Załącznik nr 6

Opis przedmiotu zamówienia

1. Przedmiotem zamówienia jest dostawa klastra wirtualizacyjnego wraz z systemem kopii zapasowych zamawianego na potrzeby realizowanego przez PSW im. Papieża Jana Pawła II w Białej Podlaskiej projektu pt. „Stawiamy na Rozwój Zintegrowany" o parametrach i funkcjonalności wskazanej poniżej.
2. Dostarczony asortyment musi być fabrycznie nowy tj. wykonany z nowych elementów, nie używany, zapakowany w oryginalne opakowania producenta.
3. Zamawiający przedstawił minimalne parametry techniczne, które spełniałyby założone wymagania techniczne i jakościowe, funkcjonalne oraz użytkowe. Wykonawca może zaoferować inny typ urządzenia, ale musi być ono równoważne jakościowo do określonego w SIWZ. Oznacza to, że w ofercie nie może być zaoferowane urządzenie o niższym standardzie i gorszych parametrach niż określone w SIWZ. Wykonawca proponujący inny typ urządzenia zobowiązany jest wykazać, że jest ono równoważne jakościowo i spełnia wymagane normy, parametry i standardy. W takim przypadku zadaniem Wykonawcy jest wskazanie i udowodnienie wymaganego przez Zamawiającego poziomu parametrów i jakości poprzez podanie typów urządzeń, producentów i opisu zawierającego co najmniej informacje zawarte w opisie przedmiotu zamówienia. W przypadku gorszych parametrów technicznych, jakościowych, funkcjonalnych oraz użytkowych przedmiotu zamówienia oferta Wykonawcy zostanie odrzucona z postępowania.
4. Warunki gwarancji nie mogą nakazywać Zamawiającemu przechowywania opakowań, w których przedmiot zamówienia zostanie dostarczony (Zamawiający może usunąć opakowania po dostawie, co nie spowoduje utarty gwarancji, a dostarczone urządzenia, mimo braku opakowań, będą podlegały usłudze gwarancyjnej).
5. Elektroniczne licencje na oprogramowanie systemu powinny być zarejestrowane u producenta. Potwierdzenie przeniesienia praw licencji na Zamawiającego powinno być dostarczone na adres e-mail wskazany przez Zamawiającego w umowie. Wykonawca zobowiązany jest do dostarczenia licencji umożliwiających uruchomienie dowolnej ilości maszyn wirtualnych z systemem operacyjnym rodziny Windows Serwer. Wymagane jest to ze względu wykorzystywania przez Zamawiającego oprogramowania opartego na technologii firmy Microsoft. Zamawiający używa oprogramowania wymagającego systemów z rodziny Windows Serwer.
6. Przedmiot zamówienia obejmuję dostawę, instalację, uruchomienie i przeszkolenie pracowników z obsługi dostarczonego przedmiotu zamówienia w ilości i asortymencie:
   6.1. Serwer Wirtualizacji - 2 szt. o parametrach nie gorszych niż:
      6.1.1. Obudowa:
         6.1.1.1. Typu Rack o wysokości max 1U wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych oraz możliwość dodania organizatora do kabli.
         6.1.1.2. Obudowa musi mieć możliwość wyposażenia w kartę umożliwiającą dostęp bezpośredni poprzez urządzenia mobilne - serwer musi posiadać możliwość konfiguracji oraz monitoringu najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej (Android/ Apple iOS) przy użyciu jednego z protokołów NFC/ BLE/ WIFI.
      6.1.2. Płyta główna z możliwością zainstalowania do dwóch procesorów, musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym.

6.1.3. Chipset dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych.
6.1.4. Zainstalowane dwa procesory ośmiordzeniowe, min. 2.1 GHz, klasy x86 dedykowane do pracy z zaoferowanym serwerem umożliwiające osiągnięcie wyniku min. 72 w teście SPECrate2017_int_base dostępnym na stronie www.spec.org dla dwóch procesorów(test wykonany na oferowanym modelu serwera).
6.1.5. Pamięć RAM:
6.1.5.1. minimalnie 256GB w konfiguracji 8x32GB,
6.1.5.2. typ: DDR4 RDIMM 2666MT/s,
6.1.5.3. na płycie głównej powinno znajdować się minimum 16 slotów przeznaczonych do instalacji pamięci.
6.1.5.4. płyta główna powinna obsługiwać do 1TB pamięci RAM.
6.1.5.5. Minimalna funkcjonalność pamięci RAM - Memory Rank Sparing, Memory Mirror, Failed DIMM isolation, Memory Address Parity Protection, Memory Thermal Throttling.
6.1.6. Sieć:
6.1.6.1. Interfejsy sieciowe/FC/SAS,
6.1.6.2. Wbudowane minimum 2 porty typu Gigabit Ethernet Base-T 1Gb/s,
6.1.6.3. Dodatkowa karta sieciowa dwuportowa 10Gb SFP+ wraz z kompletem wkładek Short Range,
6.1.6.4. Dodatkowa karta sieciowa dwuportowa 16Gb Fibre Channel.
6.1.7. Zainstalowany moduł dedykowany dla hypervisora wirtualizacyjnego, wyposażony w dwa nośniki typu flash o pojemności min. 16GB z możliwością konfiguracji zabezpieczenia synchronizacji pomiędzy nośnikami z poziomu BIOS serwera, rozwiązanie nie może powodować zmniejszenia ilości wnęk na dyski twarde.
6.1.8. Możliwość instalacji dwóch dysków M.2 SATA o pojemności min. 480GB oraz możliwość konfiguracji w RAID 1 – Te dyski nie mogą zajmować slotów z przodu obudowy.
6.1.9. Napęd optyczny DVD +/-RW, SATA.
6.1.10. Wbudowane porty:
6.1.10.1. min. 1 port USB 2.0,
6.1.10.2. 1 port micro-USB,
6.1.10.3. min. 3 porty USB 3.0,
6.1.10.4. 2 porty RJ45,
6.1.10.5. 2 porty VGA (1 na przednim panelu obudowy, drugi na tylnym), min. 1 port RS232.
6.1.11. Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1440x900.
6.1.12. Redundantne wentylatory.
6.1.13. Redundantne zasilacze, Hot-Plug maksymalnie 550W.
6.1.14. Bezpieczeństwo:
6.1.14.1. Wbudowany moduł TPM min. 1.2
6.1.14.2. Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą.
6.1.15. System operacyjny:

6.1.15.1. Microsoft Windows Serwer 2019 Data Center
6.1.15.2. licencje CAL Device w ilości 300 szt. per serwer.
6.1.16. Możliwość wyposażenia w panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS'u, zasilaniu oraz temperaturze.
6.1.17. Karta zarządzania:
6.1.17.1. Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca:
6.1.17.1.1. zdalny dostęp do graficznego interfejsu Web karty zarządzającej;
6.1.17.1.2. zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera);
6.1.17.1.3. szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika;
6.1.17.1.4. możliwość podmontowania zdalnych wirtualnych napędów;
6.1.17.1.5. wirtualną konsolę z dostępem do myszy, klawiatury;
6.1.17.1.6. wsparcie dla IPv6;
6.1.17.1.7. wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish;
6.1.17.1.8. możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer;
6.1.17.1.9. możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer;
6.1.17.1.10. integracja z Active Directory;
6.1.17.1.11. możliwość obsługi przez dwóch administratorów jednocześnie;
6.1.17.1.12. wsparcie dla dynamic DNS;
6.1.17.1.13. wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej.
6.1.17.1.14. możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera
6.1.17.1.15. możliwość zarządzania do 100 serwerów bezpośrednio z konsoli karty zarządzającej pojedynczego serwera
6.1.17.1.16. karta z możliwością wyposażenia we wbudowaną wewnętrzną pamięć SD lub USB o pojemności 16GB do przechowywania sterowników i firmware'ów komponentów serwera, umożliwiająca szybką instalację wspieranych systemów operacyjnych.
6.1.17.2. Oprogramowanie umożliwiające zarządzanie poprzez sieć, spełniające minimalne wymagania:
6.1.17.2.1. wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych;
6.1.17.2.2. możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta;
6.1.17.2.3. wsparcie dla protokołów – WMI, SNMP, IPMI, WSMan, Linux SSH;
6.1.17.2.4. możliwość oskryptowywania procesu wykrywania urządzeń;
6.1.17.2.5. możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram;
6.1.17.2.6. szczegółowy opis wykrytych systemów oraz ich komponentów;

6.1.17.2.7. możliwość eksportu raportu do CSV, HTML, XLS;
6.1.17.2.8. grupowanie urządzeń w oparciu o kryteria użytkownika;
6.1.17.2.9. automatyczne skrypty CLI umożliwiające dodawanie i edycję grup urządzeń;
6.1.17.2.10. szybki podgląd stanu środowiska;
6.1.17.2.11. podsumowanie stanu dla każdego urządzenia;
6.1.17.2.12. szczegółowy status urządzenia/elementu/komponentu;
6.1.17.2.13. generowanie alertów przy zmianie stanu urządzenia;
6.1.17.2.14. filtry raportów umożliwiające podgląd najważniejszych zdarzeń;
6.1.17.2.15. integracja z service desk producenta dostarczonej platformy sprzętowej;
6.1.17.2.16. możliwość przejęcia zdalnego pulpitu;
6.1.17.2.17. możliwość podmontowania wirtualnego napędu;
6.1.17.2.18. kreator umożliwiający dostosowanie akcji dla wybranych alertów;
6.1.17.2.19. możliwość importu plików MIB;
6.1.17.2.20. przesyłanie alertów „as-is" do innych konsol firm trzecich;
6.1.17.2.21. aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania);
6.1.17.2.22. możliwość instalacji sterowników i oprogramowania wewnętrznego bez potrzeby instalacji agenta;
6.1.17.2.23. możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów;
6.1.17.2.24. moduł raportujący pozwalający na wygenerowanie następujących informacji: nr seryjny sprzętu, konfiguracja poszczególnych urządzeń, wersje oprogramowania wewnętrznego, obsadzenie slotów PCIe i gniazd pamięci, informację o maszynach wirtualnych, aktualne informacje o stanie gwarancji, adresy IP kart sieciowych.

6.1.18. Certyfikaty:
6.1.18.1. Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2008 oraz ISO-14001.
6.1.18.2. Serwer musi posiadać deklaracja CE.
6.1.18.2.1. Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows" dla systemów Microsoft Windows Server 2012, 2012 R2, Microsoft Windows Server 2016, Microsoft Windows Server 2019.

6.1.19. Warunki gwarancji:
6.1.19.1. Firma serwisująca musi posiadać ISO 9001:2008 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty.
6.1.19.2. Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji serwera.
6.1.19.3. Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.

6.2. Macierz dyskowa w ilości 1 szt. o parametrach nie gorszych niż:
- 6.2.1. Możliwość łączenia w macierzy różnych poziomów RAID:
  - 6.2.1.1. możliwość zastosowania RAID10,
  - 6.2.1.2. możliwość zastosowania RAID5,
  - 6.2.1.3. możliwość zastosowania RAID6,
  - 6.2.1.4. możliwość zastosowania RAID0,
  - 6.2.1.5. możliwość zastosowania RAID1.
- 6.2.2. Podwójne niezależne przyłącza SAS 12Gb/s do wewnętrznych napędów dyskowych.
- 6.2.3. Odporność na awarię pamięci cache – lustrzany zapis danych oraz technologia zapewniająca ochronę danych z pamięci cache w razie utraty zasilania.
- 6.2.4. Możliwość wykonywania wszystkich napraw, rekonfiguracji, rozbudowy i upgrade'ów (zarówno sprzętu jak i oprogramowania macierzy) w trybie online (bez przerywania pracy systemu).
- 6.2.5. Możliwość zdefiniowania min. 4 dysków zapasowych dla każdego typu dysków w zaoferowanej macierzy lub odpowiednia zapasowa przestrzeń dyskowa.
- 6.2.6. Możliwość obsługi wirtualnych portów (NPIV) w taki sposób, aby awaria fizycznego portu nie powodowała konieczności przełączania ścieżek poprzez oprogramowanie do multipathing
- 6.2.7. Wspierane systemy operacyjne:
  - 6.2.7.1. Wymagane wsparcie dla różnych systemów operacyjnych, co najmniej AIX, HP-UX, MS Windows, VMware oraz Linux, APPLE IOS
    - 6.2.7.1.1. Wymagane wsparcie dla różnych systemów klastrowych, co najmniej Veritas Cluster Server, HACMP, HP Serviceguard.
    - 6.2.7.1.2. Wsparcie dla mechanizmów dynamicznego przełączania zadań I/O pomiędzy kanałami w przypadku awarii jednego z nich (path failover). Wymagane jest wsparcie dla odpowiednich mechanizmów oferowanych przez producentów systemów operacyjnych: AIX, HP-UX, MS Windows, Vmware, Linux.
    - 6.2.7.1.3. Macierz musi mieć wsparcie dla automatycznego, bez agenta, odzyskiwania bloków (space reclamation) dla systemu operacyjnego Linux i systemu plików EXT4, NTFS dla Windows 2012, VMFSv5 dla ESX oraz VxFS w przypadku zastosowania technologii Thin Provisioning.
- 6.2.8. Skalowalność:
  - 6.2.8.1. Wykonywanie rozbudowy sprzętowej w trybie online.
  - 6.2.8.2. Umożliwia rozbudowę do minimum 220 dysków 2,5".
  - 6.2.8.3. Możliwość rozbudowy macierzy za pomocą nowych dysków o większych pojemnościach oraz dysków typu SSD/Flash – zoptymalizowanych pod kątem zapisu bądź odczytu.
  - 6.2.8.4. Macierz musi umożliwiać mieszanie dysków o różnych prędkościach obrotowych w ramach jednej półki dyskowej.
- 6.2.9. Zarządzanie:
  - 6.2.9.1. Oprogramowanie do zarządzania macierzą przez administratora klienta – graficzny interfejs do monitorowania stanu i konfiguracji macierzy, diagnostyki, mapowania zasobów do serwerów (zarówno podłączanych bezpośrednio jak i przez sieć SAN – LUN Masking).

6.2.9.2. Stałe monitorowanie macierzy przez zdalne centrum serwisowe.

6.2.9.3. Monitorowanie wydajności macierzy według parametrów takich jak: przepustowość oraz liczba operacji I/O dla interfejsów zewnętrznych, wolumenów logicznych LUN, oraz kontrolerów.

6.2.9.4. Wymagana możliwość zbierania i przechowywania informacji o wydajności macierzy bez ograniczeń czasowych.

6.2.9.5. Możliwość konfigurowania wolumenów logicznych LUN o pojemności użytkowej 500TB.

6.2.9.6. Macierz musi posiadać wbudowaną funkcjonalność typu thin provisioning umożliwiającą alokację wirtualnej przestrzeni dyskowej, do której fizyczne dyski mogą być dostarczone w przyszłości.

6.2.10. Możliwość migracji danych w obrębie macierzy:

6.2.10.1. Wymagane jest posiadanie automatycznego, bez interwencji człowieka, rozkładania danych między dyskami poszczególnych typów (tzw. auto-tiering). Dane muszą być automatycznie przemieszczane miedzy rożnymi typami dysków oraz rożnymi poziomami RAID w zależności od stopnia obciążenia macierzy dyskowej. Dane często używane macierz powinny automatycznie przemieszczać na dyski o największej prędkości obrotowej, dane rzadko używane na dyski o prędkości obrotowej 7200 rpm. Dodatkowo funkcjonalność ta musi wspierać dyski SSD zoptymalizowane przez producenta dysków do zapisu lub do odczytu.

6.2.10.2. Licencja na tą funkcjonalność nie jest wymagana przez zamawiającego.

6.2.10.3. Macierz musi mieć możliwość migracji wolumenów logicznych LUN pomiędzy różnymi grupami dyskowymi RAID w obrębie macierzy. Migracja musi być wykonywana w trybie on-line. Jeżeli funkcjonalność taka wymaga dodatkowej licencji, to należy je uwzględnić w ofercie.

6.2.10.4. Macierz musi umożliwiać tworzenie jednego wolumenu logicznego LUN w obrębie wszystkich produkcyjnych dysków macierzy. Jeżeli funkcjonalność taka wymaga dodatkowej licencji, to należy je uwzględnić w ofercie. Musi również umożliwiać udostępnienie tego wolumenu logicznego LUN po protokole FC.

6.2.11. Lokalna replikacja danych:

6.2.11.1. Możliwość tworzenia kopii danych z poziomu macierzy i wewnątrz macierzy bez angażowania systemu operacyjnego hosta,

6.2.11.2. Możliwość tworzenia i utrzymywania jednocześnie minimum ośmiu lokalnych kopii danych wewnątrz macierzy dla każdego urządzenia LUN (tzw. kopie point-in-time) przez administratora,

6.2.11.3. Oferowana macierz dyskowa musi umożliwiać wykonanie lokalnej kopii danych na całej zaoferowanej przestrzeni dyskowej,

6.2.11.4. Wymaga jest również funkcjonalność wykonywania kopii wirtualnych typu snapshot. Jest wymagana licencja na pełną pojemność macierzy oraz maksymalną ilość snapshotów w obrębie macierzy.

6.2.11.5. Kopie migawkowe muszą być wykonywane metodą tzw. bez prealokacji przestrzeni dyskowej (ang. allocate-on-write, a.k.a redirect-on-write). Kopie migawkowe nie mogą być wykonywane metodą COW (ang. Copy On Write)

6.2.11.6. Kopie migawkowe muszą mieć możliwość prezentacji, jako urządzenia LUN w trybie do odczytu i zapisu. Jeżeli ta funkcjonalność wymaga dodatkowej licencji należy ja dostarczyć.

6.2.12. Macierz powinna zapewniać metody redukcji ilości danych blokowych za pomocą kompresji. Kompresja powinna odbywać się po fakcie zapisu na urządzenia dyskowe wewnątrz macierzy (dane spoczynkowe).

6.2.12.1. Kontrola przepływu danych – QoS (Zamawiający wymaga dostarczenia licencji) Macierz dyskowa powinna posiadać mechanizmy kontroli wykorzystania zasobów macierzowych na poziomie poszczególnych wolumenów. Kontrola powinna polegać na możliwości dynamicznego ograniczania przepływu danych wyrażanych w MB/s oraz w ilości IOPS poprzez administratora w dowolnym momencie.

6.2.13. Możliwość integracji środowiska VMware, Microsoft SQL z mechanizmem lokalnej replikacji danych.

6.2.14. Zdalna replikacja danych (Zamawiający nie wymaga dostarczenia licencji):

6.2.14.1. Macierz musi posiadać funkcjonalność zdalnej replikacji danych do macierzy tej samej rodziny w trybie synchronicznym oraz asynchronicznym i asynchronicznym interwałowym bez użycia dodatkowych serwerów lub innych urządzeń.

6.2.14.2. Oprogramowanie musi zapewniać funkcjonalność zawieszania i ponownej przyrostowej resynchronizacji kopii z oryginałem.

6.2.14.3. Oferowana macierz dyskowa musi umożliwiać wykonanie w trybie synchronicznym i asynchronicznym zdalnej kopii danych całej powierzchni użytkowej macierzy.

6.2.14.4. Macierz musi umożliwiać uruchomienie replikacji synchronicznej z inną macierzą z tej samej rodziny i zapewniać – w przypadku awarii i całkowitej niedostępności jednej z macierzy – bezprzerwową pracę systemów działających na platformie przetwarzania danych i korzystających z zasobów pamięci masowych. Opisana powyżej obsługa awarii (przełączenie między macierzami) musi odbywać się w sposób automatyczny i transparenty (bez przerywania dostępu do danych) dla korzystających z macierzy hostów. Opisana funkcjonalność musi integrować się z platformą wirtualizacyjną VMware ESX i posiadać certyfikację VMware vSphere Metro Storage Cluster, potwierdzoną wpisem na ogólnodostępnej liście kompatybilności producenta.

6.2.14.5. Aktualnie ta funkcjonalność nie jest wymagana. Jeżeli wymagana jest aktywacja opisanej funkcjonalności to należy zaoferować odpowiednie urządzenia oraz licencję obejmujące pełną, maksymalną pojemność oferowanej macierzy.

6.2.15. Macierz musi posiadać funkcjonalność onlinowego importu danych z macierzy innego producenta z jednoczesną konwersją wolumenu logicznego LUN do trybu „Thin Provision".

6.2.16. Wymiana dysków może być dokonywana przez klienta.

6.2.17. W przypadku awarii dyski twarde pozostają własnością zamawiającego.

6.2.18. Macierz powinna posiadać dwa redundantne kontrolery macierzowe wraz z możliwością instalacji 24 dysków 2,5" o maksymalnej wysokość 3U, Macierz

musi umożliwiać rozbudowę o moduły 12 dysków 3,5" , 24 dysków 2,5" oraz 60 dysków 3,5".

6.2.19. Obsługa minimum 220 dysków SAS/NLSAS lub SSD.

6.2.20. Macierz musi być wyposażona w 10 dysków 2,5" o pojemności min. 1.8TB SAS 10k min. SAS 12Gb/s.

6.2.21. Pamięć podręczna (cache) – 16 GB pojemności użytkowej dla danych oraz informacji kontrolnych na każdy kontroler (sumarycznie 32 GB),. Zamawiający nie dopuszcza rozwiązań rozszerzających pamięć podręczną cache dyskami SSD/Flash.

6.2.22. Macierz musi być wyposażona w min. 8 portów SAS 12Gb/s, 2 porty zarządzające 1GbE Base-T, każdy kontroler macierzy w trybie Active-Active.

6.2.23. Macierz musi być wyposażona w min 8 portów 10Gb SFP+.

6.2.24. Odporność na zanik zasilania jednej fazy lub awarię zasilacza macierzy (redundancja układu zasilania).

6.3. Przełącznik SAN 2 szt. o parametrach nie gorszych niż:

6.3.1. W ofercie wymagane jest podanie modelu, symbolu oraz producenta.

6.3.2. Przełącznik FC musi być wykonany w technologii FC minimum 16 Gb/s i zapewniać możliwość pracy portów FC z prędkościami 32, 16, 8, 4 Gb/s w zależności od rodzaju zastosowanych wkładek SFP.

6.3.3. W przypadku obsadzenia portu FC za pomocą wkładki SFP 16Gb/s przełącznik musi umożliwiać pracę tego portu z prędkością 16, 8 lub 4 Gb/s, przy czym wybór prędkości musi być możliwy w trybie autonegocjacji.

6.3.4. W przypadku obsadzenia portu FC za pomocą wkładki SFP 8Gb/s przełącznik musi umożliwiać pracę tego portu z prędkością 8, 4 Gb/s, przy czym wybór prędkości musi być możliwy w trybie autonegocjacji.

6.3.5. Przełącznik FC musi być wyposażony, w co najmniej 8 aktywnych portów FC obsadzonych 8 wkładkami SFP 16Gb/s Short Wave (multimode)

6.3.6. Wszystkie zaoferowane porty przełącznika FC muszą umożliwiać działanie bez tzw. oversubscrypcji gdzie wszystkie porty w maksymalnie rozbudowanej konfiguracji przełącznika mogą pracować równocześnie z pełną prędkością 8Gb/s lub 16Gb/s w zależności do zastosowanych wkładek FC

6.3.7. Całkowita przepustowość przełącznika FC dostępna dla maksymalnie rozbudowanej konfiguracji wyposażonej we wkładki 16Gb/s musi wynosić minimum 384 Gb/s end-to-end.

6.3.8. Zamawiający wymaga, aby możliwa była instalacja wkładek w przełączniku FC: 32 Gb/S o całkowitej przepustowości min. 768 Gb/s end-to-end

6.3.9. Oczekiwana wartość opóźnienia przy przesyłaniu ramek FC między dowolnymi portami przełącznika nie może być większa niż 900µs.

6.3.10. Rodzaj obsługiwanych portów, co najmniej: E-port, D-port oraz F-port.

6.3.11. Przełącznik FC musi mieć wysokość maksymalnie 1U (jednostka wysokości szafy montażowej) i szerokość 19" oraz zapewniać techniczną możliwość montażu w szafie 19". Wraz z przełącznikiem należy dostarczyć elementy umożliwiające montaż w szafie, oferowanej w niniejszym postępowaniu.

6.3.12. Maksymalny dopuszczalny pobór mocy przełącznika FC wyposażonego w 24 aktywne porty 32Gbps to 80W.

6.3.13. Maksymalna ilość ciepła wydzielanego przez przełącznik FC wyposażony w 24 aktywne porty 32Gbps to 250 BTU na godzinę.

6.3.14. Przełącznik FC musi mieć możliwość agregacji połączeń ISL między dwoma przełącznikami i tworzenia w ten sposób logicznych połączeń typu trunk o przepustowości minimum 256 Gb/s half duplex dla każdego logicznego połączenia. Load balancing ruchu między fizycznymi połączeniami ISL w ramach połączenia logicznego typu trunk musi być realizowany na poziomie pojedynczych ramek FC a połączenie logiczne musi zachowywać kolejność przesyłanych ramek. Jeśli funkcjonalność ta, wymaga dodatkowej licencji, nie jest wymagane jej dostarczenie w tym postępowaniu.

6.3.15. Przełącznik FC musi realizować sprzętową obsługę zoningu (przez tzw. układ ASIC) na podstawie portów i adresów WWN.

6.3.16. Przełącznik FC musi wspierać następujące mechanizmy zwiększające poziom bezpieczeństwa:

6.3.16.1. mechanizm tzw. Fabric Binding, który umożliwia zdefiniowanie listy kontroli dostępu regulującej prawa przełączników FC do uczestnictwa w sieci fabric

6.3.16.2. uwierzytelnianie (autentykacja) przełączników w sieci Fabric za pomocą protokołów DH-CHAP i FCAP

6.3.16.3. uwierzytelnianie (autentykacja) urządzeń końcowych w sieci Fabric za pomocą protokołu DH-CHAP

6.3.16.4. szyfrowanie połączenia z konsolą administracyjną. Wsparcie dla SSHv2.

6.3.16.5. definiowanie wielu kont administratorów z możliwością ograniczenia ich uprawnień za pomocą mechanizmu tzw. RBAC (Role Based Access Control)

6.3.16.6. definiowane kont administratorów w środowisku RADIUS, LDAP w MS Active Directory, Open LDAP, TACACS+

6.3.16.7. szyfrowanie komunikacji narzędzi administracyjnych za pomocą SSL/HTTPS

6.3.16.8. obsługa SNMP v1 oraz v3

6.3.16.9. IP Filter dla portu administracyjnego przełącznika

6.3.16.10. wgrywanie nowych wersji firmware przełącznika FC z wykorzystaniem bezpiecznych protokołów SCP oraz SFTP

6.3.16.11. wykonywanie kopii bezpieczeństwa konfiguracji przełącznika FC z wykorzystaniem bezpiecznych protokołów SCP oraz SFTP

6.3.17. Przełącznik FC musi mieć możliwość konfiguracji przez:

6.3.17.1. polecenia tekstowe w interfejsie znakowym konsoli terminala

6.3.17.2. przeglądarkę internetową z interfejsem graficznym lub dedykowane oprogramowanie.

6.3.18. Przełącznik FC musi być wyposażony w następujące narzędzia diagnostyczne i mechanizmy obsługi ruchu FC:

6.3.18.1. logowanie zdarzeń poprzez mechanizm „syslog”,

6.3.18.2. ciągłe monitorowanie parametrów pracy przełącznika, portów, wkładek SFP i sieci fabric z automatycznym powiadamianiem administratora (e-mail) w przypadku przekroczenia zdefiniowanych wartości granicznych. Jeśli funkcjonalność ta, wymaga dodatkowej licencji, nie jest wymagane jej dostarczenie w tym postępowaniu.

6.3.18.3. port diagnostyczny tzw. D_port. Port diagnostyczny musi umożliwiać wykonanie testów sprawdzających komunikację portu przełącznika z wkładką SFP, połączenie optyczne pomiędzy dwoma przełącznikami,

testowe obciążenie połączenia pełną przepustowością 16Gbps oraz pomiar opóźnienia i odległości między przełącznikami z dokładnością do 5m dla wkładek SFP 16Gbps. Testy wykonywane przez port diagnostyczny nie mogą wpływać w żaden sposób na działanie pozostałych portów przełącznika i całej sieci fabric,

6.3.18.4. FCping,

6.3.18.5. FC traceroute,

6.3.18.6. kopiowanie danych wymienianych pomiędzy dwoma wybranymi portami na inny wybrany port przełącznika,

6.3.19. Przełącznik FC musi zapewnić możliwość jego zarządzania przez zintegrowany port Ethernet, RS232 oraz inband IP-over-FC.

6.3.20. Przełącznik FC musi zapewniać wsparcie dla standardu zarządzającego SMI-S.

6.3.21. W przełączniku FC musi istnieć możliwość wydzielenia logicznych, izolowanych od siebie przełączników. Każdy z logicznych przełączników musi mieć własny Domain ID, własne usługi fabric (tzw. fabric services), niezależną bazę zoningu oraz możliwość przypisanie dedykowanego administratora.

6.3.22. Musi istnieć możliwość połączenia wybranych logicznych przełączników wydzielonych w różnych fizycznych przełącznikach FC za pomocą dedykowanych połączeń ISL. Połączone w ten sposób przełączniki muszą tworzyć pojedynczą sieć fabric.

6.3.23. Przełącznik FC musi realizować kategoryzację ruchu między parami urządzeń (initiator - target) oraz przydzielenie takich par urządzeń do kategorii o wysokim, średnim lub niskim priorytecie. Konfiguracja przydziału do różnych klas priorytetów musi się odbywać za pomocą standardowych narzędzi do konfiguracji zoningu.

6.3.24. Przełącznik FC musi realizować kategoryzację ruchu na podstawie wartości parametru CS_CTL w nagłówku ramki FC oraz odpowiednie przydzielenie ramki do kategorii o wysokim, średnim lub niskim priorytecie.

6.3.25. Wymagane jest wsparcie dla N_Port ID Virtualization (NPIV). Obsługa, co najmniej 255 wirtualnych urządzeń na pojedynczym porcie przełącznika.

6.3.26. Urządzenie dostarczone będzie wraz z (każdy switch z poniższym okablowaniem):

6.3.26.1. Wymaganymi kablami konsolowymi.

6.3.26.2. 16 szt patchcord LC/LC, multimode, o długości 3m

6.3.27. Dla oferowanego przełącznika FC sieci SAN Wykonawca zapewnia gwarancję na warunkach:

6.3.27.1. Wykonawca gwarantuje, że dostarczone elementy infrastruktury informatycznej oraz przeprowadzona integracja fizyczna nie spowoduje utraty lub pogorszenia warunków gwarancji na użytkowaną przez Zamawiającego infrastrukturę.

6.3.27.2. Na potwierdzenie gwarancji Wykonawca dostarczy oświadczenie Producenta o udzieleniu gwarancji na elementy będące przedmiotem zamówienia (zestawienie musi przynajmniej zawierać nazwy produktów, numery seryjne, okres na który Producent udziela gwarancji, paramenty na których producent będzie świadczył gwarancję).

6.3.27.3. Dodatkowo Zamawiający w celu weryfikacji posiadanej gwarancji, wymaga dostępu do portalu Producenta zawierającego potwierdzenie przypisanych gwarancji dla elementów będących przedmiotem Zamówienia.

6.4. Wirtualizator w ilości 1 szt. o parametrach nie gorszych niż:

6.4.1. Warstwa wirtualizacji musi być zainstalowana bezpośrednio na sprzęcie fizycznym bez dodatkowych pośredniczących systemów operacyjnych

6.4.2. Rozwiązanie musi zapewnić możliwość obsługi wielu instancji systemów operacyjnych na jednym serwerze fizycznym i powinno się charakteryzować maksymalnym możliwym stopniem konsolidacji sprzętowej.

6.4.3. Pojedynczy klaster może się skalować do 64 fizycznych hostów (serwerów) z zainstalowaną warstwą wirtualizacji.

6.4.4. Oprogramowanie do wirtualizacji zainstalowane na serwerze fizycznym potrafi obsłużyć

6.4.5. i wykorzystać procesory fizyczne wyposażone w 576 logicznych wątków oraz do 12 TB pamięci fizycznej RAM.

6.4.6. Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych 1-128 procesorowych.

6.4.7. Oprogramowanie do wirtualizacji musi zapewniać możliwość stworzenia dysku maszyny wirtualnej o wielkości do 62 TB.

6.4.8. Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych

6.4.9. z możliwością przydzielenia do 6 TB pamięci operacyjnej RAM.

6.4.10. Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych, z których każda może mieć 1-10 wirtualnych kart sieciowych.

6.4.11. Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych, z których każda może mieć 32 porty szeregowe.

6.4.12. Rozwiązanie musi umożliwiać łatwą i szybką rozbudowę infrastruktury o nowe usługi bez spadku wydajności i dostępności pozostałych wybranych usług.

6.4.13. Rozwiązanie powinno w możliwie największym stopniu być niezależne od producenta platformy sprzętowej.

6.4.14. Polityka licencjonowania musi umożliwiać przenoszenie licencji na oprogramowanie do wirtualizacji pomiędzy serwerami różnych producentów z zachowaniem wsparcia technicznego i zmianą wersji oprogramowania na niższą (downgrade). Licencjonowanie nie może odbywać się w trybie OEM.

6.4.15. Rozwiązanie musi wspierać następujące systemy operacyjne: Windows XP, Windows Vista, Windows 2000, Windows Server 2003/R2, Windows Server 2008/R2, Windows Server 2012/R2, Windows Server 2016, Windows 7, Windows 8, Windows 8.1, Windows 10, SUSE Linux Enterprise Server, Red Hat Enterprise Linux, Solaris, Oracle Enterprise Linux, Debian GNU/Linux, CentOS, FreeBSD, Asianux, NeoKylin Linux, CoreOS, Ubuntu, SCO OpenServer, SCO Unixware, Mac OS X.

6.4.16. Rozwiązanie musi umożliwiać przydzielenie większej ilości pamięci RAM dla maszyn wirtualnych niż fizyczne zasoby RAM serwera w celu osiągnięcia maksymalnego współczynnika konsolidacji.

6.4.17. Rozwiązanie musi umożliwiać udostępnienie maszynie wirtualnej większej ilości zasobów dyskowych niż jest fizycznie zarezerwowane na dyskach lokalnych serwera lub na macierzy.
6.4.18. Rozwiązanie powinno posiadać centralną konsolę graficzną do zarządzania maszynami wirtualnymi i do konfigurowania innych funkcjonalności. Centralna konsola graficzna powinna mieć możliwość działania zarówno jako aplikacja na maszynie fizycznej lub wirtualnej, jak i jako gotowa, wstępnie skonfigurowana maszyna wirtualna tzw. virtual appliance. Dostęp do konsoli może być realizowany z poziomu przeglądarki internetowej z wykorzystaniem protokołu HTML5.
6.4.19. Rozwiązanie musi zapewnić możliwość bieżącego monitorowania wykorzystania zasobów fizycznych infrastruktury wirtualnej (np. wykorzystanie procesorów, pamięci RAM, wykorzystanie przestrzeni na dyskach/wolumenach) oraz przechowywać i wyświetlać dane maksymalnie sprzed roku.
6.4.20. Oprogramowanie do wirtualizacji powinno zapewnić możliwość wykonywania kopii migawkowych instancji systemów operacyjnych (tzw. snapshot) na potrzeby tworzenia kopii zapasowych bez przerywania ich pracy.
6.4.21. Oprogramowanie do wirtualizacji musi zapewnić możliwość klonowania systemów operacyjnych wraz z ich pełną konfiguracją i danymi.
6.4.22. Oprogramowanie do wirtualizacji oraz oprogramowanie zarządzające musi posiadać możliwość integracji z usługami katalogowymi Microsoft Active Directory.
6.4.23. Rozwiązanie musi zapewniać mechanizm bezpiecznego uaktualniania warstwy wirtualizacyjnej (hosta, maszyny wirtualnej) bez potrzeby wyłączania wirtualnych maszyn. Mechanizm ten jest elementem składowym rozwiązania i nie wymaga dodatkowej licencji na system operacyjny.
6.4.24. Rozwiązanie musi zapewniać mechanizm replikacji wskazanych maszyn wirtualnych w obrębie klastra serwerów fizycznych.
6.4.25. Rozwiązanie musi mieć możliwość przenoszenia maszyn wirtualnych w czasie ich pracy pomiędzy serwerami fizycznymi. Mechanizm powinien umożliwiać 4 lub więcej takich procesów przenoszenia jednocześnie.
6.4.26. Rozwiązanie musi mieć możliwość przenoszenia zwirtualizowanych dysków maszyn wirtualnych w czasie ich pracy pomiędzy fizycznymi zasobami dyskowymi. Mechanizm powinien umożliwiać realizację co najmniej 2 takich procesów przenoszenia jednocześnie.
6.4.27. Musi zostać zapewniona odpowiednia redundancja i taki mechanizm (wysokiej dostępności HA) , aby w przypadku awarii lub niedostępności serwera fizycznego wybrane przez administratora i uruchomione nim wirtualne maszyny zostały uruchomione na innych serwerach z zainstalowanym oprogramowaniem wirtualizacyjnym.
6.4.28. Oprogramowanie do wirtualizacji musi zapewniać mechanizm takiego zabezpieczenia wybranych przez administratora wirtualnych maszyn, aby w przypadku awarii lub niedostępności serwera fizycznego maszyny, które na nim pracowały, były bezprzerwowo dostępne na innym serwerze z zainstalowanym oprogramowaniem wirtualizacyjnym. Mechanizm ten umożliwia zabezpieczenie maszyn wirtualnych wyposażonych w minimum 2 wirtualne procesory.

6.4.29. System musi posiadać funkcjonalność wirtualnego przełącznika (virtual switch) umożliwiającego tworzenie sieci wirtualnej w obszarze hosta i pozwalającego połączyć maszyny wirtualne w obszarze jednego hosta, a także na zewnątrz sieci fizycznej. Pojedynczy przełącznik wirtualny powinien mieć możliwość konfiguracji do 4000 portów.

6.4.30. Pojedynczy wirtualny przełącznik musi posiadać możliwość przyłączania do niego dwóch i więcej fizycznych kart sieciowych, aby zapewnić bezpieczeństwo połączenia ethernetowego w razie awarii karty sieciowej.

6.4.31. Wirtualne przełączniki musza obsługiwać wirtualne sieci lokalne (VLAN).

6.4.32. Oprogramowanie musi posiadać centralną konsolę graficzną do zarządzania wieloma maszynami wirtualnymi oraz ich zasobami pracującymi na wielu serwerach fizycznych:

6.4.32.1. globalne zarządzanie kontrolą dostępu do serwerów i maszyn wirtualnych

6.4.32.2. wykonywanie automatycznych bądź manualnych zadań w celu optymalizacji infrastruktury dla maszyn wirtualnych.

6.4.32.3. widok całego systemu i zbioru maszyn wirtualnych. Mapy Infrastruktury.

6.4.32.4. możliwość monitorowania dostępności i wydajności maszyn wirtualnych

6.4.32.5. możliwość raportowania dostępności i wydajności maszyn wirtualnych

6.4.32.6. funkcje ochrony dostępu zintegrowane z mechanizmem uwierzytelniania Windows

6.4.32.7. planowanie zadań i ustawianie znaczników alarmów w celu generowania automatycznych powiadomień o statusie serwerów lub maszyn wirtualnych

6.4.32.8. tworzenie obrazów maszyn wirtualnych

6.4.32.9. klonowanie maszyn wirtualnych

6.4.32.10. wykonywanie wielu kopii migawkowych (snapshoot) w każdym momencie pracy maszyny wirtualnej oraz możliwość powrotu do jej stanu z każdego momentu zrobienia kopii

6.4.33. Zamawiający wymaga dostarczenia licencji dla 4 CPU (w systemie licencjonowania „per CPU") wraz z roczną subskrypcją.

6.5. System kopii zapasowej w ilości 1 szt. o parametrach i funkcjonalności:

6.5.1. oprogramowanie tworzące system ochrony danych w skład którego wchodzi:

6.5.1.1. aplikacja backup'owa,

6.5.1.2. system raportujący,

6.5.1.3. system dedykowany do wyszukiwania danych,

6.5.1.4. system umożliwiający zabezpieczenie danych w trybie Continuous Data Protection,

6.5.1.5. system umożliwiający instalację oraz eksploatację deduplikatora,

6.5.1.6. system umożliwiający zarządzanie systemem ochrony danych,

6.5.2. Poniższe zestawienie obejmuje wymagane funkcjonalności oprogramowania dedykowanego do stworzenia systemu ochrony danych.

6.5.3. Zamawiający wymaga dostarczenia, uruchomienia i wdrożenia systemu do zabezpieczania środowiska Data Center (baz danych, maszyn wirtualnych, serwerów wolnostojących).

6.5.4. Wymagane jest dostarczenie modułów oprogramowania:

6.5.4.1. backupowego (aplikacja backupowa),

6.5.4.2. umożliwiającego stworzenie systemu raportującego,

6.5.4.3. umożliwiającego zaindeksowanie oraz przeszukiwanie danych backupowych,
6.5.4.4. umożliwiającego stworzenie rozwiązania Continuous Data Protection (CDP) dla środowisk VMware,
6.5.4.5. umożliwiającego konfigurację/instalację deduplikatora,
6.5.4.6. umożliwiające zarządzanie oferowanym środowiskiem dedykowanym do zabezpieczania danych.

6.5.5. oferowane oprogramowanie powinno spełniać wszystkie wymienione w niniejszej tabeli funkcjonalności. Wymagane wsparcie na oferowane oprogramowanie realizowane w trybie 9x5 NBD, gwarantujące dostęp do najnowszych wersji oprogramowania..

6.5.6. Wymagane jest dostarczenie licencji w/w oprogramowania do zabezpieczania danych dla środowiska obejmującego zarówno serwery niezwirtualizowane oraz zwirtualizowane, charakteryzujące się sumaryczną ilością: 4 CPU. Zamawiający przewiduje w kolejnych latach rozbudowę zabezpieczanego środowiska, dlatego wymagana jest możliwość skalowania rozwiązania stworzonego w oparciu o licencje będące przedmiotem zapytania - poprzez dokładanie kolejnych licencji, co powinno umożliwić zabezpieczenie środowiska o sumarycznej ilości 50 CPU, bez względu na rozmiar zabezpieczanego wolumenu danych. Licencje będące przedmiotem zapytania powinny umożliwić skonfigurowanie deduplikatora o pojemności nie mniejszej niż 8TB netto oraz umożliwić zabezpieczenie dowolnej ilości maszyn wirtualnych (vSphere 6.5) w trybie CDP pracujących w środowisku liczącym 4 CPU.

6.5.7. Wymagania dotyczące aplikacji backupowej:
6.5.7.1. Oprogramowanie backupowe musi wspierać (wymagane wsparcie producenta) następujące systemy operacyjne: Windows (także Microsoft Cluster) , Linux (Red Hat, SUSE, Debian, CentOS, Ubuntu), Solaris, AIX, HP-UX, FreeBSD.
6.5.7.2. Backup zasobów plików w przypadku powyższych systemów musi podlegać de-duplikacji ze zmiennym blokiem na zabezpieczanej maszynie zgodnie z przedstawionymi wymaganiami.
6.5.7.3. 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 vSphere, Hyper-V.
6.5.7.4. Backup powyższych baz danych i aplikacji musi podlegać de-duplikacji ze zmiennym blokiem na zabezpieczanej maszynie zgodnie z przedstawionymi wymaganiami.
6.5.7.5. W przypadku zabezpieczania baz danych i aplikacji wymagana możliwość realizacji kopii zapasowej kilkoma strumieniami jednocześnie (minimum 10 jednoczesnych strumieni).
6.5.7.6. Zabezpieczane serwery muszą być backupowane bezpośrednio na dyski de-duplikatora (zainstalowanego/skonfigurowanego w oparciu o licencje będące przedmiotem zapytania oraz deduplikatora sprzętowego będącego przedmiotem zapytania) bez pośrednictwa jakichkolwiek innych urządzeń/serwerów, dostarczone licencje (dotyczy aplikacji backup'owej

oraz deduplikatora) powinny umożliwiać całkowitą utylizację wymaganej przestrzeni deduplikatorów.

6.5.7.7. Transfer danych z zabezpieczanych serwerów do oferowanego de-duplikatora nie może się odbywać po sieci SAN.

6.5.7.8. Oprogramowanie backupowe musi umożliwiać dla sieci lokalnej:

6.5.7.8.1. backup pojedynczych plików,

6.5.7.8.2. backup całych systemów plików,

6.5.7.8.3. backup baz danych w trakcie ich normalnej pracy,

6.5.7.8.4. backup ustawień systemu operacyjnego Windows,

6.5.7.8.5. backup całych obrazów maszyn wirtualnych systemu VMware vSphere

6.5.7.8.6. backup całych obrazów maszyn wirtualnych systemu Hyper-V

6.5.7.9. Rozwiązanie backupowe musi umożliwiać transfer danych bezpośrednio ze zdalnych oddziałów do oferowanych deduplikatorów bez konieczności instalacji jakiegokolwiek sprzętu w oddziale. Powyższa funkcjonalność wymagana jest dla następujących typów danych:

6.5.7.9.1. backup pojedynczych plików,

6.5.7.9.2. backup całych systemów plików,

6.5.7.9.3. backup baz danych w trakcie ich normalnej pracy.

6.5.7.10. W przypadku zabezpieczania środowisk zdalnych, oferowane rozwiązanie backupowe nie może wymagać zaangażowania ze strony personelu w oddziale.

6.5.7.11. Wymaga się aby oferowane rozwiązanie backupowe było w pełni konfigurowalne ze zdalnej konsoli, w szczególności backupy maszyn w oddziałach (bazy, pliki) muszą być konfigurowalne z poziomu centralnej konsoli bez konieczności logowania się na zabezpieczaną maszynę.

6.5.7.12. Oferowane rozwiązanie backupowe musi umożliwiać odtworzenie:

6.5.7.12.1. plików,

6.5.7.12.2. baz danych.

na docelową maszynę w oddziale - z poziomu centralnej konsoli systemu backupowego. Wymagany scenariusz nie może wymagać logowania się na odtwarzaną maszynę w celu odtworzenia danych z systemu backupowego.

6.5.7.13. W celu minimalizacji ilości przesyłanych danych, oferowane rozwiązanie musi mieć możliwość przesyłania odtwarzanych danych do docelowego serwera w postaci skompresowanej, odtwarzane dane powinny zostać rozkompresowane na docelowym serwerze przez agenta oferowanego systemu.

6.5.7.14. Oprogramowanie backupowe musi posiadać funkcjonalność podziału 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 w celu polepszenia efektywności deduplikacji.

6.5.7.15. Podział na bloki musi następować bezpośrednio na zabezpieczanym serwerze.

6.5.7.16. Używany algorytm de-duplikacji 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.

6.5.7.17. Wymaga się aby oprogramowanie backupowe przesyłało na oferowane deduplikatory tylko unikalne bloki nie znajdujące się na tym urządzeniu, w efekcie skracając czas backupu, obciążenie procesora i zmniejszając ruch w sieci WAN / LAN.

6.5.7.18. Funkcjonalność deduplikacji nie może wymagać instalacji dodatkowych modułów programowych po stronie klienckiej lub serwera backupowego.

6.5.7.19. 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 ponownie odczytywany, chyba, że zmieni się jego zawartość.

6.5.7.20. Wymaga się aby oprogramowanie backupowe realizowało wyłącznie - logicznie pełne backupy systemu plików. Z zabezpieczanego systemu plików muszą odczytywane tylko nowe lub zmienione pliki, do oferowanych de-duplikatorów powinny być przesyłane dane po de-duplikacji, jednak każdy finalny backup musi być logicznie pełnym backupem. W wewnętrznej strukturze systemu musi być przechowywana informacja o każdym backupie i należących do niego danych (blokach), dzięki czemu odtworzenie jakichkolwiek danych plikowych musi być pojedynczym zadaniem identycznym z odtworzeniem danych z pełnego backupu.

6.5.7.21. Wymagana możliwość definiowania w konsoli oprogramowania backupowego ważności (retencji) danych (backupów) na podstawie kryteriów czasowych (dni, miesiące, lata). Po okresie ważności backupy musza być automatycznie usunięte.

6.5.7.22. Wymagana możliwość tworzenia z poziomu GUI (konsoli graficznej) w przypadku oferowanego oprogramowania backupowego, polityk typu „dziadek – ojciec –syn", to znaczy tworzenia polityk w których zdefiniowano:

6.5.7.22.1. Czas przechowywania backupów dziennych,

6.5.7.22.2. Czas przechowywania backupów tygodniowych,

6.5.7.22.3. Czas przechowywania backupów miesięcznych,

6.5.7.22.4. Czas przechowywania backupów rocznych.

6.5.7.23. Oferowane rozwiązanie musi umożliwiać tworzenie wykluczeń, czyli elementów nie podlegających backupowi w ramach zadania backupowego. Wymagana możliwość tworzenia wykluczeń dla dowolnej kombinacji następujących elementów:

6.5.7.23.1. wybranych typów plików, np. dla plików z rozszerzeniem mp3,

6.5.7.23.2. dla całych katalogów (np.: c:\windows),

6.5.7.23.3. dla pojedynczych plików.

6.5.7.24. Oferowane rozwiązanie musi mieć możliwość zdefiniowania aby ostatni backup dowolnego zbioru danych nigdy się nie przeterminował. Oznacza to, że jeśli dany zasób nie będzie backupowany w przyszłości to automatycznie ostatni ważny backup tego zasobu będzie przechowywany bezterminowo, jedynie administrator może zdecydować o jego usunięciu.

6.5.7.25. 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.

6.5.7.26. Wymagana możliwość generowania (poprzez konsolę) raportów określających zajętość przestrzeni przeznaczonej na składowanie de-duplikatów.

6.5.7.27. Bloki przesyłane z zabezpieczanych serwerów do oferowanych deduplikatorów muszą być kompresowane i szyfrowane algorytmem z kluczem minimum 256-bitowym.

6.5.7.28. Wymagana jest autentykacja komunikacji między klientem a serwerem backupu (farmą serwerów) oparta na certyfikatach.

6.5.7.29. Oprogramowanie backupowe musi pozwalać na odtwarzanie danych poprzez: wybór odtwarzanych danych, wymagane odtworzenie danych w jednym kroku.

6.5.7.30. Wymagana możliwość limitowania wielkości zadania backupowego, jeśli zadanie backupowe przekroczy zdefiniowaną wielkość wówczas nie może być zapisane w systemie backupowym.

6.5.7.31. Oprogramowanie backupowe musi umożliwiać ograniczenie mocy procesora używanej do wykonywania zdania backupu tak aby odpowiednia moc procesora pozostała do wykorzystania dla innych zadań.

6.5.7.32. Rozwiązanie backupowe musi wspierać backup i odtwarzanie środowisk VMware 6.0, 6.5.

6.5.7.33. Oprogramowanie backupowe musi umożliwiać w przypadku środowisk VMware następujące typy backupu:

6.5.7.33.1.1. Backup całych maszyn wirtualnych

6.5.7.33.1.2. Backup pojedynczych, wybranych dysków maszyny wirtualnej vmdk

6.5.7.33.1.3. Musi istnieć możliwość zastosowania wyrażeń regularnych do określenia które wirtualne dyski VMware mają być backupowane

6.5.7.33.1.4. W trakcie backupu odczytowi z systemu dyskowego mają podlegać tylko zmienione bloki wirtualnych maszyn systemu VMware (wymagane wykorzystanie mechanizmu CBT systemu VMware)

6.5.7.33.1.5. Wykonywanie backupu obrazów maszyn wirtualnych VMware nie może wymagać bufora dyskowego na kopię obrazów maszyn wirtualnych (plików vmdk)

6.5.7.34. Powyższe metody backupu maszyn wirtualnych muszą podlegać deduplikacji ze zmiennym blokiem przed wysłaniem danych do medium backupowego zgodnie z przytoczonymi wymaganiami dla deduplikacji.

6.5.7.35. Powyższe metody backupu muszą być wbudowane w oferowany system backupu, nie powinny wymagać tworzenia skryptów/dodatkowych komend.

6.5.7.36. Oferowany system musi pozwalać na szybkie odtworzenie

6.5.7.36.1. całych obrazów maszyn wirtualnych

6.5.7.36.2. pojedynczych dysków maszyny wirtualnej z backupu całej maszyny wirtualnej

6.5.7.37. Wymaga się aby oferowane rozwiązanie backupowe umożliwiało odtwarzanie obrazów maszyn wirtualnych VMware z następującymi funkcjonalnościami:

6.5.7.37.1. odtwarzanie całych maszyn wirtualnych musi wykorzystywać mechanizm CBT systemu VMware – odtwarzane są tylko te bloki wirtualnej maszyny/dysku które uległy zmianie od ostatniego backupu

6.5.7.37.2. odtwarzanie pojedynczych dysków maszyn wirtualnych musi wykorzystywać mechanizm CBT systemu VMware – odtwarzane są tylko te bloki wirtualnej maszyny/dysku które uległy zmianie od ostatniego backupu

6.5.7.37.3. odtworzenie pojedynczych plików z backupu obrazu maszyny wirtualnej bez konieczności odtworzenia całej maszyny wirtualnej, funkcjonalność ta musi być dostępna dla obrazów maszyn wirtualnych z zainstalowanym systemem operacyjnym Windows oraz Linux.

6.5.7.37.4. możliwość zamontowania na dowolnym serwerze (fizycznym lub wirtualnym) zbackupowanych obrazów maszyn wirtualnych Windows (plików vmdk maszyny wirtualnej Windows), w efekcie metoda ta nie odtwarza backupów a jedynie umożliwia na przeglądanie zawartości plików vmdk w backupie z poziomu Eksploratora Plików Windows na dowolnej maszynie

6.5.7.38. Powyższe metody odtworzenia muszą być wbudowane w system backupu i w pełni automatyczne nie mogą generować konieczności wykorzystania dodatkowych skryptów/ komend.

6.5.7.39. Oferowane 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.

6.5.7.40. Oferowane 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.

6.5.7.41. Oferowane oprogramowanie backupowe musi mieć możliwość automatycznego sprawdzania (weryfikacji) zbackupowanych maszyn wirtualnych VMware, wymagana możliwość ustawienia kalendarza weryfikacji maszyn wirtualnych VMware.

6.5.7.42. Weryfikacja maszyn wirtualnych musi zapewniać minimum:

6.5.7.43. odtworzenie maszyny wirtualnej na zdefiniowanym Data Center/Data Store

6.5.7.44. weryfikację podstawowych procesów

6.5.7.45. możliwość dołączenia własnego skryptu weryfikującego wybrane elementy maszyny wirtualnej

6.5.7.46. Wymagana dostępność informacji w konsoli systemu backupu o statusie (poprawna/niepoprawna) weryfikacji maszyny wirtualnej.

6.5.7.47. Administrator (właściciel) danej maszyny wirtualnej VMware vSphere musi mieć możliwość samodzielnego (bez konieczności kontaktu

z administratorem backupu czy tez administratorem VMware) odtworzenia pojedynczych plików z dowolnego backupu obrazu jego maszyny wirtualnej.

6.5.7.48. Oprogramowanie backupowe musi zawsze przechowywać pełne backupy obrazów maszyn wirtualnych środowiska VMware vSphere dla każdej wykonanej w przeszłości kopii zapasowej. Każdy backup obrazu maszyny wirtualnej musi być backupem pełnym.

6.5.7.49. Oferowane rozwiązanie backupowe musi umożliwiać na tworzenie automatycznych polityk backupowych dla:

6.5.7.49.1. Folderu

6.5.7.49.2. Resource Pool

6.5.7.50. systemu VMware vSphere. 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.

6.5.7.51. 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.

6.5.7.52. 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

6.5.7.53. Wymaga się aby inicjowanie backupu oraz odtwarzanie maszyn wirtualnych VMware dostępne było z poziomu graficznego interfejsu, linii komend oraz przez REST API

6.5.7.54. Oferowane oprogramowanie backupowe powinno umożliwiać dla środowisk Hyper-V:

6.5.7.54.1. backup pojedynczych plików i baz danych z maszyny wirtualnej ze środka maszyny wirtualnej Hyper-V.

6.5.7.54.2. backup całych maszyn wirtualnych (czyli plików vhd reprezentujących wirtualną maszynę), takie wykonanie backupu nie powinno wymagać bufora dyskowego na kopię obrazów maszyn wirtualnych (plików vhd).

6.5.7.54.3. wykonywanie backupu jak w punkcie b. powinno umożliwiać na odtworzenie pojedynczych plików z obrazu maszyny wirtualnej bez konieczności odtworzenia całej maszyny wirtualnej, funkcjonalność ta powinna być dostępna dla obrazów maszyn wirtualnych z zainstalowanym systemem operacyjnym Windows.

6.5.7.55. dopuszcza się wykonywanie snapshotów vss maszyn wirtualnych i użycie ich w trakcie backupu obrazów maszyn wirtualnych.

6.5.7.56. powyższe metody backupu muszą być wbudowane w system backupu i w pełni automatyczne bez wykorzystania skryptów/dodatkowych komend.

6.5.7.57. powyższe metody backupu maszyn wirtualnych muszą podlegać de-duplikacji ze zmiennym blokiem w momencie odczytu danych zgodnie z wymaganiami powyżej.

6.5.7.58. Oferowane oprogramowanie backupowe musi zapewniać spójny backup Exchange / MSSQL przy backupie obrazów maszyn wirtualnych środowiska Hyper-V
6.5.7.59. Wymagana możliwość odtworzenia danych
6.5.7.59.1. z zabezpieczanego serwera / komputera
6.5.7.59.2. z konsoli systemu backupowego
6.5.7.60. Wymagana możliwość odtworzenia:
6.5.7.60.1. Pojedynczego pliku
6.5.7.60.2. Zabezpieczanej bazy danych
6.5.7.61. W przypadku systemów Windows 2012, Windows 2016 wymagana funkcjonalność Bare Metal Recovery - automatycznego odtworzenia całego serwera (system operacyjny + ustawienia systemu operacyjnego + dane) w jednym kroku bezpośrednio z oferowanego urządzenia,
6.5.7.62. Funkcjonalność ta powinna być wbudowana w rozwiązanie backupowe.
6.5.7.63. W przypadku odtwarzania danych poprzez interfejs dostępny na zabezpieczanym serwerze/laptopie wymagany mechanizm autentykacji użytkowników spełniający funkcjonalności:
6.5.7.63.1. mechanizm wbudowany w system backupowy
6.5.7.63.2. mechanizm zintegrowany z usługami katalogowymi
6.5.7.63.3. w przypadku wykorzystania AD, użytkownicy będący w domenie nie muszą się logować do systemu backupu w przypadku konieczności:
6.5.7.63.3.1.1. odtworzenia danych,
6.5.7.63.3.1.2. przeszukania zwartości swoich backupów,
6.5.7.63.3.1.3. wykonania backup.
6.5.7.64. 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 odczytać z backupu i przesłać tylko te pliki które znajdują się w backupie a których brakuje na odtwarzanej maszynie.
6.5.7.65. Oferowany system backupu musi być dostępny (dla backupu i odtwarzania) przez 24h na dobę 7 dni w tygodniu, wyklucza się istnienie okresów w przypadku których system backupowy nie może wykonywać backupu lub odtwarzania (tzw. BLACKOUT WINDOWS).
6.5.7.66. Wymaga się aby oferowany system backupu posiadał możliwość bezpośredniego raportowania o błędach do serwisu producenta
6.5.7.67. Oferowany system backupu powinien mieć możliwość instalacji agentów jako plików msi. Wymagana możliwość automatyzacji instalacji agentów poprzez uruchomienie skryptu na zabezpieczanej maszynie, przyporządkowującego maszynę automatycznie do określonej polityki backupowej.
6.5.7.68. Oferowany system backupu powinien posiadać możliwość automatycznej samo-aktualizacji poprzez automatyczne ściąganie nowych wersji oprogramowania od producenta.
6.5.8. Oferowany system backupu musi mieć możliwość automatycznej aktualizacji oprogramowania agentów wykonywanej bezpośrednio z serwera backupu.

6.5.9. W ramach oferowanych licencji wymaga się następujących funkcjonalności – dotyczących monitorowania, raportowania oraz przeszukiwania backupów:
- 6.5.9.1. W ramach dostarczonych licencji musi być zapewniona możliwość monitorowania, raportowania, szczegółowego rozliczania z użycia komponentów systemu backupowego oraz analizy błędów dla środowiska kopii zapasowej Zamawiającego. Wymagana dostępność następujących raportów:
- 6.5.9.2. Podsumowanie zadań backupowych (liczba backupów udanych, nieudanych, aktywnych, łączny rozmiar zbackupowanych danych)
- 6.5.9.3. Podsumowanie zadań odtworzeniowych (liczba odtworzeń udanych, nieudanych, aktywnych, łączny rozmiar odtworzonych danych)
- 6.5.9.4. Zbiorcze procentowe zestawienie udanych zadań backupowych z poszczególnych serwerów
- 6.5.9.5. Zbiorcze zestawienie zabezpieczanych serwerów które w sposób ciągły (kilka razy pod rząd) maja problem z backupami
- 6.5.9.6. Zestawienie zabezpieczanych systemów plików które w ogóle nie są backupowane
- 6.5.9.7. Spodziewany czas odtwarzania zabezpieczanego serwera oraz potencjalnej utraty danych (czas między ostatnim backupem a chwilą awarii)
- 6.5.9.8. Najmniej wiarygodne zabezpieczanych serwery (procent nieudanych backupów)
- 6.5.9.9. Lista najwolniejszych/najszybszych zabezpieczanych maszyn
- 6.5.9.10. Poziom SLA (procentowa liczba udanych backupów) w odniesieniu do poziomu założonego
- 6.5.9.11. Mierzenie poziomu SLA dla poszczególnych zabezpieczanych serwerów przy uwzględnieniu założonego okna backupowego i RPO (punktu do którego przywracamy)
- 6.5.9.12. Liczba danych backupowanych dziennie
- 6.5.9.13. Liczba zadań backupowych dziennie
- 6.5.9.14. Zużycie zasobów na serwerach backupowych (procesor, pamięć, karty sieciowe LAN, SAN)
- 6.5.9.15. Zużycie mediów backupowych i napędów taśmowych
- 6.5.9.16. Aktualna konfiguracja systemu backupowego
- 6.5.9.17. Historia zmian konfiguracji systemu backupowego
- 6.5.9.18. Posiadane licencje systemu backupowego
- 6.5.9.19. Wykorzystanie systemu backupowego przez poszczególne działy / grupy użytkowników (chargeback per cost center)

6.5.10. W ramach dostarczonych licencji wymagana możliwość zaindeksowania oraz przeszukiwania backupów z poziomu graficznego interface'u (GUI), wymagana także możliwość wyszukania dowolnych fraz w nazwach plików.

6.5.11. W ramach oferowanych licencji wymaga się następujących funkcjonalności – dotyczy rozwiązań Continuous Data Protection dla środowisk Vmware.
- 6.5.11.1. integracja na poziomie VMware vCenter Plug-in (ORCHESTRATION, MANAGEMENT) , vSphere Web Client GUI
- 6.5.11.2. wsparcie dla HA, DRS, S-DRS, VMotion, S-VMotion
- 6.5.11.3. możliwość integracji z VMware vRealize Operations Manager

6.5.11.4. rozwiązanie dostarczane w postaci oprogramowania instalowanego na platformie ESXi
6.5.11.5. zabepieczenie dowolnej maszyny wirtualnej wraz z aplikacjami w trybie ciągłym tzn. umożliwiającym odtworzenie do dowolnego punktu w czasie (tzw. PIT – Point In Time), wymagane wsparcie dla VMware ESXi 6.0, 6.5
6.5.11.6. możliwość tworzenia tzw. CONSISTENCY GROUP zapewniających identyczną konsystencję dla przynależących do danej grupy maszyn wirtualnych (VM)
6.5.11.7. zabezpieczenie realizowane za pośrednictwem ciągłej replikacji (a nie za pomocą SNAPSHOT'ów) na poziomie VMDK oraz RDM, niezależnie od użytego storage'u (tzw. Storage Agnostic -warunkiem jest wsparcie przez VMware), wymagane wsparcie dla połączeń: FC, FCoE, iSCSI, NAS oraz DAS
6.5.11.8. wsparcie dla replikacji (bi-directional) asynchronicznej oraz synchronicznej (realizowanej na poziomie dostarczanego oprogramowania), połączonych z mechanizmem tzw. JOURNALING umożliwiającego odnotowanie wszystkich zmian zabezpieczanego środowiska
6.5.11.9. odporność na krótkotrawałe problemy (przeciążenie, zaniki) związane z siecią WAN
6.5.11.10. wbudowana funkcjonalność deduplikacji oraz kompresji w przypadku transmisji danych poprzez WAN
6.5.11.11. wsparcie dla równoległej replikacji zabezpieczanego środowiska do różnych ośrodków docelowych (min. 3-ech), wsparcie dla replikacji równoległej powinno być zapewnione również na poziomie grup konsystencji (CONSISTENCY GROUP)
6.5.11.12. proponowane rozwiązanie powinno umożliwiać:
6.5.11.12.1. stworzenia DISASTER RECOVERY dla całego zabezpieczanego wirtualnego środowiska zbudowanego w oparciu o VMware vSphere
6.5.11.12.2. operacyjne ODTWARZANIE dowolnej maszyny VM wraz z aplikacjami
6.5.11.12.3. MIGRACJI danych w trybie ON-LINE na inne zasoby dyskowe
6.5.11.13. równoległe wsparcie środowisk lokalnych oraz zdalnych, wymagana możliwość pracy w 3-ech trybach, tzw.: CDP (Continuous Data Protection … tryb replikacji lokalnej), CRR (Continuous Remote Replication … tryb replikacji zdalnej), CLR (Continuous Local and Remote Replication … połączenie CDP oraz CLR … tryb replikacji lokalnej oraz zdalnej) w ramach dostarczonych licencji
6.5.11.14. granularność umożliwiająca pominięcie określonych plików VMDK związanych z wirtualnymi serwerami VM objętych protekcją
6.5.11.15. architektura FAULT-TOLERANT, brak pojedynczego punktu awarii
6.5.11.16. działanie rozwiązania będącego przedmiotem zapytania nie może mieć negatywnego wpływu na wydajność zabezpieczanych maszyn i aplikacji
6.5.11.17. wyskalowanie systemu powinno gwarantować RPO (Recovery Point Objective) w przypadku codziennej pracy ciągłej na poziomie pojedynczych sekund

6.5.11.18. proponowana konfiguracja systemu powinna zapewnić następującą retencję przechowywanych kopii bezpieczeństwa:
6.5.11.18.1. RPO=30s z ostatnich 24h,
6.5.11.18.2. RPO=24h z ostatniego tygodnia,
6.5.11.18.3. RPO=1tydzień z ostatniego miesiąca
6.5.11.19. możliwość odtworzenia zabezpieczanego środowiska do DOWOLNEGO punktu w czasie
6.5.11.20. możliwość trybu pracy umożliwiającego objęciem protekcją w sposób automatyczny nowo dodanych maszyn wirtualnych (VM)
6.5.11.21. rozwiązanie powinno dopuszczać zmiany HW na poziomie infrastruktury zabezpieczanego środowiska bez negatywnego wpływu na działanie systemu
6.5.11.22. możliwość użycia mechanizmu typu BOOKMARK dla oznaczenia konsystentnych kopii zabezpieczanych aplikacji
6.5.11.23. wsparcie dla VSS, zapewnienie konsystencji aplikacji na poziomie VSS
6.5.11.24. możliwość automatycznego przeprowadzania operacji typu FAILOVER/FAILBACK do dowolnego punktu w czasie dla określonych produkcyjnych serwerów wirtualnych (VM), w tym: odtworzenie, uruchomienie (z zachowaniem wymaganej sekwencji), konfigurację
6.5.11.25. możliwość automatycznego przeprowadzania operacji typu FAILOVER/FAILBACK do dowolnego punktu w czasie określonych testowych maszyn wirtualnych (VM)
6.5.11.26. możliwość automatycznego zainicjowania procesu REVERSE REPLICATION w przypadku procesów FAILOVER/FAILBACK
6.5.11.27. możliwość przeprowadzania testów DR bez wpływu na zabezpieczane serwery produkcyjne oraz bez konieczności zmian w działaniu replikacji (np.: PAUSE, REVERSE, …)
6.5.11.28. możliwość skryptowego tworzenia planów RECOVERY

6.5.12. Wymagania funkcjonalne dotyczące deduplikatora skonfigurowanego w oparciu o licencje będące przedmiotem zapytania (wymagany rozmiar deduplikatora został podany wcześniej)
6.5.12.1. Rozwiązanie powstałe w wyniku instalacji/konfiguracji licencji będących przedmiotem zapytania musi być przeznaczone do deduplikacji, dedykowane do przechowywania kopii zapasowych. Urządzenie musi spełniać wymagania wyspecyfikowane poniżej.
6.5.12.2. Oprogramowanie będące przedmiotem zapytania musi umożliwiać konfigurację deduplikatora na platformie VMware vSphere 6.5 oraz Microsoft Windows Server 2012 R2 z Hyper-V, o wcześniej określonej przestrzeni (powierzchni użytkowej dedykowanej do przechowywania deduplikatów) bez uwzględniania mechanizmów protekcji, wymagane skalowanie do min. 90TB powierzchni netto w ramach tego samego urządzenia.
6.5.12.3. Deduplikator musi zapewniać jednoczesny dostęp wszystkimi poniższymi protokołami:
6.5.12.3.1. CIFS
6.5.12.3.2. NFS

6.5.12.3.3. deduplikacja na źródle (alternatywnie OST/BOOST/CATALYST)

6.5.12.4. w obrębie oferowanej pojemności urządzenia.

6.5.12.5. Wymagane jest dostarczenie licencji zapewniających funkcjonalność: ENCRYPTION (szyfrowanie) w obrębie maksymalnej wymaganej pojemności urządzenia.

6.5.12.6. Urządzenie musi pozwalać na jednoczesną obsługę minimum 20 strumieni

6.5.12.7. Oferowane urządzenie musi deduplikować 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.

6.5.12.8. Technologia de-duplikacji musi wykorzystywać algorytm bazujący na zmiennym, dynamicznym bloku.

6.5.12.9. Algorytm ten musi samoczynnie i automatycznie dopasowywać się do otrzymywanego strumienia danych. Oznacza to, że urządzenie musi dzielić otrzymany pojedynczy strumień danych na bloki o różnej długości.

6.5.12.10. De-duplikacja zmiennym, dynamicznym blokiem musi oznaczać, że wielkość każdego bloku (na jakie są dzielone dane pojedynczego strumienia backupowego) może być inna niż poprzedniego i jest indywidualnie ustalana przez algorytm urządzenia w celu maksymalnego zwiększenia efektywności deduplikacji.

6.5.12.11. Niedopuszczalna jest deduplikacja stałym blokiem o ustalonej tej samej długości, możliwość manulanej zmiany (bądź poprzez oskryptowanie) długości bloku deduplikacji również nie może zastąpić wymogu automatycznego doboru długości bloku, na jaki dzielony jest każdy strumień danych.

6.5.12.12. Oferowany produkt musi posiadać obsługę mechanizmów globalnej deduplikacji dla danych otrzymywanych jednocześnie wszystkimi protokołami (CIFS, NFS, deduplikacja na źródle) przechowywanych w obrębie całego urządzenia.

6.5.12.13. W obrębie całego urządzenia, raz otrzymany i zapisany w urządzeniu fragment danych nie może być ponownie zapisany bez względu na to, jakim protokołem zostanie ponownie otrzymany.

6.5.12.14. Powyższe oznacza również, że oferowany produkt musi również posiadać obsługę mechanizmów globalnej deduplikacji pomiędzy dowolnymi dwoma udziałami NFS, CIFS. Blok danych otrzymany i zapisany na udział CIFS, nie może zostać ponownie zapisany jeśli trafi do udziału NFS w obrębie tego samego urządzenia (to samo dotyczy deduplikacji na źródle)

6.5.12.15. Przestrzeń składowania zdeduplikowanych danych musi być jedna dla wszystkich protokołów dostępowych.

6.5.12.16. Wszystkie unikalne bloki przed zapisaniem na dysk muszą być dodatkowo skompresowane

6.5.12.17. Oferowane rozwiązanie musi wspierać oferowaną aplikację backup'ową oraz co najmniej: VERITAS NetBackup, EMC Networker, Veeam, Oracle RMAN, Microsoft SQL Server Management Studio.

6.5.12.18. W przypadku współpracy z każdą z poniższych aplikacji:
- 6.5.12.18.1.1. RMAN (dla ORACLE)
- 6.5.12.18.1.2. Microsoft SQL Server Management Studio (dla Microsoft SQL)
- 6.5.12.18.1.3. VERITAS NetBackup
- 6.5.12.18.1.4. EMC NetWorker
- 6.5.12.18.1.5. Veeam

6.5.12.19. urządzenie musi umożliwiać de-duplikację na źródle (deduplikację na zabezpieczanej maszynie) i przesyłanie nowych, nie znajdujących się jeszcze na urządzeniu bloków poprzez sieć LAN.

6.5.12.20. Deduplikacja w wyżej wymienionych przypadkach musi zapewniać aby z serwerów do oferowanego urządzenia były transmitowane poprzez sieć LAN tylko fragmenty danych nie znajdujące się dotychczas na urządzeniu.

6.5.12.21. W przypadku de-duplikacji na źródle poprzez sieć IP (LAN oraz WAN), musi być możliwość szyfrowania komunikacji kluczem minimum 256 bitów.

6.5.12.22. Urządzenie powinno dopuszczać co najmniej 90% utylizację powierzchni netto, bez widocznego spadku wydajności. Dokumentacja urządzenia nie może wskazywać na jakiekolwiek problemy czy obostrzenia, które mogą pojawić się przy zapełnieniu urządzenia poniżej 90%.

6.5.12.23. Oferowane urządzenie musi umożliwiać bezpośrednią replikację danych (bez pośrednictwa dodatkowych modułów) do drugiego urządzenia tego samego typu oraz deduplikatora sprzętowego będącego przedmiotem zapytania, wymagane następujące tryby pracy replikacji:
- 6.5.12.23.1. jeden do jednego,
- 6.5.12.23.2. wiele do jednego,
- 6.5.12.23.3. jeden do wielu,
- 6.5.12.23.4. kaskadowej (urządzenie A replikuje dane do urządzenia B które te same dane replikuje do urządzenia C).

6.5.12.24. Replikacja musi się odbywać w trybie asynchronicznym. Transmitowane mogą być tylko te fragmenty danych (bloki) które nie znajdują się na docelowym urządzeniu, rozwiązanie replikacyjne nie powinno wymagać aby obszar na który dane są replikowane był większy od obszaru źródłowego (replikowanego) w przypadku schematu „jeden do jednego" – weryfikacja na podstawie ogólnie dostępnej dokumentacji producenta oraz zaleceń. Ewentualna licencja na replikację musi być dostarczona w ramach postępowania.

6.5.12.25. W przypadku wykorzystania portów Ethernet do replikacji urządzenie musi umożliwiać przyjmowanie backupów, odtwarzanie danych, przyjmowanie strumienia replikacji, wysyłanie strumienia replikacji tymi samymi portami.

6.5.12.26. W przypadku replikacji danych między dwoma urządzeniami kontrolowanej przez systemy: oferowaną aplikację backupową/ VERITAS NetBackup /EMC NetWorker muszą być możliwe do uzyskania jednocześnie wszystkie następujące funkcjonalności:
- 6.5.12.26.1. replikacja odbywa się bezpośrednio między dwoma urządzeniami bez udziału serwerów pośredniczących

6.5.12.26.2. replikacji podlegają tylko te fragmenty danych, które nie znajdują się na docelowym urządzeniu

6.5.12.26.3. replikacja zarządzana jest z poziomu aplikacji backupowej, aplikacja backupowa posiada informację o obydwu kopiach zapasowych znajdujących się w obydwu urządzeniach bez konieczności przeprowadzania procesu inwentaryzacji

6.5.12.27. Narzut na wydajność związany z replikacją nie może zmniejszyć wydajności urządzenia o więcej niż 10%.

6.5.12.28. Wymagana możliwość ograniczenia pasma używanego do replikacji między dwoma urządzeniami.

6.5.12.29. Deduplikator musi umożliwiać wykonywanie oraz przechowywanie SnapShot'ów (min. 50 jednocześnie), czyli możliwość zamrożenia obrazu danych (stanu backupów) w urządzeniu na określoną chwilę. Oferowane urządzenie musi również umożliwiać odtworzenie danych ze Snapshot'u.

6.5.12.30. Odtworzenie danych ze Snapshot'u nie może wymagać konieczności nadpisania danych produkcyjnych jak również nie może oznaczać przerwy w normalnej pracy urządzenia (przyjmowania backupów / odtwarzania).

6.5.12.31. Deduplikator musi pozwalać na podział na logiczne części. Dane znajdujące się w każdej logicznej części muszą być między sobą de-duplikowane (globalna de-duplikacja między logicznymi częściami urządzenia).

6.5.12.32. Deduplikator 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.

6.5.12.33. Dla każdej z 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 i nie mogą widzieć żadnych innych zasobów oferowanego urządzenia.

6.5.12.34. Wymagana możliwość zaprezentowania każdej z logicznych części oferowanego urządzenia, jako niezależnego urządzenia dostępnego poprzez:

6.5.12.34.1. CIFS,

6.5.12.34.2. NFS,

6.5.12.34.3. wymagany protokół umożliwiający deduplikację na źródle.

6.5.12.35. Urządzenie musi automatycznie usuwać przeterminowane dane (bloki danych nie należące do backupów o aktualnej retencji) w procesie czyszczenia.

6.5.12.36. Proces usuwania przeterminowanych danych (czyszczenia) nie może uniemożliwiać pracy procesów backupu / odtwarzania danych (zapisu / odczytu danych z zewnątrz do systemu), nie może wymagać (zgodnie z oficjalnymi zaleceniami producenta) definiowania BLACKOUT WINDOW czyli okna czasowego dedykowanego dla procesu czyszczenia podczas którego nie są realizowane procesy backupu / odtwarzania danych czy replikacji.

6.5.12.37. Wymagana możliwość zdefiniowania maksymalnego obciążenia urządzenia procesem usuwania przeterminowanych danych (poziomu obciążenia procesora).
6.5.12.38. Wymagana możliwość zdefiniowania czasu w którym wykonywany jest proces usuwania przeterminowanych danych (czyszczenia).
6.5.12.39. Standardowa częstotliwość usuwania przeterminowanych danych (czyszczenie) nie powinna być większa niż 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).
6.5.12.40. Urządzenie musi mieć możliwość zarządzania poprzez:
6.5.12.40.1. interfejs graficzny dostępny z przeglądarki internetowej,
6.5.12.40.2. poprzez linię komend (CLI) dostępną z poziomu ssh (secure shell).
6.5.13. Wymagania funkcjonalne dotyczące środowiska umożliwiającego zarządzanie środowiskiem dedykowanym do zabezpieczania danych stworzonego w oparciu o oprogramowanie będące przedmiotem zapytania
6.5.13.1. Możliwość uruchomienia zdalnych konsol dla:
6.5.13.1.1. aplikacji backup'owej,
6.5.13.1.2. systemu dedykowanego do raportowania,
6.5.13.1.3. systemu dedykowanego do przeszukiwania danych backup'owych,
6.5.13.1.4. systemu CDP,
6.5.13.1.5. deduplikatorów.
6.5.13.2. stworzonych w oparciu o oprogramowanie będące przedmiotem zapytania, możliwość zdalnego uruchomienia oraz wyłączenia w/w komponentów
6.5.13.3. Zapewnienie podglądu on-line takich elementów jak:
6.5.13.3.1. aktywność procesów backup'owych,
6.5.13.3.2. aktywność procesów replikacyjnych,
6.5.13.3.3. aktualny status,
6.5.13.3.4. alarmy.
W przypadku zaoferowanej aplikacji backup'owej oraz deduplikatora.
6.5.13.4. Możliwość zarządzania procesem wyszukiwania danych backup'owych
6.5.13.5. Integracja z oferowanym rozwiązaniem dedykowanym do raportowania, możliwość inicjowania raportów.
6.6. Serwer backup w ilości 1 szt. o parametrach nie gorszych niż:
6.6.1. Obudowa:
6.6.1.1. Obudowa Rack o wysokości max 1U z możliwością instalacji min. 10 dysków 2.5" Hot-Plug wraz z kompletem szyn umożliwiających montaż w szafie rack.
6.6.1.2. Przedni panel zamykany na klucz oraz możliwość dodania organizatora do kabli.
6.6.1.3. Obudowa musi mieć możliwość wyposażenia w kartę umożliwiającą dostęp bezpośredni poprzez urządzenia mobilne - serwer musi posiadać możliwość konfiguracji oraz monitoringu najważniejszych komponentów

serwera przy użyciu dedykowanej aplikacji mobilnej (Android/ Apple iOS) przy użyciu jednego z protokołów NFC/ BLE/ WIFI.

6.6.2. Płyta główna z możliwością zainstalowania do dwóch procesorów. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym.

6.6.3. Chipset dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych

6.6.4. Zainstalowane dwa procesory ośmiordzeniowe, min. 1.8 GHz, klasy x86 dedykowane do pracy z zaoferowanym serwerem umożliwiające osiągnięcie wyniku min. 65.3 w teście SPECrate2017_int_base dostępnym na stronie www.spec.org dla dwóch procesorów(test wykonany na oferowanym modelu serwera).

6.6.5. Pamięć RAM:

6.6.5.1. 64GB (2x32GB) DDR4 RDIMM 2666MT/s,

6.6.5.2. na płycie głównej powinno znajdować się minimum 16 slotów przeznaczonych do instalacji pamięci.

6.6.5.3. Płyta główna powinna obsługiwać do 1TB pamięci RAM.

6.6.6. Funkcjonalność pamięci RAM:Memory Rank Sparing, Memory Mirror, Failed DIMM isolation, Memory Address Parity Protection, Memory Thermal Throttling

6.6.7. Interfejsy sieciowe/FC/SAS Wbudowane minimum 2 porty typu Gigabit Ethernet Base-T 1Gb/s.

6.6.8. Dodatkowa karta sieciowa dwuportowa 10Gb SFP+ wraz z kompletem wkładek Short Range.

6.6.9. Zainstalowane 8 dysków 2,5” 2.4TB SAS 10k typu Hot-Plug.

6.6.10. Możliwość instalacji dwóch dysków M.2 SATA o pojemności min. 480GB oraz możliwość konfiguracji w RAID 1 – Te dyski nie mogą zajmować slotów na dyski z przodu obudowy.

6.6.11. Kontroler RAID Sprzętowy kontroler dyskowy, możliwe konfiguracje poziomów RAID: 0, 1, 5, 10, 50

6.6.12. Napęd optyczny Brak napędu optycznego

6.6.13. Wbudowane porty min. 1 port USB 2.0, 1 port micro-USB oraz min. 3 porty USB 3.0, 2 porty RJ45, 2 porty VGA (1 na przednim panelu obudowy, drugi na tylnym), min. 1 port RS232.

6.6.14. Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1440x900

6.6.15. Wentylatory Redundantne.

6.6.16. Zasilacze Redundantne, Hot-Plug maksymalnie 550W.

6.6.17. Bezpieczeństwo:

6.6.17.1. Wbudowany moduł TPM min. 1.2

6.6.17.2. Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą.

6.6.18. System operacyjny Microsoft Windows Server Standard 2019

6.6.19. Możliwość wyposażenia w panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS’u, zasilaniu oraz temperaturze.

6.6.20. Karta Zarządzania Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca:
- 6.6.20.1. zdalny dostęp do graficznego interfejsu Web karty zarządzającej;
- 6.6.20.2. zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera);
- 6.6.20.3. szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika;
- 6.6.20.4. możliwość podmontowania zdalnych wirtualnych napędów;
- 6.6.20.5. wirtualną konsolę z dostępem do myszy, klawiatury;
- 6.6.20.6. wsparcie dla IPv6;
- 6.6.20.7. wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish;
- 6.6.20.8. możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer;
- 6.6.20.9. możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer;
- 6.6.20.10. integracja z Active Directory;
- 6.6.20.11. możliwość obsługi przez dwóch administratorów jednocześnie;
- 6.6.20.12. wsparcie dla dynamic DNS;
- 6.6.20.13. wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej.
- 6.6.20.14. możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera
- 6.6.20.15. możliwość zarządzania do 100 serwerów bezpośrednio z konsoli karty zarządzającej pojedynczego serwera
- 6.6.20.16. karta z możliwością wyposażenia we wbudowaną wewnętrzną pamięć SD lub USB o pojemności 16GB do przechowywania sterowników i firmware'ów komponentów serwera, umożliwiająca szybką instalację wspieranych systemów operacyjnych.

6.6.21. Dodatkowe oprogramowanie umożliwiające zarządzanie poprzez sieć, spełniające minimalne wymagania:
- 6.6.21.1. wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych;
- 6.6.21.2. możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta;
- 6.6.21.3. wsparcie dla protokołów – WMI, SNMP, IPMI, WSMan, Linux SSH;
- 6.6.21.4. możliwość oskryptowywania procesu wykrywania urządzeń;
- 6.6.21.5. możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram;
- 6.6.21.6. szczegółowy opis wykrytych systemów oraz ich komponentów;
- 6.6.21.7. możliwość eksportu raportu do CSV, HTML, XLS;
- 6.6.21.8. grupowanie urządzeń w oparciu o kryteria użytkownika;
- 6.6.21.9. automatyczne skrypty CLI umożliwiające dodawanie i edycję grup urządzeń;
- 6.6.21.10. szybki podgląd stanu środowiska;
- 6.6.21.11. podsumowanie stanu dla każdego urządzenia;
- 6.6.21.12. szczegółowy status urządzenia/elementu/komponentu;

6.6.21.13. generowanie alertów przy zmianie stanu urządzenia;
6.6.21.14. filtry raportów umożliwiające podgląd najważniejszych zdarzeń;
6.6.21.15. integracja z service desk producenta dostarczonej platformy sprzętowej;
6.6.21.16. możliwość przejęcia zdalnego pulpitu;
6.6.21.17. możliwość podmontowania wirtualnego napędu;
6.6.21.18. kreator umożliwiający dostosowanie akcji dla wybranych alertów;
6.6.21.19. możliwość importu plików MIB;
6.6.21.20. przesyłanie alertów „as-is" do innych konsol firm trzecich;
6.6.21.21. aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania);
6.6.21.22. możliwość instalacji sterowników i oprogramowania wewnętrznego bez potrzeby instalacji agenta;
6.6.21.23. możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów;
6.6.21.24. moduł raportujący pozwalający na wygenerowanie następujących informacji: nr seryjny sprzętu, konfiguracja poszczególnych urządzeń, wersje oprogramowania wewnętrznego, obsadzenie slotów PCIe i gniazd pamięci, informację o maszynach wirtualnych, aktualne informacje o stanie gwarancji, adresy IP kart sieciowych.

6.6.22. Certyfikaty Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2008 oraz ISO-14001.
6.6.23. Serwer musi posiadać deklaracja CE.
6.6.24. Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows" dla systemów Microsoft Windows Server 2012, 2012 R2, Microsoft Windows Server 2016, Microsoft Windows Server 2019.
6.6.25. Warunki gwarancji:
6.6.25.1. Firma serwisująca musi posiadać ISO 9001:2008 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty.
6.6.25.2. Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji serwera
6.6.25.3. W przypadku awarii dyski twarde pozostają własnością Zamawiającego.
6.6.26. Dokumentacja użytkownika:
6.6.26.1. Zamawiający wymaga dokumentacji w języku polskim lub angielskim.
6.6.26.2. Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.

6.7. Zasilacz UPS 1 szt. o parametrach nie gorszych niż:
6.7.1. Moc 10000VA/10000W,
6.7.2. Zakres napięcia 120- 276V,
6.7.3. Zakres częstotliwości wejściowej, kiedy energia jest pobierana z sieci, a bateria jest doładowywana 40Hz-70hz,
6.7.4. Zniekształcenia THDi <3%,
6.7.5. Faza 1 fazowy z uziemieniem,
6.7.6. Napięcie 220V / 230V / 240V,

6.7.7. Regulacja napięcia ± 1%,
6.7.8. Częstotliwość 50Hz / 60Hz ± 0,05Hz,
6.7.9. Współczynnik mocy (PF) 1,
6.7.10. Współczynnik szczytu 3:1,
6.7.11. THDv (zniekształcenia harmoniczne) < 1% THD obciążenie liniowe |<5% THD obciążenie nie liniowe,
6.7.12. Kształt napięcia (wyjściowego) Sinusoida,
6.7.13. Praca równoległa do 3 jednostek,
6.7.14. Wydajność:
6.7.14.1.1. Tryb liniowy 95%,
6.7.14.1.2. Tryb bateryjny 92%,
6.7.14.1.3. Tryb ECO 98%.
6.7.15. Czas ładowania maksymalny 3h do 90%
6.7.16. Łańcuch baterii Konfigurowalny 192V ~ 240V
6.7.17. CZAS PRZEŁĄCZENIA
6.7.17.1.1. falownik « » bateryjny 0 ms,
6.7.17.1.2. falownik « » bypass 0 ms,
6.7.17.1.3. eco « » bateryjny 10 ms.
6.7.18. Wyświetlacz LCD,
6.7.19. Wymiary maksymalne (szer. X wys. X gł.) 438 x 86 x 573 (UPS) 438 x 129 x 593 (baterie),
6.7.20. Wysokość w szafie 19 2U (UPS) 3U (baterie),
6.7.21. Poziom hałasu w obrębie 1m <55dB,
6.7.22. Temperatura pracy 0°C – 40°C,
6.7.23. komunikacja RS232/USB,
6.7.24. Zewnętrzny slot na kartę SNMP,
6.7.25. Alarmy dźwiękowe,
6.7.26. PDU montowane w szafie poziomo PDU zarządzane z oprogramowania UPS, z wydzielonymi 2 sekcjami wyjść każda składająca się z (2x IEC16 +1xIEC19), oraz z listwy zaciskowej i By-passu zewnętrznego
6.7.27. Zakres napięcia By-passu 176~264Vac,
6.7.28. EPO,
6.7.29. Moduł bateryjny 2 x UPS GT S 11 RT EBM szafka 16x7Ah
6.7.30. Karta SNMP,
6.7.31. Szyny montażowe,
6.7.32. Bypass Rack 19",
6.7.33. Listwy zasilające zgodne z UPS 2 sztuki (10xC13+2xC19)

6.8. Szafa RACK w ilości 1 szt. o parametrach:
6.8.1. 42U,
6.8.2. Wymiary: 800/1000 mm (szer./gł.),
6.8.3. Drzwi perforowane z przodu,
6.8.4. drzwi dzielone perforowane z tyłu,
6.8.5. moduł wentylatorów wraz z termostatem,
6.8.6. organizer do okablowania.

6.9. Instalacja oferowanej macierzy dyskowej
6.9.1. Montaż macierzy dyskowej w szafie Rack,
6.9.2. Podłączenie macierzy do infrastruktury sieci LAN,

6.9.3. Podłączenie macierzy do infrastruktury sieci SAN,
6.9.4. Inicjalizacja macierzy dyskowej,
6.9.5. Aktualizacja oprogramowania układowego (firmware) do najnowszej, stabilnej, zalecanej przez producenta wersji,
6.9.6. Konfiguracja przestrzeni dyskowej (pule dyskowe, grupy RAID),
6.9.7. Konfiguracja zasobów dyskowych dedykowanych dla środowiska wirtualizacji z wykorzystaniem blokowych protokołów dostępu,
6.9.8. Konfiguracja uprawnień dostępu do danych blokowych,
6.9.9. Testy wydajności,
6.9.10. Optymalizacja wydajności.

6.10. Montaż oferowanych serwerów fizycznych
6.10.1. Montaż serwerów w szafie Rack,
6.10.2. Podłączenie serwerów do zasilania,
6.10.3. Konfiguracja konsoli zdalnego dostępu,
6.10.4. Aktualizacja mikrokodu (firmware) komponentów serwera do najnowszej zalecanej przez producenta wersji,
6.10.5. Podłączenie maszyn fizycznych do infrastruktury sieci LAN/SAN.

6.11. Konfiguracja sieci SAN
6.11.1. Montaż wkładek SFP w przełącznikach FC,
6.11.2. Podłączenie oferowanej macierzy do sieci FC,
6.11.3. Podłączenie oferowanych serwerów do sieci FC,
6.11.4. Definicja stref dostępu w sieci SAN (zoning), a w szczególności:
6.11.4.1. Definicja aliasów,
6.11.4.2. Definicja stref dostępu dla zapewnienia dostępu do danych macierzy dyskowych dla maszyn fizycznych.

6.12. Wirtualizacja środowiska serwerowego
6.12.1. Instalacja systemu wirtualizacji na oferowanych maszynach fizycznych,
6.12.2. Konfiguracja parametrów serwerów wirtualizacyjnych: adresacja IP, routing, DNS, synchronizacja czasu,
6.12.3. Rejestracja serwerów wirtualizacji serwerowej w macierzy dyskowej,
6.12.4. Prezentacja przestrzeni macierzy dyskowej dla serwerów wirtualizacyjnych,
6.12.5. Organizacja systemu plików na wydzielonych zasobach macierzy dyskowej dedykowanych do składowania plików maszyn wirtualnych,
6.12.6. Konfiguracja sieci wirtualnych dedykowanych dla maszyn wirtualnych oraz mechanizmów migracji maszyn wirtualnych pomiędzy maszynami fizycznymi, w trybie on-line.
6.12.7. Instalacja oprogramowania służącego do centralnego zarządzania, monitorowania
i konfiguracji środowiskiem wirtualizacji serwerowej
6.12.8. Konfiguracja klastra wysokiej dostępności (High Availability)
6.12.9. Konfiguracja mechanizmu migracji maszyn wirtualnych pomiędzy maszynami fizycznymi w trybie on-line
6.12.10. Konwersja maszyn fizycznych do środowiska wirtualnego:
6.12.10.1. Konwersja serwera fizycznego MS SQL 2012 do klastra HA,
6.12.10.2. Przeniesienie istniejących maszyn wirtualnych do nowego środowiska.
6.12.11. Instalacja mechanizmu automatyzacji aktualizacji środowiska
6.12.12. Aktualizacja środowiska wirtualnego do najnowszej stabilnej wersji

6.12.13. Testy mechanizmów migracji maszyn wirtualnych pomiędzy maszynami fizycznymi
6.12.14. Testy mechanizmów klastra wysokiej dostępności
6.13. Migracja kontrolerów domeny do klastra HA.
6.13.1. Zainstalowanie dwóch maszyn wirtualnych z system operacyjnym MS Windows Server (po jednej na każdy z hostów fizycznych) w klastrze i wypromowanie ich na kontrolery domeny w istniejącym lesie domen
6.13.2. Transfer wszystkich 5-ciu ról FSMO na jeden z nowoutworzonych kontrolerów domeny
6.13.3. Weryfikacja poprawności replikacji bazy Active Directory oraz wolumenu SYSVOL pomiędzy kontrolerami domeny
6.13.4. Usunięcie roli kontrolera domeny z obu serwerów fizycznych
6.13.5. Weryfikacja rekordów DNS i bazy AD i (w razie potrzeby) ręczne „uporządkowanie" metadanych w bazie AD
6.13.6. Weryfikacja poprawności replikacji bazy Active Directory oraz wolumenu SYSVOL pomiędzy kontrolerami domeny
6.13.7. Instalacja i konfiguracja roli serwera DHCP na kontrolerze domeny
6.13.8. Weryfikacja przydzielania adresacji TCP/IP na stacjach roboczych
6.14. Instalacja i konfiguracja roli „Serwer Plików"
6.14.1. Instalacja nowej maszyny wirtualnej z system operacyjnym MS Windows Server w klastrze
6.14.2. Instalacja roli „Serwer Plików" (Fileserver)
6.14.3. Utworzenie udziałów sieciowych i struktury katalogów oraz nadanie im uprawnień dla grup istniejących w Active Directory
6.14.4. Utworzenie polityk grupowych (GPO) na kontrolerze domeny, umożliwiających automatyczne mapowanie wskazanych udziałów sieciowych grupom użytkowników
6.14.5. Weryfikacja poprawności przetwarzania utworzonych polityk na stacjach roboczych
6.15. Instalacja i konfiguracja roli „Serwer Wydruków"
6.15.1. Instalacja nowej maszyny wirtualnej z system operacyjnym MS Windows Server w klastrze
6.15.2. Instalacja roli „Serwer Wydruków" (Printserver)
6.15.3. Instalacja sterowników do drukarek sieciowych
6.15.4. Udostępnienie drukarek i nadanie uprawnień wydruku odpowiednim grupom użytkowników w Active Directory
6.15.5. Utworzenie polityk grupowych (GPO) na kontrolerze domeny, umożliwiających automatyczne mapowanie udostępnionych drukarek sieciowych grupom użytkowników
6.15.6. Weryfikacja poprawności przetwarzania utworzonych polityk na stacjach roboczych.
6.16. Instalacja i konfiguracja roli „Serwer Aktualizacji"
6.16.1. Instalacja nowej maszyny wirtualnej z system operacyjnym MS Windows Server w klastrze
6.16.2. Instalacja roli „Serwer Aktualizacji" (WSUS)
6.16.3. Konfiguracja ustawień w konsoli zarządzającej (klasyfikacje produktów Microsoft, wersje językowe, kategorie aktualizacji, automatyczne zatwierdzanie)

6.16.4. Utworzenie polityki grupowej (GPO) na kontrolerze domeny, umożliwiającej stacjom roboczym i laptopom automatyczne pobieranie aktualizacji wybranych produktów Microsoft z serwera aktualizacji (WSUS)
6.16.5. Weryfikacja poprawności przetwarzania utworzonych polityk na stacjach roboczych
6.17. Wdrożenie systemu backupowego
6.17.1. Montaż serwera fizycznego, dedykowanego do zadań serwera kopii zapasowych w szafie rack
6.17.2. Podłączenie serwera do sieci LAN/SAN
6.17.3. Konfiguracja serwera fizycznego
6.17.3.1. parametry dostępu do interfejsu zdalnego zarządzania serwerem
6.17.3.2. konfiguracja lokalnej przestrzeni dyskowej
6.17.4. Aktualizacja mikrokodu (firmware) komponentów serwera do najnowszej zalecanej przez producenta wersji.
6.17.5. Instalacja systemu wirtualizacji na oferowanym serwerze
6.17.6. Konfiguracja parametrów serwera wirtualizacyjnego: adresacja IP, routing, DNS, synchronizacja czasu
6.17.7. Prezentacja przestrzeni dyskowej dla serwera wirtualizacyjnego
6.17.8. Organizacja systemu plików na wydzielonych zasobach dedykowanych do składowania plików maszyn wirtualnych
6.17.9. Instalacja wirtualnego systemu backupu
6.17.9.1. Inicjalizacja wirtualnego systemu backupu (zapewnienie maszynie wirtualnej wymaganych zasobów CPU, pamięci RAM i przestrzeni dyskowej)
6.17.9.2. Konfiguracja parametrów sieciowych
6.17.10. Instalacja wirtualnego deduplikatora dyskowego
6.17.10.1. Inicjalizacja wirtualnego deduplikatora dyskowego (zapewnienie maszynie wirtualnej wymaganych zasobów CPU, pamięci RAM i przestrzeni dyskowej)
6.17.10.2. Konfiguracja parametrów sieciowych
6.17.10.3. Konfiguracja protokołów dostępowych do urządzenia
6.17.10.4. Konfiguracja przestrzeni dyskowej dedykowanej dla składowania unikatowych bloków
6.17.10.5. Prezentacja danych dla systemu backupu
6.17.11. Konfiguracja polityk ochrony dla wskazanych maszyn wirtualnych/fizycznych:
6.17.11.1. Definicje typów kopii zapasowych (obraz maszyny, dane plikowe, dane aplikacyjne w trybie online, dane aplikacyjne w trybie offline)
6.17.11.2. Definicja harmonogramów
6.17.11.3. Definicja miejsc składowania kopii zapasowych
6.17.11.4. Definicja polityk retencji
6.17.11.5. Testy odtwarzania danych
6.18. Instalacja oferowanej szafy RACK
6.18.1. Montaż szafy w pomieszczeniu serwerowni,
6.18.2. Zasilenie szafy z rodzielni elektrycznej,
6.18.3. Instalacja listw zasilających,
6.18.4. Instalacja modułów wentylatorowych.

6.19. Montaż oferowanego UPS
6.19.1. Przygotowanie przyłącza do zasilenia UPS z istniejącej rozdzielni,
6.19.2. Podłączenie modułów bateryjnych,
6.19.3. Instalacja karty SNMP,
6.19.4. Instalacja BYPASS,
6.19.5. Testy przełączeniowe.

7. Wymagane jest przeszkolenie maksymalnie pięciu osób wskazanych przez Zamawiającego z zakresu obsługi dostarczonych urządzeń i oprogramowania obejmującego całą funkcjonalności oraz ćwiczenia w praktycznym wykorzystaniu dostarczonego oprogramowania i urządzeń w wymiarze minimum trzy dni szkoleniowe min. 7 godzin szkolenia dziennie.
8. Zamawiający dopuszcza możliwość przeszkolenia pracowników w miejscu wskazanym przez Wykonawcę jednakże koszty związane przejazdem, noclegiem (w hotelu / ośrodku / pensjonacie itp. odpowiadającym standardowi pokoju w hotelu 3 gwiazdkowym) i całodziennym wyżywieniem wszystkich uczestników szkolenia pokrywa Wykonawca.
9. Wykonawca w okresie gwarancji zapewni wparcie techniczne (help desk):
   9.1. Wykonawca w uzgodnionych z Zamawiających minimum dwóch dniach roboczych każdego tygodnia okresu gwarancji zapewni wsparcie telefoniczne w godzinach 09:00 – 15:00.
   9.2. W przypadku złożonych zagadnień zapewni kontakt e-mail oraz zagwarantuje, iż wszystkie odpowiedz na zgłoszone pod wskazany adres zagadnienia zostaną odesłane w terminie do trzech dni roboczych od ich wysłania przez Zamawiającego.