*Załącznik nr 7 do SWZ*

**Opis przedmiotu zamówienia**

**Ogólne cechy rozwiązania i backup środowisk wirtualnych**

**Wymagania ogólne**

* Zamawiający wymaga dostarczenia kompletnego systemu do archiwizacji danych wraz z usługa wsparcia wdrożeniowego i powdrożeniowego świadczonego przez Dostawcę (60 godzin biznesowych [pn-pt w godz. 08:00 – 16:00], do wykorzystania w ciągu roku kalendarzowego od podpisania przez Strony umowy). Usługa konsultacyjna świadczona zdalnie, za pomocą środków elektronicznych (np. interaktywnych komunikatorów on-line, telefonu lub poczty e-mail) lub w siedzibie Wykonawcy, polegać będzie na asyście personelowi UKW, podczas wdrażania zamawianego produktu (on-line lub na miejscu, po wcześniejszym uzgodnieniu tego faktu przez Strony, w trybie operacyjnym: mail, telefon - przewiduje się co najmniej 80% świadczenia tej usługi w trybie zdalnym) oraz jego utrzymania w środowisku produkcyjnym, w zakresie czasowym do jednego roku kalendarzowego od podpisania przez Strony umowy. **Czas reakcji Wykonawcy na zgłoszenie w zakresie wsparcia Zamawiającego** (e-mail, telefon lub dedykowany portal WWW Wykonawcy): najpóźniej next business day. Wykonawca zobowiązuje się również wspierać Zamawiającego, jeżeli zajdzie konieczność zarejestrowania zgłoszenia przez Zamawiającego w portalu Producenta lub złoży takie zgłoszenie w imieniu Zamawiającego, po wcześniejszym ustaleniu operacyjnym z Zamawiającym sposobu postępowania w danej sytuacji. W sprawach technicznych usługa wsparcia świadczona będzie przez wykwalifikowany personel Wykonawcy, posiadający wiedzę i doświadczenie w zakresie świadczenia wsparcia, zgodnie z oficjalną polityką Producenta systemu do archiwizacji danych cyfrowych.
* Zamawiający wymaga dostarczenia oprogramowania umożliwiającego wykonywanie backupu z minimum 120 hostów (poziom OS) lub maszyn wirtualnych (poziom OS), niezależnie od:

- ilości posiadanej liczby rdzenie obliczeniowych na danym hoście / maszynie wirtualnej lub pamięci RAM;

- ilości hostów wirtualnych;

- Zamawiający wymaga możliwości elastycznego przeniesienia powyższych licencji z nieużywanego OS (wyjętego z polityki backup) na nową maszynę fizyczną lub wirtualną, która zostanie objęta polityką backupową. Typ licencji: licencja pozycjonowana jako „enterprise” lub równoważna do zastosowań profesjonalnych w Data Center.

* Dostarczane rozwiązanie musi umożliwiać poprawne funkcjonowanie, umożliwiające wykonywanie kopii zapasowych z w/w 120 OS. Tj. zamawiający wymaga od strony oprogramowania, w tym dostarczanego systemu (OS) lub DB, by ich planowana ilość w ofercie lub licencje nie ograniczały tej możliwości.
* Oprogramowanie musi umożliwiać wykonanie łącznie minimum 50TB danych netto, ze środowiska objętego backupem (dane na systemach plików lub cloud). Oprogramowanie nie może ograniczać ilości przechowywanych danych, jako kopii zapasowych (backupu).
* Zamawiający wymaga dostarczenia produktu, który umożliwi instalację oprogramowania nadzorczego oraz dodatkowego oprogramowania monitorującego / raportującego (jeżeli stanowi ono osobną część oferowanego rozwiązania) – zgodnie z niniejszą specyfikacją, na serwerze fizycznym lub w środowisku wirtualnym, minimum VMware w systemie do zastosowań serwerowych MS Windows lub Linux. Jeżeli wymagane jest dostarczenie takiego systemu (lub systemów) operacyjnego (czyli nie są to komponenty OS OpenSource) Zamawiający wymaga jego dostarczenia z licencją umożliwiającą uruchomienie tego systemu lub systemów na serwerze wirtualnym w środowisku VMware - parametry hosta fizycznego: min. 20 core (2 procesory fizyczne x86 po 10 core każdy) i możliwością jego aktualizacji wersji przez minimum 1 rok (z możliwością przedłużenia o minimum dwa lata). Jeżeli do działania oprogramowania nadzorczego i lub / monitorującego i lub raportującego wymagana jest baza danych, zamawiający wymaga dostarczenia odpowiednich licencji dla jej funkcjonowania (w przypadku środowiska MS Windows i bazy MS SQL, wersja standard. Zamawiający informuje, że w przypadku systemów MS Windows, z uwagi na ograniczenia środowiska Zamawiającego maksymalną wersją systemu powinna być wersja MS Windows Server 2019). Nie dopuszcza się użycia licencji baz danych typu „express”. Zamawiający wymaga, by dostarczana baza danych była objęta możliwością aktualizacji do wyższej wersji przez minimum jeden rok, z możliwością przedłużenia o kolejne dwa lata.
* UWAGA: Zamawiający nie wymaga dostarczenia ewentualnych licencji na OS i DB w maksymalnej ilości rdzeni wskazanej powyżej. Zamawiający wykazał jedynie środowisko serwerowe, z którego skorzysta w celu instalacji komponentu oprogramowania nadzorczego (master) oraz systemu monitorującego i raportującego. Instalacja ta odbędzie się na maszynie wirtualnej w środowisku VMware. Wykonawca powinien wyskalować parametry licencyjne, tym samym wydajność, mając na uwadze niniejszą specyfikację (wymagania), biorąc również pod uwagę takie parametry, jak: ilość hostów, z których dane będą archiwizowane (do 120), ilość danych backupowanych netto (ok 50TB) z wszystkich hostów, ilość danych archiwizowanych przez system, przetwarzanych na nośnikach dyskowych (ok. 100-150 TB), docelową obsługę biblioteki taśmowej oraz płynne i wydajne generowanie statystyk i raportów.
* Zamawiający wymaga możliwości instalacji minimum jednego oprogramowania nadzorczego, tzw. master, według powyższych założeń oraz minimum 10 serwerów typu proxy/media (mogących pracować również w środowisku wirtualnym, z możliwością instalacji minimum w systemie Linux), umożliwiających wykonanie backupu jak najbliżej źródła. Należy dostarczyć wszystkie licencje, jeżeli są wymagane. Instancja uruchomiona na serwerze Linux nie może mieć słabszych parametrów funkcjonalnych, niż instancja uruchamiana w innych systemach operacyjnych.
* Oferowane oprogramowanie musi posiadać wszystkie **licencje wieczyste** oraz być **objęte wsparciem – kontraktem serwisowym (i gwarancją) producenta, na okres 36 miesięcy od podpisania przez Strony umowy, z możliwością przedłużenia o kolejne 24 miesiące** (nie dotyczy ewentualnych licencji dla OS lub DB, o których mowa jest powyżej i co do których określono osobne wymagania). Oprogramowanie musi pochodzić z oficjalnego kanału dystrybucji, uznawanego przez producenta. Podczas świadczenia niniejszego wsparcia, wymagany jest dostęp do strony producenta w celu uzyskania niezbędnych poprawek i aktualizacji oferowanego oprogramowania oraz materiałów dokumentacyjnych i wszelkiego know-how, które oferuje producent w ramach kontraktu serwisowego oraz także do posiadanych licencji. Zamawiający wymaga, by mógł aktywnie zgłaszać bezpośrednio do producenta oprogramowania (za pomocą dedykowanej strony WWW) zgłoszenia serwisowe w trybie 24/7. Wymagany czas reakcji na zgłoszenie: najpóźniej w trybie next business day.
* Oprogramowanie musi być produktem przeznaczonym (pozycjonowanym przez producenta) do obsługi systemowego środowisk DataCenter. Oferowany produkt musi znajdować się w kwadracie liderów Gartner Magic Quadrant for Data Center Backup and Recovery Solutions oraz na ogólnie dostępnej liście referencyjnej Gartner: https://www.gartner.com/reviews/market/data-center-backup-and-recovery-solutions i spełniać minimalne wymaganie : - minimalna liczba referencji 150, - minimalna ocena z referencji 4,5,
* Oprogramowanie musi współpracować z infrastrukturą VMware w wersji 5.5, 6.0, 6.5, 6.7 oraz 7.0 oraz Microsoft Hyper-V 2012, 2012 R2 i 2019. Wszystkie funkcjonalności w specyfikacji muszą być dostępne na wszystkich wspieranych platformach wirtualizacyjnych, chyba, że wyszczególniono inaczej
* Oprogramowanie musi współpracować z hostami zarządzanymi przez VMware vCenter oraz pojedynczymi hostam oraz w trybie klienckim – poza lub w środowisku zwirtualizowanym z maszynami opartymi o system MS Windows oraz Linux oraz Solaris x86 10/11 .
* Oprogramowanie musi współpracować z hostami zarządzanymi przez System Center Virtual Machine Manger, klastrami hostów oraz pojedynczymi hostami.
* Oprogramowanie musi zapewniać tworzenie kopii zapasowych z sieciowych urządzeń plikowych NAS opartych o SMB, CIFS i/lub NFS oraz bezpośrednio z serwerów plikowych opartych o system MS Windows i Linux.
* Oprogramowanie musi współpracować z napędami taśmowymi (tzw. bibliotekami LTO) podłączonymi do serwera za pomocą sieci SAN (kart HBA). Zamawiający wymaga dostarczenia wraz z ofertą pełnej listy wspieranych bibliotek taśmowych. Zamawiający wymaga, jeżeli oprogramowanie musi posiadać dodatkową licencję, dostarczenie niezbędnej licencji umożliwiającej podłączenie zewnętrznej biblioteki taśmowej (minimum dwóch bibliotek). Wspierane biblioteki muszą obsługiwać taśmy minimum LTO 8. Przedmiotem niniejszego postępowania nie jest dostarczenie biblioteki taśmowej.
* Oprogramowanie musi umożliwiać tworzenie polityk backupowych, umożliwiających wykonywanie kopii w systemie D2D2t (disk to disk to tape), według zaplanowanego harmonogramu – w sposób automatyczny.
* Oprogramowanie musi być niezależne sprzętowo i umożliwiać wykorzystanie dowolnej platformy serwerowej i dyskowej.
* Oprogramowanie musi tworzyć “samowystarczalne” archiwa do odzyskania których nie wymagana jest osobna baza danych z metadanymi deduplikowanych bloków
* Oprogramowanie musi pozwalać na tworzenie kopii zapasowych w trybach: Pełny, pełny syntetyczny, przyrostowy i odwrotnie przyrostowy (tzw. reverse-inremental)
* Oprogramowanie musi mieć mechanizmy deduplikacji i kompresji w celu zmniejszenia wielkości archiwów. Włączenie tych mechanizmów nie może skutkować utratą jakichkolwiek funkcjonalności wymienionych w tej specyfikacji
* Oprogramowanie nie może przechowywać danych o deduplikacji w centralnej bazie. Utrata bazy danych używanej przez oprogramowanie nie może prowadzić do utraty możliwości odtworzenia backupu. Metadane deduplikacji muszą być przechowywane w plikach backupu.
* Oprogramowanie musi zapewniać warstwę abstrakcji nad poszczególnymi urządzeniami pamięci masowej, pozwalając utworzyć jedną wirtualną pulę pamięci na kopie zapasowe. Wymagane jest wsparcie dla nieograniczonej liczby pamięci masowych to takiej puli.
* Oprogramowanie musi pozwalać na rozszerzenie lokalnej przestrzeni backupowej poprzez integrację z co najmniej Microsoft Azure Blob, Amazon S3 oraz z innymi kompatybilnymi z S3 macierzami obiektowymi. Proces migracji danych powinien być zautomatyzowany. Jedynie unikalne bloki mogą być przesyłane w celu oszczędności pasma oraz przestrzeni na przechowywane dane. Funkcjonalność ta nie może mieć wpływu na możliwości odtwarzania danych.
* W trybie pracy z maszynami wirtualnymi - oprogramowanie nie może instalować żadnych stałych agentów wymagających wdrożenia czy upgradowania wewnątrz maszyny wirtualnej dla jakichkolwiek funkcjonalności backupu lub odtwarzania.
* Oprogramowanie musi mieć możliwość uruchamiania dowolnych skryptów przed i po zadaniu backupowym lub przed i po wykonaniu zadania snapshota.
* Oprogramowanie musi oferować portal samoobsługowy, umożliwiający odtwarzanie użytkownikom wirtualnych maszyn, i baz danych MS SQL oraz Oracle (w tym odtwarzanie point-in-time).
* Zamawiający rozważa również wdrożenie platformy MS Exchange, dla której odzyskiwanie obiektów MS Exchange odbywać się może przy pomocy konsoli instalowanej na maszynie z systemem operacyjnym Windows.
* Oprogramowanie musi zapewniać możliwość delegacji uprawnień do odtwarzania na portalu
* Oprogramowanie musi mieć możliwość integracji z innymi systemami poprzez wbudowane RESTful API.
* Oprogramowanie musi mieć wbudowane mechanizmy backupu konfiguracji w celu prostego odtworzenia systemu po całkowitej reinstalacji
* Oprogramowanie musi mieć wbudowane mechanizmy szyfrowania zarówno plików z backupami jak i transmisji sieciowej. Włączenie szyfrowania nie może skutkować utratą jakiejkolwiek funkcjonalności wymienionej w tej specyfikacji
* Oprogramowanie musi posiadać mechanizmy chroniące przed utratą hasła szyfrowania.
* Oprogramowanie musi wspierać backup maszyn wirtualnych używających współdzielonych dysków VHDX na Hyper-V (shared VHDX).
* Oprogramowanie musi posiadać architekturę klient/serwer z możliwością instalacji wielu instancji konsoli administracyjnych.
* System musi umożliwiać klasyczne wykonanie backupu w oparciu o sieć LAN - IP (także sieć typu vmkernel w środowiskach VMware) oraz sieć SAN. Dalsze wytyczne w tym zakresie zostały zamieszczone poniżej.

**Wymagania RPO**

* Oprogramowanie musi wykorzystywać mechanizmy Change Block Tracking na wszystkich wspieranych platformach wirtualizacyjnych. Mechanizmy muszą być certyfikowane przez dostawcę platformy wirtualizacyjnej
* Oprogramowanie musi wykorzystywanać mechnizmy śledzenia zmienionych plików przy zabezpieczaniu udziałów plikowych.
* Oprogramowanie musi oferować możliwość sterowania obciążeniem storage'u produkcyjnego tak aby nie przekraczane były skonfigurowane przez administratora backupu poziomy latencji. Funkcjonalność ta musi być dostępna na wszystkich wspieranych platformach wirtualizacyjnych
* Oprogramowanie musi oferować ten mechanizm z dokładnością do pojedynczego datastoru
* Oprogramowanie musi automatycznie wykrywać i usuwać snapshoty-sieroty (orphaned snapshots), które mogą zakłócić poprawne wykonanie backupu. Proces ten nie może wymagać interakcji administratora
* Oprogramowanie musi zapewniać tworzenie kopii zapasowych z bezpośrednim wykorzystaniem snapshotów macierzowych. Musi też zapewniać odtwarzanie maszyn wirtualnych z takich snapshotów. Proces wykonania kopii zapasowej nie może wymagać użycia jakichkolwiek hostów tymczasowych. Opisana funkcjonalność powinna działać w środowisku VMware i być dostępna dla następujących macierzy: HPE, Dell EMC, NetApp, Cisco, IBM, Lenovo, Fujitsu, Huawei, , Pure Storage.
* Oprogramowanie musi posiadać wsparcie dla VMware vSAN potwierdzone odpowiednią certyfikacją VMware.
* Oprogramowanie musi wspierać kopiowanie backupów na taśmy wraz z pełnym śledzeniem wirtualnych maszyn.
* Oprogramowanie musi posiadać wsparcie dla NDMP.
* Oprogramowanie musi mieć możliwość tworzenia retencji GFS (Grandfather-Father-Son)
* Oprogramowanie musi umieć korzystać z protokołu DDBOOST w przypadku, gdy repozytorium backupów jest umiejscowione na Dell EMC DataDomain. Funkcjonalność powinna wspierać łącze sieciowe lub FC.
* Oprogramowanie musi umieć korzystać z protokołu Catalyst (w tym Catalyst Copy) w przypadku, gdy repozytorium backupów jest umiejscowione na HPE StoreOnce. Funkcjonalność powinna wspierać łącze sieciowe lub FC.
* Oprogramowanie musi wspierać BlockClone API w przypadku użycia Windows Server 2016 lub 2019 z systemem pliku ReFS jako repozytorium backupu. Podobna funkcjonalność musi być zapewniona dla repozytoriów opartych o linuxowy system plików XFS.
* Repozytoria oparte o XFS muszą pozwalać na zmienność danych przez określoną ilość czasu (tzw Immutability).
* Oprogramowanie musi mieć możliwość kopiowania backupów oraz replikacji wirtualnych maszyn z wykorzystaniem wbudowanej akceleracji WAN.
* Oprogramowanie musi mieć możliwość replikacji asynchronicznej włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere pomiędzy hostami ESXi oraz pomiędzy hostami Hyper-V. Dodatkowo oprogramowanie musi mieć możliwość użycia plików kopii zapasowych jako źródła replikacji.
* Oprogramowanie musi mieć możliwość replikacji ciągłej, opartej o VMware VAIO, włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere. Dla replikacji ciągłej musi być możliwośc zdefiniowania dziennika pozwalającego na odzyskanie danych z dowolnego punku w ramach ustalonego parametru RPO.
* Oprogramowanie musi umożliwiać przechowywanie punktów przywracania dla replik
* Oprogramowanie musi umożliwiać wykorzystanie istniejących w infrastrukturze wirtualnych maszyn jako źródła do dalszej replikacji (replica seeding)
* Oprogramowanie musi wykorzystywać wszystkie oferowane przez hypervisor tryby transportu (sieć, hot-add, LAN Free-SAN)

**Wymagania RTO**

* Oprogramowanie musi umożliwiać jednoczesne uruchomienie wielu maszyn wirtualnych bezpośrednio ze zdeduplikowanego i skompresowanego pliku backupu, z dowolnego punktu przywracania, bez potrzeby kopiowania jej na storage produkcyjny. Funkcjonalność musi być oferowana dla środowisk VMware oraz Hyper-V niezależnie od rodzaju storage’u użytego do przechowywania kopii zapasowych.
* Dodatkowo dla środowiska vSphere i Hyper-V powyższa funkcjonalność powinna umożliwiać uruchomianie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna)
* Oprogramowanie musi pozwalać na migrację on-line tak uruchomionych maszyn na storage produkcyjny. Migracja powinna odbywać się mechanizmami wbudowanymi w hypervisor. Jeżeli licencja na hypervisor nie posiada takich funkcjonalności - oprogramowanie musi realizować taką migrację swoimi mechanizmami
* Oprogramowanie musi pozwalać na zaprezentowanie pojedynczego dysku bezpośrednio z kopii zapasowej do wybranej działającej maszyny wirtualnej vSpehre.
* Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny, plików konfiguracji i dysków.
* Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny bezpośrednio do co najmniej Microsoft Azure, Microsoft Azure Stack oraz Amazon EC2.
* Oprogramowanie musi umożliwić odtworzenie plików na maszynę operatora, lub na serwer produkcyjny bez potrzeby użycia agenta instalowanego wewnątrz wirtualnej maszyny. Funkcjonalność ta nie powinna być ograniczona wielkością i liczbą przywracanych plików
* Oprogramowanie musi mieć możliwość odtworzenia plików bezpośrednio do maszyny wirtualnej poprzez sieć, przy pomocy VIX API dla platformy VMware i PowerShell Direct dla platformy Hyper-V.
* Oprogramowanie musi wspierać odtwarzanie pojedynczych plików minimum z następujących systemów plików:
* Linux: ext2, ext3, ext4, ReiserFS, JFS, XFS, Btrfs
* BSD: UFS, UFS2
* Solaris: ZFS, UFS
* Mac: HFS, HFS+
* Windows: NTFS, FAT, FAT32, ReFS
* Novell OES: NSS
* Oprogramowanie musi wspierać przywracanie plików z partycji Linux LVM oraz Windows Storage Spaces.
* Oprogramowanie musi umożliwiać szybkie granularne odtwarzanie obiektów aplikacji bez użycia jakiegokolwiek agenta zainstalowanego wewnątrz maszyny wirtualnej.
* Oprogramowanie musi wspierać granularne odtwarzanie obiektów Active Directory takich jak konta komputerów, konta użytkowników oraz pozwalać na odtworzenie haseł.
* Oprogramowanie musi wspierać granularne odtwarzanie dowolnych atrybutów, rekordów DNS zintegrowanych z AD, Microsoft System Objects, certyfikatów CA oraz elementów AD Sites.
* Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Exchange 2010 i nowszych (dowolny obiekt w tym obiekty w folderze "Permanently Deleted Objects"),
* Oprogramowanie musi wspierać przywracanie danych Exchange do oryginalnego środowiska
* Oprogramowanie musi wspierać granularne odtwarzanie Microsoft SQL 2005 i nowszych
* Oprogramowanie musi wspierać odtworzenie point-in-time wraz z możliwością przywrócenia bazy do oryginalnego środowiska
* Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Sharepoint 2010 i nowszych
* Oprogramowanie musi wspierać odtworzenia elementów, witryn, uprawnień dla witryn Sharepoint.
* Oprogramowanie musi wspierać granularne odtwarzanie baz danych Oracle z opcją odtwarzanie point-in-time wraz z włączonym Oracle DataGuard. Funkcjonalność ta musi być dostępna dla baz uruchomionych w środowiskach Windows oraz Linux.
* Oprogramowanie musi pozwalać na zaprezentowanie oraz migrację online baz MS SQL oraz Oracle bezpośrednio z pliku kopii zapasowej do działającego serwera bazodanowego
* Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez Oracle RMAN.
* Oprogramowanie musi wspierać także specyficzne metody odtwarzania w tym "reverse CBT" oraz odtwarzanie z wykorzystaniem sieci SAN

**Ograniczenie ryzyka**

* Oprogramowanie musi dawać możliwość stworzenia laboratorium (izolowane środowisko) dla vSphere i Hyper-V używając wirtualnych maszyn uruchamianych bezpośrednio z plików backupu.
* Dla VMware’a oprogramowanie musi pozwalać na uruchomienie takiego środowiska bezpośrednio ze snapshotów macierzowych stworzonych na wspieranych urządzeniach.
* Oprogramowanie musi umożliwiać weryfikację odtwarzalności wielu wirtualnych maszyn jednocześnie z dowolnego backupu według własnego harmonogramu w izolowanym środowisku. Testy powinny uwzględniać możliwość uruchomienia dowolnego skryptu testującego również aplikację uruchomioną na wirtualnej maszynie. Testy muszą być przeprowadzone bez interakcji z administratorem
* Oprogramowanie musi mieć podobne mechanizmy dla replik w środowisku vSphere
* Oprogramowanie musi umożliwiać integrację z oprogramowaniem antywirusowym w celu wykonania skanu zawartości pliku backupowego przed odtworzeniem jakichkolwiek danych. Integracja musi być zapewniona minimalnie dla Windows Defender, Symantec Protection Engine oraz ESET NOD32.
* Oprogramowanie musi umożliwiać dwuetapowe, automatyczne, odtwarzanie maszyn wirtualnych z możliwością wstrzyknięcia dowolnego skryptu przed odtworzeniem danych do środowiska produkcyjnego.

**Monitoring i raportowanie**

**Monitoring**

* System musi zapewnić możliwość monitorowania środowiska wirtualizacyjnego opartego na VMware vSphere i Microsoft Hyper-V bez potrzeby korzystania z narzędzi firm trzecich
* System musi umożliwiać monitorowanie środowiska wirtualizacyjnego VMware w wersji: 5.5, 6.0, 6.5, 6.7 and 7.0 – zarówno w bezpłatnej wersji ESXi jak i w pełnej wersji ESX/ESXi zarządzane przez konsole vCenter Server lub pracujące samodzielnie.
* System musi umożliwiać monitorowanie środowiska wirtualizacyjnego Microsoft Hyper-V 2008 R2 SP1, 2012, 2012 R2, 2016 oraz 2019 zarówno w wersji darmowej jak i zawartej w płatnej licencji Microsoft Windows Server zarządzane poprzez System Center Virtual Machine Manager lub pracujące samodzielnie.
* System musi mieć status „VMware Ready” i być przetestowany i certyfikowany przez VMware.
* System musi umożliwiać kategoryzacje obiektów infrastruktury wirtualnej niezależnie od hierarchii stworzonej w vCenter.
* System musi umożliwiać tworzenie alarmów dla całych grup wirtualnych maszyn jak i pojedynczych wirtualnych maszyn.
* System musi dawać możliwość układania terminarza raportów i wysyłania tych raportów przy pomocy poczty elektronicznej w formacie HTML oraz Excel.
* System musi dawać możliwość podłączenia się do kilku instancji vCenter Server i serwerów Hyper-V jednocześnie, w celu centralnego monitorowania wielu środowisk.
* System musi mieć wbudowane predefiniowane zestawy alarmów wraz z możliwością tworzenia własnych alarmów i zdarzeń przez administratora.
* System musi mieć wbudowane połączenie z bazą wiedzy opisującą problemy z predefiniowanych alarmów.
* System musi mieć centralną konsolę z sumarycznym podglądem wszystkich obiektów infrastruktury wirtualnej (ang. Dashboard).
* System musi mieć możliwość monitorowania platformy sprzętowej, na której jest zainstalowana infrastruktura wirtualna.
* System musi zapewnić możliwość podłączenia się do wirtualnej maszyny (tryb konsoli) bezpośrednio z narzędzia monitorującego.
* System musi mieć możliwość integracji z oprogramowaniem do tworzenia kopii zapasowych tego samego producenta.
* System musi mieć możliwość monitorowania obciążenia serwerów backupowych, ilości zabezpieczanych danych oraz statusu zadań kopii zapasowych, replikacji oraz weryfikacji odzyskiwalności maszyn wirtualnych.
* System musi oferować inteligentną diagnostykę rozwiązania backupowego poprzez monitorowanie logów celem wykrycia znanych problemów oraz błędów konfiguracyjnych w celu wskazania rozwiązania bez potrzeby otwierania zgłoszenia suportowego oraz bez potrzeby wysyłania jakichkolwiek danych diagnostycznych do producenta oprogramowania backupu.
* System musi mieć możliwość granularnego monitorowania infrastruktury, zależnego od uprawnień nadanym użytkownikom dla platformy VMware.
* System musi mieć możliwość monitorowania instancji VMware vCloud Director w wersji minimum 8.x i nowszych.

**Raportowanie**

* System raportowania musi umożliwić tworzenie raportów z infrastruktury wirtualnej bazującej na VMware ESX/ESXi 5.5, 6.0, 6.5, 6.7 oraz 7.0 vCenter Server 5.x oraz 6.x jak również Microsoft Hyper-V 2008 R2 SP1, 2012, 2012 R2, 2016 oraz 2019.
* System musi wspierać wiele instancji vCenter Server i Microsoft Hyper-V jednocześnie bez konieczności instalowania dodatkowych modułów.
* System musi być certyfikowany przez VMware i posiadać status „VMware Ready”.
* System musi być systemem bezagentowym. Nie dopuszcza się możliwości instalowania przez system agentów na monitorowanych hostach ESXi i Hyper-V.
* System musi mieć możliwość eksportowania raportów do formatów Microsoft Word, Microsoft Excel, Microsoft Visio, Adobe PDF.
* System musi mieć możliwość ustawienia harmonogramu kolekcji danych z monitorowanych systemów jak również możliwość tworzenia zadań kolekcjonowania danych ad-hoc.
* System musi mieć możliwość ustawienia harmonogramu generowania raportów i dostarczania ich do odbiorców w określonych przez administratora interwałach.
* System w raportach musi mieć możliwość uwzględniania informacji o zmianach konfiguracji monitorowanych systemów.
* System musi mieć możliwość generowania raportów z dowolnego punktu w czasie zakładając, że informacje z tego czasu nie zostały usunięte z bazy danych.
* System musi posiadać predefiniowane szablony z możliwością tworzenia nowych jak i modyfikacji wbudowanych.
* System musi mieć możliwość analizowania „przeszacowanych” wirtualnych maszyn wraz z sugestią zmian w celu optymalnego wykorzystania fizycznej infrastruktury.
* System musi mieć możliwość generowania raportów na podstawie danych uzyskanych z oprogramowania do tworzenia kopii zapasowych tego samego producenta.
* System musi mieć możliwość generowania raportu dotyczącego zabezpieczanych maszyn, zdefiniowanych zadań tworzenia kopii zapasowych oraz replikacji jak również wykorzystania zasobów serwerów backupowych.
* System musi mieć możliwość generowania raportu planowania pojemności (capacity planning) bazującego na scenariuszach ‘what-if’.
* System musi mieć możliwość granularnego raportowania infrastruktury, zależnego od uprawnień nadanym użytkownikom dla platformy VMware
* System musi mieć możliwość generowania raportów dotyczących tzw. migawek-sierot (orphaned snapshots).
* System musi mieć możliwość generowania personalizowanych raportów zawierających informacje z dowolnych predefiniowanych raportów w pojedynczym dokumencie.

**Backup serwerów fizycznych i stacji roboczych**

* Rozwiązanie musi wykonywać kopię zapasową systemu MS Windows, Linux oraz Solaris x86 10/11 (dla systemu operacyjnego Solaris Zamawiający przewidział wykluczenia, o których mowa jest w dalszej części tego opisu) wykorzystując agenta znajdującego się wewnątrz systemu operacyjnego.
* Rozwiązanie musi wspierać systemy operacyjne MS Windows w wersjach klienckich oraz serwerowych.
* Rozwiązanie musi wspierać co najmniej następujące dystrybucje systemów Linux:
* Debian, Ubuntu, RHEL, CentOS, Oracle Linux, SLES, Fedora, OpenSUSE
* Rozwiązanie musi wspierać systemy operacyjne MacOS
* Rozwiązanie musi wspierać wykonywanie kopi zapasowych następujących systemów plików:
* NTFS, ReFS, FAT32, ext2, ext3, ext4, ReiserFS, JFS, XFS, F2FS, Brtfs (dla kernela 3.16 i nowszych), APFS, HFS, HFS+, NILFS2.
* Rozwiązanie musi mieć możliwość instalacji oraz zarządzania wykorzystując tryb niezależny (per agent) jak również zcentralizowany (poprzez centralną konsolę zarządzającą).
* Rozwiązanie musi wspierać systemy oparte o Microsoft Failover Cluster.
* Rozwiązanie musi wspierać zabezpieczanie do oraz odzyskiwanie z urządzeń blokowych pozwalając na odzysk całej maszyny (tzw. bare metal recovery) wybranych wolumenów, oraz wybranych plików i folderów. Dla systemu operacyjnego Solaris backup oraz odzyskiwanie danych odbywać się może wyłącznie na poziomie plików i katalogów dla tego OS.
* Rozwiązanie musi wspierać backup podłączonych dysków USB.
* Kopia zapasowa całej maszyny oraz pojedynczych wolumenów musi być wykonywana na poziomie blokowym (nie dotyczy systemu operacyjnego Solaris, dla którego odzyskiwanie może być realizowane na poziomie plików i katalogów).
* Rozwiązanie musi pozwalać na przechowywanie kopii zapasowych na:
* Lokalnych (wewnętrznych) dyskach zabezpieczanej maszyny
* Direct Attached Storage (DAS), takich jak zewnętrzne dyski USB, eSATA lub Firewire
* Network Attached Storage (NAS) pozwalającym na wystawienie swoich zasobów poprzez SMB (CIFS) lub NFS.
* Zcentralizowanym repozytorium danych
* Bezpośrednio na zasobach Chmury (dla systemu operacyjnego Solaris backup do chmury może odbywać się automatycznie z pośrednictwem lokalnego repozytorium).
* Rozwiązanie musi wspierać deduplikacje oraz kompresję na źródle. Dane wysyłane na repozytorium muszą być już odpowiednio przetworzone. Zamawiający dopuszcza w tym miejscu wyjątek dla systemu operacyjnego Solaris (w przypadku OS Solaris w ramach przetwarzania danych, na źródle następować może kompresja danych wyłącznie przy pomocy Rle/Lz4/ZlibLow/ZlibHigh).
* Rozwiązanie musi wspierać kontrolę pasma sieciowego.
* Rozwiązanie musi wspierać ograniczenie wykonywania backupów dla konkretnych sieci bezprzewodowych (nie dotyczy OS Solaris).
* Rozwiązanie musi wspierać ograniczenia wykonywania backupów dla połączeń VPN (nie dotyczy OS Solaris).
* Rozwiązanie musi wspierać śledzenie zmienionych bloków podczas wykonywania blokowych kopii zapasowych. Dla systemów Windows technologia śledzenia bloków dla systemów serwerowych musi być certyfikowana przez Microsoft. Dla systemu operacyjnego Solaris backup oraz odzyskiwanie danych odbywać się może wyłącznie na poziomie plików i katalogów.
* Rozwiązanie musi wspierać skrypty wykonywane przed i po wykonaniu zadania oraz przed i po wykonaniu migawki na poziomie wolumenu.
* Rozwiązanie musi wspierać technologię BitLocker.
* Rozwiązanie musi wspierać uruchamianie z nośnika odtwarzania (dla systemu operacyjnego Solaris dopuszcza się możliwość realizacji odzyskiwania danych za pomocą agenta instalowanego w warstwie OS, na tym systemie).
* Rozwiązanie musi wspierać odzysk pojedynczych elementów aplikacji z jednoprzebiegowej kopii zapasowej dla:
* Microsoft Exchange 2010 i nowszych,
* Microsoft Active Directory 2003 i nowszych,
* Microsoft Sharepoint 2010 i nowszych,
* Microsoft SQL 2005 i nowszych,
* Oracle 11g i nowszych.
* Rozwiązanie musi wspierać odzysk do konkretnego punktu w czasie (point-in-time) dla wspieranych systemów bazodanowych.
* Rozwiązanie musi umożliwiać natychmiastowe publikowanie baz MS SQL poprzez bezpośrednie uruchomienie ich z pliku backupu.
* Rozwiązanie musi wspierać odzysk obrazów kopii zapasowych bezpośrednio do co najmniej Microsoft Azure, Microsoft Azure Stack oraz Amazon EC2.
* Rozwiązanie musi wspierać szyfrowanie za pomocą bezpiecznych (uznawanych powszechnie w dziedzinie cyber za bezpieczne) algorytmów szyfrowania.
* Rozwiązanie musi wspierać możliwość wykonywania kopii zapasowych stacji klienckich, lokalnie do repozytorium tymczasowego (cache) gdy połączenie sieciowe do głównego repozytorium kopii zapasowych jest niedostępne.
* Rozwiązanie musi posiadać funkcjonalność automatycznego zmniejszenia szybkości przetwarzania danych, aby nie dopuścić do obniżenia wydajności systemu zabezpieczanego
* Rozwiązanie musi posiadać ochronę przed ransomware poprzez automatyczne odmontowanie nośnika po wykonanym backupie stacji klienckiej.
* Rozwiązanie musi wspierać tworzenie wielu zadań backupowych.