OPIS PRZEDMIOTU ZAMÓWIENIA

Urządzenie do przechowywania kopii zapasowych

1. Urządzenie musi być przeznaczone do deduplikacji i przechowywania kopii zapasowych.
2. Dostarczone urządzenie musi oferować przestrzeń co najmniej 25TB netto (powierzchnia użytkowa do wykorzystania na przechowywanie kopii zapasowych po odjęciu przestrzeni wykorzystywanej przez mechanizmy ochrony danych).
3. Oferowane urządzenie musi posiadać minimum:
   - 4 porty Ethernet 1 Gb/s, obsługa protokołów CIFS, NFS, OST/Boost;
   - 2 porty Ethernet 10 Gb/s RJ-45, obsługa protokołów CIFS, NFS, OST/Boost;
   - 2 porty FC 8Gb/s, wymagana obsługa protokołów: VTL, OST/Boost
4. Oferowane urządzenie dla portów Ethernet musi umożliwiać jednoczesny dostęp protokołami: CIFS, NFS, OST/Boost.
5. Wymagane jest dostarczenie licencji, pozwalającej na jednoczesną obsługę protokołów CIFS, NFS, OST/Boost do pełnej pojemności urządzenia wraz z dostarczanymi półkami dyskowymi.
6. Oferowane pojedyncze urządzenie musi osiągać zagregowaną wydajność (dla maksymalnej konfiguracji) protokołami CIFS, NFS: co najmniej 5 TB/h (według danych deklarowanych przez producenta) oraz co najmniej 13 TB/h z wykorzystaniem deduplikacji na źródle (według danych deklarowanych przez producenta).
7. Urządzenie musi pozwalać na jednoczesną obsługę co najmniej 170 strumieni w tym jednocześnie:
   - zapis danych minimum 110 strumieniami
   - odczyt danych minimum 40 strumieniami
   - replikacja minimum 20 strumieniami

   pochodzących z różnych aplikacji oraz dowolnych protokołów (CIFS, NFS, VTL, OST/Boost) oraz dowolnych interfejsów (FC, LAN) w tym samym czasie. Wymienione wartości 170 jednoczesnych strumieni dla wszystkich protokołów (110 dla zapisu, jednocześnie 40 dla odczytu i jednocześnie 20 dla replikacji) muszą mieścić się w przedziale oficjalnie rekomendowanym i wspieranym przez producenta urządzenia. Wszystkie zapisywane strumienie muszą podlegać globalnej deduplikacji przed zapisem na dysk (in-line) jak opisano w niniejszej specyfikacji.
8. Oferowane urządzenie musi mieć możliwość emulacji co najmniej następujących bibliotek taśmowych:
   - StorageTek L180
   - Adic Scalar i2000
   - Adic Scalar i6000
   - IBM 3500
9. Oferowane urządzenie musi mieć możliwość emulacji napędów taśmowych LTO1, LTO2, LTO3, LTO4, LTO5.
10. Urządzenie musi eksportować i importować definicje bibliotek taśmowych. Musi być możliwość eksportu / importu definicji bibliotek taśmowych między różnymi modelami urządzeń producenta.
11. Urządzenie musi umożliwiać przyporządkowanie minimum 120 napędów do emulowanej pojedynczej biblioteki taśmowej.

12. 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.
13. Technologia deduplikacji musi wykorzystywać algorytm bazujący na zmiennym, dynamicznym bloku. Algorytm ten musi samoczynnie i automatycznie dopasowywać się do otrzymywanego strumienia danych, co oznacza, że urządzenie musi dzielić otrzymany pojedynczy strumień danych na bloki o różnej długości, bez konieczności podejmowania czynności mających na celu ustalenie predefiniowanej długości bloków używanych do deduplikacji danych określonego typu.
14. Deduplikacja zmiennym, dynamicznym blokiem oznacza, że wielkość każdego bloku (na jaki są dzielone dane pojedynczego strumienia backupowego) może być inna niż poprzedniego oraz jest indywidualnie ustalana przez algorytm deduplikacji zastosowany w urządzeniu. Oferowane urządzenie nie może dzielić jakiegokolwiek pojedynczego strumienia danych backupowych na bloki o ustalonej, tej samej długości.
15. Oferowany produkt musi posiadać obsługę mechanizmów globalnej deduplikacji dla danych otrzymywanych jednocześnie wszystkimi protokołami (CIFS, NFS, VTL, OST/Boost) przechowywanych w obrębie całego urządzenia, co oznacza, że przechowywany na urządzeniu fragment danych nie może być ponownie zapisany bez względu na to, jakim protokołem zostanie ponownie otrzymany. Powyższe oznacza również, że oferowany produkt musi również posiadać obsługę mechanizmów globalnej de-duplikacji pomiędzy dowolnymi dwoma (i więcej) wirtualnymi bibliotekami emulowanymi w obrębie tego samego urządzenia. Blok danych otrzymany i zapisany w wirtualnej bibliotece A, nie może zostać ponownie zapisany, jeśli trafi do innej wirtualnej biblioteki B w obrębie tego samego urządzenia (to samo dotyczy udziałów NFS/CIFS).
16. Przestrzeń składowania zdeduplikowanych danych musi być jedna dla wszystkich protokołów dostępowych, co oznacza zastosowanie pojedynczej bazy deduplikatów bez względu na ilość/rodzaj używanych protokołów dostępowych.
17. Proces deduplikacji musi odbywać się in-line – w pamięci urządzenia, przed zapisem danych na nośnik dyskowy. Zapisowi na system dyskowy muszą podlegać tylko unikalne bloki danych niezapisane jeszcze na system dyskowy urządzenia. Dotyczy to każdego fragmentu przychodzących do urządzenia danych.
18. Wszystkie unikalne bloki przed zapisaniem na dysk muszą być kompresowane co najmniej jednym z algorytmów do wyboru: gz, lz.
19. Oferowane urządzenie musi wspierać (wymagane formalne wsparcie producenta urządzenia), co najmniej następujące aplikacje: HP Data Protector, VERITAS NetBackup, EMC NetWorker, EMC Avamar, Oracle RMAN, IBM Data Studio, VMware VDP, Microsoft SQL Server Management Studio, Veeam. W przypadku współpracy z każdą z poniższych aplikacji:
    - RMAN (dla ORACLE)
    - Microsoft SQL Server Management Studio (dla Microsoft SQL)
    - IBM Data Studio (dla DB2)
    - SAP BR*Tools (dla SAP/Oracle)
    - vShpehre Data Protection - VDP (dla VMware)
    - VERITAS NetBackup
    - VERITAS BackupExec
    - HP Data Protector
    - EMC NetWorker

- EMC Avamar
- Veeam

urządzenie musi umożliwiać deduplikację na źródle i przesłanie nowych, nieznajdujących się jeszcze na urządzeniu bloków poprzez sieć LAN. Deduplikacja danych odbywa się na dowolnym serwerze posiadającym funkcjonalność Media Servera NetBackup'a / klienta Avamar / serwera RMAN / serwera SQL / serwera SAP / serwera DB2/ klienta VDP / klienta systemu NetWorker nieposiadającego licencji Storage Node. Deduplikacja w wyżej wymienionych przypadkach musi zapewniać, aby z serwerów do urządzenia były transmitowane poprzez sieć LAN tylko fragmenty danych nieznajdujące się dotychczas na urządzeniu. Wymagana integracja z VDP - umożliwiająca zwiększenie przestrzeni obsługiwanej/adresowanej przez VDP z 8TB do min. 50TB, wymagane potwierdzenie funkcjonalności (wymaganej integracji) w oficjalnej dokumentacji producenta oferowanego urządzenia oraz dokumentacji VMware.

20. W przypadku przyjmowania backupów od VERITAS NetBackup, EMC NetWorker, Oracle RMAN, Microsoft MSSQL (przy wykorzystaniu Microsoft SQL Server Management Studio), IBM DB2 (przy wykorzystaniu IBM Data Studio), SAP/Oracle (przy wykorzystaniu SAP BR*Tools), Veeam urządzenie musi umożliwiać de-duplikację na źródle i przesłanie nowych, nieznajdujących się jeszcze na urządzeniu bloków poprzez sieć FC. Deduplikacja w wyżej wymienionych przypadkach musi zapewniać, aby z serwerów do urządzenia były transmitowane poprzez sieć FC tylko fragmenty danych nieznajdujące się dotychczas na urządzeniu.
21. W przypadku deduplikacji na źródle poprzez sieć IP (LAN oraz WAN), wymagana możliwość szyfrowania komunikacji kluczem minimum 256 bitów.
22. Urządzenie musi wspierać deduplikację na źródle poprzez sieć FC (SAN) minimum dla następujących systemów operacyjnych:
    - Windows
    - Linux (RedHat, SuSE)
    - HP-UX
    - AIX
    - Solaris
23. Dla aplikacji VERITAS NetBackup, EMC NetWorker, urządzenie musi pozwalać na łączenie backupów pełnych i przyrostowych bez odczytu danych z urządzenia. Zarządzanie łączeniem backupów pełnych i przyrostowych musi być wykonywane z poziomu aplikacji VERITAS NetBackup, EMC NetWorker
24. Urządzenie nie może zmniejszać swojej wydajności w czasie przybywania kolejnych danych.
25. Oferowane urządzenie musi umożliwiać bezpośrednią replikację danych do drugiego urządzenia takiego samego typu. Konfiguracja replikacji musi być możliwa w każdym z trybów:
    - jeden do jednego
    - wiele do jednego
    - jeden do wielu
    - kaskadowej (urządzenie A replikuje dane do 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. Ewentualna licencja na replikację musi być dostarczona w ramach postępowania.
26. Urządzenie musi umożliwiać wydzielenie określonych portów Ethernet dedykowanych do replikacji. W przypadku wykorzystania portów Ethernet do

replikacji urządzenie musi umożliwiać przyjmowanie backupów, odtwarzanie danych, przyjmowanie strumienia replikacji, wysyłanie strumienia replikacji tymi samymi portami.

27. W przypadku replikacji danych między dwoma urządzeniami kontrolowanej przez systemy VMware VDP / VERITAS NetBackup / VERITAS BackupExec / HP Data Protector / EMC Avamar / EMC NetWorker muszą być możliwe do uzyskania jednocześnie wszystkie następujące funkcjonalności:
    - replikacja odbywa się bezpośrednio między dwoma urządzeniami bez udziału serwerów pośredniczących
    - replikacji podlegają tylko te fragmenty danych, które nie znajdują się na docelowym urządzeniu
    - replikacja zarządzana jest z poziomu aplikacji backupowej
    - aplikacja backupowa posiada informację o obydwu kopiach zapasowych znajdujących się w obydwu urządzeniach bez konieczności przeprowadzania procesu inwentaryzacji
28. Oferowane urządzenie musi działać poprawnie przy zapełnieniu danymi na poziomie, co najmniej 90%. Dokumentacja urządzenia nie może wskazywać na ew. problemy, obostrzenia, które są efektem zapełnienia urządzenia zabezpieczanymi danymi, na poziomie mniejszym niż 90%.
29. Narzut na wydajność związany z replikacją nie może zmniejszyć wydajności urządzenia o więcej niż 10%.
30. Wymagana możliwość ograniczenia pasma używanego do replikacji między dwoma urządzeniami.
31. Zdeduplikowane i skompresowane dane przechowywane w obrębie podsystemu dyskowego urządzenia muszą być chronione za pomocą technologii co najmniej RAID 6.
32. 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.
33. Łącznie oferowane urządzenie musi posiadać zapasowe dyski typu hot-spare stanowiące minimum 7% powierzchni roboczej urządzenia.
34. Oferowane urządzenie musi umożliwiać wykonywanie SnapShot'ów, czyli umożliwiać zamrożenie obrazu danych (stanu backupów) w urządzeniu na określoną chwilę. Oferowane urządzenie musi również umożliwiać odtworzenie danych ze Snapshot'u. Odtworzenie danych ze Snapshot'u nie może wymagać konieczności nadpisania danych produkcyjnych jak również nie może oznaczać przerwy w normalnej pracy urządzenia (przyjmowania/odtwarzania backupów).
35. Urządzenie musi pozwalać na przechowywanie minimum 700 Snapshotów jednocześnie w obrębie oferowanej przestrzeni, przy zachowaniu globalnej deduplikacji oraz standardowego trybu pracy urządzenia - umożliwiającego wykorzystanie wszystkich dostępnych funkcjonalności.
36. Urządzenie musi umożliwiać podział na logiczne części. Dane znajdujące się w każdej logicznej części muszą być między sobą de-duplikowane (globalna de-duplikacja między logicznymi częściami urządzenia).
37. 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.
38. Dla każdej z w/w logicznych części oferowanego urządzenia musi być możliwość zdefiniowania oddzielnego użytkownika zarządzającego daną logiczną częścią de-duplikatora. Użytkownicy zarządzający logiczną częścią A muszą widzieć tylko i wyłącznie zasoby logicznej części A i nie mogą widzieć żadnych innych zasobów

oferowanego urządzenia.

39. Wymagana możliwość zaprezentowania każdej z logicznych części oferowanego urządzenia, jako niezależnego urządzenia dostępnego za pośrednictwem:
    - CIFS
    - NFS
    - VTL
    - OST/Boost
40. Urządzenie powinno umożliwiać zdefiniowanie blokady skasowania danych (funkcjonalność WORM). Blokada skasowania danych musi chronić plik w zdefiniowanym czasie przed usunięciem pliku, modyfikacją pliku. Blokada skasowania danych musi działać w dwóch trybach (do wyboru przez administratora):
    - 1. Możliwość zdjęcia blokady przed upływem ważności danych
    - 2. Brak możliwości zdjęcia blokady przed upływem ważności danych (COMPLIANCE)

    Licencje na blokadę usunięcia/zmiany przechowywanych plików w chwili obecnej nie muszą być dostarczone wraz z urządzeniem.
41. Urządzenie musi mieć możliwość przechowywania danych niezmienialnych:
    - Video
    - Grafika
    - Nagrania dźwiękowe
    - Pliki pdf

    na udziałach CIFS/NFS.
    Wymagane jest formalne wsparcie producenta dla przechowywania w/w danych na urządzeniu. Wymagana jest formalne wsparcie producenta dla:
    - przechowywania na urządzeniu minimum 500 milionów plików
    - dziennego zasilania urządzenia na poziomie minimum 500 tysięcy plików
42. Po niespodziewanym wyłączeniu prądu i ponownym uruchomieniu, urządzenie musi być gotowe do przyjmowania danych (backupy, archiwa) w czasie nie dłuższym niż 60 minut od włączenia.
43. Urządzenie musi weryfikować ewentualne przekłamania (zmianę danych) na poziomie:
    - systemu plików
    - grup RAID

    Wymaga się, aby urządzenie weryfikowało sumy kontrolne dla wszystkich fragmentów zapisywanych danych, niezależnie od używanego interfejsu.
44. Urządzenie musi weryfikować dane po zapisie (nie chodzi o ew. weryfikację danych indeksowych generowanych przez urządzenie, ale o weryfikację wszystkich zabezpieczanych danych backup'owych). Każda zapisana na dyskach porcja danych musi być odczytana i porównana z danymi otrzymanymi przez urządzenie. Powyższa weryfikacja powinna być realizowana w locie, czyli przed usunięciem z pamięci oryginalnych danych (otrzymanych z aplikacji backupowej), musi być realizowana w trybie ciągłym (a nie ad-hoc), wymagane parametry wydajnościowe urządzenia muszą uwzględniać tę funkcjonalność. Wymagane potwierdzenie opisanej funkcjonalności w oficjalnej dokumentacji producenta oferowanego urządzenia.
45. Urządzenie musi automatycznie (samoczynnie) wykonywać sprawdzanie spójności danych po zapisaniu danych na dysk oraz rozpoznawać i naprawiać błędy w locie. Każde zapisane na fizycznych dyskach dane muszą być odczytane i porównane z danymi otrzymanymi. Proces ten musi odbywać się „w locie" – musi być elementem procesu zapisu danych przez urządzenie.

46. Urządzenie musi automatycznie usuwać przeterminowane dane (bloki danych nienależące do backupów o aktualnej retencji) w procesie czyszczenia.
47. Proces usuwania przeterminowanych danych (czyszczenia) nie może uniemożliwiać pracy procesów backupu / odtwarzania danych (zapisu / odczytu danych z zewnątrz do systemu).
48. Musi istnieć możliwość zdefiniowania maksymalnego obciążenia urządzenia procesem usuwania przeterminowanych danych (poziomu obciążenia procesora).
49. Musi istnieć możliwość zdefiniowania czasu, w którym wykonywany jest proces usuwania przeterminowanych danych (czyszczenia).
50. 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).
51. Urządzenie musi zapewniać w przypadku dni roboczych (poniedziałek – piątek) minimum 20 godzin pełnej wydajności (dla każdej roboczej doby). Wymagana pełna wydajność, dostępna w okresie pon-pt - min. 20 godzin dziennie oznacza, że urządzenie nie może w tym czasie wykonywać wewnętrznych procesów serwisowych, w szczególności nie może wykonywać usuwania przeterminowanych danych (cleaning).
52. Urządzenie musi mieć możliwość zarządzania poprzez
    - Interfejs graficzny dostępny z przeglądarki internetowej
    - Poprzez linię komend (CLI) dostępną z poziomu ssh (secure shell)
53. Oprogramowanie do zarządzania musi rezydować na oferowanym urządzeniu de-duplikacyjnym.
54. 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.
55. Oferowany produkt musi mieć możliwość zaimplementowania funkcjonalności wewnętrznego mechanizmu szyfrowania danych przed zapisaniem na dysk realizowany na poziomie urządzenia – długość klucza minimum 256-bit. Ewentualna licencja szyfrowania nie jest przedmiotem niniejszego zamówienia.
56. Urządzenie musi być rozwiązaniem kompletnym, sprzętowym, pochodzącym od jednego producenta. Zamawiający nie dopuszcza stosowania rozwiązań typu gateway. Oferowany typ urządzenia musi być oficjalnie dostępne w ofercie producenta przed ukazaniem się niniejszego postępowania.

System wykonywania kopii zapasowych

1. Zamawiający wymaga dostarczenia, uruchomienia i wdrożenia systemu wykonywania kopii zapasowych, w tym:
    - oprogramowania do wykonywania kopii zapasowych uruchomionego na dedykowanym serwerze (tzw. appliance);
    - komponentu diagnostyczno-raportującego dla dostarczonego serwera i oprogramowania;
    - rozwiązania continous data protection dla posiadanego środowiska VMware.
2. Wymagane jest dostarczenie wszystkich modułów oprogramowania wraz z zasobami sprzętowymi pochodzącymi od tego samego producenta, zapewniających wszystkie wymagane funkcjonalności w obrębie zadeklarowanego wolumenu danych.
3. Wymagane jest, aby oferowane oprogramowania było licencjonowane

per sumaryczna ilość CPU backupowanego środowiska VMware. Wymagane jest dostarczenia licencji obejmujących co najmniej 10 CPU z możliwością rozszerzenia do co najmniej 150 CPU, bez ograniczeń co do ilości zabezpieczanych danych, ilości baz danych backupowanych w sposób on-line, ilości/rodzajów generowanych raportów oraz ilości i retencji danych składowanych w systemie backupu. Oferowane rozwiązanie musi umożliwiać w ramach dostarczonych licencji dodatkowy backup co najmniej siedmiu niezwirtualizowanych serwerów fizycznych, bez ograniczeń, co do ilości danych lub ilości baz danych wymagających backupu on-line. Wymagane jest, aby wszystkie wyspecyfikowane funkcjonalności były dostępne w ramach oferowanych licencji.

4. 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, Mac OS X, FreeBSD. Backup zasobów plikowych z powyższych systemów musi podlegać de-duplikacji ze zmiennym blokiem na zabezpieczanej maszynie zgodnie z wyspecyfikowanymi wymaganiami zawartymi w niniejszym dokumencie.
5. Oprogramowanie backupowe musi wspierać (wymagane wsparcie producenta) backup online następujących baz danych i aplikacji: MS Exchange, MS SQL, Oracle DB, IBM DB2, Lotus Notes, SharePoint, SAP, VMware, HyperV. Backup z powyższych baz danych i aplikacji musi podlegać de-duplikacji ze zmiennym blokiem na zabezpieczanej maszynie zgodnie z wyspecyfikowanymi wymaganiami zawartymi w niniejszym dokumencie.
6. W przypadku zabezpieczania baz danych i aplikacji musi istnieć możliwość pobierania kopii zapasowej kilkoma strumieniami jednocześnie (minimum 10 jednoczesnych strumieni).
7. W przypadku zabezpieczania systemu Exchange musi istnieć możliwość backupu całego obrazu bazy danych i jednocześnie odtworzenia pojedynczego maila bez konieczności odtwarzania całej bazy danych.
8. W przypadku zabezpieczania systemu SharePoint musi istnieć opcjonalna (licencja nie jest wymagana) możliwość odtworzenia pojedynczego elementu systemu SharePoint bez konieczności odtwarzania całego środowiska SharePoint.
9. Oferowane rozwiązanie musi zabezpieczać zdeduplikowane dane Windows Server 2012 bez konieczności przywracania danych Windows Server 2012 do postaci oryginalnej (nie zdeduplikowanej).
10. Zabezpieczane serwery muszą być backupowane bezpośrednio na medium backupowe (dyski zaoferowanego serwera (appliance'u) lub dyski zaoferowanego urządzenia do składowania kopii zapasowych (deduplikatora) bez pośrednictwa jakichkolwiek innych urządzeń lub serwerów. Dotyczy to backupów lokalnych, zdalnych jak również backupu stacji roboczych.
11. Oprogramowanie backupowe musi umożliwiać:
    - backup pojedynczych plików;
    - backup całych systemów plików;
    - backup baz danych w trakcie ich normalnej pracy;
    - backup ustawień systemu operacyjnego Windows;
    - backup całych obrazów maszyn wirtualnych systemu VMware;
    - backup całych obrazów maszyn wirtualnych systemu Hyper-V.
12. Rozwiązanie backupowe musi umożliwiać transfer danych bezpośrednio ze zdalnych oddziałów do zaoferowanego appliance'u bez konieczności instalacji jakiegokolwiek sprzętu w oddziale. Backup zdalnych oddziałów musi działać poprawnie w przypadku opóźnienia do 2 sekund w sieci WAN, utraty pakietów na poziomie do 50% oraz przerwą w działaniu łącza WAN do 30 min.

Powyższa funkcjonalność wymagana jest dla następujących typów danych:

- backup pojedynczych plików;
- backup całych systemów plików;
- backup baz danych w trakcie ich normalnej pracy.

Rozwiązanie backupowe nie może wymagać jakichkolwiek czynności ze strony personelu pracującego w oddziale.

Rozwiązanie backupowe musi być w pełni konfigurowalne z centralnej konsoli. W szczególności backupy maszyn w oddziałach (bazy danych, pliki) czy też backupy stacji roboczych muszą być konfigurowalne z poziomu centralnej konsoli bez konieczności logowania się na zabezpieczaną maszynę. Rozwiązanie backupowe musi mieć również możliwość odtworzenia plików i baz danych na docelowa maszynę w oddziale z poziomu centralnej konsoli systemu backupowego. Nie może być wymagane logowanie się na odtwarzaną maszynę celem odtworzenia danych z systemu backupowego.

13. W przypadku wyboru odtwarzania całego systemu plików (dysk w systemi Windows, cały system plików w Linux/UNIX) dla systemów Windows/Linux/UNIX rozwiązanie backupowe musi automatycznie i samodzielnie porównać pliki znajdujące się w kopii zapasowej z plikami znajdującymi się na 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.
14. Celem minimalizacji ilości przesyłanych danych, oferowane rozwiązanie musi mieć możliwość przesyłania odtwarzanych danych z medium backupowego do docelowego serwera w postaci skompresowanej, tak, aby odtwarzane dane były rozkompresowane na docelowym serwerze przez agenta oferowanego systemu wykonywania kopii zapasowych.
15. Oprogramowanie backupowe musi mieć funkcjonalność podziału danych (plików, baz danych, obrazów maszyn wirtualnych) na bloki o zmiennej długości. System musi się dopasowywać do struktury przesyłanych danych zapewniając podział na bloki o różnej długości w ramach pojedynczego obiektu. Podział na bloki musi następować bezpośrednio na zabezpieczanym serwerze.
16. Mechanizm deduplikacji musi również generować zmienny blok w przypadku backupu pojedynczego obiektu. Bloki wysyłane w trakcie backupu pojedynczego obiektu (z zabezpieczanej maszyny do medium de-duplikacyjnego) muszą być różnej długości jednak nie większej niż 32KB.
17. Oprogramowanie wykonujące kopie zapasowe musi backupować tylko unikalne bloki, nieznajdujące się na docelowym urządzeniu.
18. Włączenie funkcjonalności deduplikacji nie może generować wymogu instalacji dodatkowych modułów programowych po stronie zabezpieczanej maszyny lub serwera backupowego.
19. Oprogramowanie backupowe nie może odczytywać 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.
20. Oprogramowanie backupowe musi wykonywać zawsze tylko logicznie pełne backupy systemu plików. Z zabezpieczanego systemu plików muszą być odczytywane tylko nowe lub zmienione pliki, do appliance'u backupowego muszą być wysyłane dane po deduplikacji, 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.

21. W konsoli oprogramowania backupowego musi być możliwość definiowania ważności danych (backupów) na podstawie kryteriów czasowych (dni, miesiące, lata). Po okresie ważności backupy muszą być automatycznie usunięte.
22. Oferowanie oprogramowanie backupowe musi mieć możliwość tworzenia polityki, w której zdefiniowano:
    - czas przechowywania backupów dziennych;
    - czas przechowywania backupów tygodniowych;
    - czas przechowywania backupów miesięcznych;
    - czas przechowywania backupów rocznych.
23. Oferowane rozwiązanie musi umożliwiać tworzenie wykluczeń, czyli elementów niepodlegających backupowi w ramach zadania backupowego. Musi istnieć możliwość tworzenia wykluczeń dla dowolnej kombinacji następujących elementów:
    - dla wybranych typów plików, np. dla plików z danym rozszerzeniem;
    - dla całych katalogów;
    - dla pojedynczych plików.
24. Oferowane rozwiązanie musi mieć możliwość zdefiniowania, aby ostatni backup dowolnego zbioru danych nigdy się nie przeterminował. Oznacza to, że jeśli dany zasób nie jest backupowany to automatycznie ostatnie ważny backup tego zasobu jest trzymany bezterminowo. Jedynie administrator może zdecydować o jego usunięciu.
25. Musi istnieć możliwość w ramach rozbudowy systemu zainstalowania w przyszłości analogicznego serwera backupu na platformie VMware ESX (appliance wirtualny) oraz Hyper-V (appliance wirtualny). Oferowane urządzenie musi mieć możliwość replikacji danych z appliancem wirtualnym w obu kierunkach jednocześnie:
    - appliance fizyczny w ośrodku A do appliance'a wirtualnego w ośrodku B;
    - appliance wirtualny w ośrodku B do appliance'a fizycznego w ośrodku A.

    Replikacji muszą podlegać tylko bloki unikalne, nieznajdujące się na docelowym urządzeniu. Musi istnieć możliwość zdefiniowania harmonogramu replikacji między appliance'ami oraz zdefiniowania, które zadania backupowe podlegają replikacji.
26. Konsola zarządzająca systemem backupowym musi integrować się z Active Directory. Musi być możliwość przydzielania użytkownikom i grupom Active Directory dostępnych ról w systemie backupowym.
27. Konsola zarządzająca musi udostępniać raporty dotyczące zajętości przestrzeni przeznaczonej na deduplikaty.
28. Bloki przesyłane z zabezpieczanych serwerów do appliance'a backupowego lub do oferowanego deduplikatora muszą być kompresowane i szyfrowane algorytmem z kluczem minimum 256-bitowym. Musi istnieć możliwość szyfrowania danych na medium dyskowym przechowującym backupy (deduplikaty). Ewentualna licencja szyfrowania musi być dostarczona w ramach postępowania.
29. Wymagane jest uwierzytelnienie komunikacji między klientem a serwerem backupu oparte na certyfikatach.
30. Oprogramowanie backupowe musi pozwalać na odtwarzanie danych poprzez: wybór odtwarzanych danych, odtworzenie danych w jednym kroku.
31. Oprogramowanie backupowe musi mieć możliwość limitowania wielkości zadania backupowego. Jeśli zadanie backupowe przekroczy zdefiniowaną wielkość wówczas nie może być zapisane w systemie backupowych.
32. Oprogramowanie backupowe musi umożliwiać ograniczenie mocy procesora używanej do wykonywania zdania backupu tak by odpowiednia moc procesora zostawić dla innych zadań.

33. Rozwiązanie backupowe musi wspierać backup i odtwarzanie środowisk VMware 5.5 i nowszych.
34. Oprogramowanie backupowe musi umożliwiać dla środowisk VMware następujące typy backupu:
    - backup całych maszyn wirtualnych;
    - backup pojedynczych, wybranych dysków maszyny wirtualnej;
    - musi istnieć możliwość zastosowania wyrażeń regularnych do określenia, które wirtualne dyski VMware mają być backupowane;
    - w trakcie backupu odczytowi z systemu dyskowego muszą podlegać tylko zmienione bloki wirtualnych maszyn systemu VMware (wymagane jest wykorzystanie mechanizmu CBT systemu VMware);
    - wykonywanie backupu obrazów maszyn wirtualnych VMware nie może wymagać bufora dyskowego na kopię obrazów maszyn wirtualnych.

    Powyższe metody backupu maszyn wirtualnych muszą podlegać deduplikacji ze zmiennym blokiem przed wysłaniem danych do medium backupowego zgodnie z wymaganiami dla deduplikacji powyżej. Powyższe metody backupu muszą być wbudowane w system backupu.
35. Oferowany system musi pozwalać na odtworzenie całych obrazów maszyn wirtualnych lub pojedynczych dysków maszyny wirtualnej z backupu całej maszyny wirtualnej
36. Rozwiązanie backupowe musi umożliwiać odtworzenie obrazów maszyn wirtualnych VMware dostarczając następujące funkcjonalności:
    - odtworzenie całych maszyn wirtualnych musi wykorzystywać mechanizm CBT systemu VMware – odtwarzane są tylko te bloki wirtualnej maszyny/dysku, które uległy zmianie od ostatniego backupu;
    - 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;
    - 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.

    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, w pełni automatyczne bez wykorzystania skryptów/dodatkowych komend.
37. Rozwiązanie backupowe musi umożliwiać uruchomienie maszyny wirtualnej bezpośrednio z oferowanego deduplikatora bez konieczności odtwarzania (Instant Access).
38. 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.
39. Oprogramowanie backupowe musi mieć możliwość backupu / odtworzenia w trybie image backup (backup plików vmdk) maszyn wirtualnych znajdujących się na serwerach VMware ESXi bez udziału vCenter.
40. Oprogramowanie backupowe musi mieć możliwość automatycznego sprawdzania (weryfikacji) zbackupowanych maszyn wirtualnych VMware. Musi istnieć

możliwość ustawienia harmonogramu weryfikacji maszyn wirtualnych VMware.
Weryfikacja maszyn wirtualnych musi zapewniać minimum:

- odtworzenie maszyny wirtualnej na zdefiniowanym DataCenter / DataStore
- weryfikacja podstawowych procesów
- możliwość dołączenia własnego skryptu weryfikującego wybrane elementy maszyny wirtualnej.

W konsoli systemu backupu musi być wyświetlana informacja o poprawnej / niepoprawnej weryfikacji maszyny wirtualnej.

41. Administrator danej maszyny wirtualnej VMware musi mieć możliwość samodzielnego (bez konieczności kontaktu z administratorem backupu czy tez administratorem VMware) odtworzenia pojedynczych plików z dowolnego backupu obrazu jego maszyny wirtualnej.
42. 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.
43. Rozwiązanie backupowe musi pozwalać automatyczne polityki backupowe dla folderu i resource pool systemu VMware. Oznacza to, że dodanie maszyny wirtualnej do folderu hosta czy resource pool w systemie VMware spowoduje automatyczne backupowanie dodanej maszyny wirtualnej zgodnie z polityka zdefiniowana dla folderu hosta czy resource pool w systemie VMware.
44. 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.
45. 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.
46. Backup oraz odtworzenie maszyn wirtualnych VMware musi być możliwy z poziomu graficznego interfejsu, linii komend oraz przez REST API.
47. Oprogramowanie backupowe musi umożliwiać dla środowisk Hyper-V:
    - backup pojedynczych plików i baz danych z maszyny wirtualnej ze środka maszyny wirtualnej Hyper-V;
    - backup całych maszyn wirtualnych (czyli plików vhd reprezentujących wirtualną maszynę);
    - wykonywanie backupu całych maszyn wirtualnych nie może wymagać bufora dyskowego na kopię obrazów maszyn wirtualnych (plików vhd);
    - wykonywanie backupu całych maszyn wirtualnych 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 deduplikacji ze zmiennym blokiem w momencie odczytu danych zgodnie z wymaganiami niniejszej specyfikacji.
48. Oprogramowanie backupowe musi zapewniać spójny backup Exchange / MSSQL

przy backupie obrazów maszyn wirtualnych środowiska Hyper-V.

49. Musi istnieć możliwość odtworzenia danych z zabezpieczanego serwera / komputera oraz z z konsoli systemu backupowego.
50. Musi istnieć możliwość odtworzenia pojedynczego pliku oraz zabezpieczanej bazy danych.
51. Dla systemów Windows Server 2008 i nowszych oraz Windows 7 i nowszych 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.
52. W przypadku odtwarzania danych z interfejsu dostępnego na zabezpieczanym serwerze musi istnieć mechanizm uwierzytelniania użytkowników dostępny w dwóch opcjach:
    - wbudowany w system backupowy
    - zintegrowany z usługami katalogowymi.

    W przypadku wykorzystania Active Directory, użytkownicy będący w domenie nie muszą się logować do systemu backupu w przypadku konieczności odtworzenia danych, przeszukania zwartości swoich backupów oraz wykonania backupu.
53. Dla odtwarzania danych z interfejsu końcowego użytkownika muszą być dostarczone następujące funkcjonalności:
    - wyszukiwanie pliku do odtwarzania po: nazwie pliku, początkowym fragmencie nazwy pliku, końcowym fragmencie nazwy pliku, fragmencie nazwy pliku umiejscowionym gdziekolwiek w pełnej nazwie pliku
    - przeglądania zawartości zbackupowanego systemu plików i wybór zasobów do odtworzenia
    - wybór wersji odtwarzanego pliku / katalogu.
54. Rozwiązanie backupowe musi umożliwiać odtworzenie plików z dowolnego urządzenia (laptop, tablet, smartphone) poprzez przeglądarkę internetową. Odtwarzanie to musi spełniać następujące kryteria:
    - uwierzytelnienia użytkownika
    - wyszukiwanie pliku do odtwarzania po: nazwie pliku, początkowym fragmencie nazwy pliku, końcowym fragmencie nazwy pliku, fragmencie nazwy pliku umiejscowionym gdziekolwiek w pełnej nazwie pliku.
    - przeglądania zawartości zbackupowanego systemu plików i wybór zasobów do odtworzenia
    - wybór wersji odtwarzanego pliku / katalogu.
55. 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.
56. Wymagana możliwość doposażenia rozwiązania backup'owego o system wyrzutu danych na nośniki taśmowe realizowany poprzez zastosowanie gotowego modułu (pochodzącego od tego samego producenta).
57. System backupu musi być dostępny dla backupu i odtwarzania przez 24h na dobę 7 dni w tygodniu. Nie może być jakiegokolwiek przedziału czasowego czy momentu, w którym system backupowy nie może wykonywać backupu lub odtwarzania.
58. System backupu musi mieć możliwość bezpośredniego raportowania o błędach do serwisu producenta.
59. 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.

60. System backupu musi mieć możliwość automatycznej samoaktualizacji.
61. System backupu musi mieć możliwość automatycznej aktualizacji oprogramowania agentów wykonywanej bezpośrednio z serwera backupu.
62. System musi umożliwiać backup serwerów NAS z następującymi funkcjonalnościami:
    - w trakcie backupu z systemu NAS muszą być wysyłane do medium backupowego tylko zmienione pliki od ostatniego backupu
    - w przypadku odtwarzania, uprawnienia użytkowników również są odtwarzane
    - integracja z protokołem NDMP systemów NAS
    - odtworzenie plików z backupu NDMP bezpośrednio na platformę Windows/Linux

    ewentualne dodatkowe moduły/licencje dedykowane do backup'u poprzez NDMP nie są w tej chwili wymagane.
63. W ramach oferowanej licencji muszą być dostępne następujące funkcjonalności dotyczące raportowania, bezpośredniego backupu baz danych, przeszukiwania backupów:
    W ramach licencji musi być zapewniona możliwość monitorowania, raportowania, szczegółowego rozliczania z użycia komponentów systemu backupowego oraz analizy błędów dla środowiska kopii zapasowej Zamawiającego. System raportujący musi posiadać wbudowane następujące raporty:
    - podsumowanie zadań backupowych (liczba backupów udanych, nieudanych, aktywnych, łączny rozmiar zbackupowanych danych)
    - Podsumowanie zadań odtworzeniowych (liczba odtworzeń udanych, nieudanych, aktywnych, łączny rozmiar odtworzonych danych danych)
    - zbiorcze procentowe zestawienie udanych zadań backupowych z poszczególnych serwerów
    - zbiorcze zestawienie zabezpieczanych serwerów, które w sposób ciągły (kilka razy pod rząd) mają problem z backupami
    - zestawienie zabezpieczanych systemów plików, które w ogóle nie są backupowane
    - spodziewany czas odtwarzania zabezpieczanego serwera oraz potencjalnej utraty danych (czas między ostatnim backupem a chwilą awarii)
    - najmniej wiarygodne zabezpieczanych serwery (procent nieudanych backupów)
    - lista najwolniejszych/najszybszych zabezpieczanych maszyn
    - poziom SLA (procentowa liczba udanych backupów) w odniesieniu do poziomu założonego
    - mierzenie poziomu SLA dla poszczególnych zabezpieczanych serwerów przy uwzględnieniu założonego okna backupowego i RPO (punktu, do którego się odtwarzamy)
    - liczba danych backupowanych dziennie
    - liczba zadań backupowych dziennie
    - zużycie zasobów na serwerach backupowych (procesor, pamięć, karty sieciowe LAN, SAN)
    - zużycie mediów backupowych i napędów taśmowych
    - aktualna konfiguracja systemu backupowego
    - historia zmian konfiguracji systemu backupowego
    - posiadane licencje systemu backupowego
    - wykorzystanie systemu backupowego przez poszczególne działy / grupy

użytkowników (chargeback per cost center).

64. W ramach dostarczonej licencji musi być możliwość budowy rozwiązań continuous data protection dla środowisk VMware w obrębie deklarowanego środowiska (10 CPU), spełniających następujące wymagania:
    - integracja na poziomie VMware vCenter Plug-in (orchestration, management) , vSphere Web Client GUI
    - wsparcie dla HA, DRS, S-DRS, VMotion, S-Vmotion
    - możliwość integracji z VMware vRealize Operations Manager
    - rozwiązanie dostarczane w postaci oprogramowania instalowanego na platformie ESXi
    - skalowalność zapewniająca wsparcie dla 2000 VM w obrębie pojedynczego vCenter
    - zabezpieczenie 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 5.5 oraz 6.0
    - możliwość tworzenia tzw. consistency group zapewniających identyczną konsystencję dla przynależących do danej grupy maszyn wirtualnych
    - zabezpieczenie realizowane za pośrednictwem ciągłej replikacji (a nie za pomocą snapshotów) na poziomie vmdk oraz rdm, niezależnie od użytego storageu (tzw. Storage Agnostic -warunkiem jest wsparcie przez VMware), wymagane wsparcie dla połączeń: FC, FCoE, iSCSI, NAS oraz DAS
    - wsparcie dla replikacji (bi-directional) asynchronicznej oraz synchronicznej (realizowanej na poziomie dostarczanego oprogramowania), połączonych z mechanizmem tzw. journalingu umożliwiającego odnotowanie wszystkich zmian zabezpieczanego środowiska
    - odporność na krótkotrwałe problemy (przeciążenie, zaniki) związane z siecią WAN
    - wbudowana funkcjonalność deduplikacji oraz kompresji w przypadku transmisji danych poprzez WAN
    - wsparcie dla równoległej replikacji zabezpieczanego środowiska do różnych ośrodków docelowych (min. trzech), wsparcie dla replikacji równoległej powinno być zapewnione również na poziomie grup konsystencji (consistency group)
    - oferowane rozwiązanie powinno umożliwiać: stworzenia disaster recovery dla całego zabezpieczanego wirtualnego środowiska zbudowanego w oparciu o VMware, operacyjne odtwarzanie dowolnej maszyny wirtualnej wraz z aplikacjami, migrację danych w trybie on-line na inne zasoby dyskowe
    - równoległe wsparcie środowisk lokalnych oraz zdalnych, wymagana możliwość pracy w trzech 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
    - granularność umożliwiająca pominięcie określonych plików vmdk związanych z wirtualnymi serwerami objętych protekcją
    - architektura fault tolerant, brak pojedynczego punktu awarii
    - działanie rozwiązania będącego przedmiotem postępowania nie może mieć żadnego negatywnego wpływu na wydajność zabezpieczanych maszyn i aplikacji
    - wyskalowanie systemu powinno gwarantować RPO (Recovery Point Objective)

w przypadku codziennej pracy ciągłej na poziomie pojedynczych sekund
- proponowana konfiguracja systemu powinna zapewnić następującą retencję przechowywanych kopii bezpieczeństwa: RPO=30s z ostatnich 24h, RPO=24h z ostatniego tygodnia, RPO=1 tydzień z ostatniego miesiąca.
- możliwość odtworzenia zabezpieczanego środowiska do dowolnego punktu w czasie
- możliwość trybu pracy umożliwiającego objęciem protekcją w sposób automatyczny nowo dodanych maszyn wirtualnych
- rozwiązanie powinno dopuszczać zmiany sprzętowe na poziomie infrastruktury zabezpieczanego środowiska bez negatywnego wpływu na działanie systemu
- możliwość użycia mechanizmu typu bookmark dla oznaczenia konsystentnych kopii zabezpieczanych aplikacji
- wsparcie dla VSS, zapewnienie konsystencji aplikacji na poziomie VSS
- możliwość automatycznego przeprowadzania operacji typu failover/failback do dowolnego punktu w czasie dla określonych produkcyjnych serwerów wirtualnych, w tym: odtworzenie, uruchomienie (z zachowaniem wymaganej sekwencji), konfigurację
- możliwość automatycznego przeprowadzania operacji typu failover/failback do dowolnego punktu w czasie określonych testowych maszyn wirtualnych
- możliwość automatycznego zainicjowania procesu reverse replication w przypadku procesów failover/failback
- możliwość przeprowadzania testów disaster recovery bez wpływu na zabezpieczane serwery produkcyjne oraz bez konieczności zmian w działaniu replikacji
- możliwość skryptowego tworzenia planów recovery.

Usługi

1. Instalacja urządzenia deduplikacyjnego
    a) Montaż urządzenia deduplikacyjnego w szafie Rack
    b) Podłączenie urządzenia deduplikacyjnego do infrastruktury LAN
    c) Uruchomienie urządzenia
    d) Inicjalizacja urządzenia
    e) Aktualizacja oprogramowania układowego (firmware) urządzenia deduplikacyjnego do najnowszej, zalecanej przez producenta wersji
    f) Aktywacja wszystkich wymaganych funkcjonalności poprzez instalację właściwych oraz permanentnych kluczy licencyjnych
    g) Konfiguracja przestrzeni dyskowej (grupy RAID, dyski zapasowe typu hotspare), zgodnie z najlepszymi praktykami, zalecanymi przez producenta urządzenia
    h) Konfiguracja interfejsów sieciowych (agregacja portów sieciowych)
    i) Konfiguracja adresacji IP interfejsów sieciowych właściwych dla odpowiednich sieci wirtualnych VLAN
    j) Konfiguracja wirtualnych sieci VLAN na portach przełączników sieciowych, do których zostanie podłączone urządzenie deduplikacyjne
    k) Konfiguracja protokołów dostępu do urządzenia deduplikacyjnego: CIFS, NFS, OST/Boost
    l) Prezentacja przestrzeni dyskowej dla systemów informatycznych z wykorzystaniem protokołów: CIFS, NFS, OST/Boost
    m) Konfiguracja mechanizmu notyfikacji SMTP
    n) Konfiguracja mechanizmu monitorowania SNMP
    o) Konfiguracja mechanizmu automatycznego systemu powiadomień o zdarzeniach krytycznych, wysyłanych do producenta urządzenia
2. Instalacja systemu kopiowania i odtwarzania danych
    a) Montaż dedykowanego serwera (appliance) w szafie Rack
    b) Podłączenie serwera do sieci LAN
    c) Uruchomienie serwera
    d) Instalacja oprogramowania do wykonywania kopii zapasowych i odtwarzania danych
    e) Aktualizacja oprogramowania kopii zapasowych do najnowszej, stabilnej, zalecanej przez producenta wersji
    f) Konfiguracja oprogramowania kopii zapasowych
    g) Parametryzacja adresacji IP
    h) Integracja systemu kopiowania i odtwarzania danych z dostarczonym urządzeniem deduplikujących, jako repozytorium składowanych kopii zapasowych
    i) Aktywacja wszystkich wymaganych funkcjonalności poprzez instalację właściwych oraz permanentnych kluczy licencyjnych
3. Implementacja systemu kopiowania i odtwarzania danych
    a) Definicja obiektów sterujących polityką zabezpieczenia danych, zgodną z najlepszymi praktykami oraz założeniami przyjętymi przez Zamawiającego:
        - Czasy przechowywania (retencja)
        - Harmonogramy wykonywanych kopii zapasowych
        - Pule składowania danych
        - Zakresy danych chronionych
        - Grupy
    b) Integracja systemu kopiowania danych z obecnych środowiskiem maszyn wirtualnych VMware vSphere

c) Konfiguracja backupu obrazów maszyn wirtualnych, wskazanych przez Zamawiającego, zgodnie z przyjętą polityką bezpieczeństwa
   - Wykonanie kopii zapasowej
   - Wykonanie testów odtworzeniowych dla wskazanych przez Zamawiającego maszyn wirtualnych

d) Wdrożenie polityki backupowej dla wskazanych przez Zamawiającego maszyn Windows Serwer:
   - Instalacja agenta systemu kopiowania i odtwarzania danych
   - Implementacja polityki backupowej zgodnie z przyjętymi założeniami Zamawiającego
   - Wykonanie kopii zapasowej
   - Wykonanie testów odtworzeniowych dla:
     - pojedynczych plików (w miejsce oryginalne, we wskazany katalog, na inny serwer Windows),
     - pełnej maszyny (testy odtworzenia na wypadek awarii serwera),
     wskazanych przez Zamawiającego,

e) Wdrożenie polityki backupowej dla wskazanych przez Zamawiającego maszyn Linux:
   - Instalacja agenta systemu kopiowania i odtwarzania danych
   - Implementacja polityki backupowej zgodnie z przyjętymi założeniami Zamawiającego
   - Wykonanie kopii zapasowej
   - Wykonanie testów odtworzeniowych dla:
     - pojedynczych plików (w miejsce oryginalne, we wskazany katalog, na inny serwer Linux),
     - pełnej maszyny (testy odtworzenia na wypadek awarii serwera),
     wskazanych przez Zamawiającego,

f) Wdrożenie polityki backupowej dla wskazanych przez Zamawiającego aplikacji MS SQL w trybie online:
   - Instalacja agenta MS SQL systemu kopiowania i odtwarzania danych
   - Implementacja polityki backupowej zgodnie z przyjętymi założeniami Zamawiającego
   - Wykonanie kopii zapasowej
   - Wykonanie testów odtworzeniowych dla:
     - pojedynczych baz (w miejsce oryginalne, do innej bazy, na inny serwer MS SQL),
     wskazanych przez Zamawiającego,

g) Wdrożenie polityki backupowej dla wskazanych przez Zamawiającego aplikacji Oracle w trybie online:
   - Instalacja agenta Oracle systemu kopiowania i odtwarzania danych
   - Implementacja polityki backupowej zgodnie z przyjętymi założeniami Zamawiającego
   - Wykonanie kopii zapasowej
   - Wykonanie testów odtworzeniowych dla:
     - pojedynczych baz (w miejsce oryginalne, do innej bazy, na inny serwer Oracle),
     wskazanych przez Zamawiającego,

h) Wdrożenie polityki backupowej dla wskazanych przez Zamawiającego reprezentatywnych stacji roboczych Windows (komputer stacjonarny, komputer przenośny - wyposażone w system Windows 7, 10):
   - Instalacja agenta systemu kopiowania i odtwarzania danych

- Implementacja polityki backupowej
- Wykonanie kopii zapasowej
- Wykonanie testów odtworzeniowych dla:
  - pojedynczych plików (w miejsce oryginalne, we wskazany katalog, na inną maszynę Windows),
  - pełnej maszyny (testy odtworzenia na wypadek jej awarii), wskazanych przez Zamawiającego,

4. Instalacja i konfiguracja systemu raportującego, z uwzględnieniem raportów prezentujących
   a) Podsumowanie zadań backupowych (liczba backupów udanych, nieudanych, aktywnych, łączny rozmiar zbackupowanych danych)
   b) Podsumowanie zadań odtworzeniowych (liczba odtworzeń udanych, nieudanych, aktywnych, łączny rozmiar odtworzonych danych danych)
   c) Zbiorcze procentowe zestawienie udanych zadań backupowych z poszczególnych serwerów
   d) Zbiorcze zestawienie zabezpieczanych serwerów, które w sposób ciągły (kilka razy pod rząd) maja problem z backupami
   e) Zestawienie zabezpieczanych systemów plików, które w ogóle nie są backupowane
   f) Spodziewany czas odtwarzania zabezpieczanego serwera oraz potencjalnej utraty danych (czas między ostatnim backupem a chwilą awarii)
   g) Najmniej wiarygodne zabezpieczanych serwery (procent nieudanych backupów)
   h) Lista najwolniejszych/najszybszych zabezpieczanych maszyn
   i) Poziom SLA (procentowa liczba udanych backupów) w odniesieniu do poziomu założonego
      Mierzenie poziomu SLA dla poszczególnych zabezpieczanych serwerów przy uwzględnieniu założonego okna backupowego i RPO (punktu odtworzeniowego)
5. Przeprowadzenie co najmniej 2-dniowego instruktażu dla maksymalnie 4 osób z zakresu administracji wdrożonym środowiskiem przechowywania i wykonywania kopii zapasowych.

ZASTĘPCA DYREKTORA
Wydziału Informatyki i Telekomunikacji
Jarosław Buczek