**Zakup licencji do backupu środowiska DataCenter oraz wsparcia producenta**

Przedmiotem zapytania jest rozbudowa warstwy oprogramowania backup’owego umożliwiająca:

* realizację backupów w DataCenter w środowisku obejmującym sumarycznie 200 CPU, na eksploatowane urządzenia DD9400
* zabezpieczenie danych w trybie Continuous Data Protection środowiska VMware vSphere nie przekraczającego sumarycznie 200 CPU
* instalację wirtualnego deduplikatora (-ów) dedykowanego do przechowywania zabezpieczanych danych, min. pojemność netto oferowanego deduplikatora (bez uwzględnienia redukcji danych w oparciu o deduplikację) bądź sumy pojemności nie więcej niż 3-ech deduplikatorów musi wynosić 200TB, wymagana możliwość instalacji zarówno lokalnie jak i w Azure, GCP oraz AWS, w przypadku wymienionych środowisk chmurowych wymagane skalowanie pojedynczego urządzenia do 250 TB, wymagana bezpośrednia replikacja danych pomiędzy wirtualnym deduplikatorem oraz eksploatowanymi DD9400 sterowana poprzez oferowaną aplikację backup’ową a także eksploatowaną aplikację Power Protect Data Manager (w trybie Managed File Replication).

Wymagane licencjonowanie oferowanego oprogramowania powinno uwzględniać sumaryczną ilość 200 CPU zabezpieczanego środowiska bez ograniczeń dotyczących ilości zabezpieczanych danych (FET), ilości zabezpieczanych serwerów czy ilości używanych mediów dedykowanych do przechowywania danych.

Zarówno oprogramowanie jak i deduplikator powinny być dostarczone wraz z trzyletnim letnim wsparciem producenta świadczonym w trybie NBD.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Nazwa modułu | Identyfikator opcji | Nazwa opcji | Numery SKU | Liczba szt. |
|  |  |  |  |  |
| Dell EMC PowerProtect Data Manager Plus | GHG361X | Dell EMC PowerProtect Data Manager Plus Upgrade | [210-BBJW] | 1 |
| Original Purchase Date | GPLGDX8 | Original purchase AFTER Febuary 01, 2022 | [800-BBQV] | 1 |
| Current Capacity | G7A1L68 | Current Capacity PowerProtect Data Manager Plus=IA | [800-BBQV] | 50 |
| Capacity Licenses | GUXIZA6 | PowerProtect Data Manager Plus Socket=IA | [528-CSBT] | 200 |
| Sftwr Svcs-PPDM Plus (VP) | G94MRLV | ProSupport Plus PowerProtect Data Manager Plus Sftwr Spt-Maint, 36 Mies. | [487-BIVJ] | 1 |
| Instance Enablers | GD9FI24 | Instance Enablers=CA | [528-CRYV], [528-CRYX], [528-CRZJ] | 1 |
| Capacity Enablers | G524MWH | Capacity Enablers=CA | [142-BBFQ], [528-CPWX], [528-CPWY], [528-CPWZ], [528-CPXB], [528-CPXD], [528-CRYS], [528-CRYW], [528-CRYZ], [528-CRZC], [528-CRZG] | 200 |
| RecoverPoint for VM Replication | GDUEB3T | RecoverPoint for VMs=IA | [528-CRZF] | 200 |
| Cloud Snapshot Manager | G21S5Q7 | Cloud Snapshot Manager=IB | [141-BIBE] | 2000 |
| PP DDVE and Cloud Tier | GLHMY7S | PP DDVE and Cloud Tier=CC | [528-CPXC], [528-CPXF] | 200 |

**Uwarunkowania równoważności minimalnych funkcjonalności :**

Tabela nr 1

Wymagania dotyczące oprogramowania backupowego

|  |  |
| --- | --- |
| Lp. | Wymagania minimalne |
|  | Zamawiający wymaga dostarczenia, uruchomienia i wdrożenia oprogramowania do backupu środowiska DataCenter (baz danych, maszyn wirtualnych, serwerów plików, serwerów wolnostojących). |
|  | Wymagane jest dostarczenie wszystkich modułów oprogramowania backupowego tak, aby zapewnić backup całości wyspecyfikowanego środowiska oraz spełnić wszystkie wymienione w niniejszej tabeli funkcjonalności. |
|  | Wymagane jest dostarczenie licencji oprogramowania backupowego dla 200 procesorów fizycznych (zajętych socketów) w zabezpieczanych maszynach. Wymaga się aby wszystkie dostępne funkcjonalności oferowanego rozwiązania były odblokowane w ramach oferowanej licencji procesorowej. |
|  | Dostarczone licencje muszą umożliwiać backup/ odtwarzanie:* dowolnej liczby maszyn wirtualnych jako obrazów („image level”)
* agentowo, dowolnej liczby baz danych, plików, ze środka maszyn wirtualnych
* dowolnej liczby TB w zabezpieczanym środowisku.
 |
|  | Serwer backupu musi być zainstalowany jako maszyną wirtualna systemu VMware. |
|  | Serwer backupu musi być dostarczony w postaci gotowej maszyny wirtualnej  |
|  | Wymagana jest pełna integracja oferowanego rozwiązania z zaoferowanym deduplikatorem wirtualnym oraz eksploatowanymi deduplikatorami DD9400 |
|  | Wymaga się aby dla wszystkich rodzajów wspieranych środowisk, oferowane rozwiązanie wykonywało backup z deduplikacją na źródle na oferowany deduplikator a także deduplikatory DD9400 |
|  | Oprogramowanie backupowe musi zapewniać bezpośredni backup z każdej zabezpieczanej maszyny znajdującej się w sieci LAN bezpośrednio na oferowany deduplikator oraz DD9400 bez pośrednictwa jakichkolwiek innych serwerów. Powyższa funkcjonalność nie może wymagać dodatkowej licencji. |
|  | Backup z dededuplikacją na źródle musi być dostępny dla wszystkich typów danych w ramach oferowanego rozwiązania: pliki, bazy danych, obrazy maszyn wirtualnych, Kubernetes.  |
|  | Wymaga się aby oprogramowanie backupowe zapewniało szybki backup blokowy wielomilionowych systemów plików na maszynach Windows / Linux.W trakcie backupu oprogramowanie backupowe musi wykonywać kopie zapasowe fizycznych bloków a nie plików, jednocześnie wymagana jest możliwość odtworzenia * całego wolumenu
* pojedynczego pliku

Celem minimalizacji czasu backupu oprogramowanie backupowe nie może indeksować plików znajdujących się na zabezpieczanym wolumenie (zaindeksowanie wielu milionów plików powoduje duże wydłużenie czasu backupu). |
|  | Wymaga się aby oprogramowanie backupowe zapewniało pełen backup (full backup) blokowy wielomilionowych systemów plików na maszynach Windows / Linux poprzez odczyt tylko zmienionych bloków, odczyt całości zabezpieczanego dysku może być wykonany jedynie podczas pierwszego backupu bądź po restarcie serwera. Wszystkie kolejne backupy mają odczytywać z dysku jedynie zmienione bloki w stosunku do ostatniego backupu (w efekcie na deduplikatorze muszą pojawić się kopie typu full backup). Oprogramowanie backupowe musi odczytywać, jedynie zmienione na dysku bloki (a nie całe pliki). |
|  | Ze względów bezpieczeństwa rozwiązanie backupowe musi mieć możliwość wykonania kopii wewnętrznej bazy danych w trakcie pracy systemu bez konieczności ograniczania jego funkcjonalności. |
|  | Oprogramowanie backupowe musi umożliwiać zarządzanie replikacją backupów między deduplikatorami oferowanego typu oraz DD9400, bezpośrednio z poziomu interfejsu oprogramowania backupowego przy spełnieniu wszystkich poniższych wymagań* replikacji podlegają tylko te bloki które nie znajdują się na docelowym deduplikatorze
* replikacja między deduplikatorami następuje w zdefiniowanych interwałach czasowych
* oferowane oprogramowanie backupowe przechowuje informacje o wszystkich kopiach danych znajdujących się na deduplikatorach (czyli kopii oryginalnej oraz zreplikowanej)
* oferowane oprogramowanie backupowe pozwala na wybór deduplikatora z którego zostanie wykonane odtwarzanie bez konieczności przeprowadzania inwentaryzacji
 |
|  | Oprogramowanie backupowe musi umożliwiać określenie róznych retencji dla danych na podstawowym nośniku i nośniku zawierającym kopię (replika backupu). Określenie czasu retencji przechowywania dla kopii (repliki) musi być możliwe w momencie definiowania zadania backupowego. |
|  | Oferowane rozwiązanie backupowe musi pozwalać na użycie blokady WORM dostępnej na oferowanym deduplikatorze (wymagane wsparcie potwierdzone w dokumentacji deduplikatora i oprogramowania) oraz DD9400 (Retention Lock Governance oraz Compliance), zabezpieczającej przed skasowaniem/zmianą backupów w określonym czasie.  |
|  | Oprogramowanie musi umożliwiać natychmiastową aktywację blokady WORM natychmiast po zakończeniu wykonywania backupu. |
|  | Wymagana możliwość aktywacji blokady WORM - per zadanie backupowe, dla każdego zadania backupowego wymagana możliwość ustawienia innego czasu blokady backupu. |
|  | Wymaga się aby użycie blokady WORM było możliwe dla wszystkich systemów wspieranych przez oferowane oprogramowanie..  |
|  | Wymaga się aby z poziomu konsoli oprogramowania backupowego dostępna była możliwość definiowania wymaganej retencji danych (backupów) w oparciu o kryteria czasowe (dni, miesiące, lata). Po przekroczeniu okresu retencji, określone kopie backupowe muszą być automatycznie usunięte. |
|  | Dla baz danych MSSQL wymagana możliwość inicjowania backupów przez administratora MSSQL przy spełnieniu wszystkich poniższych wymagań:* backup jest wykonywany przez oferowane oprogramowanie backupowe
* inicjowanie backupu z graficznego interfejsu będącego częścią MSSQL Management Studio
* możliwość wyboru backupu pełnego, różnicowego, logów
* backup inicjowany przez administratora MSSQL nie może wymagać kontaktu z administratorem oferowanego rozwiązania backupowego
 |
|  | W przypadku zabezpieczania baz MSSQL wymagana możliwość inicjowania i wykonywania backupów przez administratora MSSQL także w przypadku gdy serwer backupu jest niedostępny |
|  | Dla baz danych MSSQL wymagana możliwość odtworzenia backupów przez administratora MSSQL przy spełnieniu wszystkich poniższych wymagań:* odtworzenie dowolnego backupu wykonanego przez oferowane rozwiązanie backupowe
* zarządzanie odtwarzaniem z graficznego interfejsu będącego częścią MSSQL Management Studio
* możliwość odtworzenia do dowolnego punktu w czasie wybranego przez administratora MSSQL w ramach przechowywanych przez oferowane oprogramowanie backupowe logów MSSQL
* odtworzenie bazy danych przez administratora MSSQL nie może wymagać kontaktu z administratorem oferowanego rozwiązania backupowego
 |
|  | Dla baz danych MSSQL wymagana możliwość realizowania samobackupującego się środowiska MS-SQL umożliwiającego automatyczny wybór backupowych baz danych w momencie startu backupu. Administrator definiuje reguły – jakie bazy danych mają być backupowane w ramach polityki – oprogramowanie backupowe backupuje wszystkie bazy danych spełniające określone reguły. |
|  | Wymaga się aby reguły (o których mowa w poprzednim punkcie), umożliwiające określenie które bazy będą backupowane uwzględniały:* nazwy backupowanych baz danych
* nazwy serwerów bazy danych
* nazwy klastrów
* typy hostów
* nazwy aplikacji

Reguły muszą pozwalać na wybór nazw:* zaczynających się od określonego tekstu
* zawierających określony tekst
* NIE zawierających określonego tekstu
* kończących się określonym tekstem
 |
|  | Rozwiązanie backupowe musi wspierać backup i odtwarzanie środowisk VMwareOprogramowanie backupowe musi umożliwiać w przypadku środowisk VMware następujące typy backupu: * backup pojedynczych plików i baz danych ze środka maszyny wirtualnej VMware.
* backup całych maszyn wirtualnych (obrazów, plików vmdk reprezentujących wirtualną maszynę). - realizacja backupu nie może wymagać bufora dyskowego na kopię obrazów maszyn wirtualnych (plików vmdk)
* backup tylko wybranych dysków maszyny wirtualnej (wybranych plików vmdk systemu vmware) - realizacja backupu nie może wymagać bufora dyskowego na kopię obrazów maszyn wirtualnych (plików vmdk)
* wszystkie backupy obrazów maszyn wirtualnych muszą być wykonywane przy pomocy technologii CBT systemu VMware to znaczy do medium backupowego z systemu VMware muszą być transferowane tylko zmienione bloki, z punktu widzenia systemu backupowego musza to być backupy pełne (full backup).

Powyższe metody backupu maszyn wirtualnych muszą podlegać deduplikacji ze zmiennym blokiem przed wysłaniem danych do oferowanego deduplikatora, metody te muszą być wbudowane w system backupu i w pełni automatyczne bez wykorzystania skryptów/dodatkowych komend. |
|  | Oferowane rozwiązanie backupowe musi umożliwiać odtwarzanie obrazów maszyn wirtualnych VMware przy zachowaniu następujących funkcjonalności:* odtworzenie całych maszyn wirtualnych musi wykorzystywać mechanizm CBT systemu VMware – odtwarzane są tylko te bloki wirtualnej maszyny/dysku które uległy zmianie od ostatniego backupu
* odtworzenie pojedynczych dysków maszyn wirtualnych musi wykorzystywać mechanizm CBT systemu VMware – odtwarzane są tylko te bloki wirtualnej maszyny/dysku które uległy zmianie od ostatniego backupu
* odtworzenie pojedynczych plików z backupu obrazu maszyny wirtualnej bez konieczności odtworzenia całej maszyny wirtualnej. Funkcjonalność musi być dostępna dla obrazów maszyn wirtualnych z zainstalowanym systemem operacyjnym Windows oraz Linux.

Powyższe metody odtworzenia muszą być wbudowane w system backupu i w pełni automatyczne bez wykorzystania skryptów/dodatkowych komend. |
|  | Skalowalność oferowanego rozwiązania dla środowisk VMware musi pozwalać na:* backup minimum 1000 maszyn wirtualnych w ramach pojedynczej instancji systemu backupu.
* równoległy backup dysków w ramach backupu pojedynczej maszyny wirtualnej VMware
 |
|  | Oferowane rozwiązanie backupowe musi umożliwiać backup minimum 25 maszyn wirtualnych z pojedynczego serwera proxy (z pojedynczego serwera odczytującego obrazy maszyn wirtualnych VMware).  |
|  | Wymaga się aby Administrator aplikacji backupowej za pośrednictwem GUI (graficzna konsola) miał dostępne następujące możliwości odtwarzania maszyn VMware:* odtworzenie całej maszyny wirtualnej VMware
* odtworzenie pojedynczego dysku uprzednio zbackupwanej całej maszyny wirtualnej
* odtworzenie plików / katalogów z backupu obrazu maszyny wirtualnej
* uruchomienie maszyny wirtualnej bezpośrednio z backupu dostępnego na oferowanym deduplikatorze bez wcześniejszego odtwarzania danych
* naprawienie aktualnej instancji maszyny wirtualnej– odtworzenie tylko zmienionych bloków od ostatniego backupu

Wszystkie w/w możliwości muszą być dostępne w postaci graficznych wizardów. |
|  | Oferowane rozwiązanie backupowe musi umożliwiać zdefiniowanie polityk backupowych dostępnych dla administratora systemu VMware z poziomu vCenter. Administrator VMware musi mieć możliwość przyporządkowania nowo tworzonych maszyn wirtualnych do polityk backupowych, przy czym całość informacji dot. backupów środowisk VMware musi być przechowywana na serwerze backupu. |
|  | Wymaga się aby maszyna wirtualna VMware zbackupowana poprzez serwer pośredniczący: A, mogła być odtworzona przez dowolny inny system pośredniczący np: B, C, ... .  |
|  | Oferowane oprogramowanie backupowe musi samo dystrybuować zadania backupu/odtwarzania obrazów maszyn wirtualnych VMware między dostępne serwery pośredniczące zapweniając równomierne obciążenie. |
|  | Wymaga się aby w przypadku srodowisk VMware oferowane rozwiązanie backupowe automatycznie rozpoznawało nowo utworzone maszyny wirtualne oraz przypisywało je do odpowiednich polityk backupowych, wymagana możliwość konfiguracji/realizacji następującego scenariusza:* + wszystkie nowo utworzone maszyny wirtualne zawierające w nazwie frazę „krytyczna” muszą być backupowana automatycznie co godzinę
	+ wszystkie nowo utworzone maszyny wirtualne zawierające w nazwie frazę „produkcja” muszą być backupowana automatycznie raz na dzień
	+ pozostałe maszyny wirtualne są backupowane raz na tydzień

Oferowane rozwiązanie backupowe musi umożliwiać realizację backupów wg. w/w scenariusza, bez jakichkolwiek akcji ze strony administratora backupu/VMware czy też jakiekolwiek innej osoby. |
|  | Wymaga się aby w przypadku srodowisk VMware oferowane oprogramowanie backupowe pozwalało na:* + automatyczne dodanie do odpowiednich polityk backupowych wszystkich maszyn wirtualnych zawierających w nazwie maszyny wirtualnej podany tekst.
	+ automatyczne dodanie do odpowiednich polityk backupowych wszystkich maszyn wirtualnych znajdujących się we wszystkich folderach zawierających w nazwie podany tekst.
	+ automatyczne dodanie do odpowiednich polityk backupowych wszystkich maszyn wirtualnych których TAG zawiera podany tekst.
	+ automatyczne dodanie do odpowiednich polityk backupowych wszystkich maszyn wirtualnych znajdujących się na wszystkich datastore’ach które w nazwie zawierają podany tekst.
 |
|  | Wymaga się aby w środowisku VMware oferowane oprogramowanie backupowe pozwalało na automatyczne usuwanie maszyn wirtualnych z polityk backupowych w tym samym momencie w którym maszyna jest usunięta z vCenter, dotychczas wykonane kopie zapasowe muszą być przechowywane zgodnie z okeśloną wcześniej retencją, umożliwiając odtworzenie tej maszyny. |
|  | Wymagana możliwośc realizacji backup’u środowisk VMware vSphere przy uzyciu vSphere API for I/O (VAIO) Filtering framework (<https://core.vmware.com/resource/vmware-vsphere-apis-io-filtering-vaio#section1>) |
|  | Oferowane rozwiązanie backupowe musi wspierać środowiska Kubernetes |
|  | Wymaga się aby podpięcie środowiska Kubernetes do oferowanego rozwiązania backupowego było maksymalnie proste, ograniczało się do podania jedynie nazwy FQDN/IP środowiska i uprawnień. |
|  | Wymaga się aby oprogramowanie backupowe automatycznie instalowało wymagane moduły w zabezpieczanym środowisku Kubernetes, wprost z repozytorium sieciowego producenta (np. github)Jeśli sieciowe repozytorium producenta jest niedostępne z poziomu środowiska Kubernetes, wymagana możliwość automatycznego pobierania modułów ze wskazanego repozytorium |
|  | Oferowane rozwiązanie musi zapewniać backup dowolnych namespace znajdujących się w środowisku Kubernetes |
|  | Wymagana możliwość wykluczenia dowolnych dysków PVC z backupu dowolnego namespace |
|  | Wymagana możliwość skonfigurowania samobackupującego się środowiska Kubernetes - w momencie startu backupu następuje automatyczny wybór backupowanych namespace zgodnie z regułami określonymi przez Administratora |
|  | Wymagana możliwość tworzenia w/w reguł używanych przy backupie określonych namespace w oparciu o: * nazwy backupowanych namespace
* etykiety backupowanych namespace

Reguły muszą pozwalać na wybór nazw :* zaczynających się od określonego tekstu
* zawierających określony tekst
* NIE zawierających określonego tekst
* kończących się określonym tekstem
 |
|  | Wymaga się aby backup realizowany był zgodnie ze zdefiniowana polityką lub inicjowany ad hoc, uruchomiony ręcznie przez administratora |
|  | W ramach dostarczonych licencji wymagana możliwość spójnego backupu baz danych i aplikacji Cassandra, MySQL, PostreSQL, MongoDB działających w obrębie zabezpieczanych środowisk Kubernetes  |
|  | Wymagana możliwość realizacji backupów syntetycznych. W przypadku środowisk Kubernetes działających w infrastrukturze VMware: odczyt jedynie zmienionych bloków, finalnie na deduplikatorze uzyskiwany jest pełen backup (full).Oferowane oprogramowanie musi umożliwiać automatyczną realizację powyższego scenariusza, nie może wymagać dodatkowych działań ze strony administratora backupu. |
|  | W przypadku środowisk Kubernetes wymagana możliwość odtworzenia całych namespace lub wybranych dysków PVC |
|  | W pprzypadku środowisk Kubernetes wymagana możliwość odtworzenia danych zarówno na oryginalne środowisko Kubernetes jak również inne środowisko Kubernetes |
|  | Wymagana możliwość bezpośredniego odtwarzania danych zarówno przez administratora backupu jak również przez administratora Kubernetes |
|  | Wymaga się aby zarządzanie zarówno w przypadku backupu, odtwarzania oraz wszystkich dostępnych funkcjonalności dla środowisk Kubernetes było dostępne za pośrednictwem jednej centralnej konsoli graficznej GUI HTML 5 |
|  | Wymaga się aby konsola oprogramowania backupowego umożliwiała definiowanie polityk backupowych obejmujących całość cyklu życia kopii zapasowej.W szczególności wymagana możliwość zdefiniowania polityki backupowej która dla dowolnej liczby zabezpieczanych systemów (zadań backupowych) zapewnia:* lokalny backup na oferowany deduplikator z retencją 30-o dniową
* replikację (na poziomie bloków) do drugiego deduplikatora oferowanego typu (retencja 60 dni)

Całość wymaganych operacji powinna być skonfigurowana poprzez pojedynczą politykę backupową stworzoną poprzez GUI oprogramowania backupowego w oparciu o dostępny „wizard”.Wymaga się aby administrator backupu za pośrednictwem konsoli (GUI) oferowanego oprogramowania backupowego mógł odtwarzać dane VMware/Kubernetes z dowolnych w/w kopii (1-2).  |

Wymagania dotyczące oprogramowania zapewniającego ochronę w trybie Continuous Data Protection dla środowisk VMware vSphere

|  |  |
| --- | --- |
|  | integracja na poziomie VMware vCenter Plug-in (ORCHESTRATION, MANAGEMENT) , vSphere Web Client GUI |
|  | wsparcie dla HA, DRS, S-DRS, VMotion, S-VMotion  |
|  | możliwość integracji z VMware vRealize Operations Manager |
|  | rozwiązanie dostarczane w postaci oprogramowania instalowanego na platformie ESXi |
|  | skalowalność zapewniająca wsparcie dla 8000 VM w obrębie poj. vCenter  |
|  | zabepieczenie dowolnej maszyny wirtualnej wraz z aplikacjami w trybie ciągłym tzn. umożliwiającym odtworzenie do dowolnego punktu w czasie (tzw. PIT – Point In Time), wymagane wsparcie dla VMware ESXi 7.x |
|  | możliwość tworzenia tzw. CONSISTENCY GROUP zapewniających identyczną konsystencję dla przynależących do danej grupy maszyn wirtualnych (VM), wymagane wsparcie dla min. 250 CONSISTENCY GROUP |
|  | zabezpieczenie realizowane za pośrednictwem ciągłej replikacji (a nie za pomocą SNAPSHOT’ów ) na poziomie VMDK oraz RDM, niezależnie od użytego storage’u (tzw. Storage Agnostic -warunkiem jest wsparcie przez VMware), wymagane wsparcie dla połączeń: FC, FCoE, iSCSI, NAS oraz DAS |
|  | wsparcie dla replikacji (bi-directional) asynchronicznej oraz synchronicznej (realizowanej na poziomie dostarczanego oprogramowania), połączonych z mechanizmem tzw. JOURNALING umożliwiającego odnotowanie wszystkich zmian zabezpieczanego środowiska |
|  | odporność na krótkotrwałe problemy (przeciążenie, zaniki) związane z siecią WAN |
|  | wbudowana funkcjonalność deduplikacji oraz kompresji w przypadku transmisji danych poprzez WAN |
|  | wsparcie dla równoległej replikacji zabezpieczanego środowiska do różnych ośrodków docelowych (min. 3-ech), wsparcie dla replikacji równoległej powinno być zapewnione również na poziomie grup konsystencji (CONSISTENCY GROUP)  |
|  | proponowane rozwiązanie powinno umożliwiać:* stworzenia DISASTER RECOVERY dla całego zabezpieczanego wirtualnego środowiska zbudowanego w oparciu o VMware
* operacyjne ODTWARZANIE dowolnej maszyny VM wraz z aplikacjami
* MIGRACJI danych w trybie ON-LINE na inne zasoby dyskowe
 |
|  | równoległe wsparcie środowisk lokalnych oraz zdalnych, wymagana możliwość pracy w 3-ech trybach, tzw.: CDP (Continuous Data Protection … tryb replikacji lokalnej), CRR (Continuous Remote Replication … tryb replikacji zdalnej), CLR (Continuous Local and Remote Replication … połączenie CDP oraz CLR … tryb replikacji lokalnej oraz zdalnej) w ramach dostarczonych licencji |
|  | granularność umożliwiająca pominięcie określonych plików VMDK związanych z wirtualnymi serwerami VM objętych protekcją |
|  | architektura FAULT-TOLERANT, brak pojedynczego punktu awarii |
|  | wyskalowanie systemu powinno gwarantować RPO (Recovery Point Objective) w przypadku codziennej pracy ciągłej na poziomie pojedynczych sekund |
|  | proponowana konfiguracja systemu powinna zapewnić następującą retencję przechowywanych kopii bezpieczeństwa:* RPO=30s z ostatnich 24h,
* RPO=24h z ostatniego tygodnia,
* RPO=1tydzień z ostatniego miesiąca
 |
|  | możliwość odtworzenia zabezpieczanego środowiska do dowolnego punktu w czasie  |
|  | możliwość trybu pracy umożliwiającego objęciem protekcją w sposób automatyczny nowo dodanych maszyn wirtualnych (VM) |
|  | rozwiązanie powinno dopuszczać zmiany HW na poziomie infrastruktury zabezpieczanego środowiska bez negatywnego wpływu na działanie systemu |
|  | możliwość użycia mechanizmu typu BOOKMARK dla oznaczenia konsystentnych kopii zabezpieczanych aplikacji |
|  | wsparcie dla VSS, zapewnienie konsystencji aplikacji na poziomie VSS |
|  | możliwość automatycznego przeprowadzania operacji typu FAILOVER/FAILBACK do dowolnego punktu w czasie dla określonych produkcyjnych serwerów wirtualnych (VM), w tym: odtworzenie, uruchomienie (z zachowaniem wymaganej sekwencji), konfigurację |
|  | możliwość automatycznego przeprowadzania operacji typu FAILOVER/FAILBACK do dowolnego punktu w czasie określonych testowych maszyn wirtualnych (VM) |
|  | możliwość automatycznego zainicjowania procesu REVERSE REPLICATION w przypadku procesów FAILOVER/FAILBACK |
|  | możliwość przeprowadzania testów DR bez wpływu na zabezpieczane serwery produkcyjne oraz bez konieczności zmian w działaniu replikacji (np.: PAUSE, REVERSE, …) |
|  | możliwość skryptowego tworzenia planów RECOVERY |

Wymagania funkcjonalne dotyczące deduplikatora (-ów) skonfigurowanego w oparciu o licencje będące przedmiotem zapytania (wymagany sumaryczny rozmiar min. 200TB netto w obrębie do trzech urządzeń skonfigurowanych lokalnie oraz 200TB w obrębie jednego urządzenia skonfigurowanego w środowisku chmurowym)

|  |  |
| --- | --- |
|  | Rozwiązanie powstałe w wyniku instalacji/konfiguracji licencji będących przedmiotem zapytania musi być przeznaczone do deduplikacji, dedykowane do przechowywania kopii zapasowych. Urządzenie musi spełniać wymagania wyspecyfikowane w niniejszej tabeli. |
|  | Oprogramowanie będące przedmiotem zapytania musi umożliwiać instalację i konfigurację deduplikatora na platformie VMware vSphere 7.x oraz Microsoft Windows Server 2016/2019/2022 z Hyper-V, o przestrzeni określonej wcześniej przez Zamawiającego (powierzchni użytkowej dedykowanej do przechowywania deduplikatów) bez uwzględniania mechanizmów protekcji, wymagane skalowanie do min. 90TB powierzchni netto w ramach tego samego urządzenia w przypadku instalacji lokalnej oraz 250TB w przypadku instalacji poj. urządzenia w środowisku chmurowym (Azure, GCP, AWS) |
|  | Deduplikator musi zapewniać jednoczesny dostęp wszystkimi poniższymi protokołami:* CIFS
* NFS
* deduplikacja na źródle wspierana przez oferowane oprogramowanie backupowe oraz eksploatowane obecnie oprogramowanie

w obrębie oferowanej pojemności urządzenia. |
|  | Urządzenie musi umożliwiać zdefiniowanie blokady skasowania danych (funkcjonalnosć WORM). Blokada skasowania danych musi chronić składowane dane w zdefiniowanym czasie przed usunięciem oraz modyfikacją.Licencje na blokadę usunięcia/zmiany przechowywanych plików muszą być dostarczone wraz z urządzeniem.Wymagane wsparcie wymaganej blokady WORM przez oferowaną aplikację backupową, co oznacza:* możliwość uruchomienia blokady WORM dla określonych danych z poziomu oferowanej aplikacji backupowej
* możliwość określenia/wymuszenia czasu blokady z poziomu oferowanej aplikacji backupowej
* możliwość raportowania od strony oferowanej aplikacji backup’owej danych zabezpieczonych przed usunięciem wymaganą blokadą WORM
 |
|  | Wymagane jest dostarczenie licencji zapewniających funkcjonalność: ENCRYPTION (szyfrowanie) w obrębie maksymalnej wymaganej pojemności urządzenia. |
|  | Urządzenie musi pozwalać na jednoczesną obsługę minimum 180 strumieni  |
|  | Oferowane urządzenie musi deduplikować dane in-line przed zapisem na nośnik dyskowy. Na wewnętrznych dyskach urządzenia nie mogą być zapisywane dane w oryginalnej postaci (niezdeduplikowanej) z jakiegokolwiek fragmentu strumienia danych przychodzącego do urządzenia. |
|  | Technologia deduplikacji musi wykorzystywać algorytm bazujący na zmiennym, dynamicznym bloku jednak o długości nie większej niż 16kB.Algorytm ten musi samoczynnie i automatycznie dopasowywać się do otrzymywanego strumienia danych. Oznacza to, że urządzenie musi dzielić otrzymany pojedynczy strumień danych na bloki o różnej długości.  |
|  | Deduplikacja zmiennym, dynamicznym blokiem musi oznaczać, że wielkość każdego bloku (na jakie są dzielone dane pojedynczego strumienia backupowego) może być inna niż poprzedniego i jest indywidualnie ustalana przez algorytm urządzenia w celu maksymalnego zwiększenia efektywności deduplikacji. |
|  | Niedopuszczalna jest deduplikacja stałym blokiem o ustalonej tej samej długości, możliwość manulanej zmiany (bądź poprzez oskryptowanie) długości bloku deduplikacji również nie może zastąpić wymogu automatycznego doboru długości bloku na jaki dzielony jest każdy strumień danych. |
|  | Oferowany produkt musi posiadać obsługę mechanizmów globalnej deduplikacji dla danych otrzymywanych jednocześnie wszystkimi protokołami (CIFS, NFS, deduplikacja na źródle) przechowywanych w obrębie całego urządzenia.W obrębie całego urządzenia, raz otrzymany i zapisany w urządzeniu fragment danych nie może być ponownie zapisany bez względu na to, jakim protokołem zostanie ponownie otrzymany. |
|  | Powyższe oznacza również, że oferowany produkt musi również posiadać obsługę mechanizmów globalnej deduplikacji pomiędzy dowolnymi dwoma udziałami NFS, CIFS. Blok danych otrzymany i zapisany na udział CIFS, nie może zostać ponownie zapisany jeśli trafi do udziału NFS w obrębie tego samego urządzenia (to samo dotyczy deduplikacji na źródle) |
|  | Przestrzeń składowania zdeduplikowanych danych musi być jedna dla wszystkich protokołów dostępowych. |
|  | Wszystkie unikalne bloki przed zapisaniem na dysk muszą być dodatkowo skompresowane  |
|  | Oferowane rozwiązanie musi wspierać oferowaną aplikację backup’ową oraz eksploatowaną obecnie aplikację backup’ową |
|  | W przypadku współpracy z oferowaną a także eksploatowaną obecnie aplikacją backupową, urządzenie musi umożliwiać deduplikację na źródle (deduplikację na zabezpieczanej maszynie) i przesyłanie nowych, nie znajdujących się jeszcze na urządzeniu bloków poprzez sieć LAN. Deduplikacja w wyżej wymienionych przypadkach musi zapewniać aby z serwerów do oferowanego urządzenia były transmitowane poprzez sieć LAN tylko fragmenty danych nie znajdujące się dotychczas na urządzeniu. |
|  | W przypadku deduplikacji na źródle poprzez sieć IP (LAN oraz WAN), musi być możliwość szyfrowania komunikacji kluczem minimum 256 bitów. |
|  | Urządzenie powinno dopuszczać co najmniej 90% utylizację powierzchni netto, bez widocznego spadku wydajności. Dokumentacja urządzenia nie może wskazywać na jakiekolwiek problemy czy obostrzenia, które mogą pojawić się przy zapełnieniu urządzenia poniżej 90%. |
|  | Oferowane urządzenie musi umożliwiać bezpośrednią replikację danych (bez pośrednictwa dodatkowych modułów) do drugiego urządzenia tego samego typu oraz DD9400, wymagane następujące tryby pracy replikacji:* jeden do jednego
* wiele do jednego
* jeden do wielu
* kaskadowej (urządzenie A replikuje dane do urządzenia B które te same dane replikuje do urządzenia C).

Replikacja musi się odbywać w trybie asynchronicznym. Transmitowane mogą być tylko te fragmenty danych (bloki) które nie znajdują się na docelowym urządzeniu, rozwiązanie replikacyjne nie powinno wymagać aby obszar na który dane są replikowane był większy od obszaru źródłowego (replikowanego) w przypadku schematu „jeden do jednego” – weryfikacja na podstawie ogólnie dostępnej dokumentacji producenta oraz zaleceń. Ewentualna licencja na replikację musi być dostarczona w ramach postępowania. |
|  | W przypadku wykorzystania portów Ethernet do replikacji urządzenie musi umożliwiać przyjmowanie backupów, odtwarzanie danych, przyjmowanie strumienia replikacji, wysyłanie strumienia replikacji tymi samymi portami. |
|  | W przypadku replikacji danych między dwoma urządzeniami kontrolowanej przez oferowaną aplikację backupową muszą być możliwe do uzyskania jednocześnie wszystkie następujące funkcjonalności:* replikacja odbywa się bezpośrednio między dwoma urządzeniami bez udziału serwerów pośredniczących
* replikacji podlegają tylko te fragmenty danych, które nie znajdują się na docelowym urządzeniu
* replikacja zarządzana jest z poziomu aplikacji backupowej, aplikacja backupowa posiada informację o obydwu kopiach zapasowych znajdujących się w obydwu urządzeniach bez konieczności przeprowadzania procesu inwentaryzacji
 |
|  | Wymagana możliwość ograniczenia pasma używanego do replikacji między dwoma urządzeniami. |
|  | Deduplikator musi umożliwiać wykonywanie oraz przechowywanie SnapShot’ów (min. 100 jednocześnie), czyli możliwość zamrożenia obrazu danych (stanu backupów) w urządzeniu na określoną chwilę. Oferowane urządzenie musi również umożliwiać odtworzenie danych ze Snapshot’u.Odtworzenie danych ze Snapshot’u nie może wymagać konieczności nadpisania danych produkcyjnych jak również nie może oznaczać przerwy w normalnej pracy urządzenia (przyjmowania backupów / odtwarzania). |
|  | Deduplikator musi pozwalać na podział na logiczne części. Dane znajdujące się w każdej logicznej części muszą być między sobą deduplikowane (globalna deduplikacja między logicznymi częściami urządzenia). |
|  | Deduplikator musi mieć możliwość podziału na minimum 14 logicznych części pracujących równolegle. Producent musi oficjalnie wspierać pracę minimum 14 logicznych części pracujących równolegle z pełną wydajnością urządzenia. |
|  | Dla każdej z logicznych części oferowanego urządzenia musi być możliwość zdefiniowania oddzielnego użytkownika zarządzającego daną logiczną częścią deduplikatora. Użytkownicy zarządzający logiczną częścią A muszą widzieć tylko i wyłącznie zasoby logicznej części i nie mogą widzieć żadnych innych zasobów oferowanego urządzenia. |
|  | Wymagana możliwość zaprezentowania każdej z logicznych części oferowanego urządzenia, jako niezależnego urządzenia dostępnego poprzez:* CIFS
* NFS
* wymagany protokół umożliwiający deduplikację na źródle
 |
|  | Urządzenie musi automatycznie usuwać przeterminowane dane (bloki danych nie należące do backupów o aktualnej retencji) w procesie czyszczenia.  |
|  | Proces usuwania przeterminowanych danych (czyszczenia) nie może uniemożliwiać pracy procesów backupu / odtwarzania danych (zapisu / odczytu danych z zewnątrz do systemu), nie może wymagać (zgodnie z oficjalnymi zaleceniami producenta) definiowania BLACKOUT WINDOW czyli okna czasowego dedykowanego dla procesu czyszczenia podczas którego nie są realizowane procesy backupu / odtwarzania danych czy replikacji. |
|  | Wymagana możliwość zdefiniowania maksymalnego obciążenia urządzenia procesem usuwania przeterminowanych danych (poziomu obciążenia procesora). |
|  | Wymagana możliwość zdefiniowania czasu w którym wykonywany jest proces usuwania przeterminowanych danych (czyszczenia). |
|  | Standardowa częstotliwość usuwania przeterminowanych danych (czyszczenie) nie powinna być większa niż 1 raz na tydzień - minimalizując czas w którym backupy/odtworzenia narażone są na spowolnienie (weryfikacja wymagania na podstawie dokumentacji typu DOBRE PRAKTYKI publikowanej przez producenta). |
|  | Urządzenie musi mieć możliwość zarządzania poprzez* interfejs graficzny dostępny z przeglądarki internetowej
* poprzez linię komend (CLI) dostępną z poziomu ssh (secure shell)
 |