

OPIS PRZEDMIOTU ZAMÓWIENIA DLA PAKIET 1

Dostawy: serwera backupowego wraz z oprogramowaniem serwerowym i backupowym i macierzą dyskową – 1 sztuka, UPS-serwer – 2 sztuki, UPS-komputer – 8 sztuk, urządzenie sieciowe typu switch – 2 sztuki.

I. Zadania Wykonawcy:

1. Dostawa urządzeń wraz z oprogramowaniem, ich instalacja i skonfigurowanie.
2. Dostarczenie wszystkich niezbędnych wkładek i kabli połączeniowych.
3. Przeprowadzenie testów symulujących awarię każdego z elementów infrastruktury.
4. Przeprowadzenie szkoleń instruktarszych dla osób wskazanych przez Zamawiającego.
5. Dostarczony sprzęt musi być nowy i wyprodukowany nie wcześniej niż w 2025 roku.
Zamawiający zastrzega sobie możliwość weryfikacji u producenta sprzętu legalności oprogramowania oraz żądanych trybów serwisu. Na żądanie Zamawiającego, Wykonawca będzie zobowiązany do dostarczenia oświadczenia producenta o spełnieniu wymogów SWZ. Wykonawca ponosi wszelkie koszty związane z dostarczeniem sprzętu i oprogramowania do siedziby Zamawiającego.
6. Oferowany sprzęt, o ile nie wskazano inaczej, musi posiadać minimum 36 miesięczne wsparcie producenta w zakresie zgłaszania problemów technicznych oraz dostępu do poprawek i uaktualnień systemu. W okresie wsparcia Zamawiający musi mieć prawo do bezpłatnej aktualizacji do najnowszej wersji produktów, jeżeli zostaną one opublikowane przez producenta dostarczonego sprzętu i oprogramowania.
7. Oferowane oprogramowanie, o ile nie wskazano inaczej, musi posiadać minimum 12 miesięczne wsparcie producenta w zakresie zgłaszania problemów technicznych oraz dostępu do poprawek i uaktualnień. W okresie wsparcia Zamawiający musi mieć prawo do bezpłatnej aktualizacji do najnowszej wersji produktów, jeżeli zostaną one opublikowane przez producenta dostarczonego oprogramowania.
8. Zamawiający dopuszcza zaoferowanie sprzętu równoważnego o parametrach nie gorszych niż przedstawione w specyfikacji, potwierdzenie równoważności spoczywa na Wykonawcy.
9. Koszt dojazdu przedstawicieli Wykonawcy i serwisu do siedziby Zamawiającego na koszt Wykonawcy.
10. W cenie oferty wliczone są transport, opakowanie, czynności związane z przygotowaniem dostawy, ubezpieczenie, przesyłka.
11. Wszystkie prace instalacyjne i konfiguracyjne muszą być przeprowadzane w taki sposób, aby nie zakłócić pracy Zamawiającego. Wykonawca realizować będzie prace stanowiące przedmiot niniejszej umowy w dniach od poniedziałku do piątku w godzinach uzgodnionych z Zamawiającym. Za zgodą i wiedzą Zamawiającego, prace wykonywać można w innych dniach i godzinach. Należy podać charakter planowanych robót, obszar oraz przewidywany czas ich trwania. Jeżeli jakkolwiek obszar wdrożenia wymaga

przerwy w dostępie do sieci czy zasobów sieciowych musi zostać uzgodniony z Zamawiającym z min. 1 dniowym wyprzedzeniem.

12. Prace instalacyjne:

- a) Prace obejmą proces fizycznej instalacji i konfigurację urządzeń dostarczonych przez Wykonawcę wraz z aktualizacją systemów operacyjnych, sterowników i firmware
- b) Konfiguracja dostarczanych urządzeń sieciowych
- c) Konfiguracja oprogramowania backup, modyfikacja istniejących zadań backup oraz wytworzenie nowych niezbędnych do uruchomienia przechowywania kopii zapasowych na dostarczanych urządzeniach (Serwer backupowy wraz z oprogramowaniem serwerowym i backupowym i macierzą dyskową oraz serwer do archiwizacji bazy danych oprogramowania do obsługi poradni oraz archiwizacji dokumentacji medycznej, skanów dokumentów dołączanych do dokumentacji)

II. OPZ dla serwer backupowy wraz z oprogramowaniem serwerowym i backupowym i macierzą dyskową – 1 sztuka

Serwer:
Obudowa: <ul style="list-style-type: none"> Obudowa Rack o wysokości 2U z możliwością instalacji min. 8 dysków 3,5” wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych oraz organizatorem do kabli. Obudowa z możliwością wyposażenia w kartę umożliwiającą dostęp bezpośredni poprzez urządzenia mobilne - serwer musi posiadać możliwość konfiguracji oraz monitoringu najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej min. (Android/ Apple iOS) przy użyciu jednego z protokołów BLE/ WIFI.
Płyta główna: <ul style="list-style-type: none"> Płyta główna z możliwością zainstalowania do dwóch procesorów. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym. Płyta główna powinna obsługiwać do 1 TB pamięci RAM.
Chipset: <ul style="list-style-type: none"> Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych.
Procesor: <ul style="list-style-type: none"> Zainstalowany jeden procesor min. 12-rdzeniowy, min. 2.1GHz, klasy x86 dedykowane do pracy z zaoferowanym serwerem umożliwiające osiągnięcie wyniku min. 168 w teście SPECrate2017_int_base, dostępnym na stronie www.spec.org dla konfiguracji dwuprocesorowej .
RAM: <ul style="list-style-type: none"> Minimum 64GB DDR4 RDIMM 3200MT/s, Na płycie głównej powinno znajdować się minimum 16 slotów przeznaczonych do instalacji pamięci.
Gniazda PCI: <ul style="list-style-type: none"> minimum jeden slot PCIe x16 Gen 4
Interfejsy sieciowe / FC / SAS: <ul style="list-style-type: none"> Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT

Dyski twarde:

- Zainstalowane 2 dyski M.2 SSD o pojemności min. 240 GB Hot-Plug z możliwością konfiguracji RAID 1
- Zainstalowane 2 dyski SAS o pojemności min. 2.4 TB, 12 Gb, 2,5" Hot-Plug.

Kontroler RAID:

- Sprzętowy kontroler dyskowy, posiadający
 - Min. 8 GB nieulotnej pamięci cache,
 - Możliwość konfiguracji poziomów RAID: 0, 1, 5, 6, 10, 50, 60.
 - Wsparcie dla dysków samoszyfrujących

Wbudowane porty:

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

Video:

- Zintegrowana karta graficzna umożliwiającą wyświetlenie rozdzielczości min. 1920x1200

Zasilacze:

- Redundantne, Hot-Plug min. 700W klasy Titanium każdy.

Bezpieczeństwo:

- Zatrask górnej pokrywy oraz blokada na ramce panelu zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych.
- Możliwość wyłączenia w BIOS funkcji przycisku zasilania.
- BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła.
- Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą.
- Moduł TPM 2.0.
- Możliwość dynamicznego włączania i wyłączania portów USB na obudowie – bez potrzeby restartu serwera.
- Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem.

Karta Zarządzania:

Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiającą:

- 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 autentykacje 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 e-mail 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 oraz z możliwością rozszerzenia funkcjonalności o:
- 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).

Oprogramowanie do zarządzania:

Możliwość zainstalowania oprogramowania producenta do zarządzania, spełniającego poniższe wymagania:

- Wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych.
- Integracja z Active Directory.
- Możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta.
- Wsparcie dla protokołów SNMP, IPMI, Linux SSH, Redfish.
- Możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram.
- Szczegółowy opis wykrytych systemów oraz ich komponentów.
- Możliwość eksportu raportu do CSV, HTML, XLS, PDF.
- Możliwość tworzenia własnych raportów w oparciu o wszystkie informacje zawarte w inwentarzu.
- Grupowanie urządzeń w oparciu o kryteria użytkownika.
- Tworzenie automatycznie grup urządzeń w oparciu o dowolny element konfiguracji serwera np. nazwa, lokalizacja, system operacyjny, obsadzenie slotów PCIe, pozostałego czasu gwarancji.
- Możliwość uruchamiania narzędzi zarządzających w poszczególnych urządzeniach.
- Szybki podgląd stanu środowiska.
- Podsumowanie stanu dla każdego urządzenia.
- Szczegółowy status urządzenia/elementu/komponentu.
- Generowanie alertów przy zmianie stanu urządzenia.
- Filtry raportów umożliwiające podgląd najważniejszych zdarzeń.
- Integracja z service desk producenta dostarczonej platformy sprzętowej.
- Możliwość przejęcia zdalnego pulpitu.
- Możliwość podmontowania wirtualnego napędu.
- Kreator umożliwiający dostosowanie akcji dla wybranych alertów.
- Możliwość importu plików MIB.
- Przesyłanie alertów „as-is” do innych konsol firm trzecich.
- Możliwość definiowania ról administratorów.
- Możliwość zdalnej aktualizacji oprogramowania wewnętrznego serwerów.
- 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 przetłączników 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.

Oprogramowanie do monitorowania

Oparta na chmurze aplikacja Producenta oferowanego urządzenia, która zapewnia proaktywne monitorowanie i rozwiązywanie problemów infrastruktury IT oraz integrację z posiadaną platformą wirtualizacji VMware. Zaproponowane rozwiązanie musi posiadać następujące funkcjonalności:

- Monitoring:
 - Ilość podłączonych oraz rozłączonych systemów
 - Stan podłączonych urządzeń
 - Informacje o potencjalnych zagrożeniach związanych z cyberbezpieczeństwem w oparciu o najlepsze praktyki i szczegółową analizę posiadanych systemów
 - Informacje o alertach z podziałem na minimum: krytyczne, błędy, ostrzeżenia
 - Informacje o statusie gwarancji dla poszczególnych urządzeń
 - Informacje o stanie licencji na posiadane oprogramowanie rozszerzające funkcjonalności urządzeń
 - Informacje w oparciu o dane historyczne umożliwiające określenie trendów krótko i długoterminowej prognozy wykorzystania przestrzeni na pamięciach masowych.
 - Wykrywanie anomalii w oparciu o analizę zajętości przestrzeni na pamięciach masowych
 - Wykrywanie anomalii wydajnościowych w oparciu o uczenie maszynowe oraz porównanie parametrów historycznych i bieżących. Funkcjonalność ta musi wspierać serwery, urządzenia sieciowe oraz systemy pamięci masowych.
 - Monitorowanie wydajności, przepustowości oraz opóźnień dla systemy pamięci masowych.
 - Zaimplementowana analityka predykcyjna umożliwiająca określenie szacowanego czasu awarii dla optyki przetłączników FC.
 - Szczegółowe informacje dla serwerów o modelu, konfiguracji, wersjach firmware poszczególnych komponentów adresacji IP karty zarządzającej.
 - Monitoring parametrów serwerów z informacją o minimum:

- Obciążeniu procesora
 - Zużyciu pamięci RAM
 - Temperaturze procesorów
 - Temperaturze powietrza wlotowego
 - Zużyciu prądu
 - Zmianach w fizycznej konfiguracji serwera
 - Dla wszystkich wymienionych parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach.
- Monitoring parametrów pamięci masowych z informacją o minimum:
 - Opóźnieniach
 - IOPS
 - Przepustowości
 - Utylizacji kontrolerów
 - Pojemność całkowita i dostępna
 - Wszystkie informacje muszą być dostępne zarówno dla całej pamięci masowej jak i poszczególnych LUN-ów.
 - Dla wszystkich wymienionych powyżej parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach.
 - Dane historyczne o wykorzystaniu przestrzeni pamięci masowej muszą być przechowywane co najmniej 2 lata
 - Informacje o poziomie redukcji danych
 - Informacje o statusie replikacji oraz snapshotów
- Monitoring parametrów przełączników sieciowych z informacją o minimum:
 - Modelu, oprogramowania, adresacji IP, MAC adres, nr seryjny
 - Stanie komponentów: zasilacze, wentylatory
 - Podłączonych hostach
 - Ilości i statusu portów
 - Utylizacji procesora
 - Utylizacji poszczególnych portów
 - Dla wszystkich wymienionych powyżej parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach.
- Aktualizacja firmware
 - możliwość aktualizacji firmware, oprogramowania zarządzającego dla systemów pamięci masowych, wraz z informacją o zalecanych wersjach oprogramowania
 - możliwość aktualizacji firmware, oprogramowania zarządzającego dla serwerów, wraz z informacją o zalecanych wersjach oprogramowania
 - możliwość aktualizacji firmware, oprogramowania zarządzającego dla rozwiązań HCI, wraz z informacją o zalecanych wersjach oprogramowania
 - możliwość aktualizacji firmware, dla systemów przełączników FC, wraz z informacją o zalecanych wersjach oprogramowania
 - możliwość aktualizacji firmware, dla deduplikatorów, wraz z informacją o zalecanych wersjach oprogramowania
- Raporty
 - Możliwość generowania raportów dla serwerów zawierających informację o:

- Nazwie hosta, modelu serwera, nr serwisowym, dacie końca okresu kontraktu serwisowego, zainstalowanym systemie operacyjnym, protokole komunikacyjnym z systemem pamięci masowej
 - Średnim obciążeniu: procesorów, pamięci RAM, IO,
- Możliwość generowania raportów dla systemów pamięci masowych zawierających informację o:
 - Nazwie, nr seryjnym, lokalizacji urządzenia, modelu urządzenia, wersji oprogramowania, zajętości systemu oraz poziomu redukcją danych, informacje o utworzonych LUN-ach i systemach pliku, status replikacji
- Generowanie raportów do plików CSV i PDF
- Cyberbezpieczeństwo
 - Analiza środowiska w oparciu o najlepsze praktyki dotyczące cyberbezpieczeństwa sprawdzająca stan poszczególnych urządzeń w środowisku i przypisujący im odpowiedni wynik bezpieczeństwa. System musi informować administratora o wykrytych lukach bezpieczeństwa oraz sposobie ich zabezpieczenia.
 - Musi istnieć możliwość tworzenia własnych polityk bezpieczeństwa w oparciu o wzorce dla poszczególnych urządzeń.
 - Stała analiza środowiska IT umożliwiająca wykrycie ataku ransomware na podstawie analizy posiadanych danych.
 - Możliwość przypisania dedykowanych ról dla poszczególnych administratorów.
- Wspierane urządzenia
 - Urządzenie Producenta dostarczane w ramach postępowania
 - Posiadane przez Zamawiającego serwery, urządzenia pamięci masowych, przełączniki sieciowe, przełączniki SAN, rozwiązania HCI, deduplikatory Producenta oferowanego urządzenia (jeśli takie są w posiadaniu Zamawiającego)
- Wirtualny asystent
 - Wbudowana w platformę funkcjonalność wirtualnego asystenta w oparciu o algorytmy GenAI przy dostępie do bazy wiedzy producenta urządzeń oraz analizie danych z monitoringu poszczególnych elementów infrastruktury;
- Możliwość rozszerzenia funkcjonalności
 - Możliwość rozbudowy systemu o zintegrowane i dodatkowe płatne moduły do monitoringu aplikacji oraz zarządzania incydentami w ramach infrastruktury IT.
- Inne
 - Oferowana platforma musi posiadać dedykowaną aplikację na urządzenia iOS oraz Android

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 spełnienie normy co najmniej Epeat Silver według normy wprowadzonej w 2019 roku - Wykonawca złoży dokument potwierdzający spełnianie wymogu.

- Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Microsoft Windows Server 2019, Microsoft Windows Server 2022.

Dokumentacja użytkownika:

- Zamawiający wymaga dokumentacji w języku polskim lub angielskim.
- Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.

Warunki gwarancji:

- Zamawiający wymaga zapewnienia gwarancji Producenta z zakresu ciągłości wdrażanej technologii na okres min. 24 miesiące (nie dotyczy gwarancji Wykonawcy).
- Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie i przez Internet.
- Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania Producenta, w tym także sprzedanego oprogramowania.
- Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy.
- 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 zakończenia diagnostyki.
- Naprawa ma się odbyć w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę.
- 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.
- Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wsparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego.
- Możliwość rozszerzenia gwarancji producenta o usługę diagnostyki sprzętu na miejscu w przypadku awarii. Charakterystyka usługi diagnostyki:
 - Możliwości utworzenia zgłoszenia 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.
- Wymagane dołączenie do protokołu odbioru oświadczenia **Producenta** potwierdzające, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta.

System operacyjny:

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

- Licencja musi uprawniać do uruchamiania serwerowego systemu operacyjnego w środowisku fizycznym i dwóch 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 zapora internetowa (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.

Oprogramowanie do wykonywania kopii zapasowych

Zamawiający wymaga dostarczenia licencji oprogramowania wraz ze wsparciem na min. 12 miesięcy z możliwością backupu min. 5 maszyn wirtualnych.

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 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 (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 VAIO, 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)

Wymaganie 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, 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 maszynę 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 jednoprzebiegowej kopii zapasowej dla Microsoft Exchange 2013 SP1 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 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.

Macierz

Procesor	Procesor 32 bit o taktowaniu nie mniejszym niż 1,7 GHz
Procesor liczba rdzeni	Nie mniej niż 4
Pamięć RAM	Nie mniej niż 2GB SODIMM DDR3
Pamięć Flash	Nie mniej niż 512MB
Liczba zatorów na dyski twarde	Minimum 4
Dyski twarde	Urządzenie musi być wyposażone w 2 dyski o pojemności 8TB znajdujące się na liście kompatybilności producenta
Obsługiwane dyski twarde	3.5” oraz 2.5” SATA oraz 2.5” SSD SATA
Pojemność dysków twardych	do 16 TB
Porty LAN 1 Gb/s	Minimum 2 RJ-45
Porty LAN 10 Gb/s	Minimum 1 SFP+
Diody LED	Status, LAN, HDD, USB

Porty USB 3.0	Minimum 4
Przyciski	Reset, Zasilanie
Typ obudowy	RACK, 1U
Dopuszczalna temperatura pracy	od 0 do 40° C
Wilgotność względna podczas pracy	5-95% R.H.
Zasilanie	Zasilacz o mocy min. 100 W
SPECYFIKACJA OPROGRAMOWANIA	
Agregacja taczy	tak
Obsługiwane systemy plików	Dyski wewnętrzne: EXT4 Dyski zewnętrzne: EXT3, EXT4, NTFS, FAT32, HFS+
Możliwość podłączenia karty WLAN na USB	Tak
Łączenie usług z interfejsem	Tak
Szyfrowanie wolumenów	Tak, min AES 256
Szyfrowanie dysków zewnętrznych	Tak
Zarządzanie dyskami	Pojedynczy Dysk, RAID 0, 1, 5, 6, 10, 5+Hot Spare Rozszerzanie pojemności Online RAID Migracja poziomów Online RAID HDD S.M.A.R.T. Skanowanie uszkodzonych bloków (pliku) Przywracanie macierzy RAID Obsługa map bitowych Globalny Hot Spare, Pula pamięci masowej
Wbudowana obsługa iSCSI	Multi-LUNs na Target Obsługa LUN Mapping & Masking Obsługa SPC-3 Persistent Reservation Obsługa MPIO & MC/S, Migawka / kopia zapasowa iSCSI LUN
Zarządzanie prawami dostępu	Ograniczenie dostępnej pojemności dysku dla użytkownika, Importowanie listy użytkowników, Zarządzanie kontami użytkowników, Zarządzanie grupą użytkowników, Zarządzanie współdzieleniem w sieci, Tworzenie użytkowników za pomocą makr, Obsługa zaawansowanych uprawnień dla podfolderów, Windows ACL,
Obsługa Windows AD	Logowanie użytkowników do domeny poprzez CIFS/SMB, AFP, FTP oraz menadżera plików sieci Web Funkcja serwera LDAP,
Funkcje backup	Oprogramowanie do tworzenia kopii bezpieczeństwa producenta urządzenia dla systemów Windows, backup na zewnętrzne dyski twarde,
Współpraca z zewnętrznymi dostawcami usług chmury	Przynajmniej: Amazon S3, Amazon Glacier, Microsoft Azure, Google Cloud Storage, Dropbox,

Darmowe aplikacje na urządzenia mobilne	Monitoring / Zarządzanie / Współdzielenie plików / obsługa kamer / Odtwarzacz muzyki Dostępne na systemy iOS oraz Android
Minimum obsługiwane serwery	Serwer plików Serwer FTP Serwer WEB Serwer baz danych MySQL Serwer kopii zapasowych Serwer multimedialny UpnP Serwer pobierania (Bittorrent / http / FTP) Serwer Monitoringu
VPN	VPN client / VPN server. Obsługa PPTP, OpenVPN, L2TP
Konteneryzacja	Możliwość uruchomienia wirtualnych kontenerów dla LXD i Docker
Administracja systemu	Połączenia http/HTTPS Powiadamianie przez e-mail (uwierzytelnianie SMTP) Powiadamianie przez SMS DDNS oraz zdalny dostęp w chmurze SNMP (v2 & v3) Obsługa UPS z zarządzaniem SNMP (USB) Obsługa sieciowej jednostki UPS Monitor zasobów Kosz sieciowy dla CIFS/SMB oraz AFP Monitor zasobów systemu w czasie rzeczywistym Rejestr zdarzeń System plików dziennika Całkowity rejestr systemowy (poziom pliku) Zarządzanie zdarzeniami systemowymi, rejestr, bieżące połączenie użytkowników on-line Aktualizacja oprogramowania Możliwość ręcznej aktualizacji oprogramowania Ustawienia: Backup, przywracania, resetowania systemu
Zabezpieczenia	Filtracja IP Ochrona dostępu do sieci z automatycznym blokowaniem Połączenie HTTPS FTP z SSL/TLS (Explicit) Obsługa SFTP (tylko admin) Szyfrowanie AES 256-bit Szyfrowana zdalna replikacja (Rsync poprzez SSH) Import certyfikatu SSL Powiadomienia o zdarzeniach za pośrednictwem Email i SMS
Możliwość instalacji dodatkowego oprogramowania	Tak, sklep z aplikacjami; możliwość instalacji z paczek *.QPKG
Montaż	Do urządzenia należy dołączyć szyny montażowe

III. OPZ dla UPS-serwer – 2 sztuki

PARAMETR	CECHA/WARTOŚĆ/WŁAŚCIWOŚĆ
----------	--------------------------

<i>Minimalne wymagania techniczne dla jednostki UPS</i>	<p>Moc znamionowa jednostki nie mniej niż 2700W / 3kVA Montowany w szafie RACK z kompletem uchwytów Technologia Double Conversion (On-Line)</p> <p>Temperatura eksploatacji 0 - 40 °C</p> <ul style="list-style-type: none"> • Wilgotność względna podczas pracy 0 - 95 % • Wysokość n.p.m. podczas pracy 0-3000m, powyżej 2000m n. p. m. następuje obniżenie wartości znamionowych • Hałas słyszalny w odległości 1 m od powierzchni urządzenia do 50dBA • Rozpraszanie ciepła w trybie online 90.0BTU/godz. • Klasa energetyczna sprzętu przeciwprzepięciowego 600 Dżule • Możliwość zimnego startu • automatyczne włączenie UPS-a po powrocie zasilania
<i>Parametry wejściowe</i>	<ul style="list-style-type: none"> • Nominalne napięcie wejściowe 220V, 230V, 240V • Zakres częstotliwości wejściowej: 40-70 Hz • Typ gniazda wejściowego: IEC-320 C20 • Zmienny zakres napięcia wejściowego w trybie podstawowym 110- 285V
<i>Parametry wyjściowe</i>	<ul style="list-style-type: none"> • Napięcie wyjściowe 220V, 230V, 240V • Zniekształcenia napięcia poniżej 3% dla obciążeń liniowych oraz poniżej 6% dla obciążeń nieliniowych • Częstotliwość na wyjściu zsynchronizowana z siecią zasilającą 50/60 Hz. (±3Hz dla zasilania z sieci lub ±0.1Hz dla zasilania z baterii) • Typ przebiegu sinusoida • Złącza/gniazda wyjściowe 6 szt. IEC 320 C13 1 szt. IEC 320 C19
<i>Akumulatory i czas podtrzymania</i>	<ul style="list-style-type: none"> • Typ akumulatora bezobsługowy szczelny akumulator kwasowo-ołowiowy z elektrolitem w postaci żelu • Czas autonomii pracy przy zasilaniu akumulatorowym: 2 minuty 54 sekundy dla pełnego obciążenia 10 minut 53 sekundy dla połowy obciążenia • Typowy czas ładowania 4 godziny • Oczekiwana żywotność akumulatora (lata) 4 – 6 • automatyczny test akumulatora

Komunikacja i zarządzanie	<ul style="list-style-type: none"> • Porty komunikacyjne: RS-232 Serial, USB, Smart Slot • Dostarczyć zasilacz UPS wraz z kompatybilną kartą zarządzania sieciowego • Moduł WEB/SNMP obsługiwane protokoły komunikacyjne: IP v.6 SNMP v.3 Modbus TCP • Panel sterowania: Wielofunkcyjna konsola sterownicza i informacyjna LCD Alarm dźwiękowy: Alarm przy zasilaniu akumulatora: alarm przy bardzo niskim poziomie naładowania akumulatora: konfigurowalne opóźnienia. • Awaryjny wyłącznik zasilania (EPO)
Certyfikaty, zgodności	<ul style="list-style-type: none"> • Znak CE, RoHS, REACH
Oprogramowanie	<ul style="list-style-type: none"> • Dostępne oprogramowanie do zarządzania/monitoringu (niektóre wersje odpłatne) z VMware® ESXi (VMware® ESXi Server 6.5 Update 3 (vMA 6.5), VMware® ESXi Server 6.5 Update 2 (vMA 6.5)); Microsoft® Hyper-V (Windows® Hyper-V Server 2019, 2012 R2); Windows® Server 2019, 2016, 2012; Windows® 10, 7; Red Hat® Enterprise Linux; SUSE® Linux®. • Dostarczyć wraz z 3 letnim wsparciem technicznym oraz aktualizacjami. • firmware dla karty sieciowej.

IV. OPZ dla UPS-komputer – 8 sztuk

Parametr	CECHA/WARTOŚĆ/WŁAŚCIWOŚĆ
Minimalne wymagania techniczne dla jednostki UPS	<p>Moc znamionowa jednostki nie mniej niż 400W / 650VA</p> <p>Topologia offline</p> <p>Temperatura eksploatacji 0 - 40 °C</p> <p>Wilgotność względna podczas pracy 0 - 90 %</p> <p>Wysokość n.p.m. podczas pracy 0-3000 m</p> <p>Klasa energetyczna sprzętu przeciwprzepięciowego 310 Dżule</p> <p>Zabezpieczenie przeciwprzepięciowe: bezpiecznik minimum 7A</p>
Parametry wejściowe	Nominalne napięcie wejściowe 230V

	<p>Częstotliwość wejściowa 47/63 Hz +/-3 Hz (automatyczne wykrywanie).</p> <p>Standard wtyczki: Francuska/Belgijska.</p> <p>Zmienny zakres napięcia wejściowego w trybie podstawowym 180 - 266V.</p>
Parametry wyjściowe	<p>Napięcie wyjściowe 230V</p> <p>Zniekształcenia napięcia wyjściowego poniżej 8%</p> <p>Częstotliwość na wyjściu (zsynchronizowana z siecią zasilającą) 47/63Hz +/- 3 Hz</p> <p>Power factor: minimum 0.6</p> <p>Typ przebiegu: Schodkowa aproksymacja sinusoidy</p> <p>Złącza/gniazda wyjściowe:</p> <p>8 gniazd francuskich/belgijskich: 6 z zabezpieczeniem przeciwprzepięciowym oraz podtrzymaniem zasilania, 2 z zabezpieczeniem przeciwprzepięciowym.</p> <p>1 gniazdo USB-A 2.4A.</p>
Akumulatory i czas podtrzymania	<p>Typ akumulatora bezobsługowy szczelny akumulator kwasowo-ołowiowy z elektrolitem w postaci żelu.</p> <p>Czas autonomii:</p> <p>2 minuty 37 sekund dla pełnego obciążenia</p> <p>10 minut dla połowy obciążenia.</p> <p>Typowy czas ładowania 16 godzin.</p> <p>Oczekiwana żywotność akumulatora (lata) 2 – 5</p> <p>Baterie wymieniane na gorąco.</p>
Komunikacja i zarządzanie	<p>Diody statusu LED: praca na baterii, on line, alert wymiany baterii</p> <p>Alarm dźwiękowy: Praca na baterii, niski poziom naładowania baterii, wyłączenie baterii, zastępcza bateria wykryta.</p>
Certyfikaty, zgodności oraz gwarancja	<p>Znak C, CE, EAC, CSA, GOST, UL 1778, VDE, RoHS, REACH</p>
Oprogramowanie	<p>Oprogramowanie do zarządzania zasilaczami UPS do bezpiecznego wyłączania i zarządzania energią dla komputerów stacjonarnych, serwerów i stacji roboczych, wykorzystujące dedykowane połączenia szeregowo lub USB i oferujące:</p> <p>Monitorowania i zarządzania zasilaczy UPS.</p>

	Bezobsługowego, bezpiecznego wyłączenia podczas problemów z zasilaniem.
--	---

V. OPZ dla urządzenie sieciowe typu switch – 2 sztuki.

Przełącznik musi być dedykowanym urządzeniem sieciowym o wysokości 1U przystosowanym do montowania w szafie Rack.
Przełącznik musi posiadać 24 porty pozwalających na obsadzenie modułami optycznymi SFP+ 1/10 Gbps.
Przełącznik musi posiadać nie mniej niż 2 wbudowane porty uplink 100 Gigabit Ethernet.
Musi istnieć możliwość wykorzystania interfejsu 100 GbE jako 4x10GbE lub 4x25 GbE.
Przełącznik musi umożliwiać rozbudowę o nie mniej niż 4 porty 10/25 Gigabit Ethernet SFP+.
Przełącznik musi wspierać metodę przełączania store-and-forward.
Przełącznik musi umożliwiać stworzenie stosu (w postaci pętli) liczącego nie mniej niż 10 urządzeń. Do łączenia w stos mogą zostać zastosowane wbudowane interfejsy 100 Gigabit Ethernet. W ramach urządzeń, z którymi może tworzyć stos muszą być urządzenia wspierające PoE oraz urządzenia wspierające prędkości portów 1 / 2,5/5/10Gbps.
Stos musi być odporny na awarie, tzn. przełącznik kontrolujący pracę stosu (master) musi być automatycznie zastąpiony przełącznikiem pełniącym rolę backup'u – wybór przełącznika backup nie może odbywać się w momencie awarii przełącznika master.
Przełącznik musi posiadać dwa wymienne zasilacze AC. Urządzenie musi posiadać co najmniej 2 moduły wentylacji. Zarówno zasilacz, jak i moduł wentylacji muszą posiadać możliwość wymiany podczas pracy urządzenia (hot swap).
Przełącznik musi być wyposażony w port konsoli oraz dedykowany interfejs Ethernet do zarządzania OOB (out-of-band).
Przełącznik musi być wyposażony w nie mniej niż 20 GB storage oraz 4 GB pamięci DDR4.
Zarządzanie urządzeniem musi odbywać się za pośrednictwem interfejsu linii komend (CLI), przez port konsoli, telnet, ssh.
Wydajność przełączania nie może być niższa niż 1080 Gbps (bidirectional). Przełącznik posiadać możliwość obsługi co najmniej 112 000 adresów MAC.
Przełącznik musi obsługiwać ramki Jumbo (9216 bajtów).
Przełącznik musi obsługiwać sieci VLAN zgodne z IEEE 802.1q w ilości nie mniejszej niż 4093.
Urządzenie musi obsługiwać agregowanie połączeń zgodne z IEEE 802.3ad - nie mniej niż 128 grup LAG, nie mniej niż 16 portów w grupie.
Przełącznik musi obsługiwać protokół Spanning Tree i Rapid Spanning Tree, zgodnie z IEEE 802.1D-2004, a także Multiple Spanning Tree zgodnie z IEEE 802.1Q-2003 (nie mniej niż 64 instancje MSTP).
Przełącznik musi obsługiwać protokół LLDP oraz LLDP-MED.
Urządzenie musi posiadać możliwość obsługi 128 000 prefiksów unicast IPv4.
Urządzenie musi obsługiwać routing statyczny.
Urządzenie musi posiadać możliwość rozbudowy licencji o obsługi protokołu VRRP, protokołów routingu dynamicznego OSPFv2/v3 oraz routingu multicast w postaci PIM-SM, PIM-SSM, PIM-DM. Licencja nie jest przedmiotem niniejszego postępowania.
Urządzenie musi posiadać możliwość rozbudowy licencji o funkcję MacSec, np. poprzez zastosowanie licencji. Licencja nie jest przedmiotem niniejszego postępowania.

Urządzenie musi posiadać możliwość rozbudowy funkcji, np. poprzez zastosowanie licencji, o obsługę protokołów routingu dynamicznego IS-IS, BGP oraz MBGP. Licencja nie jest przedmiotem niniejszego postępowania.
Urządzenie musi wspierać EVPN-VXLAN L2 GW w zakresie active-active multi-homing oraz proxy arp i arp suppression.
Urządzenie musi posiadać mechanizmy priorytetyzowania i zarządzania ruchem sieciowym (QoS) w warstwie 2 i 3. Klasyfikacja ruchu musi odbywać się w zależności od co najmniej: interfejsu, typu ramki Ethernet, sieci VLAN, priorytetu w warstwie 2 (802.1p), adresów MAC, adresów IP, wartości pola ToS/DSCP w nagłówkach IP, portów TCP i UDP. Urządzenie musi obsługiwać sprzętowo nie mniej niż 12 kolejek per port fizyczny (8 unicast i 4 multicast).
Urządzenie musi obsługiwać mechanizm Weighted Random Early Detection (WRED).
Urządzenie musi obsługiwać filtrowanie ruchu co najmniej na poziomie portu i sieci VLAN dla kryteriów z warstw 2-4. W regułach filtrowania ruchu musi być dostępny mechanizm zliczania dla zaakceptowanych lub zablokowanych pakietów. Musi być dostępna funkcja edycji reguł filtrowania ruchu na samym urządzeniu.
Przełącznik musi obsługiwać takie mechanizmy bezpieczeństwa jak limitowanie adresów MAC, Dynamic ARP Inspection, DHCP snooping, IP Source Guard.
Urządzenie musi obsługiwać protokół SNMP (wersje 2c i 3), oraz grupy RMON 1, 2, 3, 9. Musi być dostępna funkcja kopiowania (mirroring) ruchu na poziomie portu i sieci VLAN.
Architektura systemu operacyjnego urządzenia musi posiadać budowę modułową (poszczególne moduły muszą działać w odseparowanych obszarach pamięci), m.in. moduł przekazywania pakietów, odpowiedzialny za przełączanie pakietów musi być oddzielony od modułu routingu IP, odpowiedzialnego za ustalanie tras routingu i zarządzanie urządzeniem.
Urządzenie musi posiadać system montażowy producenta.
Urządzenie musi posiadać dwa kable zasilające AC z wtyczką UPS (C14).
Urządzenie musi być wyposażone w we wkładki, Zamawiający podaje odpowiednią liczbę w części dotyczącej usług.
Urządzenie musi posiadać mechanizm szybkiego odtwarzania systemu i przywracania konfiguracji. Pomoc techniczna oraz szkolenia z produktu muszą być dostępne w Polsce. Usługi te świadczone być muszą w języku polskim.
Całość dostarczanego sprzętu i oprogramowania musi pochodzić z autoryzowanego przez producenta kanału sprzedaży, na terenie Unii Europejskiej – do oferty należy dołączyć oświadczenie producenta lub autoryzowanego dystrybutora sprzętu i oprogramowania poświadczające pochodzenie sprzętu z autoryzowanego kanału sprzedaży.
Wymagane jest także zapewnienie przeszkolenia z zakresu konfiguracji i zarządzania urządzeniem. Szkolenie musi być przeprowadzone dla min. 2 osób w języku polskim i musi obejmować praktyczne ćwiczenia na środowisku Zamawiającego.
Wykonawca musi posiadać stopień najwyższy stopień certyfikacji i partnerstwa oferowanego producenta urządzeń.
Wymagane jest dostarczenie 2 sztuk przełączników.