

Macierz NAS – 1 szt. (OT 11)
Obudowa: Rack 19", max 2U
Procesor: Czterordzeniowy procesor o taktowaniu 3,35 GHz (z przyspieszeniem do 3.6 GHz)
Sprzętowy mechanizm szyfrowania: Tak (AES-NI)
Pamięć RAM: 8 GB pamięci ECC UDIMM z możliwością rozszerzenia do 32 GB
Możliwości rozbudowy: Sprzęt powinien być wyposażony w min. 12 kieszeni na dyski twarde typu hot-swap z możliwością rozszerzenia do 24 dysków łącznie przy użyciu dodatkowych jednostek rozszerzających podłączanych do jednostki głównej za pomocą gniazda rozszerzeń Infiniband
Dyski twarde: Urządzenie musi zostać dostarczone z dyskami o pojemności 4TB . Ilość dysków musi pozwalać na pełne obsadzenie macierzy. Dysku muszą znajdować się na liście kompatybilności zaproponowanego urządzenia.
Porty zewnętrzne: <ul style="list-style-type: none"> • 2 porty USB 3.2.1 • 1 gniazdo rozszerzenia
Porty sieciowe: <ul style="list-style-type: none"> • 2 porty 1GbE RJ45 (z obsługą funkcji Link Aggregation / przełączania awaryjnego) • 1 port 10GbE RJ45 • Możliwość podłączenia dodatkowych kart sieciowych 10G poprzez gniazdo rozszerzeń PCIe x8
Funkcja Wake on LAN/WAN: Tak
Gniazdo rozszerzeń PCIe 3.0: <ul style="list-style-type: none"> • 1x 4-liniowe gniazdo x8 Gen. 3
Wentylator obudowy: <ul style="list-style-type: none"> • 3 wentylatory 60 mm x 60 mm
Obsługiwane protokoły sieciowe: <ul style="list-style-type: none"> • SMB1 (CIFS), SMB2, SMB3, • NFSv3, NFSv4, NFSv4.1, NFS Kerberized sessions, • iSCSI, • HTTP, HTTPs, • FTP, • SNMP, • LDAP, • CalDAV
Obsługiwane systemy plików: <ul style="list-style-type: none"> • Wewnętrzny: Btrfs, ext4 • Zewnętrzny: Btrfs, ext4, ext3, FAT, NTFS, HFS+, exFAT
Zarządzanie pamięcią masową: <ul style="list-style-type: none"> • Maksymalny rozmiar pojedynczego wolumenu: <ul style="list-style-type: none"> ○ 200 TB (wymagana pamięć 32 GB) ○ 108 TB • Minimalny liczba wewnętrznych wolumenów: 64 • Minimalny liczba obiektów iSCSI Target: 64 • Minimalny liczba jednostek iSCSI LUN: 128 • Obsługa klonowania/migawek jednostek iSCSI LUN
Obsługiwane typy macierzy RAID: <ul style="list-style-type: none"> • SHR, • Basic, • JBOD,

<ul style="list-style-type: none"> RAID 0/1/5/6/10
<p>Funkcja udostępniania plików:</p> <ul style="list-style-type: none"> Minimalna liczba kont użytkowników: 1 000 Minimalna liczba grup użytkowników: 256 Minimalna liczba folderów współdzielonych: 256
<p>Uprawnienia:</p> <p>Uprawnienia aplikacji listy kontroli dostępu systemu Windows (ACL)</p>
<p>Wirtualizacja:</p> <p>Obsługa VMware vSphere®, Microsoft Hyper-V®, Citrix®, OpenStack®</p>
<p>Usługa katalogowa:</p> <p>Łączy się z serwerami Windows® AD/LDAP, umożliwiając użytkownikom domeny logowanie za pośrednictwem protokołów SMB/NFS/AFP/FTP/File Station przy użyciu istniejących poświadczeń.</p>
<p>Bezpieczeństwo:</p> <p>Zapora, szyfrowanie folderu współdzielonego, szyfrowanie SMB, FTP przez SSL/TLS, SFTP, rsync przez SSH, automatyczne blokowanie logowania, obsługa Let's Encrypt, HTTPS (dostosowywane mechanizmy szyfrowania)</p>
<p>Obsługiwane przeglądarki:</p> <p>Chrome®, Firefox®, Edge®, Internet Explorer® 10 i nowsze, Safari® 10 i nowsze, Safari (iOS 10 i nowsze), Chrome (Android™ 6.0 i nowsze) na tabletach</p>
<p>Oprogramowanie:</p> <ul style="list-style-type: none"> Urządzenie musi umożliwiać utworzenie przestrzeni dyskowej w oparciu o nowoczesny system plików, który będzie zapewniał obsługę migawek, generowania sum kontrolnych CRC a także lustrzanych kopii metadanych aby zapewnić całkowitą integralność danych biznesowych. Dodatkowo wspomniany system musi wspierać ustawienie limitu dla folderów współdzielonych oraz szybkie klonowanie całych folderów udostępnionych Oprogramowanie zarządzające serwerem NAS musi zapewnić darmowe, kompleksowe rozwiązanie do tworzenia kopii zapasowych przeznaczone dla heterogenicznych środowisk IT, umożliwiające zdalne zarządzanie i monitorowanie ochrony komputerów, serwerów i maszyn wirtualnych na jednym, centralnym, przyjaznym dla administratora interfejsie. Ponadto gromadzone dane na urządzeniu mają mieć możliwość replikacji jako lokalne kopie zapasowe, sieciowe kopie zapasowe i kopie zapasowe danych w chmurach publicznych przy użyciu darmowego narzędzia instalowanego z Centrum Pakietów Wymaga się zapewnienia darmowej aplikacji do realizacji chmury prywatnej bez opłat cyklicznych, która będzie posiadała wygodną konsolę administratora zarządzaną z GUI a także agenty na urządzenia PC/MAC oraz aplikację mobilną na Android/iOS. Usługa powinna umożliwiać udostępnianie zasobów serwera NAS, synchronizację i tworzenie kopii zapasowych podłączonych urządzeń a także wspierać algorytm Intelliversioning. Ponadto omawiana usługa powinna umożliwiać pracę z dokumentami biurowymi (edytor tekstowy, arkusz kalkulacyjny, pokaz slajdów) i wspierać wersjonowanie oraz edycję tworzonych plików office w czasie rzeczywistym. Urządzenie musi umożliwiać pracę w trybie klastra wysokiej dostępności (HA) aby zapewnić nieprzerwany, natychmiastowy dostęp do zasobów bez widocznych zmian w użytkowaniu (konfiguracja jako jeden spójny system). Wszystkie dane z powodzeniem zapisane na serwerze aktywnym będą na bieżąco kopiowane do serwera pasywnego zapewniając replikację w czasie rzeczywistym i dostęp do danych oraz usług w przypadku uszkodzenia jednostki aktywnej dając gwarancję ciągłości pracy. Utworzenie klastra HA ma się opierać o 2 identyczne urządzenia.
<p>Konserwacja:</p> <ul style="list-style-type: none"> Konserwację urządzenia należy przeprowadzać przy użyciu dodatkowych, wygodnych w użyciu przesuwanych szyn rack dostarczonych wraz z urządzeniem.
<p>Gwarancja:</p> <p>Wykonawca udzieli gwarancji:</p> <ul style="list-style-type: none"> 3 lata na urządzenie główne 1 rok na dodatkowe akcesoria montażowe w postaci przesuwanych szyn rack

Oprogramowanie backup - 2 szt. (OT 12, OT 13)

Wymagania ogólne:

- 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, obiektowych pamięci masowych kompatybilnych z Microsoft Azure, AWS S3 i urządzeń kompatybilnych z protokołem S3 oraz bezpośrednio z serwerów plikowych opartych o Windows i Linux.

Całkowite koszty posiadania:

- 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
- Oprogramowanie musi wymagać autoryzacji dwóch administratorów backupu do wykonania krytycznych operacji (np. skasowanie backupu, dodanie kolejnego administratora)
- Oprogramowanie musi posiadać integracje z systemami zarządzania kluczami szyfrującymi (KMS)
- Oprogramowanie musi posiadać integracje z systemami typu SIEM

- Oprogramowanie musi posiadać asystenta produktu opartego o AI, pozwalającego na przeszukiwanie dokumentacji technicznej. Powinna istnieć możliwość wyłączenia tej opcji.

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 datastore'u
- 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 (LTO oraz IBM 3592).
- 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 uruchamianie 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, Oracle i PostgreSQL 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 wspierać granularne odtwarzanie baz danych SAP HANA do oryginalnej lub innej lokalizacji
- 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 posiadać natywną integrację dla backupów wykonywanych poprzez IBM Db2
- 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 analizować indeksy systemów plików zabezpieczanych maszyn w poszukiwaniu rozszerzeń, notatek żądania okupu oraz innych oznak obecności ransomware/malware

- Oprogramowanie musi mieć możliwość skanowania plików backupu przy pomocy znanych sygnatur złośliwego oprogramowania
- Oprogramowanie, bazując na wyuczonym modelu maszynowym (machine learning) musi w locie wykrywać oznaki złośliwego oprogramowania (malware, ransomware) oraz cyberataków
- 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 deduplikację 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 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
- Rozwiązanie musi wspierać odzysk do konkretnego punktu w czasie (point-in-time) dla wspieranych systemów bazodanowych
- Rozwiązanie musi umożliwiać natychmiastowe publikowanie baz MS SQL, Oracle i PostgreSQL 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 zabezpieczonego
- 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 nadanym 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

Wsparcie techniczne:

Oprogramowanie musi zostać dostarczone wraz z opieką techniczną producenta oraz prawem do aktualizacji do najnowszej wersji na okres **24 miesięcy** i obejmować **10 instancji**.

Serwer wirtualizacji (OT 14, OT 17, OT 19, OT 20)

Obudowa:

- Obudowa Rack o wysokości max 1U z możliwością instalacji min. 8 dysków 2,5" wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych oraz organizatorem do kabli.
- Możliwość wyposażenia w panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS'u, zasilaniu oraz temperaturze.
- Obudowa z możliwością wyposażenia w kartę umożliwiającą dostęp bezpośredni poprzez urządzenia mobilne - serwer musi posiadać możliwość konfiguracji oraz monitoringu najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej min. (Android/ Apple iOS) przy użyciu jednego z protokołów BLE/ WIFI..

Płyta główna:

- Płyta główna z możliwością zainstalowania do dwóch procesorów.
- Obsługa procesorów 32 rdzeniowych.
- Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym.
- Na płycie głównej powinno znajdować się minimum 16 sloty przeznaczone do instalacji pamięci.
- Płyta główna powinna obsługiwać do 1TB pamięci RAM.

Chipset:

- Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych.

Procesor:

- Zainstalowany **jeden procesor min. 16-rdzeniowy**, min. 2,8GHz, klasy x86 dedykowane do pracy z zaoferowanym serwerem umożliwiające osiągnięcie wyniku min. 335 w teście SPECrate2017_int_base, dostępnym na stronie www.spec.org dla konfiguracji dwuprocesorowej .

RAM:

- Minimum **128GB** DDR5 RDIMM 5600MT/s,

Funkcjonalność pamięci RAM

- Demand Scrubbing,
- Patrol Scrubbing,
- Permanent Fault Detection

Gniazda PCI:

- minimum jeden slot PCIe x16 Gen 4

Interfejsy sieciowe / FC / SAS:

- Wbudowane min. **2 interfejsy sieciowe 1Gb Ethernet** w standardzie Base-T
- Dodatkowe min. **4 interfejsy sieciowe 1GB Ethernet** w standardzie Base-T (porty nie mogą być osiągnięte poprzez karty w slotach PCIe)
- **Dodatkowa karta HBA 4 interfejsy SAS 12Gb** wyprowadzone na zewnątrz serwera

Dyski twarde:

- Zainstalowane 3 dyski SSD SATA o pojemności min. 480GB Hot-Plug

Kontroler RAID:

- Sprzętowy kontroler dyskowy, posiadający możliwość konfiguracji poziomów RAID: 0, 1, 5, 6, 10, 50, 60.

Wbudowane porty:

- 3x USB, w tym min. 1 porty USB 3.0
- 2x port VGA (jeden na panelu przednim)
- Możliwość rozbudowy o port RS232

Video:

- Zintegrowana karta graficzna umożliwiającą wyświetlenie rozdzielczości min. 1920x1200

<p>Zasilacze:</p> <ul style="list-style-type: none"> • Dwa w pełni redundantne zasilacze, Hot-Plug min. 700W klasy Titanium każdy.
<p>Bezpieczeństwo:</p> <ul style="list-style-type: none"> • Zatrzask górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych. • Wbudowany w serwer mechanizm pozwalający na weryfikację niezmienności konfiguracji sprzętowej serwera od momentu produkcji do dostawy do docelowej lokalizacji. Mechanizm ma również pozwalać na kontrolę otwarcia urządzenia w trakcie transportu, niezależnie od stanu zasilania. • Możliwość wyłączenia w BIOS funkcji przycisku zasilania. • BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła • Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą. • Moduł TPM 2.0 • Możliwość dynamicznego włączania i wyłączania portów USB na obudowie – bez potrzeby restartu serwera • Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem • Serwer musi być wyposażony w rozwiązanie zapewniające ochronę oprogramowania układowego przed manipulacją złośliwego oprogramowania. Ochrona taka musi być zgodna z zaleceniami NIST SP 800-147B i NIST SP 800-155. Jednocześnie Zamawiający wymaga, aby dostarczony serwer posiadał zaimplementowane sprzętowo mechanizmy kryptograficzne poświadczające integralność oprogramowania BIOS (Root of Trust).
<p>Karta Zarządzania:</p> <p>Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiającą:</p> <ul style="list-style-type: none"> • zdalny dostęp do graficznego interfejsu Web karty zarządzającej; • zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera); • szyfrowane połączenie (TLS) oraz autentykację i autoryzację użytkownika; • możliwość podmontowania zdalnych wirtualnych napędów; • wirtualną konsolę z dostępem do myszy, klawiatury; • wsparcie dla IPv6; • wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish; • możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer; • możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer; • integracja z Active Directory; • możliwość obsługi przez dwóch administratorów jednocześnie; • wsparcie dla dynamic DNS; • wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej. • możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera • możliwość zarządzania do 100 serwerów bezpośrednio z konsoli karty zarządzającej pojedynczego serwera <p>oraz z możliwością rozszerzenia funkcjonalności o:</p> <ul style="list-style-type: none"> • Wirtualny schowek ułatwiający korzystanie z konsoli zdalnej • Przesyłanie danych telemetrycznych w czasie rzeczywistym • Dostosowanie zarządzania temperaturą i przepływem powietrza w serwerze • Automatyczna rejestracja certyfikatów (ACE)
<p>Oprogramowanie do zarządzania serwerem</p> <p>Możliwość zainstalowania oprogramowania producenta do zarządzania, spełniającego poniższe wymagania:</p> <ul style="list-style-type: none"> • Wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych • integracja z Active Directory • Możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta

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

Certyfikaty:

- Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015, ISO-50001 oraz ISO-14001
- Serwer musi posiadać deklarację CE.
- Oferowane produkty muszą zawierać informacje dotyczące ponownego użycia i recyklingu, nie mogą zawierać farb i powłok na dużych plastikowych częściach, których nie da się poddać recyklingowi lub ponownie użyć. Wszystkie produkty zawierające podzespoły elektroniczne oraz niebezpieczne składniki powinny być bezpiecznie i łatwo identyfikowalne oraz usuwalne. Usunięcie materiałów i komponentów powinno odbywać się zgodnie z wymogami Dyrektywy WEEE 2002/96/EC. Produkty muszą składać się z co najmniej w 65% ze składników wielokrotnego użytku/zdatnych do recyklingu. We wszystkich produktach części tworzyw sztucznych większe niż 25-gramowe powinny zawierać nie więcej niż śladowe ilości środków zmniejszających palność sklasyfikowanych w dyrektywie RE 67/548/EEC. Potwierdzeniem spełnienia powyższego wymogu jest wydruk ze strony internetowej www.epeat.net potwierdzający

<p>spełnienie normy co najmniej Epeat Silver według normy wprowadzonej w 2019 roku - Wykonawca wraz ze sprzętem złoży dokument potwierdzający spełnianie wymogu.</p> <ul style="list-style-type: none"> Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Microsoft Windows Server 2019, Microsoft Windows Server 2022.
<p>Dokumentacja użytkownika:</p> <ul style="list-style-type: none"> Zamawiający wymaga dokumentacji w języku polskim lub angielskim. Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.
<p>Warunki gwarancji:</p> <ul style="list-style-type: none"> Zamawiający wymaga zapewnienia gwarancji Producenta z zakresu wdrażanej technologii na okres 3 lat. Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie, przez Internet oraz z wykorzystaniem aplikacji. Zamawiający oczekuje bezpośredniego dostępu do wykwalifikowanej kadry inżynierów technicznych a w przypadku konieczności eskalacji zgłoszenia serwisowego wyznaczonego Kierownika Eskalacji po stronie Producenta (dla krytycznych zgłoszeń serwisowych) Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania Producenta, w tym także sprzedanego oprogramowania. Zgłoszenie przyjęte jest potwierdzane przez zespół pomocy technicznej (mail/telefon / aplikacja / portal) przez nadanie unikalnego numeru zgłoszenia pozwalającego na identyfikację zgłoszenia w trakcie realizacji naprawy i po jej zakończeniu. Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy. Zamawiający oczekuje rozpoczęcia diagnostyki telefonicznej / internetowej już w momencie dokonania zgłoszenia. Certyfikowany Technik Producenta z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) powinien rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym (NBD) od otrzymania zgłoszenia / zakończenia diagnostyki. Naprawa ma się odbyć w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę. Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia oraz pobieranie uaktualnień mikro kodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji serwera. Zamawiający oczekuje nieodpłatnego udostępnienia narzędzi serwisowych i procesów wsparcia umożliwiających: Wykrywanie usterek sprzętowych z predykcją awarii, automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych, wskazówki dotyczące bezpieczeństwa produktów, samodzielne wysyłanie części, a także ocena bezpieczeństwa cybernetycznego. Możliwość rozszerzenia gwarancji producenta o usługę diagnostyki sprzętu na miejscu w przypadku awarii. Charakterystyka usługi diagnostyki: <ul style="list-style-type: none"> Możliwości utworzenia zgłaszania serwisowego w wyniku, którego proces diagnostyki odbędzie się na miejscu w siedzibie zamawiającego. Po przyjeździe do siedziby Zamawiającego, pracownik serwisu przystąpi do rozwiązywania problemu. Jeśli do rozwiązania problemu będzie konieczna dodatkowa pomoc diagnostyczna lub części, pracownik serwisu może w imieniu Zamawiającego skontaktować się z producentem w celu uzyskania pomocy. Reakcja na miejscu u Zamawiającego powinna nastąpić w okresie zgodnym z czasem reakcji przypisanym do urządzenia, które posiada wykupioną usługę serwisową. Pracownik serwisu powinien skontaktować się z Zamawiającym przed przyjazdem na miejsce w celu sprawdzenia zgłoszenia, ustalenia harmonogramu i potwierdzenia wszelkich informacji niezbędnych do realizacji wizyty technika na miejscu. Jeśli w trakcie wstępnego procesu rozwiązywania problemu na miejscu awarii zostanie ustalone, że do realizacji usługi jest niezbędna jakaś część, znajdujący się na miejscu pracownik serwisu zamówi nową część i przekaże dodatkowe zgłoszenie do działu obsługi technicznej. Technik pracujący na miejscu powróci do siedziby Klienta w celu wymiany wysłanej części w ciągu czasu reakcji ustalonego zgodnie z umową serwisową zakupionego produktu. Przed podpisaniem umowy wymagane dołączenie do oferty oświadczenia Producenta potwierdzając, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta.

- Wykonawca musi posiadać certyfikat nadany przez uprawniony podmiot potwierdzający realizację usług serwisowych zgodnie z normą PN-EN ISO 27001:2017 lub certyfikat równoważny

System operacyjny:

Oprogramowanie **Microsoft Windows Server DataCenter 2025** lub równoważne spełniające poniższe warunki zgodności:

- Licencja musi uprawniać do uruchamiania serwerowego systemu operacyjnego w środowisku fizycznym i nielimitowanych wirtualnych środowisk serwerowego systemu operacyjnego za pomocą wbudowanych mechanizmów wirtualizacji.
- Możliwość wykorzystywania 240 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności min. 64TB przez każdy wirtualny serwerowy system operacyjny.
- Możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci.
- Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy.
- Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy.
- Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.
- Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy.
- Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading;
- Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.
- Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.
- Możliwość uruchamiania aplikacji internetowych wykorzystujących technologię ASP.NET.
- Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.
- Wbudowana zaporę internetową (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.
- Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe.
- Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 2 języków poprzez wybór z listy dostępnych lokalizacji.
- Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).
- Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.
- Wsparcie dostępu do zasobu dyskowego SSO poprzez wiele ścieżek (Multipath).
- Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego.
- Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.

Wraz z systemem operacyjnym należy dostarczyć licencje dostępowe dla 40 użytkowników.

Macierz dyskowa (OT 15, OT 18)

Obudowa:

System z wszystkimi komponentami do instalacji w szafie rack 19".

Dyski twarde:

- System musi zostać dostarczony w konfiguracji zawierającej minimum
 - **9 dysków 4TB NL-SAS**
 - **3 dyski 1900GB SSD**i zajmować maksymalnie **2U** w szafie rack.
- System musi ponadto wspierać dyski:
 - SSD: od 800GB do 15.3TB
 - SAS 10k od 900GB do 1800GB lub NL-SAS od 4TB do 18TB
- System musi mieć możliwość rozbudowy do minimum **95 dysków** oraz musi pozwalać na rozbudowę do wyższych modeli bez potrzeby migracji danych (przez rozbudowę do wyższego modelu zamawiający rozumie do modelu macierzy z większą ilością Cache, większą skalowalnością i mocniejszymi procesorami). Zamawiający dopuszcza rozwiązanie, które nie pozwala na taką rozbudowę w przypadku, gdy zostanie zaoferowany najwyższy z modeli macierzy skalowalny min do 500 dysków oraz pamięcią cache min 512GB.
- Macierz musi pozwalać i być przystosowana na rozbudowę do modelu NVME bez potrzeby wymiany dysków i kopiowania danych.

Kontroler:

- **Dwa kontrolery wyposażone w przynajmniej 32GB cache każdy.**
- W przypadku awarii zasilania dane niezapisane na dyski, przechowywane w pamięci muszą być zabezpieczone za pomocą podtrzymania bateryjnego przez 72 godziny lub jako zrzut na pamięć flash.
- Macierz musi pozwalać na rozbudowę cache do 32GB cache na kontroler.

Interfejsy:

- 4 porty 10Gb/s lub 25GbE SFP
- **8 portów 12Gb/s do podłączenia serwerów z kompletem okablowania 2m Mini SAS HD**
- **4 porty SAS 12 Gb/s do podłączenia półek dyskowych**

RAID:

- Wsparcie dla RAID: 0, 1, 5, 6, 10
- Dodatkowo macierz musi posiadać mechanizm tworzenia wirtualnej przestrzeni na minimum 180 dyskach macierzy wraz z wyliczaniem parzystości oraz podwójnej parzystości w celu zabezpieczenia danych. Mechanizm ten musi być przygotowany do optymalizacji procesów odtwarzania dysków pojemnościowych.
- Obliczanie sum kontrolnych (kodów parzystości) dla grup dyskowych RAID5 i RAID6 musi być realizowane w sposób sprzętowy przez dedykowany układ w macierzy.

Obsługiwane protokoły:

- FC,
 - iSCSI,
 - SAS,
 - S3,
 - CIFS,
 - NFS.
- Zamawiający dopuszcza zrealizowanie protokołu CIFS, NFS i S3 za pomocą zewnętrznego oprogramowania typu Software Defined Storage.

Inne wymagania:

- Macierz musi posiadać wsparcie dla wielościeżkowości dla systemów:
 - Microsoft® Windows Server®,
 - Red Hat Enterprise Linux®,
 - SUSE Linux Enterprise Server,

<ul style="list-style-type: none"> ○ VMware® ESX®. • Macierz musi posiadać funkcjonalność wykonywania snapshotów - minimum 128 per wolumen. • Macierz musi posiadać funkcjonalność klonowania danych • Macierz musi posiadać funkcjonalność replikacji danych po FC (po zainstalowaniu portów FC na macierzy) w trybie synchronicznym i asynchronicznym, oraz po Ethernetie w trybie asynchronicznym system musi pozwalać na wykonanie do 32 jednoczesnych replikacji. • Macierz musi posiadać możliwość tworzenia i prezentacji dysków logicznych (LUN) o pojemności większej niż zajmowana fizyczna przestrzeń dyskowa (ang. ThinProvisioning). • Macierz musi umożliwiać dynamiczną zmianę rozmiaru wolumenów logicznych bez przerywania pracy macierzy i bez przerywania dostępu do danych znajdujących się na danym wolumenie. • Macierz musi posiadać funkcjonalność partycjonowania macierzy na odseparowane od siebie logicznie systemy, na których rezydują osobne dyski logiczne dla heterogenicznych systemów. Licencja na macierzy musi pozwalać na wykonanie do 128 partycji. • Macierz musi posiadać funkcjonalność automatycznego balansowania obciążenia kontrolerów macierzy przez przełączanie w trybie online wolumenów logicznych pomiędzy nimi w zależności od wygenerowanego na nich ruchu. Musi istnieć możliwość wyłączenia tej funkcjonalności z poziomu interfejsu użytkownika. • Macierz musi pozwalać na dynamiczną migrację pomiędzy poziomami RAID. • Z poziomu graficznego interfejsu do zarządzania musi istnieć możliwość sprawdzenia stanu zużycia dysków SSD. • Macierz musi posiadać oprogramowanie do monitoringu stanu dysków, które pozwala na identyfikowanie potencjalnie zagrożonych awarią dysków • Wraz z systemem musi zostać dostarczone narzędzie do monitoringu macierzy w kontekście: <ul style="list-style-type: none"> ○ wydajności i opóźnień na wolumenach ○ wydajności I/Ops, MB/s • Macierz musi posiadać możliwość integracji z Active Directory w zakresie definicji i mapowania grup i użytkowników pod kątem autentykacji. • Macierz musi posiadać oprogramowanie do aplikacji pozwalające na integrację z: <ul style="list-style-type: none"> ○ VMware vCenter – provisioning i monitoring macierzy z widoku vCenter ○ VMware VASA ○ Microsoft Virtual Disk Service (VDS) ○ Microsoft Virtual Shadow Service (VSS) • Zamawiający dopuszcza zaoferowanie zewnętrznego oprogramowania do zapewnienia integracji i monitoring w/w aplikacji np. w formie Software Defined storage. • Macierz musi pozwalać na szyfrowania danych, realizacja procesu szyfrowania i zarządzania kluczem może się odbywać przez kontrolery macierzy lub zewnętrzne urządzenia i oprogramowanie do zarządzania kluczem • Macierz musi oferować wydajność do 500 000 IOPS – 	<p>Gwarancja i serwis:</p> <ul style="list-style-type: none"> • 2 lata serwisu producenta zapewniającego dostawę podzespołu zapasowego na następny dzień roboczy od diagnozy problemu. Możliwość zgłaszania awarii poprzez linię telefoniczną lub inne systemy firmy serwisującej. • Dostarczony system musi posiadać również 2 lata serwisu (aktualizacje i wsparcie) producenta dla dostarczonego wraz z macierzą oprogramowania, dostęp do portalu serwisowego producenta, dostęp do wiedzy i informacji technicznych dotyczących oferowanego urządzenia. • Zepsute nośniki pozostają własnością zamawiającego
---	---

Przełącznik sieciowy Typ II – 2 szt. (OT 16)**Parametry fizyczne:**

- Wymiary urządzenia muszą pozwalać na montaż w szafie rack 19", obudowa nie może być wyższa niż 1U.
- Zasilanie AC 230V.
- Maksymalny pobór mocy: 30 W.
- Minimalny zakres temperatury pracy: 0-40°C.

Interfejsy sieciowe:

- 24 porty GE RJ-45.
- 4 porty 10 GE SFP+ obsadzone wkładkami 10 GE SR.

Zarządzanie:

- Wbudowany 1 port konsoli szeregowej do pełnego zarządzania.
- Zarządzanie przez: command line (w tym poprzez SSH) oraz poprzez graficzny interfejs z wykorzystaniem przeglądarki (HTTPS).
- Wsparcie dla SNMP w wersjach 1-3
- Funkcja zarządzania poprzez dedykowany kontroler przełączników lub system zarządzania, pozwalający na automatyczne wykrywanie, centralne konfigurowanie oraz zarządzanie przełącznikami.
- Funkcja aktualizacji oprogramowania przez TFTP/FTP oraz za pomocą GUI.
- Konfiguracja w formie pliku tekstowego umożliwiającego edycję konfiguracji offline.
- Funkcja backupu konfiguracji z poziomu GUI jak również z CLI (TFTP/FTP).
- Funkcja definiowania administratorów lokalnie oraz wykorzystanie w tym celu serwerów Radius i TACACS+.
- Funkcja definiowania ról administratorów z możliwością określenia trybu dostępu (brak, tylko odczyt, odczyt oraz modyfikacja) do wybranych części konfiguracji.
- Automatycznie wykonywane rewizje konfiguracji

Parametry wydajnościowe:

- Przepustowość urządzenia - min. 125 Gbps (pełna prędkość, tzw. wire-speed na wszystkich portach) oraz min. 190 Mpps.
- Tablica adresów MAC o pojemności co najmniej 32k wpisów.
- Opóźnienie wprowadzane przez przełącznik - poniżej 2 mikrosekund.

Wymagane funkcje:

- Funkcja automatycznej negocjacji prędkości i duplexu dla połączeń.
- Obsługa Jumbo Frames.
- Obsługa 802.1d (Spanning Tree), 802.1w (Rapid Spanning Tree), 802.1s (Multiple Spanning Tree).
- Agregacja portów zgodna ze standardem 802.3ad.
- Obsługa co najmniej 4000 VLAN'ów, zgodna ze standardem 802.1Q.
- Obsługa routingu statycznego.
- Port-mirroring.
- Uwierzytelnianie 802.1x na poziomie portu.
- Uwierzytelnianie 802.1x w oparciu o adres MAC.
- W ramach 802.1x wsparcie dla dedykowanego VLAN'u dla gości (guest VLAN).
- W ramach 802.1x wsparcie dla urządzeń, które nie obsługują tego protokołu, na podstawie adresu MAC urządzenia.
- W ramach 802.1x wsparcie dla dynamicznego przypisywania VLAN.
- Obsługa protokołu sFlow.

Dodatkowe funkcje urządzenia przy integracji z systemem centralnego zarządzania:

- Przełączniki muszą wspierać tryb pracy, w którym są zarządzane przez fizyczny element nadrzędny (przełącznik lub dedykowany kontroler) (tzw. port extender lub element leaf w architekturze spine-leaf). Zakres zarządzania przez element nadrzędny musi zawierać co najmniej:
 - Centralne zarządzanie konfiguracją urządzenia
 - Aktualizacja oprogramowania realizowana z systemu centralnego zarządzania
 - Centralne zarządzanie sieciami VLAN.
 - Blokowanie ruchu pomiędzy klientami w ramach jednego VLAN'u
 - Rozpoznawanie urządzeń uzyskujących dostęp do sieci, zarówno stacji klienckich, jak i urządzeń typu drukarki, routery, przełączniki, itp..

<ul style="list-style-type: none"> ○ Przenoszenie zidentyfikowanych urządzeń do właściwych stref. W przypadku wykrycia urządzenia niepasującego do zaakceptowanych schematów, urządzenie powinno przenieść go do strefy odizolowanej. ○ Integrację z systemem kontroli dostępu. Urządzenie musi podejmować decyzje o dostępie na podstawie przynajmniej następujących czynników: nazwy hosta, nazwy użytkownika, typu urządzenia, typu systemu operacyjnego. ○ Automatyczna detekcja i rekomendacje konfiguracji. ○ Przesyłanie logów na zewnętrzny serwer syslog. ○ Funkcja uruchomienia Captive Portalu w celu identyfikacji użytkowników. ○ Obsługa białych i czarnych list adresów MAC. ○ Wykrywanie aplikacji komunikujących się w sieci. <ul style="list-style-type: none"> ● Musi być możliwe redundantne połączenie z elementami zarządzającymi. ● W ramach postępowania koniecznym jest dostarczenie wszystkich licencji niezbędnych do uruchomienia na przełączniku w/w funkcji, polegających na integracji z systemem centralnego zarządzania lub NAC.
<p>Gwarancja:</p> <ul style="list-style-type: none"> ● System musi być objęty serwisem gwarancyjnym producenta przez okres 36 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7. ○
<p>Wymagania ogólne:</p> <ul style="list-style-type: none"> ● W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca wraz ze sprzętem winien przedłożyć dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania.