimalizując opóźnienia i przeciążenia związane z uruchamianiem wirtualnych hostów na procesorach AMD.
- **Zastosowania chmurowe:** Funkcjonalność nested virtualization musi być kompatybilna z platformami chmurowymi, umożliwiając dostawcom usług chmurowych uruchamianie maszyn wirtualnych klientów w środowiskach chmurowych opartych na procesorach AMD.

Cel:

Umożliwienie korzystania z nested virtualization na procesorach AMD, co pozwala na zwiększenie elastyczności w testowaniu, rozwoju oraz wdrażaniu środowisk wirtualnych, a także wyrównanie wsparcia funkcjonalnego między platformami Intel i AMD.



Nr sprawy: BF-IV.2370.26.2024

Załącznik nr 1 do SWZ/ nr 1 do umowy

Tytuł wymagania: WDC.30.2024 - Microsoft Edge zamiast Internet Explorer

Opis wymagania:

System operacyjny musi zapewniać wsparcie dla przeglądarki Microsoft Edge jako domyślnej przeglądarki internetowej, zastępując Internet Explorer, który nie jest już wspierany. Microsoft Edge powinien być w pełni zintegrowany z systemem i dostarczać wszystkie funkcje wymagane do bezpiecznego i efektywnego przeglądania sieci.

Kluczowe aspekty:

- **Domyślna przeglądarka:** Microsoft Edge musi być ustawiony jako domyślna przeglądarka internetowa, zintegrowana z systemem operacyjnym i odpowiednio skonfigurowana do obsługi standardowych protokołów internetowych.
- **Kompatybilność i funkcjonalność:** System powinien zapewniać pełną kompatybilność Microsoft Edge z najnowszymi standardami webowymi, w tym wsparcie dla HTML5, CSS3 oraz JavaScript, a także zapewniać dostęp do najnowszych funkcji bezpieczeństwa i prywatności.
- **Migracja danych:** Proces migracji z Internet Explorer do Microsoft Edge powinien być prosty i bezproblemowy, zapewniając przeniesienie zakładek, haseł i ustawień użytkownika.
- **Wsparcie dla aplikacji:** System powinien zapewniać wsparcie dla aplikacji i stron internetowych, które wcześniej były używane z Internet Explorer, w tym umożliwiać korzystanie z trybu zgodności w Microsoft Edge, jeśli to konieczne.

Cel:

Przejsie na Microsoft Edge jako domyślną przeglądarkę internetową, co zapewnia lepszą zgodność z nowoczesnymi standardami internetowymi oraz poprawia bezpieczeństwo i wydajność przeglądania sieci.

Tytuł wymagania: WDC.31.2024 - UDP Segmentation Offload (USO)

Opis wymagania:

System operacyjny musi obsługiwać funkcję UDP Segmentation Offload (USO), co pozwala na przeniesienie operacji segmentacji pakietów UDP z poziomu oprogramowania na sprzęt sieciowy, poprawiając wydajność sieci i zmniejszając obciążenie procesora.

Kluczowe aspekty:

- **Wsparcie dla USO:** System musi być w stanie korzystać z funkcji USO, co oznacza, że sprzęt sieciowy (np. karta sieciowa) przejmuje odpowiedzialność za segmentację dużych pakietów UDP na mniejsze fragmenty przed ich wysłaniem przez sieć.
- **Optymalizacja wydajności:** USO powinno prowadzić do zmniejszenia obciążenia procesora i poprawy wydajności sieci, umożliwiając lepsze wykorzystanie dostępnych zasobów sprzętowych.

Nr sprawy: BF-IV.2370.26.2024

Załącznik nr 1 do SWZ/ nr 1 do umowy

- **Kompatybilność sprzętowa:** System musi wspierać wszystkie karty sieciowe i sprzęt, które oferują funkcję USO, zapewniając ich prawidłowe działanie i integrację z systemem.
- **Monitorowanie i diagnostyka:** System powinien umożliwiać monitorowanie i diagnozowanie funkcji USO, aby zapewnić jej poprawne działanie i umożliwić rozwiązywanie ewentualnych problemów.

Cel:

Poprawa wydajności sieci poprzez przeniesienie operacji segmentacji pakietów UDP na sprzęt, co zmniejsza obciążenie procesora i zwiększa efektywność przesyłania danych.

Tytuł wymagania: WDC.32.2024 - UDP Receive Side Coalescing (UDP RSC)

Opis

wymagania:

System operacyjny musi wspierać funkcję UDP Receive Side Coalescing (UDP RSC), co pozwala na efektywne grupowanie przychodzących pakietów UDP przed ich przetworzeniem przez system, co zmniejsza liczbę przerw i poprawia wydajność przetwarzania sieciowego.

Kluczowe aspekty:

- **Wsparcie dla UDP RSC:** System musi obsługiwać UDP RSC, umożliwiając sprzętowi sieciowemu grupowanie kilku pakietów UDP w jeden większy pakiet przed przekazaniem go do systemu operacyjnego w celu przetworzenia.
- **Optymalizacja wydajności:** UDP RSC powinno prowadzić do zmniejszenia liczby przerw procesora związanych z obsługą pakietów UDP, co poprawia wydajność i efektywność przetwarzania sieciowego.
- **Kompatybilność sprzętowa:** System musi wspierać karty sieciowe i sprzęt, które oferują funkcję UDP RSC, zapewniając ich pełną integrację z systemem operacyjnym.
- **Monitorowanie i diagnostyka:** System powinien umożliwiać monitorowanie i diagnostykę funkcji UDP RSC, zapewniając narzędzia do rozwiązywania problemów i optymalizacji działania.

Cel:

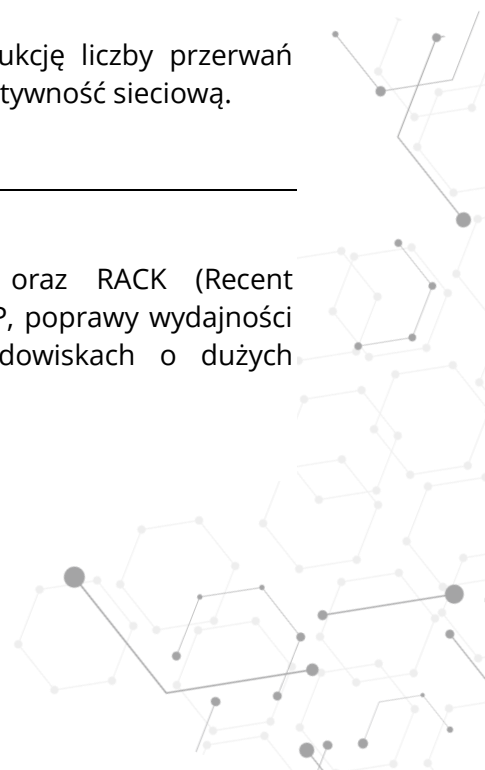
Zwiększenie wydajności przetwarzania pakietów UDP poprzez redukcję liczby przerw procesora i efektywne grupowanie pakietów, co poprawia ogólną efektywność sieciową.

Tytuł wymagania: WDC.33.2024 - TCP HyStart++ i RACK

Opis wymagania:

System operacyjny musi obsługiwać funkcje TCP HyStart++ oraz RACK (Recent Acknowledgment) w celu optymalizacji zarządzania połączeniami TCP, poprawy wydajności transmisji danych i zmniejszenia opóźnień, szczególnie w środowiskach o dużych opóźnieniach sieciowych.

Kluczowe aspekty:



Nr sprawy: BF-IV.2370.26.2024

Załącznik nr 1 do SWZ/ nr 1 do umowy

- **TCP HyStart++:** System musi wspierać HyStart++, mechanizm mający na celu poprawę wydajności początkowej fazy połączenia TCP, zmniejszając ryzyko przeciążeń w sieci i unikając przedwczesnego przekroczenia limitu przepustowości w trakcie ustanawiania połączenia.
- **RACK (Recent Acknowledgment):** System powinien obsługiwać TCP RACK, co pozwala na szybsze wykrywanie utraty pakietów oraz optymalizację retransmisji w połączeniach TCP, redukując opóźnienia i zwiększając przepustowość.
- **Poprawa wydajności w sieciach o dużych opóźnieniach:** HyStart++ i RACK powinny minimalizować negatywne skutki opóźnień sieciowych oraz poprawiać wydajność połączeń TCP w sieciach rozległych i o dużym obciążeniu.
- **Integracja z istniejącymi protokołami:** Te mechanizmy muszą być kompatybilne z istniejącymi protokołami TCP oraz działające w środowiskach sieciowych zarówno lokalnych, jak i rozproszonych.

Cel:

Zwiększenie wydajności połączeń TCP, zwłaszcza w środowiskach o wysokim opóźnieniu i dużym ruchu, poprzez zastosowanie nowoczesnych mechanizmów kontroli przepustowości i optymalizacji retransmisji, takich jak TCP HyStart++ i RACK.

Tytuł wymagania: WDC.34.2024 - Ulepszone Receive Segment Coalescing (RSC) dla wirtualnych przełączników Hyper-V

Opis wymagania:

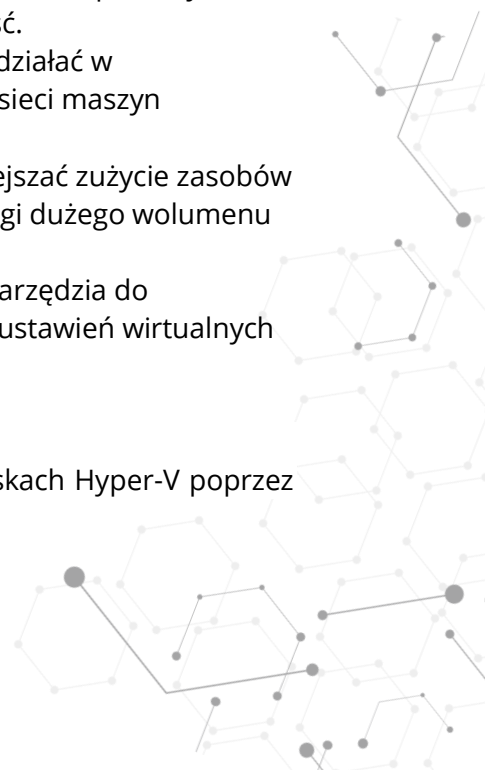
System operacyjny musi obsługiwać ulepszone mechanizmy Receive Segment Coalescing (RSC) w wirtualnych przełącznikach Hyper-V, co pozwala na efektywne grupowanie pakietów sieciowych i zmniejszenie obciążenia procesora, poprawiając wydajność wirtualnych sieci.

Kluczowe aspekty:

- **Receive Segment Coalescing (RSC):** System powinien umożliwiać RSC w wirtualnych przełącznikach Hyper-V, co pozwala na grupowanie wielu przychodzących segmentów TCP w jeden większy pakiet, zanim zostaną przetworzone przez system, co zmniejsza liczbę przerw procesora i poprawia efektywność.
- **Obsługa w wirtualnych środowiskach:** Ulepszone RSC musi działać w środowiskach wirtualnych, minimalizując wpływ na wydajność sieci maszyn wirtualnych oraz poprawiając przepustowość i skalowalność.
- **Redukcja zużycia zasobów:** Funkcja RSC musi znacząco zmniejszać zużycie zasobów procesora w środowiskach Hyper-V, szczególnie podczas obsługi dużego wolumenu ruchu sieciowego.
- **Zarządzanie i monitorowanie:** System powinien zapewniać narzędzia do monitorowania wydajności RSC oraz możliwość dostosowania ustawień wirtualnych przełączników, aby optymalizować ruch sieciowy.

Cel:

Poprawa wydajności sieci i zmniejszenie zużycia zasobów w środowiskach Hyper-V poprzez



Nr sprawy: BF-IV.2370.26.2024

Załącznik nr 1 do SWZ/ nr 1 do umowy

ulepszenie mechanizmu Receive Segment Coalescing (RSC), co zwiększa efektywność obsługi pakietów sieciowych w wirtualnych przełącznikach.

Tytuł wymagania: WDC.35.2024 - System Insights z wykrywaniem anomalii dysków

Opis wymagania:

System operacyjny musi zapewniać wsparcie dla narzędzia System Insights z funkcjonalnością wykrywania anomalii w pracy dysków, umożliwiając przewidywanie awarii, monitorowanie stanu dysków i poprawę zarządzania infrastrukturą pamięci masowej.

Kluczowe aspekty:

- **Wykrywanie anomalii:** System Insights musi posiadać funkcje wykrywania anomalii w pracy dysków, takie jak nietypowe zmiany w wydajności, zużycie pamięci masowej oraz nieprawidłowości w czasie dostępu do danych, co pozwala na wczesne wykrywanie problemów.
- **Predykcyjne analizy:** Narzędzie musi wykorzystywać analizy predykcyjne oparte na danych historycznych, aby przewidywać awarie dysków i informować administratorów o potencjalnych zagrożeniach dla infrastruktury.
- **Integracja z zarządzaniem zasobami:** System Insights musi być w pełni zintegrowany z narzędziami do zarządzania zasobami pamięci masowej, pozwalając na zautomatyzowaną konserwację, tworzenie kopii zapasowych oraz optymalizację alokacji zasobów.
- **Raportowanie i alerty:** Funkcja wykrywania anomalii musi oferować raporty oraz alerty w czasie rzeczywistym, które umożliwiają administratorom szybkie podejmowanie działań naprawczych.

Cel:

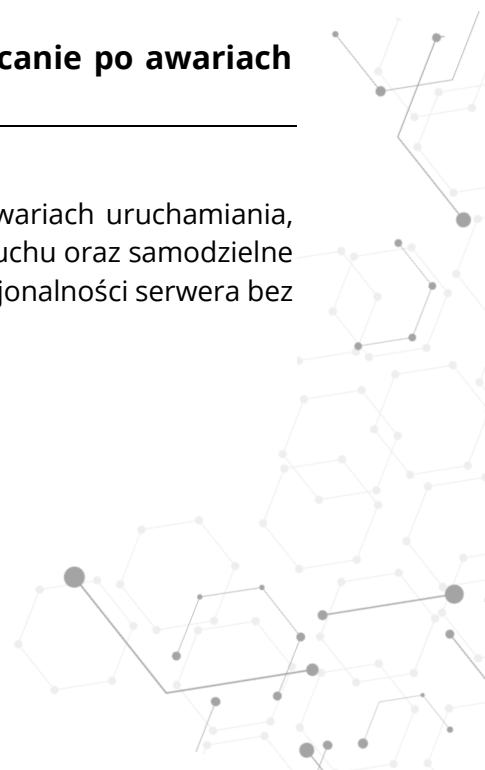
Poprawa niezawodności i wydajności infrastruktury pamięci masowej poprzez wprowadzenie funkcji wykrywania anomalii dysków w System Insights, co umożliwia przewidywanie awarii oraz szybką reakcję na potencjalne problemy związane z dyskami.

Tytuł wymagania: WDC.36.2024 - Automatyczne przywracanie po awariach uruchamiania

Opis wymagania:

System operacyjny musi wspierać automatyczne przywracanie po awariach uruchamiania, umożliwiając diagnozowanie problemów związanych z procesem rozruchu oraz samodzielne podejmowanie działań naprawczych w celu przywrócenia pełnej funkcjonalności serwera bez interwencji administratora.

Kluczowe aspekty:



Nr sprawy: BF-IV.2370.26.2024

Załącznik nr 1 do SWZ/ nr 1 do umowy

- **Automatyczna diagnostyka:** System powinien automatycznie wykrywać i diagnozować problemy podczas procesu rozruchu, takie jak uszkodzone pliki rozruchowe, błędy konfiguracji systemu czy uszkodzone sterowniki.
- **Samodzielna naprawa:** System musi posiadać mechanizmy automatycznej naprawy, które próbują przywrócić pliki systemowe, zresetować konfigurację lub naprawić błędy, które uniemożliwiają uruchomienie systemu.
- **Opcje odzyskiwania:** W przypadku braku możliwości naprawy, system powinien automatycznie uruchamiać tryb odzyskiwania, umożliwiając administratorowi ręczne rozwiązanie problemu lub przywrócenie systemu do wcześniejszego punktu przywracania.
- **Monitorowanie i powiadomienia:** System powinien oferować narzędzia monitorowania procesu rozruchu i wysłać powiadomienia do administratorów w przypadku, gdy automatyczne przywracanie nie jest skuteczne.

Cel:

Zwiększenie niezawodności serwera poprzez automatyczne przywracanie po awariach uruchamiania, co minimalizuje przestoje i zapewnia szybkie odzyskiwanie pełnej funkcjonalności systemu.

Tytuł wymagania: WDC.37.2024 - Storage Migration Service z rozszerzonymi możliwościami

Opis wymagania:

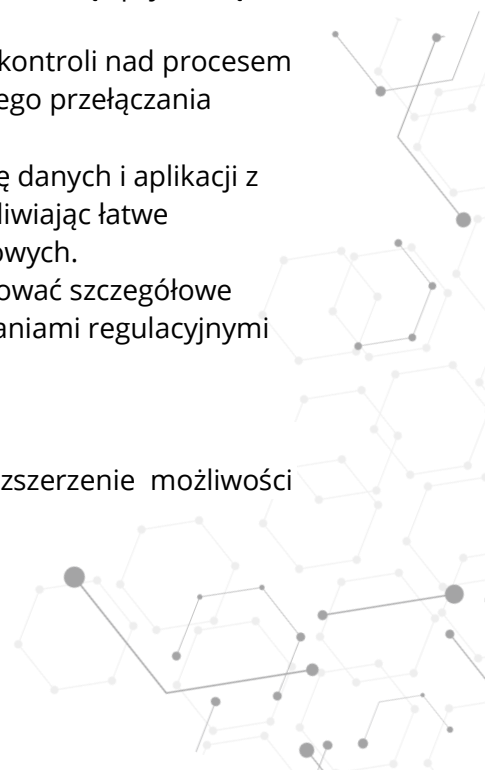
System operacyjny musi oferować rozszerzone funkcje w Storage Migration Service, które umożliwiają łatwiejszą i bardziej wszechstronną migrację danych, serwerów i systemów plików z lokalnych, chmurowych oraz hybrydowych środowisk, zapewniając większą elastyczność i kontrolę nad procesem migracji.

Kluczowe aspekty:

- **Migracja między środowiskami:** System musi umożliwiać migrację danych między różnymi środowiskami, w tym lokalnymi serwerami, chmurą publiczną i prywatną, z minimalnym przestojem i bez utraty danych.
- **Zarządzanie migracją:** Umożliwienie administratorom pełnej kontroli nad procesem migracji, w tym planowania, monitorowania oraz automatycznego przełączania zasobów, aby zminimalizować zakłócenia w działaniu.
- **Obsługa starszych systemów:** System musi wspierać migrację danych i aplikacji z starszych wersji serwerów oraz systemów operacyjnych, umożliwiając łatwe przeniesienie zasobów do nowszych wersji i środowisk chmurowych.
- **Raportowanie i zgodność:** Rozszerzone funkcje powinny oferować szczegółowe raporty dotyczące procesu migracji, w tym zgodności z wymaganiami regulacyjnymi oraz kontrolę nad integralnością przenoszonych danych.

Cel:

Zwiększenie elastyczności i wydajności migracji danych poprzez rozszerzenie możliwości



Nr sprawy: BF-IV.2370.26.2024

Załącznik nr 1 do SWZ/ nr 1 do umowy

Storage Migration Service, co ułatwia przenoszenie zasobów między różnymi środowiskami i zwiększa kontrolę nad całym procesem migracji.

Tytuł wymagania: WDC.38.2024 - Regulowana prędkość naprawy pamięci masowej

Opis wymagania:

System operacyjny musi obsługiwać funkcję regulowanej prędkości naprawy pamięci masowej, umożliwiając dynamiczne dostosowywanie prędkości procesów naprawczych, takich jak odbudowa lub synchronizacja danych, w zależności od obciążenia serwera i wymagań operacyjnych.

Kluczowe aspekty:

- **Regulacja prędkości naprawy:** System musi umożliwiać administratorom regulowanie prędkości procesów naprawczych, takich jak odbudowa RAID, synchronizacja danych czy naprawa wolumenów, w celu optymalizacji wydajności serwera i minimalizacji zakłóceń.
- **Automatyczne dostosowanie:** System powinien automatycznie dostosowywać prędkość naprawy w zależności od aktualnego obciążenia serwera, aby zapewnić równowagę między wydajnością operacyjną a czasem naprawy.
- **Minimalizacja wpływu na aplikacje:** Funkcja powinna minimalizować wpływ naprawy pamięci masowej na działające aplikacje i usługi, pozwalając na elastyczne zarządzanie zasobami podczas krytycznych operacji naprawczych.
- **Monitorowanie i zarządzanie:** System musi oferować narzędzia do monitorowania prędkości naprawy oraz możliwość ręcznego lub automatycznego dostosowania tych parametrów w zależności od priorytetów operacyjnych.

Cel:

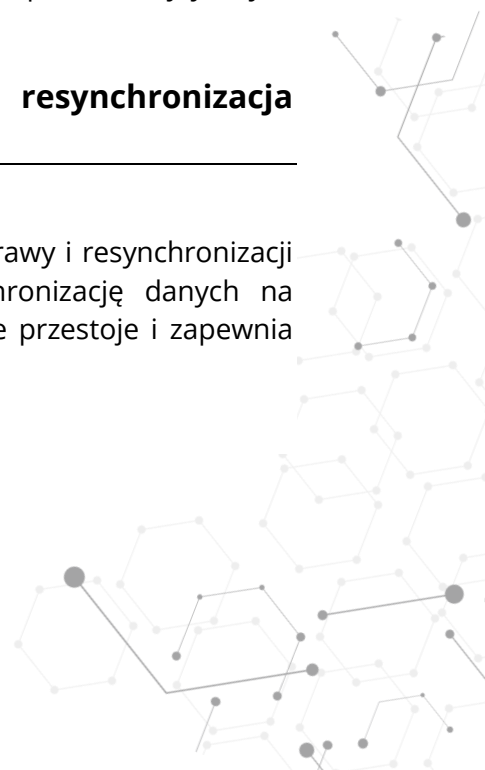
Zoptymalizowanie procesów naprawczych pamięci masowej poprzez wprowadzenie możliwości regulacji prędkości naprawy, co zwiększa elastyczność zarządzania zasobami pamięci masowej i minimalizuje negatywny wpływ na działanie systemu podczas krytycznych operacji naprawczych.

Tytuł wymagania: WDC.39.2024 - Szybsza naprawa i resynchronizacja pamięci masowej

Opis wymagania:

System operacyjny musi zapewniać wsparcie dla przyspieszonej naprawy i resynchronizacji pamięci masowej, umożliwiając szybsze odbudowywanie i synchronizację danych na wolumenach po awarii lub w przypadku uszkodzeń, co minimalizuje przestoje i zapewnia ciągłość działania.

Kluczowe aspekty:



Nr sprawy: BF-IV.2370.26.2024

Załącznik nr 1 do SWZ/ nr 1 do umowy

- **Przyspieszona resynchronizacja:** System musi obsługiwać mechanizmy optymalizujące proces resynchronizacji danych po awarii dysku lub uszkodzeniu wolumenu, skracając czas przywracania danych i poprawiając dostępność systemu.
- **Minimalizacja wpływu na wydajność:** Funkcja naprawy i resynchronizacji powinna być zaprojektowana w taki sposób, aby minimalizować wpływ na bieżące operacje i wydajność serwera, umożliwiając dalsze działanie aplikacji podczas procesu naprawy.
- **Zarządzanie priorytetami naprawy:** System musi pozwalać na dynamiczne dostosowanie priorytetów naprawy w zależności od potrzeb operacyjnych, umożliwiając elastyczne zarządzanie obciążeniami podczas napraw.
- **Zintegrowane monitorowanie:** System powinien oferować narzędzia do monitorowania postępu naprawy i resynchronizacji, dostarczając administratorom informacje w czasie rzeczywistym na temat stanu danych i operacji.

Cel:

Zapewnienie szybszego przywracania danych i minimalizacji przestoju poprzez usprawnienie procesów naprawy i resynchronizacji pamięci masowej, co zwiększa dostępność usług i bezpieczeństwo danych.

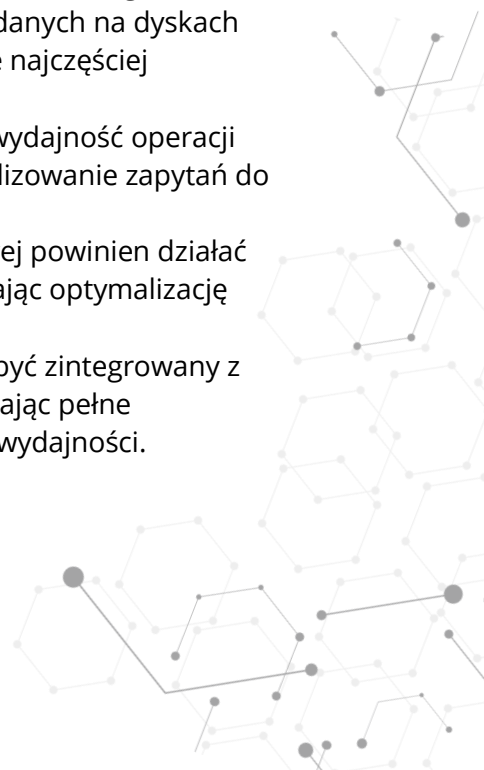
Tytuł wymagania: WDC.40.2024 - Storage bus cache dla autonomicznych serwerów

Opis wymagania:

System operacyjny musi obsługiwać funkcję cache magistrali pamięci masowej (Storage bus cache) dla autonomicznych serwerów, umożliwiając efektywną lokalną pamięć podręczną dla operacji I/O, co poprawia wydajność systemu i skraca czas dostępu do danych.

Kluczowe aspekty:

- **Lokalna pamięć podręczna:** System musi zapewniać obsługę cache magistrali pamięci masowej, który przyspiesza operacje odczytu i zapisu danych na dyskach lokalnych autonomicznych serwerów poprzez przechowywanie najczęściej używanych danych w pamięci podręcznej.
- **Zwiększenie wydajności I/O:** Funkcja cache musi poprawiać wydajność operacji wejścia/wyjścia (I/O) poprzez zredukowanie opóźnień i minimalizowanie zapytań do wolniejszej pamięci masowej.
- **Autonomiczne zarządzanie:** Cache magistrali pamięci masowej powinien działać autonomicznie, bez potrzeby stałego monitorowania, zapewniając optymalizację działania serwera niezależnie od jego konfiguracji i obciążeń.
- **Integracja z technologiami pamięci masowej:** System musi być zintegrowany z innymi technologiami zarządzania pamięcią masową, umożliwiając pełne wykorzystanie pamięci podręcznej w środowiskach o wysokiej wydajności.



Nr sprawy: BF-IV.2370.26.2024
 Załącznik nr 1 do SWZ/ nr 1 do umowy

Cel:

Zwiększenie wydajności operacji I/O w autonomicznych serwerach poprzez wykorzystanie cache magistrali pamięci masowej, co pozwala na szybszy dostęp do danych i poprawia ogólną wydajność systemu.

Tytuł wymagania: WDC.41.2024 - ReFS snapshoty na poziomie plików

Opis wymagania:

System operacyjny musi obsługiwać snapshoty na poziomie plików dla systemu plików ReFS (Resilient File System), umożliwiając administratorom tworzenie migawkowych kopii pojedynczych plików oraz ich szybkie przywracanie w przypadku utraty danych lub błędów.

Kluczowe aspekty:

- **Snapshoty plików:** System musi wspierać tworzenie snapshotów (migawek) pojedynczych plików w systemie plików ReFS, umożliwiając szybkie przywracanie poprzednich wersji plików bez konieczności przywracania całych wolumenów.
- **Efektywne zarządzanie przestrzenią:** Tworzenie snapshotów plików powinno być zoptymalizowane pod kątem minimalizacji wykorzystania przestrzeni dyskowej, korzystając z mechanizmów różnicowego przechowywania danych.
- **Szybkie przywracanie:** System musi umożliwiać administratorom szybkie przywracanie plików z wcześniej utworzonych snapshotów, co jest kluczowe w sytuacjach awaryjnych, takich jak uszkodzenie lub przypadkowe usunięcie plików.
- **Integracja z narzędziami zarządzania danymi:** Snapshoty na poziomie plików powinny być zintegrowane z innymi narzędziami do zarządzania danymi, takimi jak backupy i archiwizacja, aby ułatwić kompleksowe zarządzanie danymi.

Cel:

Zwiększenie elastyczności zarządzania danymi i szybkie odzyskiwanie plików w systemie plików ReFS poprzez wsparcie dla migawek na poziomie plików, co minimalizuje ryzyko utraty danych i przyspiesza operacje odzyskiwania.

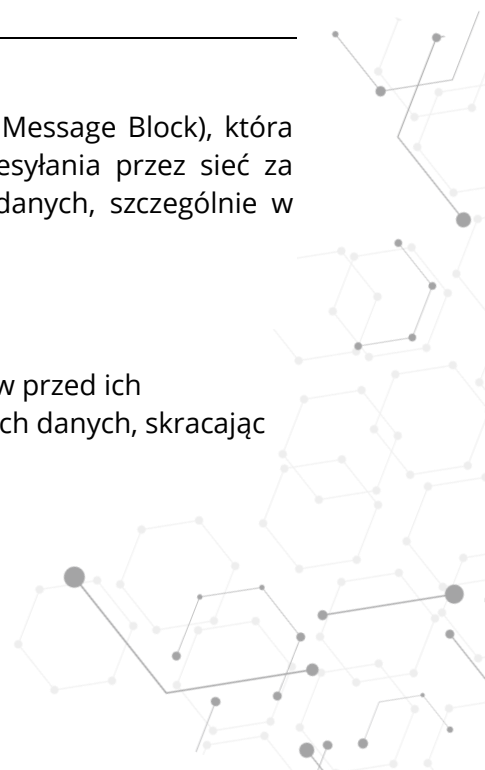
Tytuł wymagania: WDC.42.2024 - SMB kompresja

Opis wymagania:

System operacyjny musi obsługiwać funkcję kompresji SMB (Server Message Block), która pozwala na automatyczne kompresowanie plików podczas ich przesyłania przez sieć za pomocą protokołu SMB. Funkcja ta poprawia wydajność przesyłu danych, szczególnie w środowiskach o ograniczonej przepustowości sieci.

Kluczowe aspekty:

- **Kompresja danych:** System musi umożliwiać kompresję plików przed ich przesłaniem przez protokół SMB, co zmniejsza ilość przesyłanych danych, skracając czas transferu i zmniejszając obciążenie sieci.



Nr sprawy: BF-IV.2370.26.2024

Załącznik nr 1 do SWZ/ nr 1 do umowy

- **Automatyczna kompresja:** Kompresja powinna działać automatycznie w zależności od wielkości plików i dostępnej przepustowości, minimalizując ręczną interwencję administratora.
- **Redukcja zużycia zasobów:** System powinien być zoptymalizowany tak, aby kompresja SMB nie obciążała nadmiernie procesora ani pamięci, zapewniając zrównoważoną wydajność zarówno podczas przesyłu danych, jak i kompresji.
- **Kompatybilność:** Funkcja SMB kompresji musi być kompatybilna z różnymi wersjami SMB i zintegrowana z istniejącymi narzędziami do zarządzania i monitorowania ruchu sieciowego.

Cel:

Zwiększenie efektywności przesyłu danych poprzez zmniejszenie wielkości plików przesyłanych za pomocą protokołu SMB, co pozwala na szybszy transfer w sieciach o ograniczonej przepustowości i redukcję obciążenia sieciowego.

Tytuł wymagania: WDC.43.2024 - Dłuższy cykl wsparcia dla wszystkich obrazów kontenerów Windows

Opis wymagania:

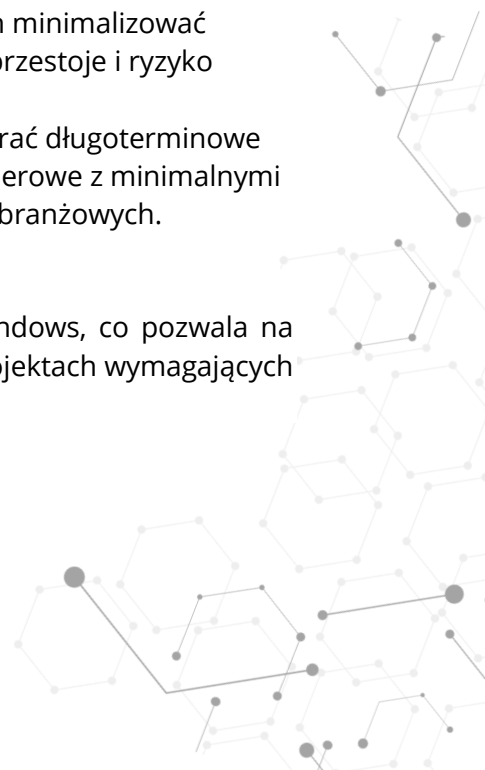
System operacyjny musi zapewniać wydłużony cykl wsparcia dla obrazów kontenerów Windows, umożliwiając użytkownikom korzystanie z aktualnych i bezpiecznych wersji obrazów przez dłuższy czas, co ułatwia zarządzanie kontenerami w długoterminowych projektach i wdrożeniach.

Kluczowe aspekty:

- **Wydłużone wsparcie:** System musi oferować dłuższy cykl wsparcia dla wszystkich oficjalnych obrazów kontenerów Windows, zapewniając dostępność aktualizacji bezpieczeństwa, poprawek i nowych funkcji przez okres dłuższy niż standardowy.
- **Bezpieczeństwo i stabilność:** Wydłużone wsparcie powinno obejmować regularne aktualizacje zabezpieczeń i poprawek, aby zapewnić stabilność i bezpieczeństwo kontenerów używanych w środowiskach produkcyjnych.
- **Minimalizacja przestoju:** Wydłużony cykl wsparcia powinien minimalizować potrzebę częstych migracji do nowych obrazów, co zmniejsza przestoje i ryzyko związane z niekompatybilnością.
- **Dostosowanie do cyklu życia projektów:** System musi wspierać długoterminowe projekty, w których wymagane jest stabilne środowisko kontenerowe z minimalnymi zmianami, dostosowując wsparcie do specyficznych wymagań branżowych.

Cel:

Zapewnienie dłuższego cyklu wsparcia dla obrazów kontenerów Windows, co pozwala na bezpieczne i stabilne zarządzanie środowiskami kontenerowymi w projektach wymagających długoterminowego utrzymania.



Nr sprawy: BF-IV.2370.26.2024

Załącznik nr 1 do SWZ/ nr 1 do umowy

Tytuł wymagania: WDC.44.2024 - Wirtualizowana strefa czasowa dla kontenerów

Opis wymagania:

System operacyjny musi obsługiwać funkcję wirtualizowanej strefy czasowej dla kontenerów, co umożliwi ustawienie różnych stref czasowych dla poszczególnych kontenerów, niezależnie od ustawień hosta. Funkcja ta jest kluczowa dla aplikacji uruchamianych w środowiskach globalnych, które muszą pracować w różnych strefach czasowych.

Kluczowe aspekty:

- **Oddzielne strefy czasowe:** System musi umożliwiać przypisywanie indywidualnych stref czasowych dla każdego kontenera, co pozwala na uruchamianie aplikacji w różnych strefach bez wpływu na czas systemowy hosta.
- **Zgodność z aplikacjami:** Wirtualizowana strefa czasowa powinna być w pełni kompatybilna z aplikacjami działającymi w kontenerach, w tym systemami, które polegają na dokładnym czasie do zarządzania danymi i transakcjami.
- **Dynamiczne zmiany:** Administratorzy powinni mieć możliwość dynamicznej zmiany strefy czasowej w kontenerze bez konieczności jego restartowania, co zwiększa elastyczność zarządzania środowiskiem.
- **Brak wpływu na hosta:** Zmiany w strefie czasowej kontenerów nie powinny wpływać na strefę czasową hosta ani innych kontenerów, zapewniając pełną izolację i niezależność.

Cel:

Umożliwienie precyzyjnego zarządzania strefami czasowymi w kontenerach, co jest kluczowe dla aplikacji działających w środowiskach globalnych, wymagających pracy w różnych strefach czasowych bez wpływu na system hosta.

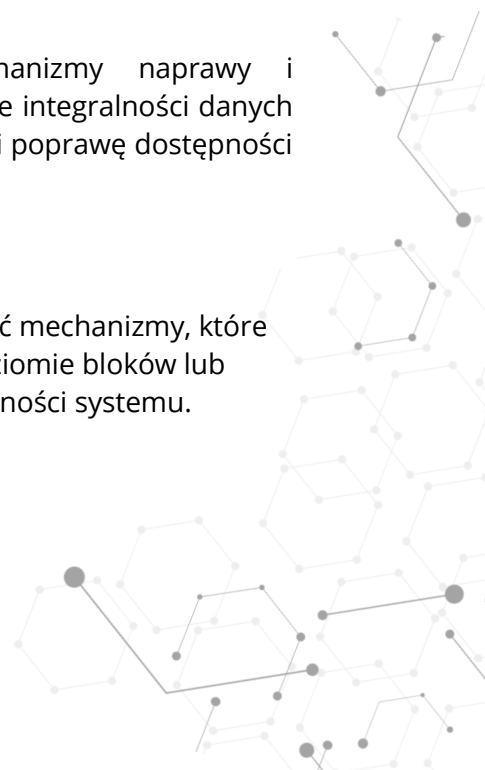
Tytuł wymagania: WDC.45.2024 - Szybsza naprawa i resynchronizacja pamięci masowej

Opis wymagania:

System operacyjny musi obsługiwać zoptymalizowane mechanizmy naprawy i resynchronizacji pamięci masowej, umożliwiając szybsze przywracanie integralności danych po awarii lub uszkodzeniu dysków, co zapewnia minimalne przestoje i poprawę dostępności usług.

Kluczowe aspekty:

- **Zoptymalizowana resynchronizacja:** System musi obsługiwać mechanizmy, które przyspieszają proces odbudowy i synchronizacji danych na poziomie bloków lub plików, skracając czas potrzebny do pełnego odzyskania sprawności systemu.



Nr sprawy: BF-IV.2370.26.2024

Załącznik nr 1 do SWZ/ nr 1 do umowy

- **Zarządzanie priorytetami naprawy:** System musi umożliwiać dynamiczne dostosowanie priorytetów naprawy i resynchronizacji w zależności od bieżącego obciążenia serwera i priorytetów operacyjnych.
- **Minimalizacja wpływu na wydajność:** Procesy naprawy powinny być zaprojektowane tak, aby minimalnie wpływały na wydajność innych operacji, pozwalając na normalne działanie aplikacji podczas naprawy danych.
- **Monitorowanie napraw:** System musi dostarczać narzędzia do monitorowania stanu napraw i resynchronizacji w czasie rzeczywistym, informując administratorów o postępach i potencjalnych problemach.

Cel:

Przyspieszenie procesów naprawy i resynchronizacji pamięci masowej, co zapewnia większą dostępność systemu i minimalizuje przestoje operacyjne po awariach lub uszkodzeniach danych.

Tytuł wymagania: WDC.46.2024 - Storage bus cache dla autonomicznych serwerów

Opis wymagania:

System operacyjny musi wspierać funkcję cache magistrali pamięci masowej (Storage bus cache) dla autonomicznych serwerów, co pozwala na zwiększenie wydajności operacji odczytu i zapisu poprzez lokalne buforowanie danych, przyspieszając dostęp do najczęściej używanych danych.

Kluczowe aspekty:

- **Lokalna pamięć podręczna:** System musi zapewniać wsparcie dla lokalnej pamięci cache, która magazynuje często używane dane na szybkim nośniku (np. SSD), co znacząco redukuje opóźnienia w dostępie do danych i zwiększa wydajność operacji I/O.
- **Optymalizacja dla autonomicznych serwerów:** Funkcja cache musi być zoptymalizowana dla serwerów działających w trybie autonomicznym, zapewniając im efektywną obsługę zadań bez stałej kontroli.
- **Automatyczne zarządzanie:** System powinien automatycznie zarządzać buforowaniem danych, dynamicznie przydzielając zasoby i adaptując się do zmieniających się obciążeń serwera, minimalizując potrzebę ręcznej interwencji.
- **Zintegrowane monitorowanie:** Storage bus cache musi być wyposażony w narzędzia do monitorowania, które pozwalają administratorom na śledzenie wydajności pamięci podręcznej i optymalizację działania serwera.

Cel:

Zwiększenie wydajności operacji I/O w autonomicznych serwerach poprzez efektywne wykorzystanie lokalnej pamięci podręcznej, co poprawia dostęp do danych i zmniejsza opóźnienia w obciążonych systemach.

Nr sprawy: BF-IV.2370.26.2024

Załącznik nr 1 do SWZ/ nr 1 do umowy

Tytuł wymagania: WDC.47.2024 - ReFS snapshoty na poziomie plików

Opis wymagania:

System operacyjny musi wspierać snapshoty (migawki) na poziomie plików w systemie plików ReFS (Resilient File System), umożliwiając szybkie tworzenie kopii zapasowych i przywracanie danych na poziomie poszczególnych plików, co poprawia zarządzanie danymi i zwiększa bezpieczeństwo.

Kluczowe aspekty:

- **Migawki na poziomie plików:** System musi wspierać tworzenie migawek pojedynczych plików lub katalogów, pozwalając na łatwe odzyskiwanie poszczególnych danych bez konieczności odtwarzania całych wolumenów.
- **Efektywność przechowywania danych:** Migawki powinny być zoptymalizowane pod kątem przechowywania tylko zmian, co zmniejsza zużycie przestrzeni dyskowej, zachowując jednocześnie pełną możliwość przywracania.
- **Szybkie przywracanie:** System musi umożliwiać szybkie przywracanie plików z migawek w przypadku uszkodzeń, przypadkowego usunięcia lub zmian danych, minimalizując czas potrzebny na odzyskanie danych.
- **Zintegrowane zarządzanie:** Narzędzia do zarządzania snapshotami powinny być w pełni zintegrowane z systemem plików ReFS, umożliwiając łatwe zarządzanie migawkami i ich automatyzację.

Cel:

Zwiększenie elastyczności zarządzania danymi i bezpieczeństwa systemu plików poprzez wprowadzenie funkcji migawek na poziomie plików w systemie plików ReFS, co pozwala na szybkie i efektywne przywracanie danych.

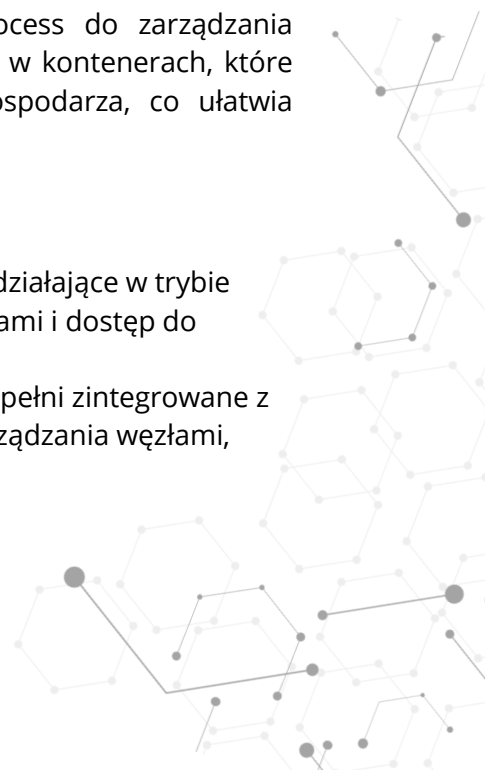
Tytuł wymagania: WDC.48.2024 - HostProcess kontenery do zarządzania węzłami

Opis wymagania:

System operacyjny musi wspierać używanie kontenerów HostProcess do zarządzania węzłami, co pozwala na uruchamianie aplikacji i usług systemowych w kontenerach, które mają bezpośredni dostęp do zasobów systemu operacyjnego gospodarza, co ułatwia zarządzanie i konfigurację węzłów w środowisku kontenerowym.

Kluczowe aspekty:

- **Kontenery HostProcess:** System musi obsługiwać kontenery działające w trybie HostProcess, który pozwala na bezpośrednie zarządzanie węzłami i dostęp do pełnych zasobów systemu operacyjnego.
- **Integracja z systemem:** Kontenery HostProcess muszą być w pełni zintegrowane z systemem operacyjnym, umożliwiając korzystanie z funkcji zarządzania węzłami, takich jak konfiguracja, monitorowanie i automatyzacja.



Nr sprawy: BF-IV.2370.26.2024

Załącznik nr 1 do SWZ/ nr 1 do umowy

- **Bezpośredni dostęp do zasobów:** Kontenery muszą mieć dostęp do zasobów systemu gospodarza, takich jak sieć i dyski, co pozwala na efektywne zarządzanie i operowanie węzłami.
- **Bezpieczeństwo i izolacja:** System powinien zapewniać odpowiednie mechanizmy izolacji i zabezpieczeń, aby kontenery HostProcess mogły działać bez wpływu na stabilność i bezpieczeństwo systemu gospodarza.

Cel:

Umożliwienie efektywnego zarządzania węzłami w środowisku kontenerowym poprzez wykorzystanie kontenerów HostProcess, które zapewniają pełen dostęp do zasobów systemu operacyjnego i wspierają zaawansowane funkcje zarządzania.

Tytuł wymagania: WDC.49.2024 - Azure Migrate App Containerization

Opis wymagania:

System operacyjny musi wspierać funkcję Azure Migrate App Containerization, która umożliwia migrację aplikacji do kontenerów oraz ich zarządzanie w chmurze Azure, zapewniając automatyzację i uproszczenie procesu konteneryzacji aplikacji.

Kluczowe aspekty:

- **Migracja aplikacji do kontenerów:** System musi wspierać narzędzia i mechanizmy umożliwiające migrację aplikacji do kontenerów, w tym automatyczne tworzenie i konfigurowanie obrazów kontenerów zgodnych z wymaganiami Azure.
- **Integracja z Azure:** Azure Migrate App Containerization musi być zintegrowana z platformą Azure, zapewniając łatwe przenoszenie i zarządzanie kontenerami w chmurze Azure.
- **Automatyzacja procesu:** System powinien oferować zautomatyzowane narzędzia do analizy aplikacji, tworzenia kontenerów i migracji, co zmniejsza czas i wysiłek związany z przenoszeniem aplikacji do chmury.
- **Wsparcie dla różnych aplikacji:** Funkcjonalność musi obsługiwać różne typy aplikacji, w tym aplikacje monolityczne i mikroserwisowe, zapewniając elastyczność i wsparcie dla szerokiego zakresu przypadków użycia.

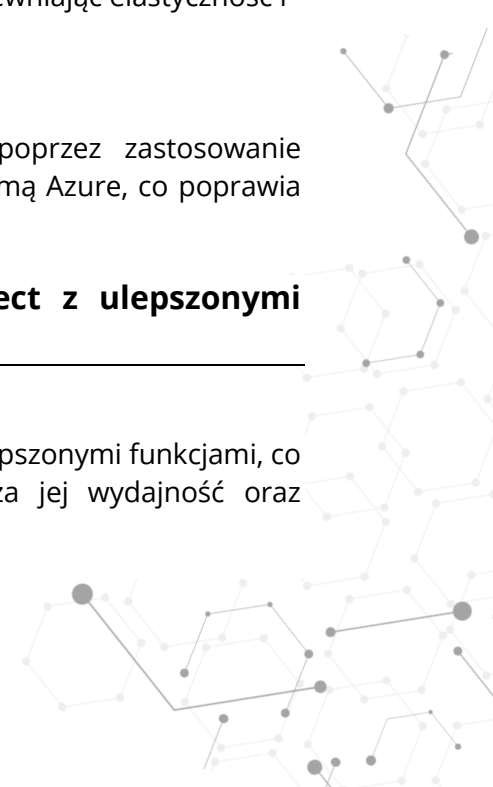
Cel:

Ułatwienie migracji aplikacji do kontenerów i chmury Azure poprzez zastosowanie zautomatyzowanych narzędzi do konteneryzacji i integracji z platformą Azure, co poprawia efektywność i zmniejsza ryzyko błędów w procesie migracji.

Tytuł wymagania: WDC.50.2024 - Storage Spaces Direct z ulepszonymi funkcjami

Opis wymagania:

System operacyjny musi obsługiwać Storage Spaces Direct (S2D) z ulepszonymi funkcjami, co zapewnia zaawansowane zarządzanie pamięcią masową, zwiększa jej wydajność oraz zapewnia lepsze możliwości skalowania i zarządzania danymi.



Nr sprawy: BF-IV.2370.26.2024
Załącznik nr 1 do SWZ/ nr 1 do umowy

Kluczowe aspekty:

- **Ulepszone funkcje zarządzania:** System powinien oferować nowe funkcje zarządzania pamięcią masową w ramach S2D, takie jak lepsze narzędzia do monitorowania, automatyzacji oraz optymalizacji.
- **Zwiększona wydajność:** Ulepszenia muszą obejmować poprawę wydajności operacji I/O, optymalizację ścieżek dostępu do danych oraz lepszą obsługę dużych wolumenów danych.
- **Lepsza skalowalność:** System powinien umożliwiać łatwe skalowanie pamięci masowej, zarówno w pionie, jak i w poziomie, z minimalnym wpływem na działanie systemu i dostępność danych.
- **Nowe mechanizmy ochrony:** Ulepszone funkcje muszą również obejmować zaawansowane mechanizmy ochrony danych, takie jak szyfrowanie, replikacja i odzyskiwanie po awariach.

Cel:

Poprawa funkcjonalności Storage Spaces Direct, co pozwala na bardziej efektywne zarządzanie pamięcią masową, zwiększa jej wydajność i skalowalność oraz poprawia bezpieczeństwo i dostępność danych.

