

Opis przedmiotu zamówienia

Dostawa i uruchomienie zunifikowanego rozwiązania do backup-u infrastruktury krytycznej (serwery/stacje robocze) dla Urzędu Miejskiego w Chrzanowie w ramach programu Cyfrowa Gmina

W ramach postępowania należy dostarczyć oraz wdrożyć:

- Oprogramowanie do backupu – 15 licencji na serwery (virtualne/fizyczne), 170 licencji dla stacji roboczych
- Serwer do backupu z przestrzenią do przechowywania min. 100TB – 1 szt
- biblioteka taśmowa z autoloaderem na 8 kaset LTO-8 – 1 szt

Parametry techniczne oprogramowania do backupu:

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 wymaganie : - minimalna liczba referencji 150, - minimalna ocena z referencji 4,5,

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

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.

Oprogramowanie musi być niezależne sprzętowo i umożliwiać wykorzystanie dowolnej platformy serwerowej i dyskowej

Oprogramowanie musi tworzyć "samowystarczalne" archiwa do odzyskania których nie wymagana jest osobna baza danych z metadanymi deduplikowanych bloków

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

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.

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.

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.

Oprogramowanie musi wspierać niezmienność kopii zapasowych na potrzeby ochrony przed ransomware poprzez niedopuszczenie do usunięcia lub modyfikacji kopii zapasowej w zadanym okresie czasu.

Oprogramowanie nie może instalować żadnych stałych agentów wymagających wdrożenia czy upgradowania wewnątrz maszyny wirtualnej dla jakichkolwiek funkcjonalności backupu lub odtwarzania

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)

Oprogramowanie musi zapewniać możliwość delegacji uprawnień do odtwarzania na portalu

Oprogramowanie musi mieć możliwość integracji z innymi systemami poprzez wbudowane RESTful API
Oprogramowanie musi mieć wbudowane mechanizmy backupu konfiguracji w celu prostego odtworzenia systemu po całkowitej reinstalacji

Oprogramowanie musi mieć wbudowane mechanizmy szyfrowania zarówno plików z backupami jak i transmisji sieciowej. Włączenie szyfrowania nie może skutkować utratą jakiegokolwiek funkcjonalności wymienionej w tej specyfikacji

Oprogramowanie musi posiadać mechanizmy chroniące przed utratą hasła szyfrowania

Oprogramowanie musi posiadać architekturę klient/serwer z możliwością instalacji wielu instancji konsoli administracyjnych.

Oprogramowanie musi posiadać natywne mechanizmy uwierzytelniania wieloskładnikowego (MFA) w celu dostępu do konsoli administracyjnej

Wymagania RPO:

Oprogramowanie musi wykorzystywać mechanizmy Change Block Tracking na wszystkich wspieranych platformach wirtualizacyjnych. Mechanizmy muszą być certyfikowane przez dostawcę platformy wirtualizacyjnej
Oprogramowanie musi wykorzystywać mechanizmy śledzenia zmienionych plików przy zabezpieczaniu udziałów plikowych.

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
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.

Oprogramowanie musi posiadać wsparcie dla VMware vSAN potwierdzone odpowiednią certyfikacją VMware.

Oprogramowanie musi wspierać kopiowanie backupów oraz zasobów plikowych na taśmy.

Oprogramowanie musi mieć możliwość tworzenia retencji GFS (Grandfather-Father-Son)

Oprogramowanie musi wspierać bezpośrednią integrację z urządzeniami deduplikacyjnymi. Minimalnie wsparcie wymagane dla Dell DataDomain, HPE StoreOnce, ExaGrid, Fujitsu CS800, Quantum DXi oraz Infinidat InfiniGuard.

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.

Oprogramowanie musi mieć możliwość kopiowania backupów oraz replikacji wirtualnych maszyn z wykorzystaniem wbudowanej akceleracji WAN.

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.

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.

Oprogramowanie musi umożliwiać przechowywanie punktów przywracania dla replik

Oprogramowanie musi umożliwiać wykorzystanie istniejących w infrastrukturze wirtualnych maszyn jako źródła do dalszej replikacji (replica seeding)

Oprogramowanie musi wykorzystywać wszystkie oferowane przez hypervisor tryby transportu (sieć, hot-add, LAN Free-SAN)

Wymagania RTO

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.

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)

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

Oprogramowanie musi pozwalać na zaprezentowanie pojedynczego dysku bezpośrednio z kopii zapasowej do wybranej działającej maszyny wirtualnej vSphere

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.

Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny, plików konfiguracji i dysków

Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny bezpośrednio do Microsoft Azure, Microsoft Azure Stack, Amazon EC2 oraz Google Cloud Platform.

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

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.

Oprogramowanie musi wspierać odtwarzanie pojedynczych plików z systemów Windows, Linux, BSD, Solaris, Mac, Novell

Oprogramowanie musi wspierać przywracanie plików z partycji Linux LVM

Oprogramowanie musi umożliwiać szybkie granularne odtwarzanie obiektów aplikacji bez użycia jakiegokolwiek agenta zainstalowanego wewnątrz maszyny wirtualnej.

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.

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.

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.

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.

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.

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.

Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez Oracle RMAN

Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez SAP HANA, SAP Oracle

Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez MS SQL VDI

Oprogramowanie musi wspierać także specyficzne metody odtwarzania w tym "reverse CBT" oraz odtwarzanie z wykorzystaniem sieci SAN

Ograniczenie ryzyka

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)

Dla VMware'a oprogramowanie musi pozwalać na uruchomienie takiego środowiska dla replik maszyn wirtualnych oraz bezpośrednio ze snapshotów macierzowych stworzonych na wspieranych urządzeniach.

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

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.

Oprogramowanie musi umożliwiać dwuetapowe, automatyczne, odtwarzanie maszyn wirtualnych z możliwością wstrzyknięcia dowolnego skryptu przed odtworzeniem danych do środowiska produkcyjnego.

Środowiska fizyczne

Rozwiązanie musi wykonywać kopię zapasową systemu Windows oraz Linux wykorzystując agenta znajdującego się wewnątrz systemu operacyjnego

Rozwiązanie musi wspierać systemy operacyjne Windows w wersjach klienckich oraz serwerowych

Rozwiązanie musi wspierać co najmniej następujące dystrybucje systemów Linux: Debian, Ubuntu, RHEL, CentOS, Oracle Linux, SLES, Fedora, openSUSE

Rozwiązanie musi wspierać system operacyjny macOS

Oprogramowanie musi wspierać odtwarzanie pojedynczych plików z systemów Windows, Linux, MacOS, Unix

Rozwiązanie musi mieć możliwość instalacji oraz zarządzania wykorzystując tryb niezależny (per agent) jak również zcentralizowany (poprzez centralną konsolę zarządzającą)

Rozwiązanie musi wspierać systemy oparte o Microsoft Failover Cluster

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

Rozwiązanie musi wspierać backup podłączonych dysków USB

Kopia zapasowa całej maszyny oraz pojedynczych wolumenów musi być wykonywana na poziomie blokowym

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)

Rozwiązanie musi wspierać deduplikacje oraz kompresję na źródle. Dane wysyłane na repozytorium muszą być już odpowiednio przetworzone

Rozwiązanie musi wspierać kontrolę pasma sieciowego

Rozwiązanie musi wspierać ograniczenie wykonywania backupów dla konkretnych sieci bezprzewodowych

Rozwiązanie musi wspierać ograniczenia wykonywania backupów dla połączeń VPN

Rozwiązanie musi wspierać śledzenie zmienionych bloków podczas wykonywania kopii zapasowych. Dla systemów Windows technologia śledzenia bloków dla systemów serwerowych musi być certyfikowana przez Microsoft

Rozwiązanie musi wspierać technologię BitLocker

Rozwiązanie musi wspierać uruchamianie z nośnika odtwarzania

Rozwiązanie musi wspierać odzysk pojedynczych elementów aplikacji z jednoprzebiegowej 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

Rozwiązanie musi wspierać odzysk do konkretnego punktu w czasie (point-in-time) dla wspieranych systemów bazodanowych

Rozwiązanie musi umożliwiać natychmiastowe publikowanie baz MS SQL i Oracle poprzez bezpośrednie uruchomienie ich z pliku backupu.

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

Rozwiązanie musi wspierać szyfrowanie

Rozwiązanie musi wspierać możliwość wykonywania kopii zapasowych stacji klienckich, lokalnie do repozytorium tymczasowego (cache) gdy połączenie sieciowe do głównego repozytorium kopii zapasowych jest niedostępne

Rozwiązanie musi posiadać funkcjonalność automatycznego zmniejszenia szybkości przetwarzania danych, aby nie dopuścić do obniżenia wydajności systemu zabezpieczanego

Rozwiązanie musi posiadać ochronę przed ransomware poprzez automatyczne odmontowanie nośnika po wykonanym backupie stacji klienckiej

Rozwiązanie musi wspierać tworzenie wielu zadań backupowych

Monitoring

System musi zapewnić możliwość monitorowania środowiska wirtualizacyjnego opartego na VMware vSphere i Microsoft Hyper-V bez potrzeby korzystania z narzędzi firm trzecich

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 konsole vCenter Server lub pracujące samodzielnie

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.

System musi umożliwiać kategoryzację obiektów infrastruktury wirtualnej niezależnie od hierarchii stworzonej w vCenter

System musi umożliwiać tworzenie alarmów dla całych grup wirtualnych maszyn jak i pojedynczych wirtualnych maszyn

System musi dawać możliwość układania terminarza raportów i wysyłania tych raportów przy pomocy poczty elektronicznej w formacie HTML oraz Excel

System musi dawać możliwość podłączenia się do kilku instancji vCenter Server i serwerów Hyper-V jednocześnie, w celu centralnego monitorowania wielu środowisk

System musi mieć wbudowane predefiniowane zestawy alarmów wraz z możliwością tworzenia własnych alarmów i zdarzeń przez administratora

System musi mieć wbudowane połączenie z bazą wiedzy opisującą problemy z predefiniowanych alarmów

System musi mieć centralną konsolę z sumarycznym podglądem wszystkich obiektów infrastruktury wirtualnej (ang. Dashboard)

System musi mieć możliwość monitorowania platformy sprzętowej, na której jest zainstalowana infrastruktura wirtualna

System musi zapewnić możliwość podłączenia się do wirtualnej maszyny (tryb konsoli) bezpośrednio z narzędzia monitorującego

System musi mieć możliwość integracji z oprogramowaniem do tworzenia kopii zapasowych tego samego producenta

System musi mieć możliwość monitorowania obciążenia serwerów backupowych, ilości zabezpieczanych danych oraz statusu zadań kopii zapasowych, replikacji oraz weryfikacji odzyskiwalności maszyn wirtualnych.

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.

System musi mieć możliwość granularnego monitorowania infrastruktury, zależnego od uprawnień nadanych użytkownikom dla platformy VMware

System musi mieć możliwość monitorowania instancji VMware vCloud Director w wersji od 10.x do 10.4

Raportowanie

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

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.

System musi wspierać wiele instancji vCenter Server i Microsoft Hyper-V jednocześnie bez konieczności instalowania dodatkowych modułów.

System musi być systemem bezagentowym. Nie dopuszcza się możliwości instalowania przez system agentów na monitorowanych hostach ESXi i Hyper-V

System musi mieć możliwość eksportowania raportów do formatów Microsoft Word, Microsoft Excel, Microsoft Visio, Adobe PDF

System musi mieć możliwość ustawienia harmonogramu kolekcji danych z monitorowanych systemów jak również możliwość tworzenia zadań kolekcjonowania danych ad-hoc

System musi mieć możliwość ustawienia harmonogramu generowania raportów i dostarczania ich do odbiorców w określonych przez administratora interwałach

System w raportach musi mieć możliwość uwzględniania informacji o zmianach konfiguracji monitorowanych systemów

System musi mieć możliwość generowania raportów z dowolnego punktu w czasie zakładając, że informacje z tego czasu nie zostały usunięte z bazy danych

System musi posiadać predefiniowane szablony z możliwością tworzenia nowych jak i modyfikacji wbudowanych

System musi mieć możliwość analizowania „przeszacowanych” wirtualnych maszyn wraz z sugestią zmian w celu optymalnego wykorzystania fizycznej infrastruktury

System musi mieć możliwość generowania raportów na podstawie danych uzyskanych z oprogramowania do tworzenia kopii zapasowych tego samego producenta

System musi mieć możliwość generowania raportu dotyczącego zabezpieczanych maszyn, zdefiniowanych zadań tworzenia kopii zapasowych oraz replikacji jak również wykorzystania zasobów serwerów backupowych.

System musi mieć możliwość generowania raportu planowania pojemności (capacity planning) bazującego na scenariuszach 'what-if'.

System musi mieć możliwość granularnego raportowania infrastruktury, zależnego od uprawnień nadanych użytkownikom dla platformy VMware

System musi mieć możliwość generowania raportów dotyczących tzw. migawek-sierot (orphaned snapshots)

System musi mieć możliwość generowania personalizowanych raportów zawierających informacje z dowolnych predefiniowanych raportów w pojedynczym dokumencie

Oferowane licencje mają być na czas nieokreślony (wieczyste) ze wsparciem technicznym na minimum 36 miesięcy.

Parametry techniczne serwera do backupu:

Serwer o obudowie typu RACK o wysokości maksymalnej 2U wyposażony w szyny umożliwiające jego całkowite wysunięcie bez rozłączania kabli. Wyposażony w dwa zasilacze o mocy, która wystarcza do pracy serwera tylko z jednym zasilaczem.

- jeden procesory w architekturze x64 przeznaczone dla serwerów, z 8 rdzeniami/16 wątkami, o częstotliwości bazowej przynajmniej 2.8GHz, a w trybie turbo 3.6GHz, z 12MB pamięci podręcznej,
- 32GB pamięci RAM ECC,
- zintegrowana karta graficzna o rozdzielczości min. 1280x1024 z wyjściem VGA (D-Sub 15),
- dwa interfejsy sieciowe RJ45 1Gbit Ethernet,
- dwa interfejsy sieciowe SFP+ wyposażone w transceiver-y światłowodowe 10Gbit Ethernet dla włókna OM4 [multi-mode],
- sprzętowy kontroler RAID z obsługą RAID: 0,1,5,6,10,50,60 i pamięcią kontrolera podtrzymywaną bateryjnie,
- 2 dyski twarde typu SATA SSD każdy o pojemności 480GB podłączone do kontrolera RAID,
- 12 dysków twardej typu SATA HDD każdy o pojemności 10TB i wszystkie podłączone do kontrolera RAID,
- sprzętowy kontroler SAS 12G z dwoma portami zewnętrznymi,

- system operacyjny Windows Serwer 2022 Standard z odpowiednią licencją na zainstalowane procesory [rdzenie] lub inny system operacyjny zgodny z zaproponowanym oprogramowaniem do backup-u
- wbudowany moduł TPM 2.0,
- serwer wyposażony w podwójny zasilacz typu hot-plug. Zasilacze dobrane w taki sposób, aby serwer mógł pracować z tylko jednym sprawnym.
- system zarządzania niezależny od zainstalowanego oprogramowania, zintegrowany z płytą główną posiadający własny port Ethernet.

Gwarancja na serwer:

Minimalnie 36 miesięcy gwarancji. Gwarancja producenta realizowana w miejscu instalacji sprzętu z określonym czasem reakcji od przyjęcia zgłoszenia wynoszącym następnym dzień roboczy. Możliwość telefonicznego i elektronicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta oraz poprzez stronę internetową producenta lub jego przedstawiciela. Dodatkowa opcja serwisowa gwarantująca, iż w przypadku awarii, uszkodzone dyski twarde pozostaną u użytkownika, a w ich miejsce zostaną dostarczone nowe.

Parametry techniczne biblioteki taśmowej:

Biblioteka taśmowa ze streamerem na 8 taśm LTO-8 w obudowie typu RACK o wysokości maksymalnej 2U.

- biblioteka taśmowa wyposażona a system automatycznej wymiany kaset
- ilość kaset w bibliotece: 8 szt
- biblioteka wyposażona w streamer na kasetki LTO-8 30TB z interfejsem SAS 12G

W ramach zamówienia należy dostarczyć:

- 12 kasetek LTO-8 o pojemności 30TB z kompletem naklejek (barcode) do ich identyfikacji w bibliotece
- 1 kasetką czyszcząca dedykowana do zastosowanego streamera
- kabel SAS do podłączenia do serwera o długości nie mniejszej niż 2m

Wymagany okres gwarancji: minimalnie 36 miesięcy

Instalacja i konfiguracja:

Serwer oraz bibliotekę taśmową należy dostarczyć do siedziby zamawiającego, zainstalować we wskazanej szafie RACK oraz dokonać pełnej integracji z zaproponowanym oprogramowaniem do backup-u danych.

W ramach integracji należy wykonać:

- konfiguracji biblioteki taśmowej do pracy automatycznej z oprogramowaniem do backup-u danych
- instalacja i konfiguracja agentów systemu backup-owego na serwerach fizycznych z zainstalowanym oprogramowaniem Microsoft Windows Serwer wersjach od 2012 do 2022 w ilości 11 szt

- instalacja i konfiguracja systemu backup-owego na serwerze Hyper-V w wersji Core z zainstalowanymi następującymi systemami operacyjnymi:

Oracle Linux 5.4.17 – 3 szt

CentOS Linux 4.18.0 – 1 szt

Wszystkie instalacje na serwerach wymagają opracowania procedur instalacji klientów i ich konfiguracji, które mają zostać udokumentowane – opis działania, warunki wykonalności, instrukcje „step-by-step”.

- instalacja i konfiguracja agentów systemu backup-owego na końcówkach użytkowników z zainstalowanym systemem operacyjnym Windows 10 lub 11. Agent skonfigurowany tak, aby wykonywać codzienną archiwizację danych profili użytkowników w zakresie:

- pulpit użytkownika
- folder Dokumenty
- Ulubione
- pozostałe dane konieczne do odtworzenia profilu
- opcjonalnie folder: Application Data

Dane mają być wysyłane na nie zamapowany zasób sieciowy.

Do instalacji na końcówkach użytkowników można wykorzystać GPO – wszystkie komputery są podłączone do domeny Microsoft Active Directory (serwer w wersji 2022). Wymaga to opracowania procedury oraz jej udokumentowania (opis działania, warunki wykonalności, instrukcja „step-by-step”).

Ilość wymaganych agentów – 170 szt.

Zamawiający w ramach dostawy rozwiązania zobowiązują się ponadto do:

- stworzenia procedur oraz scenariuszy automatycznego oraz ręcznego backup-u serwerów wirtualnych oraz fizycznych z uwzględnieniem dodatkowej kopii na bibliotecę taśmowej,
- stworzenia procedur oraz scenariuszy automatycznego oraz ręcznego backup-u końcówek użytkowników,
- stworzenie procedur i scenariuszy przywracania danych z wykonanych kopii zapisanych na serwerze oraz w bibliotece taśmowej, dla całych maszyn fizycznych/Wirtualnych, pojedynczych wolumenów tych serwerów jak i pojedynczych plików,
- dostarczenia dokumentacji z języku polskim opisującej zastosowane rozwiązania oraz wdrożone procedury i scenariusze backup-u oraz przywracania danych,
- przeszkolenie pracowników zamawiającego w zakresie obsługi biblioteki taśmowej wraz z dokumentacją w języku polskim,