ZAŁĄCZNIK NR 4B4

Specyfikacja sprzętu Stare Babice

Spis treści

1. Wstęp

Niniejszy dokument określa minimalne wymagania sprzętu dla platformy informatycznej, która powinna zostać uruchomiona w ramach realizacji projektu pn: „e-usługi między Wisłą a Kampinosem".
Projekt współfinansowany jest przez Unię Europejską ze środków Europejskiego Funduszu Rozwoju regionalnego w ramach Regionalnego Programu Operacyjnego Województwa Mazowieckiego.
Zgodnie z wnioskiem o dofinansowanie przedmiotem projektu jest rozbudowa platformy informatycznej oraz modernizacja infrastruktury sprzętowej. W ramach niniejszej części zamówienia przewiduje się dostawę, montaż i uruchomienie poniżej przedstawionego sprzętu komputerowego.
Jeśli to nie wynika z innych zapisów gwarancja na sprzęt wynosi 3 lata.

2. Serwer wraz z oprogramowaniem do wirtualizacji – 2 szt.

Komponent	Minimalne wymagania
Obudowa	Obudowa Rack o wysokości max 2U z możliwością instalacji do 8 dysków 3.5" HotPlug wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych oraz organizatorem do kabli. Posiadająca dodatkowy przedni panel zamykany na klucz, chroniący dyski twarde przed nieuprawnionym wyjęciem z serwera.
Płyta główna	Płyta główna z możliwością zainstalowania minimum dwóch procesorów ośmio, dziesięcio, dwunasto lub czternastordzeniowych. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym.
Chipset	Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych
Procesor	Dwa procesory min. dziesięciordzeniowe klasy x86 dedykowane do pracy z zaoferowanym serwerem umożliwiający osiągnięcie wyniku min. 849 punkty w teście SPECint_rate_base2006 dostępnym na stronie www.spec.org w konfiguracji dla 2 dwóch procesorów dla oferowanego rozwiązania.
Pamięć RAM	192 GB pamięci RAM typu RDIMM o częstotliwości pracy 2400MHz. Płyta powinna obsługiwać do min. 384GB pamięci RAM, na płycie głównej powinno znajdować się minimum 12 slotów przeznaczonych dla pamięci. Możliwe zabezpieczenia pamięci: Memory Rank Sparing, Memory Mirror, Lockstep
Sloty PCI Express	Min. 2 sloty x16 generacji 3 Min. 1 slot x8 generacji 3, Min. 1 slot x1 generacji 2, Min. 1 slot x8 generacji 2
Karta graficzna	Zintegrowana karta graficzna umożliwiająca rozdzielczość min. 1280x1024
Wbudowane porty	min. 3 porty USB 2.0 oraz 2 porty USB 3.0 , 4 porty RJ45, 2 porty VGA (1 na przednim panelu obudowy, drugi na tylnym), min. 1 port RS232
Interfejsy sieciowe	Wbudowana czteroportowa karta Gigabit Ethernet. Dodatkowa karta czteroportowa Gigabit Ethernet. Dodatkowo zainstalowana jedna karta (1) dwuportowa 8Gbit FC w wolne złącze PCI-E.
Wewnętrzny moduł SD	Możliwość instalacji wewnętrznego modułu dedykowanego dla hypervisora wirtualizacyjnego, wyposażonego w 2 jednakowe nośniki typu flash z możliwością konfiguracji zabezpieczenia RAID 1 z poziomu BIOS serwera, rozwiązanie nie może powodować zmniejszenia ilości wnęk na dyski twarde.
Kontroler dysków	Sprzętowy kontroler dyskowy, umożliwiający obsługę dysków z prędkościami transferu 3, 6, 12 Gb/s; umożliwiający skonfigurowanie na wewnętrznej pamięci dyskowej

	zabezpieczeń RAID: 0, 1, 5, 6, 10, 50, 60. Wyposażony w min. 1GB pamięci cache.
Wewnętrzna pamięć masowa	Możliwość instalacji wewnętrznej pamięci masowej typu SATA, NearLine SAS, SAS, SSD oraz SED dostępnych w ofercie producenta serwera. Zainstalowane dwa dyski twarde o pojemności min. 300 GB, 15K RPM. Dyski fabrycznie skonfigurowane w RAID1.
System diagnostyczny	Panel LCD lub LED umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS'u, zasilaniu oraz temperaturze.
Zasilacze	Dwa redundantne zasilacze o mocy maks. 750W każdy, pracujące w trybie (1+1)
Wentylatory	Minimum 5 redundantnych wentylatorów
System Operacyjny	Fabrycznie zainstalowany system Windows Server 2016 Standard lub równoważny spełniające wymagania na parametry serwera
Bezpieczeństwo	Zintegrowany z płytą główną moduł TPM. Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą.
Karta zarządzająca	Niezależna od zainstalowanego systemu operacyjnego, zintegrowana z płytą główną lub jako dodatkowa karta rozszerzeń (Zamawiający dopuszcza zastosowanie karty instalowanej w slocie PCI Express jednak nie może ona powodować zmniejszenia minimalnej ilości wymaganych slotów w serwerze), posiadająca minimalną funkcjonalność: - komunikacja poprzez interfejs RJ45 - podstawowe zarzadzanie serwerem poprzez protokół IPMI 2.0, DCMI 1.5, SNMP, VLAN tagging - wbudowana diagnostyka - wbudowane narzędzia do instalacji systemów operacyjnych - dostep poprzez interfejs graficzny Web karty oraz z linii poleceń - monitorowanie temperatury oraz zużycia energii przez serwer w czasie rzeczywistym - lokalna oraz zdalna konfiguracja serwera - wsparcie dla IPv4 i IPv6 Możliwość rozbudowy funkcjonalności karty o automatyczne przywracanie ustawień serwera, kart sieciowych, BIOS, wersji firmware w przypadku awarii i wymiany któregoś z komponentów z dedykowanej pamięci flash (w tym kontrolera RAID, kart sieciowych, płyty głównej).
Gwarancja	Trzy lata gwarancji realizowanej w miejscu instalacji sprzętu, z czasem reakcji do końca następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii w trybie 24x7x365 poprzez ogólnopolską linię telefoniczną producenta. Uszkodzone dyski twarde pozostają własnością Zamawiającego. Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia, oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji.
	Firma serwisująca musi posiadać ISO 9001:2008 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta serwera – dokumenty potwierdzające załączyć do oferty.
Certyfikaty	Serwer musi być wyprodukowany zgodnie z normą ISO-9001 oraz ISO-14001. Serwer musi posiadać deklaracja CE. Oferowany sewer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows" dla systemów Microsoft Windows Server 2012, Microsoft Windows Server 2012 R2, Microsoft Windows Server 2016.
Dokumentacja	Zamawiający wymaga dokumentacji w języku polskim lub angielskim. Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.

Oprogramowanie do wirtualizacji

Licencje muszą umożliwiać uruchamianie wirtualizacji na serwerach fizycznych o łącznej liczbie sześciu procesorów oraz jednej konsoli do zarządzania całym środowiskiem.

Nie przewidywana jest rozbudowa środowiska ponad tę liczbę.

Wszystkie licencje powinny być dostarczone wraz z trzy-letnim wsparciem, świadczonym przez producenta będącego licencjodawcą oprogramowania na pierwszym, drugim i trzecim poziomie, które powinno umożliwiać zgłaszanie problemów 7 dni w tygodniu przez 24h na dobę / 5 dni w tygodniu przez 12h na dobę.

Wymagania techniczne dot. oprogramowania

Konsolidacja

- Warstwa wirtualizacji musi być rozwiązaniem systemowym tzn. musi być zainstalowana bezpośrednio na sprzęcie fizycznym i nie może być częścią innego systemu operacyjnego.
- Warstwa wirtualizacji nie może dla własnych celów alokować więcej niż 200MB pamięci operacyjnej RAM serwera fizycznego.
- Rozwiązanie musi zapewnić możliwość obsługi wielu instancji systemów operacyjnych na jednym serwerze fizycznym. Wymagana jest możliwość przydzielenia maszynie większej ilości wirtualnej pamięci operacyjnej niż jest zainstalowana w serwerze fizycznym oraz większej ilości przestrzeni dyskowej niż jest fizycznie dostępna.
- Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych z możliwością dostępu do 4TB pamięci operacyjnej.
- Oprogramowanie do wirtualizacji musi zapewnić możliwość przydzielenia maszynom wirtualnym do 128 procesorów wirtualnych.
- Rozwiązanie musi umożliwiać łatwą i szybką rozbudowę infrastruktury o nowe usługi bez spadku wydajności i dostępności pozostałych wybranych usług.
- Rozwiązanie musi w możliwie największym stopniu być niezależne od producenta platformy sprzętowej.
- Rozwiązanie musi wspierać następujące systemy operacyjne: Windows XP, Windows Vista , Windows NT, Windows 2000, Windows Server 2003, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, SLES 11, SLES 10, SLES9, SLES8, Ubuntu 7.04, RHEL 5, RHEL 4, RHEL3, RHEL 2.1, Solaris wersja 10 dla platformy x86, NetWare 6.5, NetWare 6.0, NetWare 6.1, Debian, CentOS, FreeBSD, Asianux, Ubuntu 7.04, SCO OpenServer, SCO Unixware, Mac OS X.
- Rozwiązanie musi zapewniać sprzętowe wsparcie dla wirtualizacji zagnieżdżonej, w szczególności w zakresie możliwości zastosowania trybu XP mode w Windows 7 a także instalacji wszystkich funkcjonalności w tym Hyper-V pakietu Windows Server 2012 na maszynie wirtualnej.
- Rozwiązanie musi posiadać centralną konsolę graficzną do zarządzania środowiskiem serwerów wirtualnych. Konsola graficzna musi być dostępna poprzez dedykowanego klienta i za pomocą przeglądarek, minimum IE i Firefox.
- Dostęp przez przeglądarkę do konsoli graficznej musi być skalowalny tj. powinien umożliwiać rozdzielenie komponentów na wiele instancji w przypadku zapotrzebowania na dużą liczbę jednoczesnych dostępów administracyjnych do środowiska.

- Rozwiązanie musi zapewniać zdalny i lokalny dostęp administracyjny do wszystkich serwerów fizycznych poprzez protokół SSH, z możliwością nadawania uprawnień do takiego dostępu nazwanym użytkownikom bez konieczności wykorzystania konta *root*.
- Rozwiązanie musi umożliwiać składowanie logów ze wszystkich serwerów fizycznych i konsoli zarządzającej na serwerze *Syslog*. Serwer *Syslog* w dowolnej implementacji musi stanowić integralną część rozwiązania.
- Rozwiązanie musi zapewnić możliwość monitorowania wykorzystania zasobów fizycznych infrastruktury wirtualnej i zdefiniowania alertów informujących o przekroczeniu wartości progowych.
- Rozwiązanie musi umożliwiać integrację z rozwiązaniami antywirusowymi firm trzecich w zakresie skanowania maszyn wirtualnych z poziomu warstwy wirtualizacji.
- Rozwiązanie musi zapewniać możliwość konfigurowania polityk separacji sieci w warstwie trzeciej, tak aby zapewnić oddzielne grupy wzajemnej komunikacji pomiędzy maszynami wirtualnymi.
- Oprogramowanie do wirtualizacji musi zapewnić możliwość wykonywania kopii zapasowych instancji systemów operacyjnych oraz ich odtworzenia w możliwie najkrótszym czasie.
- Kopie zapasowe muszą być składowane z wykorzystaniem technik de-duplikacji danych.
- Musi istnieć możliwość odtworzenia pojedynczych plików z kopii zapasowej maszyny wirtualnej przez osoby do tego upoważnione bez konieczności nadawania takim osobom bezpośredniego dostępu do głównej konsoli zarządzającej całym środowiskiem.
- Mechanizm zapewniający kopie zapasowe musi być wyposażony w system cyklicznej kontroli integralności danych. Ponadto musi istnieć możliwość przywrócenia stanu repozytorium kopii zapasowych do punktu w czasie, kiedy wszystkie dane były integralne w przypadku jego awarii.
- Oprogramowanie do wirtualizacji musi zapewnić możliwość wykonywania kopii migawkowych instancji systemów operacyjnych na potrzeby tworzenia kopii zapasowych bez przerywania ich pracy z możliwością wskazania konieczności zachowania stanu pamięci pracującej maszyny wirtualnej.
- Oprogramowanie do wirtualizacji musi zapewnić możliwość klonowania systemów operacyjnych wraz z ich pełną konfiguracją i danymi.
- Oprogramowanie zarządzające musi posiadać możliwość przydzielania i konfiguracji uprawnień z możliwością integracji z usługami katalogowymi, w szczególności: Microsoft Active Directory, Open LDAP.
- Platforma wirtualizacyjna musi umożliwiać zastosowanie w serwerach fizycznych procesorów o dowolnej ilości rdzeni.
- Rozwiązanie musi umożliwiać tworzenie jednorodnych wolumenów logicznych o wielkości do 62TB.
- Rozwiązanie musi zapewniać możliwość dodawania zasobów w czasie pracy maszyny wirtualnej, w szczególności w zakresie ilości procesorów, pamięci operacyjnej i przestrzeni dyskowej.
- Rozwiązanie musi posiadać wbudowany interfejs programistyczny (API) zapewniający pełną integrację zewnętrznych rozwiązań wykonywania kopii zapasowych z istniejącymi mechanizmami warstwy wirtualizacyjnej.
- Rozwiązanie musi umożliwiać wykorzystanie technologii 10GbE w tym agregację połączeń fizycznych do minimalizacji czasu przenoszenia maszyny wirtualnej pomiędzy serwerami fizycznymi.
- Rozwiązanie musi zapewniać możliwość replikacji maszyn wirtualnych z dowolnej pamięci masowej w tym z dysków wewnętrznych serwerów fizycznych na dowolną pamięć masową w tym samym lub oddalonym ośrodku przetwarzania.

- Rozwiązanie musi gwarantować współczynnik RPO na poziomie minimum 5 minut
- Czas planowanego przestoju usług związany z koniecznością prac serwisowych (np. rekonfiguracja serwerów, macierzy, switchy) musi być ograniczony do minimum.
- Oprogramowanie do wirtualizacji musi obsługiwać przełączenie ścieżek SAN (bez utraty komunikacji) w przypadku awarii jednej ze ścieżek.
- Oprogramowanie do wirtualizacji musi obsługiwać przełączenie ścieżek LAN (bez utraty komunikacji) w przypadku awarii jednej ze ścieżek.
- System musi mieć możliwość uruchamiania fizycznych serwerów z centralnie przygotowanego obrazu poprzez protokół PXE.

Wysoka dostępność

- Rozwiązanie musi mieć możliwość przenoszenia maszyn wirtualnych w czasie ich pracy pomiędzy serwerami fizycznymi, pamięciami masowymi niezależnie od dostępności współdzielonej przestrzeni dyskowej, różnymi rodzajami wirtualnych przełączników sieciowych.
- Musi zostać zapewniona odpowiednia redundancja i nadmiarowość zasobów tak by w przypadku awarii np. serwera fizycznego usługi na nim świadczone zostały automatycznie przełączone na inne serwery infrastruktury.
- Rozwiązanie musi umożliwiać łatwe i szybkie ponowne uruchomienie systemów/usług w przypadku awarii poszczególnych elementów infrastruktury.
- Rozwiązanie musi zapewnić bezpieczeństwo danych mimo poważnego uszkodzenia lub utraty sprzętu lub oprogramowania.
- Rozwiązanie musi zapewniać mechanizm bezpiecznego, bezprzerwowego i automatycznego uaktualniania warstwy wirtualizacyjnej wliczając w to zarówno poprawki bezpieczeństwa jaki zmianę jej wersji.
- Rozwiązanie musi posiadać co najmniej 2 niezależne mechanizmy wzajemnej komunikacji między serwerami oraz z serwerem zarządzającym, gwarantujące właściwe działanie mechanizmów wysokiej dostępności na wypadek izolacji sieciowej serwerów fizycznych lub partycjonowania sieci.
- Decyzja o próbie przywrócenia funkcjonalności maszyny wirtualnej w przypadku awarii lub niedostępności serwera fizycznego powinna być podejmowana automatycznie, jednak musi istnieć możliwość określenia przez administratora czasu po jakim taka decyzja jest wykonywana.
- Rowiązanie musi zapewniać pracę bez przestojów dla wybranych maszyn wirtualnych (o maksymalnie dwóch procesorach wirtualnych), niezależnie od systemu operacyjnego oraz aplikacji, podczas awarii serwerów fizycznych, bez utraty danych i dostępnosci danych podczas awarii serwerów fizycznych.

Równoważenie obciążenia i przestoje serwisowe

- Czas planowanego przestoju usług związany z koniecznością prac serwisowych (np. rekonfiguracja serwerów, macierzy, switchy) musi być ograniczony do minimum. Konieczna jest możliwość przenoszenia usług pomiędzy serwerami fizycznymi, wolumenami dyskowymi, klastrami bez przerywania pracy usług.

3. System do backupu – 1 szt.

Zamawiający wymaga dostarczenia, uruchomienia i wdrożenia systemu backupowego dla systemów operacyjnych otwartych (UNIX/Linux/Windows), w tym również działających w środowiskach wirtualnych. System backupowy obejmuje oprogramowanie backupowe oraz deduplikator spełniające wyspecyfikowane poniżej wymagania.

Wymagania do systemu wykonywania i składowania kopii zapasowych	
1.	Oprogramowanie backupowe nie może mieć ograniczeń co do ilości backupowanych serwerów, baz danych , laptopów. System backupowy stworzony w oparciu o dostarczone oprogramowanie backupowe powinien umożliwiać zapis/odczyt danych na wewnętrzną przestrzeń dyskową Master Servera (min. 1TB netto) oraz na deduplilkator (wymagane zalicencjonowanie min. 3TB netto) - zapis/odczyt danych powinien być realizowany bezpośrednio z zabezpieczanego serwera na deduplikator. Oferowane rozwiązanie (przyszła rozbudowa) musi mieć możliwość replikacji do drugiego bliźniaczego rozwiązania znajdującego się w zdalnym ośrodku zgodnie z wymaganiami przedstawionymi w dalszej części. Oferowane oprogramowanie backupowe oraz deduplikator musi pochodzić od jednego producenta.
2.	Master Serwer oferowanego systemu powinien być zainstalowany na serwerze wirtualnym (VMware), oprogramowanie powinno zostać dostarczone w postaci IMAGE'u. Oprogramowanie powinno umożliwiać składowanie danych backupowych
3.	Oprogramowanie backupowe musi wspierać (wymagane wsparcie producenta) następujące systemy operacyjne: Windows (także Microsoft Cluster) , Linux (Red Hat, SUSE, Debian, CentOS, Ubnutu), Solaris, AIX, HP-UX, Mac OS X, Novell OES, FreeBSD. Backup zasobów plików z powyższych systemów musi podlegać de-duplikacji ze zmiennym blokiem na zabezpieczanej maszynie zgodnie z wymaganiami powyżej.
4.	Oprogramowanie backupowe musi wspierać (wymagane wsparcie producenta) backup online następujących baz danych i aplikacji: MS Exchange, MS SQL, Oracle, IBM DB2, Lotus Notes, SharePoint, SAP, Sybase, VMware, HyperV. Backup z powyższych baz danych i aplikacji musi podlegać de-duplikacji ze zmiennym blokiem na zabezpieczanej maszynie zgodnie z wymaganiami zawartymi w niniejszym dokumencie.
5.	W przypadku zabezpieczania baz danych i aplikacji musi istnieć możliwość pobierania kopii zapasowej kilkoma strumieniami jednocześnie (minimum 10 jednoczesnych strumieni).
6.	W przypadku zabezpieczania systemu Exchange 2013 musi istnieć możliwość backupu całego obrazu bazy danych i jednocześnie odtworzenia pojedynczego maila bez konieczności odtwarzania całej bazy danych.
7.	W przypadku zabezpieczania systemu Sharepoint musi istnieć opcjonalna (licencja nie jest wymagana) możliwość odtworzenia pojedynczego elementu systemu Sharepoint bez konieczności odtwarzania całego środowiska SharePoint.
8.	Oferowane rozwiązanie musi zabezpieczać zde-duplikowane dane Windows 2012 bez konieczności przywracania danych Windows 2012 do postaci oryginalnej (nie zde-duplikowanej).
9.	Zabezpieczane serwery muszą być backupowane bezpośrednio na medium backupowe (przestrzeń dyskową Master Servera lub oferowany deduplikator – wymagane obie możliwości) bez pośrednictwa jakichkolwiek innych urządzeń / serwerów. Powyższe wymaganie dotyczy to backupów lokalnych, zdalnych jak również backupu laptopów
10.	Oprogramowanie backupowe musi umożliwiać: • backup pojedynczych plików • backup całych systemów plików

	• backup baz danych w trakcie ich normalnej pracy • backup ustawień systemu operacyjnego Windows. • backup całych obrazów maszyn wirtualnych systemu VMWare backup całych obrazów maszyn wirtualnych systemu HyperV
11.	Rozwiązanie backupowe musi umożliwiać transfer danych bezpośrednio ze zdalnych oddziałów bez konieczności instalacji jakiegokolwiek sprzętu w oddziale. Backup zdalnych oddziałów musi działać poprawnie nawet w przypadku opóźnienia 2 sekund w sieci WAN oraz jednocześnie utraty pakietów na poziomie 60%. Powyższa funkcjonalność wymagana jest dla następujących typów danych: • backup pojedynczych plików • backup całych systemów plików • backup baz danych w trakcie ich normalnej pracy
12.	• Rozwiązanie backupowe nie może wymagać jakichkolwiek czynności ze strony personelu w oddziale. Rozwiązanie backupowe musi działać zakładając, że pracownicy oddziału nie są zaangażowani w obsługę systemu backupowego.
13.	Rozwiązanie backupowe musi być w pełni konfigurowalne z konsoli znajdującej się w centrali. W szczególności backupy maszyn w oddziałach (bazy, pliki) czy też backupy laptopów muszą być konfigurowalne z poziomu centralnej konsoli bez konieczności logowania się na zabezpieczaną maszynę.
14.	Rozwiązanie backupowe musi mieć możliwość odtworzenia • plików • baz danych na docelowa maszynę w oddziale z poziomu centralnej konsoli systemu backupowego. Nie może być wymagane logowanie się na odtwarzaną maszynę celem odtworzenia danych z systemu backupowego.
15.	W przypadku wyboru odtwarzania całego systemu plików (dysk E:\ w Windows, cały file system w Linux/UNIX) dla systemów Windows / Linux / UNIX, rozwiązanie backupowe musi automatycznie i samodzielnie porównać pliki znajdujące się w backupie i pliki znajdujące się odtwarzanej maszynie i odtworzyć tylko brakujące pliki. W przypadku wyboru odtwarzania całego dysku / całego systemu plików, rozwiązanie backupowe nie może odczytywać z medium backupowe ani przesyłać do odtwarzanej maszyny plików które znajdowały się zarówno w backupie jak i na odtwarzanej maszynie. Rozwiązanie backupowe musi samodzielnie ustalić których plików brakuje na odtwarzanym dysku zabezpieczanej maszyny i tylko te pliki odtworzyć.
16.	W celu minimalizacji ilości przesyłanych danych, oferowane rozwiązanie musi mieć możliwość przesyłania odtwarzanych danych z medium backupowego do docelowego serwera w postaci skompresowanej, tak aby odtwarzane dane były rozkompresowane na docelowym serwerze przez agenta oferowanego systemu.
17.	Oferowane rozwiązanie musi być odporne na: • Opóźnienia na łączu między oddziałem a ośrodkiem regionalnym (do 2s) • Zrywanie łącza między oddziałem a ośrodkiem regionalnym (do 30 min) Utraty pakietów (60%)
18.	Oferowane oprogramowanie backupowe musi wykorzystywać technologię deduplikacji bazującej na podziale danych (plików, baz danych, obrazów maszyn wirtualnych) na bloki o zmiennej długości. System musi się dopasowywać do struktury dokumentu zapewniając podział na bloki o różnej długości w ramach pojedynczego dokumentu. • Podział na bloki musi następować bezpośrednio na zabezpieczanym serwerze.
19.	De-duplikacja musi również generować zmienny blok w przypadku backupu pojedynczego dokumentu. Bloki wysyłane w trakcie backupu pojedynczego dokumentu (z zabezpieczanej

	maszyny do medium de-duplikacyjnego) muszą być różnej długości jednak nie większej niż 32KB.
20.	Każdy backupowany dokument w trakcie pojedynczej sesji musi być dzielony na bloki o zmiennej długości nie większej niż 32KB.
21.	Oprogramowanie backupowe musi backupować (przesyłać do serwera backupu) tylko unikalne bloki nie znajdujące się na docelowym urządzeniu, skracając czas backupu, obciążenie procesora i zmniejszając ruch w sieci WAN / LAN.
22.	Włączenie funkcjonalności deduplikacji nie może generować wymogu instalacji dodatkowych modułów programowych po stronie klienckiej lub serwera backupowego.
23.	Oprogramowanie backupowe nie może odczytywać tych plików z systemu dyskowego, które się nie zmieniły w stosunku do ostatniego backupu. Raz zbackupowany plik nie może być nigdy więcej odczytany chyba, że zmieni się jego zawartość.
24.	Oprogramowanie backupowe musi wykonywać zawsze tylko logicznie pełne backupy systemu plików. Z zabezpieczanego systemu plików muszą odczytywane tylko nowe lub zmienione pliki, do appliance'u backupowego muszą być wysyłane dane po de-duplikacji, natomiast sam backup musi być logicznie pełnym backupem. W wewnętrznej strukturze musi być przechowywana informacja o każdym backupie i należących do niego danych (blokach). Odtworzenie jakichkolwiek danych plikowych musi być pojedynczym zadaniem identycznym z odtworzeniem danych z pełnego backupu.
25.	W konsoli oprogramowania backupowego musi być możliwość definiowania ważności danych (backupów) na podstawie kryteriów czasowych (dni, miesiące, lata). Po okresie ważności backupy musza być automatycznie usunięte.
26.	Oferowanie oprogramowanie backupowe musi mieć możliwość tworzenia z poziomu GUI (konsoli graficznej) polityk typu Dziadek – ojciec –syn, to znaczy utworzenia polityki w której zdefiniowano: • Czas przechowywania backupów dziennych • Czas przechowywania backupów tygodniowych • Czas przechowywania backupów miesięcznych Czas przechowywania backupów rocznych
27.	Oferowane rozwiązanie musi umożliwiać tworzenie wykluczeń, czyli elementów nie podlegających backupowi w ramach zadania backupowego. Musi istnieć możliwość tworzenia wykluczeń dla dowolnej kombinacji następujących elementów: • wybranych typów plików, np. dla plików z rozszerzeniem mp3 • dla całych katalogów (np.: c:\windows). • dla pojedynczych plików
28.	• Oferowane rozwiązanie musi mieć możliwość zdefiniowania aby ostatni backup dowolnego zbioru danych nigdy się nie przeterminował. Oznacza to, że jeśli dany zasób nie jest backupowany to automatycznie ostatnie ważny backup tego zasobu jest trzymany bezterminowo. Jedynie administrator może zdecydować o jego usunięciu.
29.	Oferowane urządzenie musi mieć możliwość replikacji danych z analogicznym rozwiązanem dostarczanym w postaci fizycznego appliance'u w obu kierunkach jednocześnie: • appliance fizyczny w ośrodku B do appliance wirtualny w ośrodku A • appliance wirtualny w ośrodku A do appliance fizyczny w ośrodku B Replikacji muszą podlegać tylko bloki unikalne, nieznajdujące się na docelowym urządzeniu. Musi istnieć możliwość zdefiniowania kalendarza replikacji między appliance'mi oraz zdefiniowania które zadania backupowe podlegają replikacji.
30.	Konsola zarządzająca systemem backupowym musi integrować się z Active Directory. Musi być możliwość przydzielania użytkownikom i grupom Active Directory dostępnych ról (min,

	administrator, monitoring, tylko wykonywanie odtworzeń) w systemie backupowym.
31.	Konsola musi udostępniać raporty dotyczące zajętości przestrzeni przeznaczonej na de-duplikaty.
32.	Bloki przesyłane z zabezpieczanych serwerów do appliance'a backupowego lub do oferowanego de-duplikatora muszą być kompresowane i szyfrowane algorytmem z kluczem minimum 256-bitowym.
33.	Musi istnieć możliwość szyfrowania danych na medium dyskowym przechowującym backupy (de-duplikaty). Ewentualna licencja szyfrowania musi być dostarczona w ramach postępowania.
34.	Wymagana jest autentykacja komunikacji między klientem a serwerem backupu (farmą serwerów) oparta na certyfikatach.
35.	Oprogramowanie backupowe musi pozwalać na odtwarzanie danych poprzez: wybór odtwarzanych danych, odtworzenie danych w jednym kroku.
36.	Oprogramowanie backupowe musi mieć możliwość limitowania wielkości zadania backupowego. Jeśli zadanie backupowe przekroczy zdefiniowaną wielkość wówczas nie może być zapisane w systemie backupowych
37.	Oprogramowanie backupowe musi umożliwiać ograniczenie mocy procesora używanej do wykonywania zdania backupu tak by odpowiednia moc procesora zostawić dla innych zadań.
38.	Rozwiązanie backupowe musi wspierać backup i odtwarzanie środowisk VMware 6.0. Oprogramowanie backupowe musi umożliwiać dla środowisk VMware następujące typy backupu: a. Backup całych maszyn wirtualnych b. Backup pojedynczych, wybranych dysków maszyny wirtualnej vmdk c. Musi istnieć możliwość zastosowania wyrażeń regularnych do określenia które wirtualne dyski VMware mają być backupowane d. W trakcie backupu odczytowi z systemu dyskowego mają podlegać tylko zmienione bloki wirtualnych maszyn systemu VMWare (wymagane wykorzystanie mechanizmu CBT systemu VMWare) e. Wykonywanie backupu obrazó maszyn wirtualnych VMware nie może wymagać bufora dyskowego na kopię obrazów maszyn wirtualnych (plików vmdk) Powyższe metody backupu maszyn wirtualnych muszą podlegać de-duplikacji ze zmiennym blokiem przed wysłaniem danych do medium backupowego zgodnie z wymaganiami dla de-duplikacji powyżej. Powyższe metody backupu muszą być wbudowane w system backupu i w pełni automatyczne bez wykorzystania skryptów/dodatkowych komend.
39.	Oferowany system musi pozwalać na szybkie odtworzenie • całych obrazów maszyn wirtualnych pojedynczych dysków maszyny wirtualnej z backupu całej maszyny wirtualnej
40.	Rozwiązanie backupowe musi umożliwiać odtworzenie obrazów maszyn wirtualnych VMware dostarczając następujące funkcjonalności: a. Odtworzenie całych maszyn wirtualnych musi wykorzystywać mechanizm CBT systemu VMWare – odtwarzane są tylko te bloki wirtualnej maszyny/dysku które uległy zmianie od ostatniego backupu b. Odtworzenie pojedynczych dysków maszyn wirtualnych musi wykorzystywać mechanizm CBT systemu VMWare – odtwarzane są tylko te bloki wirtualnej maszyny/dysku które uległy zmianie od ostatniego backupu c. Odtworzenie pojedynczych plików z backupu obrazu maszyny wirtualnej bez konieczności odtworzenia całej maszyny wirtualnej. Funkcjonalność musi być dostępna dla obrazów maszyn wirtualnych z zainstalowanym systemem operacyjnym Windows oraz Linux. d. Możliwość zamontowania na dowolnym serwerze (fizycznym lub wirtualnym)

	zbackupowanych obrazów maszyn wirtualnych Windows (plików vmdk maszyny wirtualnej Windows). Powyższa metoda nie może fizycznie odtwarzać backupów a jedynie pozwalać na przeglądanie zawartości plików vmdk w backupie z poziomu Eksploratora Plików Windows na dowolnej maszynie. • Powyższe metody odtworzenia muszą być wbudowane w system backupu i w pełni automatyczne bez wykorzystania skryptów/dodatkowych komend.
41.	Rozwiązanie backupowe musi umożliwiać uruchomienie maszyny wirtualnej bezpośrednio z oferowanego deduplikatora bez konieczności odtwarzania (Instant Access).
42.	Oprogramowanie backupowe musi mieć możliwość prezentacji (bez konieczności odtworzenia) zbackupowanych obrazów maszyn wirtualnych VMware (plików vmdk) jako katalogów na maszynie fizycznej w celu ich przeszukiwania (wymagane przeszukiwanie po nazwach plików jak również zawartości plików) z poziomu systemu operacyjnego maszyny fizycznej.
43.	Oprogramowanie backupowe musi mieć możliwość backupu / odtworzenia w trybie „image backup" (backup plików vmdk) maszyn wirtualnych znajdujących się na serwerach VMware ESX bez udziału vCenter.
44.	Oprogramowanie backupowe musi mieć możliwość automatycznego sprawdzania (weryfikacji) zbackupowanych maszyn wirtualnych VMWare. Musi istnieć możliwość ustawienia kalendarza weryfikacji maszyn wirtualnych VMware. Weryfikacja maszyn wirtualnych musi zapewniać minimum: a. Odtworzenie maszyny wirtualnej na zdefiniowanym Data Center / Data Store b. Weryfikacja podstawowych procesów c. Możliwość dołączenia własnego skryptu weryfikującego wybrane elementy maszyny wirtualnej Informacja w konsoli systemu backupu o poprawnej / niepoprawnej weryfikacji maszyny wirtualnej.
45.	Administrator (właściciel) danej maszyny wirtualnej VMware musi mieć możliwość samodzielnego (bez konieczności kontaktu z administratorem backupu czy tez administratorem VMware) odtworzenia pojedynczych plików z dowolnego backupu obrazu jego maszyny wirtualnej.
46.	Oprogramowanie backupowe musi zawsze przechowywać pełne backupy obrazów maszyn wirtualnych środowiska VMware/HyperV dla każdej wykonanej w przeszłości kopii zapasowej. Każdy backup obrazu maszyny wirtualnej musi być backupem pełnym.
47.	Rozwiązanie backupowe musi pozwalać automatyczne polityki backupowe dla: • Folderu • Resource Pool systemu VMware Oznacza to, że dodanie maszyny wirtualnej do folderu, hosta czy resource pooli w systemie VMware spowoduje automatyczne backupowanie dodanej maszyny wirtualnej zgodnie z polityka zdefiniowana dla folderu hosta czy resource pooli w systemie VMware.
48.	Rozwiązanie backupowe musi umożliwiać zdefiniowanie polityk backupowych dostępnych dla administratora systemu VMware z poziomu vCenter. Administrator VMware musi mieć możliwość przyporządkowania nowo tworzonych maszyn wirtualnych do polityk backupowych.
49.	Oferowany system musi automatycznie naprawiać problemy związane ze snapshotami VMware. W przypadku gdy system VMware nie usunie snapshotu, oprogramowanie backupowe musi automatycznie ponawiać usunięcie snapshotu a w przypadku konieczności automatycznie konsolidować maszyny wirtualne VMware
50.	Backup oraz odtworzenie maszyn wirtualnych VMware musi być możliwy z poziomu graficznego interfejsu, linii komend oraz przez REST API
51.	Oprogramowanie backupowe musi umożliwiać dla środowisk Hyper-V: a. Backup pojedynczych plików i baz danych z maszyny wirtualnej ze środka maszyny

	wirtualnej Hyper-V. b. Backup całych maszyn wirtualnych (czyli plików vhd reprezentujących wirtualną maszynę). c. Wykonywanie backupu jak w punkcie b. nie może wymagać bufora dyskowego na kopię obrazów maszyn wirtualnych (plików vhd). d. Wykonywanie backupu jak w punkcie b. musi pozwalać na odtworzenie pojedynczych plików z obrazu maszyny wirtualnej bez konieczności odtworzenia całej maszyny wirtualnej. Funkcjonalność musi dostępna dla obrazów maszyn wirtualnych z zainstalowanym systemem operacyjnym Windows. 1. Dopuszcza się wykonywanie snapshotów vss maszyn wirtualnych i użycie ich w trakcie backupu obrazów maszyn wirtualnych. 2. Powyższe metody backupu muszą być wbudowane w system backupu i w pełni automatyczne bez wykorzystania skryptów/dodatkowych komend. 3. Powyższe metody backupu maszyn wirtualnych muszą podlegać de-duplikacji ze zmiennym blokiem w momencie odczytu danych zgodnie z wymaganiami powyżej.
52.	Oprogramowanie backupowe musi zapewniać spójny backup Exchange / MSSQL przy backupie obrazów maszyn wirtualnych środowiska Hyper-V
53.	Musi istnieć możliwość odtworzenia danych • z zabezpieczanego serwera / komputera z konsoli systemu backupowego
54.	Musi istnieć możliwość odtworzenia: • Pojedynczego pliku Zabezpieczanej bazy danych
55.	Dla systemów Windows 2008, Windows 7 musi istnieć funkcjonalność Bare Metal Recovery automatycznego odtworzenia całego serwera (system operacyjny + ustawienia systemu operacyjnego + dane) w jednym kroku bezpośrednio z oferowanego urządzenia. • Funkcjonalność musi być wbudowana w rozwiązanie backupowe.
56.	W przypadku odtwarzania danych z interfejsu dostępnego na zabezpieczanym serwerze musi istnieć mechanizm autentykacji użytkowników dostępny w dwóch opcjach: • Wbudowany w system backupowy • Zintegrowany z usługami katalogowymi • W przypadku wykorzystania AD, użytkownicy będący w domenie nie muszą się logować do systemu backupu w przypadku konieczności i. odtworzenia danych ii. przeszukania zawartości swoich backupów • wykonania backupu
57.	Dla odtwarzania danych z interfejsu końcowego użytkownika muszą być dostarczone następujące funkcjonalności: • Wyszukiwanie pliku do odtwarzania po i. nazwie pliku ii. początkowym fragmencie nazwy pliku iii. końcowym fragmencie nazwy pliku iv. fragmencie nazwy pliku umiejscowionym gdziekolwiek w pełnej nazwie pliku • Przeglądania zawartości zbackupowanego systemu plików i wybór zasobów do odtworzenia Wybór wersji odtwarzanego pliku / katalogu
58.	Rozwiązanie backupowe musi umożliwiać odtworzenie plików z dowolnego urządzenia (laptop, tablet, smartphone) poprzez przeglądarkę internetową. Odtwarzanie to musi spełniać

	następujące kryteria • Uwierzytelnienia użytkownika • Wyszukiwanie pliku do odtwarzania po i. nazwie pliku ii. początkowym fragmencie nazwy pliku iii. końcowym fragmencie nazwy pliku iv. fragmencie nazwy pliku umiejscowionym gdziekolwiek w pełnej nazwie pliku • Przeglądania zawartości zbackupowanego systemu plików i wybór zasobów do odtworzenia i. Wybór wersji odtwarzanego pliku / katalogu
59.	• W przypadku odtwarzania istniejącego systemu plików (systemu plików który utracił część zasobów) oprogramowanie backupowe musi samo, automatycznie sprawdzać których plików znajdujących się w backupie brakuje na odtwarzanej maszynie a następnie odczytywać z backupu i przesyłać tylko te pliki które znajdują się w backupie a których brakuje na odtwarzanej maszynie.
60.	• Wymagana możliwość doposażenia rozwiązania backup'owego o system wyrzutu danych na nośniki taśmowe realizowany poprzez zastosowanie gotowego modułu (pochodzącego od tego samego producenta)
61.	System backupu musi być dostępny dla backupu i odtwarzania przez 24h na dobę 7 dni w tygodniu. Nie może być jakiegokolwiek przedziału czasowego czy momentu w którym system backupowy nie może wykonywać backupu lub odtwarzania.
62.	System backupu musi mieć możliwość bezpośredniego raportowania o błędach do serwisu producenta
63.	System backupu musi mieć możliwość instalacji agentów jako plików msi. Musi istnieć możliwość automatyzacji agentów poprzez uruchomienie skryptu instalującego agenta na zabezpieczanej maszynie i przyporządkowującego maszynę automatycznie do określonej polityki backupowej.
64.	System backupu musi mieć możliwość automatycznej samo-aktualizacji poprzez automatyczne ściąganie nowych wersji od producenta
65.	System backupu musi mieć możliwość automatycznej aktualizacji oprogramowania agentów wykonywanej bezpośrednio z serwera backupu.
66.	System musi umozliwiać backup serwerów NAS z następującymi funkcjonalnościami: 1. w trakcie backupu z systemu NAS muszą być wysyłane do medium backupowego tylko zmienione pliki od ostatniego backupu 2. w przypadku odtwarzania, uprawnienia użytkowników również są odtwarzane 3. integracja z protokołem NDMP systemów NAS 4. odtworzenie plików z backupu NDMP bezpośrednio na platformę Windows/Linux ew. dodatkowe moduły/licencje dedykowane do backup'u poprzez NDMP nie są w tej chwili wymagane.
67.	Wymagane wsparcie producenta w okresie 3 lat od zakupu umożliwiajace upgrade do najnowszych wersji.

Wymagania dotyczące deduplikatora	
1.	Urządzenie musi być przeznaczone do de-duplikacji i przechowywania kopii zapasowych. Urządzenie musi spełniać wymagania wyspecyfikowane w niniejszej tabeli.

2.	Dostarczone urządzenie musi oferować przestrzeń 17TB netto (powierzchni użytkowej) bez uwzględniania mechanizmów protekcji.
3.	Oferowane urządzenie musi posiadać minimum • 4 porty Ethernet 1 Gb/s (wymagane w urządzeniu), wymagana możliwość obsługi każdym portem Ethernet protokołów CIFS, NFS, de-duplikacja na źródle;
4.	Oferowane urządzenie musi umożliwiać jednoczesny dostęp wszystkimi poniższymi protokołami czyli dla Ethernet: • CIFS, NFS, BOOST/OST urządzenie powinno również umożliwiać jednoczesny dostęp (razem z w/w interfejsami) poprzez • VTL po dołożeniu stosownej licencji (która nie jest przedmiotem niniejszego zapytania) oraz portów FC
5.	Wymagane jest dostarczenie licencji, pozwalającej na jednoczesną obsługę protokołów CIFS, NFS, BOOST/OST do pełnej pojemności urządzenia.
6.	Oferowane pojedyncze urządzenie musi osiągać zagregowaną wydajność protokołami CIFS, NFS: co najmniej 2,5 TB/h (ogólnie dostępne dane podawane przez producenta) oraz co najmniej 10 TB/h z wykorzystaniem de-duplikacji na źródle (ogólnie dostępne dane podawane przez producenta).
7.	Urządzenie musi pozwalać na jednoczesną obsługę minimum 60 strumieni w tym jednocześnie: • zapis danych minimum 35 strumieniami • odczyt danych minimum 10 strumieniami • replikacja minimum 15 strumieniami pochodzących z różnych aplikacji oraz dowolnych protokołów (CIFS, NFS, VTL, OST, BOOST) oraz dowolnych interfejsów (FC, LAN) w tym samym czasie. Wymienione wartości 60 jednoczesnych strumieni dla wszystkich protokołów (czyli jednocześnie 35 dla zapisu, i jednocześnie 10 strumieni dla odczytu i jednocześnie 15 strumieni dla replikacji) musi mieścić w przedziale oficjalnie rekomendowanym i wspieranym przez producenta urządzenia. Wszystkie zapisywane strumienie muszą podlegać globalnej de-duplikacji przed zapisem na dysk (in-line) jak opisano w niniejszej specyfikacji.
8.	Oferowane urządzenie musi mieć możliwość emulacji następujących bibliotek taśmowych: • StorageTek L180 • IBM 3500
9.	Oferowane urządzenie musi mieć możliwość emulacji napędów taśmowych LTO1, LTO2, LTO3, LTO4, LTO5
10.	Urządzenie musi eksportować i importować definicje bibliotek taśmowych. Musi być możliwość eksportu / importu definicji bibliotek taśmowych między różnymi modelami urządzeń producenta.
11.	Urządzenie musi umożliwiać przyporządkowanie minimum 60 napędów do emulowanej pojedynczej biblioteki taśmowej.
12.	Oferowane urządzenie musi de-duplikować dane in-line przed zapisem na nośnik dyskowy. Na wewnętrznych dyskach urządzenia nie mogą być zapisywane dane w oryginalnej postaci (niezdeduplikowanej) z jakiegokolwiek fragmentu strumienia danych przychodzącego do urządzenia.
13.	Technologia de-duplikacji musi wykorzystywać algorytm bazujący na zmiennym, dynamicznym bloku. Algorytm ten musi samoczynnie i automatycznie dopasowywać się do otrzymywanego strumienia danych co oznacza, że urządzenie musi dzielić otrzymany pojedynczy strumień

	danych na bloki o różnej długości, bez konieczności podejmowania czynności mających na celu ustalenie predefiniowanej długości bloków uzywanych do deduplikacji danych określonego typu.
14.	De-duplikacja zmiennym, dynamicznym blokiem oznacza, że wielkość każdego bloku (na jaki są dzielone dane pojedynczego strumienia backupowego) może być inna niż poprzedniego oraz jest indywidualnie ustalana przez algorytm deduplikacji zastosowany w urządzeniu, oferowane urządzenie nie może dzielić jakiegokolwiek pojedynczego strumienia danych backupowych na bloki o ustalonej, tej samej długości
15.	Oferowany produkt musi posiadać obsługę mechanizmów globalnej de-duplikacji dla danych otrzymywanych jednocześnie wszystkimi protokołami (CIFS, NFS, VTL, BOOST/OST) przechowywanych w obrębie całego urządzenia co oznacza, że przechowywany na urządzeniu fragment danych nie może być ponownie zapisany bez względu na to, jakim protokołem zostanie ponownie otrzymany.
16.	Powyższe oznacza również, że oferowany produkt musi również posiadać obsługę mechanizmów globalnej de-duplikacji pomiędzy dowolnymi dwoma (i więcej) wirtualnymi bibliotekami emulowanymi w obrębie tego samego urządzenia. Blok danych otrzymany i zapisany w wirtualnej bibliotece A, nie może zostać ponownie zapisany jeśli trafi do innej wirtualnej biblioteki (wirtualnej biblioteki B) w obrębie tego samego urządzenia (to samo dotyczy udziałów NFS/CIFS).
17.	Przestrzeń składowania zde-duplikowanych danych musi być jedna dla wszystkich protokołów dostępowych, co oznacza zastosowanie pojedynczej bazy deduplikatów bez względu na ilość/rodzaj używanych protokołów dostępowych.
18.	Proces de-duplikacji musi odbywać się in-line – w pamięci urządzenia, przed zapisem danych na nośnik dyskowy. Zapisowi na system dyskowy muszą podlegać tylko unikalne bloki danych nie zapisane jeszcze na system dyskowy urządzenia. Dotyczy to każdego fragmentu przychodzących do urządzenia danych.
19.	Proponowane rozwiązanie nie może w żadnej fazie korzystać (w całości lub częściowo) z bufora na składowanie danych w postaci oryginalnej (niezdeduplikowanej) w celu ich późniejszej deduplikacji (wymagana deduplikacja in-line)
20.	Wszystkie unikalne bloki przed zapisaniem na dysk muszą być kompresowane jedną z metod do wyboru: gz, lz.
21.	Oferowane urządzenie musi wspierać (wymagane formalne wsparcie producenta urządzenia), co najmniej następujące aplikacje: HP Data Protector, VERITAS NetBackup, EMC NetWorker, EMC, Avamar, Oracle RMAN, IBM Data Studio, VMware VDP, SAP HANA STUDIO , Microsoft SQL Server Management Studio, Veeam.
22.	W przypadku współpracy z każdą z poniższych aplikacji: • RMAN (dla ORACLE) • Microsoft SQL Server Management Studio (dla Microsoft SQL) • IBM Data Studio (dla DB2) • SAP BR*Tools (dla SAP/Oracle) • SAP HANA STUDIO (dla SAP HANA) • vShpehre Data Protection 6.0 - VDP (dla VMware) • VERITAS NetBackup • VERITAS BackupExec • HP Data Protector • EMC NetWorker • EMC Avamar • Veeam urządzenie musi umożliwiać de-duplikację na źródle i przesłanie nowych, nie znajdujących się

	jeszcze na urządzeniu bloków poprzez sieć LAN. De-duplikacja danych odbywa się na dowolnym serwerze posiadającym funkcjonalność Media Servera NetBackup'a / klienta Avamar / serwera RMAN / serwera SQL / serwera SAP / serwera DB2/ klienta VDP / klienta systemu NetWorker nie posiadającego licencji Storage Node. De-duplikacja w wyżej wymienionych przypadkach musi zapewniać aby z serwerów do urządzenia były transmitowane poprzez sieć LAN tylko fragmenty danych nie znajdujące się dotychczas na urządzeniu. Wymagana integracja z VDP 6.0 - umożliwiająca zwiększenie przestrzeni obsługiwanej/adresowanej przez VDP 6.0 z 8TB do min. 15TB, wymagane potwierdzenie funkcjonalności (wymaganej integracji) w oficjalnej dokumentacji producenta oferowanego urządzenia oraz dokumentacji VMware.
23.	W przypadku przyjmowania backupów od VERITAS NetBackup, EMC NetWorker, Oracle RMAN, Microsoft MSSQL (przy wykorzystaniu Microsoft SQL Server Management Studio) , IBM DB2 (przy wykorzystaniu IBM Data Studio), SAP/Oracle (przy wykorzystaniu SAP BR*Tools), SAP HANA (przy wykorzystaniu SAP HANA STUDIO), Veeam urządzenie musi umożliwiać de-duplikację na źródle i przesłanie nowych, nieznajdujących się jeszcze na urządzeniu bloków poprzez sieć FC (po dopasażeniu urządzenia w porty FC). De-duplikacja w wyżej wymienionych przypadkach musi zapewniać aby z serwerów do urządzenia były transmitowane poprzez sieć FC tylko fragmenty danych nie znajdujące się dotychczas na urządzeniu.
24.	W przypadku de-duplikacji na źródle poprzez sieć IP (LAN oraz WAN), wymagana możliwość szyfrowania komunikacji kluczem minimum 256 bitów.
25.	Urządzenie musi wspierać de-duplikację na źródle poprzez sieć FC (SAN), po doposażeniu urządzenia w porty FC, minimum dla następujących systemów operacyjnych: • Windows • Linux (RedHat, SuSE) • HP-UX • AIX • Solaris
26.	Dla aplikacji VERITAS NetBackup, EMC NetWorker, urządzenie musi pozwalać na łączenie backupów pełnych i inkrementalnych bez odczytu danych z urządzenia. Zarządzanie łączeniem backupów pełnych i inkrementalnych musi być wykonywane z poziomu aplikacji VERITAS NetBackup, EMC NetWorker
27.	Urządzenie nie może zmniejszać swojej wydajności w czasie przybywania kolejnych danych.
28.	Oferowane urządzenie musi umożliwiać bezpośrednią replikację danych do drugiego urządzenia takiego samego typu. Konfiguracja replikacji musi być możliwa w każdym z trybów: * jeden do jednego * wiele do jednego * jeden do wielu * kaskadowej (urządzenie A replikuje dane do urządznia B, które te same dane replikuje do urządzenia C). Replikacja musi się odbywać w trybie asynchronicznym. Transmitowane mogą być tylko te fragmenty danych (bloki) które nie znajdują się na docelowym urządzeniu. Ewentualna licencja na replikację musi być dostarczona w ramach postępowania.
29.	Urządzenie musi umożliwiać wydzielenie określonych portów Ethernet dedykowanych do replikacji.
30.	W przypadku wykorzystania portów Ethernet do replikacji urządzenie musi umożliwiać przyjmowanie backupów, odtwarzanie danych, przyjmowanie strumienia replikacji, wysyłanie strumienia replikacji tymi samymi portami.
31.	W przypadku replikacji danych między dwoma urządzeniami kontrolowanej przez systemy

	VMware VDP / VERITAS NetBackup / VERITAS BackupExec / HP Data Protector / EMC Avamar / EMC NetWorker muszą być możliwe do uzyskania jednocześnie wszystkie następujące funkcjonalności: • replikacja odbywa się bezpośrednio między dwoma urządzeniami bez udziału serwerów pośredniczących • replikacji podlegają tylko te fragmenty danych, które nie znajdują się na docelowym urządzeniu • replikacja zarządzana jest z poziomu aplikacji backupowej • aplikacja backupowa posiada informację o obydwu kopiach zapasowych znajdujących się w obydwu urządzeniach bez konieczności preprowadzania procesu inwentaryzacji
32.	Oferowane urządzenie musi działać poprawnie przy zapełnieniu danymi na poziomie co najmniej 90%. Dokumentacja urządzenia nie może wskazywać na ew. problemy, obostrzenia, które są efektem zapełnieniu urządzenia zabezpieczanymi danymi, na poziomie mniejszym niż 90%.
33.	Narzut na wydajność związany z replikacją nie może zmniejszyć wydajności urządzenia o więcej niż 10%.
34.	Wymagana możliwość ograniczenia pasma używanego do replikacji między dwoma urządzeniami.
35.	Zdeduplikowane i skompresowane dane przechowywane w obrębie podsystemu dyskowego urządzenia muszą być chronione za pomocą technologii RAID 6.
36.	Każda grupa RAID 6 musi mieć przynajmniej 1 dysk hot-spare automatycznie włączany do grupy RAID w przypadku awarii jednego z dysków produkcyjnych. Dyski hot-spare muszą być globalne, możliwe do wykorzystania w innych półkach, w przypadku wyczerpania w nich dysków hot-spare.
37.	Łącznie oferowane urządzenie musi posiadać zapasowe dyski typu hot-spare.
38.	Oferowane urządzenie musi umożliwiać wykonywanie SnapShot'ów, czyli umożliwiać zamrożenie obrazu danych (stanu backupów) w urządzeniu na określoną chwilę. Oferowane urządzenie musi również umożliwiać odtworzenie danych ze Snapshot'u. Odtworzenie danych ze Snapshot'u nie może wymagać konieczności nadpisania danych produkcyjnych jak również nie może oznaczać przerwy w normalnej pracy urządzenia (przyjmowania/odtwarzania backupów).
39.	Urządzenie musi pozwalać na przechowywanie minimum 500 Snapshotów jednocześnie w obrębie oferowanej przestrzeni, przy zachowaniu globalnej deduplikacji oraz standardowego trybu pracy urządzenia - umożliwiającego wykorzystanie wszystkich dostępnych funkcjonalności.
40.	Urządzenie musi umożliwiać podział na logiczne części. Dane znajdujące się w każdej logicznej części muszą być między sobą de-duplikowane (globalna de-duplikacja między logicznymi częściami urządzenia).
41.	Urządzenie musi mieć możliwość podziału na minimum 14 logicznych części pracujących równolegle. Producent musi oficjalnie wspierać pracę minimum 14 logicznych części pracujących równolegle z pełną wydajnością urządzenia.
42.	Dla każdej z w/w logicznych części oferowanego urządzenia musi być możliwość zdefiniowania oddzielnego użytkownika zarządzającego daną logiczną częścią de-duplikatora. Użytkownicy zarządzający logiczną częścią A muszą widzieć tylko i wyłącznie zasoby logicznej części A i nie mogą widzieć żadnych innych zasobów oferowanego urządzenia.
43.	Wymagana możliwość zaprezentowania każdej z logicznych części oferowanego urządzenia, jako niezależnego urządzenia dostępnego za pośrednictwem: • CIFS • NFS

	• VTL (po doposażeniu urządzenia w stosowne licencje) • BOOST/OST
44.	Urządzenie powinno umożliwiać zdefiniowanie blokady skasowania danych (funkcjonalność WORM). Blokada skasowania danych musi chronić plik w zdefiniowanym czasie przed usunięciem pliku, modyfikacją pliku. Blokada skasowania danych musi działać w dwóch trybach (do wyboru przez administratora): 1. Możliwość zdjęcia blokady przed upływem ważności danych 2. Brak możliwości zdjęcia blokady przed upływem ważności danych (COMPLIANCE) Licencje na blokadę usunięcia/zmiany przechowywanych plików w chwili obecnej nie muszą być dostarczone wraz z urządzeniem.
45.	Urządzenie musi mieć możliwość przechowywania danych niezmienialnych: • Video • Grafika • Nagrania dźwiękowe • Pliki pdf na udziałach CIFS/NFS. Wymagane jest formalne wsparcie producenta dla przechowywania w/w danych na urządzeniu. Wymagana jest formalne wsparcie producenta dla: • przechowywania na urządzeniu minimum 500 milionów plików • dziennego zasilania urządzenia na poziomie minimum 500 tysięcy plików
46.	Po niespodziewanym wyłączeniu prądu i ponownym uruchomieniu, urządzenie musi być gotowe do przyjmowania danych (backupy, archiwa) w czasie nie dłuższym niż 60 minut od włączenia.
47.	Urządzenie musi weryfikować ewentualne przekłamania (zmianę danych) na poziomie: • systemu plików oraz • grup RAID Wymaga się aby urządzenie weryfikowało sumy kontrolne dla wszystkich fragmentów zapisywanych danych, niezaleznie od używanego interfejsu.
48.	Urządzenie musi weryfikować dane po zapisie (nie chodzi o ew. weryfikację danych indeksowych generowanych przez urządzenie ale o weryfikację wszystkich zabezpieczanych danych backup'owych). Każda zapisana na dyskach porcja danych musi być odczytana i porównana z danymi otrzymanymi przez urządzenie. Powyższa weryfikacja powinna być realizowana w locie, czyli przed usunięciem z pamięci oryginalnych danych (otrzymanych z aplikacji backupowej), musi być realizowana w trybie ciągłym (a nie ad-hoc), wymagane parametry wydajnościowe urzadzenia muszą uwzględniać tę funkcjonalność. Wymagane potwierdzenie opisanej funkcjonalności w oficjalnej dokumentacji producenta oferowanego urządzenia.
49.	Urządzenie musi automatycznie (samoczynnie) wykonywać sprawdzanie spójności danych po zapisaniu danych na dysk oraz rozpoznawać i naprawiać błędy w locie. Każde zapisane na fizycznych dyskach dane muszą być odczytane i porównane z danymi otrzymanymi. Proces ten musi odbywać się „w locie" – musi być elementem procesu zapisu danych przez urządzenie.
50.	Urządzenie musi automatycznie usuwać przeterminowane dane (bloki danych nie należące do backupów o aktualnej retencji) w procesie czyszczenia.
51.	Proces usuwania przeterminowanych danych (czyszczenia) nie może uniemożliwiać pracy procesów backupu / odtwarzania danych (zapisu / odczytu danych z zewnątrz do systemu).
52.	Musi istnieć możliwość zdefiniowania maksymalnego obciążenia urządzenia procesem

	usuwania przeterminowanych danych (poziomu obciążenia procesora).
53.	Musi istnieć możliwość zdefiniowania czasu w którym wykonywany jest proces usuwania przeterminowanych danych (czyszczenia).
54.	Standardowa czestotliwość usuwania przeterminowanych danych (czyszczenie) nie powinna być większaniż 1 raz na tydzień - minimalizując czas w którym backupy/odtworzenia narażone są na spowolnienie (weryfikacja wymagania na podstawie dokumentacji typu DOBRE PRAKTYKI publikowanej przez producenta).
55.	Urządzenie musi zapewniać w przypadku dni roboczych (poniedziałek – piątek) minimum 20 godzin pełnej wydajności (dla każdej roboczej doby) . Wymagana pelna wydajność, dostępna w okresie pon-pt - min. 20 godzin dziennie oznacza, że urządzenie nie może w tym czasie wykonywać wewnętrznych procesów serwisowych, w szczegolności nie może wykonywać usuwania przeterminowanych danych (cleaning).
56.	Urządzenie musi mieć możliwość zarządzania poprzez • Interfejs graficzny dostępny z przeglądarki internetowej • Poprzez linię komend (CLI) dostępną z poziomu ssh (secure shell)
57.	Oprogramowanie do zarządzania musi rezydować na oferowanym na urządzeniu de-duplikacyjnym.
58.	Oferowane urządzenie musi mieć możliwość sprawdzenia pakietu upgrade'ującego firmware urządzenia (GUI lub CLI), to znaczy spradzenia czy nowa wersja systemu nie spowoduje problemów z urządzeniem.
59.	Oferowany produkt musi mieć możliwość zaimplementowania funkcjonalności wewnętrznego mechanizmu szyfrowania danych przed zapisaniem na dysk realizowany na poziomie urządzenia – długość klucza minimum 256-bit. Ewentualna licencja szyfrowania nie jest przedmiotem niniejszego zamówienia.
60.	Urządzenie musi być rozwiązaniem kompletnym, appliancem sprzętowym pochodzącym od jednego producenta, zarówno oprogramowanie backupowe jak i deduplikator będący przedmiotem zapytania powinny pochodzić od tego samego producenta. Zamawiający nie dopuszcza stosowania rozwiązań typu gateway. Oferowany typ urządzenia musi być oficjalnie dostępne w ofercie producenta przed ukazaniem się niniejszego postępowania.
61.	Wymagane wsparcie (5x9 NBD) producenta w okresie 3 lat od moment zakupu.

4. Macierz – 1szt.

1. Urządzenie powinno być wyposażone w przynajmniej dwa moduły do transmisji i obsługi danych z protokołami FC.
2. Macierz powinna być wyposażona w zdwojone, redundantne moduły odpowiedzialne za obsługę zarządzanej przestrzeni dyskowej, jej konfigurację, liczenie RAID oraz obsługę protokołów wymienionych w punkcie 1.
3. Moduły obliczeniowe macierzy powinny pracować w trybie aktywny/aktywny. W przypadku awarii jednego z nich drugi musi przejąć jego pracę.
4. Macierz musi być wyposażona w co najmniej 128GB pamięci podręcznej służącej do buforowania operacji odczytu oraz zapisu dostępne dla każdego wolumenu macierzy.
5. Urządzenie powinno być wyposażone w podwójny, redundantny system zasilania (pojemność efektywna dostępna dla operacji zapisu po uwzględnieniu mechanizmu cache mirror zabezpieczającego przed awarią pamięci cache).
6. Włączenie lub wyłączenie pamięci cache nie może wymagać operacji usunięcia i utworzenia na nowo wolumenów lub grup dyskowych.
7. Połączenia między dyskami a modułami obliczeniowymi macierzy powinny być redundantne (do każdego dysku dwie ścieżki – po jednej z każdego modułu obliczeniowego), w technologii SAS o przepustowości, co najmniej 6Gbit/s
8. Macierz NAS powinna współpracować równocześnie z dyskami SAS i Near Line SAS. Macierz powinna być wyposażona, w co najmniej:
   21 x 900 GB 10 tyś. RPM
9. Macierz powinna pozwalać na rozbudowę, do co najmniej 196 dysków twardych. Dodawanie kolejnych dysków, jak i kolejnych półek dyskowych powinno odbywać się w trybie on-line.
10. Urządzenie powinno umożliwiać równoczesną obsługę wielu poziomów RAID. Ze względu na zakładane przeznaczenie niniejszego urządzenia zamawiający wymaga, by obsługiwało ono, co najmniej RAID 10, 5 i 6.
11. Macierz powinna zapewniać mechanizm thin provisioning, który polega na udostępnianiu większej przestrzeni logicznej niż jest to fizycznie alokowane w momencie tworzenia zasobu. W przypadku zbliżenia się do fizycznych granic systemu plików, musi istnieć możliwość automatycznego jego rozszerzenia bez konieczności interwencji administratora.
12. Urządzenie ma obsługiwać mechanizm snapshot'ów w trybie do zapisu i odczytu, wykonywanych z poziomu macierzy. Wymagane jest, aby macierz pozwalała na wykonywanie, co najmniej 90 kopii migawkowych, istniejących na niej wolumenów. Mechanizm snapshot'ów ma umożliwiać przywrócenie zawartości całego wolumenu bazując na jego snapshot'cie.
13. Przepełnienie przestrzeni dla kopii migawkowych nie może powodować błędów zapisu na przestrzeń produkcyjną.
14. Możliwość definiowania automatycznej polityki tworzenia kopii migawkowych z wykorzystaniem interwału czasowego.
15. Macierz powinna być dostarczona wraz z licencją na zdalną replikację danych do podobnego urządzenia.
16. W przypadku odtworzenia danych z dowolnej kopii migawkowej, urządzenie musi pozwalać na poprawne zachowanie także wcześniejszych jak i późniejszych snapshotów, z zachowaniem możliwości kolejnego odtworzenia danych zarówno ze wszystkich istniejących (starszych i nowszych) kopii dostępnych dla danego zasobu.
17. Oferowane urządzenie powinno być wyposażone, w co najmniej 12 portów FC 8Gb do podłączenia do sieci SAN.

18. Macierz powinna być zarządzalna zarówno z poziomu linii komend (CLI), jak również poprzez jeden interfejs graficzny (GUI).
19. Macierz musi oferować wtyczkę do współpracy macierzy z oprogramowaniem VMware vCenter.
20. Macierz musi być fabrycznie nowa.
21. Macierz powinna oferować funkcjonalność podłączenia jej do centrum serwisowego producenta, w celu zdalnego monitorowania poprawności funkcjonowania macierzy.
22. Macierz powinna być objęta gwarancją producenta na sprzęt i oprogramowanie przynajmniej na trzy lata. Gwarancja powinna być świadczona w trybie NBD.
23. Zamawiający wymaga, aby serwis sprzętu i oprogramowania świadczony był przez organizację serwisową producenta, mającą swoją placówkę serwisową na terenie Polski.