

(177622)

OPIS PRZEDMIOTU ZAMÓWIENIA

Przedmiotem zamówienia jest: **Dostawa deduplikatorów wraz z licencjami do oprogramowania do deduplikacji danych**, zwanych dalej „Urządzeniami”.

1. Termin realizacji zamówienia – do 60 dni kalendarzowych od dnia podpisania Umowy.

2. Zamówienie obejmuje:

- 2.1. Dostawę 4 nowych Urządzeń do backupu dyskowego z deduplikacją danych wraz z licencjami do oprogramowania do deduplikacji danych, montażem oraz 36/60 miesięczną gwarancją zgodnie z pkt 3.
- 2.2. Instalację i konfigurację w 2 lokalizacjach na terenie miasta Warszawy.
- 2.3. Aktualizację oprogramowania do najnowszej stabilnej wersji, dostępnej w dniu uruchomienia.
- 2.4. Przeprowadzenie instruktażu z konfiguracji dostarczonych deduplikatorów, dla minimum 4 osób, w środowisku Zamawiającego (min. 12 godzin) opisanym w pkt 4.

3. Wymagania minimalne w zakresie dostawy nowych Urządzeń:

Dostawa 4 Urządzeń, każde o wymaganiach:

L.p.	Cecha	Wymagania minimalne
3.1.	Definicja	3.1.1. Przez Urządzenie do backupu dyskowego wraz z deduplikacją danych (dalej Urządzenie) Zamawiający rozumie rozwiązanie, pochodzące od jednego producenta oraz realizujące wszystkie wymagane funkcjonalności. 3.1.2. Urządzenie musi być specjalizowane, zaprojektowane i dedykowane wyłącznie do działania jako repozytorium do składowania kopii zapasowych (backupów). Nie dopuszcza się stosowania klasycznych macierzy dyskowych. 3.1.3. Urządzenie musi składać się z co najmniej dwóch węzłów/kontrolerów (tzw. architektura wielokontrolerowa) pracujących jako jeden system, zarządzany z poziomu pojedynczej konsoli administracyjnej (wspólnej dla wszystkich kontrolerów/węzłów).

L.p.	Cecha	Wymagania minimalne
		3.1.4. Zainstalowane procesory kontrolerów/węzłów, muszą posiadać architekturę x86. 3.1.5. Urządzenie musi być oficjalnie dostępne w ofercie producenta przed terminem publikacji niniejszego postępowania.
3.2.	Typ obudowy	3.2.1. Urządzenie musi być przystosowane do montażu w szafie rack 19". Urządzenie musi być dostarczone wraz z kompletem kabli zasilających, sieciowych i innych wymaganych do jego poprawnego podłączenia, uruchomienia i działania.
3.3.	Przestrzeń dyskowa	3.3.1. Urządzenie musi oferować pojemność minimum 1,5 PB netto dedykowaną do lokalnego przechowywania obrazów backupów na dyskach własnych (wewnętrznych). W pojemność nie wlicza się nadmiarowości potrzebnej do zabezpieczenia danych, np. RAID. Urządzenie musi oferować pojemność minimum 1,5 PB netto dedykowaną do lokalnego przechowywania obrazów backupów na dyskach własnych (wewnętrznych). Jeśli architektura Urządzenia wymaga dodatkowej przestrzeni typu cache/landing zone, to wymagane jest dostarczenie dodatkowej pojemności minimum 25% netto oferowanego urządzenia. 3.3.2. W pojemność Urządzenia nie może wliczać się przestrzeń znajdująca się w chmurze (tzw. Cloud).
3.4.	Bezpieczeństwo danych	3.4.1. Dane przechowywane w obrębie podsystemu dyskowego Urządzenia muszą być chronione za pomocą technologii RAID 6. 3.4.2. Wymagany dysk typu Hot-Spare dla każdej skonfigurowanej grupy RAID'owej. 3.4.3. Wymaga się, aby Urządzenie weryfikowało poprawność zapisu wszystkich zabezpieczanych danych. 3.4.4. Ze względów bezpieczeństwa Urządzenie powinno zabezpieczać dane przed możliwością nadpisania, a dane przeterminowane powinny być usuwane jedynie w procesie czyszczenia. 3.4.5. Urządzenie musi posiadać zintegrowany mechanizm ochrony danych przed atakami typu „ransomware”, umożliwiający odzyskanie danych zaszyfrowanych, uszkodzonych, usuniętych przez ransomware, błąd ludzki lub celowe działanie. Mechanizm musi być dostępny dla protokołów CIFS, NFS i dedykowanego protokołu, jeśli taki jest dostęp Zintegrowana ochrona przed ransomware: Urządzenie musi posiadać zintegrowany mechanizm ochrony danych przed

L.p.	Cecha	Wymagania minimalne
		nieautoryzowanymi zmianami, usunięciem (np. ataki ransomware, błędy ludzkie). Mechanizm ten może opierać się na funkcji nieusuwalności (immutability/WORM - Write Once, Read Many lub innym rozwiązaniu) dla przechowywanych danych, co uniemożliwi ich modyfikację lub usunięcie przed upływem zdefiniowanego okresu retencji. Mechanizm musi być dostępny dla protokołów CIFS, NFS i dedykowanego protokołu, jeśli taki jest dostępny. 3.4.6. Integracja mechanizmu ransomware: Mechanizm nieusuwalności danych musi być oficjalnie wspierany przez aplikację backupową Commvault używaną do zapisu danych na Urzędzeniu. Wykonawca musi przedstawić potwierdzenie tej kompatybilności, np. w postaci linku do oficjalnej dokumentacji Commvault lub oficjalnej dokumentacji producenta urządzenia. Mechanizm ten musi być konfigurowalny i kontrolowany w taki sposób, aby zapewnić skuteczną ochronę przed modyfikacją/usunięciem danych bezpośrednio na Urzędzeniu, niezależnie od prób obejścia zabezpieczeń przez oprogramowanie zewnętrzne (w tym potencjalnie skompromitowaną aplikację backupową). Mechanizm „antyransomware” musi być niezależny od używanego oprogramowania do tworzenia kopii zapasowych i musi być oparty jedynie o wewnętrzne mechanizmy dostarczanego Urzędzenia.
3.5.	Konfiguracja wysoko dostępna	3.5.1. Urządzenie musi posiadać co najmniej: • dwa kontrolery/węzły • dyski wymienne w trakcie pracy Urzędzenia, • redundantne zasilacze wymienne w trakcie pracy Urzędzenia, • dyski w konfiguracji RAID-6 z zapasowym dyskiem "hot-spare", • redundantne wentylatory 3.5.2. Awaria jednego kontrolera/węzła Urzędzenia nie może prowadzić do całkowitej niedostępności Urzędzenia. W czasie awarii kontrolera/węzła Urzędzenie powinno nadal umożliwiać wykonanie operacji backupu.
3.6.	Interfejsy	3.6.1. Urządzenie musi posiadać minimum: 12 portów Ethernet 25 Gb/s wyposażonych we wkładki SFP28. Każdy z portów Ethernet musi mieć możliwość obsługi protokołów CIFS i NFS. 3.6.2. Jeśli Urządzenie umożliwia komunikację za pomocą sieci SAN, to wymagane jest dostarczenie minimum 4 portów FC. Dostarczone Porty powinny mieć maksymalną przepustowość,

L.p.	Cecha	Wymagania minimalne
		jaką umożliwiła Urządzenie, jednak nie mniej niż 16 Gb/s per port. 3.6.3. Urządzenie powinno być wyposażone w licencje umożliwiające wykorzystanie wymaganej przestrzeni poprzez dowolny z w/w interfejsów.
3.7.	Wydajność	3.7.1. Należy podać wydajność dla każdego kontrolera/węzła z osobną oraz sumaryczną wydajność Urządzenia. Deklaracja wydajności: Wykonawca musi podać sumaryczną wydajność zapisu danych (ingestu) dla oferowanej konfiguracji Urządzenia/systemu repozytorium. Wydajność powinna być podana w TB/h. 3.7.2. Wydajność dla pojedynczego kontrolera/węzła musi być dostępna w oficjalnej i ogólnie dostępnej dokumentacji Producenta. Minimalna wymagana wydajność: Minimalna wymagana sumaryczna wydajność zapisu danych (ingestu) dla oferowanej konfiguracji Urządzenia/systemu wynosi: Min. 130 TB/h w przypadku, gdy Urządzenie/system wykorzystuje mechanizm deduplikacji na źródle (source-side deduplication), zaimplementowany i oficjalnie wspierany przez aplikację backupową Commvault (np. Commvault Client Direct) o Min. 70 TB/h w przypadku, gdy Urządzenie/system realizuje deduplikację wyłącznie po stronie Urządzenia (target-side deduplication, in-line lub post-process) i nie oferuje możliwości deduplikacji na źródle. 3.7.3. Wymagana wydajność dla oferowanej konfiguracji to min. 130TB/h w przypadku deduplikacji na źródle (jeśli jest dostępna). W przypadku, gdy Urządzenie nie posiada funkcjonalności deduplikacji na źródle, to wymagana jest wydajność min. 70 TB/h bez deduplikacji na źródle. 3.7.4. Rozwiązanie musi zapewniać natywną, efektywną deduplikację na źródle oficjalnie wspieraną przez aplikację Commvault na poziomie klienta (client direct) bez pośrednictwa dodatkowych serwerów i urządzeń lub współpracować z deduplikacją oferowaną przez aplikację CommVault.
3.8.	Sposób udostępniania zasobów	3.8.1. Standardowe protokoły: Udostępnianie zasobów repozytorium za pomocą standardowych protokołów dostępu do plików, takich jak CIFS i NFS. Udostępnianie danych za pomocą protokołów CIFS i NFS.



L.p.	Cecha	Wymagania minimalne
		3.8.2. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej oferowanej pojemności Urzędnia.
3.9.	Deduplikacja danych	3.9.1. Urządzenie musi umożliwiać optymalizację składowania długoterminowego poprzez efektywne mechanizmy kompresji i/lub deduplikacji danych. Realizacja tego wymagania może być wykonywana inline, adaptacyjnie bądź jako proces działający w tle, pod warunkiem spełnienia opisywanych wymagań pojemnościowych i wydajnościowych. 3.9.2. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności Urzędnia. 3.9.3. Urządzenie musi zapewniać globalną deduplikację czyli przechowywać jedynie unikalne bloki danych niezależnie od tego, jakim protokołem, bądź do jakiego udziału, zostały zapisane. Nie jest dopuszczalne tworzenie unikalnej bazy deduplikatów per protokół lub per udział. 3.9.4. Nie jest dopuszczalne posiadania przez Urządzenie więcej niż jednej bazy deduplikatów.
3.10.	Replikacja danych	3.10.1. Urządzenie musi umożliwiać replikację danych do drugiego urządzenia. 3.10.2. Replikacja musi się odbywać w trybie asynchronicznym. Transmitowane muszą być tylko te fragmenty danych (bloki), które nie znajdują się na docelowym urządzeniu. 3.10.3. Musi istnieć możliwość ograniczenia pasma używanego do replikacji między dwoma urządzeniami. 3.10.4. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej oferowanej pojemności Urzędnia.
3.11.	Usuwanie przeterminowanych danych	3.11.1. Urządzenie musi automatycznie usuwać przeterminowane dane (bloki danych nienależące do backupów o aktualnej retencji) w procesie czyszczenia. 3.11.2. Proces usuwania przeterminowanych danych (czyszczenia) nie może uniemożliwiać pracy procesów backupu, odtwarzania oraz replikacji danych.
3.12.	Sposób zarządzania	3.12.1. Urządzenie musi mieć możliwość zarządzania poprzez interfejs graficzny dostępny z przeglądarki internetowej oraz

L.p.	Cecha	Wymagania minimalne
		poprzez linię komend (CLI) dostępną z poziomu SSH (Secure Shell). Oprogramowanie do zarządzania musi rezydować na oferowanym Urządzeniu deduplikacyjnym. 3.12.2. Oprogramowanie musi umożliwiać generowanie raportów dotyczących zużycia przestrzeni dyskowej; 3.12.3. Urządzenie musi umożliwiać ustawienie powiadomień administratora o problemach w Urządzeniu za pomocą poczty elektronicznej.
3.13.	Integracja z systemami backup	3.13.1. Urządzenie musi współpracować z oprogramowaniem do zarządzania kopiami bezpieczeństwa Commvault. Współpraca musi być potwierdzona na stronie producenta oprogramowania: https://www.commvault.com/supported-technologies#storage
3.14.	Gwarancja	3.14.1. Gwarancja świadczona w miejscu instalacji przez okres co najmniej 36/60 miesięcy. 3.14.2. Gwarancja obejmuje: 3.14.2.1. Urządzenie (sprzęt i oprogramowanie wbudowane i oprogramowanie narzędziowe zainstalowane na sprzęcie lub niezbędne do jego poprawnego funkcjonowania) 3.14.2.2. Konfigurację. 3.14.3. Tryb zgłaszania incydentów dotyczących Urządzenia - 24 godziny na dobę, przez 7 dni w tygodniu. 3.14.4. Obsługa zgłoszeń w języku polskim. 3.14.5. Czas reakcji na incydenty dotyczące sprzętu – 4 godziny od momentu zgłoszenia. 3.14.6. Gwarantowany czas naprawy sprzętu 24 godziny od momentu zgłoszenia. Jeżeli zasadna będzie wymiana sprzętu na nowy, nastąpi to do 2 dni roboczych od zgłoszenia. 3.14.7. Jeżeli usunięcie awarii wymaga wymiany nośnika danych (dysk twardy) Zamawiający wymaga pozostawienia uszkodzonego nośnika. 3.14.8. Czas reakcji na incydenty dotyczące oprogramowania – 4 godziny od momentu zgłoszenia. 3.14.9. Dostęp do poprawek i nowych wersji oprogramowania. Dostawca w okresie gwarancji na życzenie Zamawiającego

L.p.	Cecha	Wymagania minimalne
		wykona instalację poprawek i nowych wersji oprogramowania. 3.14.10. Dostęp wyznaczonych osób Zamawiającego do baz wiedzy producenta Urzędnia.
3.15.	Aspekty środowiskowe	3.15.1. Dostawca zobowiązany jest przedstawić oświadczenie potwierdzające zgodność dostarczonych Urzędzeń z Rozporządzeniem UE 2019/424 z dnia 15 marca 2019 r. ustanawiającym wymagania dotyczące ekoprojektu dla serwerów i produktów do przechowywania danych zgodnie z dyrektywą 2009/125/WE oraz zmieniające rozporządzenie Komisji (UE) nr 617/2013

4. Instruktaż :

- 4.1 Wykonawca przeprowadzi instruktaż dla nie więcej niż 4 pracowników Zamawiającego z obsługi dostarczonych Urzędzeń i oprogramowania w wymiarze min. 12 godzin, który przygotuje wskazanych pracowników do samodzielnej administracji.
- 4.2 Instruktaż zostanie przeprowadzony w języku polskim przez osoby będące trenerami producenta lub Wykonawcy.
- 4.3 Instruktaż zostanie zorganizowany w czasie trwania wdrożenia rozwiązania i zostanie ustalony pomiędzy Zamawiającym, a Wykonawcą.
- 4.4 Wykonawca zapewni dla każdego uczestnika wersję elektroniczną materiałów dydaktycznych zawierających streszczenie/omówienie wszystkich zagadnień zawartych w programie instruktażu oraz prezentacje wykorzystane podczas instruktażu.
- 4.5 Wykonawca po zakończeniu instruktażu wystawi uczestnikom dokument/certyfikat potwierdzający odbycie instruktażu wraz z jego zakresem.