**Zamawiający:**

Polskie Wydawnictwo Muzyczne

al. Krasińskiego 11a

31-111 Kraków

Zespół Zamówień Publicznych

Telefon: (+48) 12 422 70 44

Fax.: (+48) 12 422 01 74

e – mail: zamowienia\_publiczne@pwm.com.pl

**strona internetowa:** [www.pwm.com.pl](http://www.pwm.com.pl)

**Znak postępowania: ZZP.261.18.2024**

**SPECYFIKACJA WARUNKÓW ZAMÓWIENIA**

(SWZ)

**TRYB PODSTAWOWY BEZ NEGOCJACJI**

**prowadzony zgodnie z postanowieniami ustawy z dnia 11 września 2019 r.
Prawo zamówień publicznych ( tekst jedn. Dz.U. z 2024 r. poz. 1320)**

**na dostawy pn.:**

**„Rozbudowa środowiska backupowego w PWM”**

|  |  |
| --- | --- |
| **Oznaczenie Części** | **Nazwa Części** |
| **Część III** | **Opis przedmiotu zamówienia (OPZ)**  |

**Opis Przedmiotu Zamówienia**

* **Wymagania formalne**
1. Sprzęt oraz licencje muszą pochodzić z oficjalnego kanału dystrybucyjnego dla Polski. Zamawiający zastrzega sobie możliwość weryfikacji dostawy u producenta.
2. Wykonawca winien dokonać rejestracji sprzętu oraz licencji w serwisie producenta w imieniu Zamawiającego w terminie do 14 dni od daty dostawy potwierdzonej protokołem odbioru.
3. Zawarcia umowy i wystawienie faktury musi być zrealizowane nie później niż 30 grudnia 2024 r.
4. Zamawiający jest w posiadaniu oprogramowania Commvault o CCID 1005A3 oraz biblioteki Quantum Scalar i3 o numerze seryjnym FQL1941048. Wszystkie dostarczone licencje oraz komponenty winny być kompatybilne z oprogramowaniem i sprzętem posiadanym przez Zamawiającego.
5. Zamawiający w zakresie pkt 3 „Serwery” dopuszcza składanie ofert równoważnych. Każdy Wykonawca składający ofertę równoważną, zgodnie z postanowieniami ustawy PZP, jest obowiązany wykazać w treści przedkładanej przez siebie oferty, że oferowany przez niego przedmiot zamówienia spełnia konfiguracje, parametry techniczne i funkcjonalne oraz warunki wymagane określone w SWZ, bądź też przewiduje rozwiązania lepsze niż opisywane. Przez równoważność rozumie się to, że oferowane produkty muszą posiadać co najmniej te same konfiguracje, parametry techniczne i funkcjonalne oraz warunki wymagane na poziomie, co najmniej takim jak opisane w SWZ. Wykonawca zgodnie z przepisami ustawy PZP zobowiązany jest wykazać równoważność w treści składanej oferty. Przy oferowaniu rozwiązań innych niż opisane w SWZ, Wykonawca musi wykazać szczegółowo w treści oferty ich równoważność z warunkami i wymaganiami opisanymi w SWZ, przy czym zobowiązany jest dołączyć do oferty jego szczegółowe opisy przedstawiające konfiguracje, parametry techniczne i funkcjonalne oraz warunki pozwalające na ocenę zgodności oferowanych produktów z wymaganiami SWZ. W szczególności wymaga się od Wykonawcy podania nazwy producenta, nazwy oferowanego produktu oraz szczegółowego opisu jego konfiguracji, parametrów technicznych i funkcjonalnych oraz spełnienia wymaganych warunków (kompletne karty produktowe, prospekty, katalogi, foldery itp.).

W przypadku wskazania w zapisach SWZ, nazw własnych, typów, modeli, symboli, itp., należy zapisy te rozumieć jako zapisy, którym towarzyszy sformułowanie „lub równoważny”.

Zamawiający w zakresie pkt 1 „System Commvault” oraz pkt 2 „Biblioteka Quantum” nie dopuszcza oferowania produktów równoważnych, z uwagi na konieczność zachowania kompatybilności ze sprzętem i oprogramowaniem w posiadaniu Zamawiającego, jak również z uwagi na brak alternatywnego oprogramowania spełniającego wymagania Zamawiającego.

* **Wymagania techniczne**
1. **System Commvault**

Zamawiający wymaga przedłużenia wsparcia na 36 miesięcy dla aktualnej instalacji Commvault oraz rozbudowy istniejącego systemu kopii bezpieczeństwa Commvault CCID 1005A3 o poniższe licencje wraz ze wsparciem na 36 miesięcy:

|  |  |  |
| --- | --- | --- |
| Kod produktu | Nazwa/opis | Ilość |
| CV-BKRC-C-OI | Commvault Cloud Backup & Recovery Software (500GB Capped Operating Instance), Per Operating Instance | 5 |
| CV-BKRC-VM10 | Commvault Cloud Backup & Recovery Software for Virtual Machines, Per VM (10-Pack) | 3 |
| CV-BKRC-EP | Commvault Cloud Backup & Recovery Software for Endpoint Users, Per User | 10 |
| CV-BKRC-MB | Commvault Cloud Backup & Recovery Software for Mail and Cloud Applications, Per User | 10 |

Wymóg podstawowy: wszystkie dostarczone licencje muszą być kompatybilne z oprogramowaniem Commvault.

1. **Opis licencji dla serwerów fizycznych**
2. System musi wspierać backup (posiadać dedykowanego agenta backupowego) dla backupu zasobów plikowych, elementów systemu operacyjnego (np. System State dla systemów Windows) dla systemów operacyjnych klasy: Windows Server, Linux i Unix (minimum: AIX, Solaris, HP-UX)
3. System musi wspierać backup (posiadać dedykowanego agenta backupowego) dla backupu zasobów aplikacyjnych i bazodanowych (np. Oracle, Ms SQL, SAP) dla systemów operacyjnych klasy: Windows Server, Linux i Unix (minimum: AIX, Solaris, HP-UX)
4. Musi być możliwość składowania kopii backupowej na lokalnym (zarządzanym przez serwer) zasobie: dysk wewnętrzny, udział sieciowy, napęd taśmowy, VTL czy storage obiektowy
5. System musi pozwalać na zdalne i centralne zarządzanie komponentami backupowymi z konsoli administracyjnej o zakresie minimum:
	* Instalowanie agenta
	* Modyfikacje komponentów (dodanie modułu, odinstalowanie modułu)
	* Pełne odinstalowanie agenta
	* Monitorowanie logów backupowych z modułów backupowych
	* Zarządzanie ustawieniami komunikacyjnymi dla agenta
	* Restartem komponentów
	* Definiowaniem właściciela serwera dla celów tzw. private data a więc zabezpieczenia przed odtwarzaniem danych dla innych użytkowników
6. **Opis licencji dla maszyn wirtualnych:**
7. System musi wspierać backup całych maszyn wirtualnych/kontenerów dla czołowych rozwiązań wirtualizacyjnych, kontenerowych i chmurowych:
* Alibaba Cloud
* Amazon
* Citrix Xen
* Google Cloud Platform
* Huawei FusionCompute
* Microsoft Azure
* Microsoft Azure Stack Hub
* Microsoft Azure Stack HCI
* Microsoft Hyper-V
* Kubernetes
* Nutanix Acropolis Hypervisor (AHV)
* OpenStack
* Oracle Cloud Classic
* Oracle Cloud Infrastructure
* Oracle VM
* Red Hat OpenShift
* Red Hat Virtualization
* vCloud Director
* VMware

To znaczy musi posiadać dedykowany komponent do backupu minimum całej maszyny wirtualnej/kontenera/aplikacji/wolumenu bez konieczności instalowania agenta wewnątrz np. maszyny z możliwością granualnego odtwarzania pojedynczych plików.

1. Dla maszyn wirtualnych musi być możliwość zainstalowania agenta plikowego i bazodanowego dla zabezpieczenia zasobów z wewnątrz maszyny wirtualnej – funkcjonalność ta musi być zawarta dla wszystkich wymaganych wirtualizatorów i być w cenie rozwiązania.
2. Przy odtwarzaniu danych środowisk kontenerowych musi istnieć możliwość selekcji zasobów podlegającym odtworzeniu
3. Dla backupu i odtwarzania środowisk wirtualnych opartych o Vmware musi być możliwość wyboru różnych transportów: SAN, Hot-add, NBD, SSL, NAS - gdzie transport NAS pozwala na bezpośredni odczyt i zapis danych maszyny wirtualnej z urządzenia NAS
4. System musi zapewniać automatyczne wykrywanie i dodawanie do polityki backupu nowych maszyn wirtualnych.
5. System musi umożliwiać odzyskanie i uruchomienie maszyn wirtualnych z kopii zapasowej bez oczekiwania na pełne przywrócenie maszyny wirtualnej minimum dla Vmware i Hyper-V.
6. System musi umożliwiać konwertowanie maszyn wirtualnych pomiędzy wirtualizatorami, minimum:
	* Vmware do: Hyper-V, Azure, Amazon, Google Cloud Platform, Openstack, Oracle Cloud Infrastructure
	* Hyper-V do: Azure, Amazon, Vmware
	* Amazon do: Azure, Vmware
	* Azure do: Amazon, Hyper-V, Vmware

co oznacza, iż w przypadku odtwarzania zbackupowanej maszyny wirtualnej istnieje możliwość wybrania innego wirtualizatora jako miejsce odtwarzania i uruchomienia odtworzonej maszyny wirtualnej.

1. System musi wspierać mechanizm CBT (change block tracking) minimum dla Vmware i Hyper-V
2. System musi umożliwiać konwersję zbackupowanego serwera Windows i Linux do maszyny wirtualnej w środowisku:
	* Hyper-V
	* Vmware
3. Możliwość (jako opcja) synchronizacji maszyn wirtualnych Vmware do środowiska Amazon, Azure, Hyper-V, Vmware celem budowy rozwiązania DR (Disaster Recovery) z funkcjonalnościami:
	* Failover (planowane i niezaplanowane/awaryjne)
	* Failback
4. System (jako opcja) musi oferować rozbudowę o funkcjonalność przeszukiwania i analizy zasobów plikowych dla maszyn wirtualnych (minimum Vmware) całość działać związanych musi odbywać się na kopiach backupowych maszyn wirtualnych a nie na środowisku produkcyjnym
5. **Opis licencji dla stacji roboczych:**
6. System musi zapewniać backup laptopów i desktopów – funkcjonalność ta musi być w pełni zintegrowana z systemem (ta sama konsola, to samo repozytorium danych, ta sama deduplikacja, te same komponenty backupowe), i korzystać ze wspólnej domeny backupowej z innymi obszarami backupowymi jak: backup maszyn wirtualnych czy aplikacji i baz danych.
7. Portal samoobsługowy musi być dostępny poprzez dowolną przeglądarkę sieci Internet minimum: Edge, Chrome, Opera, Mozilla, Safari
8. Logowanie do portalu samoobsługowego za pomocą SSO (Single Sign-On) z wykorzystaniem SAML i AD
9. System musi umożliwiać backup laptopów czy desktopów z systemami Windows, Linux i Macintosh
10. Dostęp do danych zbackupowanych z laptopów czy desktopów musi być możliwy z urządzeń mobilnych poprzez dedykowanego klienta minimum dla IOS
11. Dla backupu laptopów i desktopów system backupowy musi oferować dedykowanego agenta, który pozwala skonfigurować zadanie backupowe tak by było wykonane w przedziale czasowym bez podawania konkretnej daty czy czasu jego uruchomienia, agent nie może tworzyć kopii danych na lokalnych zasobach stacji/laptopa.
12. System musi zapewniać współdzielenie plików pochodzących z backupu laptopów i desktopów z użytkownikami z domeny AD oraz z użytkownikami spoza domeny czy organizacji.
13. Każdy użytkownik desktopa czy laptopa musi posiadać możliwość (konsola samoobsługowa) zarządzania własnymi danymi, minimalna oczekiwana funkcjonalność to:
	* + Odtwarzanie własnych danych
		+ Uruchomienie backupu
		+ Wstrzymanie backupu
		+ Możliwość zdefiniowania innego okna backupowego
		+ Możliwość monitorowania postępu działania zadania
		+ Możliwość przeglądania danych z stacji roboczej czy laptopa poprzez dedykowanego klienta dla urządzeń mobilnych, a więc użytkownik posiadający jedynie urządzenie mobilne może nie tylko odczytywać dane z backupowej kopi, ale także udostępniać je innym użytkownikom
		+ Jeśli użytkownik jest poza siedzibą firmy - korzysta jedynie z dostępu do internetu do przeglądania danych zbackupowanych i ich odtwarzania czy udostępniania nie jest potrzebne żadne dodatkowe połączenie VPN
14. Zabezpieczenie przed kradzieżą: system musi posiadać możliwość zdalnego zaszyfrowania danych w przypadku kradzieży laptopa, to znaczy iż w przypadku utraty urządzenia administrator lub użytkownik włącza opcję szyfrującą i jeśli urządzenie pojawi się w sieci wtenczas automatycznie dane zostaną zaszyfrowane
15. Możliwość archiwizowania danych plikowych na stacji roboczej: jeśli dane pliki spełniają kryteria archiwizacyjne to dany pliki zostaje skasowany albo zamieniony na skrót (stub)
16. Zabezpieczenie przed wyciekiem danych: system musi oferować mechanizm zabezpieczający dane przed odtwarzaniem jeśli wykonuje je ktoś inny niż właściciel, tak więc administrator systemu backupowego pomimo swoich uprawnień może rekonfigurować ustawienia, monitorować działanie agenta ale nie może uruchomić procesu odtwarzania gdyż nie jest właścicielem laptopa czy desktopa
17. Możliwość (jako opcja) włączenie pełnokontekstowego indeksowania danych backupowanych z stacji roboczych celem wyszukiwania danych wrażliwych.
18. **Opis licencji dla pakietów oprogramowania biurowego:**
19. System musi mieć możliwość backupu i odtwarzania (jako opcja) dedykowanym agentem dokumentów i maili dla Office 365 z:
	* SharePoint Online: Dokumenty, Site i subsite, Projekty PWA, Biblioteki, Listy, strony, uprawnienia, fora, wersje, szablony, ustawienia i widoki
	* Exchange Online: Wiadomości, Kalendarze, Kontakty, Zadania, Skrzynki (primary, Archive, Group, Shared, Public folder, Team)
	* OneDrive: Pliki, Foldery, Konta, Pliki OneNote, Pliki współdzielone w chatach prywatnych
* Teams: prywatne, publiczne, org-wide, Kanały: regularne, prywatne, współdzielone, posty, zakładki, Zakładki: posty, pliki, wiki, strony, Posty: konwersacje, odpowiedzi, Pliki kanałów oraz OneNote, Ruch pocztowy SMTP
1. System musi mieć możliwość pełnokontekstowego indeksowania i wyszukiwania treści (eDiscovery i Compliance Search) z danych backupowanych z:
* Skrzynek pocztowych (Exchange onpremis)
* Skrzynek journalingowych (Exchange onpremis)
* Ruchu pocztowego SMTP
* Exchange Online
* SharePoint Online
1. **Biblioteka Quantum**
2. Zamawiający wymaga odnowienia wsparcia dla aktualnego systemu na 36 miesięcy oraz rozbudowy istniejącego systemu kopii bezpieczeństwa Quantum Scalar i3 o numerze seryjnym FQL1941048 o poniższe elementy fizyczne, licencje i wsparcie serwisowe na 36 miesięcy:

|  |  |  |
| --- | --- | --- |
| Kod produktu | Nazwa/opis | Ilość |
| LSC33-ATDX-L8NA | Quantum Scalar i3 IBM LTO-8 Tape Drive Module, Half Height, 6Gb SAS, Single mini-SAS-HD 8644 Port | 1 |
| LSC33-ALAV-001A | Quantum Scalar i3 Active Vault License | 1 |
| LSC33-ALSE-001A | Quantum Scalar i3 25-Slot Capacity on Demand Upgrade License | 3 |
| MR-L8MQN-BC | Quantum data cartridge, LTO Ultrium 8 (LTO-8), pre-labeled.  | 100 |
| MR-LUCQN-BC | Quantum cleaning cartridge, LTO Ultrium Universal, pre-labeled.  | 4 |
| SSC33-RLSE-CB11-S4E | Quantum Scalar i3, 25-Slot Upgrade; Support Plan, Bronze (5x9xNBD CRU); annual, zone 1 | 9 |
| SSC33-RTDX-CB11-S4E | Quantum Scalar i3 Library, Tape Drive Module, Half Height; Support Plan, Bronze (5x9xNBD CRU); annual, zone 1 | 3 |
| SSC33-RSC0-CB11-S4E | Quantum Scalar i3 Library, 3U Control Module, 25 licensed slots, no tape drives; Support Plan, Bronze (5x9xNBD CRU); Uplift/Renewal, zone 1 | 1 |
| SSC33-RTDX-CB11-S4E | Quantum Scalar i3 Library, Tape Drive Module, Half Height; Support Plan, Bronze (5x9xNBD CRU); Uplift/Renewal, zone 1 | 2 |

1. Rozbudowa wymaga dostarczenia:
2. Napędu taśmowego klasy LTO-8 połowy wysokości z interfejsem SAS 6GbE,
3. Fizycznego modułu rozszerzeń 3U ze 50 slotami na taśmy oraz 3 miejscami na napędy taśmowe,
4. Dodatkowej licencji na 75 slotów aktywnych,
5. Licencji na Active Vault zabezpieczającej środowisko przed ransomware,
6. 100 nośników taśmowych klasy LTO8 wielokrotnego zapisu,
7. 4 nośniki taśmowe z funkcją czyszczenia napędu.
8. **Serwery – 2 sztuki**

|  |  |
| --- | --- |
| **Nazwa elementu, parametru lub cechy** | **Opis wymagań Serwerów** |
| **Obudowa** | Do instalacji w szafie Rack 19", wysokość nie więcej niż 2U, z zestawem szyn do mocowania w szafie i wysuwania do celów serwisowych. Zainstalowane ramię do zarządzania kablami.  |
| **Procesor** | Architektura x86, maksymalny TDP dla procesora – maksymalnie 150W. Wymagana ilość rdzeni dla procesora – 12. Minimalna częstotliwość pracy procesora 2.4GHz. Minimalna ilość kanałów procesora – 8. Ilość kości pamięci na kanał – 2. Wynik wydajności procesora dla proponowanego serwera nie powinien być niższy niż 240 punkty base w teście SPECrate 2017 Integer, opublikowanym przez SPEC.org (www.spec.org) dla konfiguracji dwuprocesorowej. |
| **Liczba procesorów**  | 1 |
| **Płyta główna** | Płyta główna dedykowana do pracy w serwerach, wyprodukowana przez producenta serwera z możliwością zainstalowania minimum dwóch procesorów wykonujących 64-bitowe instrukcje  |
| **Pamięć operacyjna** | Zainstalowane minimum 128GB pamięci RAM o częstotliwości 4800MHz. Pamięć zainstalowana w kościach min 32Gb.  |
| Minimum 32 sloty na pamięć. Możliwość rozbudowy do 8TB RAM.  |
| **Zabezpieczenie pamięci** | ECC, SDDC, ADDDC, Memory Mirroring  |
| **Procesor Graficzny** | Zintegrowana karta graficzna z minimum 16MB pamięci osiągająca rozdzielczość min. 1920x1200 przy 60 Hz. |
| 1 port VGA na tylnym panelu. Możliwość zainstalowania drugiego portu VGA na przednim panelu serwera.  |
| **Rozbudowa dysków** | W chwili dostawy serwer musi posiadać zainstalowane  |
| ·         Min. siedemnaście dysków NL SAS 3,5” o pojemności min. 14TB każdy  |
| ·         Min. trzy dyski SSD 3,5” o pojemności minimum 1.9TB każdy. Parametr DWDP dysku nie mniej niż 4.  |
| Serwer w momencie dostawy musi posiadać możliwość zainstalowania minimum 20 dysków 3,5” SAS / SATA |
| Wymagana możliwość instalacji minimum dysków M.2 zabezpieczonych sprzętowym RAID. Nie dopuszcza się rozwiązania, w którym dyski M.2 zajmują którykolwiek ze slotów PCIe. |
| Wymagany jest wewnętrzny slot na kartę Micro SD.  |
| **Kontroler dyskowy** | Zainstalowany sprzętowy kontroler SAS 12Gb który będzie miał możliwość obsługi wszystkich 20 zatok dyskowych. Dopuszcza się wykorzystanie kontrolera wraz z expanderem SAS. Kontroler musi posiadać 4GB pamięci Flash. Kontroler musi obsługiwać poziomy RAID - 0/1/10/5/50/6/60. |
| Zainstalowana jedna dwuportowa karta HBA SAS 12Gb ze złączami SFF-8644. Do karty dołączone dwa 2 metrowe kable SAS o złączach SFF8644 – SFF8644 |
| **Zasilacz** | Minimum dwa redundantne zasilacze o mocy minimum 1100W z certyfikatem minimum Titanium.  |
| **Interfejsy sieciowe** | Zainstalowane dwuportowa karta 10/25Gb SFP28 wraz z dedykowanymi wkładkami SFP+ SR 10Gb. Karta nie może zajmować żadnego ze slotów PCIe.  |
| **Dodatkowe sloty I/O** | Serwer w momencie dostawy musi posiadać 2 sloty PCIe 4.0 x16. |
| Serwer musi posiadać jeden slot OCP 3.0 na potrzeby instalcji karty sieciowej.  |
| **Dodatkowe porty** | ·   z przodu obudowy: 1x USB 3.2, 1x USB 2.0 (z możliwością zarządzania serwerem), możliwość instalacji portu VGA |
| ·   z tyłu obudowy: 3x USB 3.2, 1x VGA, 1x RJ-45 do zarządzania serwerem. Możliwość instalacji portu DB9.  |
| ·   wewnątrz obudowy: 1x USB 3.2 |
| Wszystkie tylne porty USB, port RJ-45 służący do zarządzania, tylny port VGA, wewnętrzny port USB, wewnętrzny port na kartę Micro SD powinny być umieszczone na osobnej dedykowanej płytce I/O, którą łączy się bezpośrednio z płytą główną serwera. |
| Możliwość instalacji dodatkowego redundantnego portu RJ45 służącego do zarządzania, w slocie OCP zamiast karty sieciowej.  |
| **Chłodzenie** | Wentylatory wspierające wymianę Hot-Swap, zamontowane nadmiarowo minimum N+1 |
| **Zarządzanie** | Wymagany wbudowany sprzętowy kontroler zdalnego zarządzania, który musi być umieszczony na osobnej dedykowanej płytce I/O (wspomnianej w sekcji Dodatkowe Porty). Płytka I/O musi posiadać swój własny min. 2 rdzeniowy procesor o taktowaniu min. 1.2GHz.  |
| · Monitoring stanu systemu (komponenty objęte monitoringiem to przynajmniej: CPU, pamięć RAM, dyski, karty PCI, zasilacze, wentylatory, płyta główna |
| · Pozyskanie następujących informacji o serwerze: nazwa, typ i model, numer seryjny, nazwa systemu, wersja UEFI oraz BMC, adres ip karty zarządzającej, utylizacja cpu, utylizacja pamięci oraz komponentów I/O, lokalizacja |
| · Logowanie zdarzeń systemowych oraz związanych z działaniami użytkownika. Każdy dziennik zdarzeń powinien mieć możliwość zapisu co najmniej 1024 rekordów.  |
| · Logowanie zdarzeń związanych z utrzymaniem systemu jak upgrade firmware, zmiana/instalacja sprzętu. System powinien umożliwiać zapisanie minimum 250 zdarzeń. |
| · Wysyłanie określonych zdarzeń poprzez SMTP oraz SNMPv3 |
| · Update systemowego firmware |
| · Monitoring i możliwość ograniczenia poboru prądu |
| · Zdalne włączanie/wyłączanie/restart  |
| · Zapis video zdalnych sesji |
| · Podmontowanie lokalnych mediów z wykorzystaniem Java Client |
| · Przekierowanie konsoli szeregowej przez IPMI |
| · Zrzut ekranu w momencie zawieszenia systemu |
| · Możliwość przejęcia zdalnego ekranu  |
| · Możliwość zdalnej instalacji systemu operacyjnego |
| · Alerty Syslog |
| · Przekierowanie konsoli szeregowej przez SSH |
| · Wyświetlanie danych aktualnych I historycznych dla użycia energii oraz temperatury serwera  |
| · Możliwość mapowania obrazów ISO z lokalnego dysku operatora |
| · Możliwość mapowania obrazów ISO przez HTTPS, SFTP, CIFS oraz NFS |
| · Możliwość jednoczesnej pracy do 6 użytkowników przez wirtualną konsolę |
| · wspierane protokoły/interfejsy: IPMI v2.0, SNMP v3, CIM, DCMI v1.5, REST API |
| · Wymaga się możliwości wykorzystania frontowego portu USB do celów serwisowych (komunikacja portu z karta zarządzającą) bez możliwości uzyskania jakiejkolwiek funkcjonalności na poziomie zainstalowanego systemu operacyjnego. Funkcjonalność ta musi być realizowana na poziomie sprzętowym i musi być niezależna od zainstalowanego systemu operacyjnego. |
| · Kontroler zarządzania musi posiadać 4Gb wewnętrznej pamięci (dopuszcza się zastosowanie karty Micro SD w celu uzyskania tej pojemności). Pamięć kontrolera zarządzania musi pełnić funkcję RDOC (Remote Disc on Card) oraz musi umożliwiać przechowywanie plików firmware. |
| · Monitorowanie zmian sprzętowych w celu wykrycia nieoczekiwanych zmian. Po wykryciu zmiany zapis w logu serwera lub uniemożliwienie boot’u.  |
| · Możliwość synchronizacji konfiguracji i poziomów firmware pomiędzy serwerami.  |
| · Możliwość monitorowania i zarządzania grupą serwerów z poziomu kontrolera zarządzania pojedynczego serwera. Ilość serwerów możliwych do zarządzania – minimum 200.  |
| Wraz z serwerem powinno zostać dostarczone dodatkowe oprogramowanie zarządzające umożliwiające: |
| - zarządzanie infrastrukturą serwerów i storage bez udziału dedykowanego agenta |
| - przedstawianie graficznej reprezentacji zarządzanych urządzeń |
| - możliwość skalowania do minimum 1000 urządzeń |
| - obsługę szyfrowanej komunikacji z zarządzanymi urządzeniami, wsparcie dla NIST 800-131A oraz FIPS 140-2 |
| - wsparcie dla certyfikatów SSL tzw. self-signed oraz zewnętrznych |
| - udostępnianie szybkiego podgląd stanu środowiska |
| - udostępnianie podsumowania stanu dla każdego urządzenia |
| - tworzenie alertów przy zmianie stanu urządzenia |
| - monitorowanie oraz tracking zużycia energii przez monitorowane urządzenie, możliwość ustalania granicy zużycia energii, |
| - konsola zarzadzania oparta o HTML 5 |
| - dostępność konsoli monitorującej na urządzeniach przenośnych ze wsparciem dla systemu Android oraz iOS, aplikacja musi umożliwiać włączenie wyłączenie oraz restart urządzenia, musi również mieć możliwość aktywowania diody lokacyjnej na urządzeniu, |
| - automatyczne wykrywanie dołączanych systemów oraz szczegółowa inwentaryzacja |
| - możliwość podnoszenia wersji oprogramowania dla komponentów zarządzanych serwerów w oparciu o repozytorium lokalne jak i zdalne dostępne na stronie producenta oferowanego rozwiązania |
| - definiowanie polityk zgodności wersji firmware komponentów zarządzanych urządzań |
| - definiowanie roli użytkowników oprogramowania  |
| - obsługa REST API oraz Windows PowerShell |
| - obsługa SNMP, SYSLOG, Email Forwarding |
| - autentykacja użytkowników: centralna (możliwość definiowania wymaganego poziomu skomplikowania danych autentykacyjnych) oraz integracja z MS AD oraz obsługa single sign on oraz SAML |
| - obsługa tzw Forward Secrecy w komunikacji z zarządzanymi urządzeniami |
| - przedstawianie historycznych aktywności użytkowników |
| -blokowanie możliwości podłączenia innego systemu zarzadzania do urządzeń zarządzanych  |
| - tworzenie dziennika zdarzeń ukończonych sukcesem lub bledem,  oraz zdarzeń będących w trakcie. Możliwość definiowania filtrów wyświetlanych zdarzeń z dziennika. Możliwość eksportu dziennika zdarzeń do pliku csv |
| - Obsługa NTP |
| - przesyłanie alertów do konsoli firm trzecich |
| - tworzenie wzorców konfiguracji zarządzanych urządzeń (definiowanie przez konsole albo kopiowanie konfiguracji z już zaimplementowanych urządzeń)  |
| - instalowanie systemów operacyjnych oraz wirtualizatorów Vmware i Hyper-V. Wymagana jest integracja konsoli zarządzania z konsolą wirtualizatora tak, aby zarządzanie środowiskiem sprzętowym mogło odbywać się z konsoli wirtualizatora. Wymaga się możliwości instalacji systemu na przynajmniej 20 nod’ach jednocześnie |
| - możliwość automatycznego tworzenia zgłoszeń w centrum serwisowym producenta dla określonych zdarzeń wraz z przesyłem plików diagnostycznych, |
| Producent serwera ponadto powinien mieć w swojej ofercie narzędzia integrujące zarządzanie infrastrukturą z następującymi produktami: VMware vCenter, Microsoft AdminCenter, Microsoft SystemCenter, RedHat CloudForms, Splunk. |
| **Urządzenia hot swap** | Dyski twarde, zasilacze, wentylatory. |
| **Funkcje zabezpieczeń** | Możliwość instalacji czujnika otwarcia obudowy zintegrowanego z modułem zarządzania serwerem, hasło włączania, hasło administratora, moduł RoT (umieszczony na dedykowanej płytce I/O wspomnianej w sekcji Dodatkowe porty) wspierający TPM2.0 oraz Platform Firmware Resiliency (PFR)., Możliwość zainstalowania przedniego panelu zamykanego na klucz. |
| **Diagnostyka** | Możliwość przewidywania awarii dla procesorów, regulatorów napięcia, pamięci, dysków wewnętrznych, wentylatorów, zasilaczy, kontrolerów RAID |
| Możliwość użycia aplikacji mobilnej na telefonie, do przeglądania awarii, konfiguracji i włączenia/wyłączenia serwera. |
| **Systemy operacyjne** | Wspierane systemy operacyjne: Microsoft Windows Server 2019, 2022; Red Hat Enterprise Linux 8.6, 8.7, 9.0, 9.1, SUSE Linux Enterprise Server 15 SP4 oraz 15 Xen SP4; VMware vSphere (ESXi) 7.0 U3, ESXI 8.0; Ubuntu 22.04 LTS |
| **Waga** | maximum: 40 kg |
| **Gwarancja** | Serwery powinny posiadać min. 36 miesięcy gwarancji producenta on-site z czasem reakcji NBD. W przypadku braku funkcjonalności przewidywania awarii dla wszystkich komponentów wymienionych w punkcie Diagnostyka wymagane jest dostarczenie serwera nadmiarowego, mogącego zastąpić funkcjonalni jak i wydajnościowo wymagane powyżej maszyny. Wszystkie komponenty serwerów powinny być sygnowane i zoptymalizowane do użycia przez producenta serwerów. |

1. **Usługa instalacji i wdrożenia:**

Usługa musi być wykonana przez osobę/-y posiadającą/-e certyfikaty:

1. Commvault Expert/Master
2. Scalar i3/i6 Training Assessment
3. Scalar i3 and Scalar i6 Break/Fix

Przewidywany minimalny zakres wdrożenia:

1. Instalacja fizyczna serwerów w obu lokalizacjach wraz z okablowaniem, aktualizacja FW, adresacja modułów zarządzania
2. Provisionowanie serwerów fizycznych (grupy RAID, system operacyjny plus hardening)
3. Rozbudowa fizyczna istniejącej biblioteki fizycznej o napędy taśmowe, moduł rozszerzeń, aktualizacja FW,
4. Provisionowanie biblioteki taśmowej (rozszerzenie partycji, stworzenie active vault)
5. Konfiguracja sieci LAN w zakresie:
	1. JumboFrame
	2. LAGów dla wybranych połączeń
6. Uruchomienie roli Commserve Primary oraz StandBy
	1. Instalacja oraz hardening OS
	2. Instalacja oprogramowania Commvault/MS SQL wraz z hardeningiem
	3. Definicja klastra Commserve Standby
	4. Uruchomienie 2FA oraz Authorization Workflows
	5. Konfiguracja Software Cache
	6. Konfiguracja powiadomień i raportowania
7. Uruchomienie roli MediaAgent/VSA/FS Proxy
	1. Instalacja oraz hardening OS
	2. Instalacja oprogramowania Media Agent
	3. Definicja pool deduplikacyjnych
	4. Definicja pool taśmowych
	5. Definicja indeksów
8. Konsultacja z Zamawiającym oraz wykreowanie Storage/Schedule Policy (Plany) dla pool deduplikacyjnych
9. Konsultacja z Zamawiającym oraz wykreowanie Storage/Schedule Policy (Plany) dla pool taśmowych
10. Poprawne wykonanie pełnych backupów wszystkich Klientów
11. Testy odtworzeniowe:
	1. VMware: wykonanie testów odtwarzania: in-place, out-of-place, pojedynczy dysk, pojedyncze pliki wewnątrz VM, uruchomienie VM bezpośrednio z backupu
	2. HyperV: wykonanie testów odtwarzania: in-place, out-of-place, pojedynczy dysk
	3. Pliki: wykonanie testów odtwarzania: in-place, out-of-place, pojedynczy dysk
12. Wykonanie dokumentacji powdrożeniowej zawierającej wykaz wykonanych prac i ustawionych parametrów pracy urządzeń oraz uwzględniającej architekturę, opis, schematy konfiguracji wdrożonych rozwiązań.
13. Wykonanie przełączenia między site dla roli Commserve, sprawdzenie poprawności polityk, backupów oraz odtwarzania.