**Zakup systemu do Archiwizacji Poczty oraz Centralnego Systemu Kopii Zapasowych wraz z appliance, pamięcią do przechowywania kopii długoterminowych oraz 3 letnim wsparciem producenta.**

Zamawiający wymaga licencji, które pokryją 2500 skrzynek pocztowych systemu IBM Lotus Domino i jednocześnie będą, bez dodatkowych kosztów, zapewniać archiwizację po zmianie systemu pocztowego na MS Exchange 2019.

Centralny System Kopii Zapasowych musi licencyjnie zabezpieczyć 100 TB danych Zamawiającego.

Wszystkie elementy systemów muszą pochodzić od jednego producenta z legalnego kanału sprzedaży na terenie Unii Europejskiej

System musi składać się z następujących elementów:

1. System archiwizacji poczty elektronicznej

|  |  |
| --- | --- |
| **Lp.** | **MINIMALNE WYMAGANIA ZAMAWIAJĄCEGO** |
| **1.** | System powinien być przeznaczony dla średnich i dużych firm, które mają rozbudowane środowiska informatyczne. Architektura oprogramowania systemu musi wspierać skalowanie wydajności poprzez dodawanie kolejnych serwerów (komponentów), które będą wykonywać zadania archiwizacyjne rozkładając obciążenie pomiędzy serwerami. |
| **2.** | System musi istnieć na rynku minimum 10 lat i musi być systemem o uznanej pozycji na rynku oraz musi znajdować się w kwadracie „Leaders” lub „Visionaries” raportu Gartnera pt. „Magic Quadrant for Enterprise Information Archiving – w okresie co najmniej trzy lata wstecz. |
| **3.** | System archiwizacji musi wspierać archiwizację ruchu pocztowego wchodzącego i wychodzącego do i z Microsoft Office 365 i umożliwiać lokalne składowanie danych z możliwością pełnego przeszukiwania i zarządzania retencją. |
| **4.** | System archiwizacji musi wspierać archiwizację wszystkich typów elementów, w tym elementów kalendarza dla następujących wersji systemów pocztowych Microsoft Exchange Server 2013 również z zainstalowanymi CU1-CU23, Microsoft Exchange Server 2016 również z zainstalowanymi CU1-CU20, Microsoft Exchange Server 2019 również z zainstalowanym CU9 jak również IBM Lotus Domino w wersjach 8-10. |
| **5.** | System musi umożliwiać zautomatyzowaną archiwizację danych z plików PST z możliwością automatycznego wykrywania i przydzielania właściciela archiwum. Funkcjonalność wykrywania właściciela powinna wspierać integrację z Active Directory. |
| **6.** | System archiwizacji musi mieć możliwość rozszerzenia funkcjonalności o archiwizację plików, danych z Microsoft SharePoint Server, przy czym zarządzanie systemem archiwizacji musi odbywać się w obrębie jednej konsoli. |
| **7.** | System archiwizacji musi mieć architekturę modułową. Oprogramowanie systemu archiwizacji musi wspierać instalację na odrębnych serwerach tworzących „farmę” systemu celem zwiększenia wydajności i przepustowości. |
| **8.** | Architektura systemu musi umożliwiać rozmieszczenie konfiguracji, metadanych, indeksów oraz archiwizowanych danych na dedykowanych zasobach pamięci masowych. Dla zarchiwizowanych danych musi istnieć możliwość składowania w chmurze lub pamięci obiektowej. |
| **9.** | System musi wspierać instalację bazy danych konfiguracji i metadanych na Microsoft SQL Server 2012 x64 edition (Enterprise i Standard), Microsoft SQL Server 2014 x64 edition (Enterprise i Standard), Microsoft SQL Server 2016 x64 edition (Enterprise i Standard), Microsoft SQL Server 2017 x64 edition (Enterprise i Standard) |
| **10.** | Oprogramowanie systemu musi wspierać instalację na następujących systemach operacyjnych: Windows Server 2012, Windows Server 2012 R2, Windows Server 2016, Windows Server 2019. |
| **11.** | Konsola administracyjna systemu musi wspierać jej uruchomienie na następujących systemach operacyjnych: Windows 8, Windows 8.1, Windows 10. |
| **12.** | System musi wspierać integrację z Active Directory na poziomie funkcjonalnym Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, Windows Server 2016. |
| **13.** | Uaktualnianie, upgrade, zmiana wersji – system musi zapewniać iż jakakolwiek zmiana wersji nie może powodować reorganizacji czy migracji danych w archiwach, archiwa musza być kompatybilne w górę to znaczy każda następna wersja oprogramowania musi obsługiwać archiwa utworzone z wcześniejszej wersji systemu. |
| **14.** | Możliwość archiwizowania tzw „social media” – zgodność z regulacją: FINRA 10-06 |
| **15.** | Musi istnieć mechanizm przełączania systemu w tryb backup tak by można było w sposób spójny wykonywać backup całego środowiska bez jego wyłączania z zachowaniem możliwości dostępu do zarchiwizowanych elementów (odczytywanie i odtwarzanie). |
| **16.** | System archiwizacji musi umożliwiać archiwizację ruchu pocztowego za pośrednictwem protokołu SMTP dla dowolnego typu aplikacji. Uruchomienie archiwizacji za pośrednictwem protokołu SMTP musi odbywać się wyłącznie w oparciu o oprogramowanie systemu archiwizacji bez konieczności instalacji usługi Windows SMTP. |
| **17.** | Archiwizacja SMTP musi wspierać przechwytywanie wszystkich metadanych, takich jak BCC, przynależność do listy dystrybucyjnej, informacje raportu dziennika (journal). |
| **18.** | Zarchiwizowane dane zebrane za pośrednictwem protokołu SMTP muszą być dostępne dla użytkownika w osobistym archiwum z podziałem na Skrzynkę Odbiorczą i Elementy Wysłane. |
| **19.** | System archiwizacji musi umożliwiać archiwizację ze skrzynek journaling-owych oprogramowania Microsoft Exchange i IBM Lotus Domino. |
| **20.** | System archiwizacji musi wspierać zarówno Standard Journaling jak i Envelope Journaling Microsoft Exchange. |
| **21.** | Archiwizacja maili ze skrzynek journaling-owych oprogramowania Microsoft Exchange powinna następować automatycznie, nie rzadziej niż co 5 min. Po archiwizacji wszystkie e-maile muszą być natychmiast kasowane, po to by nie dopuścić do przyrostu wielkości skrzynki journaling-owej. |
| **22.** | Przypisanie retencji (czas przechowywania) musi być możliwe co najmniej na poziomie skrzynki journalingowej, a więc wszystkie maile jakie znajdą się w takiej skrzynce będą zarchiwizowane z jednakową retencją. |
| **23.** | System musi oferować tak zwany selektywny journaling, a więc możliwość zdefiniowania reguł filtru tego co ma być archiwizowane. System musi oferować filtrowanie na podstawie: ciągu znaków adresu docelowego, nazwy listy dystrybucyjnej, nazwy domeny docelowej. |
| **24.** | Archiwizowanie musi odbywać się poprzez profil MS Outlook tak by nie było potrzeby instalowania oprogramowania na serwerach MS Exchange, chyba że będzie tego wymagał dostęp poprzez OWA. |
| **25.** | Musi umożliwiać definiowanie rożnych reguł, którym będą podlegać dane przeznaczone do archiwizacji, w szczególności dla MS Exchange musi być możliwość archiwizacji danych na podstawie kryteriów czasowych i w oparciu o procent wolnego miejsca w skrzynce (obie funkcje muszą być dostępne jednocześnie dla dowolnej skrzynki) dla tych funkcjonalności nie wymagane jest uruchamianie dodatkowych funkcjonalności na Exchange (np. journaling). |
| **26.** | Po zakończeniu archiwizacji w skrzynce użytkownika muszą pozostać znaczniki maili tak by dla użytkownika końcowego dostęp do danych w archiwum był taki sam jak do danych w Exchange. |
| **27.** | System musi potrafić uaktualniać znaczniki tak by w razie przeniesienia ich w inne miejsce odzyskiwanie maili obywało się bez ograniczeń. |
| **28.** | Musi integrować się z funkcjonalnością „managed folders” w Microsoft Exchange. |
| **29.** | Musi oferować możliwość migracji plików pst całkowicie automatycznie, także wtedy, gdy oprogramowanie MS Outlook jest wyłączone na stacjach użytkowników, po zakończeniu migracji musi być możliwość automatycznego blokowania dostępu, ukrywania czy kasowania przeniesionych plików pst. |
| **30.** | Musi mieć możliwość tworzenia lokalnej kopii archiwum, po to by użytkownicy mobilni mogli mieć dostęp od archiwum również gdy są nie podłączeni do sieci korporacyjnej. |
| **31.** | Konfiguracja i zarządzanie migracją plików pst musi być wykonywana z tej samej konsoli co zarządzanie systemem archiwizacji. |
| **32.** | Konfiguracja i zarządzanie migracją plików nsf musi być wykonywana z tej samej konsoli co zarządzanie systemem archiwizacji. |
| **33.** | Musi istnieć możliwość zdefiniowania zawartości znacznika, tak by użytkownik klienta pocztowego takiego jak Outlook Express mógł odczytać zawartość maila z archiwum, wraz z ewentualnymi załącznikami – mail jako strona WWW. |
| **34.** | System musi oferować (jako opcję) możliwość definiowania reguł na bazie treści czy nagłówków wiadomości pocztowych z MS Exchange tak by można było przypisywać różne wartości dot. przechowywania tych wiadomości w archiwum, a więc różne poziomy retencji danych przechowywanych w systemie bazujące między innymi na treści czy słowach kluczowych w mailach. |
| **35.** | Rozwiązanie powinno zapewniać automatyczne kasowanie danych na podstawie czasu przetrzymywania danych tzw. retention, z tym że zdefiniowanie wielu poziomów retention nie powinno powodować zmniejszenia współczynnika deduplikacji danych w archiwum. |
| **36.** | Funkcjonalność deduplikacji danych musi obejmować różne typy danych tzn. plik dołączony do zarchiwizowanego maila powinien być raz zachowany w archiwum nawet wtedy gdy byłby zarchiwizowany bezpośrednio z systemów plików czy z SharePoint’a – funkcjonalność ta musi być dostępna dla dowolnych dysków i producentów sprzętu, musi być cechą oprogramowania, a nie specyficznego sprzętu i być w cenie produktu. |
| **37.** | System powinien mieć możliwość (opcja) archiwizować dane także na taśmy, jako następny etap (poziom) składowania danych. |
| **38.** | Rozwiązanie powinno posiadać jedną centralną konsolę, która umożliwia administrowanie wszystkimi funkcjami także tymi dotyczącymi migracji plików pst, czy zarządzaniem archiwizacją zasobów plikowych czy SharePoint. |
| **39.** | Musi istnieć możliwość zarządzania archiwum poprzez przeglądarkę Internet Explorer. |
| **40.** | Musi posiadać możliwość delegowania uprawnień pomiędzy osoby (administratorów) danych komponentów np. zarządzanie storage. |
| **41.** | System archiwizacji musi tworzyć indeksy do zarchiwizowanych danych tak by można było przeszukiwać archiwa pełnokontekstowo po treści wiadomości również po treści załączników. |
| **42.** | System archiwizacji musi posiadać możliwość włączenia lub wyłączenia pełnokontekstowego indeksowania treści dla poszczególnych skarbców archiwum. |
| **43.** | Indeksy muszą być przetrzymywane tak długo jak dane w archiwach. |
| **44.** | Oprogramowanie musi rozpoznawać i indeksować treść z większości popularnych i spotykanych w świecie formatów dokumentów (np. MS Office, Open Office, PDF, JPG, CAD…), ilość rozpoznawanych typów dokumentów to minimum 300 |
| **45.** | Reindeksowanie danych nie może blokować dostępu do archiwum dla użytkowników. |
| **46.** | Funkcjonalność archiwizowania maili z dziennika (journaling) z MS Exchange musi umożliwiać przeszukiwanie danych włącznie z polami BCC. |
| **47.** | Musi posiadać jako opcję integracje z Windows Rights Management i PGP, a więc odszyfrowywanie wiadomości pocztowych celem ich indeksacji dla celów e-Discovery. |
| **48.** | Musi posiadać jako opcję komponenty umożliwiające automatyczne przeszukiwanie danych na podstawie słów kluczowych, słowników, blokowanie maili przed skasowaniem, jeśli treść wskazuje na złamanie reguł lub regulacji. |
| **49.** | Musi posiadać oddzielną aplikację dla wykonywania zaawansowanych przeszukiwań archiwów związanych z wymaganiami działów audytu czy bezpieczeństwa, aplikacja taka musi mieć własny system autoryzacji i przydzielania uprawnień do archiwów. Aplikacja taka musi oferować zaawansowane możliwości definiowania zadań przeszukiwania danych i posiadać możliwości automatycznego cyklicznego ich uruchamiania. |
| **50.** | Aplikacja obsługująca zaawansowane przeszukiwania archiwów musi potrafić wykrywać zduplikowane wiadomości tak by w raportach czy przy eksportowaniu nie powielać powtarzających się maili. |
| **51.** | Aplikacja do przeszukiwania musi posiadać mechanizm exportu danych do formatu HTML, tak aby można było je przeglądać w przeglądarce internetowej. |
| **52.** | Musi umożliwiać audytowanie wszelkich działań w systemie archiwizacyjnym w szczególności związanych ze zmianą parametrów czy kasowaniem danych z archiwum. |
| **53.** | Musi umożliwiać audytowanie operacji Wyszukiwania i Wyświetlania danych z archiwum. |
| **54.** | Wpis audytu musi zawierać następujące informacje: Data i godzina wystąpienia, nazwa użytego konta, nazwa użytego skarbca archiwum. |
| **55.** | System archiwizacji musi udostępniać możliwość wygenerowania raportu audyt. |
| **56.** | System archiwizacji musi zapewniać szczegółowe raporty dotyczące aktywności archiwizacyjnych dla Microsoft Exchange. Posiadać gotowe do użycia raporty dotyczące kondycji, trendów wykorzystania, pojemności i stanu systemu archiwizacji. |
| **57.** | System archiwizacji musi umożliwiać generowanie niestandardowych raportów. |
| **58.** | System musi umożliwiać eksportowanie raportów do formatu PDF, HTML, XLS/XLSX, CSV, XML. |
| **59.** | System archiwizacji musi posiadać dedykowany moduł dla integracji z systemem Microsoft SCOM, umożliwiający administratorom centralne śledzenie zdarzeń i aktywności. |
| **60.** | Musi posiadać możliwość dostępu do archiwum z urządzeń mobilnych, w zakresie wyszukiwania, przeglądania treści oraz pobierania danych z archiwum. |
| **61.** | Musi posiadać możliwość dostępu do archiwum poprzez klienta Outlook w taki sposób że jest ono widoczne (archiwum) jako struktura folderów w Outlook’u, dzięki czemu użytkownicy mają bezpośredni dostęp do zarchiwizowanych maili bez potrzeby używania skrótów czy uruchamiania komponentów celem operowania na archiwum, funkcjonalność musi być dostępna także wtenczas gdy Outlook pracuje w trybie offline. |
| **62.** | Musi posiadać polski interfejs (plug-in) do Outlooka, dla końcowego użytkownika. |
| **63.** | System archiwizacji musi posiadać dokumentację użytkownika końcowego archiwum w języku polskim. |

1. System kopii zapasowych

|  |  |
| --- | --- |
| **Lp.** | **MINIMALNE WYMAGANIA ZAMAWIAJĄCEGO** |
| **1.** | Oprogramowanie systemu powinno być przeznaczone dla średnich i dużych firm, posiadających rozbudowane środowisko informatyczne. |
| **2.** | W celu zapewnienia dużej elastyczności i skalowalności środowiska kopii zapasowych oprogramowanie systemu powinno posiadać trójwarstwową architekturę: Serwer Zarządzający, Serwer Mediów, Klient. |
| **3.** | Oprogramowanie systemu powinno umożliwiać wykonywanie kopii zapasowych w środowisku heterogenicznym za pomocą, dedykowanego dla platformy systemowej, klienta systemu kopii zapasowych. |
| **4.** | System powinien umożliwiać łatwą rozbudowę w miarę rozrastania się infrastruktury informatycznej Zamawiającego, poprzez dokładanie kolejnych centralnie zarządzanych Serwerów Mediów. |
| **5.** | Proponowane rozwiązanie musi umożliwiać uruchomienie serwera zarządzającego kopiami zapasowymi na głównych platformach Windows, Linux i Unix. |
| **6.** | Proponowane rozwiązanie musi wspierać wysoką dostępność (klastrowanie) serwera kontrolującego kopie zapasowe |
| **7.** | Oprogramowanie musi być niezależne pod względem sprzętowym i nie może preferować instalacji na platformie sprzętowej jednego producenta. Powinno udostępniać te same funkcjonalności niezależnie od tego na jakiej platformie systemowej będzie zainstalowane. Zamawiający musi posiadać możliwość zmiany platformy sprzętowej bez utraty funkcjonalności systemu kopii zapasowej. |
| **8.** | Proponowane rozwiązanie musi wspierać wdrożenia na sprzęcie fizycznym, infrastrukturze wirtualnej oraz w chmurze. |
| **9.** | Proponowane rozwiązanie musi umożliwiać administrację za pomocą GUI (aplikacja lub web), CLI oraz RESTful API |
| **10.** | System powinien posiadać centralną konsolę zarządzania środowiskiem kopii zapasowych. Konsola musi umożliwiać:   * monitorowanie i zarządzanie wszystkimi zadaniami wykonywania i odtwarzania kopii zapasowych, tworzenia duplikatów wykonanych kopii zapasowych, * ustawianie harmonogramów wykonywania kopii zapasowych, * monitorowanie i kontrolowanie urządzeń składowania kopii zapasowych podłączonych do Serwerów Mediów, * centralne zarządzanie konfiguracją, właściwych dla oprogramowania systemu, ustawień Serwera Zarządzającego, Serwera Mediów, Klientów, * uruchomienie odtwarzania kopii zapasowych na kliencie, |
| **11.** | Oprogramowanie systemu musi posiadać obsługę z poziomu wiersza poleceń w systemach Linux, Unix i Windows. Obsługa z poziomu wiersza poleceń musi umożliwiać:   * konfigurację i modyfikację polityk wykonywania kopii zapasowych, * konfigurację i modyfikację harmonogramów wykonywania kopii zapasowych, * konfigurację i modyfikację urządzeń składowania kopii zapasowych podłączonych do Serwerów Mediów, * konfigurację i modyfikację nośników taśmowych, * monitorowanie i kontrolowanie zadań kopii zapasowych, * konfigurację i modyfikację nośników taśmowych * konfigurację i modyfikację właściwych dla oprogramowania systemu, ustawień Serwera Zarządzającego, Serwera Mediów, Klientów, * konfigurację, modyfikację i przeglądanie dzienników Serwera Zarządzającego, Serwera Mediów, Klientów, |
| **12.** | Rozwiązanie powinno być dostępne także jako zintegrowane programowo i sprzętowo urządzenie (appliance), a więc sprzęt i oprogramowanie backupowe razem. Zintegrowane urządzenia powinny umożliwiać zbudowanie w pełni funkcjonującej trzywarstwowej architektury backupowej z funkcjonalnością deduplikacji danych. |
| **13.** | Baza katalogowa dla systemu backupowego musi być częścią systemu backupowego i wspierać platformy minimum Linux, Windows oraz Unix oraz nie powinna posiadać ograniczeń wynikających z ilości używanych w serwerze procesorów i rdzeni procesorów. |
| **14.** | Baza katalogowa musi być w cenie systemu kopii zapasowych i nie ograniczona co do ilości środowisk backupowych, mocy czy ilości serwerów czy to backupowych czy produkcyjnych. Jakakolwiek rozbudowa środowiska backupowego czy dodanie następnego nie może powodować konieczności dokupienia licencji dla tej bazy. |
| **15.** | Oprogramowanie systemu kopii zapasowych musi posiadać zintegrowane zarządzanie kluczami szyfrującymi oraz musi posiadać możliwość integracji z zewnętrznymi usługami zarządzania kluczami szyfrowania. |
| **16.** | Oprogramowanie systemu kopii zapasowych musi integrować się z urządzeniami dyskowymi (deduplikatory) wspierającymi mechanizm WORM w celu ochrony danych przed zaszyfrowaniem, modyfikacją i usunięciem. Funkcjonalność musi zapewniać, że obraz kopii zapasowej jest tylko do odczytu i nie może być modyfikowany, uszkodzony lub zaszyfrowany po utworzeniu kopii zapasowej oraz chronić obraz kopii zapasowej przed usunięciem przed upływem terminu ważności. |
| **17.** | Obsługa funkcjonalności WORM powinna być realizowana natywnie przez oprogramowanie kopii zapasowych, gdzie zarządzanie czasem ochrony przechowywanych na urządzeniu obrazów kopii zapasowych odbywa się z poziomu oprogramowania systemu backupu, a nie rozdzielnie |
| **18.** | Proponowane rozwiązanie musi wspierać ochronę klientów pracujących pod kontrolą:   * Canonical Ubuntu w wersji 16 i nowszej * CentOS 6.8 i nowsze * Debian 7 - 10 * IBM AIX 6.1 - 7.2 na architekturze IBM Power * Windows 7 - 10 * Windows Server 2008 - 2019, w tym wydania półroczne * Oracle Linux 6.8 i nowsze * Oracle Solaris 10 Update 11 i nowsze na architekturach Sparc i x64 * Red Hat Enterprise Linux 6.8 i nowsze dla architektury x64 * Red Hat Enterprise Linux 7.2 i nowsze dla architektury x64 * Red Hat Enterprise Linux 7.2 i nowsze dla architektury IBM Power * Red Hat Enterprise Linux 6.8 i 7.x na IBM System Z * SUSE Enterprise Server 12 SP2 i nowsze na architekturach x64, IBM Power i IBM System Z |
| **19.** | Proponowane rozwiązanie musi wspierać architekturę składowania kopii zapasowych D2D2T i D2D2C. |
| **20.** | Proponowane rozwiązanie musi obsługiwać dowolny typ pamięci dyskowej (DAS, NAS, SAN) dla repozytorium backupu. |
| **21.** | Proponowane rozwiązanie musi wspierać storage taśmowy (samodzielne napędy taśmowe oraz biblioteki taśmowe w tym m.in. biblioteki robotów sterowane ACS) głównych producentów. |
| **22.** | Proponowane rozwiązanie musi deduplikować dane na źródle i celu. |
| **23.** | Deduplikacja musi umożliwiać wybór pomiędzy zmiennym i stałym rozmiarem bloku. Rozmiar bloku musi umożliwiać jego wybór. |
| **24.** | Proponowane rozwiązanie musi wspierać deduplikację zarówno inline jak i postprocesową. |
| **25.** | Proponowane rozwiązanie musi wspierać urządzenia deduplikacyjne głównych producentów takich jak Dell EMC, Exagrid, HPE, Quantum, NEC |
| **26.** | Proponowane rozwiązanie musi obsługiwać wirtualne biblioteki taśmowe (VTL) |
| **27.** | Proponowane rozwiązanie musi wspierać transfer danych zarówno przez sieć LAN jak i SAN. |
| **28.** | Proponowane rozwiązanie musi wspierać głównych dostawców chmur publicznych jako magazyn kopii zapasowych. |
| **29.** | Proponowane rozwiązanie musi obsługiwać deduplikację do chmury w celu minimalizacji transferu danych. |
| **30.** | Proponowane rozwiązanie musi umożliwiać wznowienie nieudanego zadania backupowego od ostatniego punktu kontrolnego. |
| **31.** | Proponowane rozwiązanie musi automatyzować tworzenie wielu kopii zapasowych na różnych urządzeniach magazynowych z różną długością przechowywania danych. |
| **32.** | Proponowane rozwiązanie powinno posiadać możliwość wykonywania wysokowydajnych kopii zapasowych serwerów z bardzo obciążonymi systemami plików na dyskach z dużą liczbą plików (np. backup typu disk-image) |
| **33.** | Proponowane rozwiązanie musi zapewniać możliwość wykonywania backupu syntetycznego. |
| **34.** | Proponowane rozwiązanie musi umożliwiać tworzenie ręcznych kopii zapasowych ad-hoc. |
| **35.** | Proponowane rozwiązanie musi wspierać topologie replikacji danych typu jeden-do-jednego, wiele-do-jednego, jeden-do-wielu oraz kaskadową z wykorzystaniem deduplikacji danych w celu zminimalizowania ilości przesyłanych danych. |
| **36.** | Proponowane rozwiązanie musi wspierać szyfrowanie danych. |
| **37.** | Proponowane rozwiązanie musi umożliwiać wznowienie nieudanego zadania przywracania z ostatniego punktu kontrolnego. |
| **38.** | Proponowane rozwiązanie musi zapewniać funkcje umożliwiające natywne odzyskiwanie "bare metal" (w pełni zautomatyzowane odzyskiwanie obejmujące system operacyjny, konfigurację, aplikacje i dane) klientów Windows, Linux, Solaris, AIX i HPUX bez konieczności korzystania z zewnętrznych/rodzimych narzędzi do odzyskiwania/reimaging systemu operacyjnego. |
| **39.** | Proponowane rozwiązanie musi umożliwiać przywracanie różnych konfiguracji systemu oraz różnych układów dysków. |
| **40.** | Proponowane rozwiązanie musi zapewniać możliwość konwersji P2V i V2P |
| **41.** | Proponowane rozwiązanie musi umożliwiać przywracanie nawet po wygaśnięciu wsparcia technicznego oprogramowania. |
| **42.** | Proponowane rozwiązanie musi umożliwiać przywracanie pojedynczych obiektów Active Directory z kopii zapasowej Windows System State |
| **43.** | Rozwiązanie musi wspierać VMware:   * Proponowane rozwiązanie musi wspierać VMware vSphere 6.0 i nowsze * Proponowane rozwiązanie musi wspierać serwery vSphere zarządzane przez vCenter jak i samodzielne serwery ESXi * Proponowane rozwiązanie musi wspierać VMware vSAN 6.5 i nowsze * Proponowane rozwiązanie musi wspierać VMware vCloud Director 9.x * Proponowane rozwiązanie musi wspierać wszystkie tryby transportu danych obsługiwane przez VDDK 6.7.2 (SAN, NBD, NBDSSL, hot-add) * Proponowane rozwiązanie nie może wymagać instalacji agentów w maszynach wirtualnych w celu wykonywania kopii zapasowych * Proponowane rozwiązanie musi wspierać śledzenie zmian (CBT - change block tracking) * Proponowane rozwiązanie musi wspierać tworzenie syntetycznych kopii zapasowych (tworzonych na podstawie ostatniego pełnego backupu oraz backupu przyrostowego CBT) maszyn wirtualnych VMware w celu umożliwienia wykonywania backupów przyrostowych (incremental-forever) * Proponowane rozwiązanie musi zawierać mechanizm automatycznego wykrywania i ochrony maszyn wirtualnych VMware bez konieczności zmiany polityk backupu * Proponowane rozwiązanie musi umożliwiać wyłączenie z backupu maszyn wirtualnych, usuniętych bloków oraz pliku swap * Proponowane rozwiązanie musi wspierać przywracanie pojedynczego pliku z kopii zapasowej maszyny wirtualnej VMware bez konieczności uruchamiania agenta w maszynie wirtualnej oraz umieszczania wirtualnego dysku wirtualnego dysku w tymczasowej lokalizacji, jeżeli obraz kopii zapasowej jest przechowywany na taśmach * Proponowane rozwiązanie musi wspierać jednoprzebiegowy backup Microsoft Exchange, Microsoft SQL Server oraz Microsoft SharePoint z możliwością przywracania elementów granularnych zgodnie z opisem w dalszej części. * Proponowane rozwiązanie nie może wymagać wykonywania osobnego backupu na poziomie aplikacji lub wysyłki logów w przypadku backupu Microsoft Exchange, Microsoft SQL Server i Microsoft SharePoint * Proponowane rozwiązanie musi wspierać limitowanie zasobów takich jak liczba jednoczesnych zadań backupu na serwer ESXi, klaster lub magazyn danych * Proponowane rozwiązanie musi umożliwiać uruchomienie maszyny wirtualnej bezpośrednio z dyskowego repozytorium kopii zapasowych * Proponowane rozwiązanie musi zapewniać natychmiastowy dostęp do chronionych maszyn wirtualnych i ich plików * Proponowane rozwiązanie musi zapewniać dodatkowe możliwości administracji, monitorowania i odzyskiwania danych poprzez VMware vCenter Web Client |
| **44.** | Rozwiązanie musi wspierać Microsoft Hyper-V:   * Proponowane rozwiązanie musi wspierać Microsoft Hyper-V 2008 SP2 i nowsze * Proponowane rozwiązanie musi wykorzystywać Windows Management Instrumentation (WMI) dla ochrony maszyn wirtualnych działających na platformie Hyper-V 2016 i nowszych * Proponowane rozwiązanie musi wspierać ochronę maszyn wirtualnych rezydujących na systemach plików NTFS, ReFS, Windows Storage Spaces, Storage Spaces Direct oraz SMB 3.0 * Proponowane rozwiązanie musi wspierać Resilient Change Tracking (RCT) * Proponowane rozwiązanie musi wspierać tworzenie syntetycznych kopii zapasowych (tworzonych na podstawie ostatniego pełnego i przyrostowego backupu RCT) maszyn wirtualnych Hyper-V w celu umożliwienia tworzenia kopii zapasowych przyrostowych na zawsze * Proponowane rozwiązanie musi wspierać ograniczenie liczby aktywnych snapshotów lub backupów na serwer Hyper-V i klaster * Proponowane rozwiązanie musi zawierać mechanizm automatycznego wykrywania i ochrony maszyn wirtualnych Hyper-V VM bez konieczności zmiany polityk backupu. * Proponowane rozwiązanie musi umożliwiać wykluczenie usuniętych bloków i plików swap z kopii zapasowej maszyny wirtualnej Hyper-V * Proponowane rozwiązanie musi wspierać wyłączenie dysków startowych z backupu maszyn wirtualnych Hyper-V z kopii zapasowych maszyn wirtualnych Hyper-V * Proponowane rozwiązanie musi wspierać wyłączenie dysków danych z backupu maszyn wirtualnych Hyper-V kopii zapasowej maszyny wirtualnej * Proponowane rozwiązanie musi wspierać przywracanie pojedynczego pliku z kopii zapasowej maszyny wirtualnej Hyper-V bez konieczności przenoszenia dysku wirtualnego w lokalizacji tymczasowej, jeżeli obraz kopii zapasowej jest przechowywany na taśmach * Proponowane rozwiązanie musi zapewniać integrację z System Center Virtual Machine Manager (SCVMM) w celu umożliwienia odzyskiwania maszyn wirtualnych |
| **45.** | Rozwiązanie musi wspierać Nutanix:   * Proponowane rozwiązanie musi wspierać Nutanix Acropolis Hypervisor 5.10 i 5.11 * Proponowane rozwiązanie musi wspierać co najmniej crash consistent backup maszyn wirtualnych maszyn wirtualnych Nutanix Acropolis |
| **46.** | Rozwiązanie musi wspierać RHV:   * Proponowane rozwiązanie musi wspierać Red Hat Virtualization 4.2.7 - 4.4.x * Proponowane rozwiązanie musi wspierać spójne z aplikacjami kopie zapasowe (application consistent backups) |
| **47.** | Rozwiązanie musi wspierać Azure Stack:   * Proponowane rozwiązanie musi umożliwiać ochronę maszyn wirtualnych Azure Stack maszyn wirtualnych Azure Stack * Proponowane rozwiązanie musi wspierać co najmniej crash consistent backup maszyn wirtualnych maszyn wirtualnych Azure Stack |
| **48.** | Rozwiązanie musi wspierać OpenStack:   * Proponowane rozwiązanie musi wspierać minimum następujące wersje: OpenStack * Mitaka * Newton * Ocata * Pike * Queens * Train * Rocky * Stein * Proponowane rozwiązanie musi wspierać hypervisor KVM z OpenStack * Proponowane rozwiązanie musi wspierać następujące dystrybucje OpenStack: * Red Hat OpenStack Platform * Huawei FusionSphere |
| **49.** | Rozwiązanie musi wspierać Docker:   * Proponowane rozwiązanie musi umożliwiać ochronę kontenerów Docker * Proponowane rozwiązanie musi umożliwiać ochronę skonteneryzowanych aplikacji, danych aplikacji skonteneryzowanych przechowywanych na persystentnych wolumenach * Proponowane rozwiązanie musi umożliwiać ochronę skonteneryzowanych danych aplikacji, danych skonteneryzowanych aplikacji z wykorzystaniem obszaru stagingowego z wykorzystaniem podejścia dump and sweep * Proponowane rozwiązanie musi umożliwiać ochronę skonteneryzowanych aplikacji poprzez współlokalizację na kontenerze aplikacyjnym |
| **50.** | Rozwiązanie musi wspierać Apache Hadoop:   * Proponowane rozwiązanie musi wspierać Apache Hadoop 2.5.2 - 3.1 działający na systemach Red Hat Enterprise Linux 6 i 7 oraz SUSE Linux Enterprise Server 11 i 12 * Proponowane rozwiązanie nie może wymagać instalacji agentów na klastrze Hadoop (musi być bezagentowe) * Proponowane rozwiązanie musi przesyłać dane bezpośrednio z wielu węzłów równolegle |
| **51.** | Rozwiązanie musi wspierać Apache HBase:   * Proponowane rozwiązanie musi wspierać Apache HBase 1.2 - 2.0 działający na systemach Red Hat Enterprise Linux 6 i 7 oraz SUSE Linux Enterprise Server 11 i 12 * Proponowane rozwiązanie nie może wymagać instalacji agentów na klastrze HBase na klastrze HBase (musi być bezagentowe) * Proponowane rozwiązanie musi przesyłać dane bezpośrednio z wielu Region serwerów * równolegle |
| **52.** | Rozwiązanie musi wspierać IBM DB2:   * Proponowane rozwiązanie musi wspierać IBM DB2 Universal Database 10.5 i nowsze działające na systemach IBM AIX, HP-UX, Oracle Solaris, Red Hat Enterprise Linux, SUSE Linux Enterprise Server oraz Windows * Proponowane rozwiązanie musi wspierać operacje równoległego backupu i przywracania baz danych DB2 * Proponowane rozwiązanie musi wspierać operacje multipleksowanego backupu i przywracania baz danych DB2 * Proponowane rozwiązanie musi wspierać tworzenie kopii zapasowych typu snapshot oraz natychmiastowe przywracanie baz danych DB2 * Proponowane rozwiązanie musi wspierać wykonywanie kopii zapasowych baz danych DB2 spoza serwera (off-host) |
| **53.** | Rozwiązanie musi wspierać IBM Informix:   * Proponowane rozwiązanie musi wspierać IBM Informix XPS i IDS * Proponowane rozwiązanie musi obsługiwać równoległe operacje backupu i przywracania baz danych Informix * Proponowane rozwiązanie musi obsługiwać multipleksowe backupy i restore baz danych Informix * Proponowane rozwiązanie musi obsługiwać kopie zapasowe poziomu 0, 1 i 2 * Proponowane rozwiązanie musi wspierać tworzenie kopii zapasowych logów logicznych |
| **54.** | Rozwiązanie musi wspierać IBM Lotus Domino:   * Proponowane rozwiązanie musi obsługiwać zarówno kopie zapasowe inicjowane przez politykę, jak i przez użytkownika * Proponowane rozwiązanie musi wspierać IBM Lotus Domino 8 - 10 działające na systemach IBM AIX, Red Hat Enterprise Linux, SUSE Linux Enterprise Server oraz Windows * Proponowane rozwiązanie musi zapewniać wykonywanie kopii zapasowych online baz danych Lotus Notes baz danych, skrzynek pocztowych oraz dzienników transakcji * Proponowane rozwiązanie musi umożliwiać ochronę baz danych z partycjonowanych serwerów Domino * Proponowane rozwiązanie musi umożliwiać wznawianie nieudanego zadania backupu Domino od ostatniego punktu kontrolnego |
| **55.** | Rozwiązanie musi wspierać MariaDB:   * Proponowane rozwiązanie musi zapewniać ochronę baz danych MariaDB 5.5 i nowszych działających na systemach Red Hat Enterprise Linux, SUSE Linux Enterprise Server oraz Windows * Proponowane rozwiązanie musi wspierać przywracanie kopii zapasowych MariaDB do klientów oryginalnych i alternatywnych |
| **56.** | Rozwiązanie musi wspierać Microsoft Exchange:   * Proponowane rozwiązanie musi wspierać Microsoft Exchange 2010 i późniejsze * Proponowane rozwiązanie musi obsługiwać wszystkie metody backupu serwera Exchange: full, cumulative incremental oraz differential incremental * Proponowane rozwiązanie musi wykonywać kopie zapasowe online Exchange bez konieczności wyłączania serwera Exchange * Proponowane rozwiązanie musi obsługiwać zarówno serwery autonomiczne jak i Database Availability Groups * Proponowane rozwiązanie musi umożliwiać wykonywanie kopii zapasowych Exchange spoza serwera (off-host), Instant Recovery oraz wykonywanie kopii zapasowych z wykorzystaniem sprzętowych kopii migawkowych. * Zaproponowane rozwiązanie musi umożliwiać wykonywanie restartów do innej bazy danych Exchange lub na innym serwerze Exchange * Proponowane rozwiązanie musi pozwalać na wykonywanie przekierowanych restartów do alternatywnych skrzynek Exchange, folderów skrzynek, wiadomości skrzynek, folderów publicznych folderów publicznych * Proponowane rozwiązanie musi umożliwiać przywracanie poszczególnych elementów skrzynek i folderów publicznych bezpośrednio z dowolnej pełnej kopii zapasowej bazy Exchange |
| **57.** | Rozwiązanie musi wspierać Microsoft SharePoint:   * Proponowane rozwiązanie musi wspierać Microsoft SharePoint 2010 i nowsze * Proponowane rozwiązanie musi wspierać ochronę SharePoint Configuration database, SSO database, Global settings, Index files, Service applications, Web applications or Content databases, Site collections, Subsites, Poszczególnych list lub bibliotek oraz Poszczególnych dokumentów lub elementów list. * Proponowane rozwiązanie musi wykonywać kopie zapasowe SharePoint online bez konieczności wyłączania serwera SharePoint w trybie offline * Proponowane rozwiązanie musi umożliwiać przywracanie z przekierowaniem * Proponowane rozwiązanie musi umożliwiać przywracanie pojedynczych list SharePointa, elementów i zestawów dokumentów bezpośrednio z dowolnej pełnej kopii zapasowej bazy danych aplikacji webowej. * Proponowane rozwiązanie musi wspierać Claims-based authentication (CBA) dla aplikacji webowych w SharePoint |
| **58.** | Rozwiązanie musi wspierać MS SQL Server:   * Proponowane rozwiązanie musi wspierać Microsoft SQL Server 2008 i nowsze * Proponowane rozwiązanie musi wspierać SQL Server Availability Groups * Proponowane rozwiązanie musi wspierać automatyczne wykrywanie instancji SQL * Proponowane rozwiązanie nie powinno wymagać skryptów wsadowych tworzonych przez użytkownika, które posiadały instrukcje tworzenia kopii zapasowych instancji baz danych SQL oraz logów transakcyjnych * Proponowane rozwiązanie musi zapewniać wykonywanie pełnych, różnicowych i dzienników transakcji kopii zapasowych baz danych SQL * Proponowane rozwiązanie nie może wykorzystywać metody log-shipping do ochrony logów transakcyjnych SQL * Proponowane rozwiązanie musi wspierać pełne przywracanie i odzyskiwanie baz danych SQL * Proponowane rozwiązanie musi wspierać przywracanie grup plików SQL * Proponowane rozwiązanie musi wspierać przywracanie plików bazy danych SQL * Proponowane rozwiązanie musi wspierać przywracanie logów transakcyjnych SQL do określonego punktu w czasie * Proponowane rozwiązanie musi wspierać przywracanie logu transakcyjnego SQL do określonego punktu w czasie konkretnej transakcji |
| **59.** | Rozwiązanie musi wspierać MySQL:   * Proponowane rozwiązanie musi zapewniać ochronę baz danych MySQL 5.5.5 i nowszych baz danych działających na systemach Red Hat Enterprise Linux, SUSE Linux Enterprise Server oraz Windows * Proponowane rozwiązanie musi wspierać przywracanie kopii zapasowych MySQL do klientów oryginalnych i alternatywnych |
| **60.** | Rozwiązanie musi wspierać Oracle:   * Proponowane rozwiązanie musi wspierać bazy danych Oracle 11g R1 i nowsze działające na platformach IBM AIX, HP-UX, Oracle Linux, Oracle Solaris, Red Hat Enterprise Linux, SUSE Linux Enteprise Server oraz Windows * Proponowane rozwiązanie musi integrować się z funkcjami backupu i odtwarzania baz danych Oracle Recovery Manager (RMAN) * Proponowane rozwiązanie musi obsługiwać kopie zapasowe standardowych i kontenerowych baz danych Oracle * Proponowane rozwiązanie musi wspierać Oracle Real Application Clusters (RAC) * Proponowane rozwiązanie musi posiadać możliwość dynamicznego generowania skryptów do backupu znanych instancji Oracle * Proponowane rozwiązanie musi umożliwiać wykonanie skryptu stworzonego wcześniej przez administratora do wywołania RMAN w celu wykonania kopii zapasowej bazy danych * Proponowane rozwiązanie musi automatycznie generować skrypty RMAN do backupu całej bazy danych Oracle, poszczególnych przestrzeni tabel, plików danych oraz Fast Recovery Area (FRA) * Proponowane rozwiązanie musi umożliwiać konfigurację różnej ilości strumieni podczas wykonywania kopii zapasowych przestrzeni tabel lub plików danych Oracle oraz archiwalnych logów redo. * Proponowane rozwiązanie musi umożliwiać dostosowanie formatów nazw plików backupu używanych przez generowane skrypty Oracle RMAN * Proponowane rozwiązanie musi wspierać możliwości równoległego backupu i przywracania RMAN * Proponowane rozwiązanie musi umożliwiać odtworzenie bazy danych Oracle za pomocą RMAN: * Pełne kopie zapasowe, przyrostowe kopie zapasowe poziomu 0 lub kopie plików danych * Kopia zapasowa całej bazy danych (jeśli jest wymagana) * Dowolną część bazy danych (pliki danych, przestrzenie tabel) * Proponowane rozwiązanie musi dostarczać metodę klonowania baz danych Oracle ułatwiającą: * Przekierowanie plików danych * Przekierowanie plików kontrolnych * Przekierowanie logów redo * Zapewnienie walidacji operacji * Proponowane rozwiązanie musi wspierać zapisywanie kopii zapasowych Oracle do i przywracanie ich z samoidentyfikującego się i niezależnego od systemu formatu np. XML |
| **61.** | Rozwiązanie musi wspierać PostgreSQL:   * Proponowane rozwiązanie musi zapewniać ochronę baz danych PostgreSQL 9 i nowszych działających na systemach Red Hat Enterprise Linux, SUSE Linux Enterprise Server oraz Windows * Proponowane rozwiązanie musi umożliwiać przywracanie kopii zapasowych PostgreSQL do klientów oryginalnych oraz alternatywnych |
| **62.** | Rozwiązanie musi wspierać SAP:   * Proponowane rozwiązanie musi wspierać SAP R/3 z Oracle, SAPDB i MaxDB, oraz SAP HANA (w tym SAP HANA 2.0) * Proponowane rozwiązanie musi uruchamiać wszystkie kopie zapasowe SAP oraz przywracać je jednocześnie i w sposób transparentny bez konieczności podejmowania jakichkolwiek działań przez administratora rozwiązania * Proponowane rozwiązanie musi wspierać równoległe tworzenie kopii zapasowych i przywracanie możliwości SAP Tools * Proponowane rozwiązanie musi integrować się z interfejsem Backint dla SAP i SAP HANA * Proponowane rozwiązanie musi umożliwiać ręczne inicjowanie operacji przez administratora SAP HANA za pomocą SAP HANA Studio |
| **63.** | Rozwiązanie musi wspierać SQLite:   * Proponowane rozwiązanie musi zapewniać ochronę baz danych SQLite 3.10 i nowszych działających na systemach Red Hat Enterprise Linux, SUSE Linux Enterprise Server oraz Windows * Proponowane rozwiązanie musi wspierać przywracanie kopii zapasowych SQLite do klientów oryginalnych i alternatywnych |
| **64.** | Rozwiązanie musi wspierać NDMP:   * Proponowane rozwiązanie musi wspierać wykorzystanie protokołu NDMP (Network Data Management Protocol) do inicjowania i sterowania kopiami zapasowymi i przywracaniem systemów NAS (Network Attached Storage) * Proponowane rozwiązanie musi obsługiwać NDMP v2, v3 i v4 * Proponowane rozwiązanie musi wykorzystywać techniki wykrywania zmian w filerze w celu identyfikacji modyfikacji, które nastąpiły od momentu wykonania ostatniego backupu * Proponowane rozwiązanie musi obsługiwać lokalne i trójstronne kopie zapasowe NDMP * Proponowane rozwiązanie musi obsługiwać funkcję NDMP DirectCopy * Proponowane rozwiązanie musi umożliwiać przywracanie pojedynczych plików z kopii zapasowych NDMP * Proponowane rozwiązanie musi obsługiwać funkcję NDMP Direct Access Recovery (DAR) |
| **65.** | Rozwiązanie musi wspierać Snapshots:   * Proponowane rozwiązanie musi zapewniać możliwość wykonywania migawek dla następujących macierzy dyskowych: * Pure Storage FlashArray * macierze pamięci masowej HPE 3PAR * macierze pamięci masowej NetApp * Hitachi storage array * macierze klasy enterprise InfiniBox * Proponowane rozwiązanie powinno zapewniać możliwość wykonywania migawek dla następujących obciążeń w chmurze: * instancje Amazon AWS EC2 * Maszyny wirtualne Azure * Maszyny wirtualne Google * Możliwość wykonywania migawek musi być dostępna dla systemów operacyjnych Windows i Linux. |
| **66.** | Rozwiązanie musi mieć możliwość raportowania:   * Proponowane rozwiązanie musi zapewniać podstawowe i zaawansowane raportowanie, w tym m.in. ale nie tylko; raportowanie kosztów zwrotnych, oszczędności deduplikacji, statystyki backupu, raportów o błędach, raportów na poziomie biznesowym do celów prognozowania, raportowanie SLA w zakresie backupu i odzyskiwania danych. * System raportowania rozwiązania powinien umożliwiać automatyczne wysyłanie wiadomości e-mail automatycznie codziennie jako załączniki w formacie .pdf, .csv i html * Proponowane rozwiązanie musi posiadać możliwość centralnego zarządzania, monitorowanie i raportowanie w odniesieniu do środowisk oprogramowania i urządzeń, w tym wielu środowisk backupowych * Proponowane rozwiązanie musi umożliwiać wysyłanie powiadomień o zadaniach za pomocą poczty elektronicznej lub SNMP |
| **67.** | Proponowane rozwiązanie musi umożliwiać tworzenie logicznie odizolowanych środowisk dla różnych organizacji/działów (Multi-Tenancy). |
| **68.** | Proponowane rozwiązanie musi wspierać kontrolę dostępu opartą na rolach (RBAC). |
| **69.** | Proponowane rozwiązanie musi oferować samoobsługowy backup i przywracanie danych dla wielu użytkowników, w sposób bezpieczny i podzielony na partycje. |
| **70.** | Rozwiązanie musi mieć możliwość Disaster Recovery Readiness:   * Proponowane rozwiązanie powinno zapewniać pojedynczy pulpit nawigacyjny do śledzenia stanu gotowości do Disaster Recovery wszystkich wybranych aplikacji. * Proponowane rozwiązanie musi zapewniać pełną automatyzację wszystkich operacji związanych z niezawodnością przy udziale maszyn wirtualnych, aplikacji i wielowarstwowych usług biznesowych. * Proponowane rozwiązanie powinno być w stanie zaoferować prawdziwe Disaster Recovery, jak również możliwości migracji, aby być w stanie zrealizować różne aspekty planu ciągłości biznesowej, takie jak odzyskiwanie do istniejącej i/lub zdalnej lokalizacji, migracja/odzysk do wybranej chmury publicznej. * Proponowane rozwiązanie powinno umożliwiać definiowanie aplikacji wielowarstwowych, tak aby wszystkie warstwy aplikacji były migrowane do miejsca Disaster Recovery lub testowane jako jedna całość * Proponowane rozwiązanie powinno być w stanie zapewnić spójne wsparcie dla platform fizycznych i wirtualnych, w tym cross-hypervisor (konwersja maszyn wirtualnych) oraz oferować opcję odzyskiwania do technologii chmurowych. * Proponowane rozwiązanie powinno być w stanie zapewnić wielostanowiskową widoczność stanu zdrowia komponentów aplikacji w czasie rzeczywistym. stanu zdrowia komponentów aplikacji w czasie rzeczywistym * Proponowane rozwiązanie powinno wspierać wiele celów poziomu usług (Service Level Objectives) w tym RPO backupu/odtwarzania * Rozwiązanie powinno umożliwiać automatyczne wykonywanie procesów Disaster Recovery i odzyskiwania w trybie symulacji, bez żadnych trwałych zmian w środowisku Disaster Reovery, aby potwierdzić, że czy wszystkie wymagania są spełnione dla pomyślnego wykonania procedury Disaster Recovery. Powinno ono wspierać testy nienaruszające produkcyjną infrastrukturę * Rozwiązanie DR powinno posiadać mechanizm zarządzania uprawnieniami oparte o role i powinno wykorzystywać istniejące Active Directory/LDAP do zarządzania tożsamością. * Proponowane rozwiązanie musi posiadać własny mechanizm do replikacji danych, a także umożliwiać wykorzystanie mechanizmów innych producentów w celu zwiększenia elastyczności. * Proponowane rozwiązanie replikacji musi obsługiwać zarówno platformy fizyczne jak i wirtualne z wbudowaną kompresją. * Proponowane rozwiązanie powinno umożliwiać planowanie działań lub testów w przyszłych terminach, a rozwiązanie powinno automatycznie, bez żadnych zależności, inicjować procesy w zaplanowanych terminach. Alerty również powinny być generowane i powiadamiać administratora z wyprzedzeniem. * Proponowane rozwiązanie powinno mieć możliwość zatrzymania/pauzy/wznowienia w trakcie wykonywania skonfigurowanego wcześniej procesu. * Proponowane rozwiązanie powinno udostępniać status uruchomionego procesu w trakcie jego wykonywania * Proponowane rozwiązanie musi zapewniać dowód zgodności z wewnętrznymi i zewnętrznymi wymogami ciągłości biznesowej za pomocą raportów z audytów i nieprzerwanych testów odzyskiwania danych po awarii w czasie rzeczywistym. * Proponowane rozwiązanie musi zapewniać pełną automatyzację wszystkich operacji związanych z odpornością, w tym rejestrów uruchomień odzyskiwania oraz orkiestracji uruchamiania i zatrzymywania odzyskiwania dla aplikacji wielowarstwowych w celu zmniejszenia ryzyka przestojów spowodowanych błędami ludzkimi. |

1. Urządzenia typu Appliance do Backupu z deduplikacją.

Przez Urządzenie do backupu z deduplikacją danych Zamawiający rozumie rozwiązanie charakteryzujące się jednolitą budową typu „appliance” pochodzące od jednego producenta i realizujące wszystkie wymagane funkcjonalności.

Nie dopuszcza się rozwiązania zbudowanego z niezależnych komponentów sprzętowo-programowych

Dostarczone urządzenie musi być przeznaczone do deduplikacji i przechowywania kopii zapasowych Zamawiającego

|  |  |
| --- | --- |
| **Lp.** | **MINIMALNE WYMAGANIA ZAMAWIAJĄCEGO** |
| **1.** | Urządzenie musi być przystosowane do montażu w szafie rack 19” |
| **2.** | Dostarczone urządzenie musi posiadać co najmniej 12 dysków SAS o rozmiarze minimum 1TB (dyski własne urządzenia) |
| **3.** | Oferowane urządzenie musi posiadać przestrzeń na dane po deduplikacji o pojemności minimum 140TB (powierzchnia czynna) z tym, że musi odbywać się to w obrębie jednego fizycznego urządzenia z półkami dyskowymi |
| **4.** | Oferowane urządzenie musi umożliwiać rozbudowę przestrzeni na dane po deduplikacji do pojemności minimum 470TB (powierzchnia czynna) z tym, że musi odbywać się to w obrębie jednego fizycznego urządzenia z półkami dyskowymi. Półki dyskowe muszą być obsadzone minimum 12 dyskami SAS, każdy o rozmiarze maksymalnie 8TB, wraz z kompletem okablowania umożliwiającego podłączenie półek zgodnie z rekomendacjami producenta |
| **5.** | Oferowane urządzenie musi posiadać minimum   * 4 porty Ethernet 1 GbE (wymagane w urządzeniu) * portów Ethernet 10/25 GbE z wkładkami SFP+ SR (wymagane w urządzeniu) * 2 porty FC 16Gb (wymagane w urządzeniu) dla podłączenia do infrastruktury SAN z dyskami i napędami taśmowymi |
| **6.** | Oferowane urządzenie musi mieć możliwość (przyszła rozbudowa) dostosowania konfiguracji portów do zmian w infrastrukturze LAN i SAN. Zamawiający musi mieć możliwość zmiany ilości portów urządzenia, tak by po rozbudowie posiadać kombinację:   * do 4 portów Ethernet 1 Gb (wymagane w urządzeniu) * do 6 portów Ethernet 10/25 GbE z wkładkami SFP+ SR (wymagane w urządzeniu) * do 8 portów FC 16 Gb w celu rozszerzenia funkcjonalności urządzenia o odbieranie danych od klientów systemu backupowego transmitowanych również przez SAN (wymagane w urządzeniu) |
| **7.** | Dyski z systemem operacyjnym urządzenia muszą być zabezpieczone technologią nie gorszą niż RAID 1 (lustrzana kopia wolumenu) |
| **8.** | Przechowywane kopie zapasowe oraz katalog systemu kopii zapasowych muszą być zabezpieczone technologią nie gorszą niż RAID 6 (Odporność na awarię w tym samym czasie dwóch dysków) |
| **9.** | Węzeł obliczeniowy urządzenia musi posiadać minimum 1 dysk hot-spare |
| **10.** | Każda półka dyskowa urządzenia musi posiadać minimum 1 dysk hot-spare |
| **11.** | Węzły obliczeniowe urządzenia jak i półki dyskowe muszą posiadać nadmiarowe zasilacze i wentylatory |
| **12.** | Węzły obliczeniowe urządzenia jak i półki dyskowe muszą umożliwiać wymianę dysków, zasilaczy i wentylatorów w trakcie pracy urządzenia (hot-swap) |
| **13.** | W celu optymalizacji działania i poprawy stanu zabezpieczeń urządzenia, system operacyjny urządzenia oraz zainstalowane na nim oprogramowanie musi być utwardzone (hardened) i zoptymalizowane przez jego producenta |
| **14.** | Oprogramowanie pokładowe musi umożliwiać śledzenie i zapisywanie w dzienniku zdarzeń wszystkich procesów uruchomionych na urządzeniu |
| **15.** | Konfiguracja urządzenia musi być możliwa poprzez przeglądarkę internetową i poprzez konsolę znakową |
| **16.** | Urządzenie musi obsługiwać deduplikację zarówno źródłową, jak i docelową, bez korzystania z serwerów pośredniczących, aby Zamawiający mógł wybrać miejsce deduplikacji w zależności od swoich potrzeb |
| **17.** | Urządzenie musi umożliwiać wysyłanie zdeduplikowanych i skompresowanych danych do klienta systemu kopii zapasowych bez konieczności rehydracji (proces odwrotny do deduplikacji) i dekompresji przez urządzenie, podnosząc szybkość przywracania danych, zmniejszając ilość przesyłanych danych przez medium transmisyjne i znacznie odciążając zasoby obliczeniowe urządzenia |
| **18.** | W celu uzyskania wysokiej wydajności i odciążenia sieci LAN - urządzenie musi obsługiwać backup i odtworzenia w oparciu o sieć SAN Fiber Channel, w tym bezpośrednie granularne odtworzenie ze zdeduplikowanej pamięci masowej. Urządzenia muszą obsługiwać implementację OST over FC |
| **19.** | Urządzenie musi posiadać zaimplementowane oprócz deduplikacji danych także mechanizmy optymalizujące transfer danych poprzez sieć WAN (tzw: „WAN Optimization”) |
| **20.** | Urządzenie musi obsługiwać deduplikację na źródle (kliencie), na media serwerze środowiska kopii zapasowych (inline) oraz w urządzeniu (inline) |
| **21.** | Urządzenie musi oferować wiele poziomów optymalizacji procesu deduplikacji, w tym zmienną długość bloku podczas deduplikacji, automatyczną optymalizację wykorzystania procesora i pamięci, automatyczną optymalizację procesu deduplikacji w zależności od typu backupowanych danych |
| **22.** | Urządzenie musi wykonywać ciągłą kompleksową weryfikację zdeduplikowanych i przechowywanych kopii zapasowych |
| **23.** | Urządzenie musi posiadać mechanizm ciągłej weryfikacji cyklicznej kontroli nadmiarowej (CRC) danych kopii zapasowych przechowywanych w puli deduplikacji |
| **24.** | Urządzenie musi wspierać deduplikację, szyfrowanie i kompresję na źródle oraz w locie podczas zapisu na nośnik dyskowy |
| **25.** | Urządzenie musi wspierać kompresję i szyfrowanie zdeduplikowanych danych na źródle i zapisanie ich na nośnik dyskowy w niezmienionej postaci |
| **26.** | Urządzenie musi umożliwiać w przyszłości rozbudowę o funkcjonalność WORM zintegrowanej z oferowanym oprogramowaniem backupu |
| **27.** | Funkcjonalność WORM musi gwarantować ochronę obrazu kopii zapasowej tak że jest tylko do odczytu i po utworzeniu kopii zapasowej nie może być modyfikowany, uszkodzony ani zaszyfrowany oraz obraz kopii zapasowej jest chroniony przed usunięciem przed upływem terminu retencji |
| **28.** | Urządzenie z funkcjonalnością WORM musi umożliwiać obsługę przynajmniej dwóch trybów blokady okresu retencji:   * Nikt nie może nadpisać lub usunąć danych, które są chronione w trybie zgodności w zdefiniowanym okresie retencji. Po ustawieniu okresu przechowywania danych nie można go skrócić, można go jedynie wydłużyć. * Dedykowany użytkownik może wyłączyć blokadę retencji, a następnie inny użytkownik z odpowiednimi uprawnieniami może usunąć obraz kopii zapasowej.   Wszystkie zdarzenia muszą być rejestrowane w dzienniku urządzenia. |
| **29.** | Urządzenie musi wspierać centralne zarządzanie kluczami szyfrowania (KMS) działającym w oferowanym oprogramowaniu backupu |
| **30.** | Urządzenie musi wspierać szyfrowanie danych z wykorzystaniem minimum protokołu AES |
| **31.** | Wymagane jest dostarczenie urządzenia wraz z licencją, pozwalające na jednoczesną obsługę protokołów CIFS i NFS do pełnej pojemności urządzenia wraz z dostarczanymi półkami dyskowymi |
| **32.** | Oferowany produkt musi posiadać obsługę mechanizmów globalnej deduplikacji dla wszystkich obsługiwanych protokołów, raz otrzymany i zapisany w urządzeniu fragment danych nie może nigdy więcej zostać zapisany bez względu na to, jakim protokołem zostanie ponownie dostarczony |
| **33.** | Przestrzeń składowania duplikowanych danych musi być jedna dla wszystkich protokołów dostępowych |
| **34.** | Oferowane urządzenie musi umożliwiać asynchroniczną replikację/duplikację danych do drugiego urządzenia, konfiguracja replikacji musi być możliwa w każdym z trybów:   * jeden do jednego * wiele do jednego * jeden do wielu |
| **35.** | Transmitowane mogą być tylko te fragmenty danych (bloki) które nie znajdują się na docelowym urządzeniu |
| **36.** | Replikacja/Duplikacja danych między dwoma urządzeniami kontrolowana przez system backupu musi oferować następujące funkcjonalności:   * replikacja odbywa się bezpośrednio między dwoma urządzeniami bez udziału dodatkowych serwerów * replikacji podlegają tylko te fragmenty danych, które nie znajdują się w docelowym urządzeniu * sterowanie odbywa się z poziomu oferowanego oprogramowania backupu * oferowane oprogramowanie posiada informację o obydwu kopiach zapasowych znajdujących się w obydwu urządzeniach |
| **37.** | Urządzenie musi automatycznie usuwać przeterminowane dane (fragmenty danych nie należące do backupów o aktualnej retencji) w procesie czyszczenia |
| **38.** | Proces usuwania przeterminowanych danych (czyszczenia) nie może uniemożliwiać pracę procesów backupu / odtwarzania danych (zapisu / odczytu danych z zewnątrz do systemu) |

1. Zintegrowane urządzenie pamięci masowej dedykowane dla długoterminowego składowania danych.

Specjalnie zaprojektowane rozwiązanie dla długoterminowego składowania danych, które oferuje przechowywanie i udostępnianie danych protokołami opartymi na plikach. Urządzenie (Appliance) stanowiące całość, obejmujące sprzęt, oprogramowani systemowe, oprogramowanie pokładowe określone daną nazwą i typem dla którego producent publikuje parametry dot. dostępnych funkcjonalności, budowy, skalowalności, wydajności.

|  |  |
| --- | --- |
| **Lp.** | **MINIMALNE WYMAGANIA ZAMAWIAJĄCEGO** |
| **1.** | Sprzęt i oprogramowanie rozwiązania muszą pochodzić od jednego producenta |
| **2.** | Całość rozwiązania, a mianowicie sprzęt, system operacyjny i oprogramowanie rozwiązania, musi być wspierane przez jednego producenta |
| **3.** | Aktualizacja oprogramowania, wgrywanie poprawek musi uwzględniać aktualizację także systemu operacyjnego i pochodzić od producenta całego rozwiązania (urządzenia) |
| **4.** | Oferowane urządzenie musi posiadać przestrzeń na dane o pojemności minimum 240TB (powierzchnia użytkowa) |
| **5.** | Rozwiązanie musi składować dane przestrzeni dyskowej składającej się z grup dysków w konfiguracji nie gorszej aniżeli RAID6, gdzie jedna grupa składa się maksymalnie z 16 dysków |
| **6.** | Urządzenie musi posiadać możliwość rozbudowy pojemności użytkowej, poprzez dołożenie półek dyskowych, do minimum 2800TB bez konieczności wymiany dostarczonych komponentów |
| **7.** | Urządzenie musi być dostarczone ze wszystkimi komponentami do instalacji w standardowej szafie rack o szerokości 19” |
| **8.** | Rozbudowane do maksymalnej pojemności urządzenie nie może przekroczyć 24U zajętości szafy rack o szerokości 19” |
| **9.** | Ilość wydzielanego ciepła rozbudowanego do maksymalnej pojemności urządzenia nie może przekroczyć 20300 BTU/godz. |
| **10.** | Architektura urządzenia powinna posiadać wysoko dostępną architekturę, składająca się z co najmniej dwóch serwerów/główek/kontrolerów pracujących w układzie active-active, który zapewnia wysoką dostępność serwowanych danych |
| **11.** | Obudowy urządzenia i półek dyskowych muszą posiadać widoczne elementy sygnalizacyjne do informowania o stanie poprawnej pracy lub awarii urządzenia, dysków, modułów zasilających, okablowania półek dyskowych |
| **12.** | Każda półka dyskowa musi posiadać minimum jeden globalny dysk HOT-SPARE |
| **13.** | Półki dla rozbudowy muszą być wyposażone w nadmiarowy układ zasilania i chłodzenia |
| **14.** | Urządzenie musi umożliwiać obsługę protokołów plikowych: NFS v3/v4, CIFS v3, HTTP, FTP oraz Amazon Simple Storage Service (S3) i iSCSI. Jeżeli uruchomienie tej funkcjonalności wymaga dodatkowych licencji, takie licencje muszą zostać dostarczone dla całej oferowanej przestrzeni dyskowej. |
| **15.** | Urządzenie musi wspierać funkcjonalność WORM (Write Once Read Many - Jednokrotny zapis, wielokrotny odczyt) minimum dla protokołów CIFS i NFS. Jeżeli uruchomienie tej funkcjonalności wymaga dodatkowych licencji, takie licencje muszą zostać dostarczone dla całej oferowanej przestrzeni dyskowej |
| **16.** | Oferowane urządzenie musi mieć możliwość integracji z Microsoft Active Directory i LDAP |
| **17.** | Urządzenie musi wspierać blokową deduplikację składowanych danych. Jeżeli uruchomienie tej funkcjonalności wymaga dodatkowych licencji, takie licencje muszą zostać dostarczone dla całej oferowanej przestrzeni dyskowej |
| **18.** | Urządzanie musi wspierać kompresję składowanych danych. Jeżeli uruchomienie tej funkcjonalności wymaga dodatkowych licencji, takie licencje muszą zostać dostarczone dla całej oferowanej przestrzeni dyskowej |
| **19.** | Oferowane urządzenie musi zapewniać replikację synchroniczną lub asynchroniczną. Jeżeli uruchomienie tej funkcjonalności wymaga dodatkowych licencji, takie licencje muszą zostać dostarczone dla całej oferowanej przestrzeni dyskowej |
| **20.** | Oferowane urządzenie musi znajdować się na liście kompatybilności VMware w zakresie wspieranej pamięci masowej typu NAS |
| **21.** | Oferowane urządzenie musi posiadać funkcjonalność kopii chwilowych (snapshot) dla całej oferowanej przestrzeni dyskowej |
| **22.** | Oferowane urządzenie musi posiadać funkcjonalność składowania danych w chmurze publicznej lub prywatnej jako dodatkowego poziomu składowania, tak zwany Cloud Tier. Urządzenie musi wspierać następujące usług chmury publicznej: Amazon S3, Amazon Glacier, Azure, Google cloud, IBM Cloud Object Storage. Zapisywanie danych w chmurze musi być sterowane polityką i harmonogramem konfigurowanymi przez administratora urządzenia |
| **23.** | Oferowane urządzenie musi mieć minimum 4 porty 10Gb Ethernet Small Form-factor Pluggable (SFP+) (minimum 2 per serwer/główka/kontroler) dostępne do serwowania danych |
| **24.** | Oferowane urządzenie musi umożliwiać agregację interfejsów Ethernet w następujących trybach działania: 802.3ad, broadcast, balance-xor, balance-rr, balance-tlb, balance-alb, active-backup |
| **25.** | Oferowane urządzenie musi obsługiwać funkcjonalność virtual LAN (VLAN) |
| **26.** | Oferowane urządzenie musi obsługiwać funkcjonalność jumbo frames pozwalającą na zwiększenie rozmiaru ramki Ethernet ponad standardową wielkość do maksymalnej wielkości ramki 9 kB, co pozwali na zwiększenie przepustowości przy przesyłaniu dużych segmentów danych |
| **27.** | Urządzenia musi umożliwiać zarządzanie zarówno z poziomu linii komend (CLI), jak również poprzez interfejs graficzny (GUI). Dostęp do urządzenia bezpośrednio z poziomu standardowych przeglądarek internetowych oraz klientów SSH. |
| **28.** | System operacyjny urządzenia na których posadowiono rozwiązanie musi być zoptymalizowany pod kontem zadań długoterminowego składowania danych |
| **29.** | Urządzenie musi posiadać system bezpieczeństwa umożliwiający:   * Monitorowanie integralności plików w czasie rzeczywistym w zakresie identyfikacji zmian w plikach w czasie rzeczywistym, w tym kto dokonał zmiany i jaka zmiana nastąpiła * Monitorowanie konfiguracji w zakresie identyfikacji w czasie rzeczywistym naruszenia zdefiniowanych zasad i podejrzanych działań na urządzeniu * Skonsolidowane rejestrowanie zdarzeń w zakresie konsolidacji i przekazywania logów w celach długoterminowego składowania, raportowania i dalszej analizy * Zapobieganie sabotażom na plikach i systemie w zakresie blokowania zmian w konfiguracji, ustawień i plików |
| **30.** | Zarządzanie i konfiguracja urządzenia musi być możliwa również poprzez RESTful API minimum w zakresie:   * Udostępnianie i konfiguracji pamięci masowej * Monitorowania pojemności * Monitorowania zdarzeń * Sterowania umieszczania danych lokalnie lub do chmury * Konfiguracji i sterowania politykami usuwania danych * Sterowania replikacją * Sterowania kopiami migawkowymi |

1. Wdrożenie Systemu do Archiwizacji

* Instalacja i konfiguracja komponentów systemu,
* Wprowadzenie licencji,
* Integracja z AD Zamawiającego
* Konfiguracja użytkowników i uprawnień,
* Konfiguracja logowania zdarzeń,
* Testy poprawności pracy systemu,
* Uruchomienie automatu importującego lokalne archiwa poczty z klienta IBM Lotus Notes ze stacji klienckich Zamawiającego,
* Konfiguracja archiwizacji na serwerach IBM Lotus Domino zgodnie z wytycznymi Zamawiającego,
* Konfiguracja kopii zapasowej w dostarczanym systemie centralnego backupu
* Przygotowanie dokumentacji powykonawczej wraz z procedurami (disaster recovery, upgrade systemu)

1. Wdrożenie Centralnego Systemu Kopii Zapasowych

* Instalacja i konfiguracja komponentów systemu,
* Wprowadzenie licencji,
* Integracja z AD Zamawiającego
* Dodanie pilotażowo 10 serwerów klienckich
* Konfiguracja polityk Backupu,
* Konfiguracja polityk długoterminowego Backupu,
* Konfiguracja logowania zdarzeń,
* Testy poprawności pracy systemu,
* Przygotowanie dokumentacji powykonawczej wraz z procedurami (disaster recovery, upgrade systemu)

1. Instruktaż z zaoferowanych komponentów systemu dla min. 3 Administratorów

* Instruktaż musi trwać minimum 5 dni każdy po 8 godzin lekcyjnych (45 minut).
* Instruktaż musi być przeprowadzone przez certyfikowanych inżynierów.
* W trakcie szkolenia dla uczestników szkolenia w ciągu dnia, musi być dostarczony minimum jeden posiłek ciepły i dwie przerwy kawowe.
* Instruktaż musi być przeprowadzone w formie, gdzie minimum 50% czasu szkolenia to będą warsztaty praktyczne.
* Warsztaty muszą być przeprowadzone na infrastrukturze o parametrach odpowiadających przedmiotowi dostawy w niniejszym postępowaniu.
* Instruktaż musi być przeprowadzone w języku polskim.
* Dla każdego uczestnika szkolenia muszą zostać dostarczone materiały szkoleniowe w formacie przeszukiwalnym.
* Dopuszcza się szkolenie w formie online.