

Dotyczy: postępowanie o udzielenie zamówienia publicznego o nazwie:
„Zakup uzupełniający posiadanej infrastruktury obliczeniowej i symulacyjnej dla środowisk obliczeniowych” – numer postępowania: FH/02/04/24

OPIS PRZEDMIOTU ZAMÓWIENIA

Przedmiotem zamówienia jest zakup uzupełniający posiadanej infrastruktury obliczeniowej i symulacyjnej dla środowisk obliczeniowych. Zamówienie zostało podzielone na 3 części:

Część nr 1 - Oprogramowanie do kopii zapasowych maszyn wirtualnych na których realizowane są obliczenia

Wymagania ogólne

1. Oprogramowanie musi być produktem przeznaczonym do obsługi środowisk DataCenter. Oferowany produkt musi znajdować się w kwadracie liderów Gartner Magic Quadrant for Data Center Backup and Recovery Solutions oraz na ogólnie dostępnej liście referencyjnej Gartner: <https://www.gartner.com/reviews/market/data-center-backup-and-recovery-solutions> i spełniać minimalne wymagania : - minimalna liczba referencji 150, - minimalna ocena z referencji 4,5,
2. Oprogramowanie musi współpracować z infrastrukturą VMware w wersji 6.x, 7.x i 8.0 oraz Microsoft Hyper-V 2012, 2012R2, 2016, 2019 i 2022. Wszystkie funkcjonalności w specyfikacji muszą być dostępne na wszystkich wspieranych platformach wirtualizacyjnych, chyba, że wyszczególniono inaczej
3. Oprogramowanie musi zapewniać tworzenie kopii zapasowych z sieciowych urządzeń plikowych NAS opartych o SMB, CIFS i/lub NFS oraz bezpośrednio z serwerów plikowych opartych o Windows i Linux.

Całkowite koszty posiadania

1. Oprogramowanie musi być niezależne sprzętowo i umożliwiać wykorzystanie dowolnej platformy serwerowej i dyskowej
2. Oprogramowanie musi tworzyć „samowystarczalne” archiwa do odzyskania których nie wymagana jest osobna baza danych z metadanymi deduplikowanych bloków
3. Oprogramowanie musi mieć mechanizmy deduplikacji i kompresji w celu zmniejszenia wielkości archiwów. Włączenie tych mechanizmów nie może skutkować utratą jakichkolwiek funkcjonalności wymienionych w tej specyfikacji
4. Oprogramowanie nie może przechowywać danych o deduplikacji w centralnej bazie. Utrata bazy danych używanej przez oprogramowanie nie może prowadzić do utraty możliwości odtworzenia backupu. Metadane deduplikacji muszą być przechowywane w plikach backupu.
5. Oprogramowanie musi zapewniać warstwę abstrakcji nad poszczególnymi urządzeniami pamięci masowej, pozwalając utworzyć jedną wirtualną pulę pamięci na kopie zapasowe. Wymagane jest wsparcie dla nieograniczonej liczby pamięci masowych to takiej puli.
6. Oprogramowanie musi pozwalać na tworzenie repozytorium kopii zapasowych bezpośrednio na zasobach Microsoft Azure Blob, Google Cloud Storage, Amazon S3, Wasabi Cloud Storage oraz na innych kompatybilnych z S3 przestrzeniach obiektowych. Dodatkowo, oprogramowanie musi

wspierać archiwizowanie tych danych do Microsoft Azure Archive Blob Storage oraz Amazon S3 Glacier.

7. Oprogramowanie musi wspierać niezmiennosć kopii zapasowych na potrzeby ochrony przed ransomware poprzez niedopuszczenie do usunięcia lub modyfikacji kopii zapasowej w zadanym okresie czasu.
8. Oprogramowanie nie może instalować żadnych stałych agentów wymagających wdrożenia czy upgradowania wewnątrz maszyny wirtualnej dla jakichkolwiek funkcjonalności backupu lub odtwarzania
9. Oprogramowanie musi oferować portal samoobsługowy, umożliwiający odtwarzanie użytkownikom wirtualnych maszyn, obiektów MS Exchange i baz danych MS SQL, Oracle oraz PostgreSQL (w tym odtwarzanie point-in-time)
10. Oprogramowanie musi zapewniać możliwość delegacji uprawnień do odtwarzania na portalu
11. Oprogramowanie musi mieć możliwość integracji z innymi systemami poprzez wbudowane RESTful API
12. Oprogramowanie musi mieć wbudowane mechanizmy backupu konfiguracji w celu prostego odtworzenia systemu po całkowitej reinstalacji
13. Oprogramowanie musi mieć wbudowane mechanizmy szyfrowania zarówno plików z backupami jak i transmisji sieciowej. Włączenie szyfrowania nie może skutkować utratą jakiejkolwiek funkcjonalności wymienionej w tej specyfikacji
14. Oprogramowanie musi posiadać mechanizmy chroniące przed utratą hasła szyfrowania
15. Oprogramowanie musi posiadać architekturę klient/serwer z możliwością instalacji wielu instancji konsoli administracyjnych.
16. Oprogramowanie musi posiadać natywne mechanizmy uwierzytelniania wieloskładnikowego (MFA) w celu dostępu do konsoli administracyjnej

Wymagania RPO

1. Oprogramowanie musi wykorzystywać mechanizmy Change Block Tracking na wszystkich wspieranych platformach wirtualizacyjnych. Mechanizmy muszą być certyfikowane przez dostawcę platformy wirtualizacyjnej
2. Oprogramowanie musi wykorzystywać mechanizmy śledzenia zmienionych plików przy zabezpieczaniu udziałów plikowych.
3. Oprogramowanie musi oferować możliwość sterowania obciążeniem storage'u produkcyjnego tak aby nie przekraczane były skonfigurowane przez administratora backupu poziomy latencji. Funkcjonalność ta musi być dostępna na wszystkich wspieranych platformach wirtualizacyjnych z dokładnością do pojedynczego datastora
4. Oprogramowanie musi zapewniać tworzenie kopii zapasowych z bezpośrednim wykorzystaniem snapshotów macierzowych. Musi też zapewniać odtwarzanie maszyn wirtualnych z takich snapshotów. Proces wykonania kopii zapasowej nie może wymagać użycia jakichkolwiek hostów tymczasowych. Opisana funkcjonalność powinna działać w środowisku VMware.
5. Oprogramowanie musi posiadać wsparcie dla VMware vSAN potwierdzone odpowiednią certyfikacją VMware.
6. Oprogramowanie musi wspierać kopiowanie backupów oraz zasobów plikowych na taśmy.
7. Oprogramowanie musi mieć możliwość tworzenia retencji GFS (Grandfather-Father-Son)

8. Oprogramowanie musi wspierać bezpośrednią integrację z urządzeniami deduplikacyjnymi. Minimalnie wsparcie wymagane dla Dell DataDomain, HPE StoreOnce, ExaGrid, Fujitsu CS800, Quantum DXi oraz Infinidat InfiniGuard.
9. Oprogramowanie musi wspierać BlockClone API w przypadku użycia Windows Server 2016, 2019 lub 2022 z systemem pliku ReFS jako repozytorium backupu. Podobna funkcjonalność musi być zapewniona dla repozytoriów opartych o linuxowy system plików XFS.
10. Oprogramowanie musi mieć możliwość kopiowania backupów oraz replikacji wirtualnych maszyn z wykorzystaniem wbudowanej akceleracji WAN.
11. Oprogramowanie musi mieć możliwość replikacji asynchronicznej włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere pomiędzy hostami ESXi oraz pomiędzy hostami Hyper-V. Dodatkowo oprogramowanie musi mieć możliwość użycia plików kopii zapasowych jako źródła replikacji.
12. Oprogramowanie musi mieć możliwość replikacji ciągłej, opartej o VMware VAAI, włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere. Dla replikacji ciągłej musi być możliwość zdefiniowania dziennika pozwalającego na odzyskanie danych z dowolnego punktu w ramach ustalonego parametru RPO.
13. Oprogramowanie musi umożliwiać przechowywanie punktów przywracania dla replik
14. Oprogramowanie musi umożliwiać wykorzystanie istniejących w infrastrukturze wirtualnych maszyn jako źródła do dalszej replikacji (replica seeding)
15. Oprogramowanie musi wykorzystywać wszystkie oferowane przez hypervisor tryby transportu (sieć, hot-add, LAN Free-SAN)

Wymagania RTO

1. Oprogramowanie musi umożliwiać jednoczesne uruchomienie wielu maszyn wirtualnych bezpośrednio ze zdeduplikowanego i skompresowanego pliku backupu, z dowolnego punktu przywracania, bez potrzeby kopiowania jej na storage produkcyjny. Funkcjonalność musi być oferowana dla środowisk VMware, Hyper-V oraz Nutanix AHV niezależnie od rodzaju storage'u użytego do przechowywania kopii zapasowych.
2. Dodatkowo dla środowiska vSphere, Hyper-V i Nutanix AHV powyższa funkcjonalność powinna umożliwiać uruchomienie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna)
3. Oprogramowanie musi pozwalać na migrację on-line tak uruchomionych maszyn na storage produkcyjny. Migracja powinna odbywać się mechanizmami wbudowanymi w hypervisor. Jeżeli licencja na hypervisor nie posiada takich funkcjonalności - oprogramowanie musi realizować taką migrację swoimi mechanizmami
4. Oprogramowanie musi pozwalać na zaprezentowanie pojedynczego dysku bezpośrednio z kopii zapasowej do wybranej działającej maszyny wirtualnej vSphere
5. Oprogramowanie musi pozwalać na uruchomienie zasobów plikowych SMB oraz baz danych MS SQL i Oracle bezpośrednio ze skompresowanego i skompresowanego pliku backupu. Dodatkowo wspierana musi być migracja on-line tak uruchomionych zasobów na środowisko produkcyjne.
6. Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny, plików konfiguracji i dysków
7. Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny bezpośrednio do Microsoft Azure, Microsoft Azure Stack, Amazon EC2 oraz Google Cloud Platform.

8. Oprogramowanie musi umożliwić odtworzenie plików/folderów lub ich uprawnień na maszynie operatora, lub na serwer produkcyjny bez potrzeby użycia agenta instalowanego wewnątrz wirtualnej maszyny. Funkcjonalność ta nie powinna być ograniczona wielkością i liczbą przywracanych plików
9. Oprogramowanie musi mieć możliwość odtworzenia plików bezpośrednio do maszyny wirtualnej poprzez sieć, przy pomocy natywnego API dla platformy VMware i PowerShell Direct dla platformy Hyper-V.
10. Oprogramowanie musi wspierać odtwarzanie pojedynczych plików z systemów Windows, Linux, BSD, Solaris, Mac, Novell
11. Oprogramowanie musi wspierać przywracanie plików z partycji Linux LVM
12. Oprogramowanie musi umożliwiać szybkie granularne odtwarzanie obiektów aplikacji bez użycia jakiegokolwiek agenta zainstalowanego wewnątrz maszyny wirtualnej.
13. Oprogramowanie musi wspierać granularne odtwarzanie obiektów Active Directory takich jak konta komputerów, konta użytkowników, dowolnych atrybutów, rekordów DNS zintegrowanych z AD, Microsoft System Objects, certyfikatów CA, elementów AD Sites oraz pozwalać na odtworzenie haseł.
14. Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Exchange 2013SP1 i nowszych (dowolny obiekt w tym obiekty w folderze "Permanently Deleted Objects"). Odtwarzanie musi być możliwe bezpośrednio do środowiska produkcyjnego.
15. Oprogramowanie musi wspierać granularne odtwarzanie Microsoft SQL 2008 i nowszych. Odtwarzanie musi być możliwe bezpośrednio do środowiska produkcyjnego dla odzysku point-in-time, całych baz lub pojedynczych tabeli, widoków oraz procedur.
16. Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Sharepoint 2013 i nowszych. Odtwarzanie musi być możliwe bezpośrednio do środowiska produkcyjnego dla odzysku całych witryn, bibliotek oraz pojedynczych dokumentów wraz z historią ich wersji.
17. Oprogramowanie musi wspierać granularne odtwarzanie baz danych Oracle z opcją odtwarzanie point-in-time wraz z włączonym Oracle DataGuard. Funkcjonalność ta musi być dostępna dla baz uruchomionych w środowiskach Windows oraz Linux.
18. Oprogramowanie musi wspierać granularne odtwarzanie baz danych PostgreSQL z opcją odtwarzanie point-in-time. Funkcjonalność ta musi być dostępna dla baz uruchomionych w środowiskach Linux.
19. Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez Oracle RMAN
20. Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez SAP HANA, SAP Oracle
21. Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez MS SQL VDI
22. Oprogramowanie musi wspierać także specyficzne metody odtwarzania w tym "reverse CBT" oraz odtwarzanie z wykorzystaniem sieci SAN

Ograniczenie ryzyka

1. Oprogramowanie musi dawać możliwość stworzenia laboratorium (izolowane środowisko) dla vSphere i Hyper-V używając wirtualnych maszyn uruchamianych bezpośrednio z plików backupu. Powyższa funkcjonalność powinna umożliwiać uruchomienie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna)

2. Dla VMware'a oprogramowanie musi pozwalać na uruchomienie takiego środowiska dla replik maszyn wirtualnych oraz bezpośrednio ze snapshotów macierzowych stworzonych na wspieranych urządzeniach.
3. Oprogramowanie musi umożliwiać weryfikację odtwarzalności wielu wirtualnych maszyn jednocześnie z dowolnego backupu według własnego harmonogramu w izolowanym środowisku. Testy powinny uwzględniać możliwość uruchomienia dowolnego skryptu testującego również aplikację uruchomioną na wirtualnej maszynie. Testy muszą być przeprowadzone bez interakcji z administratorem
4. Oprogramowanie musi umożliwiać integrację z oprogramowaniem antywirusowym w celu wykonania skanu zawartości pliku backupowego przed odtworzeniem jakichkolwiek danych. Integracja musi być zapewniona minimalnie dla Windows Defender, Symantec Protection Engine oraz ESET NOD32.
5. Oprogramowanie musi umożliwiać dwuetapowe, automatyczne, odtwarzanie maszyn wirtualnych z możliwością wstrzyknięcia dowolnego skryptu przed odtworzeniem danych do środowiska produkcyjnego.

Środowiska fizyczne

1. Rozwiązanie musi wykonywać kopię zapasową systemu Windows oraz Linux wykorzystując agenta znajdującego się wewnątrz systemu operacyjnego
2. Rozwiązanie musi wspierać systemy operacyjne Windows w wersjach klienckich oraz serwerowych
3. Rozwiązanie musi wspierać co najmniej następujące dystrybucje systemów Linux: Debian, Ubuntu, RHEL, CentOS, Oracle Linux, SLES, Fedora, openSUSE
4. Rozwiązanie musi wspierać system operacyjny macOS
5. Oprogramowanie musi wspierać odtwarzanie pojedynczych plików z systemów Windows, Linux, MacOS, Unix
6. Rozwiązanie musi mieć możliwość instalacji oraz zarządzania wykorzystując tryb niezależny (per agent) jak również zcentralizowany (poprzez centralną konsolę zarządzającą)
7. Rozwiązanie musi wspierać systemy oparte o Microsoft Failover Cluster
8. Rozwiązanie musi wspierać zabezpieczanie do oraz odzyskiwanie z urządzeń blokowych pozwalając na odzysk całej maszyny (tzw. bare metal recovery) wybranych wolumenów, oraz wybranych plików i folderów
9. Rozwiązanie musi wspierać backup podłączonych dysków USB
10. Kopia zapasowa całej maszyny oraz pojedynczych wolumenów musi być wykonywana na poziomie blokowym
11. Rozwiązanie musi pozwalać na przechowywanie kopii zapasowych na zasobach lokalnych (wewnętrznych) dyskach zabezpieczanej maszyny, Direct Attached Storage (DAS), takich jak zewnętrzne dyski USB, eSATA lub Firewire, Network Attached Storage (NAS) pozwalającym na wystawienie swoich zasobów poprzez SMB (CIFS) lub NFS, bezpośrednio na zasobach obiektowych (w tym chmury)
12. Rozwiązanie musi wspierać deduplikację oraz kompresję na źródle. Dane wysyłane na repozytorium muszą być już odpowiednio przetworzone
13. Rozwiązanie musi wspierać kontrolę pasma sieciowego
14. Rozwiązanie musi wspierać ograniczenie wykonywania backupów dla konkretnych sieci bezprzewodowych

15. Rozwiązanie musi wspierać ograniczenia wykonywania backupów dla połączeń VPN
16. Rozwiązanie musi wspierać śledzenie zmienionych bloków podczas wykonywania kopii zapasowych. Dla systemów Windows technologia śledzenia bloków dla systemów serwerowych musi być certyfikowana przez Microsoft
17. Rozwiązanie musi wspierać technologię BitLocker
18. Rozwiązanie musi wspierać uruchamianie z nośnika odtwarzania
19. Rozwiązanie musi wspierać odzysk pojedynczych elementów aplikacji z jednorazowej kopii zapasowej dla Microsoft Exchange 2013SP1 i nowszych, Microsoft Active Directory 2008 i nowszych, Microsoft Sharepoint 2013 i nowszych, Microsoft SQL 2008 i nowszych, Oracle 11g i nowszych oraz PostgreSQL 12 i nowszych
20. Rozwiązanie musi wspierać odzysk do konkretnego punktu w czasie (point-in-time) dla wspieranych systemów bazodanowych
21. Rozwiązanie musi umożliwiać natychmiastowe publikowanie baz MS SQL i Oracle poprzez bezpośrednie uruchomienie ich z pliku backupu.
22. Rozwiązanie musi wspierać odzysk obrazów kopii zapasowych bezpośrednio do vSphere, Hyper-V, Nutanix AHV, Microsoft Azure, Microsoft Azure Stack, Amazon EC2 oraz Google Cloud Platform
23. Rozwiązanie musi wspierać szyfrowanie
24. Rozwiązanie musi wspierać możliwość wykonywania kopii zapasowych stacji klienckich, lokalnie do repozytorium tymczasowego (cache) gdy połączenie sieciowe do głównego repozytorium kopii zapasowych jest niedostępne
25. Rozwiązanie musi posiadać funkcjonalność automatycznego zmniejszenia szybkości przetwarzania danych, aby nie dopuścić do obniżenia wydajności systemu zabezpieczonego
26. Rozwiązanie musi posiadać ochronę przed ransomware poprzez automatyczne odmontowanie nośnika po wykonaniu backupu stacji klienckiej
27. Rozwiązanie musi wspierać tworzenie wielu zadań backupowych

Monitoring

1. System musi zapewnić możliwość monitorowania środowiska wirtualizacyjnego opartego na VMware vSphere i Microsoft Hyper-V bez potrzeby korzystania z narzędzi firm trzecich
2. System musi umożliwiać monitorowanie środowiska wirtualizacyjnego VMware w wersji 6.x, 7.x oraz 8.0 – zarówno w bezpłatnej wersji ESXi jak i w pełnej wersji ESX/ESXi zarządzane przez konsolę vCenter Server lub pracujące samodzielnie
3. System musi umożliwiać monitorowanie środowiska wirtualizacyjnego Microsoft Hyper-V 2012, 2012R2, 2016, 2019 oraz 2022 zarówno w wersji darmowej jak i zawartej w płatnej licencji Microsoft Windows Server zarządzane poprzez System Center Virtual Machine Manager lub pracujące samodzielnie.
4. System musi umożliwiać kategoryzację obiektów infrastruktury wirtualnej niezależnie od hierarchii stworzonej w vCenter
5. System musi umożliwiać tworzenie alarmów dla całych grup wirtualnych maszyn jak i pojedynczych wirtualnych maszyn
6. System musi dawać możliwość układania terminarza raportów i wysyłania tych raportów przy pomocy poczty elektronicznej w formacie HTML oraz Excel
7. System musi dawać możliwość podłączenia się do kilku instancji vCenter Server i serwerów Hyper-V jednocześnie, w celu centralnego monitorowania wielu środowisk

8. System musi mieć wbudowane predefiniowane zestawy alarmów wraz z możliwością tworzenia własnych alarmów i zdarzeń przez administratora
9. System musi mieć wbudowane połączenie z bazą wiedzy opisującą problemy z predefiniowanych alarmów
10. System musi mieć centralną konsolę z sumarycznym podglądem wszystkich obiektów infrastruktury wirtualnej (ang. Dashboard)
11. System musi mieć możliwość monitorowania platformy sprzętowej, na której jest zainstalowana infrastruktura wirtualna
12. System musi zapewnić możliwość podłączenia się do wirtualnej maszyny (tryb konsoli) bezpośrednio z narzędzia monitorującego
13. System musi mieć możliwość integracji z oprogramowaniem do tworzenia kopii zapasowych tego samego producenta
14. System musi mieć możliwość monitorowania obciążenia serwerów backupowych, ilości zabezpieczanych danych oraz statusu zadań kopii zapasowych, replikacji oraz weryfikacji odzyskiwalności maszyn wirtualnych.
15. System musi oferować inteligentną diagnostykę rozwiązania backupowego poprzez monitorowanie logów celem wykrycia znanych problemów oraz błędów konfiguracyjnych w celu wskazania rozwiązania bez potrzeby otwierania zgłoszenia suportowego oraz bez potrzeby wysyłania jakichkolwiek danych diagnostycznych do producenta oprogramowania backupu.
16. System musi mieć możliwość granularnego monitorowania infrastruktury, zależnego od uprawnień nadanych użytkownikom dla platformy VMware
17. System musi mieć możliwość monitorowania instancji VMware vCloud Director w wersji od 10.x do 10.4

Raportowanie

1. System musi umożliwiać raportowanie środowiska wirtualizacyjnego VMware w wersji 6.x, 7.x oraz 8.0 – zarówno w bezpłatnej wersji ESXi jak i w pełnej wersji ESX/ESXi zarządzane przez konsole vCenter Server lub pracujące samodzielnie
2. System musi umożliwiać raportowanie środowiska wirtualizacyjnego Microsoft Hyper-V 2012, 2012R2, 2016, 2019 oraz 2022 zarówno w wersji darmowej jak i zawartej w płatnej licencji Microsoft Windows Server zarządzane poprzez System Center Virtual Machine Manager lub pracujące samodzielnie.
3. System musi wspierać wiele instancji vCenter Server i Microsoft Hyper-V jednocześnie bez konieczności instalowania dodatkowych modułów.
4. System musi być systemem bezagentowym. Nie dopuszcza się możliwości instalowania przez system agentów na monitorowanych hostach ESXi i Hyper-V
5. System musi mieć możliwość eksportowania raportów do formatów Microsoft Word, Microsoft Excel, Microsoft Visio, Adobe PDF
6. System musi mieć możliwość ustawienia harmonogramu kolekcji danych z monitorowanych systemów jak również możliwość tworzenia zadań kolekcjonowania danych ad-hoc
7. System musi mieć możliwość ustawienia harmonogramu generowania raportów i dostarczania ich do odbiorców w określonych przez administratora interwałach
8. System w raportach musi mieć możliwość uwzględniania informacji o zmianach konfiguracji monitorowanych systemów

9. System musi mieć możliwość generowania raportów z dowolnego punktu w czasie zakładając, że informacje z tego czasu nie zostały usunięte z bazy danych
10. System musi posiadać predefiniowane szablony z możliwością tworzenia nowych jak i modyfikacji wbudowanych
11. System musi mieć możliwość analizowania „przeszacowanych” wirtualnych maszyn wraz z sugestią zmian w celu optymalnego wykorzystania fizycznej infrastruktury
12. System musi mieć możliwość generowania raportów na podstawie danych uzyskanych z oprogramowania do tworzenia kopii zapasowych tego samego producenta
13. System musi mieć możliwość generowania raportu dotyczącego zabezpieczanych maszyn, zdefiniowanych zadań tworzenia kopii zapasowych oraz replikacji jak również wykorzystania zasobów serwerów backupowych.
14. System musi mieć możliwość generowania raportu planowania pojemności (capacity planning) bazującego na scenariuszach 'what-if'.
15. System musi mieć możliwość granularnego raportowania infrastruktury, zależnego od uprawnień nadanym użytkownikom dla platformy VMware
16. System musi mieć możliwość generowania raportów dotyczących tzw. migawek-sierot (orphaned snapshots)
17. System musi mieć możliwość generowania personalizowanych raportów zawierających informacje z dowolnych predefiniowanych raportów w pojedynczym dokumencie

Część nr 2 - Półka dyskowa do macierzy

Opis sprzętu	Półka dyskowa do macierzy
Wewnętrzna pamięć masowa	1. Min 24 dyski SSD SAS do różnicowanego użycia z prędkością min 24Gbps o pojemności min 3,2TB
Kompatybilność	1. Półka dyskowa do macierzy ma być kompatybilna z posiadaną już przez Zamawiającego macierzą Dell PowerVault ME5
Ciągłość działania	1. Dyski mają umożliwić ich wymianę w trakcie działania
Kontroler dysków	Sprzętowy kontroler dyskowy, umożliwiający obsługę dysków z prędkościami transferu 3, 6, 12 Gb/s; umożliwiający skonfigurowanie na wewnętrznej pamięci dyskowej zabezpieczeń RAID: 0, 1, 5, 6, 10, 50, 60, wyposażony w wbudowaną, nieulotną pamięć cache o pojemności min. 4GB.
Zasilacze	Redundantne zasilacze Hot Plug wraz z kablami zasilającymi o dł.min. 2m każdy.
Gwarancja	1. Trzy lata gwarancji realizowanej w miejscu instalacji sprzętu, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii w trybie 24x7x365 poprzez ogólnopolską linię telefoniczną producenta. 2. Gwarancja zachowania własnego dysku przez 60mc 3. W przypadku awarii diagnostyka przeprowadzona przez pracownika autoryzowanego serwisu producenta w miejscu instalacji. 4. W przypadku awarii dyski twarde pozostają własnością Zamawiającego. 5. Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia, oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji serwera. 6. Firma serwisująca musi posiadać ISO 9001:2000 na świadczenie usług serwisowych oraz posiadać autoryzację producenta sprzętu – dokumenty potwierdzające załączyć do oferty. 7. Oświadczenie producenta sprzętu, że w przypadku niewywiązywania się z obowiązków gwarancyjnych oferenta lub firmy serwisującej, przejmie na siebie wszelkie zobowiązania związane z serwisem– dokumenty potwierdzające załączyć do oferty
Certyfikaty	1. sprzętu musi być wyprodukowany zgodnie z normą ISO-9001 oraz ISO-14001. Serwer musi posiadać deklaracja CE.
Dokumentacja	1. Zamawiający wymaga dokumentacji w języku polskim lub angielskim. 2. Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.
Inne wymagania:	1. Półka dyskowa po podpięciu do macierzy ma umożliwić, że z perspektywy macierzy przestrzeń dyskowa będzie możliwość zarządzania przestrzeni dyskową półki 2. Minimum jedna osoba realizujące dostawę posiadają certyfikat producenta potwierdzający kompetencje z zakresu doboru oferowanego rozwiązania

	<p>3. Wykonawca powinien posiadać status partnera Producenta sprzętu z zastrzeżeniem, że jeśli producent stosuje kilka poziomów partnerstwa, Zamawiający wymaga, aby wykonawca posiadał poziom partnerstwa nie niższy niż drugi poziom w kolejności licząc od najwyższego poziomu partnerstwa w hierarchii poziomów partnerstwa stosowanej przez Producenta. Zamawiający wyklucza, aby wyłącznie podwykonawca posiadał status, o którym mowa jest w zdaniu pierwszym.</p> <p>4. Należy dostarczyć również szyny montażowe do szafy typu rack dla oferowanej półki</p>
	24 miesięczny serwis dodatkowy Next Business Day OnSite

Część nr 3 - Rozbudowa pamięci RAM do serwerów

Przedmiotem zamówienia jest dostawa kości pamięci RAM do serwerów Dell R450, R650, R650xs i R7525

Oferowany sprzęt/produkt ma być fabrycznie nowy, nieużywany oraz nieekspozowany na wystawach lub imprezach targowych, sprawny technicznie, bezpieczny, kompletny i gotowy do pracy, a także musi spełniać wymagania techniczno-funkcjonalne wyszczególnione w opisie przedmiotu zamówienia.

1. Przedmiot zamówienia.

Przedmiotem zamówienia jest dostawa kości pamięci RAM na potrzebę rozbudowy serwerów Dell R450, R650, R650xs i R7525 posiadanych i użytkowanych przez Zamawiającego.

Zamówienie dotyczy tylko dostawy zamawianych elementów, bez usługi montażu. Instalacji wszystkich dostarczonych elementów zamówienia dokona samodzielnie pracownik Zamawiającego.

2. Specyfikacja serwerów które będą podlegały rozbudowanie.

Dostarczane pamięci RAM mają być kompatybilne z serwerami o następujących Service Tag:

- BJBYK3
- 28JTFR3
- 38JTFR3
- 17BXMS3
- J6BXMS
- 27BXMS3
- JHY52V3
- 739L4V3
- 639L4V3
- CJBYYK3
- 87JTFR3
- 97JTFR3
- 75890L3

3. Wymagania techniczne dla kości pamięci RAM do rozbudowy serwerów.

Lp. Wymagania:

1. Należy dostarczyć 70 kości o pojemności 32GB każda, typu 2Rx4 DDR4 RDIMM min. 3200MHz 8Gb Base
2. Należy dostarczyć 24 kości o pojemności 64GB każda, typu 2Rx4 DDR4 RDIMM min. 3200MHz

3. Kości pamięci muszą być:

- tego samego producenta co rozbudowywany serwer czyli firmy Dell z uwagi na konieczność zachowania aktywnej usługi wsparcia technicznego producenta serwerów.
- certyfikowane i dedykowane przez producenta do modelu konkretnego serwera podlegającego rozbudowie
- w pełni kompatybilne z kośćmi pamięci zainstalowanymi w serwerze

4. Rozbudowa nie może powodować konieczności jakiegokolwiek zmiany w konfiguracji sprzętowej serwera, montaż dostarczonych kości tylko w pozostałe, wolne sloty na płycie głównej bez konieczności relokacji kości zainstalowanych w serwerze.

5. Zamawiający samodzielnie dokona instalacji dostarczonych kości pamięci RAM w rozbudowywanych serwerach.
6. Na dostarczone kości pamięci wymagana minimum 12 miesięczna gwarancja producenta
7. Rozbudowywane serwery objęte są aktywną usługą wsparcia technicznego producenta, rozbudowa musi uwzględniać zachowanie aktualnej umowy serwisowej.