ZP.272.00030.2024
Załącznik nr 3.1

Opis przedmiotu zamówienia:

1. **Serwer typ 1 wraz z systemem operacyjnym – 2 szt.**

Lp.	Nazwa elementu, parametru lub cechy	Opis wymagań serwera typ 1
1	**Obudowa**	Do instalacji w szafie Rack 19", wysokość nie więcej niż 1U, z zestawem szyn do mocowania w szafie i wysuwania do celów serwisowych oraz ramieniem do zarządzania kablami.
2	**Procesor**	Architektura x86, maksymalny TDP dla procesora – maksymalnie 150W. Wymagana liczba rdzeni dla procesora – 10. Minimalna częstotliwość pracy procesora minimum 2.7GHz. Minimalna liczba kanałów procesora – 8. Wynik wydajności procesora zainstalowanego w oferowanym serwerze nie powinien być niższy niż 211 punktów base w teście *SPECrate 2017 Integer*, opublikowanym przez SPEC.org (www.spec.org) dla konfiguracji dwuprocesorowej. Test przeprowadzony przez producenta serwera musi być zamieszczony na stronie spec.org.
3	**Liczba procesorów**	1.
4	**Płyta główna**	Płyta główna dedykowana do pracy w serwerach, wyprodukowana przez producenta serwera, z możliwością zainstalowania przynajmniej dwóch procesorów wykonujących 64-bitowe instrukcje.
5	**Pamięć operacyjna**	Zainstalowane minimum 32GB pamięci RAM DDR5 o częstotliwości 4800MHz. Pamięć zainstalowana w 2 kościach. Minimum 32 sloty na pamięć. Możliwość rozbudowy do 8TB RAM.
6	**Zabezpieczenie pamięci**	Mirroring, ECC, SDDC, ADDDC.
7	**Procesor graficzny**	Zintegrowana karta graficzna z minimum 16MB pamięci, osiągająca rozdzielczość 1920x1200 przy 60Hz. 1 port VGA na tylnym panelu oraz możliwość instalacji portu VGA na przednim panelu serwera.
8	**Rozbudowa dysków**	W chwili dostawy każdy serwer musi posiadać zainstalowane minimum 2 dyski NVMe, o pojemności nie mniejszej niż 800GB 2,5”, DWPD min. 2.9, hot swap, oraz 2 dyski SSD SATA 480GB RI, hot swap. Obudowa ma mieć możliwość instalacji do 12 dysków 2.5. W chwili dostawy wymagana jest obecność łącznie 10 zatok 2,5 z obsługą SAS/SATA, NVMe”, z czego 6 zatok wolnych.
9	**Kontroler dyskowy**	Wymagana obecność w serwerze kontrolera RAID – z co najmniej 4GB pamięci cache z ochroną niezapisanych danych typu flash, obsługą poziomów RAID 0, 1, 10, 5, 50, 6, 60 i możliwością podłączenia min. 8 dysków – obsługującego zainstalowane dyski SATA oraz dyski NVMe jednocześnie.
10	**Zasilacz**	Minimum dwa redundantne zasilacze o mocy minimum 750W z certyfikatem minimum Titanium.
11	**Interfejsy sieciowe**	Jeden port RJ-45 o przepustowości 1GbE dedykowany dla karty zarządzającej. Co najmniej 1 karta dwuportowa 10Gbase-T.
12	**Dodatkowe sloty I/O**	Obudowa z obsługą co najmniej trzech PCIe Gen 5 i do 3 kart GPU. Dodatkowy port na kartę OCP. W momencie dostawy serwer wyposażony w minimum 2 sloty PCIe Gen 4 x16.
13	**Karty graficzne**	Możliwość jednoczesnej obsługi do 3 sztuk kart GPU pojedynczej szerokości.
14	**Dodatkowe porty**	• Z przodu obudowy: 1x USB 3.2, 1x USB 2.0 (możliwość lokalnego zarządzania serwerem przez ten port). • Z tyłu obudowy: 3x USB 3.2, 1x VGA. Możliwość instalacji portu DB9. Możliwość instalacji drugiego redundantnego dedykowanego portu zarządzania. • Wewnątrz obudowy: 1x USB3.2.

		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.
15	**Chłodzenie**	Wentylatory wspierające wymianę Hot-Swap, zamontowane nadmiarowo minimum N+1.
16	**Zarządzanie**	Niezależny od systemu operacyjnego, posiadający dedykowany port 1Gbs base-T sprzętowy kontroler zdalnego zarzadzania, wyposażony w przynajmniej 4GB pamięci flash na potrzeby przechowywania oraz instalacji firmware komponentów serwera jak i plików konfiguracyjnych. Na potrzeby utrzymaniowe oraz serwisowe wymaga się, aby kontroler zarządzania nie był integralną częścią płyty głównej serwera, lecz był na osobnej płytce I/O wspomnianej w sekcji Dodatkowe Porty. W przypadku awarii płyty głównej serwera wymaga się możliwości instalacji wykorzystywanej płytki I/O wraz z pamięcią flash (wersje firmware oraz pliki konfiguracyjne) na nowej płycie głównej. Wymaga się możliwości skonfigurowania w serwerze dwóch fizycznych portów 1Gb Base-T dedykowanych tylko na potrzeby zarządzania. Nie dopuszcza się rozwiązania, w którym którykolwiek z dwóch portów miałby być portem współdzielonym na karcie LAN. Wymagane funkcjonalności procesora serwisowego: • 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. • 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. • Możliwość zapisywania zdarzeń w formacie HTML oraz JSON. • 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. • Przekierowanie konsoli szeregowej przez IPMI oraz SSH. • Zrzut ekranu w momencie zawieszenia systemu. • Możliwość przejęcia zdalnego ekranu. • Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera niezależne od zainstalowanego systemu operacyjnego. • Możliwość zdalnej instalacji systemu operacyjnego. • Alerty Syslog. • Szyfrowane połączenie (TLS min. TLS 1.2) oraz autentykacja i autoryzacja użytkownika. • Możliwość zdefiniowania min. 12 użytkowników lokalnych na karcie zarządzającej. • Wyświetlanie danych aktualnych oraz 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. • Montowanie obrazów ISO musi być możliwe bez instalacji dodatkowych komponentów Java czy AciveX . • Możliwość jednoczesnej pracy do 6 użytkowników przez wirtualną konsolę. • Wspierane protokoły/interfejsy: IPMI v2.0, SNMP v3, CIM, DCMI v1.5, REST API. • Zgodność z FIPS 140-3 oraz NIST 800-193. • Zabezpieczenie przed nieautoryzowaną wymianą komponentów sprzętowych serwera. Wymaga się możliwości ustawienia zablokowania startu systemu na skutek wykrycia takiego zdarzenia. • Możliwość grupowania serwerów w kontekście synchronizacji jednolitej konfiguracji oraz wersji firmware dla całej grupy serwerów. • Wymaga się możliwości wykorzystania frontowego portu USB do celów serwisowych (komunikacja portu z kartą 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.
17	**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. Wymagana obecność przedniego panelu zabezpieczającego zamykanego na klucz.
18	**Urządzenia hot swap**	Dyski twarde, zasilacze, wentylatory.
19	**Diagnostyka**	Możliwość przewidywania awarii dla procesorów, regulatorów napięcia, pamięci, dysków wewnętrznych (włącznie z dyskami m.2), wentylatorów, zasilaczy, kontrolerów RAID. Możliwość użycia aplikacji mobilnej na telefonie do przeglądania awarii, konfiguracji i włączenia/wyłączenia serwera. Wymaga się, aby serwer posiadał diody sygnalizujące awarię przy każdej kości pamięci RAM, każdej zatoce dyskowej, każdym zasilaczu.
20	**Systemy operacyjne**	Wsparcie dla systemu operacyjnego Red Hat Enterprise Linux 8.9, 9.1, 9.2, 9.3. **Wraz z serwerem należy dostarczyć komplet licencji Red Hat Enterprise Linux pozwalających prawidłowo zalicencjonować procesor zaoferowany w ramach oferowanego serwera.**
21	**Gwarancja**	5 lat gwarancji producenta świadczonej w reżimie 9/5, on-site, z czasem odpowiedzi – nastepny dzień roboczy. Usługi wsparcia serwisowego świadczone bezpośrednio przez producenta sprzętu. Możliwość zgłaszania awarii w języku polskim poprzez ogólnopolską linię telefoniczną producenta. Możliwość pobierania nowych wersji firmware'ów oraz sterowników do wszystkich składowych serwera bezpośrednio ze strony producenta serwera.
22	**Dodatkowa funkcjonalność**	**Dostarczone serwery wspierane przez posiadane przez Zamawiającego oprogramowanie xClarity Administrator. Zamawiający wymaga dostarczenia wraz z serwerami odpowiedniego zestawu licencji do ww. oprogramowania, z okresem wsparcia równym okresowi wsparcia na dostarczone serwery.** **Zamawiający wymaga potwierdzenia producenta oprogramowania xClarity Administrator o zgodności oferowanych serwerów z ww. oprogramowaniem.**

2. Serwer typ 2 wraz z systemem operacyjnym – 2 szt.

Lp.	Nazwa elementu, parametru lub cechy	Opis wymagań Serwera typ 2
1	**Obudowa**	Do instalacji w szafie Rack 19", wysokość 2U, z zestawem szyn do mocowania w szafie i wysuwania do celów serwisowych oraz ramieniem do zarządzania kablami.
2	**Procesor**	Architektura x86, maksymalny TDP dla procesora – maksymalnie 150W. Wymagana liczba rdzeni dla procesora – 10. Minimalna częstotliwość pracy procesora minimum 2.7GHz. Minimalna liczba kanałów procesora – 8. Wynik wydajności procesora zainstalowanego w oferowanym serwerze nie powinien być niższy niż 211 punktów base w teście SPECrate 2017 Integer opublikowanym przez SPEC.org (www.spec.org) dla konfiguracji dwuprocesorowej. Test przeprowadzony przez producenta serwera musi być zamieszczony na stronie spec.org.
3	**Liczba procesorów**	2.
4	**Płyta główna**	Płyta główna dedykowana do pracy w serwerach, wyprodukowana przez producenta serwera z możliwością zainstalowania przynajmniej dwóch procesorów wykonujących 64-bitowe instrukcje.
5	**Pamięć operacyjna**	Zainstalowane minimum 128GB pamięci RAM DDR5 o częstotliwości 4800MHz. Pamięć zainstalowana w 4 kościach. Minimum 32 sloty na pamięć. Możliwość rozbudowy do 8TB RAM.
6	**Zabezpieczenie pamięci**	Mirroring, ECC, SDDC, ADDDC.
7	**Procesor graficzny**	Zintegrowana karta graficzna z minimum 16MB pamięci, osiągająca rozdzielczość 1920x1200 przy 60 Hz. 1 port VGA na tylnym panelu oraz możliwość instalacji portu VGA na przednim panelu serwera.
8	**Rozbudowa dysków**	W chwili dostawy każdy serwer musi posiadać zainstalowane minimum 2 dyski NVMe, o pojemności nie mniejszej niż 1,6TB 2,5", DWPD min. 3, hot swap, oraz 2 dyski SSD SATA 480GB RI, hot swap. Obudowa ma mieć możliwość instalacji do 12 dysków 2.5. W chwili dostawy wymagana jest obecność łącznie 8 zatok 2,5 z obsługą SAS/SATA, NVMe, z czego 4 zatok wolnych. Wymagana możliwość instalacji minimum dwóch dysków M.2 SATA lub NVMe, zabezpieczonych sprzętowym RAID, przy czym ustawienie sprzętowego RAID powinno być możliwe zarówno dla dysków SATA jak i NVMe. Wymaga się możliwości ustawienia programowego (bez użycia sprzętowego kontrolera) mechanizmu RAID na dyskach M.2 NVMe oraz SATA. Wymagany jest wewnętrzny slot na kartę Micro SD.
9	**Kontroler dyskowy**	Wymagana obecność w serwerze kontrolera RAID – z co najmniej 4GB pamięci cache z ochroną niezapisanych danych typu flash, obsługą poziomów RAID 0, 1, 10, 5, 50, 6, 60 i możliwością podłączenia min. 8 dysków – obsługującego zainstalowane dyski SATA oraz dyski NVMe jednocześnie.
10	**Zasilacz**	Minimum dwa redundantne zasilacze o mocy minimum 750W z certyfikatem minimum Titanium.
11	**Interfejsy sieciowe**	Jeden port RJ-45 o przepustowości 1GbE dedykowany dla karty zarządzającej. Co najmniej 1 karta dwuportowa 10Gbase-T. Zainstalowane co najmniej trzy dwuportowe karty FC o prędkości przynajmniej 16Gbs, wyposażone w dedykowane wkładki SFP.
12	**Dodatkowe sloty I/O**	W chwili dostawy serwer powinien być wyposażony min. w 8 slotów PCIe 4, w tym min. dwa x16, bez konieczności dokładania jakichkolwiek dodatkowych komponentów do serwera.
13	**Karty graficzne**	Możliwość jednoczesnej obsługi do 8 sztuk kart GPU pojedynczej szerokości oraz do minimum 3 kart podwójnej szerokości.
14	**Dodatkowe porty**	• Z przodu obudowy: 1x USB 3.2, 1x USB 2.0 (możliwość lokalnego zarządzania serwerem przez ten port).

		• Z tyłu obudowy: 3x USB 3.2, 1x VGA. Możliwość instalacji portu DB9. Możliwość instalacji drugiego redundantnego dedykowanego portu zarządzania. • Wewnątrz obudowy: 1x USB3.2. 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.
15	**Chłodzenie**	Wentylatory wspierające wymianę Hot-Swap, zamontowane nadmiarowo minimum N+1.
16	**Zarządzanie**	Niezależny od systemu operacyjnego, posiadający dedykowany port 1Gbs base-T, sprzętowy kontroler zdalnego zarzadzania, wyposażony w przynajmniej 4GB pamięci flash na potrzeby przechowywania oraz instalacji firmware komponentów serwera jak i plików konfiguracyjnych. Na potrzeby utrzymaniowe oraz serwisowe wymaga się, aby kontroler zarządzania nie był integralną częścią płyty głównej serwera, lecz był na osobnej płytce I/O, wspomnianej w sekcji Dodatkowe Porty. W przypadku awarii płyty głównej serwera, wymaga się możliwości instalacji wykorzystywanej płytki I/O wraz z pamięcią flash (wersje firmware oraz pliki konfiguracyjne) na nowe płycie głównej. Wymaga się możliwości skonfigurowania w serwerze dwóch fizycznych portów 1Gb Base-T dedykowanych tylko na potrzeby zarządzania. Nie dopuszcza się rozwiązania, w którym którykolwiek z dwóch portów miałby być portem współdzielonym na karcie LAN. Wymagane funkcjonalności procesora serwisowego: • 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. • 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. • Możliwość zapisywania zdarzeń w formacie HTML oraz JSON. • 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. • Przekierowanie konsoli szeregowej przez IPMI oraz SSH. • Zrzut ekranu w momencie zawieszenia systemu. • Możliwość przejęcia zdalnego ekranu. • Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera niezależne od zainstalowanego systemu operacyjnego. • Możliwość zdalnej instalacji systemu operacyjnego. • Alerty Syslog. • Szyfrowane połączenie (TLS min. TLS 1.2) oraz autentykacja i autoryzacja użytkowanika. • Możliwość zdefiniowania min. 12 użytkowników lokalnych na karcie zarządzającej. • Wyświetlanie danych aktualnych oraz 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. • Montowanie obrazów ISO musi być możliwe bez instalacji dodatkowych komponentów Java czy AciveX. • Możliwość jednoczesnej pracy do 6 użytkowników przez wirtualną konsolę. • Wspierane protokoły/interfejsy: IPMI v2.0, SNMP v3, CIM, DCMI v1.5, REST API. • Zgodność z FIPS 140-3 oraz NIST 800-193. • Zabezpieczenie przed nieautoryzowaną wymianą komponentów sprzętowych serwera. Wymaga się możliwości ustawienia zablokowania startu systemu na skutek wykrycia takiego zdarzenia. • Możliwość grupowania serwerów w kontekście synchronizacji jednolitej konfiguracji oraz wersji firmware dla całej grupy serwerów. • Wymaga się możliwości wykorzystania frontowego portu USB do celów serwisowych (komunikacja portu z kartą 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.
17	**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. Wymagana obecność przedniego panelu zabezpieczającego zamykanego na klucz.
18	**Urządzenia hot swap**	Dyski twarde, zasilacze, wentylatory.
19	**Diagnostyka**	Możliwość przewidywania awarii dla procesorów, regulatorów napięcia, pamięci, dysków wewnętrznych (włącznie z dyskami m.2), wentylatorów, zasilaczy, kontrolerów RAID. Możliwość użycia aplikacji mobilnej na telefonie do przeglądania awarii, konfiguracji i włączenia/wyłączenia serwera. Wymaga się, aby serwer posiadał diody sygnalizujące awarię przy każdej kości pamięci RAM, każdej zatoce dyskowej, każdym zasilaczu.
20	**Systemy operacyjne**	Wsparcie dla systemu operacyjnego Red Hat Enterprise Linux 8.9, 9.1, 9.2, 9.3. **Wraz z serwerem należy dostarczyć komplet licencji Red Hat Enterprise Linux pozwalających prawidłowo zalicencjonować procesory zaoferowane w ramach oferowanego serwera.**
21	**Gwarancja**	5 lat gwarancji producenta świadczonej w reżimie 9/5, on-site, z czasem odpowiedzi – nastepny dzień roboczy. Usługi wsparcia serwisowego świadczone bezpośrednio przez producenta sprzętu. Możliwość zgłaszania awarii w języku polskim poprzez ogólnopolską linię telefoniczną producenta. Możliwość pobierania nowych wersji firmware'ów oraz sterowników do wszystkich składowych serwera bezpośrednio ze strony producenta serwera.
22	**Dodatkowa funkcjonalność**	**Dostarczone serwery wspierane przez posiadane przez Zamawiającego oprogramowanie xClarity Administrator. Zamawiający wymaga dostarczenia wraz z serwerami odpowiedniego zestawu licencji do ww. oprogramowania, z okresem wsparcia równym okresowi wsparcia na dostarczone serwery.** **Zamawiający wymaga potwierdzenia producenta oprogramowania xClarity Administrator o zgodności oferowanych serwerów z ww. oprogramowaniem.**

3. Macierz dyskowa – 2szt.

Lp.	Nazwa elementu, parametru lub cechy	Opis wymagań macierzy dyskowej
1	**Obudowa**	• Możliwość zainstalowania w standardowej szafie RACK 19”. • Urządzenie musi wykorzystywać półki dyskowe wysokiej gęstości upakowania – co najmniej 24 dyski na 2U wysokości dla dysków 2,5” oraz półki dyskowe zawierające co najmniej 12 dysków 3,5” na wysokości 2U. • Urządzenie musi mieć możliwość wykorzystywania półek dyskowych wysokiej gęstości, umożliwiające upakowanie co najmniej 90 dysków na maksymalnej wysokości 5U. • Wysokość oferowanego rozwiązania – maksymalnie 8U.
2	**Zarządzanie**	• Urządzenie musi umożliwiać zarządzanie za pomocą interfejsu Ethernet. • Możliwość zarządzania całością dostępnych zasobów dyskowych z jednej konsoli administracyjnej. • Funkcjonalność bezpośredniego monitoringu stanu, w jakim w danym momencie macierz się znajduje. • Interfejs zarządzający GUI, CLI oraz zapewnienie możliwości tworzenia skryptów użytkownika.
3	**Porty**	• Wymagane są nie mniej niż 4 porty 10Gb Ethernet Base-T oraz 8 portów 16Gb FC wyposażonych we wkładki SFP SW.
4	**Obsługa dysków**	• Musi obsługiwać dyski: a) HDD SAS o prędkości obrotowej 10000 obr./min. i pojemności 2.4TB; b) HDD NL-SAS o prędkości obrotowej 7200 obr./min. i pojemnościach 8TB, 12TB, 16TB, 20TB; c) SSD SAS o pojemnościach 1.92 TB , 3.84 TB, 7.68 TB, 15.36 TB, 30.72 TB. • Musi wspierać obsługę co najmniej 420 dysków na parę kontrolerów z zastosowaniem dodatkowych półek. Macierz musi umożliwiać rozbudowę o pojedyncze dyski fizyczne i pojedyncze półki rozszerzeń. • Musi umożliwiać konfigurację, która w jednym rozwiązaniu łączyć będzie półki rozszerzeń na dyski 2,5” z półkami na dyski 3,5”. • Macierz musi zapewnić możliwość wymiany uszkodzonych dysków podczas pracy systemu (Hot-Swap).
5	**Pojemność dyskowa**	• Zamawiający wymaga minimum 280TiB przestrzeni użytkowej opartej o dyski HDD lub SSD. Przestrzeń użytkowa musi być zabezpieczona na wypadek jednoczesnej awarii dwóch dysków. • Zamawiający wymaga, aby minimalna wydajność macierzy wynosiła: 800 MiB/s / 12800 IOPS, przy założeniu: 100% odczyt, w tym 50% odczyt losowy, rozmiar operacji IO 64k, przy średnim opóźnieniu nieprzekraczającym 20ms, z uwzględnieniem akceleracji pamięcią cache na poziomie 50% cache hit ratio. • Przestrzeń zapasowa powinna być realizowana za pomocą przestrzeni zapasowej rozmieszczonej na wszystkich dyskach w ramach grupy RAID lub w formie dysków nadmiarowych. Liczba niezbędnych dysków nadmiarowych/przestrzeni zapasowej powinna być określona w oparciu o założenie, że dla każdych użytych w macierzy 24 dysków, jednym z dysków powinien być dysk zapasowy. W przypadku, gdy użyta w macierzy liczba dysków nie jest wielokrotnością 24 dysków, wówczas liczbę niezbędnych dysków nadmiarowych zaokrąglamy w górę.
6	**Pamięć cache**	• Macierz musi być wyposażona w minimum 64GB pamięci cache. Macierz musi umożliwiać rozbudowę pamięci cache do 128GB w ramach klastra macierzy zarządzanego z jednego interfejsu GUI, CLI.
7	**Systemy operacyjne**	• Macierz musi wspierać następujące systemy operacyjne i wirtualizatory: MS Windows Server 2016,2019/2022, VMware vSphere 7.x/8.x, Red Hat Enterprise Linux 8.x/9.x.

8	**Funkcje niezawodnościowe**	• Wszystkie krytyczne komponenty urządzenia, takie jak: kontrolery dyskowe, pamięć cache, zasilacze i wentylatory muszą być zdublowane tak, aby awaria pojedynczego elementu nie wpływała na funkcjonowanie całego systemu. • Komponenty te muszą być wymienialne w trakcie pracy macierzy. • Urządzenie musi cechować brak pojedynczego punktu awarii. • Wsparcie dla zasilania z dwóch niezależnych źródeł prądu poprzez nadmiarowe zasilacze typu Hot-Swap. • Wentylatory typu Hot-Swap. • Wbudowane co najmniej dwa kontrolery RAID. • Urządzenie musi posiadać pamięć typu Flash dla zapisu danych z pamięci cache na wypadek zaniku zasilania oraz system podtrzymania zasilania, pozwalający na zapis danych z cache do pamięci typu Flash.
9	**Funkcjonalności**	• Musi istnieć funkcjonalność Cache dla procesu odczytu. • Musi istnieć funkcjonalność Mirrored Cache dla procesu zapisu. • Możliwość wyłączenia cache dla poszczególnych wolumenów. • Funkcjonalność partycjonowania pamięci cache. • Funkcjonalność separacji przestrzeni dyskowych pomiędzy różnymi podłączonymi hostami. • Funkcjonalność dynamicznego zwiększania i zmniejszania rozmiaru wolumenów. • Funkcjonalność zarządzania liczbą operacji wejścia/wyjścia wykonywanych na danym wolumenie – zarządzanie musi być możliwe zarówno poprzez określenie liczby operacji I/O na sekundę jak również przepustowości określonej w MB/s. • Urządzenie musi obsługiwać funkcjonalność ochrony przed skasowaniem lub odmapowaniem od hosta woluminu dyskowego, do którego były przesłane operacje wejścia/wyjścia w określonym przez użytkownika czasie. • Dostępne sterowniki do obsługi wielościeżkowego dostępu do wolumenów, awarii ścieżki i rozłożenia obciążenia po ścieżkach dostępu dla podłączanych systemów operacyjnych.
10	**Obsługa wirtualnych dysków logicznych**	• Minimalna liczba wspieranych wirtualnych dysków logicznych (LUN) dla całej (globalnej) puli dyskowej musi wynosić co najmniej 2000. Funkcjonalność LUN Masking i LUN Mapping. • Urządzenie musi umożliwiać stworzenie mirrorowanych LUN pomiędzy różnymi typami dysków, dla których awaria jednej kopii lustra musi być niezauważalna dla systemu hosta.
11	**Funkcjonalność Thin Provisioning**	• Urządzenie musi obsługiwać funkcjonalność Thin Provisioning dla wszystkich wolumenów. Musi istnieć możliwość wyłączenia tej funkcjonalności dla wybranych wolumenów.
12	**Migracja wolumenów logicznych**	• Urządzenie musi mieć możliwość wykonania migracji wolumenów logicznych pomiędzy różnymi typami dysków wewnątrz macierzy, bez zatrzymywania aplikacji korzystającej z tych wolumenów. Wymaga się, aby zasoby źródłowe podlegające migracji oraz zasoby, do których są migrowane mogły być zabezpieczone różnymi poziomami RAID i egzystować na różnych technologicznie dyskach stałych (HDD, SSD).
13	**Replikacja macierzy**	• Urządzenie musi posiadać funkcjonalność replikacji danych przy użyciu synchronicznej transmisji danych przez łącza komunikacyjne IP oraz FC lub FCoE na odległość do 300km. Replikacja musi wspierać program Vmware Site Recovery Manager do odzyskiwania danych po awarii.
14	**Wirtualizacja zasobów**	• Macierz musi mieć możliwość wirtualizacji zasobów znajdujących się na innych niż oferowane macierze dyskowe na potrzeby migracji danych. Migracja musi się odbyć w trybie bezprzerwowym.
15	**Kompresja i deduplikacja danych**	• Macierz musi mieć możliwość kompresji i deduplikacji danych.
16	**Szyfrowanie**	• Macierz musi mieć możliwość uruchomienia funkcjonalności szyfrowania danych na poziomie kontrolerów macierzowych.
17	**Pozostałe wymagania**	• Macierz musi mieć możliwość dodawania kolejnych półek dyskowych oraz dysków bez przerywania pracy macierzy, dla dowolnej konfiguracji macierzy. • Macierz musi mieć możliwość aktualizacji oprogramowania macierzy (firmware) w trybie online.

		• Macierz musi umożliwiać tworzenie wolumenów o pojemności nie mniejszej niż 250 TB. • Do macierzy należy dołączyć przewody zasilające oraz 8 przewodów światłowodowych o długości 5m. • Macierz musi posiadać możliwość optymalizowania wykorzystania dysków SSD i HDD poprzez automatyczną identyfikację najbardziej obciążonych fragmentów woluminów w zarządzanych zasobach dyskowych (wewnętrznych jak i zewnętrznych, zwirtualizowanych) oraz ich automatyczną migrację na grupę dyskową składającą się z szybszych nośników. Macierz musi posiadać możliwość wykorzystania mechanizmu optymalizacji umiejscowienia danych pomiędzy przynajmniej 3 rodzajami grup dyskowych, składających się z dysków – SSD, HDD SAS oraz HDD NL-SAS, jak również przy wykorzystaniu dwóch dowolnych z wyżej wymienionych typów. Opisany powyżej proces optymalizacji musi posiadać funkcję włączenia/wyłączenia na poziomie pojedynczego woluminu. • Macierz musi optymalizować wykorzystanie dysków SSD/HDD, tak, aby w ramach puli składającej się z grup dyskowych tego samego rodzaju (pojemności/prędkości dysków) wszystkie składowe grupy dyskowe były utylizowane względem pojemności w możliwie równym stopniu. • Zaoferowana macierz musi posiadać możliwość implementacji klastra geograficznego. W ramach architektury klastra geograficznego musi być wspierane bezprzerwowe migrowanie maszyn wirtualnych pomiędzy ośrodkami. W przypadku awarii jednego z ośrodków nastąpi bezprzerwowe przełączenie do lokalizacji zapasowej. Powyższa funkcjonalność musi być realizowana niezależnie od systemu operacyjnego na poziomie przełączania ścieżek do urządzenia logicznego. • Dostarczone urządzenie musi mieć zainstalowane wszystkie najnowsze zestawy poprawek dotyczących dostarczanego sprzętu. • Oferowane produkty w przedmiotowym postępowaniu o udzielenie zamówienia publicznego muszą spełniać wymagania norm CE, tj. muszą spełniać wymogi niezbędne do oznaczenia produktów znakiem CE. • Urządzenia i ich komponenty muszą być oznakowane przez producenta w taki sposób, aby możliwa była identyfikacja zarówno produktu jak i producenta. • Urządzenie musi współpracować z siecią energetyczną o parametrach w przedziale 200V-230V, 50 Hz.
18	**Licencje**	• Należy dostarczyć licencje na wszystkie wymienione w opisie wymagań funkcjonalności, za wyjątkiem szyfrowania. Dostarczone licencje muszą obejmować całą oferowaną w ramach macierzy przestrzeń dyskową.
19	**Gwarancja i serwis**	• 5 lat gwarancji producenta świadczonej w reżimie 24/7, on-site, z reakcją w tym samym dniu roboczym od momentu zgłoszenia awarii. • Możliwość zgłaszania awarii w języku polskim poprzez ogólnopolską linię telefoniczną producenta. Możliwość pobierania poprawek oraz nowych wersji firmware'ów bezpośrednio ze strony producenta macierzy przez cały okres obowiązywania gwarancji.
20	**Dodatkowa funkcjonalność nr 1**	• **Macierz musi umożliwiać tworzenie wg ustalonego harmonogramu odpornych na zagrożenia cybernetyczne kopii wolumenów, tj. takich, których nie można zmienić, ani usunąć w wyniku błędów użytkownika, złośliwych działań lub ataków oprogramowania ransomware.**
21	**Dodatkowa funkcjonalność nr 2**	• **Macierz musi mieć funkcjonalność wykonywania pełnej kopii lokalnych wolumenów logicznych z wykorzystaniem jedynie kontrolerów macierzy. Licencja na wykonywanie kopii lokalnego wolumenu powinna umożliwiać utworzenie co najmniej 4000 kopii.**

4. **Biblioteka taśmowa – 1szt.**

Lp.	Nazwa elementu, parametru lub cechy	Opis wymagań biblioteki taśmowej
1	**Obudowa**	Przystosowana do montażu w szafie rack 19", wysokość nie większa niż 9U, z zestawem szyn do mocowania w szafie.
2	**Napędy taśmowe**	Biblioteka taśmowa musi być wyposażona w min. 3 napędy taśmowe LTO9 o natywnym interfejsie FC, połowy wysokości (Half Height). Biblioteka powinna umożliwiać wymianę napędów bez przerywania pracy (napędy typu „hot swap").
3	**Napędy taśmowe – rozbudowa**	Biblioteka musi mieć możliwość rozbudowy do 24 napędów taśmowych LTO9 (o natywnym interfejsie FC, połowy wysokości (Half Height)) łącznie. Musi być możliwość mieszania napędów różnych technologii LTO (od min. LTO-8) oraz różnych interfejsów.
4	**Napędy taśmowe – szyfrowanie**	Biblioteka musi mieć możliwość sprzętowego szyfrowania kopii zapasowych z wykorzystaniem napędów taśmowych. Klucze szyfrujące muszą być przechowywane w aplikacji backup. Licencja musi być dostarczona wraz z biblioteką.
5	**Liczba slotów – storage**	Biblioteka musi mieć min. 100 kieszeni na nośniki taśmowe, z czego 50 kieszeni musi być zalicencjonowanych do dowolnego użytku
6	**Liczba slotów – storage – rozbudowa**	Biblioteka musi mieć możliwość rozbudowy do min. (fizycznie oraz zalicencjonowanych do dowolnego użytku) 400 kieszeni na nośniki taśmowe.
7	**Liczba slotów – mail slot**	Biblioteka musi mieć możliwość zdefiniowania do 25 kieszeni typu „mail slot" w odstępach co 5 (licząc od 0).
8	**Zarządzanie**	Biblioteka musi być zarządzana z poziomu panelu dotykowego zabezpieczonego hasłem lub/i numerem PIN oraz zdalnego modułu zarządzania przez panel WWW (HTML5). Biblioteka musi udostępniać funkcje monitorowania stanu napędów i robota. Biblioteka taśmowa powinna mieć również możliwość zdalnego monitorowania stanu urządzenia i wychwytywania błędów bezpośrednio przez inżynierów producenta za pomocą odpowiedniego oprogramowania, dostarczonego razem z biblioteką taśmową. Nie jest dopuszczalne instalowanie żadnych dodatkowych systemów (wirtualnych czy fizycznych) w celu osiągnięcia tej funkcjonalności. Obsługa SNMP, Syslog. Biblioteka musi posiadać min. 1 interfejs 1GbE do zarządzania. Interfejs musi być zlokalizowany na module zarządzania biblioteką
9	**Partycjonowanie**	Biblioteka powinna być wykonana w technologii umożliwiającej sprzętowy podział na mniejsze biblioteki „logiczne", a następnie podłączane do różnych serwerów, korzystających z różnego oprogramowania do wykonywania kopii zapasowych i archiwizacji. Biblioteka musi wspierać do 21 logicznych bibliotek.
10	**Zasilanie**	W pełni redundantne dla wszystkich modułów posiadających napędy taśmowe.
11	**Gwarancja**	Biblioteka musi być serwisowana przez producenta lub autoryzowany serwis producenta w języku polskim ze wsparciem na 5 lat w trybie 5x9xNBD. W przypadku autoryzowanego serwisu producenta na terenie Polski, wymagane jest potwierdzenie kompetencji w zakresie świadczenia usług serwisowych poprzez certyfikat ISO 9001:2015 oraz minimum 3 certyfikowanych inżynierów przez producenta w serwisie dedykowanego urządzenia.
12	**Taśmy**	Sprzęt powinien być dostarczony wraz z 50 taśmami LTO-9 oraz 5 taśmami czyszczącymi.
13	**Inne**	Jeśli do jakiejkolwiek wyżej opisanej funkcjonalności lub rozbudowy fizycznej wymagane jest dostarczenie licencji, to licencje muszą być dostarczone w ramach tego postępowania.

14	Dodatkowa funkcjonalność nr 1	Biblioteka powinna mieć możliwość stworzenia bezpiecznej partycji dla nośników taśmowych w celu ochrony przed ransomware. Partycja powinna być skonfigurowana na dostępnych slotach w bibliotece nawet w przypadku, kiedy nie są one zalicencjonowane. Partycja ta nie może posiadać przypisanego napędu taśmowego oraz nie może być dostępna dla oprogramowania (hosta). Biblioteka taśmowa powinna przechwytywać operację eksportu nośników taśmowych wykonywanych przez aplikację backup i automatycznie umieszczać te nośniki w bezpiecznej partycji, niedostępnej dla oprogramowania backup, a nie w slotach typu „mail". Biblioteka powinna mieć możliwość definiowania tzw. „logical lock", który uniemożliwi użytkownikowi administracyjnemu przesunięcie nośnika taśmowego w inny slot lub napęd biblioteki taśmowej. Biblioteka powinna mieć możliwość zainstalowanego tzw. „hardware lock", który uniemożliwi fizyczną ingerencję w bibliotekę taśmową (np. serwisowe wysunięcie magazynków z nośnikami taśmowymi). Jeżeli wspomniana funkcjonalność wymaga dodatkowych licencji, należy je dostarczyć wraz z urządzeniem. Funkcjonalność powinna być realizowana natywnie przez bibliotekę.
15	Dodatkowa funkcjonalność nr 2	Biblioteka powinna być dostarczona w konfiguracji umożliwiającej zablokowanie dostępu do taśmy dla robota biblioteki poprzez częściowe wysunięcie magazynka z taśmami przy jednoczesnym zachowaniu możliwości skanowania barecode'ów. Funkcjonalność ta nie powinna wpływać na pracę i dostęp do pozostałych magazynków z taśmami w oferowanej bibliotece. Funkcjonalność powinna być realizowana natywnie przez bibliotekę.
16	Dodatkowa funkcjonalność nr 3	Biblioteka powinna wspierać Multi-Factor Authentication (MFA) dla minimum użytkowników lokalnych. Powinna być możliwość tworzenia użytkowników lokalnych oraz integracji z systemem usług katalogowych – Microsoft Active Directory.
17	Dodatkowa funkcjonalność nr 4	Biblioteka powinna posiadać min. 2 redundantne interfejsy 1GbE do zarządzania. Interfejsy powinny być zlokalizowane na module zarządzania biblioteką oraz posiadać wszystkie mechanizmy zarządzania na obu portach.
18	Dodatkowa funkcjonalność nr 5	Biblioteka taśmowa powinna mieć możliwość włączenia adresacji logicznej dla modułu kontrolnego (numer seryjny) oraz napędów taśmowych (WWN), dzięki czemu wymiana tych komponentów nie wpływa na rekonfigurację aplikacji i sieci SAN.

5. Usługi wdrożenia systemu backupu – 1 szt.
Zakres wdrożenia:

1. Ustalenie adresacji IP dla dostarczonych urządzeń i usług systemów operacyjnych.
2. Określenie lokalizacji urządzeń w szafach RACK.
3. Ustalenie szczegółów dotyczących podłączenia nowych urządzeń do przełączników sieci LAN.
4. Opracowanie i przekazanie wytycznych dla Zamawiającego w zakresie konfiguracji sieci LAN i niezbędnej widoczności sieciowej pomiędzy usługami środowiska Commvault, a infrastrukturą Zamawiającego.
5. Dostawa sprzętu do poszczególnych lokalizacji Zamawiającego oraz montaż sprzętu w szafach RACK.
6. Podłączenie okablowania zasilającego, LAN, FC, SAS (półki dyskowe w macierzy).
7. Konfiguracja sprzętowa 2 serwerów dla potrzeb Commserve:
    a) aktualizacja firmware,
    b) nadanie serwisowej adresacji IP,
    c) konfiguracja dysków dla OS Linux oraz bazy Commserve,
    d) konfiguracja powiadomień e-mail.
8. Konfiguracja sprzętowa 2 serwerów dla potrzeb Media Agentów:
    a) aktualizacja firmware,
    b) nadanie serwisowej adresacji IP,
    c) konfiguracja dysków dla OS Linux, Index Cache oraz silnika deduplikacji,
    d) konfiguracja powiadomień e-mail.
9. Konfiguracja 2 macierzy dyskowych:
    a) aktualizacja firmware,
    b) nadanie adresacji IP,
    c) konfiguracja grup RAID i wolumenów (Distributed Raid 6),
    d) udostępnienie zasobów macierzy do serwerów Media Agent (backend storage),
    e) konfiguracja powiadomień e-mail.
10. Przygotowanie środowiska systemowego dla usługi Media Agent na 2 serwerach z systemem Red Hat Enterprise Linux będących przedmiotem zamówienia, a w tym:
    a) konfiguracja interfejsów sieciowych (LAG/Teaming),
    b) konfiguracja adresów IP,
    c) konfiguracja LUN udostępnionych z macierzy,
    d) weryfikacja poprawnego działania mechanizmów MPIO.
11. Przygotowanie środowiska systemowego dla usługi Commserve na 2 serwerach fizycznych z systemem Red Hat Enterprise Linux.
12. Instalacja i konfiguracja oprogramowania usług serwera Commvault:
    a) odświeżenie oprogramowania Commserve (węzeł aktywny i pasywny),
    b) budowa repozytorium oprogramowania (FR32),
    c) instalacja oprogramowania Media Agent/VSA na nowej platformie,
    d) hardening Media Agenta w zapasowym ośrodku przetwarzania danych, m.in. udostępnienie usługi ssh na niestandardowym porcie, włączenie logowania oraz podwójnego uwierzytelnienia dla usługi ssh, blokada ruchu przychodzącego na pozostałych portach, porty zarządzające macierzą i serwerem w dedykowanej podsieci VLAN,
    e) konfiguracja silników deduplikacji,
    f) konfiguracja repozytorium składowania danych (Disk Library),
    g) konfiguracja szyfrowania danych,
    h) konfiguracja ransomware protection dla Disk Library,
    i) konfiguracja mechanizmów replikacji dla usługi CommServe na cele Disaster Recovery (Live Sync),
    j) konfiguracja MFA dla administratorów.

13. Aktualizacja pozostałych komponentów Commvault do FR32.
14. Konfiguracja biblioteki taśmowej:
    a) instalacja fizyczna urządzenia w szafie rack (jednostka kontrolna i moduły rozszerzeń), okablowanie zasilające oraz FC,
    b) konfiguracja sieci/interfejsu management,
    c) aktualizacja firmware w bibliotece oraz napędach LTO,
    d) konfiguracja partycji biblioteki dla części operacyjnej oraz części nieaktywnej,
    e) import taśm, weryfikacja działania robota biblioteki,
    f) konfiguracja biblioteki taśmowej w systemie Commvault,
    g) przeprowadzenie szkolenia z interfejsu zarządzającego oraz obsługi administracyjnej biblioteki (4 godziny); szkolenie w formie zdalnej.
15. Konfiguracja Storage Policy Copy:
    a) wykonanie repliki wszystkich danych short term,
    b) wykonanie repliki dla wszystkich danych long term.
16. Wykonanie pre-produkcyjnych testów roboczych, obejmujących zakresem:
    a) odtworzenie 5 maszyn wirtualnych,
    b) odtworzenie 2 baz danych,
    c) odtworzenie agentowe zbioru plików z 6 serwerów fizycznych/wirtualnych,
    d) Testy Commserve Failover oraz failback.
17. Wykonanie kopii „0” na nową platformę wszystkich systemów chronionych w istniejącym środowisku.
18. Przekierowanie polityk backupowych na nową platformę, przy jednoczesnym utrzymaniu kopii na starej platformie.
19. Wstępna optymalizacja systemu po uruchomieniu produkcyjnym.
20. Wykonanie produkcyjnych testów odtworzeniowych z kopii primary lub kopii utwardzonej w ośrodku zapasowym, obejmujących zakresem:
    a) odtworzenie 5 maszyn wirtualnych,
    b) odtworzenie 2 baz danych,
    c) odtworzenie agentowe zbioru plików z 6 serwerów fizycznych/wirtualnych.
21. Odinstalowanie oprogramowania Commvault z obecnej platformy MediaAgent:
    a) kasowanie pool, disklib, storage policy copy, etc.,
    b) odinstalowanie oprogramowania,
    c) usuniecie obiektów z systemu Commvault.
22. Opracowanie dokumentacji technicznej zawierającej opis przeprowadzonej konfiguracji, w tym:
    a) opis strategii wykonywania kopii w zaimplementowanym środowisku,
    b) architekturę logiczną rozwiązania,
    c) architekturę fizyczną,
    d) konfigurację usług Commvault (Commserve, MediaAgent, VSA, agenci aplikacyjni),
    e) definicje polityk backupu i harmonogramów / Planów,
    f) opis metod tworzenia kopii dla poszczególnych typów zasobów,
    g) konfigurację integracji z wirtualizatorami,
    h) definicje zadań administracyjnych,
    i) okna operacyjne,
    j) definicje grup użytkowników i ich role oraz nadane uprawnienia do zasobów Commvault,
    k) opis zdefiniowanych raportów i ich adresatów,
    l) opis zdefiniowanych alertów i ich adresatów,
    m) opis konfiguracji mechanizmu DR dla Commserve,
    n) konfigurację topologii sieci dla potrzeby wdrożonej infrastruktury Commvault,

o) listę wykorzystywanych portów TCP przez poszczególne usługi Commvault w komunikacji ze środowiskiem Zamawiającego,
p) konfigurację automatyzacji.

23. Opracowanie procedury przełączenia usługi CommServe na środowisko DR.
24. Opracowanie zestawu rekomendacji dotyczących dobrych praktyk w zakresie zarządzania bezpieczeństwem systemu Commvault.
25. Opracowanie procedury aktualizacji oprogramowania Commvault.

Uwagi:

1. Konfiguracja urządzeń sieciowych Zamawiającego w celu umożliwienia właściwej komunikacji pomiędzy wdrażaną infrastrukturą usług Commvault, a istniejącym środowiskiem, leży po stronie Zamawiającego.
2. Konfiguracja urządzeń sieciowych LAN/NGFW realizowana jest przez Zamawiającego wg wytycznych przekazanych przez Wykonawcę.