Załącznik nr 3 do SIWZ

Opis techniczny części trzeciej zamówienia

Dedykowane urządzenie do wykonywania kopii bezpieczeństwa zasobów infrastruktury informatycznej – szt. 1

Przedmiotem tej części zamówienia jest zakupienie kompletnego rozwiązania do backupu opartego na bazie sprzętu i oprogramowania.

Wyżej wymieniony system powinien się opierać o architekturę klient-serwer, z centralnym serwerem zarządzającym procesem backupu oraz klientami (agentami) instalowanymi na maszynach w sieci. System kopii zapasowych ma umożliwiać prostą promocję każdego z klientów (niezależnie od wykorzystywanego systemu operacyjnego) zarejestrowanych w centralnym systemie backupu do funkcji serwera mediów, który może posłużyć do składowania backupu z innych klientów. Powyższa funkcja ma umożliwiać promocję klienta do funkcji serwera mediów z wykorzystaniem dedykowanej funkcji interfejsu Web, w szczególności niedopuszczalne jest, aby konieczne było modyfikowanie plików konfiguracyjnych klienta oraz serwera a także konieczność zmian na samym kliencie. Z kolei funkcja serwera mediów ma umożliwiać wykorzystanie zarówno lokalnych zasobów dyskowych każdego z klientów, jak również napędu taśmowego oraz biblioteki taśmowej do nich podłączonych celem zapisania na nich backupu z pozostałych klientów.

System archiwizacji ma posiadać możliwość backupu nieograniczonej ilości danych źródłowych. Jedynym ograniczaniem może być przestrzeń dyskowa wewnętrznej macierzy. System ma zapewnić (posiadać licencję gwarantującą współpracę) współpracę z bibliotekami taśmowymi z wbudowanymi mechanizmami robotyki, bez względu na liczbę kaset oraz napędów obsługiwanych przez daną bibliotekę.

Urządzenie powinno być wyposażone minimum w 2 dyski 3,5” o łącznej pojemności min. 4TB. Wymagane zabezpieczenie macierzy nin. na poziomie RAID1, pozostawiając administratorowi przestrzeń zapisu do wykorzystania min. 2 TB danych. Dyski w urządzeniu powinny być montowane w postaci zatok na froncie urządzenia. Zatoki powinny oferować funkcjonalność hot-swap czyli wymianę dowolnego dysku w czasie pracy urządzenia.

Macierz dyskowa dostarczana wraz z urządzeniem, musi pochodzić od tego samego producenta co rozwiązanie do backupu. Nie dopuszcza się sytuacji, w której macierz i rozwiązanie do backupu pochodzą od różnych producentów.

Dyski wchodzące w skład macierzy dyskowej muszą posiadać dożywotnią gwarancje producenta niezależną od gwarancji samego urządzenia czy wykupionego wsparcia technicznego.
Urządzenie powinno umożliwiać rozbudowę o dodatkowe min. dwa dyski twarde o minimalnej pojemności 2TB na każdy z nich. Dodatkowo urządzenie powinno być:

- wyposażone w minimum dwa porty USB 3.0, celem podłączenia klawiatury lub zewnętrznych urządzeń,
- wyposażone w minimum dwa interfejsy GigabitEthernet o prędkości 1Gb/s.,
- wyposażone w redundancję zasilania w postaci dwóch niezależnych zasilaczy,
- wyposażone w panel LCD umieszczony na przednim panelu urządzenia wyświetlające jego status.

Wymagane jest również, aby rozwiązanie posiadało:

- możliwość autodetekcji dowolnego napędu taśmowego i biblioteki, która została do niego podłączona,
- możliwość ręcznej definicji dowolnego napędu taśmowego i biblioteki wraz z informacjami dotyczącymi jego budowy,
- możliwość obsługi nielimitowanej ilości klientów backupu plikowego, wykorzystanie innych typów agentów może być ograniczone tylko poprzez wgranie odpowiedniej licencji,

- być wyposażony w moduł zarządzania licencjami, gdzie poprzez interfejs Web, administrator posiada możliwość dodawania dowolnej licencji.

Moduł zarządzania licencjami ma mieć możliwość dodawania (rozbudowy) poszczególnych funkcjonalności oprogramowania bez konieczności uruchamiania ponownie żadnego z komponentów oprogramowania. Niedopuszczalna jest konieczność restartu jakichkolwiek usług wchodzących w skład oprogramowania oraz jakichkolwiek maszyn wchodzących w skład systemu kopii bezpieczeństwa (włączając w to maszyny z zainstalowaną aplikacją klienta).

Centralny serwer backupu ma zostać dostarczony w formie urządzenia dedykowanego wyłącznie do wykonywania kopii bezpieczeństwa danych.

System operacyjny w urządzeniu powinien być dostosowany przez producenta w taki sposób, aby nie wymagał od zamawiającego zarządzania, utrzymywania oraz aktualizacji wewnętrznych komponentów oraz, aby wbudowany system nie wymagał od zamawiającego zakupu dodatkowych licencji. Interfejs zarządzania serwerem backupu ma być dostępny poprzez przeglądarkę internetową. Wspierane przez producenta przeglądarki do zarządzania serwerem backupu to minimum Mozilla Firefox 3.0 lub nowszy oraz Microsoft Internet Explorer 7.0 lub nowszy. Funkcjonalność zarządzania programem przez przeglądarkę ma być dostępna jako funkcja dodatkowa, system powinien oferować możliwość wyłączenia tej funkcji i zarządzanie systemem backupu w pełni poprzez środowisko tekstowe CLI, dostępne zarówno bezpośrednio po podłączeniu klawiatury/myszy do urządzenia, jak również poprzez interfejs SSH. Interfejs systemu ma być dostępny przez przeglądarkę za pomocą protokołu HTTPS, tym samym cała komunikacja pomiędzy przeglądarką a systemem ma być szyfrowana.

System ma umożliwiać utworzenie dowolnej ilości kont użytkowników. Użytkownicy w systemie muszą mieć możliwość przypisania roli odzwierciedlającej poziom uprawnień. W domyślnej konfiguracji, system ma oferować minimum 3 rodzaje kont użytkowników systemu:

- Administrator - może wykonywać wszystkie typy operacji w systemie w tym tworzyć, modyfikować oraz usuwać obiekty i konta użytkowników;
- Operator – może uruchamiać zadania backupu, ma dostęp z uprawnieniami tylko do odczytu do konfiguracji systemu;
- Użytkownik – nie może tworzyć, usuwać ani modyfikować jakichkolwiek obiektów w systemie, ma prawo jedynie do odtwarzania kopii zapasowych.

Serwer backupu ma umożliwiać dwukierunkową komunikację z agentami. Serwer backupu ma mieć możliwość połączenia z agentem zarówno za pomocą adresu IP jak również z wykorzystaniem nazwy DNS.

Produkt ma posiadać możliwość replikacji danych pomiędzy lokalnymi zasobami dyskowymi, tym samym administrator ma mieć możliwość zwielokrotnienia tych samych danych na wielu zasobach dyskowych celem zabezpieczenia danych przed awarią pojedynczego zasobu dyskowego. Proces replikacji danych pomiędzy lokalnymi zasobami dyskowymi ma być wyzwalany na żądanie administratora. Administrator ma być w stanie określić przed rozpoczęciem replikacji:

- źródłowy logiczny zbiór danych do replikacji (z dokładnością do pojedynczego pliku);
- docelowy zasób dyskowy, na który dane mają zostać zreplikowane;
- czas retencji dla danych replikowanych;
- włączenie/wyłączenie raportowania na e-mail o szczegółach wykonania zadania replikacji;
- wyłączenie aktualizacji indeksu danych o dane zreplikowane;
- ustawienie limitu czasowego po przekroczeniu, którego proces replikacji zostanie zatrzymany.

System ma umożliwiać prostą rozbudowę o opcję związaną z szyfrowaniem backupu z wykorzystaniem przynajmniej takich algorytmów jak 3DES (z PCBC), Blowfish oraz AES256 za pomocą pojedynczego pliku licencji instalowanej na serwerze backupu. Klucze szyfrujące nie mogą być zapisywane razem z danymi backupowanymi. Klucze mają być przechowywane na kliencie (agencie) a

nie na centralnym serwerze backupu. Funkcjonalność szyfrowania danych ma zabezpieczać zarówno dane przesyłane przez sieć jak również dane zapisywane na centralnym serwerze backupu.
System ma oferować możliwość odtwarzania backupu z możliwością określenia:

- czy odtworzone mają być oryginalne prawa na plikach;
- daty modyfikacji;
- ACL w systemie POSIX oraz atrybutów rozszerzonych Linux;
- czy nadpisywać pliki, jeśli istnieją na docelowej maszynie;
- czy nadpisywać pliki, jeśli są nowsze niż te, które znajdują się w backupie.

Podczas odtwarzania, administrator ma ponadto mieć możliwość zdefiniowania systemu innego niż centralny system backupu, który będzie źródłem dla procesu odtwarzania.
System ma oferować możliwość kompresji danych backupu przed przesłaniem ich poprzez sieć na backup serwer, możliwość ta ma istnieć jako opcja dla każdego z definiowanych zadań backupu.
Wykorzystywana do backupu metoda kompresji ma bazować na algorytmie LZ77, w szczególności niedopuszczalne jest stosowanie zamkniętych algorytmów kompresji danych.

Centralny serwer backupu ma być wyposażony w mechanizm reindeksacji istniejących taśm z backupem. W przypadku uszkodzenia indeksu, funkcja ta musi mieć możliwość zaindeksowania taśm utworzonych zarówno na danym centralnym serwerze backupu, jak i na każdym innym centralnym serwerze backupu wchodzącym w skład środowiska backupu.

Mechanizm reindeksacji taśm ma umożliwiać administratorowi określenie następujących właściwości procesu przed jego rozpoczęciem:

- w przypadku znanych taśm: wybór źródłowej taśmy, wybór źródłowego napędu, wybór czy rozpocząć indeksację od momentu jej przerwania czy od początku nośnika, wybór czy wysunąć taśmę z napędu po zakończeniu procesu indeksacji oraz czy po zakończeniu procesu przesłać powiadomienie do administratora drogą elektroniczną z podsumowaniem procesu indeksacji;
- W przypadku nieznanych taśm: wybór źródłowego napędu, wybór puli taśmowej do podłączenia, wybór typu taśmy – produkt ma zawierać listę minimum 76 predefiniowanych typów taśm (w tym minimum ma oferować taśmę typu NULL oraz FILE celem testowania poprawności konfiguracji), zdefiniowania czy w zadaniu użyta ma być biblioteka taśmowa (jeśli tak, administrator ma mieć opcję wskazania, której biblioteki należy użyć podczas procesu reindeksacji oraz którego slotu tej biblioteki), wybór czy rozpocząć indeksację od momentu jej przerwania czy od początku nośnika, wybór czy wysunąć taśmę z napędu po zakończeniu procesu indeksacji oraz czy po zakończeniu procesu powiadomić administratora wiadomością e-mail z podsumowaniem procesu indeksacji.

Centralny serwer backupu ma być wyposażony w mechanizm reindeksacji istniejących zasobów dyskowych z backupem w przypadku uszkodzenia indeksu. Funkcja ta ma mieć możliwość zaindeksowania dysków z danymi zarówno na danym centralnym serwerze backupu, jak i na każdym innym centralnym serwerze backupu wchodzącym w skład środowiska backupu.

Mechanizm reindeksacji dysków ma umożliwiać administratorowi określenie takich właściwości procesu przed jego rozpoczęciem jak:

- w przypadku znanych dysków: wybór źródłowego zasobu dyskowego, wybór czy rozpocząć indeksację od momentu jej przerwania czy od początku nośnika oraz czy po zakończeniu procesu przesłać powiadomienie do administratora drogą elektroniczną z podsumowaniem procesu indeksacji;
- w przypadku nieznanych dysków: wybór hosta należącego do systemu backupu, do którego podłączony jest zasób dyskowy, definicja nazwy dla nowoutworzonego zasobu dyskowego po indeksacji, wskazanie pełnej ścieżki do indeksowanych danych, zdefiniowanie wielkości wolumenu z dokładnością do 1 megabajta, wybór czy rozpocząć indeksację od momentu jej przerwania czy od początku nośnika oraz czy po zakończeniu

procesu przesłać powiadomienie do administratora drogą elektroniczną z podsumowaniem procesu indeksacji.

System ma być wyposażony w mechanizm weryfikacji taśm, który umożliwia test czy dane zapisane na taśmie mogą być poprawnie odczytane. Funkcjonalność ta ma umożliwiać administratorowi zdefiniowanie przed rozpoczęciem procesu weryfikacji minimum następujących elementów:

- wybór taśmy do weryfikacji;
- wybór napędu, który posłuży do weryfikacji;
- wybór czy wznowić weryfikację od momentu, w którym proces został przerwany;
- wybór czy wysunąć taśmę z napędu po zakończeniu procesu weryfikacji;
- czy po zakończeniu procesu przesłać powiadomienie do administratora drogą elektroniczną z podsumowaniem procesu weryfikacji.

System ma być wyposażony w mechanizm duplikacji taśm z zapisanymi na nich kopiami bezpieczeństwa, który umożliwi utworzenie dowolnej ilości kopii danej taśmy celem zabezpieczenia danych przed awarią lub zniszczeniem nośnika. Funkcjonalność ta ma umożliwiać administratorowi zdefiniowanie przed rozpoczęciem procesu duplikacji minimum następujących elementów:

- wybór źródłowej taśmy z danymi do duplikacji;
- wybór napędu, w którym umieszczono źródłową taśmę;
- wybór napędu, w którym umieszczono taśmę docelową;
- możliwość wyboru czy podczas procesu będzie wykorzystywana biblioteka taśmowa (jeśli tak, to dodatkowo administrator ma mieć możliwość zdefiniowania, której biblioteki należy użyć podczas procesu oraz slotu w którym zainstalowano taśmę docelową);
- możliwość wymuszenia nadpisywania danych na taśmie docelowej;
- czy po zakończeniu procesu przesłać powiadomienie do administratora drogą elektroniczną z podsumowaniem procesu duplikacji.

System ma być wyposażony w mechanizm nawigacji, który umożliwia przeglądanie przez przeglądarkę Web zawartości dysków twardych wszystkich klientów zarejestrowanych w centralnym serwerze backupu oraz dodatkowo jego własne dane. Dane mają być wyświetlane w formie drzewa katalogów z możliwością przeglądania ich zawartości. Funkcjonalność ta ma działać niezależnie od systemu operacyjnego klienta oraz serwera. W każdym przypadku administrator ma mieć możliwość przeglądania plików i katalogów oraz weryfikacji poprawności komunikacji pomiędzy klientem a serwerem. Mechanizm nawigacji ma oferować możliwość weryfikacji, czy na stacji poprawnie zainstalowano agenta do hot-backupu aplikacji (agent ma wówczas w drzewie przypisanym do danego klienta wyświetlać listę takich aplikacji).

System ma być wyposażony w mechanizm automatycznego wykrywania urządzeń takich jak napędy i biblioteki taśmowe, które zostały podłączone do centralnego systemu backupu. Funkcja ta nie może wymagać od administratora uprzedniej instalacji sterowników do obsługi danego urządzenia.

System kopii zapasowych ma być dostarczony z podstawową licencją zezwalającą na korzystanie ze wszystkich podstawowych jego funkcji. Licencja ta ma zezwalać na wykonywanie backupu na dysk, na taśmę (z wykorzystaniem napędu taśmowego oraz biblioteki taśmowej).

System ma być wyposażony w mechanizm deduplikacji, który pozwoli zaoszczędzić ilość miejsca na dysku poprzez wyszukiwanie bloków zapisanych na nośniku w poprzednim zadaniu backupu. Do działania deduplikacji nie może być wymagana inna licencja niż podstawowa.

System ma być wyposażony w licencję, która gwarantuje współpracę z bibliotekami taśmowymi z wbudowanymi mechanizmami robotyki, bez względu na liczbę kaset oraz napędów obsługiwanych przez daną bibliotekę. System ma mieć możliwość autodetekcji dowolnego napędu taśmowego i biblioteki, która została do niego podłączona. Administrator ma mieć możliwość ręcznej definicji dowolnego napędu taśmowego i biblioteki wraz z informacjami dotyczącymi jego budowy. W ramach licencji można instalować nieograniczoną ilość agentów.

Produkt ma posiadać możliwość replikacji danych pomiędzy lokalnymi zasobami dyskowymi, tym samym administrator ma mieć możliwość zwielokrotnienia tych samych danych na wielu zasobach dyskowych celem zabezpieczenia danych przed awarią pojedynczego zasobu dyskowego. Proces replikacji danych pomiędzy lokalnymi zasobami dyskowymi ma być wyzwalany na żądanie administratora. Administrator ma być w stanie określić przed rozpoczęciem replikacji:

- źródłowy logiczny zbiór danych do replikacji (z dokładnością do pojedynczego pliku);
- docelowy zasób dyskowy, na który dane mają zostać zreplikowane;
- czas retencji dla danych replikowanych;
- włączenie/wyłączenie raportowania na e-mail o szczegółach wykonania zadania replikacji;
- wyłączenie aktualizacji indeksu danych o dane zreplikowane;
- ustawienie limitu czasowego po przekroczeniu, którego proces replikacji zostanie zatrzymany.

System backupu musi mieć możliwość obsługi nielimitowanej ilości klientów backupu plikowego, wykorzystanie innych typów agentów może być ograniczone tylko poprzez wgranie odpowiedniej licencji.

Oprogramowanie ma być wyposażone w funkcję łańcuchowania backupu Disk-To-Disk-To-Tape (D2D2T). Funkcjonalność ta ma umożliwiać zdefiniowanie zadania backupu na dysk, które po zakończeniu automatycznie przeniesie dane na taśmę (za pośrednictwem napędu lub biblioteki taśmowej).

Administrator ma mieć możliwość zdefiniowania odstępu czasu wyrażonego w minutach, które opóźni moment przenoszenia danych na taśmę w stosunku do momentu zakończenia zadania backupu na dysk. Czas ten ma być definiowany per zadanie backupu. Funkcjonalność łańcuchowania D2D2T ma być możliwa także dla backupów zaplanowanych z harmonogramu. Przy definiowaniu zadania backupu z uaktywnionym łańcuchowaniem D2D2T administrator ma mieć możliwość określenia polityki wykorzystywania taśm (użycie istniejących taśm do końca lub wykorzystanie nowych taśm), określenia retencji dla backupu na taśmie oraz możliwość włączenia szczegółowego raportowania na e-mail o statusie zadania. Administrator ma mieć możliwość zdefiniowania zautomatyzowanego mechanizmu D2D2T dla danych zapisanych na dysku, przy czym wyzwolenie zdarzenia łańcuchowania będzie związane minimum z: wielkością wykorzystywanego miejsca na wybranym zasobie dyskowym z dokładnością do 1MB, ilością pozostałego miejsca na zasobie dyskowym z dokładnością do 1MB. Administrator ma mieć także możliwość zdefiniowania kolejności z jaką dane będą zapisywane na taśmie od najstarszych do najnowszych. Administrator ma mieć możliwość zdefiniowania czy po zakończeniu procesu łańcuchowania D2D2T dane na zasobie dyskowym mają być usunięte czy pozostawione.

Sytem backupu ma wspierać hot-backup (backup w czasie pracy) dla platform wirtualizacyjnych Xen oraz Citrix XenServer w wersjach 5.5 i wyższych. Backup maszyn wirtualnych w środowisku Xen bez konieczności instalacji agenta na każdej z pracujących maszyn (backup na poziomie hypervisora).

Backup maszyn wirtualnych w środowisku Xen ma być realizowany jako backup pełny z uwzględnieniem wszystkich maszyn wirtualnych, zarówno pracujących jak również zatrzymanych.

Przywracanie backupu maszyn wirtualnych środowiska Xen ma zapewniać możliwość przywracania wszystkich maszyn wirtualnych lub pojedynczych, zdefiniowanych przed administratora maszyn.

Przywracanie maszyn wirtualnych ma być niezależne. Proces przywracania nie ma wymagać od administratora wykorzystywania innych maszyn niż centralnego serwera backupu oraz docelowego hosta Xen/XenServer, na którym maszyny zostaną odtworzone.

Przywracanie maszyn wirtualnych ma być możliwe z przekierowaniem Hypervisora (zmiana miejsca docelowego dla odtwarzanego backupu) ze wskazaniem hosta docelowego.

System ma zapewniać zarządzanie zadaniami backupu i przywracania dla platformy wirtualnej z poziomu przeglądarki internetowej. System ma mieć możliwość uaktywnienia mechanizmu deduplikacji danych dla backupu maszyn wirtualnych. Funkcjonalność deduplikacji ma być możliwa po stronie backupowanej maszyny. Funkcjonalność ta ma być definiowana (także włączana lub

wyłączana) na poziomie pojedynczego zadania backupu. System ma mieć możliwość uaktywnienia kompresji danych dla backupu maszyn wirtualnych. Administrator ma mieć możliwość wyboru pomiędzy przynajmniej dwoma algorytmami kompresji, przy czym produkt ma umożliwiać wybór minimum algorytmów LZRW1 oraz LZRW3-A.

Zapewnienie funkcjonalności archiwizacji dla produktów firmy Microsoft - System musi posiadać możliwość (licencję) archiwizacji nielimitowanej ilości instancji usług MS SQL Server, MS Exchange, MS SharePoint oraz MS Active Directory.

1. **Backup serwera pocztowego MS Exchange:**
   - Agent backupu ma wspierać hot-backup (backup w czasie pracy) dla serwera MS Exchange w wersjach 2000, 2003, 2007, 2010 oraz 2013.
   - Backup ma być realizowany jako backup pełny, przyrostowy oraz dyferencyjny zarówno dla magazynów informacji (Information Stores), grup przechowywania (Storage Groups) jak i baz danych.
   - Agent backupu ma wykorzystywać technologie Extensible Storage Engine (ESE) lub Volume Shadow-Copy Service (VSS), wykonując zadania backupu w trakcie pracy serwera Exchange i nie zakłócając działania usługi.
   - Agent backupu ma używać wbudowanego w Extensible Storage Engine (ESE) interfejsu programowania aplikacji (API), zachowując przestrzeganie ścisłych formatów backupu Microsoft zapewniając pełną integrację danych.
   - System ma pozwalać na przywracanie danych do Recovery Storage Groups (Exchange 2007) i Recovery Databases (Exchange 2010) na poziomie całych skrzynek jak i poszczególnych wiadomości.
   - Agent backupu ma wspierać usługę replikacji (Site Replication Service), zapewniając kompatybilność pomiędzy serwerami MS Exchange 5.5 i 2000.
   - Agent musi obsługiwać backup serwerów zarządzających kluczami (Key Management Server), pozwalając na odzyskanie danych zaszyfrowanych.
   - Agent backupu musi umożliwiać pełne przywrócenie bazy serwera Exchange do stanu z określonego momentu (point-in-time).
   - System musi umożliwiać backup klastrów CCR/LCR/SCR (Exchange 2007).
   - System ma mieć możliwość uaktywnienia mechanizmu deduplikacji danych dla backupu środowiska MS Exchange.
   - Funkcjonalność deduplikacji ma być możliwa zarówno na poziomie centralnego serwera backupu jak i po stronie backupowanej maszyny. Funkcjonalność ta ma być definiowana (także włączana lub wyłączana) na poziomie pojedynczego zadania backupu.
   - System ma mieć możliwość uaktywnienia kompresji danych dla backupu środowiska MS Exchange.
   - Administrator ma mieć możliwość wyboru pomiędzy przynajmniej dwoma algorytmami kompresji, przy czym produkt ma umożliwiać wybór minimum algorytmów LZRW1 oraz LZRW3-A.

2. **Backup baz danych MS-SQL:**
   - Agent backupu ma wspierać hot-backup (backup w czasie pracy) dla bazy danych MS-SQL w wersjach 2000, 2005, 2008, 2008 R2, 2012.
   - Backup ma być możliwy zarówno dla całych instancji, jak również dla poszczególnych baz danych, grup plików oraz indywidualnych plików.
   - Backup ma być realizowany jako backup pełny, kopia (VSS), backup przyrostowy (VDI) oraz dyferencyjny.
   - Przykracanie bazy ma odbywać się w jednym z trzech trybów: do oryginalnej lokalizacji, na inny serwer, do innej lokalizacji.

- System ma wspierać relokację baz danych do innych instancji, pracujących nawet na innym hoście.
- System ma wspierać relokację z jednoczesną zmianą nazwy odtwarzanych obiektów.
- System ma mieć możliwość uaktywnienia mechanizmu deduplikacji danych dla backupu bazy danych MS-SQL.
- Funkcjonalność deduplikacji ma być możliwa zarówno na poziomie centralnego serwera backupu jak i po stronie backupowanej maszyny. Funkcjonalność ta ma być definiowana (także włączana lub wyłączana) na poziomie pojedynczego zadania backupu.
- System ma mieć możliwość uaktywnienia kompresji danych dla backupu bazy danych MS-SQL.
- Administrator ma mieć możliwość wyboru pomiędzy przynajmniej dwoma algorytmami kompresji, przy czym produkt ma umożliwiać wybór minimum algorytmów LZRW1 oraz LZRW3-A.

3. Backup środowiska Active Directory

- Agent backupu ma wspierać hot-backup (backup w czasie pracy) dla środowisk Active Directory w wersjach dla systemów Windows 2003, 2008 oraz 2008 R2, 2012 R2.
- Backup ma być możliwy w trybie pełnym, całego katalogu Active Directory.
- Backup ma być realizowany z wykorzystaniem mechanizmu VSS, niedopuszczalne jest stosowanie innych trybów backupu.
- System ma wspierać odtwarzanie środowiska Active Directory w oryginalną lokalizację, na inną maszynę (migracja) oraz w formie pliku na dowolnej maszynie z zainstalowanym agentem systemu backupu.
- System powinien umożliwiać odtwarzanie backupu na kontrolerze domeny w jednym z 3 trybów:
  - Przywrócenie do oryginalnej lokalizacji;
  - Przywrócenie do innej lokalizacji;
  - Przywrócenie ze wskazaniem miejsca na dysku.
- System powinien umożliwiać odtwarzanie autorytatywne z możliwością oznaczania poszczególnych obiektów drzewa Active Directory.
- System ma mieć możliwość uaktywnienia mechanizmu deduplikacji danych dla backupu Active Directory.
- Funkcjonalność deduplikacji ma być możliwa zarówno na poziomie centralnego serwera backupu jak i po stronie backupowanej maszyny. Funkcjonalność ta ma być definiowana (także włączana lub wyłączana) na poziomie pojedynczego zadania backupu.
- System ma mieć możliwość uaktywnienia kompresji danych dla backupu usługi Active Directory.
- Administrator ma mieć możliwość wyboru pomiędzy przynajmniej dwoma algorytmami kompresji, przy czym produkt ma umożliwiać wybór minimum algorytmów LZRW1 oraz LZRW3-A.

Zapewnienie funkcjonalności archiwizacji środowisk wirtualizacyjnych. System archiwizacji musi umożliwiać (posiadać licencję) archiwizację nielimitowanej ilości maszyn wirtualnych z poziomu hypervisora. Rozwiązanie powinno umożliwić wykonanie kopii więcej niż jednego typu środowiska wirtualizacyjnego. Dokładne parametry agentów/konektorów dla środowisk wirtualizacyjnych powinny być zgodne z kolejnymi sekcjami.

1. Backup środowiska wirtualnego Microsoft Hyper-V:

- agent backupu ma wspierać hot-backup (backup w czasie pracy) dla platformy wirtualizacyjnej Microsoft Hyper-V w wersjach Windows Server 2008, Windows Server 2008 R2 oraz Windows Server 2012,

- backup ma być możliwy zarówno dla całych obrazów maszyn wirtualnych, jak i na poziomie poszczególnych wykorzystanych bloków,
- backup ma być realizowany jako backup pełny oraz backup inkrementacyjny z wykorzystaniem technologii śledzenia zmienionych bloków,
- funkcjonalność agenta backupu ma umożliwiać backup zarówno zatrzymanych jak również pracujących maszyn wirtualnych bez konieczności instalacji agenta na każdej z tych maszyn (backup na poziomie hypervisora),
- agent backupu ma umożliwiać backup tylko danych fizycznie zapisanych na wirtualnym dysku,
- agent backupu ma zapewniać możliwość przywracania wszystkich maszyn wirtualnych lub pojedynczych, zdefiniowanych przed administratora maszyn,
- przywracanie maszyn wirtualnych ma być niezależne. Proces przywracania nie ma wymagać od administratora wykorzystywania innych maszyn niż centralnego serwera backupu oraz docelowego hosta Hyper-V, na którym maszyny zostaną odtworzone,
- przywracanie maszyn wirtualnych ma być możliwe z przekierowaniem hypervisora (zmiana miejsca docelowego dla odtwarzanego backupu) ze wskazaniem hosta docelowego,
- agent backupu ma pozwalać na wykonanie backupu na poziomie bloków przy wsparciu mechanizmu Changed Block Tracking (CBT),
- system ma zapewniać zarządzanie zadaniami backupu i przywracania dla platformy wirtualnej z poziomu przeglądarki internetowej,
- system ma wspierać wiele mechanizmów transportu, w szczególności system ma wspierać backup maszyn wirtualnych bez konieczności użycia sieci LAN (z wykorzystaniem sieci SAN), za pośrednictwem wirtualnej sieci LAN lub bezpośrednio na urządzenie podłączone za pośrednictwem interfejsu SCSI,
- system ma mieć możliwość uaktywnienia mechanizmu deduplikacji danych dla backupu maszyn wirtualnych,
- Funkcjonalność deduplikacji ma być możliwa zarówno na poziomie centralnego serwera backupu jak i po stronie backupowanej maszyny. Funkcjonalność ta ma być definiowana (także włączana lub wyłączana) na poziomie pojedynczego zadania backupu,
- system ma mieć możliwość uaktywnienia kompresji danych dla backupu maszyn wirtualnych,
- system ma umożliwiać hot-backup aplikacji pracujących na maszynach wirtualnych z wykorzystaniem technologii VSS po stronie hypervisora bez konieczności instalacji agentów na każdej z maszyn wirtualnych,
- powyższa funkcjonalność ma umożliwiać hot-backup przynajmniej takich aplikacji jak: Mictosoft Exchange, Microsoft SQL Server, Microsoft Sharepoint oraz bazy danych Oracle,
- system ma umożliwiać eksport pliku VHD z przeprowadzonego backupu na maszynę z systemem Windows 7 lub Windows 2008 celem zamontowania pliku obrazu i odzyskania poszczególnych plików z obrazu maszyny wirtualnej,
- administrator ma mieć możliwość wyboru pomiędzy przynajmniej dwoma algorytmami kompresji, przy czym produkt ma umożliwiać wybór minimum algorytmów LZRW1 oraz LZRW3-A.

2. Backup środowiska wirtualnego VMware vSphere:

- agent backupu ma wspierać hot-backup (backup w czasie pracy) dla platformy wirtualizacyjnej VMware vSphere w wersjach ESXi 4.x, 5.x, ESX 4.x, vCenter 4.0, 4.1, 5.x,
- Agent backupu ma wspierać obsługę środowiska wirtualizacji vStorage na platformach CentOS 5, Red Hat Enterprise Linux 5, 6, SUSE Enterprise Server 10, 11, Windows Server 2003 SP2, Windows Server 2008 SP1 and R2, Windows Desktop: 7, Vista, XP SP3,

- funkcjonalność agenta backupu ma umożliwiać backup zarówno zatrzymanych jak również pracujących maszyn wirtualnych bez konieczności instalacji agenta na każdej z tych maszyn (backup na poziomie hypervisora),
- backup ma być możliwy zarówno dla całych obrazów maszyn wirtualnych, jak i na poziomie poszczególnych wykorzystanych bloków,
- backup ma być realizowany jako backup pełny, jako backup przyrostowy i dyferencyjny na poziomie bloków,
- agent backupu ma umożliwiać backup tylko danych fizycznie zapisanych na wirtualnym dysku,
- agent backupu ma zapewniać możliwość przywracania danych na poziomie poszczególnych plików oraz folderów w systemach Windows i Linux dla maszyn wirtualnych (możliwość wyodrębnienia dowolnego pliku/plików oraz katalogu/katalogów) z backupu obrazu maszyny wirtualnej,
- przywracanie plików z maszyny wirtualnej ma być niezależne i możliwe bez konieczności użycia platformy VMware (ESX lub vCenter),
- przywracanie maszyn wirtualnych ma być możliwe z przekierowaniem Hypervisora (zmiana miejsca docelowego dla odtwarzanego backupu) , jak również ma zapewnić możliwość wyboru data center, klastra lub hosta docelowego,
- agent backupu ma pozwalać na wykonanie backupu na poziomie bloków przy wsparciu technologi Raw Device Mapping (RDM) wraz z mechanizmem Changed Block Tracking (CBT),
- agent backupu ma integrować się z oprogramowaniem vCenter pozwalając na zarządzanie backupem na kilku hostach fizycznych,
- agent backupu ma wspierać rozwiązanie vApp, zapewniając backup grupy wspólnie pracujących maszyn,
- system ma zapewniać zarządzanie zadaniami backupu i przywracania dla platformy wirtualnej z poziomu przeglądarki internetowej.
- system ma wspierać wiele mechanizmów transportu, w szczególności system ma wspierać backup maszyn wirtualnych bez konieczności użycia sieci LAN (z wykorzystaniem sieci SAN), za pośrednictwem wirtualnej sieci LAN lub bezpośrednio na urządzenie podłączone za pośrednictwem interfejsu SCSI,
- system ma mieć możliwość uaktywnienia mechanizmu deduplikacji danych dla backupu maszyn wirtualnych,
- funkcjonalność deduplikacji ma być możliwa zarówno na poziomie centralnego serwera backupu jak i po stronie backupowanej maszyny. Funkcjonalność ta ma być definiowana (także włączana lub wyłączana) na poziomie pojedynczego zadania backupu,
- system ma mieć możliwość uaktywnienia kompresji danych dla backupu maszyn wirtualnych,
- administrator ma mieć możliwość wyboru pomiędzy przynajmniej dwoma algorytmami kompresji, przy czym produkt ma umożliwiać wybór minimum algorytmów LZRW1 oraz LZRW3-A.

Założenia dodatkowe - system musi posiadać licencję na archiwizację nielimitowanej ilości instancji usług MySQL, PostgresSQL, Groupwise, eDirectory oraz LDAP. Licencja ma umożliwiać korzystanie z technologii Remote Storage Option opisanej w dalszych punktach.

1. **Backup baz danych MySQL:**
   - Agent backupu ma wspierać hot-backup (backup w czasie pracy) dla bazy danych MySQL w wersjach 3.23 i nowszych na platformach AIX, FreeBSD, NetBSD, HP-UX, Linux, Mac OS, Tru64 i Windows.
   - Backup ma być możliwy zarówno dla całych baz danych, jak również dla poszczególnych tabel.

- System ma wspierać także backup dziennika binarnego (binary-log), celem późniejszego odtworzenia bazy do stanu z momentu wykonywania kopii zapasowej.
- Backup ma być realizowany jako backup pełny, jako backup przyrostowy oraz dyferencyjny.
- System ma mieć możliwość uaktywnienia mechanizmu deduplikacji danych dla backupu bazy danych MySQL.
- Funkcjonalność deduplikacji ma być możliwa zarówno na poziomie centralnego serwera backupu jak i po stronie backupowanej maszyny. Funkcjonalność ta ma być definiowana (także włączana lub wyłączana) na poziomie pojedynczego zadania backupu.
- System ma mieć możliwość uaktywnienia kompresji danych dla backupu bazy danych MySQL.
- Administrator ma mieć możliwość wyboru pomiędzy przynajmniej dwoma algorytmami kompresji, przy czym produkt ma umożliwiać wybór minimum algorytmów LZRW1 oraz LZRW3-A.

2. Backup baz danych danych PostgreSQL:

- Agent backupu ma wspierać hot-backup (backup w czasie pracy) dla bazy danych PostgreSQL w wersjach 7.2 i nowszych na platformach FreeBSD, NetBSD, OpenBSD, Linux, Solaris.
- Backup ma być możliwy zarówno dla całych instancji, jak również dla poszczególnych baz danych.
- Backup ma być realizowany jako backup pełny.
- System ma mieć możliwość uaktywnienia mechanizmu deduplikacji danych dla backupu bazy danych PostgreSQL.
- Funkcjonalność deduplikacji ma być możliwa zarówno na poziomie centralnego serwera backupu jak i po stronie backupowanej maszyny. Funkcjonalność ta ma być definiowana (także włączana lub wyłączana) na poziomie pojedynczego zadania backupu.
- System ma mieć możliwość uaktywnienia kompresji danych dla backupu bazy danych PostgreSQL.
- Administrator ma mieć możliwość wyboru pomiędzy przynajmniej dwoma algorytmami kompresji, przy czym produkt ma umożliwiać wybór minimum algorytmów LZRW1 oraz LZRW3-A.

3. Backup usług Novell Groupwise:

- Agent backupu ma wspierać hot-backup (backup w czasie pracy) dla usługi Novell Groupwise w dowolnej wersji zainstalowanej na systemach SLES 10, SLES 11, OES2, OES11 oraz Netware 6.5.
- Backup usługi Novell Groupwise ma być możliwy zarówno z wykorzystaniem dedykowanego API SMS TSA, jak również poprzez standardowy backup plikowy.
- Backup na poziomie API SMS TSA powinien być możliwy także w czasie gdy plik jest otwarty (kompatybilność z funkcją Novell CopyOnWrite).
- Backup Novell Groupwise ma być realizowany jako backup pełny, inkrementacyjny oraz dyferencyjny.
- System powinien wspierać odtwarzanie na poziomie domeny primary, na poziomie domeny secondary, na poziomie post office, na poziomie indywidualnej bazy danych, na poziomie usuniętych obiektów ze skrzynki.
- System powinien wspierać odtwarzanie pliku z jednoczesnym przekierowaniem na inną maszynę (także wówczas, gdy maszyna nie posiada zainstalowanego środowiska Groupwise).
- System powinien wspierać odtwarzanie katalogu Novell Groupwise z jednoczesnym przekierowaniem go na inną maszynę.

- System powinien umożliwiać backup także wówczas, gdy środowisko Novell Groupwise pracuje w oparciu o klaster
- System ma mieć możliwość uaktywnienia mechanizmu deduplikacji danych dla backupu środowiska Novell Groupwise.
- Funkcjonalność deduplikacji ma być możliwa zarówno na poziomie centralnego serwera backupu jak i po stronie backupowanej maszyny. Funkcjonalność ta ma być definiowana (także włączana lub wyłączana) na poziomie pojedynczego zadania backupu.
- System ma mieć możliwość uaktywnienia kompresji danych dla backupu środowiska Novell Groupwise.
- Administrator ma mieć możliwość wyboru pomiędzy przynajmniej dwoma algorytmami kompresji, przy czym produkt ma umożliwiać wybór minimum algorytmów LZRW1 oraz LZRW3-A.

4. Backup usług Novell eDirectory:

- Agent backupu ma wspierać hot-backup (backup w czasie pracy) dla usługi Novell eDirectory w dowolnej wersji zainstalowanej na systemach SLES 10, SLES 11, OES2, OES11 oraz Netware 6.5.
- Backup usługi Novell eDirectory ma być możliwy zarówno z wykorzystaniem dedykowanego API SMS TSA, jak również poprzez standardowy backup plikowy.
- Backup na poziomie API SMS TSA powinien być możliwy także w czasie gdy plik jest otwarty (kompatybilność z funkcją Novell CopyOnWrite).
- Backup Novell eDirectory ma być realizowany jako backup pełny.
- System powinien umożliwiać backup także wówczas, gdy środowisko Novell eDirectory pracuje w oparciu o klaster
- System ma mieć możliwość uaktywnienia mechanizmu deduplikacji danych dla backupu środowiska Novell eDirectory.
- Funkcjonalność deduplikacji ma być możliwa zarówno na poziomie centralnego serwera backupu jak i po stronie backupowanej maszyny. Funkcjonalność ta ma być definiowana (także włączana lub wyłączana) na poziomie pojedynczego zadania backupu.
- System ma mieć możliwość uaktywnienia kompresji danych dla backupu środowiska Novell eDirectory.
- Administrator ma mieć możliwość wyboru pomiędzy przynajmniej dwoma algorytmami kompresji, przy czym produkt ma umożliwiać wybór minimum algorytmów LZRW1 oraz LZRW3-A.

5. Backup usług serwera LDAP:

- Agent backupu ma wspierać hot-backup (backup w czasie pracy) dla serwera OpenLDAP oraz innych serwerów LDAP zgodnych z wersją 3 tego protokołu (np. Novell OES eDirectory).
- Backup ma być możliwy dla całego katalogu struktury LDAP jak również dla poszczególnych jego elementów z możliwością wyboru CN lub OU do backupu.
- Backup ma być realizowany jako backup pełny oraz backup przyrostowy dla każdego z elementów struktury LDAP.
- Proces odtwarzania wybranych elementów, jak również całego katalogu LDAP nie powinien wymagać zatrzymywania ani restartu usługi katalogowej.
- Konfiguracja danych autoryzacji do usługi katalogowej LDAP powinna być możliwa zarówno z poziomu pliku konfiguracyjnego agenta, jak również z poziomu interfejsu Web.
- Agent backupu musi umożliwiać pełne odtworzenie struktury katalogu LDAP do momentu w którym wykonano backup (odrzucenie wpisów dodanych w późniejszym okresie) jak również odtwarzanie z zachowaniem tychże wpisów (z nadpisaniem wpisów uszkodzonych).

- Administrator ma mieć możliwość wyboru pomiędzy przynajmniej dwoma algorytmami kompresji, przy czym produkt ma umożliwiać wybór minimum algorytmów LZRW1 oraz LZRW3-A.

Wyżej zamawiany system archiwizacji danych powinien również umożliwiać:

- korzystanie z lokalnych zasobów (dysk twardy, napęd taśmowy, biblioteka taśmowa) każdego z klientów backupu na potrzeby zapisu danych backupowanych,
- udostępnione zasoby dyskowe klientów muszą być zupełnie niezależne od zasobów serwera backupu,
- zapis danych w zasobach serwera mediów musi odbywać bez pośrednictwa głównego serwera backupu (Niedopuszczalne jest, aby dane przesyłane pomiędzy klientem backupu a serwerem mediów transferowane były pośrednio przez główny serwer backupu),
- funkcja udostępniania zasobów powinna dawać dostęp do zasobów lokalnych danego klienta backupu jemu samemu oraz każdemu z pozostałych klientów,
- Klient udostępniający swoje zasoby dyskowe musi zostać wypromowany do roli serwera mediów,
- system ma umożliwiać promocję każdego z klientów zarejestrowanych w centralnym systemie backupu do funkcji serwera mediów, który może posłużyć do składowania backupu z innych klientów,
- powyższa funkcja ma umożliwiać promocję klienta do funkcji serwera mediów z wykorzystaniem dedykowanej funkcji interfejsu Web, w szczególności niedopuszczalne jest, aby konieczne było modyfikowanie plików konfiguracyjnych klienta oraz serwera a także konieczność zmian na samym kliencie,
- funkcja serwera mediów ma umożliwiać wykorzystanie zarówno lokalnych zasobów dyskowych każdego z klientów, jak również napędu taśmowego oraz biblioteki taśmowej do nich podłączonych celem zapisania na nich backupu z pozostałych klientów.
- jedynym ograniczeniem skorzystania z funkcjonalności promocji klienta do roli serwera mediów może być licencja,
- system ma umożliwiać wykorzystanie zasobów w ramach sieci SAN i umożliwiać wykonywania zadań backupu z wykorzystaniem serwera mediów z pominięciem sieci LAN.
- funkcja zdalnego udostępniania zasobów musi współpracować z klientami pracującymi pod kontrolą systemów z rodziny Linux (niezależnie od wersji i dystrybucji), Solaris, AIX i systemami z rodziny Windows (co najmniej Windows Vista, 7, Server 2000, Server 2003 i Server 2008),
- zarządzanie udostępnianymi przez serwer mediów zasobami musi odbywać się przez poprzez centralną konsolę Web serwera backupu.
- Administrator ma mieć możliwość wykorzystania zasobów serwera mediów bezpośrednio na potrzeby zadań backupu, jak i na potrzeby replikacji danych.

Zamawiający wymaga w ramach dostawy, uruchomienia i wdrożenia w siedzibie zamawiającego systemu backupu obejmujących również sporządzenie dokumentacji technicznej. Zamawiający wymaga w ramach dostawy świadczenia wsparcia technicznego w systemie 8x5.