PI.272.23.2024

Załącznik nr 1 do SWZ

Opis Przedmiotu Zamówienia

dla zamówienia pn. Dostawa i wdrożenie rozbudowy serwera w ramach projektu Cyberbezpieczny Powiat Lwówecki

1. Wykonawca dostarczy przedmiot zamówienia pod adres:

Starostwo Powiatowe w Lwówku Śląskim

Ul. Szpitalna 4

59-600 Lwówek Śląski

Pomieszczenia na I piętrze (brak windy)

1. Wykonawca pokrywa koszty transportu, odpowiada za prawidłowe warunki transportu oraz ponosi koszty usunięcia ewentualnych uszkodzeń podczas dostawy. Zapewnia rozładunek oraz wniesienie do wskazanych pomieszczeń. Ponadto zmontuje, zamontuje i uruchomi wskazane elementy dostawy.
2. Wykonawca przed rozpoczęciem dostaw jest zobowiązany do opracowania i przekazania przedstawicielowi Zamawiającego kalendarza dostaw składającego się z listy dostarczanego sprzętu, szacowanej daty wysyłki i dostawy. Ponadto Wykonawca poinformuje Zamawiającego o nadaniu przesyłki oraz przekaże informacje niezbędne do śledzenia przesyłki.
3. Dostawa obejmuje sprzęt nowy, nie używany, nie powystawowy, nie polizingowy, nie po regeneracji i nie po serwisowy.
4. Na elementy oznaczone \* Wykonawca udzieli gwarancji nie krótszej niż **12 miesięcy** na przedmiot zamówienia, o ile w ofercie nie przyjęto wydłużenia okresu gwarancji, co jest kryterium oceny.
5. Wykonawca może powierzyć wykonanie części zamówienia podwykonawcom. Wykonawca zobowiązany jest wskazać w ofercie części zamówienia, których wykonanie zamierza powierzyć podwykonawcom.
6. Wykonawca dołączy do oferty przedmiotowe środki dowodowe pod postacią karty katalogowej oferowanego produktu wraz z potwierdzeniem uzyskania wymaganego limitu punktów benchmark w jednym z wyszczególnionych w SWZ testów.
7. W pozycjach wymaganych Wykonawca dołączy jako przedmiotowy środek dowodowy do oferty zarchiwizowane potwierdzenie uzyskania wymaganej liczby punktów benchmark w testach SPECrate2017\_int\_base przez procesor zainstalowany w urządzeniu. Potwierdzenie nie może być starsze niż 5 dni przed złożenia oferty. Wyniki testów są publikowane na stronie [www.spec.org](http://www.spec.org/)
8. Zamawiający w opisie przedmiotu zamówienia nie uwzględnia aspektów społecznych, środowiskowych oraz etykiety.
9. Dostawy objęte zamówieniem nie będą się powtarzać ani podlegać wznowieniu.
10. Zamówienie obejmuje sprzęt komputerowy przeznaczony do celów edukacyjnych co Zamawiający potwierdzi przez wystawienie na wniosek Wykonawcy wymaganych oświadczeń.
11. Wykonawca pokrywa wszelkie niewymienione koszty niezbędne do realizacji przedmiotu zamówienia.
12. Termin realizacji zamówienia **60 dni** od podpisania umowy.
13. Zakres tolerancji parametrów oraz kryterium równoważności dla poniższej specyfikacji:

W postępowaniu określono minimalne wymagane parametry Zamawiający nie określa górnej granicy sprzętu jaki może zaoferować wykonawca. Za równoważne będą uważane również urządzenia i materiały, których parametry odbiegają w zakresie - 10% (-1% dla wartości przekątnych ekranu) od podanych w dokumentacji z jednoczesnym zachowaniem cech umożliwiających ich zastosowanie w projektowanej lokalizacji, pod względem parametrów technicznych, użytkowych oraz eksploatacyjnych ma w szczególności zapewnić uzyskanie parametrów nie gorszych od założonych w OPZ.

1. Zamawiający informuje, że przedmiotem zamówienia jest rozbudowa istniejącej infrastruktury, Opis Przedmiotu Zamówienia został sporządzony w celu uzyskania kompatybilności z istniejącymi rozwiązaniami. Zamawiający określił swoje wymagania w sposób pozwalający na uzyskanie optymalnych efektów i spełnienie potrzeb.
2. Zakres równoważności oprogramowania systemowego oraz pakietów biurowych (dotyczy wszystkich zapisów poniższej specyfikacji):

Z uwagi na fakt, utrzymania standaryzacji oprogramowania i pełnej jego kompatybilności w projektowanej lokalizacji, w opisie przedmiotu zamówienia wskazano znak towarowy firmy Microsoft. W oparciu o art. 99 ust. 5 Ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych (Dz.U. z 2023 r poz. 1605) wskazano w OPZ, znaki towarowe firmy Microsoft jako wzorzec funkcjonalno-jakościowy przedmiotu zamówienia.

Oznacza to tym samym, że Zamawiający dopuszcza i uzna za równoważne złożenie oferty na oprogramowanie operacyjne oraz służące do tworzenia i edycji dokumentów, o parametrach funkcjonalnych i jakościowych tożsamych z parametrami oprogramowania określonego we wzorcu, o ile jednocześnie zostaną zachowane pozostałe wymagania, określone w specyfikacji i zaoferowane oprogramowanie będzie w pełni i poprawnie funkcjonowało z posiadanym i użytkowanym przez Zamawiającego oprogramowaniem tj.:

• Pakiet zabezpieczenia antywirusowego firmy ESET

• System elektronicznego obiegu dokumentów El-Dok

• Pakiety oprogramowania do podpisu kwalifikowanego ProCertum i Szafir

• System Informacji Oświatowej VULCAN

• Aplikacje geodezyjne Geo info Mapa, GI Ośrodke, Delta, TSL,

• Aplikacje księgowo kadrowe: Softres Płace, Księgowość, Środki Trwałe, Płatnik, Kadry. Inwentaryzacja, Plan B

• Pakiet Legislator

• ZOOM

System operacyjny powinien zawierać zintegrowane rozwiązania pozwalające na funkcjonowanie w sieci wewnętrznej urzędu oraz możliwość dostępu do Internetu.

Możliwość tworzenia wielu kont użytkowników o różnym poziomie dostępu na urządzeniu (administrator i użytkownicy).

Zamawiający nie dopuszcza zaoferowania pakietów biurowych, programów i planów licencyjnych opartych o stałych cyklicznych opłat w okresie używania zakupionego produktu (cyklicznych abonamentów). Opłata licencyjna musi być poniesiona jednorazowo (licencja wieczysta).

Licencje na oprogramowanie biurowe muszą pozwalać na przenoszenie oprogramowania pomiędzy stacjami roboczymi (np. w przypadku wymiany stacji roboczej).

Zamawiający wymaga, aby wszystkie elementy oprogramowania systemu operacyjnego i pakietu biurowego posiadały Interfejs użytkownika w pełnej polskiej wersji językowej.

Możliwość automatycznej instalacji komponentów pakietu. Klucz licencyjny w wersji fizycznej (naklejka, karta, pudełko) lub zestawu licencji w wersji elektronicznej.

Oprogramowanie równoważne musi być kompatybilne i w sposób niezakłócony współdziałać z ww. programami.

Możliwość zintegrowania uwierzytelnienia użytkowników z usługą katalogową (Active Directory).

Tworzenie i edycja dokumentów elektronicznych w ustalonym formacie, który spełnia następujące warunki:

1) posiada kompletny i publicznie dostępny opis formatu,

2) Posiada zdefiniowany układ informacji w postaci XML,

3) Umożliwia wykorzystanie schematów XML,

4) Wspiera w swojej specyfikacji podpis elektroniczny w formacie XADES,

5) Możliwość automatycznego odzyskiwania dokumentów elektronicznych w wypadku nieoczekiwanego zamknięcia aplikacji, np. w wyniku wyłączenia zasilania komputera,

6) Prawidłowe odczytywanie i zapisywanie danych w dokumentach w formatach: DOC, DOCX, XLS, XLSX, XLSM, PPT, PPTX, MDB, ACCDB, w tym obsługa formatowania, makr, formuł i formularzy w plikach wytworzonych w MS Office 2003, MS Office 2007, MS Office 2010, MS Office 2013 i MS Office 2016, bez utraty danych oraz bez konieczności reformatowania dokumentów,

7) Wszystkie aplikacje w pakiecie oprogramowania biurowego muszą być integralną częścią tego samego pakietu, współpracować ze sobą (osadzania i wymiana danych, posiadać jednolity interfejs oraz ten sam jednolity sposób obsługi),

8) Edytor tekstowy powinien zapewnić możliwość tworzenia dokumentów dostępnych cyfrowo. Powinien zawierać narzędzie „inspektor dostępności” sprawdzające część wymagań dostępności w wytworzonym dokumencie. Edytor powinien pozwalać również na opisywanie osadzonych wszelakich obiektów w tekście (np.: tabela, wykres, grafika itp.) tekstem alternatywnym. Zgodnie z wytycznym zawartymi w Ustawa z 4 kwietnia 2019r. o dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych

Pakiet zintegrowanych aplikacji biurowych musi składać się co najmniej z następujących aplikacji:

1) edytora tekstów,

2) arkusza kalkulacyjnego,

3) narzędzia do przygotowywania i prowadzenia prezentacji,

4) narzędzia do zarządzania informacją osobistą (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami),

5) narzędzie do komunikacji głosowej i wideo oraz telekonferencji zbiorowej,

6) narzędzie do tworzenia publikacji drukowanych.

Jednocześnie Zamawiający zakłada, że wykazanie równoważności złożonej oferty leży po stronie Wykonawcy i – w razie wątpliwości – powinno zostać udokumentowane w możliwie najbardziej obiektywny sposób.

W przypadku zaoferowania przez Wykonawcę oprogramowania do tworzenia i edycji dokumentów innego niż MS Office - oświadczenie tego Wykonawcy zostanie przesłane do producenta ww. oprogramowania, celem jego weryfikacji

1. Rozbudowa serwera Fujitsu RX2540 M5

| **Lp.** | **Pozycja** | **Minimalne wymagania** |
| --- | --- | --- |
|  | Parametry komponentu\* | * Wykonawca dostarczy i zainstaluje kartę HBA SAS w posiadanym przez Zamawiającego serwerze Fujitsu RX2540 M5 * Karta musi posiadać minimum 2 porty zewnętrzne SAS SFF-8644 * Złącze minimum PCIe 3.0 x8 * Karta przystosowana do instalacji w zatoce o pełnej wysokości oraz w zatoce o niskim profilu |
|  | Gwarancja \* | Minimum 12 miesięcy z możliwością wydłużenia do okresu 36 miesięcy punktowane jako poza cenowe kryterium wyboru. |

1. Odnowienie gwarancji, opieki serwisowej dla serwera Fujitsu RX2540 M5

| **Lp.** | **Pozycja** | **Minimalne wymagania** |
| --- | --- | --- |
|  | Zakres | 1. Serwer Fujitsu PY RX2540 M5, SN: YMSQ010984 |
|  | Okres gwarancji | Co najmniej 2 lata |
|  | Poziom gwarancji | Gwarancji producenta serwera w trybie on-site z gwarantowaną wizytą technika serwisu i naprawą do końca następnego dnia od zgłoszenia. Naprawa realizowana przez producenta serwera lub autoryzowany przez producenta serwis. |

1. Serwer Typ A (2 szt.)

| **Lp.** | **Pozycja** | **Minimalne wymagania** |
| --- | --- | --- |
|  | Obudowa | * Typu RACK, wysokość maksymalnie 2U; * Szyny umożliwiające wysunięcie serwera z szafy stelażowej wraz z ramieniem porządkującym kable z tyłu obudowy; * Możliwość zainstalowania 16 dysków twardych hot plug 2,5”; * Możliwość zainstalowania fizycznego zabezpieczenia (np. na klucz lub elektrozamek) uniemożliwiającego fizyczny dostęp do dysków twardych; * Zainstalowane minimum 2 szt. dysków M.2 SSD 480GB skonfigurowane w RAID podpięte do sprzętowego kontrolera; * Możliwość zainstalowania dysku M.2 NVMe PCIe4.0 x4; * Możliwość zainstalowania dedykowanego wewnętrznego napędu blu-ray. * Możliwość zainstalowania dedykowanego wewnętrznego napędu LTO-8. |
|  | Płyta główna | * Dwuprocesorowa; * Wyprodukowana i zaprojektowana przez producenta serwera; * Możliwość instalacji procesorów 60-rdzeniowych; * Zainstalowany moduł TPM 2.0; * Minimum 6 złącz PCI Express generacji 5 w tym:   + 4 fizyczne złącza o prędkości x16;   + 2 fizyczne złącza o prędkości x8;   + Opcjonalnie możliwość uzyskania 2 złącz typu pełnej wysokości;   + Opcjonalnie możliwość uzyskania 9 aktywnych interfejsów PCI-e; * 32 gniazda pamięci RAM; * Obsługa minimum 8 TB pamięci RAM DDR5; * Wsparcie dla technologii:   + Memory Scrubbing;   + SDDC;   + ECC;   + Memory Mirroring;   + ADDDC; * Możliwość instalacji 2 dysków M.2 na płycie głównej (lub dedykowanej karcie PCI Express)  dyski nie mogą zajmować klatek dla dysków hot-plug. |
|  | Procesor | Dwa procesor minimum 16-rdzeniowe, architektura x86 - 64 bity, osiągający w testach SPECrate2017\_int\_base minimum 330 punktów w konfiguracji dwuprocesorowej. Wynik testu musi być opublikowany na stronie www.spec.org. |
|  | Pamięć RAM | * Minimum 256 GB pamięci RAM; * Minimum DDR5 Registered 4800MT/s; |
|  | Kontroler LAN | Interfejsy LAN, nie zajmujące żadnego z dostępnych slotów PCI Express:   * Co najmniej 5x 1Gbit Base-T; * Możliwość uzyskania dwóch interfejsów 100Gbit QSFP28 bez konieczności instalacji kart w slotach PCIe;   Interfejsy LAN zainstalowane w slotach PCI-e:   * Co najmniej 2x 10Gbit SFP+ obsadzone wkładkami MMF LC. |
|  | Kontroler I/O | * Kontroler SAS RAID dla dysków wewnętrznych posiadający 4GB pamięci cache, obsługujący poziomy RAID: 0,1,10,5,50,6,60 z podtrzymaniem pamięci cache w przypadku utraty zasilania; * Dwuportowa karta FC 16Gbps; |
|  | Porty | * Zintegrowana karta graficzna ze złączem VGA z tyłu serwera; * Minimum 1 porty USB 3.0 wewnętrzny; * Minimum 2 porty USB 3.0 dostępne z tyłu serwera; * Minimum 2 porty USB 3.0 na panelu przednim; * Opcjonalny port serial, możliwość wykorzystania portu serial do zarządzania serwerem; * Ilość dostępnych złącz USB nie może być osiągnięta poprzez stosowanie zewnętrznych przejściówek, rozgałęziaczy czy dodatkowych kart rozszerzeń zajmujących jakikolwiek slot PCI Express i/lub USB serwera. |
|  | Zasilanie, chłodzenie | * Redundantne zasilacze hotplug o sprawności 96% (tzw. klasa Titanium) o mocy minimum 900W; * Redundantne wentylatory hotplug. |
|  | Zarządzanie | * Wbudowane diody informacyjne lub wyświetlacz informujące o stanie serwera - system przewidywania, rozpoznawania awarii;   + informacja o statusie pracy (poprawny, przewidywana usterka lub usterka) co najmniej następujących komponentów:     - karty rozszerzeń zainstalowane w dowolnym  slocie PCI Express;     - procesory CPU;     - pamięć RAM z dokładnością umożliwiającą jednoznaczną identyfikację uszkodzonego modułu pamięci RAM;     - status karty zarządzającej serwera;     - wentylatory;     - bateria podtrzymująca ustawienia BIOS płyty głównej;     - zasilacze; * Zintegrowany z płytą główną serwera kontroler sprzętowy zdalnego zarządzania zgodny z IPMI 2.0 o funkcjonalnościach:   + Niezależny od systemu operacyjnego, sprzętowy kontroler umożliwiający pełne zarządzanie, zdalny restart serwera;   + Dedykowana karta LAN 1 Gb/s, dedykowane złącze RJ-45 do komunikacji wyłącznie z kontrolerem zdalnego zarządzania z możliwością przeniesienia tej komunikacji na inną kartę sieciową współdzieloną z systemem operacyjnym;   + Dostęp poprzez przeglądarkę Web, SSH;   + Zarządzanie mocą i jej zużyciem oraz monitoring zużycia energii;   + Zarządzanie alarmami (zdarzenia poprzez SNMP);   + Możliwość przejęcia konsoli tekstowej;   + Przekierowanie konsoli graficznej na poziomie sprzętowym oraz możliwość montowania zdalnych napędów i ich obrazów na poziomie sprzętowym (cyfrowy KVM);   + Obsługa serwerów proxy (autentykacja);   + Obsługa VLAN;   + Możliwość konfiguracji parametru Max. Transmission Unit (MTU);   + Wsparcie dla protokołu SSDP;   + Obsługa protokołów TLS 1.2, SSL v3;   + Obsługa protokołu LDAP;   + Synchronizacja czasu poprzez protokół NTP;   + Możliwość backupu i odtwarzania ustawień bios serwera oraz ustawień karty zarządzającej; * Oprogramowanie zarządzające i diagnostyczne wyprodukowane przez producenta serwera umożliwiające konfigurację kontrolera RAID, instalację systemów operacyjnych, zdalne zarządzanie, diagnostykę i przewidywanie awarii w oparciu o informacje dostarczane w ramach zintegrowanego w serwerze systemu umożliwiającego monitoring systemu i środowiska (m.in. temperatura, dyski, zasilacze, płyta główna, procesory, pamięć operacyjna); * Wbudowania w kartę zarządzającą (lub zainstalowana) pamięć flash dająca możliwość zdalnej reinstalacji systemu lub aplikacji z obrazów zainstalowanych w obrębie dedykowanej pamięci flash bez użytkowania zewnętrznych nośników lub kopiowania danych poprzez sieć LAN; * Serwer musi posiadać możliwość konfiguracji i wykonania aktualizacji BIOS, Firmware, sterowników serwera bezpośrednio z GUI (graficzny interfejs) karty zarządzającej serwera bez pośrednictwa innych nośników zewnętrznych i wewnętrznych poza obrębem karty zarządzającej. |
|  | Wsparcie dla systemów operacyjnych | Co najmniej dla:   * Microsoft Windows Server 2022; * Vmware vSphere 8.0; * Suse Linux Enterprise Server 15; * Red Hat Enterprise Linux 9, 8; * Microsoft Hyper-V Server 2019 |
|  | Gwarancja | * Minimum 5 lat gwarancji producenta serwera w trybie on-site z gwarantowaną wizytą technika serwisu i naprawą do końca następnego dnia od zgłoszenia. Naprawa realizowana przez producenta serwera lub autoryzowany przez producenta serwis. Dyski twarde nie podlegają zwrotowi organizacji serwisowej; * Funkcja zgłaszania usterek i awarii sprzętowych poprzez automatyczne założenie zgłoszenia w systemie helpdesk/servicedesk producenta sprzętu; * Firma serwisująca musi posiadać ISO 9001:2000 na świadczenie usług serwisowych; * Bezpłatna dostępność poprawek i aktualizacji BIOS/Firmware/sterowników dożywotnio dla oferowanego serwera – jeżeli funkcjonalność ta wymaga dodatkowego serwisu lub licencji producenta serwera, takowy element musi być uwzględniona w ofercie; * Możliwość odpłatnego wydłużenia gwarancji producenta do 7 lat w trybie onsite z gwarantowanym skutecznym zakończeniem naprawy serwera najpóźniej w następnym dniu roboczym od zgłoszenia usterki. |
|  | Wymagania dodatkowe | * Elementy, z których zbudowane są serwery muszą być produktami producenta tych serwerów lub być przez niego certyfikowane oraz całe muszą być objęte gwarancją producenta, o wymaganym w specyfikacji poziomie gwarancji – wymagane na etapie realizacji oświadczenie wykonawcy lub producenta; * Serwer musi być fabrycznie nowy i pochodzić z oficjalnego kanału dystrybucyjnego w UE – wymagane na etapie realizacji oświadczenie wykonawcy lub producenta; * Ogólnopolska, telefoniczna infolinia/linia techniczna producenta serwera, w ofercie należy podać link do strony producenta na której znajduje się nr telefonu oraz maila na który można zgłaszać usterki; * W czasie obowiązywania gwarancji na sprzęt, możliwość po podaniu na infolinii numeru seryjnego urządzenia weryfikacji pierwotnej konfiguracji sprzętowej serwera, w tym model i typ dysków twardych, procesora, ilość fabrycznie zainstalowanej pamięci operacyjnej, czasu obowiązywania i typ udzielonej gwarancji; * Należy dostarczyć i wstępnie skonfigurować system zarządzania infrastrukturą IT. Musi być możliwość monitorowania stanu środowiska IT minimum dla oferowanych serwerów oraz macierzy. System zarządzania posiada jeden spójny interfejs GUI HTML do zarządzania całym oferowanym środowiskiem sprzętowym. System zarządzania opiera się o tzw. Virtual Appliance kompatybilny z platformą wirtualną VMware vSphere, Microsoft Hyper-V, KVM. System zarządzania umożliwia aktualizację oprogramowanie systemowego (firmware) na serwerach w zakresie wszystkich istotnych elementów sprzętowych min: BIOS, kontrolery RAID, kontrolery KVM, karty sieciowe. System zarządzania posiada wsparcie dla następujących mechanizmów komunikacji zewnętrznej: HTTPS, SNMP, IPMI. System zarządzania musi mieć możliwość wyeksportowania inwentarza środowiska co najmniej w postaci pliku CSV. * Możliwość aktualizacji i pobrania sterowników do oferowanego modelu serwera w najnowszych certyfikowanych wersjach bezpośrednio z sieci Internet za pośrednictwem strony www producenta serwera; * Możliwość pracy w pomieszczeniach o wilgotności w zawierającej się w przedziale 8 - 85 %; * Zgodność z normami: CB, RoHS, WEEE  oraz CE. |

1. Serwer Typ B (1 szt.)

| **Lp.** | **Pozycja** | **Minimalne wymagania** |
| --- | --- | --- |
|  | Obudowa | * Typu RACK, wysokość maksymalnie 1U; * Szyny umożliwiające wysunięcie serwera z szafy stelażowej wraz z ramieniem porządkującym kable z tyłu obudowy; * Możliwość zainstalowania 4 dysków twardych hot plug 2,5”; * Możliwość zainstalowania fizycznego zabezpieczenia (np. na klucz lub elektrozamek) uniemożliwiającego fizyczny dostęp do dysków twardych; * Zainstalowane minimum 2 szt. dysków SSD 480GB Hot-Plug DWPD>4; * Możliwość zainstalowania dysku M.2 NVMe bezpośrednio na płycie głównej; * Możliwość zainstalowania dedykowanego wewnętrznego napędu blu-ray. |
|  | Płyta główna | * Wyprodukowana i zaprojektowana do zastosowania w proponowanym urządzeniu przez producenta serwera; * Możliwość instalacji procesorów 8-rdzeniowych; * Wyposażona w moduł TPM 2.0; * Złącza PCI Express:   + Minimum 2 fizyczne złącza PCIe 5.0 o prędkości x8;   + Opcjonalnie możliwość uzyskania złącza typu pełnej wysokości; * 4 gniazda pamięci RAM; * Obsługa minimum 128 GB pamięci RAM DDR5 ECC; * Możliwość instalacji 2 dysków M.2 NVMe skonfigurowanych w RAID-1 na płycie głównej lub dedykowanej karcie PCI Express, dyski nie mogą zajmować klatek dla dysków hot-plug. |
|  | Procesor | Jeden procesor minimum 8-rdzeniowy, architektura x86 - 64 bity, osiągający w testach SPECrate2017\_int\_base minimum 57 punktów w konfiguracji jednoprocesorowej. Wynik testu musi być opublikowany na stronie www.spec.org. |
|  | Pamięć RAM | * Minimum 32 GB pamięci RAM; * Pamięci obsadzone w trybie dwukanałowym. |
|  | Kontroler LAN | Interfejsy LAN, nie zajmujące żadnego z dostępnych slotów PCI Express:   * 2x 1Gbit Base-T; |
|  | Kontroler I/O | * Kontroler SAS RAID dla dysków wewnętrznych, obsługujący poziomy RAID: 0,1,10; |
|  | Porty | * Zintegrowana karta graficzna ze złączem VGA z tyłu serwera; * Minimum 4x USB 3.2 Gen1 Type A wyprowadzone na tył obudowy * Minimum 2x USB 3.2 Gen1 Type A + minimum 1x USB3.2 Gen2x2 Type C wyprowadzone na przód obudowy * Minimum 5x SATA 6G * Opcjonalny port serial, możliwość wykorzystania portu serial do zarządzania serwerem; * Ilość dostępnych złącz USB/SATA nie może być osiągnięta poprzez stosowanie zewnętrznych przejściówek, rozgałęziaczy czy dodatkowych kart rozszerzeń zajmujących jakikolwiek slot PCI Express i/lub USB serwera. |
|  | Zasilanie, chłodzenie | * Redundantne zasilacze hotplug o sprawności 96% (tzw. klasa Titanium) o mocy minimum 500W; * Redundantne wentylatory hotplug. |
|  | Zarządzanie | * Wbudowane diody informacyjne lub wyświetlacz informujące o stanie serwera - system przewidywania, rozpoznawania awarii;   + informacja o statusie pracy (poprawny, przewidywana usterka lub usterka) co najmniej następujących komponentów:     - karty rozszerzeń zainstalowane w dowolnym  slocie PCI Express;     - procesory CPU;     - pamięć RAM z dokładnością umożliwiającą jednoznaczną identyfikację uszkodzonego modułu pamięci RAM;     - status karty zarządzającej serwera;     - wentylatory;     - bateria podtrzymująca ustawienia BIOS płyty głównej;     - zasilacze; * Zintegrowany z płytą główną serwera kontroler sprzętowy zdalnego zarządzania zgodny z IPMI 2.0 o funkcjonalnościach:   + Niezależny od systemu operacyjnego, sprzętowy kontroler umożliwiający pełne zarządzanie, zdalny restart serwera;   + Dedykowana karta LAN 1 Gb/s, dedykowane złącze RJ-45 do komunikacji wyłącznie z kontrolerem zdalnego zarządzania z możliwością przeniesienia tej komunikacji na inną kartę sieciową współdzieloną z systemem operacyjnym;   + Dostęp poprzez przeglądarkę Web, SSH;   + Zarządzanie mocą i jej zużyciem oraz monitoring zużycia energii;   + Zarządzanie alarmami (zdarzenia poprzez SNMP);   + Możliwość przejęcia konsoli tekstowej;   + Przekierowanie konsoli graficznej na poziomie sprzętowym oraz możliwość montowania zdalnych napędów i ich obrazów na poziomie sprzętowym (cyfrowy KVM);   + Obsługa serwerów proxy (autentykacja);   + Obsługa VLAN;   + Możliwość konfiguracji parametru Max. Transmission Unit (MTU);   + Wsparcie dla protokołu SSDP;   + Obsługa protokołów TLS 1.2, SSL v3;   + Obsługa protokołu LDAP;   + Synchronizacja czasu poprzez protokół NTP;   + Możliwość backupu i odtwarzania ustawień bios serwera oraz ustawień karty zarządzającej; * Oprogramowanie zarządzające i diagnostyczne wyprodukowane przez producenta serwera umożliwiające konfigurację kontrolera RAID, instalację systemów operacyjnych, zdalne zarządzanie, diagnostykę i przewidywanie awarii w oparciu o informacje dostarczane w ramach zintegrowanego w serwerze systemu umożliwiającego monitoring systemu i środowiska (m.in. temperatura, dyski, zasilacze, płyta główna, procesory, pamięć operacyjna); * Wbudowania w kartę zarządzającą (lub zainstalowana) pamięć flash dająca możliwość zdalnej reinstalacji systemu lub aplikacji z obrazów zainstalowanych w obrębie dedykowanej pamięci flash bez użytkowania zewnętrznych nośników lub kopiowania danych poprzez sieć LAN; * Serwer musi posiadać możliwość konfiguracji i wykonania aktualizacji BIOS, Firmware, sterowników serwera bezpośrednio z GUI (graficzny interfejs) karty zarządzającej serwera bez pośrednictwa innych nośników zewnętrznych i wewnętrznych poza obrębem karty zarządzającej. |
|  | Wsparcie dla systemów operacyjnych | Co najmniej dla:   * Microsoft Windows Server 2022; * Vmware vSphere 8.0; * Suse Linux Enterprise Server 15; * Red Hat Enterprise Linux 9, 8; * Ubuntu 22.04 |
|  | Gwarancja | * Minimum 5 lat gwarancji producenta serwera w trybie on-site z gwarantowaną wizytą technika serwisu i naprawą do końca następnego dnia od zgłoszenia. Naprawa realizowana przez producenta serwera lub autoryzowany przez producenta serwis. Dyski twarde nie podlegają zwrotowi organizacji serwisowej; * Funkcja zgłaszania usterek i awarii sprzętowych poprzez automatyczne założenie zgłoszenia w systemie helpdesk/servicedesk producenta sprzętu; * Firma serwisująca musi posiadać ISO 9001:2000 na świadczenie usług serwisowych; * Bezpłatna dostępność poprawek i aktualizacji BIOS/Firmware/sterowników dożywotnio dla oferowanego serwera – jeżeli funkcjonalność ta wymaga dodatkowego serwisu lub licencji producenta serwera, takowy element musi być uwzględniona w ofercie; * Możliwość odpłatnego wydłużenia gwarancji producenta do 7 lat w trybie onsite z gwarantowanym skutecznym zakończeniem naprawy serwera najpóźniej w następnym dniu roboczym od zgłoszenia usterki. |
|  | Wymagania dodatkowe | * Elementy, z których zbudowane są serwery muszą być produktami producenta tych serwerów lub być przez niego certyfikowane oraz całe muszą być objęte gwarancją producenta, o wymaganym w specyfikacji poziomie gwarancji – wymagane na etapie realizacji oświadczenie wykonawcy lub producenta; * Serwer musi być fabrycznie nowy i pochodzić z oficjalnego kanału dystrybucyjnego w UE – wymagane na etapie realizacji oświadczenie wykonawcy lub producenta; * Ogólnopolska, telefoniczna infolinia/linia techniczna producenta serwera, w ofercie należy podać link do strony producenta na której znajduje się nr telefonu oraz maila na który można zgłaszać usterki; * W czasie obowiązywania gwarancji na sprzęt, możliwość po podaniu na infolinii numeru seryjnego urządzenia weryfikacji pierwotnej konfiguracji sprzętowej serwera, w tym model i typ dysków twardych, procesora, ilość fabrycznie zainstalowanej pamięci operacyjnej, czasu obowiązywania i typ udzielonej gwarancji; * Należy dostarczyć i wstępnie skonfigurować system zarządzania infrastrukturą IT. Musi być możliwość monitorowania stanu środowiska IT minimum dla oferowanych serwerów oraz macierzy. System zarządzania posiada jeden spójny interfejs GUI HTML do zarządzania całym oferowanym środowiskiem sprzętowym. System zarządzania opiera się o tzw. Virtual Appliance kompatybilny z platformą wirtualną VMware vSphere, Microsoft Hyper-V, KVM. System zarządzania umożliwia aktualizację oprogramowanie systemowego (firmware) na serwerach w zakresie wszystkich istotnych elementów sprzętowych min: BIOS, kontrolery RAID, kontrolery KVM, karty sieciowe. System zarządzania posiada wsparcie dla następujących mechanizmów komunikacji zewnętrznej: HTTPS, SNMP, IPMI. System zarządzania musi mieć możliwość wyeksportowania inwentarza środowiska co najmniej w postaci pliku CSV. * Możliwość aktualizacji i pobrania sterowników do oferowanego modelu serwera w najnowszych certyfikowanych wersjach bezpośrednio z sieci Internet za pośrednictwem strony www producenta serwera; * Możliwość pracy w pomieszczeniach o wilgotności w zawierającej się w przedziale 8 - 85 %; * Zgodność z normami: CB, RoHS, WEEE  oraz CE. |

1. Serwerowe systemy operacyjne

Licencja na serwerowy system operacyjny musi uprawniać do zainstalowania serwerowego systemu operacyjnego w środowisku fizycznym (na 2 serwerach Typ A) oraz umożliwiać zainstalowanie 1000 instancji wirtualnych tego serwerowego systemu operacyjnego. Licencja musi zostać tak dobrana, aby była zgodna z zasadami licencjonowania producenta oraz pozwalała na legalne używanie na serwerach Typ A, które stanowią przedmiot zamówienia. Wymaga się, aby oferowane licencje umożliwiały korzystanie 65 użytkownikom.

| **Lp.** | **Serwerowy system operacyjny musi posiadać następujące, wbudowane cechy.** |
| --- | --- |
|  | Możliwość wykorzystania 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym. |
|  | Możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności do 64TB przez każdy wirtualny serwerowy system operacyjny. |
|  | Możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania 7000 maszyn wirtualnych. |
|  | 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. |
|  | Wbudowane wsparcie instalacji i pracy na wolumenach, które:   1. pozwalają na zmianę rozmiaru w czasie pracy systemu, 2. umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów, 3. umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów, 4. umożliwiają zdefiniowanie list kontroli dostępu (ACL). |
|  | 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 uruchamianie 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. |
|  | Dostępne dwa rodzaje graficznego interfejsu użytkownika:   1. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy, 2. Dotykowy umożliwiający sterowanie dotykiem na monitorach dotykowych. |
|  | Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe, |
|  | Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji. |
|  | Mechanizmy logowania w oparciu o:   1. Login i hasło, 2. Karty z certyfikatami (smartcard), 3. Wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM), |
|  | Możliwość wymuszania wieloelementowej dynamicznej kontroli dostępu dla: określonych grup użytkowników, zastosowanej klasyfikacji danych, centralnych polityk dostępu w sieci, centralnych polityk audytowych oraz narzuconych dla grup użytkowników praw do wykorzystywania szyfrowanych danych. |
|  | Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play). |
|  | Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu. |
|  | Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa. |
|  | Pochodzący od producenta systemu serwis zarządzania polityką dostępu do informacji w dokumentach (Digital Rights Management). |
|  | Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach. |
|  | Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:   1. Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC, 2. Usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji:    * 1. Podłączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną,      2. Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,      3. Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza.      4. Bezpieczny mechanizm dołączania do domeny uprawnionych użytkowników prywatnych urządzeń mobilnych opartych o iOS i Windows 8.1. 3. Zdalna dystrybucja oprogramowania na stacje robocze. 4. Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej 5. Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:    * 1. Dystrybucję certyfikatów poprzez http      2. Konsolidację CA dla wielu lasów domeny,      3. Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen,      4. Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509. 6. Szyfrowanie plików i folderów. 7. Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec). 8. Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów. 9. Serwis udostępniania stron WWW. 10. Wsparcie dla protokołu IP w wersji 6 (IPv6), 11. Wsparcie dla algorytmów Suite B (RFC 4869), 12. Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows, 13. Wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie do 1000 aktywnych środowisk wirtualnych systemów operacyjnych. Wirtualne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności. Mechanizmy wirtualizacji mają zapewnić wsparcie dla:     * 1. Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych,       2. Obsługi ramek typu jumbo frames dla maszyn wirtualnych.       3. Obsługi 4-KB sektorów dysków       4. Nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra       5. Możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API.       6. Możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk mode) |
|  | Możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta serwerowego systemu operacyjnego umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet. |
|  | Wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath). |
|  | Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego. |
|  | Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty. |
|  | Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF. |
|  | Zorganizowany system szkoleń i materiały edukacyjne w języku polskim. |

1. Macierz dyskowa (1 szt.)

| **Lp.** | **Pozycja** | **Minimalne wymagania** |
| --- | --- | --- |
|  | System | * System musi być dostarczony ze wszystkimi komponentami do instalacji w standardowej szafie rack 19” z zajętością maks. 2U w tej szafie. Każdy skonfigurowany moduł/obudowa musi posiadać układ nadmiarowy zasilania i chłodzenia, zapewniający bezprzerwową pracę macierzy bez ograniczeń czasowych w przypadku utraty redundancji w danym układzie (zasilania lub chłodzenia). Każdy moduł/obudowa powinien posiadać widoczne elementy sygnalizacyjne do informowania o stanie poprawnej pracy lub awarii. * Macierz musi umożliwiać takie podłączenie półek aby awaria lub/i usunięcie jednej z półek nie powodowało utraty dostępu do danych znajdujących się na pozostałych modułach. * Macierz musi obsługiwać  min. 160 dysków wykonanych w technologii hot-plug. * Macierz musi posiadać 4 porty SAS 12 Gb/s do podłączenia dodatkowych półek dyskowych. |
|  | Pojemność macierzy | * Co najmniej 11 szt. dysków minimum 1,9TB SSD-SAS |
|  | Kontrolery | * Macierz musi być dostarczona z zainstalowanymi minimum 2 kontrolerami. * Każdy z kontrolerów macierzy musi posiadać po minimum 32GB pamięci podręcznej Cache. * W przypadku awarii zasilania dane niezapisane na dyski, przechowywane w pamięci kontrolera muszą być zabezpieczone za pomocą podtrzymania bateryjnego przez 72 godziny lub jako zrzut na pamięć flash. * Macierz musi obsługiwać rozbudowę pamięci podręcznej cache dla operacji  odczytu o minimum 4TiB poprzez instalację dodatkowych modułów pamięci w kontrolerach lub wykorzystanie pojemności zainstalowanych dysków SSD. * Macierz musi obsługiwać wymianę kontrolera RAID bez utraty danych zapisanych na dyskach. * 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. * Każdy z kontrolerów RAID powinien posiadać dedykowany interfejs RJ-45 Ethernet obsługujący połączenia z prędkością minimum 1Gb/s dla zdalnej  komunikacji z oprogramowaniem zarządzającym i konfiguracyjnym macierzy. * Kontrolery macierzy muszą obsługiwać do 84 grup dyskowych w całym rozwiązaniu, bez konieczności wymiany dostarczonych kontrolerów. * Oferowana macierz musi mieć wyprowadzone 2 porty dualne FC 16Gbps / iSCSI 10Gbps (obsadzone modułami LC MMF) do dołączenia serwerów bezpośrednio lub do sieci SAN na każdy kontroler RAID. * Macierz musi umożliwiać dołożenie dodatkowych portów do transmisji danych na każdy kontroler RAID:   + 2x SAS 12 Gbps   + 4x iSCSI 25 Gbps SFP28   + 4x FC 32 Gbps   + 2x iSCSI 10Gbps Base-T   + 4x iSCSI 10Gbps SFP+ * Dołożenie portów jw. nie może powodować wymiany samych kontrolerów RAID w oferowanym rozwiązaniu a w przypadku konieczność licencjonowania tej funkcjonalności macierz ma być dostarczona z aktywną licencja na instalację i obsługę każdego z wymienionych protokołów transmisji danych. |
|  | Poziomy RAID | * Macierz musi zapewniać poziom zabezpieczenia danych na dyskach definiowany poziomami RAID:   + Raid-1   + Raid-10   + Raid-5   + Raid-6 * Obliczanie sum kontrolnych (kodów parzystości) dla grup dyskowych RAID5 i RAID6 musi być realizowane w sposób sprzętowy przez dedykowany układ w macierzy. * Macierz musi posiadać mechanizm tworzenia wirtualnej przestrzeni na dyskach macierzy wraz z wyliczaniem parzystości oraz podwójnej parzystości w celu zabezpieczenia danych. Mechanizm ten musi być przygotowany do optymalizacji procesów odtwarzania dysków pojemnościowych. * Macierz musi pozwalać na dynamiczną migrację pomiędzy poziomami RAID, czyli zmianę sposobu zabezpieczenia grupy dyskowej z jednego poziomu RAID na drugi. |
|  | Dyski | * Oferowana macierz musi wspierać dyski hot-plug:   + dyski elektroniczne SSD   + mechaniczne HDD z interfejsem SAS12Gb/s   + dyski mechaniczne HDD o prędkości obrotowej 7,2 krpm, 10 krpm, * Macierz musi obsługiwać mieszaną konfigurację dysków hot-plug SSD i HDD w rozmiarach 2,5” i 3,5” zainstalowanych w dowolnym module rozwiązania. * Wszystkie dyski wspierane przez oferowany model macierzy muszą być wykonane w technologii hot-plug. * Macierz musi obsługiwać 120 dysków SAS SSD w całym rozwiązaniu, bez konieczności dokupowania/wymiany żadnych innych elementów sprzętowych czy licencyjnych innych niż same półki dyskowe wraz z dyskami. * Macierz musi posiadać oprogramowanie do monitoringu stanu dysków, które pozwala na identyfikowanie potencjalnie zagrożonych awarią dysków oraz z poziomu graficznego interfejsu do zarządzania musi być możliwość sprawdzenia stanu zużycia dysków SSD. * Macierz musi umożliwiać skonfigurowanie każdego zainstalowanego dysku hot-plug jako dysk hot-spare (dysk zapasowy). * W przypadku awarii dysku fizycznego i wykorzystania wcześniej skonfigurowanego  dysku zapasowego, wymiana uszkodzonego dysku na sprawny nie może powodować powrotnego kopiowania danych z dysku hot-spare na wymieniony dysk (tzw. CopyBackLess). * Macierz musi pozwalać na zaszyfrowanie danych na dedykowanych do tego dyskach kluczem AES256-bit zgodnie z wytycznymi Information Technology Laboratory przy National Institute of Standards and Technology (NIST). * Macierz musi posiadać możliwość skasowania wszystkich danych z dysku FDE celem bezpiecznego ponownego użycia w innym środowisku (Secure Erase). |
|  | Opcje programowe | * Macierz musi być wyposażona w system kopii migawkowych umożliwiający wykonanie 128 kopii migawkowych. * Macierz musi umożliwiać zdefiniowanie min. 500 woluminów  (LUN). * Macierz musi mieć możliwość tworzenia wolumenów łączonych tzw Contetenated. * Macierz powinna umożliwiać podłączenie logiczne z serwerami i stacjami poprzez min. 128 ścieżek logicznych FC. * Macierz musi umożliwiać aktualizację oprogramowania wewnętrznego kontrolerów RAID i dysków bez konieczności wyłączania macierzy oraz bez konieczności wyłączania ścieżek logicznych FC/iSCSI dla podłączonych stacji/serwerów. * 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 wsparcie dla systemów operacyjnych:   + Microsoft Windows Server 2016, 2019, 2022   + SuSE Linux Enterprise Server 15, 12   + Red Hat Linux Enterprise Server 9, 8, 7   + Oracle Linux 9, 8, 7   + Solaris 11   + Vmware vSphere 7.0, 8.0; * Macierz musi być dostarczona z licencją na oprogramowanie wspierające  technologię typu multipath (obsługa nadmiarowości dla ścieżek transmisji danych pomiędzy macierzą i serwerem)  dla połączeń FC i iSCSI. * Macierz musi posiadać możliwość uruchamiania mechanizmów zdalnej replikacji danych, w trybie synchronicznym i asynchronicznym, bez konieczności stosowania zewnętrznych urządzeń konwersji. Funkcjonalność replikacji danych musi być zapewniona z poziomu oprogramowania wewnętrznego macierzy, jako tzw. storage-based data replication. Replikacja danych musi być obsługiwana w połączeniu macierzą z tej samej rodziny urządzeń wspierającą obsługę zdalnej replikacji danych. * Macierz musi posiadać możliwość tworzenia lokalnych tj. w obrębie zasobów macierzy, pełnych kopii danych (tzw. klony danych). * Macierz musi obsługiwać mechanizmy Thin Provisioning, czyli przydziału dla obsługiwanych środowisk woluminów logicznych o sumarycznej pojemności większej od sumy pojemności dysków fizycznych zainstalowanych w macierzy. |
|  | Zarządzanie | * Oprogramowanie do zarządzania musi być zintegrowane z systemem operacyjnym systemu pamięci masowej. * Komunikacja z wbudowanym oprogramowaniem zarządzającym macierzą musi być możliwa w trybie graficznym np. poprzez przeglądarkę WWW oraz w trybie tekstowym. * Musi być możliwe zdalne zarządzanie macierzą z wykorzystaniem standardowej przeglądarki internetowej (minimum Microsoft Edge, Google Chrome, Mozilla Firefox) bez konieczności instalacji żadnych dodatkowych aplikacji na stacji administratora. * Wbudowane oprogramowanie macierzy musi obsługiwać połączenia z modułem zarządzania macierzy poprzez szyfrowanie komunikacji protokołami: SSL dla komunikacji poprzez przeglądarkę WWW i protokołem SSH dla komunikacji poprzez CLI. * Wraz z system musi zostać dostarczone narzędzie do monitoringu macierzy w kontekście:   + wydajności i opóźnień na wolumenach   + wydajności I/Ops, MB/s   + trafności w cache * Macierz musi posiadać możliwość integracji z Active Directory w zakresie definicji i mapowania grup i użytkowników pod kątem autentykacji. * Macierz musi posiadać oprogramowanie pozwalające na integrację Vmware vCenter – provisioning i monitoring macierzy z widoku vCenter * Macierz musi posiadać wsparcie dla VMware vSphere Storage APIs Array Integration (VAAI) |
|  | Gwarancja | * Całe rozwiązanie musi być objęte minimum 5 letnim okresem gwarancji z naprawą miejscu instalacji urządzenia i z gwarantowanym czasem wizyty technika do końca następnego dnia roboczego od dnia zgłoszenia awarii do organizacji serwisowej producenta macierzy. * Uszkodzone dyski twarde nie podlegają zwrotowi organizacji serwisowej. * Serwis gwarancyjny musi obejmować dostęp do poprawek i nowych wersji oprogramowania wbudowanego, które są elementem zamówienia. * Macierz musi pochodzić z oficjalnego kanału sprzedaży producenta w UE. Nie dopuszcza się użycia macierzy odnawianych, demonstracyjnych lub powystawowych. * Urządzenie musi być wykonane zgodnie z europejskimi dyrektywami RoHS i WEEE stanowiącymi o unikaniu i ograniczaniu stosowania substancji szkodliwych dla zdrowia. * Możliwość odpłatnego wydłużenia gwarancji producenta do 7 lat w trybie onsite z gwarantowanym skutecznym zakończeniem naprawy serwera najpóźniej w następnym dniu roboczym od zgłoszenia usterki (podać koszt na dzień składania oferty). * Producent oferowanej macierzy musi posiadać dedykowaną, ogólnie dostępną stronę internetową, gdzie po wpisaniu numeru seryjnego macierzy można zweryfikować co najmniej: czas i poziom oferowanego serwisu gwarancyjnego producenta zarówno dla macierzy jak i dowolnej z półek dyskowych, datę zakończenia wsparcia gwarancyjnego, datę zakończenia wsparcia producenta dla oferowanego urządzenia – w formularzu ofertowym należy podać adres internetowy strony producenta macierzy,  gdzie można zweryfikować wymagane informacje. |

1. System backupu

| **Lp.** | **Minimalne wymagania** |
| --- | --- |
|  | Oprogramowanie musi być produktem przeznaczonym do obsługi środowisk DataCenter. |
|  | 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. |
|  | 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 jakiejkolwiek 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 dwuch administratorów backupu do wykonania krytycznych operacji (np skasowanie backupu, dodanie kolejnego administratora) |
|  | Oprogramowanie musi posiadać integracje z systemami zarządania kluczami szyfrującymi (KMS) |
|  | Oprogramowanie musi posiadać integracje z systemami typu SIEM |
|  | 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 datastoru |
|  | 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 punku 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) |
|  | 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 uruchomianie 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 vSpehre |
|  | 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 |
|  | 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 uruchomianie 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 wyuczonynym 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. |
|  | 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 kategoryzacje 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 |
|  | 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 nadanym 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 |
|  | Wymagane jest dostarczenie licencji wieczystych zapewniających zabezpieczenie minimum 15 maszyn wirtualnych pracujących pod kontrolą systemu MS Hyper-V. Licencje muszą być objęte co najmniej 5 letnim wsparciem producenta oprogramowania, charakteryzującym się następującymi parametrami:   * możliwość instalacji aktualizacji oprogramowania oraz najnowszych dostępnych wersji w czasie aktywnego wsparcia, * obsługa zgłoszeń w trybie 24x7 * zarządzenie licencjami oprogramowania |

1. Biblioteka taśmowa (1 szt.)

| **Lp.** | **Pozycja** | **Minimalne wymagania** |
| --- | --- | --- |
|  | Technologia | LTO-9 Ultrium wspierająca technologię partycjonowania nośników. Urządzenie powinno mieć możliwość instalowania w tej samej obudowie także napędów LTO szóstej, siódmej i ósmej generacji. |
|  | Wbudowany napęd | Napęd LTO-9 wyposażony w złącze SAS 12Gb. Oferowane urządzenie musi mieć możliwość instalowania i wykorzystania w tej samej obudowie także napędów LTO z interfejsem FC oraz wspierać technologię LTFS (Linear Tape File System). Prędkość zapisu zainstalowanego napędu bez kompresji – minimum 300 MB/sek. Zainstalowany napęd musi dynamicznie i płynnie dopasowywać prędkość zapisu do napływających danych (speed matching) w przedziale od 100 do 300 MB/sek., oferować funkcję SkipSync zapewniającą dużą szybkość zapisu małych plików bez konieczności zatrzymywania i przewijania dysku oraz stosować szyfrowanie danych metodą AES 256-bit zgodną ze standardem FIPS 140-2. |
|  | Ilość slotów i magazynki | Minimalnie 8 slotów na nośniki podzielone na dwa magazynki. Urządzenie powinno być dostarczone z kompletem magazynków. Wymagana ilość mail slot (I/E): 1. Możliwość zdalnego wysuwania magazynków poprzez web GUI. |
|  | Pojemność | Pojemność bez kompresji – minimum 144TB |
|  | Zarządzanie | Za pomocą panelu kontrolnego znajdującego się na froncie urządzenia oraz zdalne przez sieć poprzez przeglądarkę internetową (web GUI) za pomocą interfejsu FastEthernet. Wymagane wsparcie SNTP, protokołów SSL/TLS i IPv6 oraz definiowanie minimum 4 poziomów zarządzania urządzeniem i dostępem do niego. Urządzenie musi mieć możliwość zabezpieczania swojej konfiguracji na podłączony, poprzez slot USB, PenDrive. Operacja powinna być możliwa zarówna poprzez web GUI jak i poprzez panel kontrolny urządzenia. Wymagana możliwość zdalnego wysuwania magazynków, restartowania biblioteki oraz wyłączania zasilania napędów poprzez webGUI. |
|  | Dodatkowe interfejsy | Biblioteka musi być wyposażone w interfejs sieciowy, interfejs USB oraz interfejs ADI. |
|  | Obsługa urządzenia | Możliwość wymiany napędu, zasilacza i modułu portów zarządzania u użytkownika bez konieczności demontażu urządzenia z szafy przemysłowej oraz bez konieczności zdejmowania pokrywy głównej. Zarówno napęd jaki moduł interfejsów powinny być wyposażone w lamki kontrolne, informujące o stanie technicznym i widoczne na odwrotnej stronie urządzenia. |
|  | Obudowa | Typu rack 19” o wysokości maksymalnie 1U. Wszystkie elementy do montażu muszą być dostarczone wraz z urządzeniem. |
|  | Wyposażenie | Urządzenie musi być wyposażone w czytnik kodów kreskowych, kabel zasilający, kabel komunikacyjny konieczny do podłączenia urządzenia do odpowiedniego kontrolera serwera i umożliwiającego komunikację z urządzeniem – długość kabla min. 2m oraz zestaw 8-miu nośników danych o pojemności bez kompresji minimum 18 TB każdy wraz z nośnikiem czyszczącym, przy czym wszystkie dostarczone nośniki muszą być kompatybilne i dedykowane do współpracy z oferowanym urządzeniem oraz wyposażone w naklejki z kodami kreskowymi. Kompatybilność nośników taśmowych z urządzeniem musi zostać potwierdzona przez oświadczenie producenta dostarczone wraz z ofertą. |
|  | Gwarancja | Minimum 5 letnia gwarancja świadczona w miejscu instalacji urządzenia z czasem reakcji w ciągu 4 godzin. Czas przyjmowania zgłoszeń serwisowych w trybie 24x7. Przystąpienie do fizycznej naprawy najpóźniej w następnym dniu roboczym od zgłoszenia awarii z terminem naprawy najpóźniej do 48 godzin od rozpoczęcia naprawy. Gwarantowana możliwość rozszerzenia oferowanego serwisu do 84 miesięcy. Zgłaszania awarii wyłącznie poprzez ogólnopolską linię telefoniczną producenta lub autoryzowany serwis producenta posiadający certyfikat ISO9001 na usługi serwisowe – kontakt z serwisem wyłącznie w języku polskim.  Pisemne oświadczenia wystawione przez producenta:  - o gwarancji świadczonej w miejscu instalacji urządzenia w rygorze 24x7x4 realizowanej przez producenta lub jego autoryzowany serwis posiadający ISO9001 na usługi serwisowe wraz z potwierdzeniem możliwości przedłużenia gwarancji do 84 miesięcy. W oświadczeniu wymagane jest podanie wszystkich danych kontaktowych z serwisem (mail, telefon, adres) oraz potwierdzenie wykupienia przez wykonawcę wymienionych usług serwisowych u producenta. |

1. Zasilacz awaryjny (1 szt.)

| **Lp.** | **Pozycja** | **Minimalne wymagania** |
| --- | --- | --- |
|  | Moc pozorna | Co najmniej 5000 VA |
|  | Moc rzeczywista | Co najmniej 4500 W |
|  | Topologia (klasyfikacja IEC 62040-3) | Podwójna konwersja on-line |
|  | Typ obudowy | Uniwersalna tower/rack |
|  | Sprawność UPS'a | Co najmniej 93% w trybie podwójnego przetwarzania on-line przy 100% obciążeniu, co najmniej 98% w trybie podwyższonej sprawności |
|  | Liczba, typ gniazd wyjściowych | Zaciski, minimum 8 gniazd C13, minimum 2 gniazda C19 |
|  | Typ gniazda wejściowego | Listwa zaciskowa |
|  | Czas podtrzymania dla obciążenia mocą 4500 W (baterie wewnętrzne w UPS) | Co najmniej 3 minuty |
|  | Dodatkowe baterie | Możliwość wydłużenia czasu podtrzymania do co najmniej 80 minut przy obc. mocą 4500 W poprzez dołożenie dodatkowych modułów baterii zewnętrznych. |
|  | Napięcie znamionowe | 230 V |
|  | Tolerancja napięcia prostownika | 176-276 V (100-276 V przy obniżonej mocy) |
|  | Częstotliwość znamionowa | 50/60 Hz autodetekcja |
|  | Tolerancja częstotliwości | 40 – 70 Hz |
|  | Kształt napięcia | Sinusoidalny |
|  | Napięcie znamionowe wyjściowe | 230 V (domyślnie) / 200/208/220/240 V |
|  | Zakres zmian napięcia wyjściowego | +/-1% napięcia nominalnego |
|  | Częstotliwość wyjściowa | 50/60 Hz +/-0,5% |
|  | Całkowite odkształcenia napięcia THDu | < 2% dla obciążenia liniowego |
|  | Baterie wymieniane przez użytkownika "na gorąco" | Tak |
|  | Ochrona przed przeładowaniem | Tak (ograniczenie prądu ładowarki, wyłączenie ładowarki / alarm) |
|  | Ochrona przed głębokim rozładowaniem | Tak |
|  | Okresowy automatyczny test baterii | Tak (standardowo co tydzień) |
|  | Zimny start | Tak |
|  | System zarządzania pracą baterii | System nieciągłego ładowania baterii. Do oferty dołączyć należy opis algorytmu ładowania nieciągłego baterii. W opisie znaleźć się muszą informacje nt. trwania okresów ładowania forsującego, konserwującego i okresu spoczynkowego (tzw. restingu). Okres spoczynkowy w jednym cyklu nie może być krótszy niż 14 dni. Opis powinien być materiałem firmowym producenta lub musi być przez niego potwierdzony. |
|  | Interfejs komunikacyjny | * USB * RS232 DB-9 żeński (HID) * miniport wyłącznik awaryjny RPO * miniport wyłącznik ON/OFF * DB-9 port przekaźnikowy * karta SNMP |
|  | Panel sterowania z wyświetlaczem LCD | * Panel LCD obrotowy (do ułatwienia odczytów przy obu wariantach montażu UPS’a) ze wskazaniami chwilowego poziomu obciążenia i poziomu naładowania baterii, z możliwością sterowania poszczególnymi segmentami odbiorów oraz pomiarem sprawności i zużycia energii przez odbiory (w kWh) * Poziomy rząd przycisków sterowania * Poziomy rząd wskaźników stanu: trybu online (zielony), trybu bateryjnego (pomarańczowy), trybu bypass (pomarańczowy), usterki (czerwony) |
|  | Przyciski sterujące i wskaźniki diodowe LED | * sygnalizator akustyczny (awaria, serwis, niski stan naładowania baterii, przeciążenie) * przycisk Escape (anulowanie) * przyciski funkcyjne (przewijanie w górę i w dół) * przycisk Enter (potwierdzający) |
|  | Wyposażenie dodatkowe | * kabel RS232 * kabel USB * Gigabitowa Karta SNMP * uchwyty kablowe * podstawki do montażu pionowego (wieża) * 2 przewody IEC 10A * zestaw szyn montażowych do szafy 19" |
|  | Karta SNMP | * cyberbezpieczeństwo (szyfry TLS, MQTT) * certyfikaty CA i PKl * prędkość gigabit’owa (half-duplex, full-duplex) * różne poziomy nadawania dostępu do konta administratora lub użytkownika |
|  | Protokoły i certyfikaty cyberbezpieczeństwa | UL 2900-2-2/IEC 62443-4-2/HTTPS/MQTT/  /RNDIS/LDAP/NVD//SSH/PKI /  pakiet szyfrów TLS 1.2 z minimum SHA256 |
|  | Monitorowanie temperatury i wilgotności | Możliwość podłączenia opcjonalnego czujnika pod kartę sieciową |
|  | Dołączone oprogramowanie | Do bezpiecznego zamykania systemów operacyjnych przy wyczerpaniu baterii (minimum: Windows: 2000, XP, 2003, Vista, Server 2008, 7, 8, 10; Linux: Red Hat, Fedora Core, SuSE). Oprogramowanie musi mieć możliwość wyboru polskiej wersji językowej. |
|  | Maksymalna wysokość UPS | Maksymalnie 3U |
|  | Poziom hałasu | Nie więcej niż 45 dBA, mierzone w odległości 1m. |
|  | Zgodność z normami UE | Deklaracja zgodności producenta |
|  | Dodatkowe cetyfikaty | ISO9001 producenta urządzenia |
|  | Gwarancja producenta | Co najmniej 24 miesiące |

1. Przełącznik sieciowy (5 szt.)

| **Lp.** | **Minimalne wymagania** |
| --- | --- |
|  | Musi posiadać co najmniej 48 portów gigabitowych w standardzie 100/1000BaseT. |
|  | Musi posiadać co najmniej 4 porty 1000BaseX ze stykiem definiowanym przez SFP (dopuszcza się porty typu Combo, współdzielone z portami 10/100/1000BaseT). |
|  | Musi posiadać minimum 4 porty 10Gb SFP+. Dla zwiększenia niezawodności porty SFP+ powinny być umieszczone na module pozwalającym na ich wymianę. Moduł z portami SFP+ musi obsługiwać MACsec. |
|  | Musi posiadać minimum 2 dedykowane porty stackujące (niezależne od portów SFP+), pozwalające na połączenie w stos minimum 10 przełączników. Agregowana prędkość magistrali stackującej nie może być mniejsza niż 100Gb/s. Stos musi być widoczny jako jedno urządzenie (wspólne zarządzanie z jednej linii komend, analogiczne do przełącznika modularnego). Dopuszcza się rozwiązanie, w którym porty stackujące dostępne są w postaci opcjonalnego modułu (niezależnego od modułów 10Gb i 40Gb opisanych w punktach powyżej), który jednak musi być dostępny w chwili składania oferty i zaoferowany. Do przełącznika musi być dołączony kabel służący do połączenia w stos o długości co najmniej 0,5m.  Dodatkowo Wykonawca dostarczy jeden kabel stackujący o długości co najmniej 3 m w celu połączenia urządzeń stos (1 kabel na wszystkie przełączniki). |
|  | Przepustowość: minimum 175 Gb/s (pełna prędkość, tzw. wire-speed, na wszystkich portach przełącznika), nie licząc magistrali stackującej. |
|  | Wydajność: minimum 110 Mp/s. |
|  | Tablica adresów MAC o wielkości minimum 32000 pozycji. |
|  | Musi posiadać obsługę ramek Jumbo. |
|  | Musi posiadać minimum 4GB pamięci stałej typu Flash, minimum 1GB pamięci RAM. |
|  | Musi posiadać minimum 12MB bufora pakietów. |
|  | Musi posiadać dedykowany port do zarządzania poza pasmowego (Ethernet, RJ-45), w pełni niezależny od portów liniowych. |
|  | Musi posiadać port USB. |
|  | Musi posiadać minimum dwa, modularne, wewnętrzne zasilacze prądu zmiennego. Przy wykorzystaniu obydwu źródeł zasilania – zasilacze powinny pracować w trybie redundantnym oraz być wymieniane na gorąco. |
|  | Routing IPv4 – minimum: statyczny, RIPv2, OSPF. |
|  | Routing IPv6 – minimum: statyczny, RIPng, OSPFv3. |
|  | Musi posiadać obsługę protokołu VRRP. |
|  | Wielkość sprzętowej tablicy rutingu: minimum 2000 wpisów dla IPv4, 1000 wpisów dla IPv6. |
|  | Musi wspierać: IGMPv1/v2/v3 Snooping; MLDv1/v2 Snooping, PIM Dense Mode, PIM Sparse Mode. |
|  | Musi posiadać obsługę VxLAN. |
|  | Musi posiadać obsługę IEEE 802.1s Multiple SpanningTree / MSTP oraz IEEE 802.1w Rapid Spanning Tree Protocol. |
|  | Musi posiadać obsługę 4094 tagów IEEE 802.1Q oraz minimum 2000 jednoczesnych sieci VLAN. |
|  | Musi posiadać funkcję Root Guard oraz BPDU protection |
|  | Musi umożliwiać realizację łączy agregowanych (LACP) w ramach różnych przełączników będących w stosie. |
|  | Musi posiadać wsparcie dla funkcji DHCP server, DHCP Relay oraz DHCP Snooping. |
|  | Musi posiadać funkcję list ACL na bazie informacji z warstw 2/3/4 modelu OSI. |
|  | Musi posiadać obsługę standardu 802.1p – min. 8 kolejek na porcie |
|  | Musi posiadać funkcję mirroringu portów. |
|  | Musi posiadać obsługę IEEE 802.1AB Link Layer Discovery Protocol (LLDP) i LLDP Media Endpoint Discovery (LLDP-MED). |
|  | Musi posiadać funkcję autoryzacji użytkowników zgodna z 802.1x. |
|  | Musi posiadać funkcję autoryzacji logowania do urządzenia za pomocą serwerów RADIUS albo TACACS+. |
|  | Musi posiadać funkcję RADIUS Accounting. |
|  | Musi posiadać wsparcie dla protokołu OpenFlow w wersji 1.0 oraz 1.3. |
|  | OpenFlow musi posiadać możliwość konfiguracji przetwarzania pakietów przez przełącznik w oparciu o ciąg tablic. |
|  | Musi być możliwe wielotablicowe przetwarzanie zapytań OpenFlow zawierająca następujące tablice do przetwarzania reguł sprzętowo w oparciu o: źródłowe i docelowe adresy MAC, źródłowy i docelowy adres IP oraz nr portu, numer portu wejściowego (pole IP DSCP oraz VLAN PCP) |
|  | Musi być możliwe przypisywanie więcej niż jednej akcji zadanemu wpisowi OpenFlow. |
|  | Musi być możliwe tworzenie logicznych tuneli poprzez komunikaty SNMP i możliwość ich wykorzystania w kierowaniu ruchem w sposób sterowany za pomocą protokołu OpenFlow. |
|  | Musi posiadać wsparcie dla Energy-efficient Ethernet (EEE) IEEE 802.3az. |
|  | Musi umożliwiać zarządzanie poprzez port konsoli (pełne) (RS-232 i USB), SNMP v.1, 2c i 3, Telnet, SSH v.2, http i https. |
|  | Musi posiadać obsługę Syslog. |
|  | Musi posiadać obsługę SNTPv4 lub NTP. |
|  | Musi posiadać możliwość przechowywania co najmniej dwóch wersji oprogramowania na przełączniku. |
|  | Musi posiadać możliwość przechowywania co najmniej trzech plików konfiguracyjnych na przełączniku, możliwość wgrywania i zgrywania pliku konfiguracyjnego w postaci tekstowej do stacji roboczej. |
|  | Musi posiadać wsparcie dla funkcji Private VLAN lub równoważnego. |
|  | Musi posiadać obsługę mechanizmu wykrywania łączy jednokierunkowych typu Uni-Directional Link Detection (UDLD), Device Link Detection Protocol (DLDP) lub równoważnego |
|  | Minimalny zakres pracy od 0°C do 45°C. |
|  | Wysokość w szafie 19” – 1U, głębokość nie większa niż 50 cm. |
|  | Jeżeli do działania któregokolwiek z wymienionych protokołów i funkcji wymagana jest dodatkowa licencja to należy ją dostarczyć w ramach tego postępowania. |
|  | Wszystkie dostępne na przełączniku funkcje muszą być dostępne przez cały okres jego użytkowania (permanentne), nie dopuszcza się licencji czasowych i subskrypcji, o ile nie wyspecyfikowano inaczej. |
|  | Dożywotnia (minimum 5 lat po zakończeniu produkcji, przy czym, jeżeli data zakończenia produkcji jest ogłoszona to nie może być ona krótsza niż 2 lata po dostarczeniu sprzętu) gwarancja producenta obejmująca wszystkie elementy przełącznika (również zasilacze i wentylatory) zapewniająca wysyłkę sprzętu na podmianę maksymalnie na następny dzień roboczy. Gwarancja musi zapewniać również dostęp do poprawek, wsparcia technicznego i aktualizacji oprogramowania przez cały okres trwania gwarancji. Gwarancja musi być świadczony bezpośrednio przez autoryzowany serwis producenta sprzętu. Cała komunikacja odbywać się musi bezpośrednio pomiędzy Zamawiającym i autoryzowanym serwisem producentem sprzętu. |
|  | Wykonawca dostarczy moduły (Transceiver) kompatybilne z przełącznikiem:   * Co najmniej 2 szt. 1Gb SFP jednomodowe * Co najmniej 2 szt. 1Gb SFP wielomodowe * Co najmniej 2 szt. 10Gb SFP+ wielomodowe * Co najmniej 2 szt. 10Gb SFP+ RJ45   Powyższa ilość dotyczy pojedynczego przełącznika.  Gwarancja: co najmniej 24 miesiące. |
|  | Wykonawca dostarczy okablowanie optyczne i miedzianej niezbędne do zapewnienia komunikacji pomiędzy przełącznikami sieciowymi, a poszczególnymi elementami infrastruktury dostarczanej w ramach przedmiotu zamówienia. |

1. Wdrożenie

| **Lp.** | **Pozycja** | **Minimalne wymagania** |
| --- | --- | --- |
|  | Serwery, macierz dyskowa, serwerowe systemy operacyjne | * Instalacja sprzętu w istniejącej szafie rack * Wgranie najnowszych wersji firmware * Konfiguracja serwera, macierzy, * Budowa klastra Hyper-v * Migracja maszyn wirtualnych * Rekonfiguracja obecnego serwera * Dodanie dodatkowego serwera do AD * Testy środowiska |
|  | Serwer backupu, biblioteka taśmowa, system backapu | * Instalacja sprzętu w istniejącej szafie rack * Wgranie najnowszych wersji firmware * Instalacja systemu backupu * Konfiguracja systemu backupu zgodnie z polityką bezpieczeństwa Zamawiającego * Testy odtworzeniowe środowiska |
|  | Przełączniki sieciowe | * Instalacja sprzętu w istniejącej szafie rack * Wgranie najnowszych wersji firmware * Konfiguracja przełączników wg. wytycznych Zamawiającego |
|  | Zasilacz awaryjny | * Instalacja sprzętu w istniejącej szafie rack * Wgranie najnowszych wersji firmware * Konfiguracja oprogramowania zarządzającego |
|  | Dokumentacja | * Wykonawca przygotuje dokumentację techniczną, która będzie zawiera wszelkie niezbędne informacje potrzebne Zamawiającemu do przejęcia środowiska i zarzadzania nim we własnym zakresie. |
|  | Szkolenie | * W ramach zakresu przedmiotu zamówienia Wykonawca zrealizuje szkolenie powdrożeniowe. * Szkolenie odbędzie się w siedzibie Zamawiającego. * Szkolenie będzie trwało co najmniej 8 godzin. |
|  | Wsparcie powdrożeniowe | Okres świadczenia: co najmniej 12 miesięcy od zakończenia wdrożenia.  Wymiar godzin: co najmniej 96 roboczogodzin.  Okno świadczenia wsparcia: w dni robocze, w godzinach od 8 do 16.  Tryb świadczenia wsparcia: zdalne.  Raport z wykorzystania: minimum raz w miesiącu  Wykonawca zapewni dostęp do portalu servicedesk, gdzie będą widoczne zgłoszenia.  Jednostka rozliczeniowa: co najmniej jedna roboczogodzina. |