

Dedykowany system backupu i deduplikacji danych z funkcją DR-Ready

1. Postanowienia Ogólne

1.1. Przedmiotem niniejszego zamówienia jest dostawa, montaż, uruchomienie oraz integracja fabrycznie nowego, dedykowanego urządzenia pamięci masowej przeznaczonego do składowania i sprzętowo-programowej deduplikacji kopii zapasowych (backupu), w pełni przystosowanego do pracy w środowisku wirtualizacji i ochrony danych Zamawiającego.

1.2. Urządzenie musi być kompletnym rozwiązaniem sprzętowym typu „appliance”, pochodzącym od jednego producenta (lub certyfikowanym rozwiązaniem zintegrowanym). Urządzenie musi być oficjalnie dostępne w ofercie producenta przed ukazaniem się niniejszego postępowania.

1.3. Oferowane urządzenie musi być fabrycznie nowe, wyprodukowane nie wcześniej niż 12 miesięcy przed datą dostarczenia do Zamawiającego i pochodzić z oficjalnego kanału dystrybucyjnego na rynek polski. Zamawiający zastrzega sobie, aby Wykonawca na żądanie Zamawiającego przedłożył oświadczenie Producenta oferowanego sprzętu, w języku polskim, potwierdzające pochodzenie sprzętu z autoryzowanego kanału sprzedaży z Polski.

1.4. Producent urządzenia musi oferować autoryzowane szkolenie z zaoferowanego produktu w języku polskim.

2. Warstwa Sprzętowa

2.1. Typ obudowy

2.1.1. Wielkość obudowy: Urządzenie zmontowane fabrycznie w standardzie do montażu w szafie rack 19" o maksymalnej wysokości do 4U (dopuszcza się urządzenia 2U, 3U lub 4U zapewniające wymaganą przestrzeń). W zestawie należy dostarczyć dedykowane, oryginalne szyny montażowe.

2.2. Przestrzeń dyskowa

2.2.1. Pojemność surowa (Raw Capacity): Minimum 144 TB przestrzeni fizycznej dostarczonej w obrębie urządzenia głównego (wraz z ewentualnymi dołączonymi półkami dyskowymi).

2.2.2. Pojemność użyteczna (Netto): Minimum 108 TB faktycznej przestrzeni dostępnej na składowanie kopii zapasowych po skonfigurowaniu bezpiecznej struktury RAID 6 (lub równoważnego mechanizmu usuwania nadmiarowości typu erasure coding), zapewniającego nieprzerwaną pracę systemu i ochronę przed jednoczesną awarią minimum 2 dysków danych w grupie.

2.3. Bezpieczeństwo danych

2.3.1. Dane przechowywane w obrębie podsystemu dyskowego urządzenia muszą być chronione przed utratą spójności danych w przypadku jednoczesnej awarii dwóch dowolnych dysków w grupie RAID.

2.3.2. Urządzenie musi weryfikować ewentualne przekłamanie danych. Wymaga się, aby system sprawdzał sumy kontrolne zapisywanych fragmentów danych. Urządzenie musi automatycznie rozpoznawać i naprawiać błędy w locie (funkcja self-healing).

2.3.3. Urządzenie musi umożliwiać bezpieczne usuwanie danych poprzez mechanizm wielokrotnego nadpisania przeterminowanych danych, działający zgodnie z dobrymi praktykami bezpieczeństwa (np. standard NIST SP 800-88).

2.4. Możliwość rozbudowy

2.4.1. Konstrukcja wewnętrzna urządzenia musi umożliwiać późniejszą rozbudowę pojemnościową (w tej samej obudowie lub poprzez dołożenie zewnętrznych półek dyskowych) w celu osiągnięcia pojemności minimum 216 TB netto.

2.5. Interfejsy Sieciowe i Komunikacja

2.5.1. Urządzenie musi posiadać wydzielony port zarządzający (np. RJ45 1GbE) połączony z procesorem serwisowym (IPMI/iLO/iDRAC lub równoważny), umożliwiający pełny monitoring sprzętowy, zdalne włączanie/wyłączanie, podgląd konsoli oraz raportowanie błędów za pomocą bezpiecznych protokołów (HTTPS, SNMPv3, SSH).

2.5.2. Interfejsy zintegrowane: Minimum 2 wbudowane porty miedziane 10GBASE-T (RJ45) obsługujące prędkości 1GbE oraz 10GbE.

2.5.3. Dedykowana karta rozszerzeń: System musi być wyposażony w dodatkową dwuportową kartę sieciową Ethernet obsługującą prędkości transmisji 10GbE oraz 25GbE na port (interfejs SFP+/SFP28).

2.5.4. Wyposażenie optyczne: W ramach dostawy Wykonawca zobowiązany jest dostarczyć minimum 2 sztuki oryginalnych, w pełni kompatybilnych z oferowaną kartą rozszerzeń wkładek światłowodowych wielomodowych (Transceiver) standardu 25GbE SR SFP28.

2.5.5. Urządzenie musi umożliwiać opcjonalne dodanie minimum 2 portów Fibre Channel 16/32Gb lub dodatkowych portów Ethernet 10/25Gb.

2.5.6. Urządzenie musi umożliwiać udostępnianie zasobów po standardowych protokołach sieciowych oraz obsługiwać deduplikację na źródle.

2.6. Redundancja

2.6.1. Urządzenie musi być wyposażone w minimum dwa nadmiarowe, wydajne zasilacze typu hot-plug.

2.6.2. Układ chłodzenia w pełni nadmiarowy, oparty na wentylatorach typu hot-swap.

3. Logika Backupowa, Deduplikacja i DR (Disaster Recovery)

3.1. Wydajność

3.1.1. Urządzenie musi osiągać w maksymalnej konfiguracji wydajność backupu co najmniej 25 TB/h (dane podawane przez producenta), dopuszcza się osiągnięcie tej wydajności z wykorzystaniem technologii deduplikacji na źródle (np. OST, DD Boost, Catalyst, Veeam Data Mover).

3.1.2. Architektura systemu musi zapewniać wysoką wydajność niezależnie od stopnia zapełnienia przestrzeni dyskowej (do poziomu rekomendowanego przez producenta).

3.1.3. Urządzenie musi pozwalać na jednoczesną obsługę minimum 250 strumieni (zapis, odczyt, replikacja).

3.2. Sposób udostępniania zasobów

3.2.1. Urządzenie musi umożliwiać jednoczesny dostęp do pojemności poprzez natywne protokoły deduplikacji dla wspieranych aplikacji backupowych przez interfejsy Ethernet.

3.2.2. Oferowane urządzenie musi obsługiwać deduplikację globalną dla danych otrzymywanych z różnych źródeł.

3.2.3. Oferowane urządzenie musi mieć możliwość emulacji napędów taśmowych LTO oraz emulacji bibliotek taśmowych.

3.3. Deduplikacja danych

3.3.1. Urządzenie musi zapewniać sprzętowo-programową deduplikację danych. Dopuszcza się deduplikację realizowaną w trybie „in-line” (w locie) lub z wykorzystaniem wydzielonej, wysokowydajnej strefy buforowej (tzw. landing

zone) zapewniającej najszybsze odtwarzanie danych z ostatnich punktów przywracania.

3.3.2. Algorytm deduplikacji musi skutecznie redukować dane pochodzące ze środowisk zwirtualizowanych, bazodanowych i plikowych (z wykorzystaniem bloku o zmiennej lub stałej wielkości w zależności od technologii producenta).

3.3.3. Wszystkie unikalne, zdeduplikowane bloki muszą być poddane kompresji.

3.4. Replikacja danych

3.4.1. Urządzenie musi umożliwiać replikację danych do drugiego urządzenia. Replikacja musi się odbywać przesyłając wyłącznie unikalne fragmenty danych (bloki), które nie znajdują się na docelowym urządzeniu.

3.4.2. Zarządzanie procesem replikacji musi być możliwe bezpośrednio z interfejsu urządzenia lub z poziomu posiadanego oprogramowania backupowego (Veeam).

3.4.3. Musi istnieć możliwość ograniczenia pasma (throttling) używanego do replikacji.

3.5. Szyfrowanie danych

3.5.1. Urządzenie musi posiadać funkcjonalność szyfrowania danych w spoczynku (Data-at-Rest) z użyciem algorytmu AES-256.

3.6. Usuwanie przeterminowanych danych

3.6.1. Urządzenie musi realizować proces zwalniania przestrzeni (usuwania przeterminowanych danych) w sposób niepowodujący krytycznego wpływu na bieżące okna backupowe i procesy odtwarzania.

3.7. Sposób zarządzania i bezpieczeństwo dostępu

3.7.1. Zarządzanie urządzeniem musi odbywać się poprzez dedykowany interfejs graficzny dostępny z przeglądarki internetowej, umożliwiający podgląd stanu zdrowia, zajętości, wydajności oraz konfigurację alertów e-mail.

3.7.2. Dostęp do interfejsu graficznego musi wspierać logowanie wieloskładnikowe (MFA/2FA). Dodatkowo, przy operacjach niszczących dane, system musi posiadać mechanizm zabezpieczający przed ich przypadkowym/celowym usunięciem przez skompromitowane konto (np. podwójna autoryzacja, mechanizmy immutability).

3.8. Kompatybilność i Integracja z Veeam

3.8.1. Urządzenie musi posiadać formalne wsparcie dla systemu Veeam Backup & Replication, udokumentowane statusem „Veeam Ready” (w kategoriach Repository, a opcjonalnie Integrated/Object).

3.8.2. Oferowane rozwiązanie musi zapewniać:

- a) Natywną integrację z Veeam Data Mover lub obsługę protokołów zaawansowanych (np. Catalyst, DD Boost, Fast Clone, S3 Object Lock) w celu przyspieszenia operacji syntetycznych pełnych kopii zapasowych.
- b) Obsługę mechanizmów zapewniających niezmiennność danych (Immutability), zabezpieczających kopie przed modyfikacją przez ataki typu Ransomware.

3.9. Integracja z magazynami S3 i Macierzami

3.9.1. Urządzenie lub dostarczone oprogramowanie musi posiadać możliwość archiwizacji (tieringu) starszych kopii zapasowych na obiektywne systemy pamięci masowej (S3), lokalne lub chmurowe o sumarycznej pojemności co najmniej 400TB.

3.9.2. Zamawiający wymaga, aby zaoferowane rozwiązanie (sprzęt i/lub oprogramowanie) umożliwiało wykonanie kopii zapasowej/migawek posiadanej macierzy HPE Nimble o pojemności 21 TB Raw, zgodnie z najlepszymi praktykami ochrony danych (np. za pomocą integracji Veeam Storage API dla HPE Nimble).

3.9.3. Kopie te stanowić mają dodatkową linię ochrony oraz zabezpieczenie materiału dowodowego, w celu dochowanie należytej staranności dla zapewnienia zgodności z UKSC, RODO, UZK, DORA.

3.10. Ochrona przed Ransomware (Niezmienność Danych - Data Immutability)

3.10.1. System musi zapewniać mechanizm tzw. „twardej retencji” (WORM - Write Once Read Many / Immutability) na poziomie sprzętowym lub repozytorium obiektywego (S3 Object Lock). Rozwiązanie musi gwarantować, że nawet w przypadku przejęcia kontroli nad serwerem Veeam, intruz nie będzie w stanie usunąć zablokowanych punktów przywracania przed upływem określonego czasu.

3.11. Disaster Recovery

3.11.1. Urządzenie musi posiadać nielimitowaną licencję na replikację danych pomiędzy dwoma systemami tego samego producenta.

3.11.2. Ruch replikacyjny przesyłany przez sieć WAN musi być szyfrowany (np. AES-256 / TLS).

4. Serwis, Wsparcie Techniczne i Gwarancja Ochrony Danych (DMR)

4.1. Zamawiający wymaga wsparcia technicznego producenta na okres minimum 3 lat (36 miesięcy), w trybie 24x7x365.

4.2. Zdalna odpowiedź inżyniera musi nastąpić maksymalnie do 2 godzin od zgłoszenia awarii krytycznej. Ewentualne naprawy sprzętowe realizowane będą w miejscu instalacji (On-site).

4.3. Klauzula DMR (Defective Media Retention): W przypadku awarii nośnika danych, uszkodzony podzespół pozostaje własnością Zamawiającego bez prawa producenta do żądania jego zwrotu.

4.4. W okresie gwarancji Zamawiający musi posiadać bezpłatne prawo do instalowania aktualizacji firmware i oprogramowania z portalu producenta.

5. Wymogi Wdrożeniowe

5.1. Wykonawca dostarczy, zamontuje i podłączy sprzęt.

5.2. Wykonawca zaktualizuje firmware do wersji zalecanej, skonfiguruje sieć, agregację portów i separację ruchu VLAN.

5.3. Wykonawca przeprowadzi integrację urządzenia z systemem Veeam Backup & Replication, skonfiguruje polityki retencji (w tym Immutability) oraz optymalizację strumieni danych.

5.4. Warunkiem odbioru będą testy wydajności, testy wysokiej dostępności (odłączenie ścieżek sieciowych/zasilania) oraz pomyślny test Instant VM Recovery uruchamiający VM w czasie krótszym niż 5 minut.

5.5. Wykonawca dostarczy dokumentację powykonawczą i przeprowadzi instruktaż stanowiskowy dla minimum 2 administratorów.

6. Wymagania Wobec Zespołu Inżynieryjnego

6.1. Wykonawca skieruje do wdrożenia inżyniera posiadającego autoryzowany certyfikat producenta zaoferowanego urządzenia.