**SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA**

**Zadanie 1: Rozbudowa serwerowni.**

Wymagany termin dostawy sprzętu w całości **do 30.11.2020 r.**

Zamawiający wymaga przeprowadzenia montażu, instalacji, konfiguracji zamawianego sprzętu i oprogramowania oraz przeszkolenia pracowników Działu Informatyki Białostockiego Centrum Onkologii **do 31.12.2020 r.** (w zakresie określonym w dalszej części Załącznika nr 3.1).

1. **System zapewniający kopię zapasową serwerów oraz macierzy.**
2. Zamawiający wymaga, aby dostarczony deduplikator oraz oprogramowanie do backupu pochodziło od tego samego producenta w celu zapewnienia pełnej kompatybilności sprzętu i oprogramowania oraz świadczenia jednolitego, powiązanego serwisu zarówno sprzętu jak i oprogramowania.
3. Zamawiający wymaga dostarczenia, uruchomienia oraz konfiguracji całości dostarczonego systemu wraz z przeprowadzeniem testów wykonywania kopii zapasowych oraz ich odzyskiwania.
4. Zamawiający wymaga przeprowadzenia min. 5-dniowego szkolenia z obsługi i zarządzania dostarczonym systemem dla dwóch osób. Szkolenie ma odbyć się w siedzibie producenta lub dystrybutora oferowanego systemu całkowicie na koszt Wykonawcy.
5. Wykonawca zobowiązuje się dokonać instalacji oraz konfiguracji całego sprzętu w infrastrukturze Zamawiającego.
6. Wymagany okres gwarancji jest parametrem podlegającym ocenie w kryterium „Gwarancja”, i określony w pkt III.7 SIWZ.
7. Wykonawca zobowiązuje się udzielić wsparcia technicznego w obsłudze sprzętu przez zadeklarowany okres gwarancji.

**A.1. Wymagane parametry:**

1. Urządzenie musi być przeznaczone do de-duplikacji, dedykowane do przechowywania kopii zapasowych.
2. Urządzenie musi oferować przestrzeń 48TB netto (powierzchni użytkowej dedykowanej do przechowywania deduplikatów) bez uwzględniania mechanizmów protekcji, wymagane skalowanie do 288TB powierzchni netto w ramach tego samego urządzenia, rozbudowa do wymaganej pojemności powinna być możliwa poprzez dołożenie kolejnych półek z dyskami oraz odpowiednich licencji, rozbudowa nie może pociągać konieczności dołożenia dodatkowych kontrolerów, nie może być również realizowana poprzez zwielokrotnienie ilości oferowanych urządzeń.
3. Oferowane urządzenie musi posiadać minimum:
4. 4 porty Ethernet 10 Gb/s OP – wymagana możliwość obsługi każdym z portów protokołów CIFS, NFS, de-duplikacja na źródle;
5. 4 porty FC 16 Gb/s – wymagana możliwość obsługi każdym z portów protokołów VTL, de-duplikacja na źródle;

Oferowane urządzenie musi umożliwiać rozbudowę o co najmniej (bez konieczności usuwania ww. portów Ethernet) 4 porty Ethernet 10 Gb/s RJ45 – wymagana możliwość obsługi każdym z portów protokołów CIFS, NFS, de-duplikacja na źródle;

1. Oferowane urządzenie musi zapewniać jednoczesny dostęp wszystkimi poniższymi protokołami, czyli dla Ethernet:
   * CIFS, NFS, de-duplikacja na źródle (alternatywnie OST/BOOST/CATALYST)

oraz jednocześnie dla FC (po dodaniu odpowiednich portów):

* + VTL, de-duplikacja na źródle (alternatywnie OST/BOOST/CATALYST).

w obrębie oferowanej pojemności urządzenia.

1. Wymagane jest dostarczenie licencji pozwalającej na jednoczesną obsługę protokołów CIFS, NFS, VTL w przypadku pojemności oferowanego urządzenia na poziomie 288TB netto co oznacza, że rozbudowa urządzenia z wymaganych 48TB netto do 288TB netto nie może pociągać konieczności dodania kolejnych licencji w przypadku wykorzystywania protokołów CIFS, NFS, VTL w obrębie wymaganej maksymalnej pojemności urządzenia.
2. Wymagane jest dostarczenie licencji zapewniających funkcjonalność: WORM (blokada skasowania danych) w obrębie maksymalnej wymaganej pojemności urządzenia.

Blokada skasowania danych musi chronić plik w zdefiniowanym czasie przed usunięciem bądź modyfikacją.

Blokada skasowania danych musi działać w dwóch trybach (do wyboru przez administratora):

1. umożliwiającym zdjęcia blokady przed upływem ważności danych,
2. nieumożliwiającym zdjęcia blokady przed upływem ważności danych (compliance).
3. Wymagane jest dostarczenie licencji zapewniających funkcjonalność: ENCRYPTION (szyfrowanie) w obrębie maksymalnej wymaganej pojemności urządzenia.
4. Wymaga się, aby pojedyncze urządzenie dla maksymalnej pojemności (48TB netto) osiągało zagregowaną wydajność w przypadku protokołów CIFS, NFS na poziomie co najmniej 15 TB/h (dane podawane przez producenta w ogólnie dostępnych dokumentach) oraz co najmniej 33 TB/h z wykorzystaniem de-duplikacji na źródle (dane podawane przez producenta w ogólnie dostępnych dokumentach).
5. Urządzenie musi pozwalać na jednoczesną obsługę minimum 560 strumieni w tym jednocześnie:
6. zapis danych minimum 400 strumieniami,
7. odczyt danych minimum 110 strumieniami,
8. replikacja minimum 50 strumieniami,

pochodzących z różnych aplikacji oraz dowolnych protokołów (CIFS, NFS, VTL, de-duplikacja na źródle) oraz dowolnych interfejsów (FC, LAN) w tym samym czasie.

Wymienione wartości 560 jednoczesnych strumieni dla wszystkich protokołów (czyli jednocześnie 400 dla zapisu, jednocześnie 110 strumieni dla odczytu oraz jednocześnie 50 strumieni dla replikacji) musi mieścić w przedziale oficjalnie rekomendowanym i wspieranym przez producenta urządzenia.

Wszystkie zapisywane strumienie muszą podlegać globalnej de-duplikacji przed zapisem na dysk (in-line) jak opisano w niniejszej specyfikacji.

1. Oferowane urządzenie musi mieć możliwość emulacji następujących bibliotek taśmowych:
2. StorageTek L180,
3. IBM 3500.
4. Oferowane urządzenie musi mieć możliwość emulacji napędów taśmowych LTO1, LTO2, LTO3, LTO4, LTO5.
5. Urządzenie musi umożliwiać eksport oraz import definicji bibliotek taśmowych. Musi być możliwość eksportu / importu definicji bibliotek taśmowych.
6. Urządzenie musi umożliwiać jednoczesną emulację min. 500 napędów oraz 60 000 slotów w przypadku trybu VTL.
7. Oferowane urządzenie musi de-duplikować dane in-line przed zapisem na nośnik dyskowy. Na wewnętrznych dyskach urządzenia nie mogą być zapisywane dane w oryginalnej postaci (niezdeduplikowanej) z jakiegokolwiek fragmentu strumienia danych przychodzącego do urządzenia.
8. Technologia de-duplikacji musi wykorzystywać algorytm bazujący na zmiennym, dynamicznym bloku.

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.

1. 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.
2. Niedopuszczalna jest de-duplikacja stałym blokiem o ustalonej tej samej długości, możliwość manualnej zmiany (bądź poprzez oskryptowanie) długości bloku deduplikacji również nie może zastąpić wymogu automatycznego doboru długości bloku na jaki dzielony jest każdy strumień danych.
3. Oferowany produkt musi posiadać obsługę mechanizmów globalnej de-duplikacji dla danych otrzymywanych jednocześnie wszystkimi protokołami (CIFS, NFS, VTL, deduplikacja na źródle) przechowywanych w obrębie całego urządzenia.

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.

1. Powyższe oznacza również, że oferowany produkt musi również posiadać obsługę mechanizmów globalnej de-duplikacji pomiędzy dowolnymi dwoma wirtualnymi bibliotekami. Blok danych otrzymany i zapisany w wirtualnej bibliotece A, nie może zostać ponownie zapisany, jeśli trafi do innej wirtualnej biblioteki (wirtualnej biblioteki B) w obrębie tego samego urządzenia (to samo dotyczy udziałów NFS/CIFS).
2. Przestrzeń składowania zde-duplikowanych danych musi być jedna dla wszystkich protokołów dostępowych.
3. Proces de-duplikacji musi odbywać się in-line – w pamięci urządzenia, przed zapisem danych na nośnik dyskowy. Zapisowi na system dyskowy muszą podlegać tylko unikalne bloki danych nie znajdujące się jeszcze w systemie dyskowym urządzenia. Dotyczy to każdego fragmentu przychodzących do urządzenia danych.
4. Proponowane rozwiązanie nie może w żadnej fazie korzystać (w całości lub częściowo) z dodatkowego bufora na składowanie danych w postaci oryginalnej (niezdeduplikowanej).
5. Wszystkie unikalne bloki przed zapisaniem na dysk muszą być kompresowane jedną z metod do wyboru przez klienta: gz, lz.
6. Oferowane urządzenie musi wspierać (wymagane formalne wsparcie producenta urządzenia) co najmniej następujące aplikacje backupujące bezpośrednio na oferowane urządzenie: HP Data Protector, IBM TSM, VERITAS NetBackup, EMC Networker, EMC Avamar, Oracle RMAN, IBM BRMS, IBM Data Studio, VMware VDP, SAP BR\*Tools, SAP HANA Studio, Microsoft SQL Server Management Studio, Veeam.
7. W przypadku współpracy z każdą z poniższych aplikacji:
8. RMAN (dla ORACLE),
9. Microsoft SQL Server Management Studio (dla Microsoft SQL),
10. IBM Data Studio (dla DB2),
11. SAP BR\*Tools (dla SAP/Oracle),
12. SAP HANA STUDIO (dla SAP HANA),
13. vShpehre Data Protection - VDP (dla VMware),
14. Symantec NetBackup,
15. Symantec BackupExec,
16. HP Data Protector,
17. EMC NetWorker,
18. EMC Avamar,
19. Veeam.

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

De-duplikacja danych odbywa się na dowolnym serwerze posiadającym funkcjonalność Media servera NetBackup / agenta Avamar / serwera RMAN / serwera SQL / serwera SAP / serwera DB2, maszyny VDP / klienta systemu NetWorker nie posiadającego licencji Storage Node.

De-duplikacja 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.

Wymagana integracja z VDP - umożliwiająca zwiększenie przestrzeni obsługiwanej/adresowanej przez VDP z 8TB do min. 50TB przy zachowaniu deduplikacji na źródle, wymagane potwierdzenie funkcjonalności (wymaganej integracji) w oficjalnej dokumentacji producenta oferowanego urządzenia oraz dokumentacji VMware.

1. W przypadku przyjmowania backupów z VERITAS NetBackup, EMC NetWorker, Oracle RMAN, Microsoft MSSQL (przy wykorzystaniu Microsoft SQL Server Management Studio), IBM DB2 (przy wykorzystaniu IBM Data Studio), SAP/Oracle (przy wykorzystaniu SAP BR\*Tools), SAP HANA (przy wykorzystaniu SAP HANA STUDIO), Veeam urządzenie musi umożliwiać de-duplikację na źródle (de-duplikację na zabezpieczanej maszynie) i przesłanie nowych, nieznajdujących się jeszcze na urządzeniu bloków poprzez sieć FC (po rozbudowie o porty FC).

De-duplikacja w wyżej wymienionych przypadkach musi zapewniać, aby z serwerów do urządzenia były transmitowane poprzez sieć FC tylko fragmenty danych nieznajdujące się dotychczas na urządzeniu.

1. W przypadku de-duplikacji na źródle poprzez sieć IP (LAN oraz WAN), musi być możliwość szyfrowania komunikacji kluczem minimum 256 bitów.
2. Urządzenie musi wspierać de-duplikację na źródle w sieci FC (SAN) minimum dla następujących systemów operacyjnych:
3. Windows,
4. Linux (RedHat, SuSE),
5. HP-UX,
6. AIX,
7. Solaris.
8. Dla aplikacji VERITAS NetBackup, EMC NetWorker, urządzenie musi pozwalać na łączenie backupów pełnych i inkrementalnych bez odczytu danych z urządzenia. Zarządzanie łączeniem backupów pełnych i inkrementalnych musi być wykonywane z poziomu aplikacji VERITAS NetBackup, EMC NetWorker.
9. 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%.
10. Oferowane urządzenie musi umożliwiać bezpośrednią replikację danych (bez pośrednictwa dodatkowych modułów) do drugiego urządzenia tego samego, wymagane następujące tryby pracy replikacji:
11. jeden do jednego,
12. wiele do jednego,
13. jeden do wielu,
14. kaskadowej (urządzenie A replikuje dane do urządzenia B, które te same dane replikuje do urządzenia C).

Replikacja musi się odbywać w trybie asynchronicznym. Transmitowane mogą być tylko te fragmenty danych (bloki) które nie znajdują się na docelowym urządzeniu, 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 nie musi być dostarczona w ramach niniejszego postępowania.

1. Urządzenie musi również umożliwiać wydzielenie określonych portów Ethernet do replikacji.
2. W przypadku wykorzystania portów Ethernet do replikacji urządzenie musi umożliwiać przyjmowanie backupów, odtwarzanie danych, przyjmowanie strumienia replikacji, wysyłanie strumienia replikacji tymi samymi portami.
3. W przypadku replikacji danych między dwoma urządzeniami kontrolowanej przez systemy VMware VDP /VERITAS NetBackup / HP Data Protector / EMC Avamar / EMC NetWorker muszą być możliwe do uzyskania jednocześnie wszystkie następujące funkcjonalności:
4. replikacja odbywa się bezpośrednio między dwoma urządzeniami bez udziału serwerów pośredniczących,
5. replikacji podlegają tylko te fragmenty danych, które nie znajdują się na docelowym urządzeniu,
6. 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
7. Narzut na wydajność związany z replikacją nie może zmniejszyć wydajności urządzenia o więcej niż 10%.
8. Wymagana możliwość ograniczenia pasma używanego do replikacji między dwoma urządzeniami.
9. Zdeduplikowane i skompresowane dane przechowywane w obrębie podsystemu dyskowego urządzenia muszą być chronione za pomocą technologii RAID 6.
10. Każda grupa RAID 6 musi mieć przynajmniej 1 dysk hot-spare automatycznie włączany do grupy RAID w przypadku awarii jednego z dysków produkcyjnych. Dyski hot-spare muszą być globalne, możliwe do wykorzystania w innych półkach, w przypadku wyczerpania w nich dysków hot-spare.
11. Łącznie oferowane urządzenie musi posiadać zapasowe dyski typu hot-spare.
12. Oferowane urządzenie musi umożliwiać wykonywanie SnapShot’ów, czyli możliwość zamrożenia obrazu danych (stanu backupów) w urządzeniu na określoną chwilę. Oferowane urządzenie musi również umożliwiać odtworzenie danych ze Snapshot’u.

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

1. Urządzenie musi pozwalać na przechowywanie minimum 500 Snapshotów jednocześnie.
2. Urządzenie 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).
3. Urządzenie musi mieć możliwość podziału na minimum 14 logicznych części pracujących równolegle. Producent musi oficjalnie wspierać pracę minimum 14 logicznych części pracujących równolegle z pełną wydajnością urządzenia.
4. 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.
5. Wymagana możliwość zaprezentowania każdej z logicznych części oferowanego urządzenia jako niezależnego urządzenia dostępnego poprzez:
6. CIFS,
7. NFS,
8. VTL,
9. wymagany protokół umożliwiający deduplikację na źródle.
10. Urządzenie musi umożliwiać przechowywanie danych niezmienialnych:
11. Video,
12. Grafika,
13. Nagrania dźwiękowe,
14. Pliki pdf,

na udziałach CIFS/NFS.

Wymagane jest formalne wsparcie producenta dla przechowywania powyższych danych na urządzeniu, dodatkowo wymagane jest formalne wsparcie producenta dla:

1. przechowywania na urządzeniu minimum 500 milionów plików,
2. dziennego zasilenia urządzenia na poziomie minimum 500 tysięcy plików.
3. Wymagana gotowość do pracy urządzenia tzn.: możliwość zapisu oraz odtwarzania danych (przy założeniu równoległego wykorzystania wszystkich wymaganych interfejsów) po niespodziewanym wyłączeniu prądu i ponownym uruchomieniu, w czasie nie dłuższym niż 60 minut od włączenia.
4. Urządzenie musi weryfikować wszystkie zabezpieczane dane podczas procesu zapisu (nie chodzi o ew. weryfikację danych indeksowych generowanych przez urządzenie, ale o weryfikację wszystkich zabezpieczanych danych backup’owych). Każda zapisana na dyskach porcja danych musi być odczytana i porównana z danymi otrzymanymi przez urządzenie, opisana funkcjonalność powinna być częścią procesu zapisywania danych co oznacza, że weryfikacja realizowana podczas produkcyjnego dostępu do danych (w trakcie procesu RESTORE) a nie podczas procesu zapisu danych na urządzeniu - nie spełnia niniejszych wymagań. Powyższa weryfikacja musi odbywać się w locie, czyli przed usunięciem z pamięci oryginalnych danych (otrzymanych z aplikacji backupowej), musi być realizowana w trybie ciągłym (a nie ad-hoc), wymagane parametry wydajnościowe urządzenia muszą uwzględniać tę funkcjonalność.

Wymagane potwierdzenie opisanej funkcjonalności w oficjalnej dokumentacji producenta oferowanego urządzenia.

1. Urządzenie musi automatycznie usuwać przeterminowane dane (bloki danych nie należące do backupów o aktualnej retencji) w procesie czyszczenia.
2. 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.
3. Wymagana możliwość zdefiniowania maksymalnego obciążenia urządzenia procesem usuwania przeterminowanych danych (poziomu obciążenia procesora).
4. Wymagana możliwość zdefiniowania czasu, w którym wykonywany jest proces usuwania przeterminowanych danych (czyszczenia).
5. 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. Urządzenie musi zapewniać w dni robocze (poniedziałek – piątek) minimum 20 godzin pełnej wydajności. W czasie pełnej wydajności (poniedziałek – piątek, minimum 20 godzin dziennie) urządzenie nie może wykonywać jakichkolwiek wewnętrznych procesów w tym nie może wykonywać usuwania przeterminowanych danych.
7. Proces usuwania przeterminowanych danych nie może zajmować więcej niż 4 godziny dziennie w dni robocze (poniedziałek – piątek).
8. Urządzenie musi mieć możliwość zarządzania poprzez:
9. interfejs graficzny dostępny z przeglądarki internetowej,
10. poprzez linię komend (CLI) dostępną z poziomu ssh (secure shell).
11. Oprogramowanie do zarządzania musi rezydować na oferowanym urządzeniu de-duplikacyjnym.
12. Oferowane urządzenie musi mieć możliwość sprawdzenia pakietu upgrade’ującego firmware urządzenia (GUI lub CLI), to znaczy sprawdzenia czy nowa wersja systemu nie spowoduje problemów z urządzeniem.
13. Urządzenie musi być rozwiązaniem kompletnym, appliancem sprzętowym pochodzącym od jednego producenta. Zamawiający nie dopuszcza stosowania rozwiązań typu gateway. Urządzenie musi być oficjalnie dostępne w ofercie producenta na dzień składania ofert.
14. Dostarczone urządzenie musi stanowić całość pochodzącą od jednego producenta (oprogramowanie oraz sprzęt) i być serwisowane przez autoryzowany serwis producenta ze wsparciem na okres oferowanej gwarancji, z czasem reakcji na zgłoszenia awarii NBD (następny dzień roboczy).
15. W przypadku awarii dysku po jego wymianie dysk pozostaje własnością Zamawiającego.

**A.2 Wymagania na system wykonywania i składowania kopii zapasowych**

1. Zamawiający wymaga dostarczenia, uruchomienia i wdrożenia centralnego systemu do backupu serwerów systemów otwartych (Windows/ Linux/UNIX), w tym
2. Maszyn wirtualnych,
3. Serwerów fizycznych,
4. Serwerów znajdujących się w zdalnych oddziałach,
5. Maszyn wirtualnych znajdujących się w zdalnych oddziałach,
6. Laptopów połączonych z centralą siecią GSM.
7. Oferowane licencje muszą zapewnić backup / odtwarzanie środowiska VMware składającego się z 3 serwerów ESX posiadających łącznie 6 fizycznych procesorów oraz serwerów fizycznych posiadających łącznie 4 fizyczne procesory.
8. System centralnego backupu musi być umożliwiać dla powyżej definiowanego środowiska backup/odtwarzanie nielimitowanej liczby:
9. maszyn wirtualnych: Zarówno backup obrazów maszyn wirtualnych jak również backup ze środka maszyn wirtualnych wszystkimi dostępnymi agentami oprogramowania backupowego,
10. serwerów,
11. systemów operacyjnych,
12. baz danych,
13. serwerów w zdalnych lokalizacjach,
14. maszyn wirtualnych w zdalnych lokalizacjach.
15. Wymaga się by w ramach oferowanych licencji system umożliwiał backup maszyn wirtualnych w każdym trybie:
16. Jako obrazy maszyn wirtualnych VMware (pliki vmdk)
17. Ze środka, agentem plikowym / bazo-danowym / aplikacyjnym dla sytemów plików Oracle, SQL, Sybase, DB2, Exchange, Lotus, Sharepoint
18. Serwer backupu we wskazanej lokalizacji musi być dostarczony w formie maszyny wirtualnej VMware zarządzającej backupem i odtwarzaniem całości zabezpieczanego środowiska. Wymagane jest by maszyna wirtualna obsługiwała minimum 2TB przestrzeni netto przeznaczonej na informacje o backupach, konfiguracji backupów, itp.
19. Oferowany system musi tworzyć centralny system backupu wykonujący kopie zapasowe oraz zapewniać przechowywanie wszystkich zdeduplikowanych kopii zapasowych na dyskach.
20. Podana poniżej specyfikacja oprogramowania backupowego określa parametry minimalne. Dostarczane oprogramowanie backupowe zarządzania kopiami zapasowymi musi spełniać następujące wymagania. W ramach licencji na zdefiniowane poniżej środowisko, wszystkie poniższe funkcjonalności musza być dostępne.
21. System backupu musi zapewnić realizację centralnego systemu do tworzenia i zarządzania kopiami zapasowymi maszyn wirtualnych i serwerów (VMware/HyperV/ Linux/Windows/UNIX), w tym również:
22. działających w oferowanym środowisku wirtualnym,
23. działających w zdalnych lokalizacjach,
24. stacji roboczych.
25. Każda z maszyn wirtualnych pełniąca rolę serwera backupu zostanie zainstalowane w oddzielnym ośrodku. Każda z maszyn wirtualnych pełniąca rolę serwera backupu musi umożliwiać:
26. zarządzanie backupem lokalnego środowiska i związanych z nim zdalnych lokalizacji,
27. przechowywanie backupów na dyskach,
28. zarządzanie replikacją,
29. odtworzenie zreplikowanych backupów również w przypadku całkowitego zniszczenia zdalnego ośrodka, czyli zniszczenia całości zdalnego środowiska backupu,
30. stanowić kompletny system centralnego backupu z agentami do backupu plików, baz danych, środowisk wirtualnych.
31. Dostarczony system musi przechowywać kopie zapasowe na dyskach. Nie dopuszcza się przechowywania danych na taśmach magnetycznych czy też zabezpieczanych maszynach.
32. Dostarczony system powinien umożliwiać przesłanie backupu w chmurę (Cloud Backup). System powinien współpracować z ogólnie dostępnymi dostawcami usług składowania danych w chmurze AWS, AZURE, GOOGLE.
33. Oprogramowanie backupowe musi wspierać (wymagane wsparcie producenta) następujące systemy operacyjne: Windows (także Microsoft Cluster), Linux (Red Hat, SUSE, Debian, CentOS, Ubnutu, Novell OES), Solaris, AIX, HP-UX, Mac OS X, FreeBSD.

Backup zasobów plików z powyższych systemów musi podlegać de-duplikacji ze zmiennym blokiem na zabezpieczanej maszynie zgodnie z wymaganiami w mniejszej specyfikacji.

1. Oprogramowanie backupowe musi wspierać (wymagane wsparcie producenta) backup online następujących baz danych i aplikacji: MS Exchange, MS SQL, Oracle, IBM DB2, Lotus Notes, SharePoint, SAP, Sybase, VMware, HyperV.

Backup z powyższych baz danych i aplikacji musi podlegać de-duplikacji ze zmiennym blokiem na zabezpieczanej maszynie zgodnie z wymaganiami zawartymi w mniejszej specyfikacji.

1. W przypadku zabezpieczania baz danych i aplikacji musi istnieć możliwość pobierania kopii zapasowej kilkoma strumieniami jednocześnie (minimum 10 jednoczesnych strumieni).
2. Zabezpieczane serwery muszą być backupowane bezpośrednio na medium backupowe (dyski oferowanego applaince’u lub dyski oferowanego de-duplikatora) bez pośrednictwa jakichkolwiek innych urządzeń / serwerów.

Dotyczy to backupów lokalnych, zdalnych jak również backupu laptopów

1. Oprogramowanie backupowe musi umożliwiać dla sieci lokalnej:
2. backup pojedynczych plików,
3. backup całych systemów plików,
4. backup baz danych w trakcie ich normalnej pracy,
5. backup ustawień systemu operacyjnego Windows,
6. backup całych obrazów maszyn wirtualnych systemu VMware,
7. backup całych obrazów maszyn wirtualnych systemu HyperV.
8. Backup zdalnych oddziałów musi działać poprawnie nawet w przypadku opóźnienia 200 ms w sieci WAN oraz jednocześnie utraty pakietów na poziomie 10%. Powyższa funkcjonalność wymagana jest dla wszystkich typów backupowanych danych.
9. Rozwiązanie backupowe nie może wymagać jakichkolwiek czynności ze strony personelu w oddziale. Rozwiązanie backupowe musi działać zakładając, że pracownicy oddziału nie wiedzą w ogóle o istnieniu rozwiązania backupowego.
10. Rozwiązanie backupowe musi być w pełni konfigurowalne z konsoli znajdującej się w centrali. W szczególności backupy maszyn w oddziałach (bazy, pliki) czy też backupy laptopów muszą być konfigurowalne z poziomu centralnej konsoli bez konieczności logowania się na zabezpieczaną maszynę.
11. Rozwiązanie backupowe musi mieć możliwość odtworzenia:
12. plików,
13. baz danych,

na docelową maszynę w oddziale z poziomu centralnej konsoli systemu backupowego. Nie może być wymagane logowanie się na odtwarzaną maszynę celem odtworzenia danych z systemu backupowego.

1. W przypadku wyboru odtwarzania całego systemu plików dla systemów Windows / Linux / UNIX, rozwiązanie backupowe musi automatycznie i samodzielnie porównać pliki znajdujące się w backupie i pliki znajdujące się odtwarzanej maszynie i odtworzyć tylko brakujące pliki.

W przypadku wyboru odtwarzania całego dysku / całego systemu plików, rozwiązanie backupowe nie może odczytywać z medium backupowego ani przesyłać do odtwarzanej maszyny plików, które znajdowały się zarówno w backupie jak i na odtwarzanej maszynie.

Rozwiązanie backupowe musi samodzielnie ustalić których plików brakuje na odtwarzanym dysku zabezpieczanej maszyny i tylko te pliki odtworzyć.

1. Oferowane rozwiązanie musi być odporne na:
2. Opóźnienia na łączu między oddziałem a ośrodkiem regionalnym (do 200ms),
3. Zrywanie łącza między oddziałem a ośrodkiem regionalnym (do 30 min),
4. Utraty pakietów (do 10%).
5. Wymagane jest by dla wszystkich backupowanych systemów i danych de-duplikacja odbywała się na źródle.
6. Wymagany jest następujący scenariusz transmisji danych w trakcie backupu:
7. odczyt danych na zabezpieczanym systemie,
8. de-duplikacja danych na zabezpieczanym systemie,
9. transmisja unikalnych, nieznajdujących się na serwerze bloków do oferowanego serwera.
10. Włączenie funkcjonalności deduplikacji nie może generować wymogu instalacji dodatkowych modułów programowych po stronie klienckiej lub serwera backupowego.
11. Oprogramowanie backupowe nie może odczytywać tych plików z systemu dyskowego, które się nie zmieniły w stosunku do ostatniego backupu. Raz zbackupowany plik nie może być nigdy więcej odczytany, chyba, że zmieni się jego zawartość.
12. Oprogramowanie backupowe musi wykonywać zawsze tylko logicznie pełne backupy systemu plików. Z zabezpieczanego systemu plików muszą odczytywane tylko nowe lub zmienione pliki, do appliance’u backupowego muszą być wysyłane dane po de-duplikacji, natomiast sam backup musi być logicznie pełnym backupem. W wewnętrznej strukturze musi być przechowywana informacja o każdym backupie i należących do niego danych (blokach).

Odtworzenie jakichkolwiek danych plikowych musi być pojedynczym zadaniem identycznym z odtworzeniem danych z pełnego backupu.

1. W konsoli oprogramowania backupowego musi być możliwość definiowania ważności danych (backupów) na podstawie kryteriów czasowych (dni, miesiące, lata). Po okresie ważności backupy musza być automatycznie usunięte.
2. Oferowanie oprogramowanie backupowe musi mieć możliwość tworzenia z poziomu GUI (konsoli graficznej) polityk typu Dziadek – ojciec –syn, to znaczy utworzenia polityki, w której zdefiniowano:
3. Czas przechowywania backupów dziennych,
4. Czas przechowywania backupów tygodniowych,
5. Czas przechowywania backupów miesięcznych,
6. Czas przechowywania backupów rocznych.
7. Oferowane rozwiązanie musi umożliwiać tworzenie wykluczeń, czyli elementów nie podlegających backupowi w ramach zadania backupowego. Musi istnieć możliwość tworzenia wykluczeń dla dowolnej kombinacji następujących elementów:
8. wybranych typów plików, np. dla plików z rozszerzeniem mp3,
9. dla całych katalogów (np.: c:\windows),
10. dla pojedynczych plików.
11. Oferowane rozwiązanie musi mieć możliwość zdefiniowania by ostatni backup dowolnego zbioru danych nigdy się nie przeterminował. Oznacza to, że jeśli dany zasób nie jest backupowany to automatycznie ostatnie ważny backup tego zasobu jest trzymany bezterminowo. Jedynie administrator może zdecydować o jego usunięciu.
12. Musi być możliwość (przyszła rozbudowa) zainstalowania serwera backupu jako appliance’u fizycznego. Musi być możliwość migracji informacji o backupach, ustawień konfiguracji, metadanych między obecnym serwerem w postaci maszyny wirtualnej a przyszłym fizycznym applience’m.
13. Oferowane serwery backupu w postaci maszyn wirtualnych muszą zarządzać replikacją backupów. Całość konfiguracji replikacji backupów musi odbywać się z konsoli serwera backupu.
14. Wymaga się by replikacja między backupami znajdujących się na dyskach odbywała się w obu kierunkach jednocześnie:
15. Backupy z serwera z ośrodka podstawowego do serwera z ośrodka zapasowego,
16. Backupy z serwera z ośrodka zapasowego do serwera z ośrodka podstawowego.

Całość replikacji zarządzana tylko i wyłącznie z poziomu oprogramowania backupowego (serwerów backupu w postaci maszyn wirtualnej w każdym ośrodku).

1. Musi istnieć możliwość zdefiniowania kalendarza replikacji między serwerami oraz zdefiniowania, które zadania backupowe podlegają replikacji.
2. Serwer backupu musi udostępniać (pokazywać w konsoli GUI) backupy które zostały do niego zreplikowane ze zdalnej lokalizacji. Musi być możliwość odtworzenia backupów zreplikowanych do lokalnego serwera backupu ze zdalnej lokalizacji. Odtworzenie musi dobywać się poprzez interfejs GUI. Odtworzenie musi być możliwe w przypadku całkowitej niedostępności zdalnego systemu backupu (nieodstępność zdalnego serwera backupu).
3. Każdy serwer backupu w każdej lokalizacji musi udostępniać (pokazywać w konsoli GUI) zarówno lokalne backupy jak wszystkie również backupy zreplikowane do ośrodka zdalnego.
4. W przypadku odtwarzania danych w ośrodku A w trakcie definiowania zadania odtwarzania musi być możliwość zdefiniowania czy odtwarzamy backupy z lokalnej kopii czy też odtwarzamy ze zdalnej kopii z ośrodka B.
5. 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. Konsola musi udostępniać raporty dotyczące zajętości przestrzeni przeznaczonej na de-duplikaty.
7. Bloki przesyłane z zabezpieczanych serwerów do appliance’a backupowego lub do oferowanego de-duplikatora muszą być kompresowane i szyfrowane algorytmem z kluczem minimum 256-bitowym.
8. Wymagana jest autentyfikacja komunikacji między klientem a serwerem backupu (farmą serwerów) oparta na certyfikatach.
9. Oprogramowanie backupowe musi pozwalać na odtwarzanie danych poprzez: wybór odtwarzanych danych, odtworzenie danych w jednym kroku.
10. Oprogramowanie backupowe musi mieć możliwość limitowania wielkości zadania backupowego. Jeśli zadanie backupowe przekroczy zdefiniowaną wielkość wówczas nie może być zapisane w systemie backupowych.
11. Oprogramowanie backupowe musi umożliwiać ograniczenie mocy procesora używanej do wykonywania zdania backupu tak by odpowiednia moc procesora zostawić dla innych zadań.
12. Rozwiązanie backupowe musi wspierać backup i odtwarzanie środowisk VMware 5.5, 6.0, 6.5, 6.7.

Oprogramowanie backupowe musi umożliwiać dla środowisk VMware następujące typy backupu:

1. Backup całych maszyn wirtualnych,
2. Backup pojedynczych, wybranych dysków maszyny wirtualnej vmdk,
3. W trakcie backupu odczytowi z systemu dyskowego mają podlegać tylko zmienione bloki wirtualnych maszyn systemu VMWare (wymagane wykorzystanie mechanizmu CBT systemu VMWare),
4. Wszystkie backupy obrazów maszyn wirtualnych muszą być wykonywane przy pomocy technologii CBT systemu VMware to znaczy do medium backupowego z systemu VMware muszą być transferowane tylko zmienione bloki.

Jednocześnie z punktu widzenia systemu backupowego musza to być backupy pełne (full backup). To znaczy z punktu widzenia systemu backupu muszą to być backupy identyczne z wykonywanym od zera pełnym backupem,

1. Musi istnieć możliwość zastosowania wyrażeń regularnych do określenia, które wirtualne dyski VMware mają być backupowane,
2. Wykonywanie backupu obrazów maszyn wirtualnych VMware nie może wymagać bufora dyskowego na kopię obrazów maszyn wirtualnych (plików vmdk).

Powyższe metody backupu maszyn wirtualnych muszą podlegać de-duplikacji ze zmiennym blokiem przed wysłaniem danych do medium backupowego zgodnie z wymaganiami dla de-duplikacji powyżej.

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

1. Oferowany system musi pozwalać na szybkie odtworzenie
2. całych obrazów maszyn wirtualnych,
3. pojedynczych dysków maszyny wirtualnej z backupu całej maszyny wirtualnej.
4. Rozwiązanie backupowe musi umożliwiać odtworzenie obrazów maszyn wirtualnych VMware dostarczając następujące funkcjonalności:
5. Odtworzenie całych maszyn wirtualnych musi wykorzystywać mechanizm CBT systemu VMWare – odtwarzane są tylko te bloki wirtualnej maszyny/dysku które uległy zmianie od ostatniego backupu,
6. Odtworzenie pojedynczych dysków maszyn wirtualnych musi wykorzystywać mechanizm CBT systemu VMWare – odtwarzane są tylko te bloki wirtualnej maszyny/dysku które uległy zmianie od ostatniego backupu,
7. Odtworzenie pojedynczych plików z backupu obrazu maszyny wirtualnej bez konieczności odtworzenia całej maszyny wirtualnej. Funkcjonalność musi być dostępna dla obrazów maszyn wirtualnych z zainstalowanym systemem operacyjnym Windows oraz Linux.
8. Możliwość zamontowania na dowolnym serwerze (fizycznym lub wirtualnym) zbackupowanych obrazów maszyn wirtualnych Windows (plików vmdk maszyny wirtualnej Windows). Powyższa metoda nie może fizycznie odtwarzać backupów a jedynie pozwalać na przeglądanie zawartości plików vmdk w backupie z poziomu Eksploratora Plików Windows na dowolnej maszynie.

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

1. Rozwiązanie backupowe musi umożliwiać uruchomienie maszyny wirtualnej bezpośrednio z medium backupowego bez konieczności odtwarzania (Instant Access).
2. Oprogramowanie backupowe musi mieć możliwość prezentacji (bez konieczności odtworzenia) zbackupowanych obrazów maszyn wirtualnych VMware (plików vmdk) jako katalogów na maszynie fizycznej celem ich przeszukiwania (wymagane przeszukiwanie po nazwach plików jak również zawartości plików) z poziomu systemu operacyjnego maszyny fizycznej.
3. 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.
4. Skalowalność rozwiązania dla środowisk VMware musi być na poziomie:
5. Minimum 3000 maszyn wirtualnych w ramach pojedynczej instancji systemu backupu,
6. Minimum 100 maszyn wirtualnych backupowanych w ciągu godziny w ramach pojedynczej instancji systemu backupu.
7. Rozwiązanie backupowe musi umożliwiać backup i odtwarzanie w tym samym czasie minimum 50 maszyn wirtualnych VMware.
8. Oprogramowanie backupowe musi mieć możliwość automatycznego sprawdzania (weryfikacji) zbackupowanych maszyn wirtualnych VMware. Musi istnieć możliwość ustawienia kalendarza weryfikacji maszyn wirtualnych VMware.

Weryfikacja maszyn wirtualnych musi zapewniać minimum:

1. Odtworzenie maszyny wirtualnej na zdefiniowanym Data Center / Data Store,
2. Weryfikacja podstawowych procesów,
3. Możliwość dołączenia własnego skryptu weryfikującego wybrane elementy maszyny wirtualnej.

Informacja w konsoli systemu backupu o poprawnej / niepoprawnej weryfikacji maszyny wirtualnej.

1. Administrator (właściciel) danej maszyny wirtualnej VMware musi mieć możliwość samodzielnego (bez konieczności kontaktu z administratorem backupu czy też administratorem VMware) odtworzenia pojedynczych plików z dowolnego backupu obrazu jego maszyny wirtualnej.
2. Oprogramowanie backupowe musi zawsze przechowywać pełne backupy obrazów maszyn wirtualnych środowiska VMware/Hyper-V dla każdej wykonanej w przeszłości kopii zapasowej.

Każdy backup obrazu maszyny wirtualnej musi być backupem pełnym.

1. Rozwiązanie backupowe musi pozwalać automatyczne polityki backupowe dla:
2. Folderu,
3. Resource Pool,

systemu VMware.

Oznacza to, że dodanie maszyny wirtualnej do folderu, hosta czy resource pooli w systemie VMware spowoduje automatyczne backupowanie dodanej maszyny wirtualnej zgodnie z polityka zdefiniowana dla folderu hosta czy resource pooli w systemie VMware.

1. 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.
2. 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.
3. Backup oraz odtworzenie maszyn wirtualnych VMware musi być możliwy z poziomu graficznego interfejsu, linii komend oraz przez REST API.
4. Oprogramowanie backupowe musi umożliwiać dla środowisk Hyper-V:
5. Backup pojedynczych plików i baz danych z maszyny wirtualnej ze środka maszyny wirtualnej Hyper-V,
6. Backup całych maszyn wirtualnych (czyli plików VHD reprezentujących wirtualną maszynę),
7. Pełny (full) backup całych maszyn wirtualnych HyperV (image level) musi odbywać się poprzez odczyt tylko zmienionych bloków dysków VHD,
8. Wykonywanie backupu jak w punkcie b. oraz c. nie może wymagać bufora dyskowego na kopię obrazów maszyn wirtualnych (plików vhd),
9. Wykonywanie backupu jak w punkcie b. oraz c. musi pozwalać na odtworzenie pojedynczych plików z obrazu maszyny wirtualnej bez konieczności odtworzenia całej maszyny wirtualnej. Funkcjonalność musi dostępna dla obrazów maszyn wirtualnych z zainstalowanym systemem operacyjnym Windows.

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

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

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

1. Oprogramowanie backupowe musi zapewniać spójny backup Exchange / MSSQL przy backupie obrazów maszyn wirtualnych środowiska Hyper-V.
2. Musi istnieć możliwość odtworzenia danych:
3. z zabezpieczanego serwera / komputera,
4. z konsoli systemu backupowego.
5. Musi istnieć możliwość odtworzenia:
6. Pojedynczego pliku,
7. Zabezpieczanej bazy danych.
8. Dla systemów Windows 2012, Windows 2016 musi istnieć funkcjonalność Bare Metal Recovery automatycznego odtworzenia całego serwera (system operacyjny + ustawienia systemu operacyjnego + dane) w jednym kroku bezpośrednio z oferowanego urządzenia.

Funkcjonalność musi być wbudowana w rozwiązanie backupowe.

1. W przypadku odtwarzania danych z interfejsu dostępnego na zabezpieczanym serwerze musi istnieć mechanizm autentyfikacji użytkowników dostępny w dwóch opcjach:
2. Wbudowany w system backupowy,
3. Zintegrowany z usługami katalogowymi,
4. W przypadku wykorzystania AD, użytkownicy będący w domenie nie muszą się logować do systemu backupu w przypadku konieczności:

* odtworzenia danych,
* przeszukania zwartości swoich backupów,
* wykonania backupu.

1. Dla odtwarzania danych z interfejsu końcowego użytkownika dostępnego na zabezpieczanym laptopie / PC muszą być dostarczone następujące funkcjonalności:
2. Wyszukiwanie pliku do odtwarzania po:

* nazwie pliku,
* początkowym fragmencie nazwy pliku,
* końcowym fragmencie nazwy pliku,
* fragmencie nazwy pliku umiejscowionym gdziekolwiek w pełnej nazwie pliku.

1. Przeglądania zawartości zbackupowanego systemu plików i wybór zasobów do odtworzenia,
2. Wybór wersji odtwarzanego pliku / katalogu.
3. Rozwiązanie backupowe musi umożliwiać odtworzenie plików z dowolnego urządzenia (laptop, tablet, smartphone) poprzez przeglądarkę internetową. Odtwarzanie to musi spełniać następujące kryteria:
4. Uwierzytelnienia użytkownika,
5. Wyszukiwanie pliku do odtwarzania po:

* nazwie pliku,
* początkowym fragmencie nazwy pliku,
* końcowym fragmencie nazwy pliku,
* fragmencie nazwy pliku umiejscowionym gdziekolwiek w pełnej nazwie pliku.

1. Przeglądania zawartości zbackupowanego systemu plików i wybór zasobów do odtworzenia,
2. Wybór wersji odtwarzanego pliku / katalogu.
3. W przypadku odtwarzania istniejącego systemu plików (systemu plików który utracił część zasobów) oprogramowanie backupowe musi samo, automatycznie sprawdzać których plików znajdujących się w backupie brakuje na odtwarzanej maszynie a następnie odczytywać z backupu i przesyłać tylko te pliki które znajdują się w backupie a których brakuje na odtwarzanej maszynie.
4. System backupu musi mieć funkcjonalność wyrzutu na taśmę.

Opcja wyrzutu na taśmę nie musi być elementem niniejszej oferty.

1. System backupu musi mieć możliwość bezpośredniego raportowania o błędach do serwisu producenta.
2. System backupu musi mieć możliwość instalacji agentów jako plików msi. Musi istnieć możliwość automatyzacji agentów poprzez uruchomienie skryptu instalującego agenta na zabezpieczanej maszynie i przyporządkowującego maszynę automatycznie do określonej polityki backupowej.
3. System backupu musi mieć możliwość automatycznej samo-aktualizacji poprzez automatyczne ściąganie nowych wersji od producenta.
4. System backupu musi mieć możliwość automatycznej aktualizacji oprogramowania agentów wykonywanej bezpośrednio z serwera backupu.
5. System musi pozwalać na backup serwerów NAS z następującymi funkcjonalnościami:
6. W trakcie backupu z systemu NAS muszą być wysyłane do medium backupowego tylko zmienione pliki od ostatniego backupu,
7. W przypadku odtwarzania, uprawnienia użytkowników również są odtwarzane,
8. Integracja z protokołem NDMP systemów NAS,
9. Odtworzenie plików z backupu NDMP bezpośrednio na platformę Windows/Linux.
10. W ramach licencji musi być zapewniona możliwość monitorowania, raportowania, szczegółowego rozliczania z użycia komponentów systemu backupowego oraz analizy błędów dla środowiska kopii zapasowej Zamawiającego. Musza być dostępne między innymi następujące raporty: System raportujący musi posiadać wbudowane następujące raporty:
11. Podsumowanie zadań backupowych (liczba backupów udanych, nieudanych, aktywnych, łączny rozmiar zbackupowanych danych),
12. Podsumowanie zadań odtworzeniowych (liczba odtworzeń udanych, nieudanych, aktywnych, łączny rozmiar odtworzonych danych danych),
13. Zbiorcze procentowe zestawienie udanych zadań backupowych z poszczególnych serwerów,
14. Zbiorcze zestawienie zabezpieczanych serwerów które w sposób ciągły (kilka razy pod rząd) maja problem z backupami,
15. Zestawienie zabezpieczanych systemów plików które w ogóle nie są backupowane,
16. Spodziewany czas odtwarzania zabezpieczanego serwera oraz potencjalnej utraty danych (czas między ostatnim backupem a chwilą awarii),
17. Najmniej wiarygodne zabezpieczanych serwery (procent nieudanych backupów),
18. Lista najwolniejszych/najszybszych zabezpieczanych maszyn,
19. Poziom SLA (procentowa liczba udanych backupów) w odniesieniu do poziomu założonego,
20. Mierzenie poziomu SLA dla poszczególnych zabezpieczanych serwerów przy uwzględnieniu założonego okna backupowego i RPO (punktu, do którego się odtwarzamy)
21. Liczba danych backupowanych dziennie,
22. Liczba zadań backupowych dziennie,
23. Zużycie zasobów na serwerach backupowych (procesor, pamięć, karty sieciowe LAN, SAN),
24. Zużycie mediów backupowych i napędów taśmowych,
25. Aktualna konfiguracja systemu backupowego,
26. Historia zmian konfiguracji systemu backupowego,
27. Posiadane licencje systemu backupowego,
28. Wykorzystanie systemu backupowego przez poszczególne działy / grupy użytkowników (chargeback per cost center).
29. W ramach dostarczonych licencji musi być możliwość przeszukiwania backupów z poziomu graficznego interface’u (GUI). Musi być możliwość wyszukania dowolnych fraz w nazwach plików.
30. Wymagane wsparcie na oferowane oprogramowanie realizowane przez producenta w okresie oferowanej gwarancji, gwarantujące dostęp do najnowszych wersji oprogramowania.
31. **Rozbudowa istniejącego klastra złożonego z dwóch fizycznych serwerów o dwa nowe serwery wraz ze stosownymi licencjami**
32. Zamawiający w chwili obecnej posiada klaster dwóch serwerów pracujących w klastrze vSAN w oparciu o licencje Standard. Poniżej przedstawiona jest obecna konfiguracja sprzętowa posiadanych serwerów:
33. Serwery 1-procesorowe – CPU Intel Xeon Silver 4216,
34. Pamięć RAM 8 x 32GB RDIM 2933MT/s w modułach dwubankowych,
35. 5 dysków SSD 3,84TB SAS 12Gb/s 512e 2.5” RI PM5 1 DWPD 7008 TBW,
36. Dedykowna karta do instalacji system operacyjnego VMware w RAID 1 – 2 x M.2 240GB,
37. Kontroler SAS 12Gbps,
38. Podwójny nadmiarowy zasilacz 1+1 750W,
39. Karta sieciowa Broadcom 57412 2 porty 10Gb/s SFP+ plus 5720 2 porty 1Gb/s Base-T,
40. Karta sieciowa Broadcom 57412 2 porty 10Gb/s SFP+,
41. VMware 6,7 U3.
42. Zamawiający wymaga dostarczenia aktualizacji licencji vSAN z wersji Standard do Advanced dla posiadanych licencji – (VMware Order / License Confirmation 24847156) oraz wykupienia wsparcia na zaktualizowane licencje Advanced na okres 5 lat od momentu dostarczenia aktualizacji (obecnie posiadane wsparcie vSAN – Contract 498049993)
43. Zamawiający wymaga dostarczenia dwóch serwerów fizycznych w pełni zgodnych z opisanymi powyżej parametrami oraz w pełni kompatybilnymi z rozwiązaniem vSAN w celu uruchomienia klastra vSAN w wersji Advaced na klastrze 4 serwerów fizycznych. Wszystkie komponenty oferowanych serwerów muszą znajdować się na liście kompatybilności VMware vSAN.
44. Zamawiający wymaga przeprowadzenia aktualizacji obecnego środowiska vSAN do wersji Advanced oraz instalacji uruchomienia i konfiguracji nowo dostarczonych serwerów w celu uruchomienia klastra vSAN w funkcjonalności Advanced na 4 fizycznych serwerach.

**B.1 Parametry minimalne wymaganych serwerów vSAN:**

| **Lp.** | **Parametr** | **Charakterystyka (minimalne wymagania)** |
| --- | --- | --- |
| **1** | **2** | **3** |
| **1** | **Obudowa** | Obudowa Rack o wysokości max 1U z możliwością instalacji do 8 dysków 2.5" Hot-Plug wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych oraz organizatorem do kabli. Obudowa musi mieć możliwość (jako opcja) wyposażenia w kartę umożliwiającą dostęp bezpośredni poprzez urządzenia mobilne  - serwer musi posiadać możliwość konfiguracji oraz monitoringu najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej min. (Android/ Apple iOS) przy użyciu jednego z protokołów NFC/ BLE/ WIFI. |
| **2** | **Płyta główna** | Płyta główna z możliwością zainstalowania minimum dwóch procesorów. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym. |
| **3** | **Chipset** | Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych |
| **4** | **Procesor** | Zainstalowany jeden procesor min. szesnasto-rdzeniowe dedykowany do pracy z zaoferowanym serwerem umożliwiający osiągnięcie wyniku min. 175 punktów w teście SPECrate2017\_int\_base dostępnym na stronie www.spec.org dla dwóch procesorów. |
| **5** | **RAM** | Min. 256GB DDR4 RDIMM 2933MT/s, na płycie głównej powinno znajdować się minimum 24 slotów przeznaczonych do instalacji pamięci. Płyta główna powinna obsługiwać do 3TB pamięci RAM. |
| **6** | **Zabezpieczenia pamięci RAM** | Memory Rank Sparing, Memory Mirror, Lockstep |
| **7** | **Gniazda PCI** | Minimum dwa sloty x16 generacji 3 połowy wysokości |
| **8** | **Interfejsy sieciowe/FC/SAS** | Wbudowane dwa interfejsy sieciowe 1Gb Ethernet w standardzie BaseT oraz dwa interfejsy sieciowe 10Gb Ethernet ze złączami w standardzie SFP+.  Dodatkowa karta sieciowa z dwoma interfejsami 10Gb Ethernet w standardzie SFP+.  Możliwość instalacji wymiennie modułów udostępniających:   1. dwa interfejsy sieciowe 1Gb Ethernet w standardzie BaseT oraz dwa interfejsy sieciowe 10Gb Ethernet ze złączami w standardzie BaseT, 2. dwa interfejsy sieciowe 1Gb Ethernet w standardzie BaseT oraz dwa interfejsy sieciowe 10Gb Ethernet ze złączami w standardzie SFP+, 3. cztery interfejsy sieciowe 1Gb Ethernet w standardzie BaseT, 4. dwa interfejsy sieciowe 25Gb Ethernet ze złączami SFP28. |
| **9** | **Napęd optyczny** | Nie wymagany |
| **10** | **Dyski twarde** | Możliwość instalacji dysków SATA, SAS, SSD.  Zainstalowane 2x240GB SSD M.2 na dedykowanej karcie wewnątrz serwera pracujące w konfiguracji RAID 1.  Możliwość instalacji modułu dedykowanego dla hypervisora wirtualizacyjnego, możliwość wyposażenia modułu w 2 jednakowe nośniki typu flash o pojemności min. 64GB z możliwością konfiguracji zabezpieczenia synchronizacji pomiędzy nośnikami z poziomu BIOS serwera, rozwiązanie nie może powodować zmniejszenia ilości wnęk na dyski twarde. |
| **11** | **Kontroler RAID** | SAS 12Gbps |
| **12** | **System operacyjny** | Zamawiający wymaga dostarczenia systemu operacyjnego klasy Server obsługujący min. 16 rdzeni procesora (B1 pkt 4) wraz z pełną licencją na oferowany serwer oraz ilość procesorów oraz zestawem nośników.  Zainstalowany dostępny na rynku licencjonowany 64-bitowy serwerowy system operacyjny z gwarantowanym podstawowym wsparciem producenta do min. 31.12.2024 r. umożliwiający automatyczne poświadczenie i zalogowanie się do domeny Active Directory akceptujący zasady grupowe, polityki GPO obowiązujące w tej domenie; który pozwoli na uruchomienie co najmniej 4 maszyn wirtualnych z systemem operacyjnym umożliwiającym uruchomienie serwera Active Directory, licencjonowany zgodnie z zaproponowanymi procesorami wraz z zestawem nośników. |
| **13** | **Wbudowane porty** | Min. 3 porty USB 2.0 oraz 2 porty USB 3.0, 4 porty RJ45, 2 porty VGA (1 na przednim panelu obudowy, drugi na tylnym), min. 1 port RS232 |
| **14** | **Video** | Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1920x1200 |
| **15** | **Wentylatory** | Redundantne |
| **16** | **Zasilacze** | Redundantne, Hot-Plug maksymalnie 750W każdy. |
| **17** | **Bezpieczeństwo** | Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą. |
| **18** | **Diagnostyka** | Panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS’u, zasilaniu oraz temperaturze. |
| **19** | **Karta Zarządzania** | Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowane port RJ-45 Gigabit Ethernet umożliwiająca:   1. szyfrowane połączenie (SSLv3) oraz autentykacje i autoryzację użytkownika, 2. wsparcie dla IPv6, 3. wsparcie dla SNMP; IPMI2.0, VLAN tagging, Telnet, SSH, 4. możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer, 5. możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer, 6. wsparcie dla dynamic DNS, 7. wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej, 8. możliwość podłączenia lokalnego poprzez złącze RS-232, 9. możliwość zarządzania bezpośredniego poprzez złącze USB umieszczone na froncie obudowy, 10. możliwość konfiguracji przepływu powietrza na każdym slocie PCIe, 11. musi umożliwiający zdalne podłączenie do konsoli graficznej serwera i zdalne sterowanie nim oraz zdalne montowanie obrazów ISO. |
| **20** | **Certyfikaty** | Serwer musi być wyprodukowany zgodnie z normą ISO-9001 oraz ISO-14001 (lub normami równoważnymi). Serwer musi posiadać deklarację CE. |
| **21** | **Warunki gwarancji** | 1. Wymagany okres gwarancji jest parametrem podlegającym ocenie w kryterium „Gwarancja”, i określony w pkt III.7 SIWZ. 2. Realizowana w miejscu instalacji sprzętu, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii w trybie 365x7x24 poprzez linię telefoniczną producenta (komunikacja w języku polskim). 3. W przypadku awarii dyski twarde pozostają własnością zamawiającego. 4. Wykonawca lub firma serwisująca musi posiadać ISO 9001 (lub równoważną) na świadczenie usług serwisowych oraz posiadać na świadczenie usług serwisowych dotyczących oferowanych serwerów autoryzacje producenta. 5. Wymagane oświadczenie producenta, że w przypadku nie wywiązywania się z obowiązków gwarancyjnych Wykonawcy lub firmy serwisującej, przejmie na siebie wszelkie zobowiązania związane z serwisem. |
| **22** | **Dokumentacja użytkownika** | Zamawiający wymaga dokumentacji w języku polskim lub angielskim.  Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela. |

1. **Rozbudowa routera brzegowego UTM o niezbędne licencje oraz wsparcie techniczne wraz ze szkoleniem**
2. Zamawiający wymaga dostarczenia wsparcia dla posiadanego klastra urządzeń firewall Sonicwall NSA4600 na okres 5 lat. (Zamawiający posiada: ADVANCED GATEWAY SECURITY SUITE BUNDLE FOR NSA 4600 5YR – 01-SSC-1494).
3. Wraz z dostarczonym wsparciem Zamawiający wymaga autoryzowanego szkolenia z obsługi wymienionych urządzeń firewall w zakresie:
4. podstawy zarządzania klastrem firewall,
5. podstawy konfiguracji zaawansowanych ustawień VPN, filtrowania treści, detekcji i zapobiegania włamań,
6. podstawy analizy logów ruchu przepływającego przez urządzenie.
7. Szkolenie musi być przeprowadzone przez Producenta urządzeń bądź też autoryzowanego Dystrybutora urządzeń Sonicwall w centrum szkoleniowym producenta lub dystrybutora we wskazanym zakresie trwające co najmniej 24 godziny szkoleniowe (3 dni szkoleniowe).
8. **Rozbudowa istniejącej macierzy o dodatkowy kontroler**
9. Zamawiający wymaga dostarczenia dwóch kontrolerów do posiadanej przez Zamawiającego macierzy Dell SCv3020 (Zamawiający posiada: numer seryjny - 265892)
10. Zamawiający w celu zapewnienia pełnej kompatybilności z posiadaną macierzą wymaga dostawy następujących kontrolerów:

2 kontrolery Dell 406-BBLX - IO, 16Gb FC, 4Port, PCI-E, Full height

1. Dostarczone kontrolery muszą być nowe, nie mogą być używane wcześniej w innych projektach oraz nie mogą naruszać gwarancji serwisowej macierzy, w których zostaną zainstalowane.
2. W ramach zamówienia Wykonawca przeprowadzi instalację i konfigurację kontrolerów w macierzy oraz przeprowadzi pełną konfigurację systemu wraz z dopięciem do posiadanej infrastruktury Vmware, przełączników SAN oraz drugiej macierzy Dell SCv3020.