**Załącznik nr 1 do Umowy**

**Zakup infrastruktury serwerowej i macierzy dyskowych na potrzeby na potrzeby utrzymania Centralnych Usług Infrastrukturalnych PK w OPDR**

Spis treści

[**Załącznik nr 1 do Umowy** 1](#_Toc173422936)

[1.1. **SERWERY RACK** 3](#_Toc173422937)

[**1.1.1.** **Serwer rack typu I – 11 sztuk** 3](#_Toc173422938)

[**1.1.2.** **Serwer rack typu II – 33 sztuki** 10](#_Toc173422939)

[**1.2.** **MACIERZE DYSKOWE** 17](#_Toc173422940)

[**1.2.1** **Macierz blokowa Typ I – 11 sztuk** 17](#_Toc173422941)

[**1.3.** **DEDUPLIKATORY** 23](#_Toc173422942)

[**1.3.1** **Deduplikator typ I – 10 sztuk** 23](#_Toc173422943)

[**1.3.2** **Deduplikator typ II – 1 sztuka** 32](#_Toc173422944)

[**1.4.** **SPRZĘT LAN** 43](#_Toc173422945)

[**1.4.1** **Przełącznik LAN – 11 sztuk** 43](#_Toc173422946)

[**1.5.** **OPROGRAMOWANIE** 46](#_Toc173422947)

[**1.5.1** **Oprogramowanie wirtualizacyjne – 1232 licencje na rdzeń procesora** 46](#_Toc173422948)

[**1.5.2** **Oprogramowanie do wykonywania i odtwarzania kopii zapasowych** 74](#_Toc173422949)

[**1.6.** **USŁUGI** 80](#_Toc173422950)

[**1.6.1** **Dostawa sprzętu i oprogramowania** 80](#_Toc173422951)

[**1.6.2** **Projekt techniczny** 81](#_Toc173422952)

[**1.6.3** **Wymagania na montaż sprzętu, instalacja i konfiguracja sprzętu oraz oprogramowania (usługa)** 82](#_Toc173422953)

[**1.6.4** **Konfiguracja środowisk zgodnie z Projektami Technicznymi (usługa)** 84](#_Toc173422954)

[**1.6.5** **Migracja danych (usługa)** 84](#_Toc173422955)

[**1.6.6** **Wymagania na przeprowadzenie testów wg zaakceptowanych przez Zamawiającego scenariuszy testów (usługa)** 85](#_Toc173422956)

[**1.6.7** **Wymagania na opracowanie dokumentacji powykonawczej (dokument)** 85](#_Toc173422957)

[**1.6.8** **Wymagania na przeprowadzenie szkolenia dla administratorów** 86](#_Toc173422958)

[**1.6.9** **Wymagany zespół Wykonawcy** 89](#_Toc173422959)

# Opis Przedmiotu Zamówienia

* 1. **Słownik pojęć i skrótów.**

**POPD** – środowisko produkcyjne w Podstawowym Ośrodku Przetwarzania Danych,

**ZOPD** – środowisko produkcyjne w Zapasowym Ośrodku Przetwarzania Danych,

**OOPD** – Odizolowany Ośrodek Przetwarzania Danych

**Oprogramowanie** – wartości niematerialne i prawne dostarczane w ramach przedmiotowego postępowania

**ITS** – infrastruktura techniczno-systemowa

**Urządzenie/Sprzęt** – sprzęt teleinformatyczny dostarczany w ramach przedmiotowego postępowania

* 1. **Kontekst postepowania**

W jednostkach Prokuratur Regionalnych eksploatowana jest infrastruktura teleinformatyczna w postaci 2 klastrów wirtualizacyjnych oraz macierzy dyskowej.

Sprzęt i oprogramowanie są pozbawione wsparcia producenta – większość sprzętu ma ponad 9 lat, co stanowi ryzyko dla ciągłości działania jednostek tych jednostek z uwagi na brak aktualizacji bezpieczeństwa i podatność na awarie.

Dwa serwery Dell R720 – 256GB RAM, 2 CPU (2x10core), trzy serwery Dell R630 – 256GB RAM,2CPU (2x10core) oraz serwer backup Dell R630 128GB RAM, 2 CPU (2x6core) oraz macierz Dell EMC Unity 400. Całość podłączona jest do sieci LAN poprzez dwa przełączniki Cisco Nexus 3524x. Rozwiązanie wykorzystuje oprogramowanie wirtualizacyjne Vmware 6.5 oraz 6.7.

* 1. **Przedmiot postępowania**

Postępowanie przetargowe ma na celu wymianę posiadanej infrastruktury na nowe, bieżące rozwiązanie, posiadające pakiet usług gwarancyjnych producenta, zrealizowane w sposób zapewniający redundancję sprzętową oraz umożliwiające wykonywanie kopii zapasowych i ich replikację do posiadanego przez Zamawiającego rozwiązania typu CyberBunkier odmiejscowionego geograficznie od lokalizacji w których planowane jest wdrożenie. Zamawiający zakłada centralne zarządzanie wdrożonym rozwiązaniem przez grupę wskazanych administratorów Zamawiającego w poszczególnych obszarach. Wdrożona infrastruktura ma na celu umożliwienie oprócz aktualnie zgromadzonych zasobów również maszyn wirtualnych i rozwiązań z poziomu prokuratur okręgowych.

* 1. **SERWERY RACK**
     1. **Serwer rack typu I – 11 sztuk**

**Producent ………………………….….**

**Model ……………………….…….**

| **Identyfikator wymagania** | **Wymaganie** | **Opis wymagania** |
| --- | --- | --- |
| SR1-1 | Obudowa | 1. Maksymalnie 1U RACK 19 cali (wraz z szynami montażowymi oraz ramieniem do prowadzenia kabli, umożliwiającymi serwisowanie serwera w szafie rack bez wyłączania urządzenia). 2. Wyposażona w minimum 8 zatok dyskowych SFF (2,5”) typu Hot Swap wspierających dyski SAS oraz SATA. 3. Wyposażona w zamykany, zdejmowany panel przedni chroniący przed nieuprawionym dostępem do dysków. 4. Wyposażona w czujnik otwarcia obudowy współpracujący z kartą zarządzającą. |
| SR1-2 | Płyta główna | Płyta główna umożliwiająca zainstalowanie co najmniej 2 procesorów od 8 do 64 rdzeniowych o taktowaniu bazowym do minimum 3.9GHz. |
| SR1-3 | Procesor | Procesor szesnastordzeniowy, klasy x86 - 64 bity, osiągający w zaoferowanym modelu serwera w testach SPECrate2017\_int\_base dla konfiguracji 2 procesorowej wynik nie gorszy niż 319 punktów. Wynik testu musi być opublikowany i ogólnie dostępny na stronie <https://spec.org/> - dołączony do oferty wydruk ze strony <https://spec.org/> potwierdzający. że oferowany model serwera w oferowanej konfiguracji tj.: (serwer/procesory) umożliwia osiągniecie powyższego wyniku. |
| SR1-4 | Liczba procesorów | 1 procesor. |
| SR1-5 | Pamięć operacyjna | 1. Minimum 512GB RDIMM DDR5 minimum 4800 MT/s w modułach o pojemności minimum 64GB każdy. 2. Płyta główna z minimum 32 slotami na pamięć i umożliwiająca instalację do minimum 8TB pamięci (przy zastosowaniu odpowiednich procesorów). |
| SR1-6 | Sloty rozszerzeń | Minimum 2 aktywne gniazda PCI-Express generacji 4, wszystkie x16 (szybkość slotu – bus width). |
| SR1-7 | Dysk twardy | Zainstalowane:   1. 2 dyski M.2 NVMe o pojemności minimum 480 GB każdy, pracujące w RAID 1. Rozwiązanie nie zajmujące zatok dyskowych opisanych w sekcji „Obudowa”. 2. 3 dyski SSD Mixed Use, każdy o pojemności minimum 1,92TB, dyski typu Hot Swap. |
| SR1-8 | Kontroler | Serwer wyposażony w kontroler sprzętowy z minimum 8GB cache z mechanizmem podtrzymywania zawartości pamięci cache w razie braku zasilania, zapewniający obsługę 8 napędów dyskowych SAS oraz obsługujący poziomy: RAID 0/1/10/5/50/6/60. |
| SR1-9 | Interfejsy Ethernet | 1. Minimum 4 porty Ethernet 100/1000 Mb/s RJ-45 z funkcją Wake-On-LAN, wsparciem dla PXE, zainstalowane w dedykowanym slocie OCP 3.0. 2. Minimum 1 karta 2 portowa 10/25 Gb Ethernet SFP28, wspierające: SR-IOV, Receive Side Scaling (RSS), Jumbo frames, VMware NetQueue, Microsoft VMQ, IEEE 1588, wszystkie porty wyposażone we wkładki SFP+ 10/25Gb SR. |
| SR1-10 | Karta graficzna | Zintegrowana karta graficzna. |
| SR1-11 | Porty | 1. Minimum 5 x USB w tym minimum 4 x USB 3.0, minimum 1 z wymaganych portów USB 3.0 na przednim panelu obudowy, minimum 1 z wymaganych portów USB 3.2 wewnątrz serwera. 2. Minimum 2 x VGA lub 1x VGA i 1x DisplayPort, minimum 1 z wymaganych portów video na przednim panelu obudowy. 3. Minimum 1 x RJ45 do zarządzania na tylnym panelu obudowy oraz 1x USB do zarządzania na przednim panelu obudowy. |
| SR1-12 | Zasilacz | 2 sztuki, typu Hot-plug, redundantne, każdy o mocy minimum 750W oraz o sprawności co najmniej klasy Titanium. |
| SR1-13 | Chłodzenie | Zestaw wentylatorów redundantnych typu hot-plug. |
| SR1-14 | Karta/moduł zarządzający | Niezależna od system operacyjnego, zintegrowana z płytą główną serwera posiadająca minimalną funkcjonalność:   1. monitorowanie podzespołów serwera: temperatura, zasilacze, wentylatory, procesory, pamięć RAM, kontrolery macierzowe i dyski(fizyczne i logiczne), karty sieciowe 2. wparcie dla agentów zarządzających lub możliwość pracy w trybie bezagentowym – bez agentów zarządzania instalowanych w systemie operacyjnym z generowaniem alertów SNMP 3. dostęp do karty zarządzającej poprzez dedykowany port RJ45 z tyłu serwera 4. dostęp do karty możliwy z poziomu przeglądarki webowej (GUI), z poziomu linii komend, poprzez interfejs IPMI 2.0 (Intelligent Platform Management Interface) 5. wbudowane narzędzia diagnostyczne 6. zdalna konfiguracji serwera (BIOS) i instalacji systemu operacyjnego 7. wbudowany mechanizm logowania zdarzeń serwera i karty zarządzającej w tym włączanie/wyłączanie serwera, restart, zmiany w konfiguracji 8. przesyłanie alertów poprzez e-mail oraz przekierowanie SNMP (SNMP passthrough) 9. obsługa zdalnego serwera logowania (remote syslog) 10. wirtualna zdalna konsola, tekstowa i graficzna, z dostępem do myszy i klawiatury i możliwością podłączenia wirtualnych napędów FDD, CD/DVD i USB i wirtualnych folderów 11. monitorowanie zasilania oraz zużycia energii przez serwer w czasie rzeczywistym z możliwością graficznej prezentacji 12. konfiguracja maksymalnego poziomu pobieranej mocy przez serwer (capping) 13. zdalna aktualizacja oprogramowania (firmware) 14. zarządzanie grupami serwerów, w tym:     1. tworzenie i konfiguracja grup serwerów     2. sterowanie zasilaniem (wł./wył.)     3. możliwość równoczesnej obsługi przez 2 administratorów 15. autentykacja dwuskładnikowa (Kerberos) 16. wsparcie dla Microsoft Active Directory 17. obsługa TSL i SSH 18. wsparcie dla IPv4 oraz iPv6, obsługa SNMP v3 oraz RESTful API 19. możliwość autokonfiguracji sieci karty zarządzającejj (DNS/DHCP) |
| SR1-15 | Oprogramowanie do zarządzania | Dodatkowe oprogramowanie umożliwiające zarządzanie poprzez sieć, spełniające minimalne wymagania:   1. integracja z Active Directory; 2. możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta; 3. wsparcie dla protokołów SNMP, IPMI, Linux SSH, Redfish; 4. szczegółowy opis wykrytych systemów oraz ich komponentów; 5. możliwość eksportu raportu do CSV, HTML, PDF; 6. grupowanie urządzeń w oparciu o kryteria użytkownika; 7. tworzenie automatycznie grup urządzeń w oparciu o dowolny element konfiguracji serwera np.: nazwa, lokalizacja, system operacyjny, obsadzenie slotów PCIe, pozostałego czasu gwarancji; 8. możliwość uruchamiania narzędzi zarządzających w poszczególnych urządzeniach; 9. szybki podgląd stanu środowiska; 10. podsumowanie stanu dla każdego urządzenia; 11. szczegółowy status urządzenia/elementu/komponentu; 12. generowanie alertów przy zmianie stanu urządzenia; 13. integracja z service desk Producenta dostarczonej platformy sprzętowej; 14. możliwość przejęcia zdalnego pulpitu; 15. możliwość podmontowania wirtualnego napędu; 16. kreator umożliwiający dostosowanie akcji dla wybranych alertów; 17. przesyłanie alertów „as-is” do innych konsol firm trzecich; 18. możliwość definiowania ról administratorów; 19. możliwość zdalnej aktualizacji oprogramowania wewnętrznego serwerów; 20. aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania); 21. możliwość instalacji oprogramowania wewnętrznego bez potrzeby instalacji agenta; 22. możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów; 23. 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; 24. możliwość tworzenia sprzętowej konfiguracji bazowej i na jej podstawie weryfikacji środowiska w celu wykrycia rozbieżności; 25. wdrażanie serwerów, rozwiązań modularnych oraz przełączników sieciowych w oparciu o profile; 26. możliwość migracji ustawień serwera wraz z wirtualnymi adresami sieciowymi (MAC, WWN, IQN) między urządzeniami; 27. tworzenie gotowych paczek informacji umożliwiających zdiagnozowanie awarii urządzenia przez serwis producenta; 28. zdalne uruchamianie diagnostyki serwera; |
| SR1-16 | Wsparcie dla systemów operacyjnych i systemów wirtualizacyjnych | 1. Microsoft Windows Server 2019 oraz 2022 – potwierdzenie spełnienia tego wymogu poprzez wydruk ze strony <https://www.windowsservercatalog.com/> dołączony do oferty. 2. Red Hat Enterprise Linux (RHEL) 8.6 oraz 9 - potwierdzenie spełnienia tego wymogu poprzez wydruk ze strony <https://catalog.redhat.com/> dołączony do oferty. 3. VMware ESXi 7.0 U3, 8.0 U2 oraz 8.0 U3 - potwierdzenie spełnienia tego wymogu poprzez wydruk ze strony <https://www.vmware.com/resources/compatibility> dołączony do oferty. |
| SR1-17 | Certyfikaty | 1. Certyfikat ISO 9001 dla producenta sprzętu obejmujący proces projektowania i produkcji – dołączony do oferty dokument potwierdzający spełnienie tego wymogu. 2. Certyfikat ISO 14001 dla producenta sprzętu – dołączony do oferty dokument potwierdzający spełnienie tego wymogu. 3. Urządzenia wyprodukowane są przez producenta, zgodnie z normą PN-EN ISO 50001 lub oświadczenie producenta o stosowaniu w fabrykach polityki zarządzania energią, która jest zgodna z obowiązującymi przepisami na terenie Unii Europejskiej – dołączony do oferty dokument potwierdzający spełnienie tego wymogu. 4. Deklaracja zgodności CE – dołączona do oferty. 5. 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 Bronze według normy wprowadzonej w 2019 roku – dołączony do oferty dokument potwierdzający spełnienie tego wymogu. 6. Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia producenta serwera (wg wytycznych Krajowej Agencji Poszanowania Energii S.A, zawartych w dokumencie „Opracowanie propozycji kryteriów środowiskowych dla produktów zużywających energię możliwych do wykorzystania przy formułowaniu specyfikacji na potrzeby zamówień publicznych”, pkt 3.4.2.1; dokument z grudnia 2006 r.), w szczególności zgodności z normą ISO 1043-4 dla płyty głównej oraz elementów wykonanych z tworzyw sztucznych o masie powyżej 25 gr – dołączony do oferty dokument potwierdzający spełnienie tego wymogu. 7. Oświadczenie producenta serwera, potwierdzające, że sprzęt pochodzi z oficjalnego kanału dystrybucyjnego producenta – dołączone do oferty. |
| SR1-18 | Warunki gwarancji: | 1. Gwarancja producenta 36 miesięcy, świadczona na miejscu u klienta. 2. Czas reakcji serwisu - do końca następnego dnia roboczego od chwili zgłoszenia. 3. Serwis urządzeń musi być realizowany przez producenta lub Autoryzowanego Partnera Serwisowego producenta – dołączone do oferty oświadczenie producenta potwierdzające, że serwis będzie realizowany przez Autoryzowanego Partnera Serwisowego producenta lub bezpośrednio przez producenta. 4. Firma serwisująca musi posiadać ISO 9001 na świadczenie usług serwisowych oraz posiadać autoryzację producenta serwera – dołączony do oferty dokument potwierdzający spełnienie tego wymogu. 5. W przypadku awarii dysku twardego dysk pozostaje u Zamawiającego. |
| SR1-19 | Inne | 1. Możliwość sprawdzenia na stronie internetowej producenta oferowanego serwera, po podaniu numeru seryjnego - konfiguracji sprzętowej serwera oraz warunków gwarancji. 2. Dostęp do najnowszych sterowników i uaktualnień na stronie producenta serwera, realizowany poprzez podanie na stronie internetowej producenta numeru seryjnego lub modelu serwera. |

* + 1. **Serwer rack typu II – 33 sztuki**

**Producent ………………………….….**

**Model ……………………….…….**

| **Identyfikator wymagania** | **Wymaganie** | **Opis wymagania** |
| --- | --- | --- |
| SR2-1 | Obudowa | 1. Maksymalnie 2U RACK 19 cali (wraz z szynami montażowymi oraz ramieniem do prowadzenia kabli, umożliwiającymi serwisowanie serwera w szafie rack bez wyłączania urządzenia). 2. Wyposażona w minimum 16 zatok dyskowych SFF (2,5”) typu Hot Swap wspierających dyski SAS oraz SATA. 3. Wyposażona w zamykany, zdejmowany panel przedni chroniący przed nieuprawionym dostępem do dysków. 4. Wyposażona w czujnik otwarcia obudowy współpracujący z kartą zarządzającą. |
| SR2-2 | Płyta główna | Płyta główna umożliwiająca zainstalowanie co najmniej 2 procesorów, od 8 do 64 rdzeniowych o taktowaniu bazowym do minimum 3.9GHz. |
| SR2-3 | Procesor | Procesor szesnastordzeniowy, klasy x86 - 64 bity, osiągający zaoferowanym modelu serwera w testach SPECrate2017\_int\_base dla konfiguracji 2 procesorowej wynik nie gorszy niż 320 punktów. Wynik testu musi być opublikowany i ogólnie dostępny na stronie <https://spec.org/> - dołączony do oferty wydruk ze strony <https://spec.org/> potwierdzający. że oferowany model serwera w oferowanej konfiguracji tj.: (serwer/procesory) umożliwia osiągniecie powyższego wyniku. |
| SR2-4 | Liczba procesorów | 2 procesory. |
| SR2-5 | Pamięć operacyjna | 1. Minimum 1536GB RDIMM DDR5 minimum 4800 MT/s w modułach o pojemności minimum 64GB każdy. 2. Płyta główna z minimum 32 slotami na pamięć i umożliwiająca instalację do minimum 8TB (przy zastosowaniu odpowiednich procesorów). |
| SR2-6 | Sloty rozszerzeń | Minimum 8 aktywnych gniazd PCI-Express generacji 4, w tym minimum 2 sloty x16 (szybkość slotu – bus width), minimum 6 slotów powinno umożliwiać montaż kart pełnej wysokości (full height). |
| SR2-7 | Dysk twardy | Zainstalowane:  2 dyski SSD Mixed Use, każdy o pojemności minimum 1,92TB, dyski typu Hot Swap. |
| SR2-8 | Kontroler | Serwer wyposażony w kontroler sprzętowy z minimum 8GB cache z mechanizmem podtrzymywania zawartości pamięci cache w razie braku zasilania, zapewniający obsługę 16 napędów dyskowych SAS oraz obsługujący poziomy: RAID 0/1/10/5/50/6/60. |
| SR2-9 | Interfejsy Ethernet | 1. Minimum 4 porty Ethernet 100/1000 Mb/s RJ-45 z funkcją Wake-On-LAN, wsparciem dla PXE, zainstalowane w dedykowanym slocie OCP 3.0. 2. Minimum 2 karty 2 portowe 10/25 Gb Ethernet SFP28, wspierające: SR-IOV, Receive Side Scaling (RSS), Jumbo frames, VMware NetQueue, Microsoft VMQ, IEEE 1588, wszystkie porty wyposażone we wkładki SFP+ 10/25Gb SR. |
| SR2-10 | Karta graficzna | Zintegrowana karta graficzna. |
| SR2-11 | Karta FC | Minimum 1 karta FC - 2 porty FC 32Gb, wszystkie porty wyposażone we wkładki SFP+ 32Gb SW. |
| SR2-12 | Porty | 1. Minimum 4 x USB w tym minimum 2 x USB 3.0, minimum 1 z wymaganych portów USB na przednim panelu obudowy, minimum 1 z wymaganych portów USB wewnątrz serwera. 2. Minimum 2 x VGA lub 1x VGA i 1x DisplayPort, minimum 1 z wymaganych portów video na przednim panelu obudowy. 3. Minimum 1 x RJ45 do zarządzania na tylnym panelu obudowy oraz 1x USB do zarządzania na przednim panelu obudowy. |
| SR2-13 | Zasilacz | 2 sztuki, typu Hot-plug, redundantne, każdy o mocy minimum 1000W oraz o sprawności co najmniej klasy Titanium. |
| SR2-14 | Chłodzenie | Zestaw wentylatorów redundantnych typu hot-plug. |
| SR2-15 | Karta/moduł zarządzający | Niezależna od system operacyjnego, zintegrowana z płytą główną serwera, posiadająca minimalną funkcjonalność:   1. monitorowanie podzespołów serwera: temperatura, zasilacze, wentylatory, procesory, pamięć RAM, kontrolery macierzowe i dyski(fizyczne i logiczne), karty sieciowe 2. wparcie dla agentów zarządzających lub możliwość pracy w trybie bezagentowym – bez agentów zarządzania instalowanych w systemie operacyjnym z generowaniem alertów SNMP 3. dostęp do karty zarządzającej poprzez dedykowany port RJ45 z tyłu serwera, 4. dostęp do karty możliwy z poziomu przeglądarki webowej (GUI), z poziomu linii komend, poprzez interfejs IPMI 2.0 (Intelligent Platform Management Interface) 5. wbudowane narzędzia diagnostyczne 6. zdalna konfiguracji serwera (BIOS) i instalacji systemu operacyjnego 7. wbudowany mechanizm logowania zdarzeń serwera i karty zarządzającej w tym włączanie/wyłączanie serwera, restart, zmiany w konfiguracji 8. przesyłanie alertów poprzez e-mail oraz przekierowanie SNMP (SNMP passthrough) 9. obsługa zdalnego serwera logowania (remote syslog) 10. wirtualna zdalna konsola, tekstowa i graficzna, z dostępem do myszy i klawiatury i możliwością podłączenia wirtualnych napędów FDD, CD/DVD i USB i i wirtualnych folderów 11. monitorowanie zasilania oraz zużycia energii przez serwer w czasie rzeczywistym z możliwością graficznej prezentacji 12. konfiguracja maksymalnego poziomu pobieranej mocy przez serwer (capping) 13. zdalna aktualizacja oprogramowania (firmware) 14. zarządzanie grupami serwerów, w tym:     1. tworzenie i konfiguracja grup serwerów     2. sterowanie zasilaniem (wł./wył.)     3. możliwość równoczesnej obsługi przez 2 administratorów 15. autentykacja dwuskładnikowa (Kerberos) 16. wsparcie dla Microsoft Active Directory 17. obsługa TSL i SSH 18. wsparcie dla IPv4 oraz iPv6, obsługa SNMP v3 oraz RESTful API 19. możliwość autokonfiguracji sieci karty zarządzającejj (DNS/DHCP) |
| SR2-16 | Oprogramowanie do zarządzania | Dodatkowe oprogramowanie umożliwiające zarządzanie poprzez sieć, spełniające minimalne wymagania:   1. integracja z Active Directory; 2. możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta; 3. wsparcie dla protokołów SNMP, IPMI, Linux SSH, Redfish; 4. szczegółowy opis wykrytych systemów oraz ich komponentów; 5. możliwość eksportu raportu do CSV, HTML, PDF; 6. grupowanie urządzeń w oparciu o kryteria użytkownika; 7. tworzenie automatycznie grup urządzeń w oparciu o dowolny element konfiguracji serwera np.: nazwa, lokalizacja, system operacyjny, obsadzenie slotów PCIe, pozostałego czasu gwarancji; 8. możliwość uruchamiania narzędzi zarządzających w poszczególnych urządzeniach; 9. szybki podgląd stanu środowiska; 10. podsumowanie stanu dla każdego urządzenia; 11. szczegółowy status urządzenia/elementu/komponentu; 12. generowanie alertów przy zmianie stanu urządzenia; 13. integracja z service desk Producenta dostarczonej platformy sprzętowej; 14. możliwość przejęcia zdalnego pulpitu; 15. możliwość podmontowania wirtualnego napędu; 16. kreator umożliwiający dostosowanie akcji dla wybranych alertów; 17. przesyłanie alertów „as-is” do innych konsol firm trzecich; 18. możliwość definiowania ról administratorów; 19. możliwość zdalnej aktualizacji oprogramowania wewnętrznego serwerów; 20. aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania); 21. możliwość instalacji oprogramowania wewnętrznego bez potrzeby instalacji agenta; 22. możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów; 23. 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; 24. możliwość tworzenia sprzętowej konfiguracji bazowej i na jej podstawie weryfikacji środowiska w celu wykrycia rozbieżności; 25. wdrażanie serwerów, rozwiązań modularnych oraz przełączników sieciowych w oparciu o profile; 26. możliwość migracji ustawień serwera wraz z wirtualnymi adresami sieciowymi (MAC, WWN, IQN) między urządzeniami; 27. tworzenie gotowych paczek informacji umożliwiających zdiagnozowanie awarii urządzenia przez serwis producenta; 28. zdalne uruchamianie diagnostyki serwera; |
| SR2-17 | Wsparcie dla systemów operacyjnych i systemów wirtualizacyjnych | 1. Microsoft Windows Server 2019 oraz 2022 – potwierdzenie spełnienia tego wymogu poprzez wydruk ze strony <https://www.windowsservercatalog.com/> dołączony do oferty. 2. Red Hat Enterprise Linux (RHEL) 8.6 oraz 9 - potwierdzenie spełnienia tego wymogu poprzez wydruk ze strony <https://catalog.redhat.com/> dołączony do oferty. 3. VMware ESXi 7.0 U3, 8.0 U2 oraz 8.0 U3 - potwierdzenie spełnienia tego wymogu poprzez wydruk ze strony <https://www.vmware.com/resources/compatibility> dołączony do oferty. |
| SR2-18 | Certyfikaty | 1. Certyfikat ISO 9001 dla producenta sprzętu obejmujący proces projektowania i produkcji – dołączony do oferty dokument potwierdzający spełnienie tego wymogu. 2. Certyfikat ISO 14001 dla producenta sprzętu – dołączony do oferty dokument potwierdzający spełnienie tego wymogu. 3. Urządzenia wyprodukowane są przez producenta, zgodnie z normą PN-EN ISO 50001 lub oświadczenie producenta o stosowaniu w fabrykach polityki zarządzania energią, która jest zgodna z obowiązującymi przepisami na terenie Unii Europejskiej – dołączony do oferty dokument potwierdzający spełnienie tego wymogu. 4. Deklaracja zgodności CE – dołączona do oferty. 5. 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 Bronze według normy wprowadzonej w 2019 roku – dołączony do oferty dokument potwierdzający spełnienie tego wymogu. 6. Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia producenta serwera (wg wytycznych Krajowej Agencji Poszanowania Energii S.A, zawartych w dokumencie „Opracowanie propozycji kryteriów środowiskowych dla produktów zużywających energię możliwych do wykorzystania przy formułowaniu specyfikacji na potrzeby zamówień publicznych”, pkt 3.4.2.1; dokument z grudnia 2006 r.), w szczególności zgodności z normą ISO 1043-4 dla płyty głównej oraz elementów wykonanych z tworzyw sztucznych o masie powyżej 25 gr – dołączony do oferty dokument potwierdzający spełnienie tego wymogu. 7. Oświadczenie producenta serwera, potwierdzające, że sprzęt pochodzi z oficjalnego kanału dystrybucyjnego producenta – dołączone do oferty. |
| SR2-19 | Warunki gwarancji: | 1. Gwarancja producenta 36 miesięcy, świadczona na miejscu u klienta. 2. Czas reakcji serwisu - do końca następnego dnia roboczego od chwili zgłoszenia. 3. Serwis urządzeń musi być realizowany przez producenta lub Autoryzowanego Partnera Serwisowego producenta – dołączone do oferty oświadczenie producenta potwierdzające, że serwis będzie realizowany przez Autoryzowanego Partnera Serwisowego producenta lub bezpośrednio przez producenta. 4. Firma serwisująca musi posiadać ISO 9001 na świadczenie usług serwisowych oraz posiadać autoryzację producenta serwera – dołączony do oferty dokument potwierdzający spełnienie tego wymogu. 5. W przypadku awarii dysku twardego dysk pozostaje u Zamawiającego. |
| SR2-20 | Inne | 1. Możliwość sprawdzenia na stronie internetowej producenta oferowanego serwera, po podaniu numeru seryjnego - konfiguracji sprzętowej serwera oraz warunków gwarancji. 2. Dostęp do najnowszych sterowników i uaktualnień na stronie producenta serwera, realizowany poprzez podanie na stronie internetowej producenta numeru seryjnego lub modelu serwera. |

* 1. **MACIERZE DYSKOWE**
     1. **Macierz blokowa Typ I – 11 sztuk**

**Producent ………………………….….**

**Model ……………………….…….**

| **Identyfikator wymagania** | **Wymaganie** | **Opis wymagania** |
| --- | --- | --- |
| MB1-1 | Licencja | Rozwiązanie musi być dostarczone z licencjami na wszystkie dostępne dla systemu funkcjonalności oraz maksymalnej do uzyskania w oferowanym modelu pojemności RAW. |
| MB1-2 | Standard RACK | Wymagane jest rozwiązanie mieszczące się w standardowej, pojedynczej szafie RACK 19”, Preferowane jest rozwiązanie kompaktowe tj. o jak najmniejszym rozmiarze fizycznym. |
| MB1-3 | Ochrona nośników danych | Musi być realizowana za pomocą tzw. rozproszonej parzystości na poziomie blokowym. Niedopuszczalne są klasyczne realizacje ochrony danych oparte o grupy dysków w RAID 4/5/6 czyli niedopuszczalne jest stosowanie dedykowanych dysków parzystości tzw. parity drives.  Niedopuszczalne jest stosowanie dysków dedykowanych tylko do konkretnych typów danych. |
| MB1-4 | Bezpieczeństwo danych | Rozwiązanie musi szyfrować wszystkie przechowywane dane minimum algorytmem AES-256 lub silniejszym oraz mieć możliwość szyfrowania wszystkich nośników obsługiwanych w urządzeniu.  Szyfrowanie danych nie może mieć wpływu na wydajność rozwiązania*.*  Klucz szyfrujący musi być przechowywany na macierzy i generowany w sposób uniemożliwiający odczyt danych z usuniętych z macierzy nośników. |
| MB1-5 | Zasoby dyskowe | Macierz musi mieć możliwość utworzenia grupy RAID w której dwa dyski, które będą przechowywać dane parzystości.  Awaria dwóch dowolnych dysków w obrębie takiej pojedynczej grupy RAID nie może spowodować utraty danych.  Kontrolery macierzy dyskowej muszą obsługiwać minimum 700 dysków oraz pojemność surową minimum 3PB.  Należy dodatkowo dostarczyć dyski zapasowe lub pojemność zapasową w ilości zgodnej z zaleceniami producenta dla oferowanej konfiguracji – nie mniej niż 1 zapasowy dysk lub jego pojemność na 30 dysków danego typu.  Podczas awarii dysku kontroler macierzy dyskowej musi automatycznie rozpoczynać odtwarzanie danych na fizycznym dysku zapasowym lub pojemności zapasowej.  W przypadku stosowania dysku zapasowego proces odtwarzania danych nie może wiązać się z procesem przenoszenia danych po wymianie dysku uszkodzonego (dysk wymieniony musi być automatycznie uznany za zapasowy).  Oferowana macierz musi zawierać:  a. 6 dysków SSD 400GB 12Gb SAS  b. 6 dysków SSD 3.2TB 12GB SAS  c. 56 dysków 1.8TB 2.5” o prędkości obr. 10 000 obr/min 12Gb SAS |
| MB1-6 | Kontrolery macierzy dyskowej | Macierz dyskowa musi być złożona z minimum jednej pary identycznych kontrolerów tworzących klaster wysokiej dostępności (high availability cluster). Kontrolery muszą udostępniać dane poprzez iSCSI, FCP, CIFS oraz NFS.  Obszar pamięci cache przeznaczony do zapisów danych, musi posiadać lustrzaną kopię (ang. mirror).  W przypadku awarii zasilania dane nie zapisane na dyskach muszą być zabezpieczone za pomocą podtrzymania bateryjnego przez minimum 72 godziny lub zachowane w pamięci nieulotnej kontrolera do momentu przywrócenia zasilania.  Kontrolery w klastrze wysokiej dostępności muszą oferować funkcjonalność automatycznego przejmowania funkcjonalności i zadań w przypadku awarii drugiego kontrolera w tej samej parze.  Macierz musi mieć minimum 192GB pamięci cache obsługującej zapis i odczyt dostępnej dla wszystkich wolumenów macierzy.  W przypadku wyposażenia macierzy w dyski różnych typów (SSD, SAS, NL\_SAS), system operacyjny kontrolerów musi natywnie obsługiwać automatyczny tiering bloków danych pomiędzy tymi dyskami.  Macierz musi mieć możliwość obsługi różnych poziomów RAID równocześnie. Minimum RAID 1 (lub 10) i 6. Macierz musi umożliwiać konstrukcję urządzenia LUN w taki sposób, aby zawierał dane zabezpieczone poziomami RAID 1 (lub 10), RAID 6 jednocześnie.  Awaria dowolnego pojedynczego aktywnego elementu macierzy dyskowej nie może powodować przerwy w dostępie do danych.  Musi być możliwe utworzenie minimum 1500 wolumenów blokowych o rozmiarze minimum 100TB i plikowych o rozmiarze minimum 100TB.  Macierz musi posiadać wbudowaną funkcjonalność typu thin provisioning umożliwiającą alokację wirtualnej przestrzeni dyskowej, do której fizyczne dyski mogą być dostarczone w przyszłości.  Należy zapewnić możliwość natywnej replikacji danych na poziomie kontrolerów z posiadanymi przez Zamawiającego macierzami Dell Unity. |
| MB1-7 | Interfejsy | Rozwiązanie musi posiadać możliwość instalacji każdego z typów portów:   1. FC 32 Gb 2. 10GBaseT/iSCSI 3. 10GbE/iSCSI 4. 25GbE/iSCSI   Porty przeznaczone do podłączenia hostów nie mogą być wykorzystane do połączeń wewnątrz macierzy (np. pomiędzy kontrolerami).  Oferowana macierz musi posiadać minimum 8 portów FC 32Gb/s z modułami SFP+ SR do dołączenia serwerów bezpośrednio lub do dołączenia do sieci SAN, rozłożone symetrycznie na kontrolery RAID. |
| MB1-8 | Kopie migawkowe | System operacyjny macierzy dyskowej musi natywnie obsługiwać mechanizm kopii migawkowych, który będzie dostępny dla wszystkich rodzajów danych udostępnianych. Niedopuszczalne są rozwiązania wykonujące kopie migawkowe jedynie w trybie Copy On Write dla dowolnego rodzaju danych (blokowe lub plikowe). Licencja na wszystkie opisane funkcjonalności musi obejmować całą powierzchnię użytkową macierzy.  Odtwarzanie plików i folderów z kopii migawkowych wykonanych dla wolumenów plikowych udostępnionych dla systemów typu Windows i Unix musi być dostępne za pomocą wydzielonego udziału sieciowego z zachowaniem praw dostępu na poziomie użytkownika.  System operacyjny macierzy dyskowej musi umożliwiać i wykonywanie kopii migawkowych wolumenów plikowych, w trybie on-line, bez zatrzymywania operacji odczytu i zapisu. Deklarowana przez producenta liczba kopii migawkowych musi wynosić minimum 256 na wolumen.  Musi być możliwe odtwarzanie danych z kopii migawkowych bezpośrednio na wolumen produkcyjny.  Musi być możliwe zaprezentowanie kopii migawkowej w trybie do odczytu i zapisu.  Należy dostarczyć oprogramowanie do wykonywania spójnych kopii danych aplikacji: Exchange, SQL Server, Oracle, VMware dla blokowych i plikowych datastore. Spójne kopie rozumiane jako funkcjonalność automatycznego przełączenia aplikacji w tryb wykonania spójnej kopii swoich danych. Oprogramowanie to musi rozpoznać na których wolumenach logicznych aplikacja składuje swoje dane i wykonać kopie tylko tych wolumenów. |
| MB1-9 | Obsługiwane protokoły | System operacyjny macierzy dyskowej musi mieć możliwość udostępniania danych za pomocą protokołów: NFS, CIF, iSCSI i FCP.  Jednoczesna obsługa różnych protokołów dostępu do danych nie może być zrealizowana za pomocą dodatkowego oprogramowania ani dodatkowych urządzeń pośredniczących typu wirtualizator, gateway, switch, etc. Macierz musi umożliwiać jednoczesne prezentowanie urządzeń typu LUN za pomocą protokołów FC oraz iSCSI. |
| MB1-10 | Pozostałe wymagania | System operacyjny macierzy dyskowej musi umożliwiać dynamiczną zmianę rozmiaru wolumenów danych: (zwiększanie) bez przerywania pracy i bez przerywania użytkownikom zewnętrznym dostępu do danych  Musi być możliwość konfiguracji macierzy dyskowej za pomocą GUI, zbieranie i wyświetlanie informacji o stanie zasobów macierzy dyskowej, prezentowanie i gromadzenie zdarzeń zachodzących w macierzy dyskowej oraz prezentowanie bieżących statystyk wydajnościowych macierzy dyskowej, podgląd parametrów wydajnościowych macierzy dyskowej w czasie rzeczywistym.  Dostęp do CLI systemu operacyjnego kontrolerów musi odbywać się przy użyciu połączenia szyfrowanego.  W systemie operacyjnym kontrolera musi być możliwość utworzenia wirtualnych serwerów plików, a każdy wirtualny serwer plików musi obsługiwać użytkowników z innej domeny Microsoft [MS Active Directory).  W celu zabezpieczania danych macierz dyskowa musi mieć możliwość replikacji jej zasobów na zasoby innej macierzy tej samej rodziny. Replikacja musi działać na poziomie systemu operacyjnego macierzy i pracować w trybie asynchronicznym bez potrzeby użycia urządzeń zewnętrznych typu gatawey, serwer pośredniczący, etc. Musi istnieć możliwość odwrócenia kierunku replikacji. Replikacja danych między macierzami nie może być zrealizowana zewnętrznym narzędziem software'owym. Licencja na replikację jest przedmiotem obecnego postępowania.  System operacyjny kontrolerów macierzy musi oferować funkcjonalność QoS (Quality of Service) dla dowolnego wolumenu blokowego, to znaczy musi być możliwość ograniczenia liczby operacji na sekundę lub przepustowości w kB (lub analogicznych jednostkach) na sekundę, jaka jest możliwa do uzyskania ze wskazanego przez administratora wolumenu.  Wymagane jest szyfrowanie danych na dyskach. Należy dostarczyć niezbędne licencje na całą pojemność macierzy. |
| MB1-11 | Certyfikaty | Certyfikat ISO 9001 dla producenta sprzętu obejmujący proces projektowania i produkcji – dołączony do oferty dokument potwierdzający spełnienie tego wymogu.  Certyfikat ISO 14001 dla producenta sprzętu – dołączony do oferty dokument potwierdzający spełnienie tego wymogu.  Urządzenia wyprodukowane są przez producenta, zgodnie z normą PN-EN ISO 50001 lub oświadczenie producenta o stosowaniu w fabrykach polityki zarządzania energią, która jest zgodna z obowiązującymi przepisami na terenie Unii Europejskiej – dołączony do oferty dokument potwierdzający spełnienie tego wymogu.  Oświadczenie producenta macierzy, potwierdzające, że sprzęt pochodzi z oficjalnego kanału dystrybucyjnego producenta – dołączone do oferty. |
| MB1-12 | Warunki gwarancji | Gwarancja producenta 36 miesięcy, świadczona na miejscu u klienta.  Czas reakcji serwisu - do końca następnego dnia roboczego od chwili zgłoszenia.  Serwis urządzeń musi być realizowany przez producenta lub Autoryzowanego Partnera Serwisowego producenta – dołączone do oferty oświadczenie producenta potwierdzające, że serwis będzie realizowany przez Autoryzowanego Partnera Serwisowego producenta lub bezpośrednio przez producenta.  Firma serwisująca musi posiadać ISO 9001 na świadczenie usług serwisowych oraz posiadać autoryzację producenta serwera – dołączony do oferty dokument potwierdzający spełnienie tego wymogu.  W przypadku awarii dysku twardego dysk pozostaje u Zamawiającego. |

* 1. **DEDUPLIKATORY**
     1. **Deduplikator typ I – 10 sztuk**

**Producent ………………………….….**

**Model ……………………….…….**

| Identyfikator wymagania | Opis wymagania |
| --- | --- |
| DD1-1 | Urządzenie musi być przeznaczone do deduplikacji i przechowywania kopii zapasowych. Urządzenie musi spełniać wymagania wyspecyfikowane w niniejszej tabeli. |
| DD1-2 | Dostarczone urządzenie musi oferować przestrzeń min. 16TB netto (powierzchni użytkowej) bez uwzględniania mechanizmów protekcji – przestrzeń dedykowana do gromadzenia deduplikatów. |
| DD1-3 | Wymagane wsparcie funkcjonalności SmartScale w połączeniu z eksploatowanymi przez Zamawiajacego urządzeniami DD9400. |
| DD1-4 | Dostarczone urządzenie musi umożliwiać rozbudowę o warstwę typu CLOUD dedykowaną do długotrwałego przechowywania danych (tzw. Long Term Retention) – dane o określonej retencji (zgodnie z założoną polityka retencyjną), bez pośrednictwa dodatkowych urządzeń (typu GATEWAY) powinny zostać przemigrowane (w postaci zdeduplikowanej) na dodatkową warstwę (wymagane wsparcie lokalne dla eksploatowanaego przez Zamawiającego ECS oraz w chmurze publicznej dla AWS, Microsoft Azure oraz GCP ). Wymagana enkrypcja danych przechowywanych na warstwie typu Cloud. Wymagane dostarczenie licencji na przestrzeń min. 60TB netto dla warstwy CLOUD. Wymagana funkcjonalność musi oficjalnie wspierać eksploatowaną przez Zamawiającego aplikację NetWorker. |
| DD1-5 | Oferowane urządzenie musi posiadać minimum  8 portów Ethernet 10Gb/s OP (wymagana pełna obsada wkładek)  4 porty 10Gb/s Eth BaseT  wymagana możliwość obsługi każdym z w/w portów protokołów CIFS, NFS, deduplikacja na źródle  2 porty FC 16Gb/s  wymagana możliwość obsługi poprzez porty FC protokołów VTL oraz deduplikacji na źródle. |
| DD1-6 | Oferowane urządzenie musi umożliwiać jednoczesny dostęp wszystkimi poniższymi protokołami:  CIFS, NFS  zapewniającym deduplikację na źródle, wymagane wsparcie dla Veeam Backup and Replication, NetWorker  VTL (min. 10 jednocześnie) |
| DD1-7 | Wymagane jest dostarczenie licencji, pozwalającej na jednoczesną obsługę protokołów CIFS, NFS, dedupliakacja na źródle, VTL do oferowanej pojemności urządzenia |
| DD1-8 | Oferowane pojedyncze urządzenie musi osiągać zagregowaną wydajność (dla maksymalnej konfiguracji) protokołami: NFS co najmniej 10 TB/h (dane podawane przez producenta) oraz co najmniej 20 TB/h z wykorzystaniem deduplikacji na źródle (dane podawane przez producenta). |
| DD1-9 | Urządzenie musi pozwalać na jednoczesną obsługę minimum 250 strumieni w tym jednocześnie:  zapis danych minimum 150 strumieniami  odczyt danych minimum 50 strumieniami  replikacja minimum 50 strumieniami  pochodzących z różnych aplikacji oraz dowolnych protokołów (CIFS, NFS, VTL, deduplikacja na źródle) oraz dowolnych interfejsów (FC, LAN) w tym samym czasie.  Wymienione wartości 250 jednoczesnych strumieni dla wszystkich protokołów (czyli jednocześnie 150 dla zapisu i jednocześnie 50 strumieni dla odczytu i jednocześnie 50 strumieni dla replikacji) musi mieścić w przedziale oficjalnie rekomendowanym i wspieranym przez producenta urządzenia.  Wszystkie zapisywane strumienie muszą podlegać globalnej deduplikacji przed zapisem na dysk (in-line) jak opisano w niniejszej specyfikacji. |
| DD1-10 | Oferowane urządzenie musi mieć możliwość emulacji następujących bibliotek taśmowych:  StorageTek L180  IBM TS 3500 |
| DD1-11 | Oferowane urządzenie musi mieć możliwość emulacji napędów taśmowych min. LTO5 oraz LTO7 |
| DD1-12 | Urządzenie musi umożliwiać (w przypadku VTL’a) emulację minimum 250 napędów, emulację min. 30 000 slotów w przypadku poj. biblioteki taśmowej oraz emulację sumarycznie min. 60 000 slotów. |
| DD1-13 | Oferowane urządzenie musi deduplikować dane in-line przed zapisem na nośnik dyskowy. Na wewnętrznych dyskach urządzenia nie mogą być zapisywane dane w oryginalnej postaci (niezdeduplikowanej) z jakiegokolwiek fragmentu strumienia danych przychodzącego do urządzenia. |
| DD1-14 | Technologia deduplikacji musi wykorzystywać algorytm bazujący na zmiennym, dynamicznym bloku jednak o wielkości nie większej niż 12 kB.  Algorytm ten musi samoczynnie i automatycznie dopasowywać się do otrzymywanego strumienia danych co oznacza, że urządzenie musi dzielić otrzymany pojedynczy strumień danych na bloki o różnej długości, bez konieczności podejmowania czynności mających na celu ustalenie predefiniowanej długości bloków używanych do deduplikacji danych określonego typu. Deduplikacja zmiennym, dynamicznym blokiem oznacza, że wielkość każdego bloku (na jaki są dzielone dane pojedynczego strumienia backupowego) może być inna niż poprzedniego oraz jest indywidualnie ustalana przez algorytm deduplikacji zastosowany w urządzeniu, oferowane urządzenie nie może dzielić jakiegokolwiek pojedynczego strumienia danych backupowych na bloki o ustalonej, tej samej długości. |
| DD1-15 | Oferowany produkt musi posiadać obsługę mechanizmów globalnej deduplikacji dla danych otrzymywanych jednocześnie wszystkimi protokołami (CIFS, NFS, VTL, deduplikacja na źródle) przechowywanych w obrębie całego urządzenia co oznacza, że przechowywany na urządzeniu fragment danych nie może być ponownie zapisany bez względu na to, jakim protokołem zostanie ponownie otrzymany. Wszystkie emulowane jednocześnie w obrębie urządzenia biblioteki wirtualne (VTL) oraz udziały NFS/CIFS również powinny podlegać globalnej deduplikacji – blok danych otrzymany i zapisany w wirtualnej bibliotece „A”, nie może zostać ponownie zapisany jeśli trafi do innej wirtualnej biblioteki „B” w obrębie tego samego urządzenia (to samo dotyczy udziałów NFS/CIFS). Przestrzeń składowania zdeduplikowanych danych musi być jedna dla wszystkich protokołów dostępowych, co oznacza zastosowanie pojedynczej bazy deduplikatów bez względu na ilość/rodzaj używanych jednocześnie protokołów dostępowych. |
| DD1-16 | Proces deduplikacji musi odbywać się in-line – w pamięci urządzenia, przed zapisem danych na nośnik dyskowy. Zapisowi na system dyskowy muszą podlegać tylko unikalne bloki danych nie zapisane jeszcze na system dyskowy urządzenia. Dotyczy to każdego fragmentu przychodzących do urządzenia danych. Wymaganie nie będzie spełnione jeżeli deduplikacja in-line realizowana będzie przez zewnętrzną aplikację backup’ową. Wymaganie deduplikacji in-line dotyczy zapisu danych przez każdy z wymaganych intefejsów, w przypadku interfejsów: NFS, CIFS oraz VTL realizacja deduplikacji in-line nie może w żadnym stopniu zależeć od konkretnej aplikacji backu’owej, dane zapisywane poprzez interfejsy NFS CIFS bez użycia jakiejkolwiek aplikacji backup’owej również muszą być deduplikowane w sposób in-line |
| DD1-17 | Proponowane rozwiązanie nie może w żadnej fazie korzystać (w całości lub częściowo) z bufora na składowanie danych w postaci oryginalnej (niezdeduplikowanej) w celu ich późniejszej deduplikacji (wymagana deduplikacja in-line) |
| DD1-18 | Wszystkie unikalne bloki przed zapisaniem na dysk muszą być dodatkowo kompresowane. |
| DD1-19 | Tryb zapisu zabezpieczanych danych nie może umożliwiać nadpisywania danych, dane mogą być zapisywane jedynie w trybie append-only, dane dla których wygasła retencja powinny zostać usunięte podczas procesu czyszczenia tzw. Cleaning, wymaganie dotyczy wszystkich danych zapisanych na urządzeniu a nie wybranych grup danych objętych działaniem blokad zabezpieczających przed usunięciem/modyfikacją danych. |
| DD1-20 | Oferowane urządzenie musi wspierać (wymagane formalne wsparcie producenta urządzenia), co najmniej następujące aplikacje: NetWorker, RMAN, Microsoft SQL Server Management Studio.  W przypadku współpracy z każdą z poniższych aplikacji:  NetWorker  RMAN (dla ORACLE)  Microsoft SQL Server Management Studio (dla Microsoft SQL)  urządzenie musi umożliwiać deduplikację na źródle i przesłanie nowych, nie znajdujących się jeszcze na urządzeniu bloków poprzez sieć LAN.  Deduplikacja w wyżej wymienionych przypadkach musi zapewniać aby z zabezpieczanych serwerów do urządzenia były transmitowane poprzez sieć LAN jedynie fragmenty danych nie znajdujące się dotychczas na urządzeniu. |
| DD1-21 | W przypadku przyjmowania backupów z NetWorker, Oracle RMAN oraz Microsoft MSSQL (przy wykorzystaniu Microsoft SQL Server Management Studio), urządzenie musi umożliwiać deduplikację na źródle i przesłanie nowych, nieznajdujących się jeszcze na urządzeniu bloków poprzez sieć FC.  Deduplikacja w wyżej wymienionych przypadkach musi zapewniać aby z serwerów do urządzenia były transmitowane poprzez sieć FC tylko fragmenty danych nie znajdujące się dotychczas na urządzeniu. |
| DD1-22 | Oferowane urządzenie musi umożliwiać uruchamianie maszyn wirtualnych VMware bezpośrednio z danych backupowych bez konieczności odtwarzania danych, funkcjonalność ta musibyć wspierana przez aplikację NetWorker. |
| DD1-23 | Wymagana funkcjonalność Load Balancing oraz Link Failover w obrębie portów wykorzystywanych przez aplikację backupową, wymagane wsparcie tej funkcjonlaności w przypadku aplikacji NetWorker. |
| DD1-24 | Wymagane wsparcie dla backupów typu Virtual Synthetics w przypadku eksploatowanej aplikacji NetWorker. |
| DD1-25 | W przypadku deduplikacji na źródle poprzez sieć IP (LAN oraz WAN), wymagana możliwość szyfrowania komunikacji kluczem minimum 256 bitów. |
| DD1-26 | Urządzenie musi umożliwiać zaszyfrowanie przechowywanych danych, wymagane licencje umożliwiające zaszyfrowanie i przechowywanie zaszyfrowanych danych w obrębie maksymalnej pojemności oferowanego urządzenia. |
| DD1-27 | Urządzenie musi wspierać deduplikację na źródle poprzez sieć FC (SAN) minimum dla następujących systemów operacyjnych:   1. Windows 2. Linux (RedHat, SuSE) |
| DD1-28 | Oferowane urządzenie musi umożliwiać bezpośrednią replikację danych do drugiego urządzenia takiego samego typu oraz urządzeń DD9400 eksploatowanych przez Zamawiającego. Konfiguracja replikacji musi być możliwa w każdym z trybów:  \* jeden do jednego  \* wiele do jednego  \* jeden do wielu  \* kaskadowej (urządzenie A replikuje dane do urządznia B, które te same dane replikuje do urządzenia C).  Replikacja musi się odbywać w trybie asynchronicznym. Transmitowane mogą być tylko te fragmenty danych (bloki) które nie znajdują się na docelowym urządzeniu. Ewentualna licencja na replikację musi być dostarczona w ramach postępowania. |
| DD1-29 | Urządzenie musi umożliwiać wydzielenie określonych portów Ethernet dedykowanych do replikacji. |
| DD1-30 | W przypadku wykorzystania portów Ethernet do replikacji urządzenie musi umożliwiać przyjmowanie backupów, odtwarzanie danych, przyjmowanie strumienia replikacji, wysyłanie strumienia replikacji tymi samymi portami. |
| DD1-31 | W przypadku replikacji danych między urządzeniami oferowanego typu a także oferowanym urządzeniem oraz urządzeniami DD9400 eksploatowanymi przez Zamawiającego, wymagana możliwość kontroli przez: NetWorker, RMAN oraz Microsoft SQL Server Management Studio, muszą być możliwe do uzyskania jednocześnie wszystkie następujące funkcjonalności:   1. replikacja odbywa się bezpośrednio między dwoma urządzeniami bez udziału serwerów pośredniczących 2. replikacji podlegają tylko te fragmenty danych, które nie znajdują się na docelowym urządzeniu 3. replikacja zarządzana jest z poziomu wymaganej aplikacji 4. aplikacja posiada informację o obydwu kopiach zapasowych znajdujących się w obydwu urządzeniach bez konieczności przeprowadzania procesu inwentaryzacji |
| DD1-32 | Oferowane urządzenie musi działać poprawnie przy zapełnieniu danymi na poziomie co najmniej 90%. Dokumentacja urządzenia nie może wskazywać na ew. problemy, obostrzenia, które są efektem zapełnieniu urządzenia zabezpieczanymi danymi, na poziomie mniejszym niż 90%. |
| DD1-33 | Wymagana możliwość ograniczenia pasma używanego do replikacji między dwoma urządzeniami – oferowane urządzenie powinno być wyposażone w mechanizm umożliwiający zarządzaniem stopnia wykorzystania pasma na potrzeby replikacji. |
| DD1-34 | Zdeduplikowane i skompresowane dane przechowywane w obrębie podsystemu dyskowego urządzenia muszą być chronione za pomocą technologii RAID 6 bądź równoważnej. |
| DD1-35 | Oferowane urządzenie musi umożliwiać wykonywanie SnapShot’ów, czyli umożliwiać zamrożenie obrazu danych (stanu backupów) w urządzeniu na określoną chwilę. Oferowane urządzenie musi również umożliwiać odtworzenie danych ze Snapshot’u.  Odtworzenie danych ze Snapshot’u nie może wymagać konieczności nadpisania danych produkcyjnych jak również nie może oznaczać przerwy w normalnej pracy urządzenia (przyjmowania/odtwarzania backupów).  Wymagana możliwość wykorzystania funkcjonalności SnapShot dla danych przesyłanych dowolnym z wymaganych interfejsów urządzenia. |
| DD1-36 | Urządzenie musi pozwalać na przechowywanie minimum 700 Snapshotów jednocześnie w obrębie oferowanej przestrzeni, przy zachowaniu globalnej deduplikacji oraz standardowego trybu pracy urządzenia – umożliwiającego wykorzystanie wszystkich dostępnych funkcjonalności. |
| DD1-37 | Urządzenie musi umożliwiać podział na logiczne części. Dane znajdujące się w każdej logicznej części muszą być między sobą deduplikowane (globalna deduplikacja między logicznymi częściami urządzenia). |
| DD1-38 | Urządzenie musi mieć możliwość podziału na minimum 10 logicznych części pracujących równolegle. Producent musi oficjalnie wspierać pracę minimum 10 logicznych części pracujących równolegle z pełną wydajnością urządzenia. |
| DD1-39 | Dla każdej z w/w logicznych części oferowanego urządzenia musi być możliwość zdefiniowania oddzielnego użytkownika zarządzającego daną logiczną częścią deduplikatora. Użytkownicy zarządzający logiczną częścią A muszą widzieć tylko i wyłącznie zasoby logicznej części A i nie mogą widzieć żadnych innych zasobów oferowanego urządzenia. |
| DD1-40 | Wymagana możliwość zaprezentowania każdej z logicznych części oferowanego urządzenia, jako niezależnego urządzenia dostępnego za pośrednictwem:  CIFS  NFS  VTL  deduplikacja na źródle |
| DD1-41 | Urządzenie musi umożliwiać zdefiniowanie blokady skasowania danych (funkcjonalność WORM). Blokada skasowania danych musi chronić plik w zdefiniowanym czasie przed usunięciem pliku, modyfikacją pliku.  Blokada skasowania danych musi działać w dwóch trybach (do wyboru przez administratora):  Możliwość zdjęcia blokady przed upływem ważności danych  Brak możliwości zdjęcia blokady przed upływem ważności danych (COMPLIANCE), w tym wypadku wymagane wsparcie norm SEC 17a-4(f), ISO Standard 15489-1 oraz CFTC Rule 1.31b w zakresie ochrony danych (wymagane potwierdzenie w ogólno dostępnej dokumentacji oferowanego urządzenia)  Wymagana blokada WORM musi być zintegrowana z eksploatowaną aplikacją backup’ową NetWorker co oznacza:  możliwość uruchomienia blokady WORM dla określonych danych z poziomu aplikacji NetWorker  możliwość określenia/wymuszenia czasu blokady z poziomu aplikacji NetWorker  możliwość raportowania od strony aplikacji NetWorker danych zabezpieczonych przed usunięciem wymaganą blokadą WORM  Wymagana możliwość działania z wybranym opóźnieniem wymaganej blokady na określonym katalogu. Licencje na blokadę usunięcia/zmiany przechowywanych plików muszą być dostarczone wraz z urządzeniem.  Wymagana możliwość automatycznego uruchamiania blokady (podczas zapisu) WORM dla danych zapisywanych na obszar objęty działaniem wspomnianej blokady, a także możliwość używania blokady WORM dla obrazu danych uzyskanych poprzez użycie wymaganej funkcjonalności SnapShot. |
| DD1-42 | Urządzenie musi mieć możliwość przechowywania danych niezmienialnych:   1. Video 2. Grafika 3. Nagrania dźwiękowe 4. Pliki pdf na udziałach CIFS/NFS. |
| DD1-43 | Urządzenie musi weryfikować dane po zapisie (nie chodzi o ew. weryfikację danych indeksowych generowanych przez urządzenie ale o weryfikację wszystkich zabezpieczanych danych backup’owych). Każda zapisana na dyskach porcja danych musi być odczytana i porównana z danymi otrzymanymi przez urządzenie. Powyższa weryfikacja musi być realizowana w locie, czyli przed usunięciem z pamięci oryginalnych danych (otrzymanych z aplikacji backupowej), musi być realizowana w trybie ciągłym (a nie ad-hoc), wymagane parametry wydajnościowe urzadzenia muszą uwzględniać tę funkcjonalność. Wymagane potwierdzenie opisanej funkcjonalności w oficjalnej dokumentacji producenta oferowanego urządzenia. Zamawiający zastrzega możliwość prośby o dostarczenie ogólnodostępnej dokumentacji oferowanego produktu potwierdzającego spełnienie wymaganej funkcjonalności). |
| DD1-44 | Urządzenie musi automatycznie usuwać przeterminowane dane (bloki danych nie należące do backupów o aktualnej retencji) w procesie czyszczenia. |
| DD1-45 | Proces usuwania przeterminowanych danych (czyszczenia) nie może uniemożliwiać pracy procesów backupu / odtwarzania danych (zapisu / odczytu danych z zewnątrz do systemu). |
| DD1-46 | Wymagana możliwość zdefiniowania maksymalnego obciążenia urządzenia procesem usuwania przeterminowanych danych (poziomu obciążenia procesora), wymagane potwierdzenie w ogólno dostępnej dokumentacji. Zamawiający zastrzega możliwość prośby o dostarczenie ogólnodostępnej dokumentacji oferowanego produktu potwierdzającego spełnienie wymaganej funkcjonalności) |
| DD1-47 | Wymagana możliwość zdefiniowania harmonogramu wg. którego wykonywany jest proces usuwania przeterminowanych danych (czyszczenia), realizowany równolegle z procesami backup/restore/replication. |
| DD1-48 | Standardowa częstotliwość usuwania przeterminowanych danych (czyszczenie) nie powinna być większa niż 1 raz na tydzień - minimalizując czas w którym backupy/odtworzenia narażone są na spowolnienie (weryfikacja wymagania na podstawie dokumentacji typu DOBRE PRAKTYKI publikowanej przez producenta). |
| DD1-49 | Urządzenie musi posiadać wbudowany mechanizm umożliwiający usunięcie danych poprzez ich nadpisanie, wymagana zgodność ze standardem DoD 5220.22-M |
| DD1-50 | Urządzenie musi umożliwiać systemowo (wbudowana funkcjonalność) - realizację procesu pierwszego czyszczenia dopiero po przekroczeniu 75% zajętości oferowanej przestrzeni. |
| DD1-51 | Urządzenie musi mieć możliwość zarządzania poprzez  Interfejs graficzny dostępny z przeglądarki internetowej  Poprzez linię komend (CLI) dostępną z poziomu ssh (secure shell) |
| DD1-52 | Oprogramowanie do zarządzania musi rezydować na oferowanym na urządzeniu deduplikacyjnym. |
| DD1-53 | Oferowane urządzenie musi mieć możliwość sprawdzenia pakietu upgrade’ującego firmware urządzenia (GUI lub CLI), to znaczy sprawdzenia czy nowa wersja systemu nie spowoduje problemów z urządzeniem. |
| DD1-54 | Urządzenie musi być rozwiązaniem kompletnym, appliancem sprzętowym pochodzącym od jednego producenta. Zamawiający nie dopuszcza stosowania rozwiązań typu gateway. Oferowany typ urządzenia musi być oficjalnie dostępny w ofercie producenta przed ogłoszeniem niniejszego postępowania. |
| DD1-55 | Certyfikat ISO 9001 dla producenta sprzętu obejmujący proces projektowania i produkcji – dołączony do oferty dokument potwierdzający spełnienie tego wymogu.  Certyfikat ISO 14001 dla producenta sprzętu – dołączony do oferty dokument potwierdzający spełnienie tego wymogu.  Urządzenia wyprodukowane są przez producenta, zgodnie z normą PN-EN ISO 50001 lub oświadczenie producenta o stosowaniu w fabrykach polityki zarządzania energią, która jest zgodna z obowiązującymi przepisami na terenie Unii Europejskiej – dołączony do oferty dokument potwierdzający spełnienie tego wymogu.  Oświadczenie producenta deduplikatora, potwierdzające, że sprzęt pochodzi z oficjalnego kanału dystrybucyjnego producenta – dołączone do oferty. |
| DD1-56 | Gwarancja producenta 36 miesięcy, świadczona na miejscu u klienta.  Czas reakcji serwisu - do końca następnego dnia roboczego od chwili zgłoszenia.  Serwis urządzeń musi być realizowany przez producenta lub Autoryzowanego Partnera Serwisowego producenta – dołączone do oferty oświadczenie producenta potwierdzające, że serwis będzie realizowany przez Autoryzowanego Partnera Serwisowego producenta lub bezpośrednio przez producenta.  Firma serwisująca musi posiadać ISO 9001 na świadczenie usług serwisowych oraz posiadać autoryzację producenta serwera – dołączony do oferty dokument potwierdzający spełnienie tego wymogu.  W przypadku awarii dysku twardego/nośnika danych, nośnik pozostaje u Zamawiającego. |

* + 1. **Deduplikator typ II – 1 sztuka**

**Producent ………………………….….**

**Model ……………………….…….**

| Identyfikator wymagania | Opis wymagania |
| --- | --- |
| DD2-1 | Urządzenie musi być przeznaczone do deduplikacji i przechowywania kopii zapasowych. Urządzenie musi spełniać wymagania wyspecyfikowane w niniejszej tabeli. |
| DD2-2 | Dostarczone urządzenie musi oferować przestrzeń min. 32TB netto (powierzchni użytkowej) bez uwzględniania mechanizmów protekcji – przestrzeń dedykowana do gromadzenia deduplikatów. |
| DD2-3 | Wymagane wsparcie funkcjonalności SmartScale w połączeniu z eksploatowanymi przez Zamawiajacego urządzeniami DD9400. |
| DD2-4 | Dostarczone urządzenie musi umożliwiać rozbudowę o warstwę typu CLOUD dedykowaną do długotrwałego przechowywania danych (tzw. Long Term Retention) – dane o określonej retencji (zgodnie z założoną polityka retencyjną), bez pośrednictwa dodatkowych urządzeń (typu GATEWAY) powinny zostać przemigrowane (w postaci zdeduplikowanej) na dodatkową warstwę (wymagane wsparcie lokalne dla eksploatowanaego przez Zamawiającego ECS oraz w chmurze publicznej dla AWS, Microsoft Azure oraz GCP ). Wymagana enkrypcja danych przechowywanych na warstwie typu Cloud. Wymagane dostarczenie licencji na przestrzeń min. 60TB netto dla warstwy CLOUD. Wymagana funkcjonalność musi oficjalnie wspierać eksploatowaną przez Zamawiającego aplikację NetWorker. |
| DD2-5 | Oferowane urządzenie musi posiadać minimum  8 portów Ethernet 10Gb/s OP (wymagana pełna obsada wkładek)  4 porty 10Gb/s Eth BaseT  wymagana możliwość obsługi każdym z w/w portów protokołów CIFS, NFS, deduplikacja na źródle  2 porty FC 16Gb/s  wymagana możliwość obsługi poprzez porty FC protokołów VTL oraz deduplikacji na źródle. |
| DD2-6 | Oferowane urządzenie musi umożliwiać jednoczesny dostęp wszystkimi poniższymi protokołami:  CIFS, NFS  zapewniającym deduplikację na źródle, wymagane wsparcie dla Veeam Backup and Replication, NetWorker  VTL (min. 10 jednocześnie) |
| DD2-7 | Wymagane jest dostarczenie licencji, pozwalającej na jednoczesną obsługę protokołów CIFS, NFS, dedupliakacja na źródle, VTL do oferowanej pojemności urządzenia |
| DD2-8 | Oferowane pojedyncze urządzenie musi osiągać zagregowaną wydajność (dla maksymalnej konfiguracji) protokołami: NFS co najmniej 10 TB/h (dane podawane przez producenta) oraz co najmniej 20 TB/h z wykorzystaniem deduplikacji na źródle (dane podawane przez producenta). |
| DD2-9 | Urządzenie musi pozwalać na jednoczesną obsługę minimum 250 strumieni w tym jednocześnie:  zapis danych minimum 150 strumieniami  odczyt danych minimum 50 strumieniami  replikacja minimum 50 strumieniami  pochodzących z różnych aplikacji oraz dowolnych protokołów (CIFS, NFS, VTL, deduplikacja na źródle) oraz dowolnych interfejsów (FC, LAN) w tym samym czasie.  Wymienione wartości 250 jednoczesnych strumieni dla wszystkich protokołów (czyli jednocześnie 150 dla zapisu i jednocześnie 50 strumieni dla odczytu i jednocześnie 50 strumieni dla replikacji) musi mieścić w przedziale oficjalnie rekomendowanym i wspieranym przez producenta urządzenia.  Wszystkie zapisywane strumienie muszą podlegać globalnej deduplikacji przed zapisem na dysk (in-line) jak opisano w niniejszej specyfikacji. |
| DD2-10 | Oferowane urządzenie musi mieć możliwość emulacji następujących bibliotek taśmowych:  StorageTek L180  IBM TS 3500 |
| DD2-11 | Oferowane urządzenie musi mieć możliwość emulacji napędów taśmowych min. LTO5 oraz LTO7 |
| DD2-12 | Urządzenie musi umożliwiać (w przypadku VTL’a) emulację minimum 250 napędów, emulację min. 30 000 slotów w przypadku poj. biblioteki taśmowej oraz emulację sumarycznie min. 60 000 slotów. |
| DD2-13 | Oferowane urządzenie musi deduplikować dane in-line przed zapisem na nośnik dyskowy. Na wewnętrznych dyskach urządzenia nie mogą być zapisywane dane w oryginalnej postaci (niezdeduplikowanej) z jakiegokolwiek fragmentu strumienia danych przychodzącego do urządzenia. |
| DD2-14 | Technologia deduplikacji musi wykorzystywać algorytm bazujący na zmiennym, dynamicznym bloku jednak o wielkości nie większej niż 12 kB.  Algorytm ten musi samoczynnie i automatycznie dopasowywać się do otrzymywanego strumienia danych co oznacza, że urządzenie musi dzielić otrzymany pojedynczy strumień danych na bloki o różnej długości, bez konieczności podejmowania czynności mających na celu ustalenie predefiniowanej długości bloków używanych do deduplikacji danych określonego typu. Deduplikacja zmiennym, dynamicznym blokiem oznacza, że wielkość każdego bloku (na jaki są dzielone dane pojedynczego strumienia backupowego) może być inna niż poprzedniego oraz jest indywidualnie ustalana przez algorytm deduplikacji zastosowany w urządzeniu, oferowane urządzenie nie może dzielić jakiegokolwiek pojedynczego strumienia danych backupowych na bloki o ustalonej, tej samej długości. |
| DD2-15 | Oferowany produkt musi posiadać obsługę mechanizmów globalnej deduplikacji dla danych otrzymywanych jednocześnie wszystkimi protokołami (CIFS, NFS, VTL, deduplikacja na źródle) przechowywanych w obrębie całego urządzenia co oznacza, że przechowywany na urządzeniu fragment danych nie może być ponownie zapisany bez względu na to, jakim protokołem zostanie ponownie otrzymany. Wszystkie emulowane jednocześnie w obrębie urządzenia biblioteki wirtualne (VTL) oraz udziały NFS/CIFS również powinny podlegać globalnej deduplikacji – blok danych otrzymany i zapisany w wirtualnej bibliotece „A”, nie może zostać ponownie zapisany jeśli trafi do innej wirtualnej biblioteki „B” w obrębie tego samego urządzenia (to samo dotyczy udziałów NFS/CIFS). Przestrzeń składowania zdeduplikowanych danych musi być jedna dla wszystkich protokołów dostępowych, co oznacza zastosowanie pojedynczej bazy deduplikatów bez względu na ilość/rodzaj używanych jednocześnie protokołów dostępowych. |
| DD2-16 | Proces deduplikacji musi odbywać się in-line – w pamięci urządzenia, przed zapisem danych na nośnik dyskowy. Zapisowi na system dyskowy muszą podlegać tylko unikalne bloki danych nie zapisane jeszcze na system dyskowy urządzenia. Dotyczy to każdego fragmentu przychodzących do urządzenia danych. Wymaganie nie będzie spełnione jeżeli deduplikacja in-line realizowana będzie przez zewnętrzną aplikację backup’ową. Wymaganie deduplikacji in-line dotyczy zapisu danych przez każdy z wymaganych intefejsów, w przypadku interfejsów: NFS, CIFS oraz VTL realizacja deduplikacji in-line nie może w żadnym stopniu zależeć od konkretnej aplikacji backu’owej, dane zapisywane poprzez interfejsy NFS CIFS bez użycia jakiejkolwiek aplikacji backup’owej również muszą być deduplikowane w sposób in-line |
| DD2-17 | Proponowane rozwiązanie nie może w żadnej fazie korzystać (w całości lub częściowo) z bufora na składowanie danych w postaci oryginalnej (niezdeduplikowanej) w celu ich późniejszej deduplikacji (wymagana deduplikacja in-line) |
| DD2-18 | Wszystkie unikalne bloki przed zapisaniem na dysk muszą być dodatkowo kompresowane. |
| DD2-19 | Tryb zapisu zabezpieczanych danych nie może umożliwiać nadpisywania danych, dane mogą być zapisywane jedynie w trybie append-only, dane dla których wygasła retencja powinny zostać usunięte podczas procesu czyszczenia tzw. Cleaning, wymaganie dotyczy wszystkich danych zapisanych na urządzeniu a nie wybranych grup danych objętych działaniem blokad zabezpieczających przed usunięciem/modyfikacją danych. |
| DD2-20 | Oferowane urządzenie musi wspierać (wymagane formalne wsparcie producenta urządzenia), co najmniej następujące aplikacje: NetWorker, RMAN, Microsoft SQL Server Management Studio.  W przypadku współpracy z każdą z poniższych aplikacji:  NetWorker  RMAN (dla ORACLE)  Microsoft SQL Server Management Studio (dla Microsoft SQL)  urządzenie musi umożliwiać deduplikację na źródle i przesłanie nowych, nie znajdujących się jeszcze na urządzeniu bloków poprzez sieć LAN.  Deduplikacja w wyżej wymienionych przypadkach musi zapewniać aby z zabezpieczanych serwerów do urządzenia były transmitowane poprzez sieć LAN jedynie fragmenty danych nie znajdujące się dotychczas na urządzeniu. |
| DD2-21 | W przypadku przyjmowania backupów z NetWorker, Oracle RMAN oraz Microsoft MSSQL (przy wykorzystaniu Microsoft SQL Server Management Studio), urządzenie musi umożliwiać deduplikację na źródle i przesłanie nowych, nieznajdujących się jeszcze na urządzeniu bloków poprzez sieć FC.  Deduplikacja w wyżej wymienionych przypadkach musi zapewniać aby z serwerów do urządzenia były transmitowane poprzez sieć FC tylko fragmenty danych nie znajdujące się dotychczas na urządzeniu. |
| DD2-22 | Oferowane urządzenie musi umożliwiać uruchamianie maszyn wirtualnych VMware bezpośrednio z danych backupowych bez konieczności odtwarzania danych, funkcjonalność ta musibyć wspierana przez aplikację NetWorker. |
| DD2-23 | Wymagana funkcjonalność Load Balancing oraz Link Failover w obrębie portów wykorzystywanych przez aplikację backupową, wymagane wsparcie tej funkcjonlaności w przypadku aplikacji NetWorker. |
| DD2-24 | Wymagane wsparcie dla backupów typu Virtual Synthetics w przypadku eksploatowanej aplikacji NetWorker. |
| DD2-25 | W przypadku deduplikacji na źródle poprzez sieć IP (LAN oraz WAN), wymagana możliwość szyfrowania komunikacji kluczem minimum 256 bitów. |
| DD2-26 | Urządzenie musi umożliwiać zaszyfrowanie przechowywanych danych, wymagane licencje umożliwiające zaszyfrowanie i przechowywanie zaszyfrowanych danych w obrębie maksymalnej pojemności oferowanego urządzenia. |
| DD2-27 | Urządzenie musi wspierać deduplikację na źródle poprzez sieć FC (SAN) minimum dla następujących systemów operacyjnych:   1. Windows 2. Linux (RedHat, SuSE) |
| DD2-28 | Oferowane urządzenie musi umożliwiać bezpośrednią replikację danych do drugiego urządzenia takiego samego typu oraz urządzeń DD9400 eksploatowanych przez Zamawiającego. Konfiguracja replikacji musi być możliwa w każdym z trybów:  \* jeden do jednego  \* wiele do jednego  \* jeden do wielu  \* kaskadowej (urządzenie A replikuje dane do urządznia B, które te same dane replikuje do urządzenia C).  Replikacja musi się odbywać w trybie asynchronicznym. Transmitowane mogą być tylko te fragmenty danych (bloki) które nie znajdują się na docelowym urządzeniu. Ewentualna licencja na replikację musi być dostarczona w ramach postępowania. |
| DD2-29 | Urządzenie musi umożliwiać wydzielenie określonych portów Ethernet dedykowanych do replikacji. |
| DD2-30 | W przypadku wykorzystania portów Ethernet do replikacji urządzenie musi umożliwiać przyjmowanie backupów, odtwarzanie danych, przyjmowanie strumienia replikacji, wysyłanie strumienia replikacji tymi samymi portami. |
| DD2-31 | W przypadku replikacji danych między urządzeniami oferowanego typu a także oferowanym urządzeniem oraz urządzeniami DD9400 eksploatowanymi przez Zamawiającego, wymagana możliwość kontroli przez: NetWorker, RMAN oraz Microsoft SQL Server Management Studio, muszą być możliwe do uzyskania jednocześnie wszystkie następujące funkcjonalności:   1. replikacja odbywa się bezpośrednio między dwoma urządzeniami bez udziału serwerów pośredniczących 2. replikacji podlegają tylko te fragmenty danych, które nie znajdują się na docelowym urządzeniu 3. replikacja zarządzana jest z poziomu wymaganej aplikacji 4. aplikacja posiada informację o obydwu kopiach zapasowych znajdujących się w obydwu urządzeniach bez konieczności przeprowadzania procesu inwentaryzacji |
| DD2-32 | Oferowane urządzenie musi działać poprawnie przy zapełnieniu danymi na poziomie co najmniej 90%. Dokumentacja urządzenia nie może wskazywać na ew. problemy, obostrzenia, które są efektem zapełnieniu urządzenia zabezpieczanymi danymi, na poziomie mniejszym niż 90%. |
| DD2-33 | Wymagana możliwość ograniczenia pasma używanego do replikacji między dwoma urządzeniami – oferowane urządzenie powinno być wyposażone w mechanizm umożliwiający zarządzaniem stopnia wykorzystania pasma na potrzeby replikacji. |
| DD2-34 | Zdeduplikowane i skompresowane dane przechowywane w obrębie podsystemu dyskowego urządzenia muszą być chronione za pomocą technologii RAID 6 bądź równoważnej. |
| DD2-35 | Oferowane urządzenie musi umożliwiać wykonywanie SnapShot’ów, czyli umożliwiać zamrożenie obrazu danych (stanu backupów) w urządzeniu na określoną chwilę. Oferowane urządzenie musi również umożliwiać odtworzenie danych ze Snapshot’u.  Odtworzenie danych ze Snapshot’u nie może wymagać konieczności nadpisania danych produkcyjnych jak również nie może oznaczać przerwy w normalnej pracy urządzenia (przyjmowania/odtwarzania backupów).  Wymagana możliwość wykorzystania funkcjonalności SnapShot dla danych przesyłanych dowolnym z wymaganych interfejsów urządzenia. |
| DD2-36 | Urządzenie musi pozwalać na przechowywanie minimum 700 Snapshotów jednocześnie w obrębie oferowanej przestrzeni, przy zachowaniu globalnej deduplikacji oraz standardowego trybu pracy urządzenia – umożliwiającego wykorzystanie wszystkich dostępnych funkcjonalności. |
| DD2-37 | Urządzenie musi umożliwiać podział na logiczne części. Dane znajdujące się w każdej logicznej części muszą być między sobą deduplikowane (globalna deduplikacja między logicznymi częściami urządzenia). |
| DD2-38 | Urządzenie musi mieć możliwość podziału na minimum 10 logicznych części pracujących równolegle. Producent musi oficjalnie wspierać pracę minimum 10 logicznych części pracujących równolegle z pełną wydajnością urządzenia. |
| DD2-39 | Dla każdej z w/w logicznych części oferowanego urządzenia musi być możliwość zdefiniowania oddzielnego użytkownika zarządzającego daną logiczną częścią deduplikatora. Użytkownicy zarządzający logiczną częścią A muszą widzieć tylko i wyłącznie zasoby logicznej części A i nie mogą widzieć żadnych innych zasobów oferowanego urządzenia. |
| DD2-40 | Wymagana możliwość zaprezentowania każdej z logicznych części oferowanego urządzenia, jako niezależnego urządzenia dostępnego za pośrednictwem:  CIFS  NFS  VTL  deduplikacja na źródle |
| DD2-41 | Urządzenie musi umożliwiać zdefiniowanie blokady skasowania danych (funkcjonalność WORM). Blokada skasowania danych musi chronić plik w zdefiniowanym czasie przed usunięciem pliku, modyfikacją pliku.  Blokada skasowania danych musi działać w dwóch trybach (do wyboru przez administratora):  Możliwość zdjęcia blokady przed upływem ważności danych  Brak możliwości zdjęcia blokady przed upływem ważności danych (COMPLIANCE), w tym wypadku wymagane wsparcie norm SEC 17a-4(f), ISO Standard 15489-1 oraz CFTC Rule 1.31b w zakresie ochrony danych (wymagane potwierdzenie w ogólno dostępnej dokumentacji oferowanego urządzenia)  Wymagana blokada WORM musi być zintegrowana z eksploatowaną aplikacją backup’ową NetWorker co oznacza:  możliwość uruchomienia blokady WORM dla określonych danych z poziomu aplikacji NetWorker  możliwość określenia/wymuszenia czasu blokady z poziomu aplikacji NetWorker  możliwość raportowania od strony aplikacji NetWorker danych zabezpieczonych przed usunięciem wymaganą blokadą WORM  Wymagana możliwość działania z wybranym opóźnieniem wymaganej blokady na określonym katalogu. Licencje na blokadę usunięcia/zmiany przechowywanych plików muszą być dostarczone wraz z urządzeniem.  Wymagana możliwość automatycznego uruchamiania blokady (podczas zapisu) WORM dla danych zapisywanych na obszar objęty działaniem wspomnianej blokady, a także możliwość używania blokady WORM dla obrazu danych uzyskanych poprzez użycie wymaganej funkcjonalności SnapShot. |
| DD2-42 | Urządzenie musi mieć możliwość przechowywania danych niezmienialnych:   1. Video 2. Grafika 3. Nagrania dźwiękowe 4. Pliki pdf na udziałach CIFS/NFS. |
| DD2-43 | Urządzenie musi weryfikować dane po zapisie (nie chodzi o ew. weryfikację danych indeksowych generowanych przez urządzenie ale o weryfikację wszystkich zabezpieczanych danych backup’owych). Każda zapisana na dyskach porcja danych musi być odczytana i porównana z danymi otrzymanymi przez urządzenie. Powyższa weryfikacja musi być realizowana w locie, czyli przed usunięciem z pamięci oryginalnych danych (otrzymanych z aplikacji backupowej), musi być realizowana w trybie ciągłym (a nie ad-hoc), wymagane parametry wydajnościowe urzadzenia muszą uwzględniać tę funkcjonalność. Wymagane potwierdzenie opisanej funkcjonalności w oficjalnej dokumentacji producenta oferowanego urządzenia. Zamawiający zastrzega możliwość prośby o dostarczenie ogólnodostępnej dokumentacji oferowanego produktu potwierdzającego spełnienie wymaganej funkcjonalności). |
| DD2-44 | Urządzenie musi automatycznie usuwać przeterminowane dane (bloki danych nie należące do backupów o aktualnej retencji) w procesie czyszczenia. |
| DD2-45 | Proces usuwania przeterminowanych danych (czyszczenia) nie może uniemożliwiać pracy procesów backupu / odtwarzania danych (zapisu / odczytu danych z zewnątrz do systemu). |
| DD2-46 | Wymagana możliwość zdefiniowania maksymalnego obciążenia urządzenia procesem usuwania przeterminowanych danych (poziomu obciążenia procesora), wymagane potwierdzenie w ogólno dostępnej dokumentacji. Zamawiający zastrzega możliwość prośby o dostarczenie ogólnodostępnej dokumentacji oferowanego produktu potwierdzającego spełnienie wymaganej funkcjonalności) |
| DD2-47 | Wymagana możliwość zdefiniowania harmonogramu wg. którego wykonywany jest proces usuwania przeterminowanych danych (czyszczenia), realizowany równolegle z procesami backup/restore/replication. |
| DD2-48 | Standardowa częstotliwość usuwania przeterminowanych danych (czyszczenie) nie powinna być większa niż 1 raz na tydzień - minimalizując czas w którym backupy/odtworzenia narażone są na spowolnienie (weryfikacja wymagania na podstawie dokumentacji typu DOBRE PRAKTYKI publikowanej przez producenta). |
| DD2-49 | Urządzenie musi posiadać wbudowany mechanizm umożliwiający usunięcie danych poprzez ich nadpisanie, wymagana zgodność ze standardem DoD 5220.22-M |
| DD2-50 | Urządzenie musi umożliwiać systemowo (wbudowana funkcjonalność) - realizację procesu pierwszego czyszczenia dopiero po przekroczeniu 75% zajętości oferowanej przestrzeni. |
| DD2-51 | Urządzenie musi mieć możliwość zarządzania poprzez  Interfejs graficzny dostępny z przeglądarki internetowej  Poprzez linię komend (CLI) dostępną z poziomu ssh (secure shell) |
| DD2-52 | Oprogramowanie do zarządzania musi rezydować na oferowanym na urządzeniu deduplikacyjnym. |
| DD2-53 | Oferowane urządzenie musi mieć możliwość sprawdzenia pakietu upgrade’ującego firmware urządzenia (GUI lub CLI), to znaczy sprawdzenia czy nowa wersja systemu nie spowoduje problemów z urządzeniem. |
| DD2-54 | Urządzenie musi być rozwiązaniem kompletnym, appliancem sprzętowym pochodzącym od jednego producenta. Zamawiający nie dopuszcza stosowania rozwiązań typu gateway. Oferowany typ urządzenia musi być oficjalnie dostępny w ofercie producenta przed ogłoszeniem niniejszego postępowania. |
| DD2-55 | Certyfikat ISO 9001 dla producenta sprzętu obejmujący proces projektowania i produkcji – dołączony do oferty dokument potwierdzający spełnienie tego wymogu.  Certyfikat ISO 14001 dla producenta sprzętu – dołączony do oferty dokument potwierdzający spełnienie tego wymogu.  Urządzenia wyprodukowane są przez producenta, zgodnie z normą PN-EN ISO 50001 lub oświadczenie producenta o stosowaniu w fabrykach polityki zarządzania energią, która jest zgodna z obowiązującymi przepisami na terenie Unii Europejskiej – dołączony do oferty dokument potwierdzający spełnienie tego wymogu.  Oświadczenie producenta deduplikatora, potwierdzające, że sprzęt pochodzi z oficjalnego kanału dystrybucyjnego producenta – dołączone do oferty. |
| DD2-56 | Gwarancja producenta 36 miesięcy, świadczona na miejscu u klienta.  Czas reakcji serwisu - do końca następnego dnia roboczego od chwili zgłoszenia.  Serwis urządzeń musi być realizowany przez producenta lub Autoryzowanego Partnera Serwisowego producenta – dołączone do oferty oświadczenie producenta potwierdzające, że serwis będzie realizowany przez Autoryzowanego Partnera Serwisowego producenta lub bezpośrednio przez producenta.  Firma serwisująca musi posiadać ISO 9001 na świadczenie usług serwisowych oraz posiadać autoryzację producenta serwera – dołączony do oferty dokument potwierdzający spełnienie tego wymogu.  W przypadku awarii dysku twardego/nośnika danych, nośnik pozostaje u Zamawiającego. |

* 1. **SPRZĘT LAN**
     1. **Przełącznik LAN – 22 sztuki**

**Producent …………………………………**

**Model …………………………………**

|  |  |
| --- | --- |
| ***Identyfikator wymagania*** | ***Opis wymagania*** |
| **LAN4-01** | **Funkcjonalności warstwy L2:** |
| LAN4-01.01 | Trunking IEEE 802.1Q VLAN; |
| LAN4-01.02 | Wsparcie sprzętowe dla obsługi co najmniej 3.000 sieci VLAN; |
| LAN4-01.03 | Funkcjonalność izolowania portów znajdujących się w tym samym VLAN |
| LAN4-01.04 | Wsparcie sprzętowe dla minimum 250.000 adresów MAC |
| LAN4-01.05 | IEEE 802.1w Rapid Spanning Tree (RST) |
| LAN4-01.06 | IEEE 802.1s Multiple Spanning Tree (MST) – co najmniej 32 instancje |
| LAN4-01.07 | Wsparcie sprzętowe dla tunelowania QinQ |
| LAN4-01.08 | Zabezpieczenie przeciwko incydentom w topologii Spanning Tree |
| LAN4-01.09 | Internet Group Management Protocol (IGMP) Versions 2, 3; |
| LAN4-01.10 | Terminowanie pojedynczej wiązki EtherChannel na 2 niezależnych przełącznikach |
| LAN4-01.11 | Link Aggregation Control Protocol (LACP): IEEE 802.3ad z możliwością zgrupowania minimum 8 interfejsów fizycznych w wiązce |
| LAN4-01.12 | Ramki Jumbo dla wszystkich portów (minimum 9100 bajtów); |
| **LAN4-02** | **Funkcjonalności warstwy L3** |
| LAN4-02.01 | Sprzętowe przełączanie pakietów w warstwie L3 |
| LAN4-02.02 | Routing w oparciu o trasy statyczne |
| LAN4-02.03 | Routing dynamiczny w oparciu o co najmniej OSPF, BGP dla protokołów IPv4 oraz IPv6. |
| LAN4-02.04 | Policy Based Routing (PBR) dla IPv4 |
| LAN4-02.05 | VRRP v3 |
| LAN4-02.06 | Wsparcie dla BFDv6 (Bidirectional Forwarding Protocol) |
| LAN4-02.07 | Wsparcie dla IPv4 multicast w oparciu o protokół PIMv2 SM (Sparse Mode) i SSM (Source Specific Multicast) |
| LAN4-02.08 | Wsparcie dla IGMPv3 oraz MSDP |
| LAN4-02.09 | Wsparcie sprzętowe dla minimum 1000 tras multicastowych |
| LAN4-02.10 | Wsparcie dla minimum 1.000 instancji VRF wraz z funkcjonalnością importu/eksportu tras (route leaking) |
| LAN4-02.11 | Wybór do 64 jednoczesnych ścieżek o równej metryce (ECMP) |
| LAN4-02.12 | Minimum 1.000 wejściowych oraz 1.000 wyjściowych wpisów dla ACL - access control list |
| **LAN4-03** | **Sprzętowe wsparcie dla szyfrowania portów Ethernet z wykorzystaniem technologii MACSec IEEE 802.1ad i z wykorzystaniem klucza 256 bit** |
| **LAN4-04** | **Mechanizmy związane z funkcjonalnością VXLAN:** |
| LAN4-04.01 | obsługa co najmniej 250 sprzętowych VTEP (VXLAN Tunnel Endpoint) |
| LAN4-04.02 | sprzętowy VXLAN Bridging (VXLAN/VLAN Gateway) |
| LAN4-04.03 | obsługa ruchu rozgłoszeniowego (multicast, broadcast, unknown unicast) z mapowaniem VXLAN do IP Multicast Group i wykorzystaniem funkcjonalności PIM Anycast RP |
| LAN4-04.04 | obsługa ruchu rozgłoszeniowego (multicast, broadcast, unknown) poprzez statyczną replikację (bez konieczności wykorzystania IP Multicast) |
| LAN4-04.05 | implementacja VXLAN BGP EVPN (Ethernet VPN) z dystrybucją informacji o adresach MAC i adresach IP poprzez MP-BGP i ograniczeniem ruchu ARP (Address Resolution Protocol) |
| LAN4-04.06 | obsługa routingu między VXLAN-ami (VXLAN Routing) z wykorzystaniem BGP EVPN oraz funkcjonalności Anycast Gateway (obsługą danego SVI na wszystkich VTEP w domenie VXLAN). |
| **LAN4-05** | **Mechanizmy związane z zapewnieniem jakości usług w sieci:** |
| LAN4-05.01 | layer 2 IEEE 802.1p (CoS); |
| LAN4-05.02 | klasyfikacja QoS w oparciu o listy ACL (Access control list) – w warstwach 2, 3, 4; |
| LAN4-05.03 | kolejkowanie na wyjściu w oparciu o CoS 802.1p; |
| LAN4-05.04 | bezwzględne (strict-priority) kolejkowanie na wyjściu; |
| LAN4-05.05 | kolejkowanie WRR (Weighted Round-Robin) na wyjściu lub mechanizm równoważny |
| LAN4-05.06 | ograniczanie ruchu (policing) do zadanej przepływności na interfejsach wejściowych i wyjściowych |
| LAN4-05.07 | kształtowanie (shaping) ruchu do zadanej przepływności na interfejsach wyjściowych |
| LAN4-05.08 | protokół PFC (Priority Flow Control) IEEE 802.1Qbb |
| **LAN4-06** | **Mechanizmy związane z zapewnieniem bezpieczeństwa w sieci:** |
| LAN4-06.01 | wejściowe ACL (standardowe oraz rozszerzone); |
| LAN4-06.02 | standardowe oraz rozszerzone ACL dla warstwy 2 w oparciu o: adresy MAC adresy IP, typ protokołu; |
| LAN4-06.03 | standardowe oraz rozszerzone ACL dla warstw 3 oraz 4 w oparciu o: IPv4 i IPv6, Internet Control Message Protocol (ICMP), TCP, User Datagram Protocol (UDP); |
| LAN4-06.04 | ACL oparte o VLAN-y (VACL); |
| LAN4-06.05 | ACL oparte o porty (PACL); |
| LAN4-06.06 | DHCP Snooping |
| LAN4-06.07 | ARP Inspection |
| LAN4-06.08 | IP Source Guard |
| LAN4-06.09 | prewencja niekontrolowanego wzrostu ilości ruchu (storm control), dla ruchu unicast, multicast, broadcast |
| LAN4-07 | Funkcjonalności dla obszaru zarządzania i zabezpieczenia przełącznika: |
| LAN4-07.01 | RMON (przynajmniej grupy Events, Alarms) |
| LAN4-07.02 | sFlow lub netFlow |
| LAN4-07.03 | IEEE 802.1ab LLDP |
| LAN4-07.04 | możliwość zachowania stanu (checkpoint) i powrotu do poprzedniej konfiguracji (rollback) |
| LAN4-07.05 | ograniczanie ruchu kierowanego do warstwy sterowania (control plane policing) |
| LAN4-07.06 | kopiowanie ruchu ze źródłowych fizycznych portów Ethernet, wiązek PortChannel, sieci VLAN, na interfejs docelowy za pośrednictwem specjalnego mechanizmu (mirror) |
| LAN4-07.07 | Network Time Protocol (NTP); |
| LAN4-07.08 | ping, traceroute |
| **LAN4-08** | **Narzędzia programowania i zarzadzania przełącznikiem:** |
| LAN4-08.01 | interfejs programistyczny REST API wraz z upublicznionym SDK |
| **LAN4-09** | **zasilacze zmiennoprądowe pracujące w konfiguracji redundantnej** |
| **LAN4-10** | **obudowa przeznaczona do montażu w szafie rackowej 19”** |
| **LAN4-13** | **Przełącznik musi posiadać:** |
| LAN4-13.01 | minimum 48 portów 1/10/25GE definiowanych za pomocą wkładek SFP bezpośrednio w obudowie przełącznika lub na karcie liniowej |
| LAN4-13.02 | minimum 4 porty 40/100GE definiowanych za pomocą wkładek QSFP, przy czym każdy z tych portów QSFP musi posiadać możliwość pracy zarówno w trybie 40Gbps oraz w trybie 100Gbps |
| LAN4-13.03 | dedykowany interfejs GE 100/1000 na potrzeby zarządzania |
| LAN4-13.04 | Wykonawca dostarczy minimum 18 sztuk wkładek SFP 1 GB RJ45, 18 sztuk wkładek SFP 10 Gbit/s lub 10/25Gbit/s MM SR; wszytskie dostarczane wkładki muszą być kompatybilne z pozostałymi dostarczanymi rozwiązaniami; w przypadku konieczności dostarczenia większej ilości wkładek lub wkładek innego rodzaju (o parametrach nie gorszych niż wyspecyfikowane) Wykonawca musi przewidzieć to w składanej ofercie. Zamawiajacy wymaga realizacji połączeń w sposób nadmiarowy do 2 dostarczanych do każdej z lokalizacji przełączników. |
| **LAN4-14** | **Parametry wydajnościowe:** |
| LAN4-14.01 | prędkość przełączania „wirespeed” dla każdego portu przełącznika |
| LAN4-14.02 | urządzenie sprzętowo przełącza pakiety w warstwie L2 i L3 |
| LAN4-14.03 | obsługiwana łączna przepływność (pasmo) min. 4,8Tbps |
| LAN4-14.04 | obsługiwana łączna przepustowość pakietowa przełącznika min. 2,5 Bpps |
| LAN4-14.05 | opóźnienie przełączania pakietów nie większe niż 1 µs |
| LAN4-14.06 | Bufor minimum 40MB |

* 1. **OPROGRAMOWANIE**
     1. **Oprogramowanie wirtualizacyjne – 1232 licencje na rdzeń procesora**

**Producent ………………………….….**

**Model ……………………….…….**

Zamawiający wymaga zaoferowania oprogramowania do wirtualizacji mocy obliczeniowej wraz z dodatkowymi komponentami

|  |  |
| --- | --- |
| Nazwa produktu | VMware vSphere |
| Wersja produktu | 8 |

lub oprogramowania równoważnego spełniającego poniższe wymagania:

| **Identyfikator wymagania** | **Wymaganie** | **Opis wymagania** |
| --- | --- | --- |
| OPPW-1 | Ogólne | Wszystkie dostarczone licencje zaoferowanego oprogramowania muszą być licencjami subskrypcyjnymi, tj. licencja na określony czas wraz ze wsparciem technicznym do tych licencji świadczonym przez producenta zaoferowanego oprogramowania.  Wszystkie wymagane poniżej komponenty/moduły muszą pochodzić od jednego producenta oprogramowania. |
| OPPW-2 | Wirtualizacja mocy obliczeniowej | • Licencje zaoferowanego oprogramowania muszą być zaoferowane w formie „per core” fizyczny procesora fizycznego.  • Zaoferowane oprogramowanie musi być instalowane bezpośrednio na sprzęcie fizycznym i nie może być ono częścią innego systemu operacyjnego  • W zaoferowanym oprogramowaniu warstwa wirtualizacji nie może dla własnych celów alokować więcej niż 700MB pamięci operacyjnej RAM serwera fizycznego  • Zaoferowane oprogramowanie do wirtualizacji zainstalowane na serwerze fizycznym musi potrafić obsłużyć i wykorzystać procesory fizyczne tego serwera wyposażone w 768 logicznych wątków, 24TB pamięci fizycznej RAM tego serwera oraz 16 procesorów fizycznych tego serwera  • Zaoferowane oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych z ilością od 1 do 768 procesorów wirtualnych  • Zaoferowane oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych z możliwością przydzielenia do 24 TB pamięci operacyjnej RAM  • Zaoferowane oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych z możliwością przydzielenia od 1 do 10 wirtualnych kart sieciowych dla każdej z nich. Dodatkowo, oprogramowanie musi posiadać możliwość utworzenia maszyny wirtualnej bez przydzielonej wirtualnej karty sieciowej.  • Zaoferowane oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych, z których każda może mieć 32 porty szeregowe, 3 porty równoległe i 20 urządzeń USB  • Zaoferowane oprogramowanie musi wspierać minimum następujące systemy operacyjne: Windows Server 2012/2016/2019/2022, Windows 8/10/11, RHEL 6/7/8/9, SLES 12/15, Debian 10/11, CentOS 7/8, Ubuntu 16/18/20/22, Photon OS 2/3/4, Oracle Linux 6/7/8/9, FreeBSD 12/13  • W celu osiągnięcia maksymalnego współczynnika konsolidacji, zaoferowane oprogramowanie musi umożliwiać przydzielenie łącznie większej ilości pamięci RAM dla maszyn wirtualnych niż fizyczne zasoby RAM serwera, na którym maszyny te są posadowione  • Rozwiązanie musi umożliwiać udostępnienie maszynie wirtualnej większej ilości zasobów dyskowych niż jest fizycznie dostępne na zasobach dyskowych  • Zaoferowane oprogramowanie musi umożliwiać integrację z rozwiązaniami antywirusowymi firm trzecich w zakresie skanowania maszyn wirtualnych z poziomu warstwy wirtualizacji bez ingerencji w systemy operacyjne maszyn wirtualnych (bezagentowość)  • Zaoferowane oprogramowanie musi zapewniać zdalny i lokalny dostęp administracyjny do wszystkich serwerów fizycznych poprzez protokół SSH, z możliwością nadawania uprawnień do takiego dostępu nazwanym użytkownikom bez konieczności wykorzystania konta „root”  • Zaoferowane oprogramowanie do wirtualizacji musi zapewnić możliwość powielania maszyn wirtualnych wraz z ich pełną konfiguracją i danymi  • Zaoferowane oprogramowanie do wirtualizacji musi zapewnić możliwość wykonywania kopii migawkowych instancji systemów operacyjnych na potrzeby tworzenia kopii zapasowych bez przerywania ich pracy z możliwością konieczności zachowania stanu pamięci pracującej maszyny wirtualnej.  • Konsola zarządzająca zaoferowanego oprogramowania musi posiadać możliwość przydzielania i konfiguracji uprawnień z możliwością integracji z usługami katalogowymi, minimalnie z: Microsoft Active Directory i Open LDAP oraz umożliwiać federacyjne zarządzanie tożsamością w oparciu o Microsoft Active Directory Federation Services (ADFS).  • Zaoferowane oprogramowanie musi zapewniać możliwość dodawania zasobów w czasie pracy maszyny wirtualnej, w szczególności w zakresie ilości procesorów, pamięci operacyjnej i przestrzeni dyskowej  • Zaoferowane oprogramowanie musi posiadać funkcjonalność tworzenia wirtualnego przełącznika (virtual switch) umożliwiającego tworzenie sieci wirtualnej w obszarze hosta (hypervisora wirtualizacyjnego) i pozwalającego połączyć tym przełącznikiem maszyny wirtualne w obszarze jednego hosta, a także na zewnątrz sieci fizycznej. Pojedynczy przełącznik wirtualny powinien mieć możliwość konfiguracji aż do 4096 portów  • Pojedynczy wirtualny przełącznik w zaoferowanym oprogramowaniu, w celu zapewnienia bezpieczeństwa połączenia ethernetowego w razie awarii fizycznej karty sieciowej, musi posiadać możliwość przyłączania do niego minimum dwóch fizycznych kart sieciowych  • Wirtualne przełączniki w zaoferowane oprogramowaniu muszą posiadać funkcjonalność obsługi wirtualnych sieci lokalnych (VLAN)  • Zaoferowane oprogramowanie musi umożliwiać wykorzystanie technologii przepustowości sieci komputerowych do 200GbE poprzez agregację połączeń fizycznych do minimalizacji czasu przenoszenia maszyny wirtualnej pomiędzy serwerami fizycznymi  • Zaoferowane oprogramowanie do wirtualizacji musi obsługiwać przełączenie ścieżek LAN (bez utraty komunikacji) w przypadku awarii jednej ze ścieżek  • Zaoferowane oprogramowanie musi zapewnić możliwość zdefiniowania alertów informujących o przekroczeniu wartości progowych  • Zaoferowane oprogramowanie, w przypadku działania pod zarządcą klastra VMware vCenter, musi zapewniać możliwość replikacji maszyn wirtualnych z dowolnej pamięci masowej w tym z dysków wewnętrznych serwerów fizycznych na dowolną pamięć masową w tym samym lub oddalonym ośrodku przetwarzania. Replikacja musi gwarantować współczynnik RPO (ang. Recovery Point Objective) na poziomie minimum 5 minut  • Zaoferowane oprogramowanie do wirtualizacji musi obsługiwać przełączenie ścieżek SAN (bez utraty komunikacji) w przypadku awarii jednej ze ścieżek  • Zaoferowane oprogramowanie, w przypadku działania pod zarządcą klastra VMware vCenter, musi mieć możliwość przenoszenia maszyn wirtualnych pomiędzy serwerami fizycznymi bez przerywania pracy usług na przenoszonych maszynach wirtualnych. Wymaga się wsparcia natywnego szyfrowania ruchu sieciowego dla maszyn wirtualnych podczas ich przenoszenia między serwerami fizycznymi  • Zaoferowane oprogramowanie, w przypadku działania pod zarządcą klastra VMware vCenter, oraz w środowisku z więcej niż pojedynczym wirtualizatorem, musi umożliwiać automatyczne, ponowne uruchomienie maszyn wirtualnych w przypadku awarii jednego z wirtualizatorów na kolejnym, działającym w tym samym klastrze wirtualizatorze (funkcjonalność HA) (ang. high availability)  • Zaoferowane oprogramowanie, w przypadku działania pod zarządcą klastra VMware vCenter w środowisku z minimalnie dwoma wirtualizatorami oraz w przypadku potrzeby wgrania aktualizacji do warstwy wirtualizacji, musi posiadać możliwość w przypadku wywołania startu aktualizacji, automatycznego przeniesienia bezprzerwowego działających maszyn wirtualnych do innego wirtualizatora nie objętego aktualizacją, przed rozpoczęciem samej aktualizacji  • Zaoferowane oprogramowanie musi posiadać co najmniej 2 niezależne mechanizmy wzajemnej komunikacji między serwerami z zainstalowanym wirtualizatorem oraz z serwerem zarządzającym, gwarantujące właściwe działanie mechanizmów wysokiej dostępności na wypadek izolacji sieciowej serwerów fizycznych lub partycjonowania sieci  • Zaoferowane oprogramowanie, w przypadku działania pod zarządcą klastra VMware vCenter, w środowisku z minimum dwoma wirtualizatorami, musi zapewniać pracę bez przestojów dla wybranych maszyn wirtualnych (o maksymalnie dwóch procesorach wirtualnych), niezależnie od systemu operacyjnego oraz aplikacji, podczas awarii wirtualizatora, bez utraty danych i dostępności danych na maszynach wirtualnych objętych ochroną  • Zaoferowane oprogramowanie do wirtualizacji musi zapewniać możliwość stworzenia dysku maszyny wirtualnej o wielkości 62 TB  • Zaoferowane oprogramowanie musi posiadać wbudowany interfejs programistyczny (API) zapewniający pełną integrację zewnętrznych rozwiązań wykonywania kopii zapasowych z istniejącymi mechanizmami warstwy wirtualizacyjnej  • Producent zaoferowanego oprogramowania do wirtualizacji musi wspierać rozwiązania do automatyzacji procesów oraz wirtualizacji sieci (SDN, ang. software defined network).  • Zaoferowane oprogramowanie musi wspierać mechanizmy zaawansowanego uwierzytelniania do systemu operacyjnego wirtualnej maszyny za pomocą technologii Smart Card Reader  • Zaoferowane oprogramowanie musi wspierać TPM 2.0. Minimalne wymaganie Zamawiającego dla TPM oznacza, że TPM zapewnia mechanizm gwarantujący, że serwer fizyczny, na którym zainstalowane jest zaoferowane oprogramowanie, uruchomił się z włączoną opcją Secure Boot. Po potwierdzeniu, że Secure Boot jest włączone, system gwarantuje, poprzez weryfikację podpisu cyfrowego, że hypervisor uruchomił się w niezmienionej formie  • Wirtualizator w zaoferowanym oprogramowaniu musi mieć możliwość włączenia funkcji “Microsoft virtualization-based security”, tzw. Microsoft VBS dla systemów operacyjnych maszyn wirtualnych opartych o system operacyjny Microsoft Windows 10, Microsoft Windows Server 2016 oraz Microsoft Windows Server 2019  • Zaoferowane oprogramowanie musi posiadać certyfikację FIPS-140-2 min. dla modułu jądra wirtualizatora odpowiedzialnego za szyfrowanie danych  • Zaoferowane oprogramowanie musi posiadać funkcjonalność wirtualnego TPM 2.0 dla maszyn wirtualnych z zainstalowanym Microsoft Windows 10 oraz Microsoft Windows 2016. Zamawiający wymaga aby z punktu widzenia maszyny wirtualnej z systemem operacyjnym Microsoft Windows 10 lub Microsoft Windows 2016 wirtualny TPM widziany był jako standardowy TPM, gdzie można przechowywać bezpiecznie wrażliwe dane np. certyfikaty. Zawartość wirtualnego TPM musi być przechowywana w pliku przynależnym do maszyny wirtualnej oraz musi być szyfrowana.  • Zaoferowane oprogramowanie musi posiadać funkcjonalność szybkiego uruchamiania wirtualizatora po przeprowadzonym procesie jego aktualizacji. Zamawiający wymaga aby w procesie aktualizacji wirtualizatora, jeśli wymagany jest jego restart, funkcjonalność szybkiego uruchamiania powodowała eliminację czasochłonnej fazy inicjalizacji serwera fizycznego  • Zaoferowane oprogramowanie, w przypadku działania pod zarządcą klastra VMware vCenter, musi posiadać możliwość aktualizacji i kontroli wersji oprogramowania do wirtualizacji w ramach klastra serwerów z poziomu centralnej konsoli zarządzającej. Dodatkowo centralna konsola zarządzająca musi posiadać funkcjonalność aktualizacji firmware komponentów serwera fizycznego (dyski, kontrolery, karty sieciowe) z poziomu konsoli zarządzającej wirtualizatora. Konsola zarządzająca musi mieć możliwość automatycznej weryfikacji, czy zainstalowane komponenty serwera posiadają rekomendowaną wersję sterowników i firmware, eliminując ryzyko pracy na nieaktualnych wersjach. Taka funkcjonalność powinna być dostępna dla minimum dwóch producentów serwerów obecnych na rynku  • Zaoferowane oprogramowanie musi posiadać wsparcie dla natywnych dysków 4K  • Zaoferowane oprogramowanie musi wspierać protokół precyzyjnej synchronizacji czasu PTP (ang. Precision Time Protocol)  • Zaoferowane oprogramowanie, w przypadku działania pod zarządcą klastra VMware vCenter, musi posiadać mechanizm, który ogranicza dostęp do indywidualnego zarządzania warstwą wirtualizacji na serwerach fizycznych w ramach klastra serwerów w celu utwardzenia/hardening (maksymalnego zwiększenia bezpieczeństwa dostępu) systemu wirtualizacji.  • Zaoferowane oprogramowanie musi mieć funkcjonalność migracji w trybie rzeczywistym dysków działających maszyn wirtualnych z jednego podsystemu dyskowego do innego bez konieczności przerywania pracy maszyny wirtualnej, której dysk jest migrowany  • Zaoferowane oprogramowanie obejmuje walidację FIPS, a także zaktualizowane przewodniki audytów.  • Zaoferowane oprogramowanie musi mieć możliwość utworzenia, poprzez API, maszyny wirtualnej jako tzw. Instant Clone poprzez klonowanie działającej maszyny wirtualnej w wyniku którego powstanie nowa działająca maszyna wirtualna identyczna z klonowaną. Nowa maszyna wirtualna musi powstawać w pamięci operacyjnej wirtualizatora  • Zaoferowane oprogramowanie, w przypadku działania pod zarządcą klastra VMware vCenter, musi mieć możliwość monitorowania i wyświetlania za pomocą grafu w konsoli bieżącego poboru energii elektrycznej dla hosta wirtualizacyjnego oraz dla maszyn wirtualnych na nim posadowionych  • Zaoferowane oprogramowanie podczas pracy w klastrze zarządzanym przez VMware vCenter musi umożliwiać automatyczne równoważenie obciążenia CPU/MEM serwerów fizycznych pracujących jako platforma dla infrastruktury wirtualnej  • Zaoferowane oprogramowanie musi posiadać certyfikację dla pakietu NVIDIA AI Enterprise, natywnego dla chmury zbioru zoptymalizowanych aplikacji AI i frameworków przeznaczonych dla kompleksowego rozwiązania AI;  • Zaoferowane oprogramowanie musi umożliwiać włączenie najnowszej generacji procesorów graficznych NVIDIA do swojego środowiska wirtualnego i skorzystanie z takich funkcji jak Multi-Instance GPU (MIG), pozwalające na współdzielenie cykli GPU przez wielu użytkowników.  • Zaoferowane oprogramowanie do wirtualizacji, w przypadku działania pod zarządcą klastra VMware vCenter, musi zapewniać mechanizm pozwalający tworzyć profil (szablon konfiguracji) wybranego serwera wirtualizacyjnego (Hypervisora), a następnie wymuszać ten profil/konfigurację na innych serwerach fizycznych lub sprawdzać zgodność konfiguracji pomiędzy zdefiniowanym wcześniej profilem a wskazanym serwerem fizycznym  • Zaoferowane oprogramowanie, w przypadku działania pod zarządcą klastra VMware vCenter, musi umożliwiać utworzenie w nim jednorodnego, wirtualnego przełącznika sieciowego, rozproszonego na wszystkie serwery fizyczne istniejące w tym klastrze. Przełącznik taki musi zapewniać możliwość konfiguracji parametrów sieciowych maszyny wirtualnej z granulacją na poziomie portu tego przełącznika. Pojedyncza maszyna wirtualna musi mieć możliwość wykorzystania jednego lub wielu portów przełącznika z niezależną od siebie konfiguracją. Przełącznik rozproszony musi współpracować z protokołem NetFlow  • Zaoferowane oprogramowanie umożliwia uruchamianie poufnych kontenerów w serwerach opartych na procesorach EPYC ™ firmy AMD.  • Zaoferowane oprogramowanie do wirtualizacji, w ramach zaimplementowanego w nim rozproszonego przełącznika sieciowego, powinno zapewniać możliwość integracji z produktami (przełącznikami wirtualnymi) firm trzecich, tak aby umożliwić granularną delegację zadań w zakresie zarządzania konfiguracją sieci do zespołów sieciowych  • Zaimplementowany w zaoferowanym oprogramowaniu przełącznik rozproszony musi umożliwiać funkcjonalność duplikowania ruchu sieciowego dowolnego jego portu wirtualnego na inny port  • Zaimplementowany w zaoferowanym oprogramowaniu przełącznik rozproszony musi mieć wbudowane mechanizmy składowania kopii konfiguracji, przywracania tej kopii a także mechanizmy automatycznie zapobiegające niewłaściwej konfiguracji sieciowej, które w całości lub w części mogą eliminować błędy ludzkie i utratę łączności sieciowej  • Zaoferowane oprogramowanie musi mieć wbudowany mechanizm kontrolowania i monitorowania ruchu sieciowego oraz ustalania priorytetów w zależności od jego rodzaju na poziomie konkretnych maszyn wirtualnych  • Zaoferowane oprogramowanie, w przypadku działania pod zarządcą klastra VMware vCenter, musi mieć możliwość uruchamiania fizycznych serwerów z centralnie przygotowanego obrazu poprzez protokół PXE  • Zaoferowane oprogramowanie, w przypadku działania pod zarządcą klastra VMware vCenter, musi zapewnić możliwość bieżącego monitorowania wykorzystania zasobów fizycznych infrastruktury wirtualnej (np. wykorzystanie procesorów, pamięci RAM, wykorzystanie przestrzeni na dyskach/wolumenach) oraz przechowywać i wyświetlać dane historyczne  • Zaoferowane oprogramowanie, w przypadku działania pod zarządcą klastra VMware vCenter, musi mieć możliwość przenoszenia maszyn wirtualnych w czasie ich pracy pomiędzy serwerami fizycznymi, pamięciami masowymi niezależnie od dostępności współdzielonej przestrzeni dyskowej, różnymi rodzajami wirtualnych przełączników sieciowych oraz pomiędzy różnymi Centrami Przetwarzania Danych platformami wirtualnej  • Zaoferowane oprogramowanie, w przypadku działania pod zarządcą klastra VMware vCenter, w środowisku z minimum dwoma wirtualizatorami, musi zapewniać pracę bez przestojów dla wybranych maszyn wirtualnych (o maksymalnie ośmiu procesorach wirtualnych), niezależnie od systemu operacyjnego oraz aplikacji, podczas awarii wirtualizatora, bez utraty danych i dostępności danych na maszynach wirtualnych objętych ochroną  • Zaoferowane oprogramowanie musi mieć wbudowany mechanizm kontrolowania i monitorowania ruchu do pamięci masowych oraz ustalania priorytetów dostępu do nich na poziomie konkretnych wirtualnych maszyn  • Zaoferowane oprogramowanie, w przypadku działania pod zarządcą klastra VMware vCenter, musi mieć możliwość grupowania pamięci masowych o podobnych parametrach w grupy i przydzielania ich do wirtualnych maszyn zgodnie z ustaloną przez administratora polityką  • Zaoferowane oprogramowanie musi umożliwiać udostępnianie pojedynczego urządzenia fizycznego (PCIe) jako logicznie separowanego wirtualnego urządzenia dedykowanego dla poszczególnych maszyn wirtualnych  • Zaoferowane oprogramowanie, w przypadku działania pod zarządcą klastra VMware vCenter musi mieć możliwość równoważenia obciążenia i zajętości pamięci masowych wraz z pełną automatyką i przenoszeniem plików wirtualnych maszyn z bardziej zajętych na mniej zajęte przestrzenie dyskowe lub/i z przestrzeni dyskowych bardziej obciążonych operacjami I/O na mniej obciążone  • Zaoferowane oprogramowanie musi wspierać technologię rozproszonego udostępniania procesora graficznego Nvidia Grid vGPU zainstalowanego w serwerze fizycznym do maszyn wirtualnych  • Zaoferowane oprogramowanie musi wspierać funkcjonalność trwałej, nieulotnej pamięci (ang. Persistent Memory)  • Zaoferowane oprogramowanie musi wspierać protokół Remote Direct Memory Access (RDMA) poprzez konwergentny Ethernet, lub RoCE (“rocky”) v2 i iSCSI rozszerzenie dla RDMA (iSER). Wymaga się aby maszyny wirtualne można było konfigurować z wykorzystaniem protokołu RDMA  • Zaoferowane oprogramowanie musi posiadać możliwość testowania wybranych serwerów (w szczególności tych, na których uruchomione są aplikacje przetwarzające dane wrażliwe i które mają dostęp do kluczy szyfrujących maszyny wirtualne) w celu weryfikacji, czy oprogramowanie jest autentyczne i nie zostało zmodyfikowane. Funkcjonalność ta powinna działać w oparciu o chip TPM 2.0 zainstalowany w serwerze i powinna odbywać się poza centralną konsolą zarządzającą (która sama jest maszyną wirtualną) wyłącznie w oparciu o sprzętowe źródło zaufania (hardware root of trust). Tylko serwery, które przejdą weryfikację mogą mieć dostęp do kluczy szyfrujących  • W przypadku pracy w oparciu o zarządzanie z centralnej konsoli zarządzającej, centralna konsola zarządzająca musi wspierać możliwość wcześniejszego i automatycznego przetestowania wpływu jej aktualizacji na pozostałe podłączone do niej komponenty klastra oraz uruchomione na nim funkcjonalności. Musi również wspierać proces aktualizacji całego klastra poprzez automatyczne raportowanie kolejności aktualizacji podłączonych do niej komponentów i rekomendowanej ich wersji.  • Zaoferowane oprogramowanie musi wspierać możliwość eksportu konfiguracji centralnej konsoli zarządzającej wirtualizacją przez API i umożliwiać wykorzystanie jej jako szablonu przy kreowaniu kolejnych instancji centralnej konsoli zarządzającej oraz do weryfikacji poprawności konfiguracji zainstalowanych już instancji.  • Zaoferowane oprogramowanie musi wspierać funkcje DPU (ang. Digital Processing Unit) na zasadzie przekazywania obciążen sieci wirtualnej z hipervisora do oddzielnej jednostki DPU zainstalowanej w serwerze fizycznym  • Zaoferowane oprogramowanie musi wspierać funkcjonalność bezpośredniego tworzenia kontenerów oraz klastrów Kubernetes na hiperwizorze (warstwie wirtualizatora) za pomocą dostarczonej konsoli zarządzającej Kubernetes (Kubectl) |
| OPPW-3 | Zarządzanie klastrem wirtualizacyjnym | • Ilość instancji zaoferowanego oprogramowania do zarządzania klastrem wirtualizacyjnym musi być równa liczbie fizycznych core zaoferowanych w oprogramowaniu do wirtulizacji mocy obliczeniowej  • Zaoferowane oprogramowanie musi posiadać konsolę graficzną do zarządzania maszynami wirtualnymi i do konfigurowania innych funkcjonalności. min: zasobów dyskowych oraz zasobów sieci komputerowej. Konsola graficzna powinna działać jako zainstalowana aplikacja na maszynie wirtualnej. Dodatkowo wymaga się aby maszyna z aplikacją była wstępnie skonfigurowana i dostępna jako tzw. virtual appliance. Instalacja w/w virtaul appliance nie może wiązać się z potrzebą dostawy dodatkowego oprogramowania takiego jak np. system operacyjny lub baza danych.  • Zaoferowane oprogramowanie musi posiadać wbudowany serwer ściany ogniowej (ang. firewall) dający możliwość konfiguracji blokady lub akceptacji ruchu pomiędzy konsolą zarządzającą a serwerami oraz serwerami wirtualnymi na nich posadowionymi, przy założeniu blokowania całego ruchu a nie poszczególnych portów  • Zaoferowane oprogramowanie musi mieć możliwość konfiguracji uwierzytelniania użytkowników logujących się do niego w oparciu o minimum: domenę Microsoft Active Directory, Microsoft Active Directory over LDAP oraz Open LDAP.  • Zaoferowane oprogramowanie musi posiadać konsole graficzną, która musi być dostępna poprzez dedykowanego klienta (za pomocą przeglądarek minimum Mozilla Firefox oraz Chrome) lub poprzez konsolę graficzną, która zbudowana jest z wykorzystaniem języka HTML5  • Zaoferowane oprogramowanie musi posiadać funkcjonalność zcentralizowanego zarządzania hostami opartymi na rozwiązaniu VMware vSphere  • Zaoferowane oprogramowanie musi posiadać natywne mechanizmy do wykonywania kopii zapasowej swojej konfiguracji. Dodatkowo wymaga się możliwości ustawienia harmonogramu wykonywania kopii zapasowej. Wymaga się aby kopie zapasowe wspierały protokoły: FTPS, HTTPS, SCP, FTP oraz HTTP  • Zaoferowane oprogramowanie, poprzez rozszerzenie o dodatkową licencję oferowaną przez tego samego producenta musi posiadać wbudowaną funkcjonalność zarządzania wirtualną przestrzenią dyskową SDS (ang. Software Defined Storage)  • Zaoferowane oprogramowanie musi posiadać interfejs graficzny do prowadzenia prac administracyjnych w zakresie swojej konfiguracji oraz monitoringu (możliwość monitorowania obciążenia min. vCPU, vRAM, vHDD, sieci, bazy danych). Interfejs graficzny powinien być wykonany w standardzie HTML5  • Zaoferowane oprogramowanie zawiera możliwość automatyzacji instalacji wielu konsoli zarządzania poprzez użycie schematów konfiguracji.  • Zaoferowane oprogramowanie umożliwia aktualizowanie wielu wirtualizatorów równocześnie.  • Rozwiązanie musi pozwalać na wykorzystanie łącz o szybkości do 100 GbE do bezawaryjnego przenoszenia maszyn wirtualnych między wirtualizatorami.  • Rozwiązanie musi zapewniać natywne mechanizmy wysokiej dostępności HA (ang. high availability) w niezawodnej architekturze Active-Passive-Witness dla wszystkich składowych komponentów centralnej konsoli graficznej zarządzającej platformą wirtualną  • Zaoferowane oprogramowanie zapewnia podstawowe funkcje serwera zarządzania kluczami (KMS), które upraszcza włączenie szyfrowania i zaawansowanych funkcji bezpieczeństwa.  • Zaoferowane oprogramowanie, w przypadku zarządzania serwerami opartymi o VMware vSphere, musi prezentować poziom zbalansowania mocy obliczeniowej w klastrze opartym o w/w wirtualizatory  • Zaoferowane oprogramowanie musi wspierać zarządzanie nielimitowaną liczbą hostów wirtualizacyjnych  • Dostęp przez przeglądarkę do konsoli graficznej w zaoferowanym oprogramowaniu musi być skalowalny tj. powinien umożliwiać rozdzielenie komponentów na wiele instancji w przypadku zapotrzebowania na dużą liczbę jednoczesnych dostępów administracyjnych do środowiska |
| OPPW-4 | Monitorowanie | • Licencje zaoferowanego oprogramowania muszą być zaoferowane w formie „per core” fizyczny procesora fizycznego. Liczba core musi być równa liczbie core zaoferowanego oprogramowania do wirtualizacji mocy obliczeniowej.  ● Zaoferowane oprogramowanie musi uzyskiwać informacje na temat wydajności środowiska wirtualnego pod kątem zarządzania pojemnością  ● Zaoferowane oprogramowanie musi za pomocą wbudowanych inteligentnych algorytmów przewidywać trendy związane z pojemnością środowiska wirtualnego opartego na rozwiązaniu VMware vSphere  ● Zaoferowane oprogramowanie musi posiadać funkcjonalność dającą możliwość analizy środowiska wirtualnego pod kątem optymalizacji wykorzystania zasobów (CPU, RAM, zasoby dyskowe)  ● Zaoferowane oprogramowanie musi mieć możliwość tworzenia unikalnego zbioru obiektów korespondujących funkcjami z obiektami Datacenter, tzn. musi być możliwe grupowanie obiektów w logiczne zbiory, dla których będzie istniała możliwość informowania o alertach, pojemności, ryzykach zgromadzonych w zbiorze obiektów. Obiekty mogą pochodzić z różnych Data Center objętych tym rozwiązaniem.  ● Zaoferowane oprogramowanie musi mieć możliwość tworzenia unikalnego/dedykowanego profilu pojemności, tzn. będzie możliwe grupowanie obiektów z Data Center w logiczne zbiory, dla których będzie istniała możliwość informowania o alertach, pojemności, ryzykach zgromadzonych w zbiorze obiektów.  ● Zaoferowane oprogramowanie musi mieć funkcjonalność tworzenia scenariuszy predykcyjnego obliczania pojemności na zasadzie: "co jeśli" dla minimum: co jeśli dodamy kolejne maszyn wirtualne. Rozwiązanie będzie umożliwiało definiowanie poziomów buforów potrzebnych do zachowania wysokiej dostępności. Analiza pojemności musi odnosić się zarówno do średniego obciążenia środowiska, jak również do tzw. skoków obciążenia  ● Zaoferowane oprogramowanie musi mieć funkcjonalność zapisywania i przechowywania różnych scenariuszy "co by było gdyby" w obszarze zarządzania pojemnością. Zapisane scenariusze muszą wpływać na prognozowanie analizy pojemności  ● Zaoferowane oprogramowanie musi w obszarze zarządzania pojemnością mieć funkcjonalność definiowania poziomu konsolidacji/wirtualizacji (ilość wirtualnych rdzeni do fizycznych lub ilość wirtualnej pamięci do fizycznej) po to aby w zakresie poprawnie wykonywać predykcję pojemności w przyszłości w modelu przypisanych zasobów wirtualnych (ilość wirtualnych rdzeni do fizycznych lub ilość wirtualnej pamięci do fizycznej)  ● Zaoferowane oprogramowanie musi monitorować infrastrukturę opartą o rozwiązania VMware vSphere oraz VMware vSAN.  ● Zaoferowane oprogramowanie, w obrębie monitorowania, będzie posiadało rozwiązanie generowania alertów na podstawie korelacji wykrytych w środowisku wirtualnym anomalii i symptomów, a nie pojedynczych monitorowanych metryk  ● Zaoferowane oprogramowanie musi posiadać funkcjonalność dostarczania informacji na temat rekomendowanych przez producenta posiadanego środowiska opartego o VMware vSPhere działań, mających na celu prawidłowe działanie środowiska opartego na rozwiązaniu VMware vSphere  ● Zaoferowane oprogramowanie musi posiadać wbudowane komponenty integracyjne obsługujące zewnętrzne kolektory logów i zdarzeń  ● Zaoferowane oprogramowanie musi posiadać funkcjonalność monitorowania i alertowania na temat zgodności serwerów opartych na rozwiązaniu VMware vSphere z najlepszymi praktykami bezpieczeństwa "VMware vSphere hardening" oraz DISA (Defence Information Systems Agency), FISMA (Federal Information Security Management Act), ISO, CIS (center of internet security), PCI (Payment Card Industry) i HIPAA (Health Insurance Portability and Accountability Act).  ● Zaoferowane oprogramowanie musi posiadać bazę wiedzy eksperckiej, która będzie używana przez administratorów, jako źródło dobrych praktyk, sugestii, opisu typowych problemów i błędów związanych ze środowiskiem zwirtualizowanym  ● Zaoferowane oprogramowanie musi wizualizować w trybie online obciążenie środowiska wirtualnego wraz z tzw. funkcjonalnością „drill down” do minimum 2 poziomów zagnieżdzenia  ● Zaoferowane oprogramowanie musi posiadać funkcjonalność graficznej prezentacji wyników (ang. dashboard)  ● Zaoferowane oprogramowanie musi posiadać funkcjonalność aktywnych map graficznych ukazujących elementy lub całe środowisko wirtualne bez konieczności korzystania z usługi wsparcia technicznego producenta do ich dodatkowego wytwarzania podczas używania oprogramowania  ● Zaoferowane oprogramowanie musi dokonywać automatycznej predykcji wykorzystania zasobów maszyn fizycznych na podstawie analiz zebranych danych, informacji pochodzących z modułu zarządzania cyklem życia maszyn wirtualnych (wbudowanego w zaoferowane oprogramowanie) oraz planów uruchomienia kolejnych serwerów wirtualnych. Zakres historii do analityki predykcyjnej musi wynosić co najmniej 6 miesięcy  ● Zaoferowane oprogramowanie musi umożliwiać przeglądanie linii trendu monitorowanych parametrów  ● Zaoferowane oprogramowanie musi umożliwiać tworzenie raportów pojemnościowych dla monitorowanego środowiska, zarówno dla urządzeń wirtualnych jak i fizycznych, związanych z wirtualiztorem opartym o rozwiązanie VMware vSphere oraz fizycznymi zasobami dyskowymi poza środowiskiem wirtualnym  ● Zaoferowane oprogramowanie musi umożliwiać monitorowanie środowisk w czasie rzeczywistym (przeglądane informacje powinny ukazywać się w trybie rzeczywistym – dopuszczane jest maksymalne opóźnienie nie większe niż 5 minut)  ● Zaoferowane oprogramowanie musi pozyskiwać oraz prezentować, w formie wykresów oraz tabelaryczno-tekstowej, zbiorczo oraz osobno, dla każdego systemu operacyjnego, aktualne i historyczne dane dotyczące utylizacji CPU, RAM, zasobów dyskowych oraz interfejsów sieciowych  ● Zaoferowane oprogramowanie musi umożliwiać przeglądanie wszystkich zbieranych statystyk w dowolnie wybranym zakresie czasu w postaci wykresów . Stopień szczegółowości zapisywania metryk musi wynosić co najmniej 5 punktów danych na minutę w ciągu 10 lat  ● Zaoferowane oprogramowanie musi umożliwiać szczegółowe monitorowanie komponentów serwerów fizycznych (CPU, Ethernet, RAM, zasoby dyskowe)  ● Zaoferowane oprogramowanie musi umożliwiać definiowanie progów wydajności i pojemności w celu identyfikacji przypadków wąskich gardeł  ● Zaoferowane oprogramowanie musi posiadać możliwość kasowania, wykonywania kopii migawkowych (ang. snapshot), włączania oraz wyłączania maszyn wirtualnych posadowionych na monitorowanym środowisku wirtualnym  ● Zaoferowane oprogramowanie musi automatycznie przeszukiwać i analizować zebrane dane w celu wynajdywania nadmiarowości oraz niedoborów przyznanych zasobów (CPU, RAM, HDD) w monitorowanym środowisku  ● Zaoferowane oprogramowanie musi posiadać funkcjonalność automatycznego alarmowania w sytuacji nietypowych (system monitoringu obserwuje i analizuje zachowanie platformy wirtualnej, na tej podstawie podnosi alarmy o minimum nie normalnym w tym dniu zwiększonym obciążeniu elementu platformy wirtualnej)  ● Zaoferowane oprogramowanie musi posiadać możliwość dowolnego przypisywania powiadamiania o alertach w środowisku dla różnych grup odbiorców (także z użyciem alertów stworzonych we własnym zakresie przez użytkownika)  ● Zaoferowane oprogramowanie musi pozwalać na odczyt wyświetlanych alarmów dotyczących monitorowanego środowiska wirtualnego wraz z powiązanymi z nimi poradami eksperckim  ● Zaoferowane oprogramowanie musi umożliwiać definiowanie alertów związanych z: zarządzaniem pojemnością, zarządzaniem wydajnością, anomaliami w środowisku, zarządzaniu dostępnością dla monitorowanego środowiska  ● Zaoferowane oprogramowanie musi mieć posiadać funkcjonalność przypisania alertu do administratora/operatora rozwiązującego problem  ● Zaoferowane oprogramowanie musi integrować się z produktem VMware Log Insight (poprzez integracje Zamawiający rozumie możliwość przesyłania danych z rozwiązania VMware Log Insight do zaoferowanego oprogramowania). Zamawiający dodatkowo wymaga, aby konfiguracja dostępu/integracji do/z VMware Log Insight odbywała się z konsoli zaoferowanego oprogramowania poprzez podanie danych dostępowych i adresowych do systemu VMware Log Insight  ● Zaoferowane oprogramowanie musi mieć możliwość generowania gotowych, predefiniowanych raportów o stanie monitorowanego środowiska  ● Zaoferowane oprogramowanie musi integrować się z produktem VMware Network Insight (przez integrację Zamawiający rozumie możliwość dostarczania danych o wykrywaniu aplikacji z rozwiązania VMware Network Insight do oferowanego oprogramowania). Musi również zapewnić możliwość wyszukiwania w kontekście obiektów w interfejsie VMware Network Insight.  ● Zaoferowane oprogramowanie musi posiadać funkcjonalność gotowego pulpitu kierowniczego (ang. dashboard) za pomocą którego administrator będzie posiadał gotowe kolumny z następującymi informacjami:  o Zdarzenia jakie wystąpiły w zadanym okresie czasu dla analizowanego problemu, min. dla: wirtualnych maszyn, sieci wirtualnej, wirtualnej przestrzeni dyskowej  o Anomalie, jakie wystąpiły w zadanym okresie czasu dla analizowanego problemu  o Zmiany w konfiguracji monitorowanej infrastruktury jakie wystąpiły w zadanym okresie czasu dla analizowanego problemu  o Analiza danych ukazująca powyższe wyniki prezentowane w dashboard musi odbywać się automatycznie poprzez mechanizmy uczenia się maszynowego zaoferowanego oprogramowania do monitorowania na podstawie zakresu czasowego definiowanego przez użytkownika tego Dashborad. Dodatkowo użytkownik musi mieć możliwość definiowania, dla którego obiektu, np. wybranej maszyny wirtualnej należy przeprowadzić analizę, a następnie wyświetlić jej wyniki.  ● Zaoferowane oprogramowanie musi wspierać kolektory do zdalnego zbierania danych w sieciach o słabej wydajności (do 200 ms)  ● Oferowane oprogramowanie musi wspierać zbieranie do 0,5 mln obiektów na klaster z 50 mln metryk; ilość obsługiwanych jednoczesnych wywołań Rest API do pobierania danych wynosi co najmniej 3000  ● Zaoferowane oprogramowanie musi posiadać możliwość zastosowania dodatkowych adapterów umożliwiających integrację z systemami firm trzecich monitorującymi infrastrukturę  ● Zaoferowane oprogramowanie musi posiadać możliwość zastosowania dodatkowych paczek monitorujących dla rozwiązań firm trzecich  ● Zaoferowane oprogramowanie musi umożliwiać konfiguracje trybu wysokiej dostępności (ang. HA) dla każdego swojego komponentu w celu unikania awarii pojedynczego elementu. Należy zapewnić architekturę, która zapobiega utracie danych w przypadku awarii jednego z węzłów klastra.  ● Zaoferowane oprogramowanie musi posiadać funkcjonalność zmiany parametrów maszyn wirtualnych, minimum CPU i RAM, za pomocą wygenerowanego w tym oprogramowaniu zadania. Dodatkowo, wymagana jest funkcjonalność odkładania w czasie w/w zadania, po wygenerowaniu (zadanie może być uruchamiane w momencie utworzenia lub w dowolnie skonfigurowanym przez użytkownika czasie)  ● Zaoferowane oprogramowanie musi posiadać możliwość zastosowania dodatkowych adapterów odpowiadających za monitorowanie systemów zewnętrznych takich jak m.in: macierze dyskowe, chmury obliczeniowe, serwery fizyczne, przełączniki LAN/SAN, umożliwiając tym samym wykorzystanie dedykowanych dodatkowych mechanizmów monitorujących określone komponenty  ● Zaoferowane oprogramowanie musi umożliwiać elastyczne dostosowanie wyglądu interfejsu użytkownika w zależności od indywidualnych potrzeb  ● Oferowane oprogramowanie musi zapewniać kompleksowe możliwości wyszukiwania po wszystkich przechowywanych obiektach, ich właściwościach i wartościach metryk  ● Zaoferowane oprogramowanie musi posiadać funkcję tzw. konfiguratora własnych widoków zgromadzonych danych, który musi umożliwiać tworzenie zaawansowanych widoków dotyczących wszystkich monitorowanych metryk  ● Zaoferowane oprogramowanie musi posiadać funkcję tzw. konfiguratora własnych pulpitów kierowniczych (ang. dashboard) na podstawie zgromadzonych danych w rozwiązaniu. Za pomocą tej funkcjonalności rozwiązanie musi umożliwiać tworzenie zaawansowanych pulpitów kierowniczych (dashborad)  ● Zaoferowane oprogramowanie musi posiadać funkcjonalność monitorowania systemów operacyjnych serwerów wirtualnych opartych na platformie VMware (w tym Windows, Linux) bez udziału agentów i dostarczać takich danych jak: zużycie pamięci, nazwa DNS, wykorzystanie systemu plików  ● Oferowane oprogramowanie musi posiadać funkcjonalność wykrywania usług (Service Discovery) serwerów wirtualnych opartych o platformę VMware (w tym Windows, Linux) bez agentów. Administrator może wybrać pożądaną usługę z biblioteki lub określić własną.  ● Zaoferowane oprogramowanie musi posiadać funkcjonalność monitorowania systemów operacyjnych (m.in. Windows, Linux) za pomocą zainstalowanego agenta w monitorowanym systemie operacyjnym  ● Zaoferowane oprogramowanie musi posiadać funkcjonalność integracji z rozwiązaniem VMware Skyline, VMware ServiceNow oraz VMware vRealize Automation  ● Zaoferowane oprogramowanie musi posiadać gotowe paczki do monitorowania (ang. management packs) dla produktów VMware vRealize Orchestrator, VMware SDDC, VMware vRealize Automation  ● Zaoferowane oprogramowanie musi mieć funkcjonalność tworzenia scenariuszy pojemnościowych na zasadzie: "co jeśli" dla minimum: CPU, RAM, oraz przestrzeni dyskowej dla następujących elementów:  o Dodawania nowych serwerów fizycznych  o Dodawania dodatkowych elementów VMware vSAN  o Migracji do VMware Cloud on AWS, AWS (Amazon Web Services), Microsoft Azure, Google Cloud Platform, IBM lub VMware Cloud Provider Program  ● Zaoferowane oprogramowanie musi posiadać możliwość matematycznego wyliczania wartości super metryki na podstawie innych, gromadzonych i monitorowanych metryk podstawowych. Super metryka to formuła matematyczna, która zawiera jedną lub więcej metryk. Jest to niestandardowa metryka, którą można zaprojektować w rozwiązaniu, aby pomóc śledzić kombinacje metryk, z jednego obiektu lub z wielu obiektów  ● Zaoferowane oprogramowanie musi wykrywać usługi uruchomione na monitorowanych maszynach wirtualnych, a następnie budować relacje lub zależności między usługami z różnych maszyn wirtualnych na podstawie komunikacja sieciowej  ● Zaoferowane oprogramowanie musi posiadać możliwość, po uruchomieniu alarmu, wykonywać na podstawie tego alarmu, automatyczne działania dotyczących akcji naprawczych  ● Zaoferowane oprogramowanie musi posiadać funkcjonalność monitorowania urządzeń firm trzecich typu macierze dyskowe, urządzenia sieciowe, a także wirtualizatorów innych niż rozwiązanie VMware vSphere za pomocą specjalnie przygotowanych paczek do monitorowania  ● Zaoferowane oprogramowanie musi umożliwiać wykazanie zrównoważonego rozwoju (sustainability) w centrach danych klienta poprzez pokazanie redukcji śladu węglowego wynikającej z wdrożenia wirtualizacji serwerów, optymalizacji obciążeń i innych działań  ● Zamawiający wymaga, aby w ramach oprogramowania do monitoringu można było uruchamiać w nim dedykowane wtyczki i konektory do monitoringu dla poniżej przedstawionych rozwiązań:  o Arista EOS  o Cisco Catalyst  o Cisco Nexus  o Cisco MDS  o Citrix ADC  o F5 Big IP  o Palo Alto Networks  o Wtyczka do monitorowania urządzeń sieciowych w oparciu o SNMP  o IBM PowerVC  o IBM HMC  o Microsoft Hyper-V  o VMware Tanzu Application Service  o Microsoft SCOM  o Nagios  o Oracle Enterprise Manager  o Service Now |
| OPPW-5 | Logowanie | ● Licencje zaoferowanego oprogramowania muszą być zaoferowane w formie „per core” fizyczny procesora fizycznego. Liczba core musi być równa liczbie core zaoferowanego oprogramowania do wirtualizacji mocy obliczeniowej.  ● Zaoferowane oprogramowanie musi zapewniać możliwość centralnego gromadzenia i analizy wszystkich logów z urządzeń fizycznych wykorzystujących technologię „Syslog”  ● Zaoferowane oprogramowanie musi integrować się z wymaganym w przedmiotowym postępowaniu oprogramowaniem do monitorowania w ten sposób, że z poziomu konsoli użytkownika oprogramowania do monitorowania musi istnieć możliwość uzyskania natychmiastowego dostępu do logów konkretnego urządzenia fizycznego  ● Zaoferowane oprogramowanie musi umożliwiać personalizację i wizualizację logów w postaci wykresów minimum: liniowych, kołowych oraz słupkowych  ● Zaoferowane oprogramowanie musi w pełni integrować się z zaoferowanym oprogramowaniem do zarządzania klastrem wirtualizacyjnym  ● Zaoferowane oprogramowanie musi posiadać wbudowaną bazę wiedzy dotycząca logów oraz zdarzeń dla platformy wirtualizacyjnej VMware  ● Zaoferowane oprogramowanie musi posiadać możliwość udostępniania raportów za pomocą URL kierującego do systemu logowania wysyłanego do odbiorcy  ● Zaoferowane oprogramowanie musi umożliwiać łatwą korelację wybranych zdarzeń w infrastrukturze fizycznej/wirtualnej oraz ich graficzną prezentację  ● Zaoferowane oprogramowanie musi posiadać możliwość personalizacji interfejsu graficznego w zależności od użytkownika/operatora  ● Zaoferowane oprogramowanie musi umożliwiać łatwe i szybkie przeszukiwanie logów w oparciu o zdefiniowane przez użytkownika kryteria  ● Zaoferowane oprogramowanie musi posiadać funkcjonalność implementacji dedykowanych modułów do analizy logów innych urządzeń fizycznych np. macierzy dyskowych, przełączników LAN,itp., tak aby analiza i korelacja wszystkich wiadomości systemowych mogła odbywać się z jednej konsoli zarządzającej  ● Zaoferowane oprogramowanie musi posiadać mechanizmy efektywnej analizy wszystkich rodzajów logów, takich jak np. logi aplikacji, logi sieciowe, pliki konfiguracyjne, informacje, dane wydajnościowe, zrzuty awaryjne itp., a także logów ‘nieustrukturyzowanych”  ● Zaoferowane oprogramowanie musi umożliwiać definiowanie struktury dla logów nieustrukturyzowanych  ● Zaoferowane oprogramowanie musi mieć możliwość raportowania utylizacji klastra wytworzonego na potrzeby przyjmowania dużych obciążen EPS oraz przedstawiania tego zużycia w postaci grafów  ● Zaoferowane oprogramowanie musi dawać możliwość zabezpieczenia kanału wysyłania logów na zewnątrz oprogramowania za pomocą SSL  ● Zaoferowane oprogramowanie musi mieć możliwość granularnej aktualizacji pojedynczych agentów zainstalowanych na systemach operacyjnych  ● W zaoferowanym oprogramowaniu uprawnienia do interfejsu prezentacji i analizy logów muszą dopuszczać rozłączność z uprawnieniami do infrastruktury, z której zbierane są logi  ● Zaoferowane oprogramowanie musi umożliwiać generowanie i eksportowanie dowolnych raportów związanych z zarejestrowanymi zdarzeniami i logami. Oprogramowanie musi pozwalać na tworzenie raportów, które można wysyłać za pomocą zdefiniowanych parametrów czasowych (ang. schedule)  ● Zaoferowane oprogramowanie musi zapewniać możliwość stworzenie klastra składającego się z co najmniej 18 węzłów, z którego każdy ma wydajność 15 000 EPS (ang. Events Per Second), co sumarycznie daje 270 000 EPS oraz 60 TB przestrzeni dyskowej  ● Zaoferowane oprogramowanie musi zapewniać wsparcie dla transformacji logów takich jak: filtrowanie logów (Log Filtering), przekazywanie logów do innych systemów (Forwarding) i maskowanie logów (Masking)  ● Zaoferowane oprogramowanie musi posiadać możliwość logowania zdarzeń z platformy Kubernetes za pomocą agenta fluentd  ● Zaoferowane oprogramowanie musi mieć możliwość określania czasu retencji danych, tzn. Administrator w konsoli graficznej do zarządzania platformą do zbierania i korelacji logów musi mieć możliwość określenia czasu po jakim zebrane logi będą archiwizowane (eksportowane) na zewnętrznej macierzy dyskowej po protokole NFS. Dodatkowo wymaga się aby retencja mogła być ustawiana granularnie, tj. np. inny czas retencji dla logów z urządzeń klasy firewall a inny czas retencji dla logów z hyperwizorów  ● Zaoferowane oprogramowanie musi mieć możliwość instalacji swoich agentów na systemach operacyjnych Windows i Linux w celu zbierania z nich logów. Zaoferowane oprogramowanie musi posiadać możliwość granularnej aktualizacji poszczególnych agentów zainstalowanych na systemach operacyjnych. |
| OPPW-6 | Platforma do konteneryzacji | ● Zaoferowane oprogramowanie musi być certyfikowane przez Cloud Native Computing Foundation (CNCF) w ramach programu certyfikacji zgodności z oprogramowaniem Kubernetes. Link to strony CNCF https://www.cncf.io/certification/software-conformance/  ● Licencje zaoferowanego oprogramowania muszą być zaoferowane w formie „per core” fizyczny procesora fizycznego. Liczba core musi być równa liczbie core zaoferowanego oprogramowania do wirtualizacji mocy obliczeniowej.  ● Platforma musi umożliwiać deklaratywne definiowanie limitów zasobów systemowych takich jak pamięć RAM i moc procesora, które będą dostępne dla projektu (grupy obiektów tj. wiele klastrów kubernetes, maszyn wirtualnych), jak i dla poszczególnych kontenerów aplikacji.  ● Platforma musi umożliwiać automatyczne stworzenie i zarządzanie min. 100 klastrami kubernetes. Licencja wraz ze wsparciem technicznym nie może ograniczać w żaden sposób tej ilości.  ● Platforma musi umożliwiać uruchamianie wielu aplikacji równocześnie na współdzielonych zasobach sprzętowych umożliwiając budowanie aplikacji pracujących w oparciu o maszyny wirtualne oraz mikro-serwisy.  ● Platforma do automatycznego tworzenia i zarządzania klastrami kubernetes musi posiadać narzędzia do zarządzania infrastrukturą (automatyczne tworzenie klastrów kubernetes, modyfikowanie ilości węzłów i ich wielkości (moc CPU, pojemność RAM, pojemność dyskowa), usuwanie klastrów kubernetes, aktualizowanie do nowszej wersji klastrów kubernetes) poprzez Cluster API wraz ze wsparciem technicznym producenta całości oferowanej platformy.  ● Platforma musi zapewniać środowisko wykonawcze kontenera, które umożliwia interakcję z wtyczkami sieciowymi (w standardzie CNI) i pamięcią masową (w standardzie CSI).  ● Platforma musi posiadać możliwość wyboru co najmniej dwóch różnych rodzajów oprogramowania sieciowego w ramach automatycznego tworzenia klastra Kubernetes przez użytkownika platformy poprzez interfejs CNI. Dodatkowo musi być wspierana integracja z zewnętrznym (poza kubernetes) rozwiązaniami klasy SDN (ang. Software Defined Network), tak aby była możliwość tworzenia polityk bezpieczeństwa z poziomu rozwiązania SDN.  ● Platforma poprzez zintegrowaną wtyczkę CSI musi umożliwiać realizowanie trwałych zasobów bezpośrednio na kompatybilnej z platformą pamięci masowej co najmniej w trybie pojedynczego odczytu  ● Platforma do tworzenia i zarządzania klastrami Kubernetes musi umożliwiać pracę w środowiskach zamkniętych (ang. air-gapped enviroments).  ● Platforma musi umożliwiać przesyłanie logów do zewnętrznych systemów logowania.  ● Platforma musi umożliwiać budowanie i uruchamianie aplikacji stanowych i bezstanowych na bazie orkiestratora Kubernetes. Orkiestrator Kubernetes musi posiadać wsparcie producenta oprogramowania.  ● Platforma musi umożliwiać izolację aplikacji przy użyciu technologii kontenerów w taki sposób, że na jednej instancji systemu operacyjnego równocześnie może być uruchomionych wiele odizolowanych aplikacji mających dostęp do ograniczonych zasobów systemowych takich jak pamięć RAM, moc procesora i system plików.  ● Platforma powinna zapewniać przekazywanie danych do systemu SIEM.  ● Platforma musi mieć możliwość uruchomienia i zarządzania w chmurze prywatnej opartej o wirtualizator VMware vSphere w wersji 7 lub nowszy. |

* + 1. **Oprogramowanie do wykonywania i odtwarzania kopii zapasowych**

**Producent ………………………….….**

**Model ……………………….…….**

| **Identyfikator wymagania** | **Wymaganie** | **Opis wymagania** |
| --- | --- | --- |
| OPPW-1 | Ogólne | Oprogramowanie musi integrować się z posiadanym przez Zamawiającego oprogramowaniem Dell Data Protection Suite 4 VMware w celu tworzenia i zarządzania harmonogramami wykonywania kopii zapasowych maszyn wirtualnych z poziomu konsoli serwera Networker oraz zapewniać wszystkie funkcjonalności dostępne w aplikacji NetWorker oraz Avamar w szczególności w kontekście współpracy z eksploatowanymi urządzeniami DD9400 |
| OPPW-2 | Pozostałe | Oprogramowanie musi umożliwiać skonfigurowanie środowiska zapewniającego:   * + odtworzenie aktualnie eksploatowanego środowiska NetWorker poprzez zaimportowanie aktualnie wykorzystywanej bazy katalogowej w tym środowisku   + bezpośrednią replikację danych z Avamar Virtual Edition (AVE), umożliwiającą kontynuację działania (realizacja nowych backup’ów oraz możliwość odtwarzania danych zreplikowanych) rozwiązania w przypadku awarii dotychczasowego środowiska AVE * Oprogramowanie musi umożliwiać deduplikację na źródle (na poziomie zwykłego klienta) w przypadku składowania danych na urządzeniach DataDomain/PowerProtect * Oprogramowanie musi umożliwiać replikację Managed File Replication oraz MTree Replication pomiędzy urządzeniami DataDomain/PowerProtect * Oprogramowanie musi być wspierane przez oprogramowanie Cyber Recovery definiujące plan synchronizacji danych z Cyber Bunkrem, zarządzające portami komunikacyjnymi, realizacją kopii danych przechowywanych w trybie Compliance, udostępnianie zasobów do celów testowych bądź odtworzeniowych * Oprogramowanie musi umożliwiać Retention Lock Governance oraz Compliance na eksploatowanych urządzeniach DataDomain/PowerProtect:   + wymagana możliwość uruchomienia blokady dla określonych danych z poziomu aplikacji backup’owej   + wymagana możliwość określenia/wymuszenia czasu blokady z poziomu aplikacji backup’owej   + wymagana możliwość raportowania od strony aplikacji backup’owej danych zabezpieczonych przed usunięciem blokadą Retention Lock   + wymagane wsparcie dla Data Domain Automatic Retention Lock * Oprogramowanie musi umożliwiać realizycję backup’ów typu Virtual Synthetic Full w przypadku użycia DataDomain/PowerProtect * Oprogramowanie musi umożliwiać realizację backup’ów Block Based Backup w przypadku użycia DataDomain/PowerProtect * Oprogramowanie musi umożliwiać realizację backup’ów systemu plików w przypadku Windows oraz Linux z deduplikacja na źródle w przypadku urządzeń DataDomain/PowerProtect, bez pośrednictwa aplikacji backup’owej * Oprogramowanie w przypadku ochrony środowisk VMware vSphere w trybie Continuous Data Protection, musi zapewniać: * integrację na poziomie VMware vCenter Plug-in (ORCHESTRATION, MANAGEMENT) , vSphere Web Client GUI * wsparcie dla HA, DRS, S-DRS, VMotion, S-VMotion * możliwość integracji z VMware vRealize Operations Manager * możliwość instalacji na platformie ESXi * skalowalność zapewniająca wsparcie dla 8000 VM w obrębie poj. vCenter * zabepieczenie dowolnej maszyny wirtualnej wraz z aplikacjami w trybie ciągłym tzn. umożliwiającym odtworzenie do dowolnego punktu w czasie (tzw. PIT – Point In Time), wymagane wsparcie dla VMware ESXi 7.x, 8.x * możliwość tworzenia tzw. CONSISTENCY GROUP zapewniających identyczną konsystencję dla przynależących do danej grupy maszyn wirtualnych (VM), wymagane wsparcie dla min. 250 CONSISTENCY GROUP * zabezpieczenie realizowane za pośrednictwem ciągłej replikacji (a nie za pomocą SNAPSHOT’ów ) na poziomie VMDK oraz RDM, niezależnie od użytego storage’u (tzw. Storage Agnostic - warunkiem jest wsparcie przez VMware), wymagane wsparcie dla połączeń: FC, FCoE, iSCSI, NAS oraz DAS * wsparcie dla replikacji (bi-directional) asynchronicznej oraz synchronicznej (realizowanej na poziomie dostarczanego oprogramowania), połączonych z mechanizmem tzw. JOURNALING umożliwiającego odnotowanie wszystkich zmian zabezpieczanego środowiska * odporność na krótkotrwałe problemy (przeciążenie, zaniki) związane z siecią WAN * wbudowaną funkcjonalność deduplikacji oraz kompresji w przypadku transmisji danych poprzez WAN * wsparcie dla równoległej replikacji zabezpieczanego środowiska do różnych ośrodków docelowych (min. 3-ech), wsparcie dla replikacji równoległej musi być zapewnione również na poziomie grup konsystencji (CONSISTENCY GROUP) * możliwość:   + stworzenia DISASTER RECOVERY dla całego zabezpieczanego wirtualnego środowiska zbudowanego w oparciu o VMware   + operacyjne ODTWARZANIE dowolnej maszyny VM wraz z aplikacjami   + MIGRACJI danych w trybie ON-LINE na inne zasoby dyskowe * równoległe wsparcie środowisk lokalnych oraz zdalnych, wymagana możliwość pracy w 3-ech trybach, tzw.: CDP (Continuous Data Protection … tryb replikacji lokalnej), CRR (Continuous Remote Replication … tryb replikacji zdalnej), CLR (Continuous Local and Remote Replication … połączenie CDP oraz CLR … tryb replikacji lokalnej oraz zdalnej) w ramach dostarczonych licencji * granularność umożliwiająca pominięcie określonych plików VMDK związanych z wirtualnymi serwerami VM objętych protekcją * architekturę FAULT-TOLERANT, brak pojedynczego punktu awarii * możliwość odtworzenia zabezpieczanego środowiska do dowolnego punktu w czasie * możliwość trybu pracy umożliwiającego objęciem protekcją w sposób automatyczny nowo dodanych maszyn wirtualnych (VM) * możliwość zmian HW na poziomie infrastruktury zabezpieczanego środowiska bez negatywnego wpływu na działanie systemu * możliwość użycia mechanizmu typu BOOKMARK dla oznaczenia konsystentnych kopii zabezpieczanych aplikacji * wsparcie dla VSS, zapewnienie konsystencji aplikacji na poziomie VSS * możliwość automatycznego przeprowadzania operacji typu FAILOVER/FAILBACK do dowolnego punktu w czasie dla określonych produkcyjnych serwerów wirtualnych (VM), w tym: odtworzenie, uruchomienie (z zachowaniem wymaganej sekwencji), konfigurację * możliwość automatycznego przeprowadzania operacji typu FAILOVER/FAILBACK do dowolnego punktu w czasie określonych testowych maszyn wirtualnych (VM) * możliwość automatycznego zainicjowania procesu REVERSE REPLICATION w przypadku procesów FAILOVER/FAILBACK * możliwość przeprowadzania testów DR bez wpływu na zabezpieczane serwery produkcyjne oraz bez konieczności zmian w działaniu replikacji (np.: PAUSE, REVERSE, …) * możliwość skryptowego tworzenia planów RECOVERY * Oprogramowanie musi umożliwiać backup środowisk VMware vSphere przy uzyciu vSphere API for I/O (VAIO) Filtering framework (<https://core.vmware.com/resource/vmware-vsphere-apis-io-filtering-vaio#section1>) * Oprogramowanie musi umożliwiać monitorowanie, raportowanie, szczegółowe rozliczanie z użycia komponentów systemu backupowego oraz analizę błędów dla środowiska kopii zapasowej, wymagana dostępność następujących raportów:   + podsumowanie zadań backupowych (liczba backupów udanych, nieudanych, aktywnych, łączny rozmiar zbackupowanych danych)   + podsumowanie zadań odtworzeniowych (liczba odtworzeń udanych, nieudanych, aktywnych, łączny rozmiar odtworzonych danych danych)   + zbiorcze procentowe zestawienie udanych zadań backupowych z poszczególnych serwerów   + zbiorcze zestawienie zabezpieczanych serwerów które w sposób ciągły (kilka razy pod rząd) maja problem z backupami   + zestawienie zabezpieczanych systemów plików które w ogóle nie są backupowane   + spodziewany czas odtwarzania zabezpieczanego serwera oraz potencjalnej utraty danych (czas między ostatnim backupem a chwilą awarii)   + najmniej wiarygodne zabezpieczanych serwery (procent nieudanych backupów)   + lista najwolniejszych/najszybszych zabezpieczanych maszyn   + poziom SLA (procentowa liczba udanych backupów) w odniesieniu do poziomu założonego   + mierzenie poziomu SLA dla poszczególnych zabezpieczanych serwerów przy uwzględnieniu założonego okna backupowego i RPO (punktu do którego się odtwarzamy)   + liczba danych backupowanych dziennie   + liczba zadań backupowych dziennie   + zużycie zasobów na serwerach backupowych (procesor, pamięć, karty sieciowe LAN, SAN)   + zużycie mediów backupowych i napędów taśmowych   + aktualna konfiguracja systemu backupowego   + historia zmian konfiguracji systemu backupowego   + posiadane licencje systemu backupowego   + wykorzystanie systemu backupowego przez poszczególne działy / grupy użytkowników (chargeback per cost center) |

* 1. **USŁUGI**
     1. **Dostawa sprzętu i oprogramowania**

| **Identyfikator wymagania** | **Opis wymagania** |
| --- | --- |
| UDSO-1 | Wykonawca opracuje szczegółową specyfikację dostaw realizowanych przez Wykonawcę w ramach Umowy – Plan Dostaw. |
| UDSO-2 | Plan dostawy musi zawierać szczegółowy harmonogram dostaw do miejsca wskazanego przez Zamawiającego. |
| UDSO-3 | Plan dostaw musi zawierać procedurę odbioru jakościowego. |
| UDSO-4 | Plan dostaw musi zawierać procedurę zmian terminów w trakcie realizacji dostaw. |
| UDSO-5 | Plan dostaw musi zawierać procedurę obsługi uszkodzeń sprzętu w trakcie dostawy |
| UDSO-6 | Plan dostaw musi zawierać specyfikację niezbędnych dokumentów i protokołów potwierdzających prawidłowość dostawy |
| UDSO-7 | Wykonawca dostarczy całość sprzętu w miejsce wskazane przez Zamawiającego w poszczególnych lokalizacjach Zamawiającego. |
| UDSO-8 | Wykonawca dostarczy sprzęt w godzinach od 7:00 do 16:00 w dni robocze od poniedziałku do piątku. |
| UDSO-9 | Wykonawca zapewni we własnym zakresie środki transportu umożliwiające rozładunek i przewóz sprzętu z samochodu do pomieszczeń składowania lub serwerowni. |
| UDSO-10 | Wykonawca musi zapewnić we własnym zakresie zasoby ludzkie umożliwiające rozładunek i przewóz sprzętu z samochodu do pomieszczeń składowania lub serwerowni. |
| UDSO-11 | Wykonawca jest zobowiązany do wywiezienia we własnym zakresie wszelkich opakowań, palet, folii itp. materiałów pozostałych po dostarczonych elementach infrastruktury i oprogramowania. Wykonawca musi zapewnić we własnym zakresie zasoby ludzkie i środki transportu umożliwiające wykonanie tych prac. |
| UDSO-12 | Dostarczana infrastruktura techniczno-systemowa musi być zgodna z prawem obowiązującym podmioty publiczne. W szczególności wymagana jest zgodność z rozporządzeniem Rady Ministrów z dnia 12 kwietnia 2012 roku w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych |
| UDSO-13 | Wykonawca musi zapewnić, że wszystkie dostarczane produkty (dotyczy to zarówno sprzętu jak i oprogramowania) są ze sobą kompatybilne w zakresie, w jakim wymagana jest ich wzajemna współpraca. |
| UDSO-14 | Wszystkie urządzenia muszą zawierać osprzęt wymagany przez producentów oferowanego rozwiązania (na przykład: okablowanie energetyczne, urządzenia zasilające) niezbędny do jego prawidłowego podłączenia z siecią energetyczną Zamawiającego o parametrach: 230 V ± 10% , 50 Hz |
| UDSO-15 | Zamawiający wymaga, aby dostarczone urządzenia były fabrycznie nowe (tzn. bez śladów używania i uszkodzenia, wprowadzone na rynek zgodnie z przepisami obowiązującymi na terenie Unii Europejskiej, urządzenia muszą być dostarczone Zamawiającemu w oryginalnych opakowaniach fabrycznych zabezpieczających przed uszkodzeniem w trakcie transportu i składowania. |
| UDSO-16 | Wykonawca dostarczy wszystkie licencje wymagane do działania systemu. |
| UDSO-17 | Wykonawca dostarczy wszystkie klucze licencyjne wymagane do instalacji i działania dostarczanego Oprogramowania Gotowego. |
| UDSO-18 | Wykonawca dostarczy dokładny opis zasad licencjonowania dostarczanego Oprogramowania Gotowego. |
| UDSO-19 | W przypadku, gdy licencja oprogramowania objęta jest opłatą okresowej opieki wówczas Wykonawca poda wszystkie dane umożliwiające przedłużenie czasu opieki przez Zamawiającego. |

* + 1. **Projekt techniczny**

| **Identyfikator wymagania** | **Opis wymagania** |
| --- | --- |
| UPT-1 | Wykonawca opracuje Projekt Techniczny umożliwiający instalację i konfigurację wszystkich wymaganych komponentów. Projekt zostanie opracowany w uzgodnieniu z Zamawiającym. Zamawiający przekaże Wykonawcy wytyczne w zakresie konfiguracji poszczególnych elementów. |
| UPT-2 | Wykonawca opracuje projekt rozmieszczenia szaf „rack” w pomieszczeniach serwerowni, rozmieszczenia i instalacji dostarczanego sprzętu w szafach, doprowadzenia i podłączenia zasilania energetycznego do urządzeń.  Zamawiający dostarczy dokumentację projektową, będącą w jego posiadaniu i istotną dla opracowania projektu technicznego montażu i instalacji sprzętu, w terminie 3 dni roboczych od dnia podpisania Umowy. |
| UPT-3 | Dla projektowanej infrastruktury Wykonawca wykorzysta zasoby dostarczone w ramach niniejszego postępowania. |
| UPT-4 | Projekt musi zawierać minimum:   1. Rozmieszczenie sprzętu w szafie rack. 2. Projekt zasilania energetycznego. Wymagania na zasilanie oraz moc chłodniczą. 3. Projekt segmentu centralnego zarządzania wdrożoną infrastrukturą i oprogramowaniem oraz integracji z posiadanymi przez Zamawiającego rozwiązaniami wirtualizacji oraz backup. 4. Projekt adresacji IP LAN dostarczanego sprzętu oraz wykorzystania usług zapewnianych przez Zamawiającego z POPD i ZOPD - DNS, DHCP, serwer czasu 5. Projekt połączeń macierzy do serwerów. 6. Projekt konfiguracji LUN oraz układów RAID macierzy. 7. Projekt konfiguracji RAID serwerów. 8. Projekt włączenia serwerów do monitorowania centralnego. 9. Projekt nowych klastrów wirtualizacyjnych zbudowanych w oparciu o nowe serwery i macierze wraz z konfiguracją sieci LAN. 10. Projekt migracji danych z istniejących serwerów i klastrów wirtualizacyjnych na nowe serwery i klastry wirtualizacyjne. 11. Projekt wdrożenia rozwiązania systemu kopii zapasowych oraz integracji z posiadanym przez Zamawiającego rozwiązaniem. 12. Projekt wdrożenia okresowej synchronizacji kopii zapasowych z dostarczanych deduplikatorów z użytkowanym przez Zamawiającego rozwiązaniem typu „CyberBunkier”. 13. Projekt scenariuszy testowych umożliwiających weryfikację wdrożonego rozwiązania. |

* + 1. **Wymagania na montaż sprzętu, instalacja i konfiguracja sprzętu oraz oprogramowania (usługa)**

| **Identyfikator wymagania** | **Opis wymagania** |
| --- | --- |
| UMIKSO-1 | Wykonawca dostarczy, zainstaluje i skonfiguruje wszystkie komponenty zgodnie z opracowanym szczegółowym projektem technicznym. |
| UMIKSO-2 | Wykonawca dostarczy licencje oprogramowania, których liczba oraz zasady instalacji oprogramowania umożliwią eksploatację systemu. |
| UMIKSO-3 | Wykonawca zainstaluje szafy rack w pomieszczeniach wskazanych przez Zamawiającego zgodnie z opracowanym projektem technicznym. |
| UMIKSO-3 | Wykonawca zdemontuje istniejący sprzęt we wskazanych szafach RACK i zainstaluje w nich nowy dostarczany sprzęt (serwery, macierze, przełączniki LAN, deduplikatory) z uwzględnieniem kolejności migracji poszczególnych elementów. |
| UMIKSO-4 | Wykonawca dostarczy wszelkie niezbędne elementy do wykonania prac w szczególności kable elektryczne, światłowody, kable Ethernet kat. 6e, bezpieczniki, gniazda zasilające, moduły PDU do szaf rack, organizery okablowania itp. w ilości oraz długości pozwalającej na prawidłowe podłączenie wszystkich urządzeń zarówno dostarczanych w ramach przedmiotowego postępowania. **W ramach prac Wykonawcy leży podłączenie wszystkich oferowanych rozwiązań do sieci LAN i SAN Zamawiającego w ramach dostarczanego przełącznika oraz interfejsów macierzy.** |
| UMIKSO-5 | Wykonawca dokona montażu całości sprzętu w szafach RACK w pomieszczeniach wskazanych przez Zamawiającego zgodnie z opracowanym szczegółowym projektem technicznym. |
| UMIKSO-6 | Wykonawca dokona podłączenia dostarczonych urządzeń do sieci energetycznej Zamawiającego w sposób zapewniający redundancję. |
| UMIKSO-7 | Wykonawca wykona odpowiednie przyłącza elektryczne od rozdzielni elektrycznych w budynku do paneli PDU w szafach rack. Każde urządzenie posiadające redundantne zasilacze zostanie podłączone do dwóch niezależnych torów zasilania elektrycznego. W każdej szafie rack pozostanie wolnych co najmniej 5 gniazd elektrycznych z każdego toru zasilania. |
| UMIKSO-8 | Wykonawca wykona niezbędne otwory w podłodze technicznej w celu doprowadzenia okablowania. |
| UMIKSO-9 | Wykonawca ułoży okablowanie instalowanego sprzętu w przeznaczonych do tego celu korytkach, organizerach okablowania, szufladach zapasu itp. |
| UMIKSO-10 | Wykonawca dokona aktualizacji oprogramowania układowego (firmware, BIOS) wszystkich urządzeń i oprogramowania do najnowszych stabilnych wersji. |
| UMIKSO-11 | Wszystkie nośniki danych dostarczane wraz z urządzeniami pozostają w siedzibie Zamawiającego. Wykonawca dostarczy na płytach CD/DVD lub nośnikach USB komplet sterowników systemowych i niezbędne oprogramowanie narzędziowe i fabryczne. |

* + 1. **Konfiguracja środowisk zgodnie z Projektami Technicznymi (usługa)**

| **Identyfikator wymagania** | **Opis wymagania** |
| --- | --- |
| UKS-1 | Wykonawca przeprowadzi proces aktualizacji oprogramowania sprzętowego dostarczonych urządzeń do najnowszych dostępnych stabilnych wersji oprogramowania. |
| UKS-2 | Wykonawca zainstaluje i skonfiguruje wszystkie dostarczane urządzenia i oprogramowanie zgodnie z opracowanymi Projektami Technicznymi. |

* + 1. **Migracja danych (usługa)**

| **Identyfikator wymagania** | **Opis wymagania** |
| --- | --- |
| UMD-1 | Wykonawca migrację danych z istniejących w lokalizacjach prokuratury objętych wdrożeniem klastrów VMware na wdrażane rozwiązanie |
| UMD-2 | Migracja danych musi odbywać się z uwzględnieniem minimalnej niedostępności systemów. |
| UMD-3 | Okno serwisowe na migrację danych każdorazowo będzie uzgadniane i zatwierdzane przez Zamawiającego. |

* + 1. **Wymagania na przeprowadzenie testów wg zaakceptowanych przez Zamawiającego scenariuszy testów (usługa)**

| **Identyfikator wymagania** | **Opis wymagania** |
| --- | --- |
| UPT-1 | Wykonawca przeprowadzi testy zgodnie z opracowanymi i zatwierdzonymi scenariuszami testowymi. Przeprowadzenie testów musi być zakończone opracowaniem raportu z testów. |
| UPT-2 | Wykonawca opracuje dla każdego rodzaju testów Plan Testów który musi być zaakceptowany przez Zamawiającego. |
| UPT-3 | Testami zostanie objęta cała dostarczona Infrastruktura Techniczno- Systemowa. |
| UPT-4 | Wykonawca przeprowadzi testy sprawdzające niezawodność na wypadek awarii pojedynczego punktu infrastruktury według scenariuszy przygotowanych przez Wykonawcę i zatwierdzonych przez Zamawiającego |
| UPT-5 | Testy funkcjonalne weryfikujące poszczególne elementy sprzętowe oraz programowe powinny obejmować co najmniej:  sprawdzeniu poprawności funkcjonowania Sprzętu poprzez wykonanie testów fabrycznych (producenta) każdego dostarczonego Sprzętu,  sprawdzeniu logów w urządzeniach (stwierdzeniu braku błędów w logach),  wykonaniu testów sprawdzających poprawność działania poprzez zasymulowanie uszkodzenia dowolnego rodzaju redundantnego elementu w dowolnym urządzeniu oraz zasymulowanie uszkodzenia zasilania zewnętrznego. |

* + 1. **Wymagania na opracowanie dokumentacji powykonawczej (dokument)**

| **Identyfikator wymagania** | **Opis wymagania** |
| --- | --- |
| UDP-1 | Wykonawca opracuje szczegółową dokumentację techniczną powykonawczą zawierającą dokładny opis montażu, instalacji i konfiguracji zainstalowanego sprzętu |
| UDP-2 | Dokumentacja powykonawcza będzie zawierała szczegółowe opisy zastosowanych rozwiązań wraz ze wskazaniem miejsca, w którym zawarto opis spełnienia każdego z wymagań. |
| UDP-3 | Dokumenty będą dostarczone Zamawiającemu w języku polskim, w wersji elektronicznej, edytowalnej (plik MS Word) a także w wersji Portable Document Format (zgodny z ISO 32000-1:2008). Na żądanie Zamawiającego lub jeśli wynika to z Umowy Wykonawca dostarczy dokument w wersji drukowanej (wydruk kolorowy) i/lub w wersji stanowiącej skan Dokumentu. |
| UDP-4 | Wykonawca opracuje „Dokumentację administratora”. |
| UDP-5 | Dokumentacja administratora powinna zawierać co najmniej:  Procedury administracyjne  Procedury instalacji i konfiguracji  Procedury bieżących działań administracyjnych  Procedury okresowych/planowanych działań administracyjnych  Procedury aktualizacji standardowych elementów dostarczonego sprzętu  Procedury włączenia i wyłączenia całości dostarczanego sprzętu w przypadku prac planowych. |
| UDP-6 | Dokumentacja administracyjna oraz użytkowa musi być spójna z dokumentacją powykonawczą |
| UDP-7 | Projekt Techniczny montażu i instalacji sprzętu powinien zostać zaktualizowany do postaci dokumentacji powykonawczej w chwili przekazywania infrastruktury Zamawiającemu do akceptacji. |
| UDP-7 | Wykonawca dokona aktualizacji Polityki Wykonywania Kopii Zapasowych o wdrożone w poszczególnych lokalizacjach rozwiązanie do wykonywania kopii zapasowych. |
| UDP-7 | Wykonawca dokona aktualizacji Polityki Ciągłości Działania Systemów Teleinformatycznych uwzględniając wdrożone rozwiązanie w poszczególnych lokalizacjach wraz z przeprowadzeniem analizy ryzyka zasobów informatycznych objętych migracją, określeniem poziomu ich krytyczności oraz określeniem harmonogramu wykonywania kopii zapasowych we wdrożonym rozwiązaniu i synchronizacji krytycznych zasobów do rozwiązania typu CyberBunkier posiadanego przez Zamawiającego. |

* + 1. **Wymagania na przeprowadzenie warsztatów dla administratorów**

| **Identyfikator wymagania** | **Opis wymagania** |
| --- | --- |
| SZKOL-01 | Wykonawca zapewni szkolenia i warsztaty z dostarczanych produktów. Przewidywana ilość uczestników warsztatów to maksymalnie 40 osób wskazanych przez Zamawiającego. |
| SZKOL-02 | Wykonawca opracuje plan warsztatów oraz plan szkoleń z zakresu wdrażanego rozwiązania. Warsztaty z zakresu wdrażanego rozwiązania będą trwać 3 dni robocze. W ramach warsztatów nastąpi omówienie wdrożonego rozwiązania, plan migracji zasobów z dotychczas użytkowanego sprzętu, planu backupów systemów Zamawiającego oraz zabezpieczenie kopii zapasowych z wdrażanego środowiska w rozwiązaniu CyberBunkier. Zapewnienie odpowiedniego środowiska warsztatowego leży po stronie Wykonawcy. |
| SZKOL-03 | W zakresie warsztatów zadaniem Wykonawcy jest zapewnienie:   * 1. bazy noclegowej – dla organizatorów i uczestników      1. Obiekt nie może być w trakcie prac remontowych w czasie trwania warsztatów.      2. Wykonawca zapewnia wszystkie miejsca noclegowe w sposób zapewniający samodzielny pobyt w pokoju (Zamawiający dopuszcza zakwaterowanie samodzielne jednego uczestnika w pokoju dwuosobowym)      3. Każdy z pokoi noclegowych z łazienką, TV, łącze internetowe (Wi-Fi) posiadających otwierane okna lub działającą klimatyzację.      4. Obiekt co najmniej \*\*\* (trzy gwiazdki), w rozumieniu przepisów § 2 ust. 2 pkt 1 rozporządzenia Ministra Gospodarki i Pracy z dnia 19 sierpnia 2004 r. w sprawie obiektów hotelarskich i innych obiektów, w których są świadczone usługi hotelarskie (Dz. U. z 2006 r., Nr 22, poz. 169 ze zm.). Na każde żądanie Zamawiającego Wykonawca obowiązany jest okazać kopię decyzji właściwego Marszałka Województwa o nadaniu kategorii hoteli na podstawie art. 38 ust.1 i art. 42 ustawy z dnia 29 sierpnia 1997 r. o usługach turystycznych (Dz. U. z 2014 r., poz. 196 ze zm.),      5. Na terenie obiektu lub w bezpośrednim jego sąsiedztwie powinien znajdować się bezpłatny parking.      6. Obiekt powyżej trzech pięter powinien zostać wyposażony w windę      7. Warsztaty, nocleg oraz wyżywienie powinny odbywać się na terenie tego samego obiektu.   2. sala szkoleniowa musi być klimatyzowana i wyposażona w rzutnik multimedialny, ekran do wyświetlania prezentacji, tablicę do pisania lub flipchart z arkuszami papieru i pisakami, skaner,. Wykonawca zapewni w miejscu przeprowadzania szkoleń/warsztatów urządzenia sieciowe celem połączenia ze środowiskiem warsztatowym zorganizowanym po stronie Wykonawcy. Czas wykorzystania sal pierwszego dnia od godz. 12.00 do 20.00, pozostałe dni od godz. 8.00 do 19.00. Uczestnicy warsztatów będą posiadać własne komputery przenośne.   3. noclegów dla uczestników szkolenia/warsztatów w pokojach jednoosobowych z łazienkami lub dwuosobowych z łazienkami do samodzielnego wykorzystania **(Wykonawca ma obowiązek zapewnić nocleg każdej osobie w odrębnym pokoju).** Czas trwania doby hotelowej od godz. 11.00 pierwszego dnia szkolenia do godz. 16.00 ostatniego dnia szkolenia. Miejsca noclegowe muszą znajdować się na terenie tego samego obiektu, co sale wykładowe.   4. Wyżywienia dla uczestników szkolenia składającego się z:  1. śniadania podawanego w formie bufetu, obejmujące:   - pieczywo jasne i ciemne,  - wędliny (3 rodzaje),  - ser żółty  - ser biały  - jaja  - dżem  - miód  - ciepłe mleko  - płatki śniadaniowe (co najmniej 2 rodzaje)  - jogurt  - jedno danie ciepłe  - świeże warzywa (co najmniej 3 rodzaje)  - napoje (kawa, herbata, woda mineralna, sok 100%)  - masło, cytryna, mleko, cukier   1. obiadu w formie bufetu obejmującego:   - zupę,  - sałatki (minimum 2 rodzaje)  - dania ciepłe (rybne, mięsne, warzywne)  - dodatki skrobiowe  - desery  - napoje (kawa, herbata, woda mineralna, sok 100%)   1. kolacji w formie bufetu obejmującej:   - sałatki (minimum 2 rodzaje)  - pieczywo jasne i ciemne,  - wędliny (3 rodzaje),  - ser (3 rodzaje)  - dania ciepłe (rybne, mięsne, warzywne)  - napoje (kawa, herbata, woda mineralna, sok 100%)  - masło, cytryna, mleko, cukier   1. przerw kawowych (całodziennych, uzupełniany serwis konferencyjny), składający się:   - świeżo parzoną gorącą kawę naturalną oraz herbatę w torebkach  - cytrynę, cukier, mleko,  - sok owocowy 100%,  - butelkowana woda mineralna gazowana i niegazowana,  - co najmniej 3 rodzaje kruchych ciasteczek.   1. Posiłki, które będą podawane podczas szkoleń/warsztatów muszą być przygotowywane na terenie obiektu w którym odbywa się szkolenie. Wyklucza się ich dowożenie.    1. W zakresie wyżywienia Wykonawca zobowiązany jest do: 2. Terminowego przygotowania posiłków zgodnie z ustalonym harmonogramem. 3. Zachowania zasad higieny i obowiązujących przepisów sanitarnych przy przygotowywaniu posiłków. 4. Przygotowywania posiłków zgodnie z zasadami racjonalnego żywienia, urozmaiconych (każdego dnia szkolenia inne menu), przygotowywanych ze świeżych produktów z ważnymi terminami przydatności do spożycia. 5. Wyżywienie dla trenerów oraz innych osób zaangażowanych w obsługę szkolenia/warsztatów Wykonawca zapewnia na swój koszt. |
| SZKOL-04 | Wykonawca zobowiązany będzie do przygotowania i przedstawienia Zamawiającemu, co najmniej na 10 dni przed rozpoczęciem warsztatów, odpowiednich materiałów szkoleniowych, włączając w to materiały dla uczestników. Zamawiający zastrzega sobie prawo do żądania wprowadzenia poprawek i zmian do materiałów szkoleniowych. |
| SZKOL-05 | Wykonawca, w uzgodnieniu z Zamawiającym, przygotuje szczegółowe harmonogramy szkoleń i warsztatów. Zamawiający zastrzega sobie możliwość korekty przedstawionych dokumentów. Harmonogram zajęć powinien zawierać informacje dotyczące czasu i miejsca realizacji danego warsztatu lub szkolenia. |
| SZKOL-06 | Program szkoleń i warsztatów powinien zawierać informacje dotyczące tematyki prowadzonych zajęć z podziałem na zajęcia teoretyczne i praktyczne. Program powinien zawierać również informacje dotyczące wiedzy i umiejętności, jakie zdobędą uczestnicy po zakończeniu szkoleń i warsztatów. Zamawiający zastrzega sobie prawo do korekty programu szkoleń / warsztatów w uzgodnionym zakresie.  Minimalny zakres warsztatów:  a.1. W zakresie macierzy:  a.1.1. Architektura macierzy;  a.1.2. Funkcjonalności GUI;  a.1.3. Zalecenia dotyczące konfiguracji i udostępniania zasobów dyskowych dla serwerów;  a.1.4. Możliwości i zasady monitorowania;  a.1.5. Metody analizy błędów;  a.1.6. Zasady zabezpieczeń;  a.1.7. Ćwiczenia praktyczne.  a.2. W zakresie wirtualizacji:  a.2.1. Omówienie wirtualizatora;  a.2.2. Rozwiązania sieciowe wirtualizatora;  a.2.3. Zarządzanie zasobami dyskowymi dla hostów w klastrze ( w tym wykreowanie obszaru na macierzy + podłączenie do hosta);  a.2.4. Tworzenie maszyn wirtualnych (serwer + konfiguracja sieci + synchronizacja czasu + przydzielenie dysków);  a.2.5. Usuwanie maszyn wirtualnych;  a.2.6. Klonowanie maszyn wirtualnych;  a.2.7. Migracja maszyn między hostami;  a.2.8 Ćwiczenia praktyczne.  a.3. W zakresie kopii zapasowych i wdrożonych deduplikatorów:  a.3.1. Architektura deduplikatorów; integracja z CyberBunkrem  a.3.2. Backup maszyn wirtualnych;  a.3.3. Odtwarzanie maszyn wirtualnych  a.3.4. Ćwiczenia praktyczne  a.4. Wspólny segment zarządzania oraz podział odpowiedzialności pomiędzy administratorami Zamawiającego |
| SZKOL-07 | Potwierdzeniem prawidłowej realizacji warsztatów będzie podpisany bez zastrzeżeń przez Zamawiającego Protokół odbioru warsztatu wraz z dołączonymi załącznikami tj. oryginalną listą obecności, harmonogramem i programem warsztatu. |

* + 1. **Wymagany zespół Wykonawcy**

| **Identyfikator wymagania** | **Opis wymagania** |
| --- | --- |
| WKW-1 | **Kierownik Projektu Wykonawcy (KWP)**  KWP odpowiada za realizację projektu po stronie Wykonawcy. KWP realizuje swoje zadania pod nadzorem Kierownika Projektu Zamawiającego (KPZ).  KWP odpowiada za koordynację prac Zespołu Realizacyjnego Wykonawcy i jest pojedynczym punktem kontaktu dla KPZ.  KWP zarządza harmonogramem projektu oraz współpracuje z administratorami lokalnymi w celu realizacji wdrożenia. KPW nadzoruje wszystkie prace zespołów Wykonawcy oraz koordynuje działania z KPZ. Jego rolą jest dbanie o poprawność metodyczną, poprawne działanie procedur projektowych, planowanie pracy, opracowywanie harmonogramów szczegółowych, nadzór nad dokumentacją projektową, zarządzanie ryzykami w obszarze przedmiotu Umowy w szczególności jest zobowiązany do:   1. Udziału w spotkaniach zarządczych odbywających się w siedzibie 2. Zamawiającego, których celem będzie omówienie bieżących postępów prac, 3. zagadnień istotnych dla realizacji zamówienia, proponowanych przez 4. Wykonawcę rozwiązań, w szczególności mające wpływ na przedmiot i termin jego realizacji, 5. Sporządzania raportów przedkładanych Zamawiającemu. Raporty muszą zawierać informacje dotyczące postępu wykonywanych prac, zagadnień, i ryzyk, niezgodności z Harmonogramem realizacji Umowy, przewidywanych zagrożeń. Wykonawca zobowiązany jest składać następujące raporty w terminach:  * Raport miesięczny – co 30 dni począwszy od dnia podpisania umowy; * Raport końcowy Etapu/ Umowy– wraz z Protokołem odbioru końcowego.  1. Udziału w spotkaniach zwoływanych w sytuacjach nadzwyczajnych zaistniałych w toku realizacji projektu, na każde wezwanie Zamawiającego, 2. Niezwłocznego informowania Zamawiającego o zaistniałych nieprawidłowościach i przeszkodach w terminowym realizowaniu zamówienia. 3. Realizacji i czynnego udziału w odbiorach przedmiotu zamówienia, w obecności osób wskazanych przez Zamawiającego. |
| WKW-2 | **Wymagania dla architekta rozwiązań storage:**   1. posiada minimum 5 letnie doświadczenie zawodowe w zakresie tworzenia architektury storage 2. b) posiada kwalifikacje eksperckie z obszaru dostarczonej architektury potwierdzone certyfikatem wydanym przez producenta oferowanego rozwiązania w oficjalnie dostępnej ścieżce certyfikacji. |
| WKW-4 | **Wymagania dla inżyniera świadczącego usługi instalacji oraz konfiguracji dostarczonego sprzętu serwerowego i macierzy**:   1. posiada minimum 5 letnie doświadczenie zawodowe w zakresie administracji środowiskiem serwerowym 2. posiada kwalifikacje eksperckie z obszaru dostarczonej architektury rozwiązania potwierdzone certyfikatem wydanym przez producenta oferowanego rozwiązania w oficjalnie dostępnej ścieżce certyfikacji. 3. posiada minimum 5 letnie doświadczenie zawodowe w zakresie instalacji oraz konfiguracji środowiska macierzowego i wirtualizacyjnego. |