ROZDZIAŁ II – OPIS PRZEDMIOTU ZAMÓWIENIA DLA CZĘŚCI II

Dostawa Urządzeń wraz z Oprogramowaniem, wsparciem technicznym oraz usługami wdrożeniowymi w celu budowy środowiska (4 części) – część II

1. Nazwa zamówienia:

Dostawa kompleksowego rozwiązania platformy konteneryzacyjnej wraz z gwarancją i usługą wsparcia technicznego

2. Kody CPV:

48000000 – 8 - Pakiety oprogramowania i systemy informatyczne

48820000 – 2 – Serwery

71356300 – 1 – Usługi wsparcia technicznego

72267000 – 4 – Usługi w zakresie konserwacji i napraw oprogramowania

72250000 – 2 – Usługi w zakresie konserwacji i wsparcia systemów

3. Wymagania ogólne dotyczące przedmiotu zamówienia:

3.1. Zastosowane definicje i skróty:

Aktualizacje	jakiekolwiek uaktualnienia Oprogramowania dostarczonego w ramach Umowy, w tym wyższe wersje (update/upgrade), niższe wersje (downgrade), wydania uzupełniające, patche, zmiany, nowe wersje, poprawki oraz inne dostosowania, w tym wskazane w OPZ, zapewniające prawidłowe korzystanie z Oprogramowania;
Awaria	nieprawidłowe działanie Kompleksowego rozwiązania platformy konteneryzacyjnej, w szczególności brak możliwości korzystania z Urządzeń lub Oprogramowania w sposób zgodny z ich przeznaczeniem, z dokumentacją producenta lub Dokumentacją powykonawczą. Awaria dzieli się na Awarię Krytyczną lub Awarię Zwykłą;
Awaria Krytyczna	Awaria wywołująca nieprawidłowe działanie Kompleksowego rozwiązania platformy konteneryzacyjnej powodujące całkowity brak możliwości korzystania z niej lub takie ograniczenie korzystania z Kompleksowego rozwiązania platformy konteneryzacyjnej uniemożliwiające spełnianie jej podstawowych funkcji, wstrzymująca operacje biznesowe, w znacznym stopniu ograniczająca wydajność lub dostęp do danych, bez możliwości naprawy poprzez Obejście;
Awaria Zwykła	Awaria niebędąca Awarią Krytyczną;

Dni robocze	dni od poniedziałku do piątku od 09:00 do 17:00, z wyłączeniem dni ustawowo wolnych od pracy na terenie Rzeczypospolitej Polskiej;
Dokumentacja powykonawcza	dokumentacja zawierająca szczegółowy wykaz wszystkich elementów Kompleksowego rozwiązania platformy konteneryzacyjnej oraz szczegółowy opis ich instalacji wraz z konfiguracją oraz rysunkami technicznymi;
Kompleksowe rozwiązanie platformy konteneryzacyjnej	Urządzenia wraz z Oprogramowaniem tworzące wspólną całość dostarczanego rozwiązania;
Lokalizacje	dwa miejsca na terenie miasta stołecznego Warszawy, do których ma nastąpić dostawa przedmiotu zamówienia. Dokładne adresy zostaną podane do wiadomości Wykonawcy niezwłocznie po podpisaniu umowy;
Obejście	działanie Wykonawcy polegające na przeprowadzeniu diagnozy Awarii oraz usunięciu jej w sposób tymczasowy. Obejście nie stanowi usunięcia Awarii i nie zwalnia Wykonawcy od obowiązku jej usunięcia;
Oprogramowanie	całość lub dowolny element oprogramowania opisanego w OPZ wraz z licencjami, spełniającego wymagania określone w OPZ;
OPZ	niniejszy Opis Przedmiotu Zamówienia;
Urządzenie	element fizyczny dostarczonego kompleksowego rozwiązania sprzętowego, spełniający wymagania określone w OPZ;
Zgłoszenie	poinformowanie o wystąpieniu Awarii. Za moment Zgłoszenia przyjmuje się dzień i godzinę poinformowania przez Zamawiającego o Awarii przez jeden ze wskazanych w pkt 3.5.4.1. kanałów komunikacji. Jeżeli Awaria została zgłoszona więcej niż jednym kanałem, za moment Zgłoszenia uznaje się to Zgłoszenie, które zostało dokonane wcześniej.

3.2. Przedmiotem zamówienia jest:

3.2.1. Dostawa Kompleksowego rozwiązania platformy konteneryzacyjnej wraz z montażem, wdrożeniem i konfiguracją w dwóch Lokalizacjach, instruktaż stanowiskowy oraz przygotowanie Dokumentacji powykonawczej. Kompleksowe rozwiązanie platformy konteneryzacyjnej składa się z:

- 3.2.1.1. Serwerów obliczeniowych opisanych w punkcie 4.1.,
- 3.2.1.2. Systemu pamięci obiektowo – blokowej opisanego w punkcie 4.2.,
- 3.2.1.3. Środowiska zarządzania kontenerami opisanego w punkcie 4.3.,
- 3.2.1.4. Systemu backup opisanego w punkcie 4.4.

3.2.2. Zapewnienie gwarancji i wsparcia technicznego dla Kompleksowego rozwiązania platformy konteneryzacyjnej.

3.3. Terminy realizacji:

3.3.1. Przedmiot zamówienia wskazany w pkt 3.2.1. zostanie wykonany w terminie do 90 dni od zawarcia umowy;

3.3.2. Gwarancja i wsparcie techniczne, o których mowa w punkcie 3.2.2. będą świadczone przez okres 36 miesięcy od dnia odbioru końcowego przedmiotu zamówienia wskazanego w pkt 3.2.1.

3.4. Wymagania ogólne w zakresie wskazanym w pkt 3.2.1.:

3.4.1. Wykonawca na potrzeby wdrożenia i uruchomienia Kompleksowego rozwiązania platformy konteneryzacyjnej dostarczy Urządzenia wraz z Oprogramowaniem i licencjami na Oprogramowanie do dwóch Lokalizacji;

3.4.2. Zamawiający zastrzega, że niniejszy przedmiot zamówienia jest przeznaczony do dalszej odsprzedaży. Wszelkie dokumenty rejestracyjne, licencyjne muszą być wystawione na docelowego licencjobiorcę, jakim jest Skarb Państwa reprezentowany przez Ministra Cyfryzacji, ul. Królewska 27, 00-060 Warszawa;

3.4.3. Wykonawca wraz z dostawą przekaże Zamawiającemu aktualne zestawienie w formacie *.xlsx wszystkich dostarczonych Urządzeń, zawierające informacje dotyczące miejsca dostawy, daty dostawy, typu i modelu Urządzenia, numeru seryjnego, ilości, ceny jednostkowej netto, kwoty VAT oraz ceny jednostkowej brutto Urządzeń;

3.4.4. Wykonawca wraz z dostawą jest zobowiązany do przekazania Zamawiającemu aktualnego zestawienia w formacie *.xlsx wszystkich dostarczonych pozycji w zakresie Oprogramowania zawierającego – o ile są udostępnione przez producenta Oprogramowania – informacje m.in. part numer, pełną nazwę produktu, metrykę licencyjną, wersję i edycję Oprogramowania, rodzaj licencji, okres obowiązywania licencji, ilość licencji, okres obowiązywania wsparcia technicznego, poziom wsparcia technicznego oraz cenę jednostkową netto, kwotę VAT oraz cenę jednostkową brutto;

3.4.5. Wykonawca wraz z Urządzeniami dokona dostawy wszystkich elementów niezbędnych do ich montażu i uruchomiania w Lokalizacjach takich jak: śrubki, nakrętki, kable zasilające itp.;

3.4.6. Wykonawca dokona wniesienia, montażu Urządzeń oraz wdrożenia Kompleksowego rozwiązania platformy konteneryzacyjnej w pomieszczeniach wskazanych przez Zamawiającego;

3.4.7. Dostawa, montaż i wdrożenie Kompleksowego rozwiązania platformy konteneryzacyjnej będzie realizowana w Dni robocze, chyba że Strony postanowią inaczej;

3.4.8. Urządzenia muszą być fabrycznie nowe, nieużywane wcześniej oraz muszą posiadać najnowszą dostępną stabilną wersję Oprogramowania;

3.4.9. Data zakończenia świadczenia wsparcia dla Urządzeń deklarowana przez producenta „EOSL" – „End Of Service Life" nie może być krótsza niż 5 lat licząc od dnia ogłoszenia postępowania;

3.4.10. Wykonawca w dniu podpisania protokołu odbioru ilościowego zobowiązany jest dostarczyć Zamawiającemu na adres e-mail, który zostanie wskazany w Umowie:

3.4.10.1. dokument potwierdzający objęcie Oprogramowania wsparciem technicznym,

3.4.10.2. adresy poczty elektronicznej, nr telefonów oraz dane dostępowe do portalu klienckiego, umożliwiające Zamawiającemu korzystanie z gwarancji i wsparcia technicznego,

3.4.10.3. dokumenty licencji na Oprogramowanie, w tym certyfikaty licencyjne wystawione przez producenta, umowy/warunki licencyjne producenta Oprogramowania;

3.4.11. Jeśli Oprogramowanie nie jest możliwe do pobrania online, Wykonawca dostarczy Zamawiającemu nośniki instalacyjne Oprogramowania;

3.4.12. Przedmiot zamówienia nie może naruszać bezpieczeństwa publicznego lub istotnego interesu bezpieczeństwa państwa, mając na względzie m.in. fakt, że Zamawiający zgodnie

z art. 4 pkt. 7 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa należy do Krajowego systemu cyberbezpieczeństwa, którego celem jest zgodnie z art. 3 ww. ustawy, zapewnienie cyberbezpieczeństwa na poziomie krajowym, w tym zapewnienie niezakłóconego świadczenia usług kluczowych i usług cyfrowych, przez osiągnięcie odpowiedniego poziomu bezpieczeństwa systemów informacyjnych służących do świadczenia tych usług oraz zapewnienie obsługi incydentów. Tym samym, przedmiot zamówienia musi być zgodny z celem Krajowego systemu cyberbezpieczeństwa i przepisami ww. ustawy oraz nie zagrażać cyberbezpieczeństwu, bezpieczeństwu publicznemu lub istotnemu interesowi bezpieczeństwa państwa;

3.4.13. W ramach dostarczanych technologii zostanie przeprowadzony instruktaż stanowiskowy zgodnie z poniższymi warunkami:

3.4.13.1. Instruktaż będzie prowadzony przez doświadczonych wdrożeniowców posiadających certyfikaty producenta danego rozwiązania dla łącznie maksymalnie 16 osób wyznaczonych przez Zamawiającego, w minimum dwóch grupach, w terminach uzgodnionych przez strony,

3.4.13.2. Instruktaż stanowiskowy obejmie zagadnienia z zakresu obsługi dostarczonych elementów Kompleksowego rozwiązania platformy konteneryzacyjnej, w szczególności cały cykl życia produktów począwszy od podstaw funkcjonalności i planowania „operacje dnia zerowego" przez prace wdrożeniowo - utrzymaniowe, „operacje dnia pierwszego" oraz prace optymalizacyjne, rozwojowe i naprawcze „operacje dnia drugiego",

3.4.13.3. Instruktaż może być przeprowadzony online, w formie prezentacji i wirtualnych laboratoriów z ćwiczeniami,

3.4.13.4. Podczas przeprowadzania instruktażu stosunek procentowy ćwiczeń praktycznych do wiedzy teoretycznej musi stanowić minimum 50%,

3.4.13.5. Instruktaż stanowiskowy z każdego obszaru technologicznego Kompleksowego rozwiązania platformy konteneryzacyjnej zostanie potwierdzony imiennym zaświadczeniem ukończenia instruktażu z danego zakresu przekazywanej wiedzy,

3.4.13.6. Zaświadczenie będzie wydawane przez Wykonawcę dla każdego z uczestników z osobna,

3.4.13.7. Szczegółowy zakres instruktażu stanowiskowego dla poszczególnych elementów Kompleksowego rozwiązania platformy konteneryzacyjnej został przedstawiony w punktach 4.2.2.9., 4.3.75. i 4.4.2.94. OPZ.

3.5. Wymagania w zakresie gwarancji i wsparcia technicznego dla Kompleksowego rozwiązania platformy konteneryzacyjnej:

3.5.1. Wykonawca zapewni objęcie Kompleksowego rozwiązania platformy konteneryzacyjnej 36-miesięczną gwarancją i wsparciem technicznym, które będą świadczone przez producenta Urządzeń i Oprogramowania lub podmiot autoryzowany przez tego producenta;

3.5.2. Warunki wsparcia technicznego pozostaną niezmienne przez cały okres świadczenia wsparcia;

3.5.3. Dostarczone przez Wykonawcę Oprogramowanie i Aktualizacje będą wolne od mechanizmów celowo blokujących ich funkcje i wolne od wirusów, koni trojańskich, robaków i innych szkodliwych programów. Wykonawca zobowiązuje się do realizacji świadczeń gwarancyjnych i wsparcia technicznego w sposób zapobiegający utracie danych, do których będzie miał dostęp w czasie wykonywania czynności;

3.5.4. W ramach gwarancji Wykonawca zobowiązuje się zapewnić:

3.5.4.1. rejestrowanie i zgłaszanie Awarii w trybie 24/7 (24 godziny na dobę, 7 dni w tygodniu, we wszystkie dni w roku) poprzez dedykowany portal zgłoszeniowy

umożliwiający Zamawiającemu śledzenie statusów Zgłoszeń, e-mail lub nr telefonu wskazane w umowie. W przypadku dokonania Zgłoszenia przez telefon Wykonawca niezwłocznie potwierdzi otrzymanie Zgłoszenia na adres e-mail Zamawiającego,

3.5.4.2. reakcję na zgłoszenie Awarii maksymalnie w ciągu 4 godzin od Zgłoszenia,

3.5.4.3. usunięcie Awarii Zwykłej w ciągu 48 godzin od Zgłoszenia,

3.5.4.4. usunięcie Awarii Krytycznej w ciągu 24 godzin od Zgłoszenia,

3.5.4.5. W przypadku Awarii Oprogramowania, która może zostać usunięta wyłącznie przez producenta Oprogramowania objętego Awarią, Wykonawca w terminie odpowiadającym rodzajowi Awarii wskazanym odpowiednio w punkcie 3.5.4.3. lub 3.5.4.4. zawiadomi Zamawiającego o tym fakcie co najmniej w formie dokumentowej oraz przekaże Zgłoszenie producentowi Oprogramowania objętego Awarią. W takim wypadku Wykonawca nie odpowiada za niedochowanie czasu usunięcia Awarii,

3.5.4.6. Regulacji z punktu 3.5.4.5. nie stosuje się do Awarii Oprogramowania będącego Oprogramowaniem wbudowanym (firmware);

3.5.5. W razie niedotrzymania przez Wykonawcę terminu usunięcia Awarii zgodnie z powyższymi punktami Zamawiający ma prawo zlecić jej usunięcie osobie trzeciej, przy czym będzie ona realizowana w całości na koszt Wykonawcy. W takiej sytuacji Zamawiający wezwie Wykonawcę do zaprzestania dalszych działań związanych z obsługą Zgłoszenia oraz przekaże informację o przekierowaniu Zgłoszenia do strony trzeciej;

3.5.6. W przypadku braku możliwości usunięcia Awarii poprzez naprawę Urządzenia w miejsce Urządzenia, które nie może być przez Wykonawcę naprawione, Wykonawca zobowiązany jest do dostarczenia Zamawiającemu innego urządzenia, wolnego od wad, o parametrach technicznych nie gorszych od parametrów technicznych Urządzenia naprawianego oraz zapewniającego nie gorszy poziom bezpieczeństwa, a następnie świadczenia wsparcia technicznego w stosunku do tego urządzenia przez okres obowiązywania umowy;

3.5.7. W przypadku wystąpienia Awarii i zastosowania w terminie przewidzianym dla usunięcia Awarii Obejścia zastosowanie Obejścia wstrzymuje naliczenie Wykonawcy kar umownych z tytułu niedochowania terminu usunięcia Awarii, jednak nie dłużej niż 30 dni kalendarzowych liczonych od daty dostarczenia Obejścia;

3.5.8. Wszelkie uszkodzone nośniki danych pozostaną własnością Zamawiającego. W przypadku stwierdzenia uszkodzenia nośnika danych (typu dysk twardy), będzie on wymieniony przez Wykonawcę na nowy, wolny od wad, bez konieczności zwrotu uszkodzonego nośnika danych i dokonywania jego ekspertyzy poza miejscem korzystania z przedmiotu umowy (Lokalizacje);

3.5.9. Usunięcie Awarii zostanie potwierdzone w formie pisemnej przez przedstawiciela Zamawiającego i Wykonawcy;

3.5.10. W ramach wsparcia technicznego Zamawiający otrzyma dostęp do informacji w postaci elektronicznej (bazy wiedzy), w języku polskim lub angielskim, na temat posiadanego Oprogramowania, wykaz znanych symptomów i rozwiązań w języku polskim lub angielskim (w tym programy korygujące do Oprogramowania), biuletynów technicznych, dokumentacji technicznych poprawek błędów i zabezpieczeń, dostęp do źródeł, kodów binarnych, dokumentacji Oprogramowania oraz bazy danych zgłoszonych problemów technicznych przez 24 godziny na dobę, 7 dni w tygodniu - pod wskazanym przez Wykonawcę portalem producenta. Dodatkowo portal powinien umożliwiać:

3.5.10.1. Dostęp do bazy wiedzy zawierającej rozpoznane i rozwiązane problemy, artykuły eksperckie oraz pełną dokumentację techniczną,

3.5.10.2. Pobieranie i korzystanie aktualizacji i poprawek Oprogramowania.

4. Wymagania szczegółowe:

4.1. Serwery obliczeniowe:

sztuk: 12 (po 6 serwerów do każdej z Lokalizacji)

4.1.1. **Obudowa:**

4.1.1.1. typu Rack, wysokość maksimum 1U

4.1.1.2. dostarczona wraz z szynami umożliwiającymi pełne wysunięcie serwera z szafy Rack

4.1.2. **Płyta główna:**

4.1.2.1. dwuprocesorowa, wyprodukowana i zaprojektowana przez producenta serwera, możliwość instalacji procesorów minimum dwudziestoośmio-rdzeniowych

4.1.2.2. wyposażona w minimum 24 gniazda pamięci obsługujące co najmniej RAM DDR4 2900 MT/s lub MHz

4.1.2.3. wyposażona w moduł TPM w wersji 2.0

4.1.2.4. minimum 3 złącza PCI Express generacji w tym min. 2 o prędkości x16 i jeden o prędkości x8 (nie wliczając ewentualnego złącza dedykowanego dla kontrolera RAID)

4.1.2.5. W każdym przypadku opis slotu dotyczy jego przepustowości, a nie tylko długości

4.1.2.6. wszystkie złącza PCI Express muszą być aktywne

4.1.2.7. minimum 2 sloty dla dysków M.2 na płycie głównej (lub dedykowanej karcie PCI Express) nie zajmujące klatek dla dysków hot-plug

4.1.2.8. możliwość integracji dedykowanej, wewnętrznej pamięci flash przeznaczonej dla wirtualizatora w slocie M.2 bez zajmowania wnęk dyskowych serwera , z możliwością konfiguracji zabezpieczenia RAID 1

4.1.2.9. kompatybilność BIOS

4.1.2.10. kompatybilność z UEFI i PXE

4.1.2.11. kompatybilność z UEFI kompatybilność z PCI Express generacji 3

4.1.2.12. bootowanie systemu operacyjnego z dysku m.2

4.1.3. **Procesory**

4.1.3.1. zainstalowane dwa procesory 28-rdzeniowe w architekturze x86 osiągające w testach wydajności wynik SPECrate2017_int_base minimum 350 punktów

4.1.3.2. NIE dopuszcza się serwerów o innej ilości procesorów oraz procesorów o innej ilości rdzeni fizycznych z uwagi na optymalizację kosztową licencjonowania aplikacji i systemów operacyjnych

4.1.3.3. procesory muszą obsługiwać technologię automatycznego, asymetrycznego podnoszenia taktowania częstotliwości zegara rdzeni fizycznych

4.1.4. **Pamięć RAM**

4.1.4.1. zainstalowane min. 384 GB pamięci RAM typu DDR4 Registered, minimum 2900 MT/s lub MHz w kościach o pojemności 32 GB

4.1.4.2. technologie zabezpieczania pamięci:

4.1.4.2.1. system kodowania korekcyjnego ((ang. ECC – error correction coding) - np. Advanced ECC lub Extended ECC,

4.1.4.2.2. technologia umożliwiająca pracę serwera w przypadku uszkodzenia pojedynczego modułu pamięci RAM – np. SDDC

4.1.4.2.3. technologie umożliwiające uruchomienie funkcjonalności dodatkowej redundancji np. memory mirroring lub memory sparing,

4.1.4.3. możliwość rozbudowy pamięci RAM serwera do pojemności co najmniej 768GB

4.1.5. **Kontrolery LAN**

4.1.5.1. minimum 4 porty o szybkości 1Gbit/s, niezajmujące slotu PCI Express (dopuszcza się instalację w slocie PCI Express pod warunkiem dostarczenia serwera z większą niż wymagana ilości slotów PCI Express)

4.1.5.2. minimum 4 porty 25Gb realizowane przez dwie dwuportowe karty 10/25 Gbit/s w pełni obsadzone wkładkami SFP28 SR LC

4.1.6. **Porty**

4.1.6.1. zintegrowana karta graficzna ze złączem VGA

4.1.6.2. min 1 x USB 2.0 dostępne na froncie obudowy

4.1.6.3. min 2 x USB 3.0 dostępne z tyłu serwera

4.1.6.4. Ilość dostępnych złącz VGA i USB nie może być osiągnięta poprzez stosowanie zewnętrznych przejściówek, rozgałęziaczy czy dodatkowych kart rozszerzeń zajmujących jakikolwiek slot PCI Express serwera

4.1.7. **Zasilanie, chłodzenie**

4.1.7.1. redundantne zasilacze hotplug o sprawności 94% i efektywnej mocy gwarantującej stabilną pracę przy maksymalnym obciążeniu serwera

4.1.7.2. dwa przewody zasilające C13-C14 o minimalnej długości 1,8 m

4.1.7.3. redundantne wentylatory hotplug

4.1.8. **Zarządzanie**

4.1.8.1. wbudowane diody informacyjne lub wyświetlacz informujące o stanie serwera minimum sygnalizacja (poprawna praca/usterka) dla komponentów serwerów

4.1.8.2. sygnalizacja pracy\zasilania

4.1.8.3. identyfikacji serwera (włączana zdalnie)

4.1.8.4. zintegrowany z płytą główną serwera kontroler sprzętowy zdalnego zarządzania zgodny z IPMI wersji 2.0

4.1.8.5. niezależny od systemu operacyjnego, sprzętowy kontroler umożliwiający pełne zarządzanie, zdalny restart serwera

4.1.8.6. dedykowana karta LAN 1 Gb/s RJ-45 do komunikacji wyłącznie z kontrolerem zdalnego zarządzania z możliwością przeniesienia tej komunikacji na inną kartę sieciową współdzieloną z systemem operacyjnym

4.1.8.7. wsparcie dla VLAN tagging

4.1.8.8. dostęp poprzez przeglądarkę Web (SSL) i SSH

4.1.8.9. integracja z zewnętrznym systemem uwierzytelniania i uprawniania (LDAP, Active Directory)

4.1.8.10. zarządzanie mocą i jej zużyciem oraz monitoring zużycia energii

4.1.8.11. możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer

4.1.8.12. zarządzanie alarmami

4.1.8.13. możliwość przejęcia konsoli tekstowej

4.1.8.14. przekierowanie konsoli graficznej na poziomie sprzętowym oraz możliwość montowania zdalnych napędów i ich obrazów na poziomie sprzętowym (cyfrowy KVM) pełne wsparcie dla technologii HTML5

4.1.8.15. sprzętowy monitoring serwera w tym stanu dysków twardych i kontrolera RAID (bez pośrednictwa agentów systemowych)

4.1.8.16. rozwiązanie musi umożliwiać instalację obrazów oprogramowania podsystemów, własnych narzędzi diagnostycznych w obrębie dostarczonej dedykowanej pamięci (pojemność dostępna dla obrazów własnych – minimum 16GB). Dopuszcza się zastosowanie zewnętrznej pamięci FLASH o tej pojemności z interfejsem min. USB 3.0 podłączonej z tyłu serwera o długości nieprzekraczającej 25mm

4.1.8.17. możliwość konfiguracji i wykonania aktualizacji BIOS, UEFI, Firmware, sterowników serwera bezpośrednio z GUI (graficzny interfejs) karty zarządzającej serwera bez pośrednictwa innych nośników zewnętrznych i wewnętrznych poza obrębem karty zarządzającej (w szczególności bez pendrive, dysków twardych wewn. i zewn., itp.) – możliwość manualnego wykonania aktualizacji jak również możliwość automatyzacji

4.1.8.18. rozwiązanie musi umożliwiać konfigurację i uruchomienie automatycznego powiadomienia serwisu o zbliżającej się lub istniejącej usterce serwera (co najmniej

dyski twarde, zasilacze, pamięć RAM, procesory, wentylatory, kontrolery RAID, karty rozszerzeń)

4.1.8.19. oprogramowanie zarządzające i diagnostyczne wyprodukowane przez producenta serwera umożliwiające konfigurację kontrolera RAID, instalację systemów operacyjnych, zdalne zarządzanie, diagnostykę i przewidywanie awarii w oparciu o informacje dostarczane w ramach zintegrowanego w serwerze systemu umożliwiającego monitoring systemu i środowiska (m.in. temperatura, dyski, zasilacze, płyta główna, procesory, pamięć operacyjna itd.)

4.1.8.20. współpraca z rozwiązaniami automatyzującymi administrację infrastrukturą informatyczną (Ansible, Salt, itp.) przy konfiguracji, zarządzaniu i aktualizacji serwera

4.1.8.21. zintegrowany z płytą główną serwera kontroler sprzętowy zdalnego zarządzania zgodny z IPMI wersji 2.0. kompatybilność z IPv6

4.1.8.22. kompatybilność ze standardem Redfish

4.1.9. **Centralne zarządzanie serwerami**

4.1.9.1. Oprogramowanie wraz z licencjami umożliwiające zarządzanie wieloma serwerami poprzez ich wbudowane kontrolery. Jeżeli kontrolery zarządzania zainstalowane w serwerach wymagają dodatkowych licencji do współpracy z oprogramowaniem należy je dostarczyć wraz z serwerami

4.1.9.2. Centralna konsola zarządzania cyklem życia serwerów musi umożliwiać: zdalną zmianę konfiguracji, aktualizację oprogramowania układowego i sterowników, monitorowanie stanu pracy komponentów znajdujących się w serwerach, uruchamianie skryptów

4.1.9.3. Wspierane OS :

4.1.9.3.1. Windows Server 2019

4.1.9.3.2. Windows Server 2016

4.1.9.3.3. VMWare

4.1.9.3.4. SLES

4.1.9.3.5. RHEL

4.1.10. **Dokumentacja, inne**

4.1.10.1. certyfikacja producenta serwera do poprawnej pracy ciągłej urządzenia w oferowanej konfiguracji w temperaturze otoczenia nie przekraczającej 35 stopni Celsjusza – wymagane oświadczenie producenta serwera przy odbiorze sprzętu

4.1.10.2. serwer musi być fabrycznie nowy i pochodzić z oficjalnego kanału dystrybucyjnego

4.1.10.3. ogólnopolska, telefoniczna infolinia/linia techniczna producenta serwera lub serwis www) w czasie obowiązywania gwarancji na sprzęt lub strona Web umożliwiające po podaniu numeru seryjnego urządzenia weryfikację:

4.1.10.3.1. konfiguracji sprzętowej serwera, w tym model i typ dysków twardych

4.1.10.3.2. procesora

4.1.10.3.3. ilość fabrycznie zainstalowanej pamięci operacyjnej

4.1.10.3.4. czasu obowiązywania i typ udzielonej gwarancji

4.1.10.4. możliwość aktualizacji i pobrania sterowników do oferowanego modelu serwera w najnowszych certyfikowanych wersjach bezpośrednio z sieci Internet za pośrednictwem strony www producenta serwera

4.1.11. **Kontrolery dyskowe, I/O**

4.1.11.1. możliwość skonfigurowania RAID 0, 1, 10, 5, 50, 6, 60

4.1.11.2. zainstalowany kontroler dysków twardych certyfikowany do współpracy z wirtualizatorem posiadający minimum 2GB pamięci podręcznej cache z zapisem na nieulotną pamięć w przypadku awarii zasilania

4.1.12. **Dyski twarde**

4.1.12.1. Zainstalowane dwa dyski SSD m.2 o pojemności minimum 400GB każdy pracujące w reżimie RAID1 umożliwiające rozruch systemu operacyjnego [1]

4.1.12.2. Zainstalowane dwa dyski SSD o pojemności minimum 400GB 2,5 cala

4.1.12.3. Obudowa serwera musi umożliwiać rozbudowę o min. 6 dysków 2,5 cala (6 wolnych wnęk dla dysków twardych Hotplug 2,5'')

4.2. System pamięci obiektowo-blokowej

Zamawiający wymaga dostarczenia systemu pamięci obiektowo-blokowej - dwóch macierzy dyskowych: (po jednej dla pojedynczego centrum przetwarzania danych - Lokalizacji)

4.2.1. **Główne wymagania systemu:**

4.2.1.1. System pamięci obiektowo – blokowej o wysokości do 6 U

4.2.1.2. Obsługiwane protokoły z których macierz będzie wystawiać przestrzeń dyskową : iSCSI, NFS, CIFS, FC, S3

4.2.1.3. Funkcje: deduplikacja, kompresja, snapshot'y (w tym dla baz Oracle)

4.2.1.4. Kompatybilność z systemami AIX (IBM Power)

4.2.1.5. Obsługa replikacji danych pomiędzy systemami umieszczonymi w dwóch ośrodkach przetwarzania

4.2.1.6. Zabezpieczenia przed utratą danych typu RAID 6 (pozwalające na bezprzerwową pracę w przypadku awarii 2 dysków w grupie)

4.2.1.7. Min. jeden dysk nadmiarowy (spare)

4.2.1.8. Redundatne kontrolery sprzętowe

4.2.1.9. Redundatne zasilacze

4.2.1.10. Skalowanie do min. 50 PB

4.2.1.11. Interfejsy sieciowe min. :

4.2.1.11.1. 4x 25GbE z wkładkami sfp+ dla każdego kontrolera

4.2.1.11.2. 4x 32Gb FC z wkładkami FC dla każdego kontrolera

4.2.1.11.3. Pojemność netto 45TB realizowana przez dyski SSD nvme

4.2.2. **Szczegółowy opis funkcjonalności i parametrów technicznych:**

4.2.2.1. Obudowa i komponenty

System musi być dostarczony ze wszystkimi komponentami do instalacji w szafie rack 19''. Podzespoły urządzenia tj. wentylatory, zasilacze muszą być w pełni redundantne, żeby zapewnić odpowiedni poziom bezpieczeństwa

4.2.2.2. Pojemność

4.2.2.2.1. NVME od 900GB do 15 400GB

4.2.2.2.2. System musi zostać dostarczony w konfiguracji zawierającej minimum: 18 dysków 3.84 TB NVMe SSD

4.2.2.2.3. posiadać możliwość rozbudowy o kolejne dyski System musi wspierać dyski o wielkościach: SSD od 960GB do co najmniej 15400GB

4.2.2.3. Kontroler

4.2.2.3.1. Dwa kontrolery wyposażone w przynajmniej 128GB cache każdy

4.2.2.3.2. W przypadku awarii zasilania dane nie zapisane na dyski, przechowywane w pamięci muszą być zabezpieczone za pomocą podtrzymania bateryjnego przez minimum 72 godziny lub za pomocą zrzutu danych na pamięć nie ulotną

[1] Stanowi kryterium oceny ofert

4.2.2.3.3. Macierz musi pozwalać na rozbudowę klastra do 12 kontrolerów (6 macierzy po dwa kontrolery) lub musi pozwalać na obsługę przynajmniej 1500 dysków w obrębie pary kontrolerów lub klastra

4.2.2.3.4. Rozwiązanie musi pozwalać także na rozbudowę kontrolerów w technologii NVMe z obsługą do min 560 dysków w technologii NVME

4.2.2.3.5. Zamawiający dopuści rozwiązanie, które nie wspiera dysków NVME przy założeniu zaoferowania rozwiązania z min 896GB pamięci cache opartej o RAM do odczytu i zapisu

4.2.2.4. Interfejsy

4.2.2.4.1. Oferowana macierz musi posiadać minimum:

4.2.2.4.1.1. 8 portów 25GbE (SFP+)

4.2.2.4.1.2. 8 portów 32Gb (FC)

4.2.2.4.1.3. 4 porty 10GbE

4.2.2.4.1.4. 2 porty 1GbE RJ45

4.2.2.4.1.5. 8 portów 12Gb SAS

4.2.2.4.2. Jeśli korzystanie z któregoś z wyżej wymienionych portów wymaga zastosowania wkładek (np. SFP+), zamawiający wymaga ich dostarczenia wraz z urządzeniem

4.2.2.4.3. System przestrzeni dyskowej musi wspierać rozbudowę o porty:

4.2.2.4.3.1. 32Gb FC minimum 8 sztuk

4.2.2.4.3.2. 100GbE minimum 8 sztuk

4.2.2.4.4. Zamawiający dopuszcza rozwiązanie, które nie wspiera portów 100GbE o ile zaoferowane rozwiązanie w ramach klastra max 4 kontrolerów będzie pozwalać na rozbudowę do min 60 portów 25GbE

4.2.2.5. RAID

System RAID musi zapewniać taki poziom zabezpieczania danych, aby był możliwy do nich dostęp w sytuacji awarii minimum dwóch dysków w grupie RAID

4.2.2.6. Kopie migawkowe

Macierz musi być wyposażona w system kopii migawkowych, dostępny dla wszystkich rodzajów danych przechowywanych na macierzy. System kopii migawkowych nie może powodować spadku wydajności macierzy +/-5%.

4.2.2.7. Obsługiwane protokoły:

Macierz musi obsługiwać jednocześnie protokoły FC; iSCSI; NFS; CIFS/SMB; S3. Zamawiający w tym postępowaniu wymaga dostarczenia licencji na wszystkie wymienione protokoły

4.2.2.8. Inne wymagania

4.2.2.8.1. Macierz musi posiadać funkcjonalność eliminacji (deduplikacji) identycznych bloków danych in-line

4.2.2.8.2. Macierz musi posiadać także funkcjonalność kompresji danych in-line

4.2.2.8.3. Jeżeli oferowane rozwiązanie nie pozwala na deduplikację i kompresję w locie lub nie posiada możliwości deduplikacji i kompresji zamawiający wymaga dostarczenie 4-krotnej pojemności wyspecyfikowanej w powyższym punkcie 4.2.2.2 „Pojemność”

4.2.2.8.4. Macierz musi posiadać wsparcie dla wielościeżkowości dla systemów Windows 2003/2008, Linux, RHEV, Vmware, Unix

4.2.2.8.5. Macierz musi posiadać funkcjonalność priorytetyzacji zadań w tym ustawienie max parametrów (I/Ops i Mbps) dla poszczególnych LUN

4.2.2.8.6. Macierz musi posiadać natywną obsługę protokołu S3, tj. bez żadnych zewnętrznych elementów pośredniczących. Protokół S3 powinien być serwowany bezpośrednio przez macierz

4.2.2.8.7. Macierz musi umożliwiać dynamiczną zmianę rozmiaru wolumenów logicznych bez przerywania pracy macierzy i bez przerywania dostępu do danych znajdujących się na danym wolumenie

4.2.2.8.8. Macierz musi posiadać funkcjonalność replikacji danych z inna macierzą tego samego producenta w trybie synchronicznym i asynchronicznym. Funkcjonalność replikacji danych musi być natywnym narzędziem macierzy. Przed procesem replikacji macierz musi umożliwiać włączenie procesu deduplikacji danych i kompresji danych w celu optymalizacji wykorzystania łącza dla replikowanych zasobów lub zamawiający wymaga dostarczenia zewnętrznego narzędzia do deduplikowania replikowanych danych lub dwukrotnego zwiększenia pojemności ze względu na rozważaną w przyszłości replikację całości zasobów. Zamawiający dopuści rozwiązanie bez wsparcia deduplikowanych danych w przypadku gdy oferujący dostarczy 4-krotnie większą pojemność macierzy z uwagi na brak praktycznego wykorzystania deduplikacji i kompresji danych

4.2.2.8.9. Macierz musi posiadać funkcjonalność klonowania danych bez potrzeby fizycznego kopiowania danych na nośnikach

4.2.2.8.10. Macierz musi posiadać funkcjonalność wykonania spójnego snapshot-u dla następujących aplikacji:

- 4.2.2.8.10.1. Vmware
- 4.2.2.8.10.2. SAP
- 4.2.2.8.10.3. Oracle
- 4.2.2.8.10.4. MS Exchange oraz MS SQL

4.2.2.8.11. Oferowana konfiguracja macierzy musi pozwalać na osiągnięcie wydajności do 250 000IOPS przy 8Kb bloku i stosunku 70%/30% odczyt/zapis. Zamawiający wraz z ofertą wymaga dostarczenia oficjalnego dokumentu producenta z wymiarowaniem wydajności oraz dopuszcza możliwość sprawdzenia wydajności macierzy przy odbiorze

4.2.2.8.12. Macierz musi posiadać narzędzie umożliwiające generowanie raportu o konfiguracji, utworzonych dyskach logicznych i woluminach oraz ich zajętości wraz z podziałem na rzeczywiste dane, kopie migawkowe oraz dane wewnętrzne macierzy

4.2.2.8.13. Macierz musi być wyposażona oprogramowanie do audytu zasobów plikowych w szczególności pozwalać na:

- 4.2.2.8.13.1. blokowanie zapisywania plików z określonym (do zdefiniowania przez administratora) rozszerzeniem
- 4.2.2.8.13.2. monitorowaniu operacji wykonywanych na plikach

4.2.2.8.14. Wszystkie funkcjonalności muszą być dostarczone na maksymalną pojemność macierzy

4.2.2.8.15. Z macierzą zamawiający wymaga dostarczenia oprogramowania które pozwala na:

- 4.2.2.8.15.1. monitoring wykorzystania przestrzeni na macierzy
- 4.2.2.8.15.2. monitoring grup RAIDowych
- 4.2.2.8.15.3. monitoring wykonywanych backupów/replikacji danych między macierzami
- 4.2.2.8.15.4. monitoring wydajności macierzy
- 4.2.2.8.15.5. analizę i diagnozę spadku wydajności

4.2.2.8.16. Wszystkie funkcjonalności muszą być dostarczone na maksymalną pojemność urządzenia i pozwalać na wspólne działanie (żadna funkcjonalność nie może wykluczać działania innej funkcjonalności)

4.2.2.8.17. Możliwość skonfigurowania grup RAID potrójnej parzystości[2]

4.2.2.9. Wykonawca zapewni instruktaż stanowiskowy w zakresie użytkowania i administrowania systemem pamięci obiektowo - blokowej operacyjnymi zgodnie z zakresem przedstawionym poniżej:

4.2.2.9.1. Eksploatacja sprzętu fizycznego w zakresie podłączenia sprzętu, wymiany elementów hot-plug i innych podstawowych czynności administracyjno-utrzymaniowych

4.2.2.9.2. Przegląd funkcjonalności

4.2.2.9.3. Zarządzanie sprzętem z poziomu konsoli GUI

4.2.2.9.4. Zarządzanie sprzętem z poziomu konsoli CLI

4.2.2.9.5. Przeprowadzenie konfiguracji sprzętu

4.2.2.9.6. Konfiguracja dysków i grup dyskowych

4.2.2.9.7. Udostępnienie danych po protokołach (iSCSI, FC, NFS, CIFS, S3)

4.2.2.9.8. Kopie typu „Snapshot”

4.2.2.9.9. Przeprowadzenie aktualizacji systemu

4.2.2.9.10. Konfiguracja replikacji pomiędzy macierzami (w dwóch lokalizacjach)

4.2.2.9.11. Zgłaszanie awarii i zarządzanie zgłoszeniami

4.2.2.9.12. Odtwarzanie po awarii

4.2.2.9.13. Praktyczne wykorzystanie pozostałych funkcjonalności

4.2.2.9.14. Inne niezbędne podstawowe funkcjonalności administracyjno-utrzymaniowe

4.3. Środowisko zarządzania kontenerami

Zamawiający wymaga dostarczenia oprogramowania do zarządzania kontenerami wraz z licencjami umożliwiającymi pracę tego oprogramowania na serwerach wymienionych w punkcie 4.1 „Serwery obliczeniowe”. Licencje muszą być dostarczone w ilości która w pełni pokryje zasoby sprzętowe serwerów i umożliwi wykorzystanie w pełni ich zasobów sprzętowych pracujących w dwóch lokalizacjach. Rozwiązanie ma pozwolić na uruchomianie nielimitowanej ilości kontenerów i maszyn wirtualnych.

Środowisko zarządzania kontenerami musi spełniać następujące wymagania:

4.3.1. Musi umożliwiać instalację na serwerach fizycznych działających pod kontrolą systemu operacyjnego klasy Linux

4.3.2. Umożliwiać instalację w konfiguracji wysokiej dostępności bez pojedynczego punktu awarii, gdzie każdy komponent mający wpływ na dostępność Oprogramowania będzie uruchomiony w co najmniej dwóch aktywnych instancjach

4.3.3. Umożliwiać izolację aplikacji przy użyciu technologii kontenerów w taki sposób, że na jednej instancji systemu operacyjnego równocześnie może być uruchomionych wiele odizolowanych aplikacji mających dostęp do ograniczonych zasobów systemowych takich jak pamięć RAM, moc procesora i system plików

4.3.4. Do izolacji kontenerów na poziomie systemu operacyjnego muszą być wykorzystywane mechanizmy SElinux, Cgroups, Namespaces

4.3.5. Umożliwiać deklaratywne definiowanie limitów zasobów systemowych takich jak pamięć RAM i moc procesora, które będą dostępne dla całej aplikacji jak i dla poszczególnych kontenerów aplikacji

4.3.6. Umożliwiać deklaratywne definiowanie globalnych limitów zasobów systemowych takich jak pamięć RAM i moc procesora, które są współdzielone przez wiele aplikacji

[2] Stanowi kryterium oceny ofert

4.3.7. Zawierać wbudowany rejestr obrazów Docker i OCI
4.3.8. Umożliwiać instalację we wbudowanym rejestrze i uruchomienie dowolnych obrazów Docker i OCI
4.3.9. Zawierać mechanizm umożliwiający agregację wielu wersji obrazów (tagów) pod jedną wspólną nazwą, która może być użyta jako referencja do wersji obrazu w konfiguracji Oprogramowania środowiska zarządzania kontenerami
4.3.10. Umożliwiać uruchamianie aplikacji stanowych, które zapisują i odczytują dane z trwałego nośnika poprzez jeden z interfejsów: NFS v3 i v4, Ceph RDB, GlusterFS, Openstack Cinder, iSCSi, Fibre Channel, Google GCE Volumes, Amazon EBS Volumes, Azure Disk, Azure File, VMWare vSphere
4.3.11. Umożliwiać instalację warstwy trwałych nośników danych bezpośrednio na węzłach klastra w taki sposób, żeby nośniki danych były dostępne lokalnie
4.3.12. Komunikacja pomiędzy aplikacjami i usługami uruchomionymi na Środowisku zarządzania kontenerami musi odbywać się poprzez wewnętrzną wirtualną sieć utworzoną w ramach Oprogramowania
4.3.13. Umożliwiać konfigurację sieci w taki sposób, żeby poszczególne aplikacje mogły być od siebie sieciowo odizolowane i jakakolwiek komunikacja pomiędzy nimi była zablokowana
4.3.14. Umożliwiać mikrosegmentację sieci w taki sposób, że można precyzyjnie określić jakie usługi mogą się komunikować z innymi usługami z dokładnością co do określenia konkretnego portu
4.3.15. Komunikacja pomiędzy użytkownikami (także systemami zewnętrznymi) a aplikacjami uruchomionymi na środowisku zarządzania kontenerami musi odbywać się poprzez dedykowany moduł (router) zapewniający komunikację HTTP, HTTPS, Websocket, TLS i SNI
4.3.16. Umożliwiać jednoczesne uruchomienie dwóch wersji aplikacji lub usługi i procentowe rozdzielenie ruchu sieciowego do poszczególnych wersji aplikacji lub usługi
4.3.17. Umożliwiać taką konfigurację aplikacji, żeby cały ruch sieciowy ze wszystkich usług danej aplikacji wychodził poza środowiskiem zarządzania kontenerami z jednego wybranego adresu IP bez względu na to na którym węźle klastra dana usługa jest uruchomiona
4.3.18. Umożliwiać budowanie kontenerów i uruchamianie aplikacji tworzonych w następujących technologiach: Node.js 8/10/12, Ruby 2.4/2.5/2.6, Perl 5.26, PHP 7.2/7.3, Python 2.7/3.6 bez konieczności definiowania pliku Dockerfile
4.3.19. Umożliwiać budowanie i uruchamianie aplikacji tworzonych w technologii J2EE 6 i J2EE 7 bez konieczności definiowania pliku Dockerfile
4.3.20. Umożliwiać budowanie kontenerów i uruchamianie aplikacji tworzonych w technologii Microsoft .NET Core 2.1/3.0/3.1 bez konieczności definiowania pliku Dockerfile
4.3.21. Umożliwiać budowanie kontenerów i uruchomienie dowolnych bibliotek framework'ów zgodnych z wyżej wymienionymi technologiami bez konieczności definiowania pliku Dockerfile
4.3.22. Zawierać wbudowane mechanizmy umożliwiające automatyzację budowania kontenerów, wdrożenia i uruchomienia aplikacji bezpośrednio z kodu źródłowego aplikacji bez konieczności definiowania pliku Dockerfile
4.3.23. Umożliwiać budowanie i uruchamianie aplikacji stanowych i bezstanowych
4.3.24. Zawierać gotowe szablony aplikacji, które umożliwiają po parametryzacji zbudowanie i uruchomienie na środowisku zarządzania kontenerami aplikacji bez konieczności definiowania pliku Dockerfile
4.3.25. Zawierać gotowe narzędzia umożliwiające automatyczne zbudowanie aplikacji razem z zależnościami w formacie obrazu Docker lub OCI
4.3.26. Umożliwiać skonteneryzowanie i uruchomienie aplikacji dostarczonych w postaci binarnej bez konieczności kompilacji kodu źródłowego i tworzenia pliku Dockerfile

4.3.27. Obrazy Docker zbudowane w środowisku zarządzania kontenerami muszą dawać możliwość uruchomienia zarówno na innych instancjach Oprogramowania jak i poza nią w dowolnym środowisku uruchomieniowym Docker lub OCI
4.3.28. Zawierać gotowe narzędzia umożliwiające automatyczne zbudowanie aplikacji opisanej plikiem konfiguracyjnym Dockerfile i jej uruchomienie na środowisku zarządzania kontenerami
4.3.29. Umożliwiać uruchomienie z gotowych obrazów Docker serwera aplikacji J2EE zgodnego ze standardami J2EE 6 i J2EE 7
4.3.30. Zawierać i umożliwiać uruchomienie z gotowych obrazów Docker kontenera serwletów zgodnego ze standardami servlet 3.0, servlet 3.1 i servlet 4.0
4.3.31. Zawierać i umożliwiać uruchomienie z gotowych obrazów Docker aplikacji J2SE 1.8 zbudowanych w oparciu o SpringBoot
4.3.32. Zawierać i umożliwiać uruchomienie z gotowych obrazów Docker komponentów middleware takich jak rozproszony bufor danych (in memory data grid), platforma kolejkowa (messaging), platforma integracyjna, silnik reguł biznesowych, silnik automatyzacji procesów bizensowych, serwer pojedyńczego logowania (SSO)
4.3.33. Zawierać i umożliwiać uruchomienie z gotowych obrazów Docker serwerów baz danych, w tym minimalnie wersji:
  4.3.33.1. MySQL 8.0 i nowsze,
  4.3.33.2. MariaDB 10.2 i nowsze
  4.3.33.3. PostgreSQL 9.6 i nowsze
  4.3.33.4. MongoDB 3.4 i nowsze
4.3.34. Zawierać i umożliwiać uruchomienie z gotowych obrazów Docker serwera CI/CD Jenkins
4.3.35. Umożliwiać dostęp do publicznego rejestru obrazów, z którego można pobrać aktualizowane i certyfikowane przez dostawcę Pakietu Oprogramowania wyżej wymienione obrazy Docker
4.3.36. Zawierać i umożliwiać uruchomienie centralnego serwera agregacji logów aplikacji opartego na technologii ElasticSearch, Kibana i Fluentd, który umożliwia długotrwałe przechowywanie logów na trwałych nośnikach danych
4.3.37. Zawierać i umożliwiać uruchomienie serwera agregacji metryk aplikacji działających na środowisku oraz samego środowiska opartego na technologii Prometheus który umożliwia długotrwałe przechowywanie metryk na trwałych nośnikach danych
4.3.38. Umożliwiać zbieranie i przechowywanie metryk aplikacji przez określony czas
4.3.39. Udostępniać interfejs API dający dostęp do metryk aplikacji z zewnętrznych narzędzi
4.3.40. W przypadku uruchamiania aplikacji z obrazów Docker muszą one dawać możliwość uruchomienia jako użytkownik systemowy bez pełnych praw administracyjnych. Niedozwolone jest aby kontener aplikacji był uruchomiany z obrazu Docker na prawach użytkownika root
4.3.41. Umożliwiać przenoszenie aplikacji pomiędzy różnymi instancjami środowiska zarządzania kontenerami które mogą być uruchomione w różnych konfiguracjach (serwery fizyczne, wirtualne, chmura prywatna, publiczna)
4.3.42. Umożliwiać uruchomienie nowej wersji aplikacji przy zachowaniu pełnej dostępności aplikacji i bez konieczności jej zatrzymania lub ograniczenia dostępności (rolling upgrade)
4.3.43. Umożliwiać automatyczne cofnięcie wdrożenia aplikacji (deployment) do jednej z poprzednich wersji
4.3.44. Zawierać wbudowany mechanizm automatycznego uruchamiania wdrożenia nowej wersji kontenera w momencie dostarczenia do rejestru obrazów nowej wersji obrazu
4.3.45. Umożliwia elastyczne konfigurowanie topologii aplikacji w tym klastra kilku instancji z możliwością rozmieszczenia poszczególnych instancji pomiędzy różne serwery fizyczne lub wirtualne

4.3.46. W przypadku klastrowania aplikacji rozwiązanie musi zapewniać mechanizm rozłożenia ruchu pomiędzy instancjami aplikacji (load balancing)
4.3.47. Umożliwiać podłączenie zewnętrznych komponentów do rozkładania ruchu pomiędzy instancjami aplikacji (zewnętrzny load balancer)
4.3.48. Umożliwiać uruchamiania wielu aplikacji równocześnie na współdzielonych zasobach sprzętowych
4.3.49. Zawierać wbudowany mechanizm skalowania, który pozwala określić deklaratywnie ile instancji danej aplikacji ma być uruchomionych jednocześnie i pozwala na dynamiczne jej modyfikowanie
4.3.50. Zawierać konfigurowalne mechanizmy monitorowania stanu aplikacji oraz automatyczne mechanizmy przywracania topologii aplikacji zgodnego ze zdefiniowaną topologią i konfiguracją mechanizmu skalowania
4.3.51. Zawierać wbudowane mechanizmy automatycznego skalowania aplikacji (uruchamiania lub wyłączania kolejnych instancji aplikacji) w oparciu o metryki zużycia zasobów systemowych przez aplikację
4.3.52. Zawierać wbudowaną konsolę administracyjną umożliwiającą wykonywanie zadań administracyjnych przez przeglądarkę internetową
4.3.53. Zawierać wbudowany portal samoobsługowy, który umożliwia uruchomienie nowej aplikacji oraz konfigurację i monitorowanie istniejących aplikacji przez przeglądarkę internetową
4.3.54. Zawierać wbudowane narzędzia umożliwiające administrację i konfigurację rozwiązania z poziomu linii poleceń działające na systemach operacyjnych:
    4.3.54.1. Microsoft Windows Server 2016 i nowsze
    4.3.54.2. Red Hat Enterprise Linux 7 i nowsze
    4.3.54.3. MacOS X
4.3.55. Zawierać wbudowany interfejs programistyczny API dostępny przez protokół REST umożliwiający administrację rozwiązaniem przy użyciu narzędzi zewnętrznych
4.3.56. Zawierać wbudowane mechanizmy uwierzytelniania i autoryzacji użytkowników oparte na OAuth 2.0, oraz umożliwia konfigurację dostępu opartego na rolach dla różnych grup użytkowników w tym administratorów i programistów
4.3.57. Umożliwiać definiowanie różnych projektów dla poszczególnych aplikacji i przypisywania uprawnień do nich dla określonych grup programistów
4.3.58. Zapewniać integrację z zewnętrznymi repozytoriami użytkowników w tym Microsoft Active Directory lub LDAP oraz serwerami autoryzacji zgodnymi z OAuth 2.0
4.3.59. Umożliwiać zablokowanie uruchomienia kontenera z obrazu, którego zawartość jest nieznana lub zawiera lukę bezpieczeństwa
4.3.60. Zawierać wbudowany mechanizm umożliwiający administratorom określenie uprawnień dla uruchamianych na rozwiązaniu kontenerów takich jak nazwy i uprawnienia użytkownika, dostępy do zasobów sprzętowych oraz profile seccomp
4.3.61. Umożliwiać uruchamianie kontenerów OCI lub Docker bez konieczności instalacji oprogramowania Docker
4.3.62. Zawierać rozwiązanie do kopiowania obrazów pomiędzy rejestrami oraz systemem plików bez konieczności instalacji oprogramowania Docker
4.3.63. Pełny kod źródłowy Oprogramowania musi być dostępny na warunkach licencyjnych oprogramowania typu open source
4.3.64. Środowisko zarządzania kontenerami musi umożliwiać bezpośrednią integrację z urządzeniem balansującym ruch sieciowy marki F5 posiadany przez zamawiającego
4.3.65. Relacja wsparcia technicznego między urządzeniem balansującym, a środowiskiem zarządzania kontenerami musi zapewniać pełny zakres wsparcia technicznego dla obu modeli integracji wtyczki routera urządzenia balansującego ruch sieciowy i kontrolera po stronie rozwiązania

4.3.66. Zawierać wbudowany dedykowany moduł do zarządzania i monitorowania komunikacji sieciowej dla aplikacji budowanych w architekturze mikroserwisów (Service Mesh)
4.3.67. Zawierać zintegrowane środowisko programistyczne (IDE), które umożliwia rozwijanie kodu aplikacji, jego kompilację i uruchomienie na środowisku zarządzania kontenerami bez konieczności jej konteneryzacji
4.3.68. Silnik klastra kontenerów będzie pracował w oparciu o technologię Kubernetes z zachowaniem pełnej zgodności z komendami sterującymi klastrem Kubernetes oraz interfejsem API
4.3.69. Oprogramowanie musi umożliwiać separację i bezpieczną izolacje logiczną zasobów wielu środowisk w ramach jednej infrastruktury fizycznej
4.3.70. Oprogramowanie musi umożliwiać zarządzanie uprawnieniami użytkowników i grup oraz przypisywanie ich do konkretnych środowisk (grup maszyn wirtualnych i kontenerów)
4.3.71. Środowisko konteneryzacji będzie posiadać funkcjonalność hypervisora umożliwiającego uruchamianie maszyn wirtualnych i zarządzanie nimi bazującego na silniku wirtualizacji KVM
4.3.72. W ramach funkcjonalności hypervisora, będzie możliwe uruchomienie systemów Linux w liczbie nie ograniczonej licencyjnie, objętych wsparciem technicznym producenta
4.3.73. Rozwiązanie będzie umożliwiało zarządzanie wieloma instancjami i klastrami kontenerów w Lokalizacjach z poziomu jednej - centralnej konsoli administratora oferujące centralne zarządzanie i dystrybucję aplikacji oraz centralne zarządzanie i wdrażanie polityk bezpieczeństwa w ramach zarządzanych puli.
4.3.74. Funkcjonalność centralnego zarządzania klastrami kontenerów będzie umożliwiać współpracę z środowiskami chmurowymi
4.3.75. Wykonawca zapewni instruktaż stanowiskowy w zakresie użytkowania i administrowania Środowiskiem zarządzania kontenerami zgodnie z zakresem przedstawionym poniżej:
  4.3.75.1. Charakterystyka modułów i funkcjonalności
  4.3.75.2. Instalacja i konfiguracja oprogramowania dla dwóch serwerowni
  4.3.75.3. Konfiguracja uprawnień, dostępów i zarządzanie bezpieczeństwem
  4.3.75.4. Zarządzanie oprogramowaniem przez interfejsy graficzne i tekstowe
  4.3.75.5. Tworzenie klastra Kubernetes, konfiguracja, i orkiestracja
  4.3.75.6. Konfiguracja klastrów pomiędzy dwoma lokalizacjami i zarządzanie
  4.3.75.7. Tworzenie serwisów w kontenerach i zarządzanie nimi
  4.3.75.8. Administracja kontenerami poprzez Service Mesh
  4.3.75.9. Konfiguracja izolacji pomiędzy kontenerami i projektami
  4.3.75.10. Tworzenie niestandardowych obrazów w kontenerach
  4.3.75.11. Wdrażanie aplikacji z użyciem rejestru prywatnego
  4.3.75.12. Wdrażanie aplikacji multi –kontenerowych
  4.3.75.13. Tworzenie polityk sieciowych (SDN) i rozwiązywanie problemów
  4.3.75.14. Wykorzystanie modułów oprogramowania do realizacji cyklu CI/CD
  4.3.75.15. Administracja harmonogramem zadań
  4.3.75.16. Monitorowanie metryk, stanu działania i wydajności
  4.3.75.17. Konfiguracja testów automatycznych
  4.3.75.18. Skrypty automatyzujące i narzędzia zewnętrzne do automatyzacji
  4.3.75.19. Wdrożenie bezpłatnego oprogramowania Ansible
  4.3.75.20. Automatyzacja codziennych prac wdrożeniowo – administracyjnych z Ansible
  4.3.75.21. Najczęstsze problemy występujące w Ansible i Środowisku konteneryzacji oraz rozwiązywanie ich
  4.3.75.22. Tworzenie i administracja maszynami wirtualnymi
  4.3.75.23. Integracja z technologiami sieciowymi SDN, Load Balancer
  4.3.75.24. Zgłaszanie awarii i zarządzanie zgłoszeniami

4.3.75.25. Wiedza z pozostałych obszarów niezbędna do obsługi rozwiązania na poziomie DevOps / SecOps

4.4. System backup

Zamawiający wymaga dostarczenia kompletnego rozwiązania systemowo-sprzętowego do wykonywania kopii zapasowej i archiwizacji danych. Rozwiązanie będzie składało się z sprzętu i oprogramowania dostarczonego do dwóch Lokalizacji a całość rozwiązania nie może przekraczać wielkości 2U dla każdej z Lokalizacji. Rozwiązanie musi oferować replikacje danych pomiędzy Lokalizacjami.

4.4.1. **Główne wymagania systemu backup:**

4.4.1.1. Oprogramowanie musi pozwalać na backup nieograniczonej ilości aplikacji dedykowanym agentem zainstalowanym wewnątrz serwera wirtualnego

4.4.1.2. system backup musi umożliwiać rozbudowę w ramach jednej lokalizacji jak i w ramach wielu lokalizacji

4.4.1.3. Rozwiązanie musi umożliwiać transmisję danych przy użyciu minimum dwóch połączeń 10GbE, dwóch połączeń 16Gb FC oraz portu 1GbE Base-T dla zarządzania systemem. Wszystkie porty muszą zostać wyposażone w odpowiednie wkładki (SFP / FC)

4.4.1.4. Backup min. 50 maszyn wirtualnych o łącznym rozmiarze 5 TiB

4.4.1.5. Backup min. 50 kontenerów aplikacyjnych o łącznym rozmiarze 15 TiB

4.4.1.6. Backup min. 2 serwerów fizycznych RISC z bazą danych i filesystemem (łącznie 10 TiB)

4.4.1.7. Backup min. 2 instancji danych prezentowanych obiektowo z użyciem protokołu S3 (łącznie 10 TiB)

4.4.1.8. Polityka wykonywania backupu zakłada kryterium - kopie zapasowe maszyn wirtualnych, plików i obiektów S3 są wykonywane następująco:

4.4.1.8.1. pełna kopia raz na tydzień, przyrostowa raz na dobę

4.4.1.8.2. pełna kopia bazy danych raz na dobę oraz backup logów transakcyjnych co 15 minut

4.4.1.9. Pojemność systemu musi umożliwiać retencję wszystkich backupów wynoszącą 3 miesiące

4.4.1.10. Backup danych będzie przechowywany przy użyciu dysków twardych zainstalowanych wewnątrz rozwiązania (dyski HDD akcelerowane dyskami SSD)

4.4.1.11. Przestrzeń dyskowa składowanych danych musi oferować minimum 65 TiB przestrzeni użytkowej na zapisywane dane dla rozwiązania instalowanego w pojedynczej Lokalizacji osiągana poprzez zastosowanie dysków twardych NLSAS

4.4.1.12. Dyski SSD akcelerujące operacje backup'u muszą być zainstalowane w ilości oferującej min. 5% pojemności dostarczanej w ramach dysków NLSAS

4.4.1.13. Konfiguracja sprzętowa dostarczonego rozwiązania dla każdej Lokalizacji musi oferować redundantne komponenty (zasilacze, karty sieciowe, pamięć ram, procesory) oraz zapewniać ciągłość działania w przypadku niedostępności dwóch dowolnych dysków w ramach urządzenia

4.4.2. **Wymagania funkcjonalne systemu backup:**

4.4.2.1. Rozwiązanie musi reprezentować architekturę trójwarstwową (serwer zarządzający, serwer medialny oraz klient), taka architektura pozwoli na elastyczną skalowalność rozwiązania bez względu na dynamikę przyrostu danych

4.4.2.2. Oprogramowanie nie może preferować platformy sprzętowej, nie może być profilowane pod konkretnego dostawcę sprzętu serwerowego oraz pamięci masowych. Niedopuszczalne jest aby funkcjonalności związane z zabezpieczaniem

danych były w jakikolwiek sposób związane czy zależne od konkretnego typu czy producenta urządzenia

4.4.2.3. Jeśli system backup korzysta z bazy danych to wszelkie potrzebne licencje na oprogramowanie muszą być dostarczone i stanowić całość oferty, z tym iż licencje dla silnika bazodanowego muszą pozwalać na zainstalowanie go: na serwerze fizycznym (minimum 2xCPU po 8 core), klastrze active-passive czy serwerze wirtualnym w środowisku Vmware i Hyper-V

4.4.2.4. Oprogramowanie musi pozwalać na stworzenie dla serwera zarządzającego rozwiązania wysokodostępnego z czasem przełączenia nie dłuższym niż 15 minut. Jeśli do stworzenia takowego rozwiązania potrzebne są licencje replikacyjne, klastrowe, współdzielona przestrzeń dyskowa - to muszą zostać zaoferowane. Licencje na oprogramowanie muszą pozwalać na skonfigurowanie serwerów zarządzających oraz ich replikację do drugiej lokalizacji typu standby dla serwera zarządzającego

4.4.2.5. Rozwiązanie musi zapewnić interfejs graficzny do zarządzania i instalacji

4.4.2.6. Oprogramowanie musi umożliwiać zdalne instalowanie i odinstalowywanie klienta systemu z centralnego serwera dla systemów Windows, Linux i Unix – musi być to możliwe z jednego serwera pełniącego rolę cache dla wszystkich binariów klienckich

4.4.2.7. System musi zapewniać funkcjonalność odtwarzania po awarii konfiguracji serwera zarządzającego tworzeniem kopii bezpieczeństwa i archiwów

4.4.2.8. System musi pozwalać na składowanie danych na taśmach celem przechowywania długoterminowego. Składowane dane na taśmach muszą być w formie nie zdeduplikowanej (nawodnione) po to by była możliwość odtwarzania ich bezpośrednio, a więc bez konieczności pośrednictwa dysków, buforów czy importu

4.4.2.9. System musi pozwalać na zarządzanie całością działania systemu (backup serwerów, komputerów, baz danych, maszyn wirtualnych i aplikacji) z jednej graficznej konsoli administracyjnej oraz także z użyciem Rest API

4.4.2.10. Komunikacja agentów systemu z serwerami musi odbywać się poprzez SSL – konfiguracja tego typu transferu nie może powodować konieczności instalowania dodatkowego oprogramowania

4.4.2.11. System musi pozwalać na współdzielenie napędów taśmowych w środowisku sieci SAN

4.4.2.12. System musi umożliwić przechowywanie jedynie unikalnych bloków danych tzw. deduplikacja. Funkcjonalność ta musi działać na poziomie blokowym i być wykonywana online podczas procesu tworzenia kopii danych. Deduplikacja musi być realizowana poprzez oprogramowanie systemu na dowolnym sprzęcie czy to w warstwie serwera systemu czy klienta. Pojedynczy serwer systemu musi umożliwiać przechowywanie danych po deduplikacji minimum do 200 TB (rozbudowa do tej wielkości może nastąpić tylko poprzez dodanie dodatkowych dysków czy macierzy dyskowej)

4.4.2.13. Włączenie funkcjonalności deduplikacji na kliencie musi być możliwe dla różnych systemów operacyjnych: Windows, Linux czy Unix

4.4.2.14. Globalna deduplikacja – system musi oferować deduplikację globalną co oznacza, iż niezależnie z jakich klientów dane będą deduplikowane (serwery fizyczne, hosty wirtualne, bazy i aplikacje) – deduplikacja musi opierać się na jednej centralnej bazie deduplikacyjnej

4.4.2.15. Włączenie funkcjonalności deduplikacji nie może generować wymogu instalacji dodatkowych modułów programowych po stronie klienckiej lub serwera systemu. Niedopuszczalne jest łączenie systemu z dodatkowym oprogramowaniem dla uzyskania funkcjonalności deduplikacji danych

4.4.2.16. System musi umożliwiać wykonywanie kopii w post procesie do drugiej lokalizacji przesyłając jedynie unikalne bloki danych (dla dowolnych danych: czy to z procesu backupu czy archiwizacji). A więc replikacja danych do innej lokalizacji musi być

wykonywana na danych po deduplikacji i funkcjonalność ta musi być realizowana i zarządzana z poziomu systemu

4.4.2.17. Proces przesyłania danych (replikacji) na inny serwer systemu celem tworzenia dodatkowej kopii danych nie może być zależny od warstwy sprzętowej, a więc dowolny producent serwera, dowolny producent macierzy/półki dyskowej

4.4.2.18. System musi pozwalać na instalację bazy deduplikacyjnej w układzie wysokiej dostępności (minimum na dwóch serwerach) w taki sposób, aby awaria pojedynczego serwera nie powodowała utraty możliwości deduplikacji i odtwarzania danych

4.4.2.19. System musi pozwalać na odtwarzanie zdeduplikowanych danych nawet w momencie, gdy baza deduplikacyjna jest niedostępna. Proces odtwarzania (nawadniania) zdeduplikowanych danych nie wykorzystuje bazy deduplikacyjnej

4.4.2.20. Na jednym serwerze systemu (na jednej instancji systemu operacyjnego) mogą być zainstalowane minimum dwie bazy deduplikacyjne pozwalające zwiększyć skalowalność systemu

4.4.2.21. System musi zapewniać dostęp zintegrowany z usługą katalogową, minimum to Active Directory, a więc tak zwany „Single Sign On” – pojedyncze logowanie: użytkownik po zalogowaniu do domeny AD, nie potrzebuje wykonywać następnego logowania aby zarządzać systemem poprzez konsolę administracyjną

4.4.2.22. System musi zapewniać elastyczne delegowanie uprawnień oraz audytowanie działań użytkowników. Z tym, że delegowanie uprawnień musi pozwalać na przydział uprawnień per serwer czy grupa serwerów, przydział uprawnień musi pozwalać na definiowanie uprawnień dla grup użytkowników z domeny AD

4.4.2.23. System musi pozwalać na zarządzanie poprzez „cmd” z tym, że uruchomienie jakiejkolwiek komendy/polecenia musi zostać poprzedzone koniecznością zalogowania (autentyfikacji) do systemu, funkcjonalność musi dotyczyć dowolnej platformy (minimum Windows/Linux) i nie może polegać na konieczności instalowania czy konfigurowania dodatkowych komponentów np. SSH

4.4.2.24. Komunikacja pomiędzy agentem a serwerem systemu musi opierać się na certyfikatach

4.4.2.25. System musi posiadać funkcjonalność blokowania danych do odczytu dla administratora, to znaczy, że administrator systemu nawet mając pełne uprawnienia nie może odtworzyć danych, jeśli nie jest ich właścicielem, funkcjonalność ta musi być dostępna nie tylko dla danych z laptopów/desktopów ale i dla serwerów (także dla danych plikowych i bazodanowych)

4.4.2.26. System musi pozwalać na skonfigurowanie mechanizmu podwójnej autentyfikacji administratora – do uruchomienia konsoli administracyjnej systemu potrzebne jest nie tylko logowanie, ale i dodatkowy tymczasowy kod wysyłany do administratora np. poprzez mail lub aplikację mobilną 2FA

4.4.2.27. Szyfrowanie danych musi pozwalać na wybór algorytmu (minimum dwa algorytmy: Blowfish, AES 256) także dla danych deduplikowanych na kliencie systemu

4.4.2.28. Możliwość szyfrowania musi pozwalać na elastyczny wybór miejsca szyfrowania: szyfrowanie danych na kliencie, szyfrowanie danych na serwerze backupowym i szyfrowanie tylko transmisji pomiędzy klientem backupowym a serwerem

4.4.2.29. System musi wspierać mechanizm szyfrowania danych na napędach taśmowych LTO

4.4.2.30. System musi pozwalać na ustawianie haseł dostępu do nośników tzw: media password

4.4.2.31. System musi pozwalać na integrację z zewnętrznymi repozytoriami do przechowywania kluczy szyfrującym

4.4.2.32. System musi mieć wbudowane mechanizmy zabezpieczające przed złośliwym oprogramowaniem (Ransomware), minimum to:

4.4.2.32.1. Zabezpieczenie ścieżek dostępu do danych składowanych (kopii backupowych) na dyskach – tylko procesy systemu mogą zapisywać i modyfikować dane

4.4.2.32.2. Monitorowanie nietypowych aktywności na serwerach za pomocą np. metody: Honeypot
4.4.2.32.3. Monitorowanie dużych aktywności na serwerach plikowych i desktopach, monitorowanie musi odbywać się nie rzadziej, niż co 5 minut i każdy niestandardowy wynik jest automatycznie wysyłany w postaci alertu lub notyfikacji
4.4.2.33. System musi posiadać rozbudowany system powiadamiania o zdarzeniach poprzez e-mail
4.4.2.34. System musi posiadać rozbudowany system raportowania dla administratorów, minimalny zestaw dostępnych raportów to:
4.4.2.34.1. Raport zmian/wzrostu środowiska systemu
4.4.2.34.2. Raport wykorzystania licencji
4.4.2.34.3. Raport wykonanych zadań backupowych
4.4.2.34.4. Raport wykonanych zadań odtworzeniowych
4.4.2.34.5. Zbiorcze procentowe zestawienie udanych zadań backupowych z poszczególnych serwerów
4.4.2.34.6. Zestawienie serwerów z problemami backupu
4.4.2.34.7. Zestawienie systemów nie zabezpieczanych
4.4.2.35. System musi udostępniać narzędzie do budowania raportów na podstawie zapytań do bazy danych
4.4.2.36. System musi mieć możliwość automatycznego wysyłania dowolnych raportów do wybranych użytkowników poprzez mail
4.4.2.37. System musi mieć możliwość automatycznego zapisywania raportów w formacie minimum: PDF, HTML i CSV
4.4.2.38. System musi pozwalać na definiowanie alertów per zadanie backupowe
4.4.2.39. System musi zapewniać funkcjonalność wznawiania zadań backupowych
4.4.2.40. System musi zapewniać funkcjonalność wykonywania zadania backupu wieloma równoległymi strumieniami – tzw. multistreaming. Polega ona na tym iż agent systemu równolegle czyta różne obszary danych i bez pośredniczenia dysków automatycznie wysyła je do serwera, który zapisuje te dane albo na dyski albo na nośniki taśmowe. Funkcjonalność ta musi być dostępna dla dowolnych typów danych: backup plikowy, bazodanowy
4.4.2.41. Funkcjonalność multistreamingu musi być dostępna dla deduplikacji bez względu czy następuje na kliencie czy na serwerze systemu
4.4.2.42. Rozwiązanie musi posiadać możliwość wykonywania backupu pełnego, przyrostowego, różnicowego oraz syntetycznego
4.4.2.43. System musi oferować funkcjonalność backupu blokowego, polegającego na tym, iż agent buduje własną bazę zmian bloków danych, przez co backup przyrostowy nie wymaga odczytu całych plików tylko zmienionych bloków wielokrotnie przyspieszając backup. Funkcjonalność ta musi być dostępna dla backupu danych plikowych
4.4.2.44. System musi posiadać funkcję szyfrowania i kompresji danych transmitowanych przez LAN, możliwość wykorzystania szyfrowania i kompresji musi być dostępna w dowolnej kombinacji
4.4.2.45. System ma realizować procesy backupu oraz odzyskiwania danych
4.4.2.46. System ma umożliwić tworzenie zadań backupowych w oparciu o kalendarz
4.4.2.47. System musi realizować funkcjonalność weryfikacji wykonanych kopii
4.4.2.48. System powinien umożliwiać wykorzystanie funkcjonalności Bare Metal Restore dla odtwarzania systemu po awarii, wsparcie musi być dostępne dla systemów:
4.4.2.48.1. Windows: 2016/2012/2008/2003/10/8.1/8
4.4.2.48.2. Linux: Debian/Oracle Linux/RHEL/CentOS/SUSE/Ubuntu
4.4.2.48.3. Unix: AIX/Solaris

4.4.2.48.4. OpenVMS

4.4.2.49. System musi umożliwiać integrację z mechanizmami kopii migawkowych czołowych producentów pamięci masowych minimum: HDS, Dell, HP, NetApp, EMC, IBM, Pure Storage, Nimble Storage z tym że takowy backup sterowany przez system a wykonywany przez daną macierz dyskową musi być dostępny nie tylko dla zasobów plikowych ale i aplikacji

4.4.2.50. Dla producentów: NetApp, EMC i HDS system musi umożliwiać nie tylko integrację z mechanizmami tworzenia kopii migawkowych (tzw. Snapshot) ale musi integrować się także z mechanizmami replikacyjnymi, a więc sterować replikami wykonywanymi przez macierze

4.4.2.51. System musi posiadać możliwość wykonywania kopii oraz archiwów na urządzenia dyskowe i taśmowe

4.4.2.52. System powinien umożliwiać rozszerzenie funkcjonalności o obsługę mechanizmów składowania danych w chmurze, minimum: Azure, Amazon, Google

4.4.2.53. System musi umożliwiać odtwarzanie danych plikowych pomiędzy systemami operacyjnymi np. odtwarzanie danych plikowych Linux na systemie Windows

4.4.2.54. System musi pozwalać na odtwarzanie tylko samych uprawnień do plików

4.4.2.55. System musi umożliwiać odtwarzanie zasobów plikowych bez praw dostępu (tzw. ACL)

4.4.2.56. System powinien umożliwiać rozszerzenie funkcjonalności o analizę logów z systemów zewnętrznych, na bazie zdefiniowanych kryteriów powinien generować alarmy lub akcje. Minimalne wsparcie to: Windows Event Log

4.4.2.57. Możliwość odtwarzania backupów plikowych poprzez udostepnienia CIFS lub NFS. A więc dostęp do zbackupowanych danych widocznych jako udostępnione przez sieć zasoby CIFS/NFS

4.4.2.58. System musi posiadać wbudowany mechanizm tworzenia kopii otwartych plików na platformie Windows i Linux

4.4.2.59. System musi wspierać wykonanie kopii na systemach klasy Windows (także Microsoft Cluster), Linux i Unix

4.4.2.60. System musi posiadać szerokie wsparcie dla środowisk Linux, minimum: RHEL, SUSE oraz opcjonalnie dla: Debian, Fedora, Oracle Linux, Ubuntu

4.4.2.61. System musi posiadać szerokie wsparcie dla środowisk Unix, minimum: AIX, HP-UX, Solaris

4.4.2.62. System musi wspierać funkcjonalność odtwarzania fizycznego serwera do środowiska wirtualnego, minimum: dla serwera Windows do środowiska Vmware

4.4.2.63. System musi umożliwiać uruchamianie skryptów przed i po backupie, z tym iż musi posiadać mechanizm definiowania konta użytkownika na którym te skrypty byłyby uruchamiane. Mechanizm ten musi być centralnie zarządzany poprzez konsolę administracyjną. Niedopuszczalna jest konieczność np. zmiany konta serwisowego dla danego agenta – konta serwisowe muszą być centralnie definiowane i zarządzane

4.4.2.64. System musi wspierać czołowe rozwiązania wirtualizacyjne: VMware, Hyper-V, Citrix Xen, RHEV, OracleVM. To znaczy musi posiadać dedykowanego agenta do backupu minimum całej maszyny wirtualnej bez konieczności instalowania agenta wewnątrz maszyny

4.4.2.65. System musi wspierać wersje środowisk VMware 6.0, 6.0.1, 6.5, 6.7 poprzez integrację z vStorage API

4.4.2.66. Dla backupu i odtwarzania środowisk wirtualnych opartych o Vmware musi być możliwość wyboru różnych transportów: SAN, Hot-add, NBD, SSL, NAS - gdzie transport NAS pozwala na bezpośredni odczyt i zapis danych maszyny wirtualnej z urządzenia NAS

4.4.2.67. System musi wspierać środowisko Hyper-V dla:

4.4.2.67.1. Microsoft Windows Server 2016 i nowsze (z Core Edition)

4.4.2.67.2. Microsoft Hyper-V Server 2016 i nowsze (z Core Edition)

4.4.2.68. System w kontekście platform VMware i Hyper-V - w przypadku kopii pliku maszyny wirtualnej musi wspierać granularne odtwarzanie pojedynczych plików

4.4.2.69. System musi zapewniać automatyczne wykrywanie i dodawanie do polityki backupu nowych maszyn wirtualnych

4.4.2.70. System musi umożliwiać odzyskanie i uruchomienie maszyn wirtualnych z kopii zapasowej bez oczekiwania na pełne przywrócenie maszyny wirtualnej – minimum dla Vmware

4.4.2.71. System musi umożliwiać odtworzenie zbackup'owanej maszyny wirtualnej VMware na środowisko Hyper-V

4.4.2.72. System musi wspierać mechanizm CBT (change block tracking) minimum dla Vmware i Hyper-V

4.4.2.73. System musi umożliwiać wykonanie kopii na gorąco bazy danych MySQL, PostgreSQL, Oracle, na dowolnej platformie systemu operacyjnego (Windows/Linux/Unix) poprzez dedykowanego agenta bazodanowego, transfer danych musi odbywać się bez pośredniczenia dysków, a więc transfer danych z agenta bazodanowego bezpośrednio do serwera backupowego celem zapisu na dany nośnik

4.4.2.74. System musi umożliwiać wykonanie kopii na gorąco bazy danych MS SQL, Oracle, MySQL, PostgreSQL, DB2, Informix konfiguracja agenta nie może powodować konieczności tworzenia skryptów uruchamianych po stronie klienta niezależnie czy jest to serwer fizyczny czy wirtualny. Brak skryptów musi dotyczyć dowolnych typów backupów: backup automatyczny uruchamiany poprzez harmonogram, backup manualny

4.4.2.75. Odtwarzanie danych z backupu bazodanowego (MS SQL, Oracle, MySQL, PostgreSQL, DB2) musi odbywać się poprzez konsolę administracyjną bez konieczności konfigurowania skryptów

4.4.2.76. Konfiguracja agentów backupowych dla: MS SQL, Oracle, MySQL musi odbywać się poprzez interfejs graficzny, jakakolwiek modyfikacja zasobów do backupu (np. dodanie nowej bazy) nie może powodować konieczności modyfikacji skryptów czy to dla backupów planowanych czy wykonywanych na żądanie

4.4.2.77. System musi umożliwiać wykonanie kopii na gorąco Active Directory a następnie odzyskania pojedynczych obiektów i atrybutów AD wraz z hasłami użytkowników

4.4.2.78. System musi umożliwiać odtwarzanie backupu wykonywanego online dedykowanym agentem, do pliku celem późniejszego odtwarzania bez udziały systemu. Funkcjonalność ta musi być dostępna minimum dla MS SQL, Oracle i Exchange

4.4.2.79. System musi umożliwiać wykonanie kopii na gorąco aplikacji MS Exchange a następnie odzyskania pojedynczych wiadomości

4.4.2.80. System musi umożliwiać wykonanie kopii na gorąco dla SharePoint, SAP, Sybase

4.4.2.81. Automatyczny backup logów transakcyjnych dla baz danych w oparciu o procent wolnego miejsca na systemie plikowym, minimum dla: Oracle, SQL, Notes, SAP/Oracle.

4.4.2.82. Dla MS SQL możliwość skonfigurowania rozszerzenia pozwalającego backupować i odtwarzać bazy bezpośrednio z konsoli Management Studio

4.4.2.83. Wsparcie dla backupu online dla minimum MS SQL Server 2016/2014/2012/2008/2005

4.4.2.84. Dedykowany agent bazodanowy dla backupu MS SQL na platformie Linux: Ubuntu, SUSE, RHEL

4.4.2.85. Odtwarzanie bazy SAP opartej na silniku Oracle do pliku, a więc odtwarzanie backupu online na dysk (tzw. application free restore)

4.4.2.86. Możliwość integracji kopii migawkowych dla backupu konsystentnego aplikacji i baz danych minimum: Vmware, Hyper-V, MS SQL, Exchange, MySQL, Oracle – zarządzanie

kopiami migawkowymi musi odbywać się z konsoli administracyjnej systemu backupowego a integracja zarządzania nie może odbywać się na bazie skryptów

4.4.2.87. System musi oferować mechanizm składowania kopii backupowych (retencja danych) oparty o czas i cykle. Oznacza to, iż kopia backupowa jest przechowywana w repozytorium przez określony czas (np. tydzień, miesiąc, rok) a jej automatyczne skasowanie jest wykonane jeśli spełniony jest jednocześnie warunek ilości cykli a więc ilość backupów typu pełnego lub backupów syntetycznych znajdujących się w systemie

4.4.2.88. System musi oferować rozbudowę o funkcjonalność przeszukiwania i analizy zasobów plikowych dla maszyn wirtualnych (minimum Vmware) całość działać związanych musi odbywać się na kopiach backupowych maszyn wirtualnych a nie na środowisku produkcyjnym

4.4.2.89. Musi istnieć możliwość zarządzania systemem poprzez Windows PowerShell

4.4.2.90. System musi zamierać moduł do monitorowania i zarządzania taśmami wynoszonymi z bibliotek taśmowych o funkcjonalnościami minimum:

- 4.4.2.90.1. Identyfikacja taśm, które muszą być wyciągnięte z biblioteki
- 4.4.2.90.2. Identyfikacja taśm, które można z powrotem wstawić do biblioteki taśmowej
- 4.4.2.90.3. Automatyczne przenoszenie taśm w bibliotece i notyfikacja administratorów
- 4.4.2.90.4. Identyfikacja i monitorowanie nośników (taśm) w trakcie transportu

4.4.2.91. Możliwość backupu minimum baz Oracle bez instalacji oprogramowania backupowego natomiast dane zbackupowane muszą być składowane i zarządzane przez system backupowy

4.4.2.92. Możliwość backupu środowisk konteneryzacji pracujących w technologii Kubernetes dedykowanym agentem służącym do tego rodzaju backupu bez używania zewnętrznych skryptów i narzędzi

4.4.2.93. Kryterium dodatkowo punktowane: Funkcjonalność wykonywania kopii backupowych poprzez protokół S3 na repozytorium w postaci storage'u obiektowego[3]

4.4.2.94. Wykonawca zapewni instruktaż stanowiskowy w zakresie użytkowania i administrowania Systemem Backup zgodnie z zakresem przedstawionym poniżej:

- 4.4.2.94.1. Instalacja i konfiguracja Urządzenia z Oprogramowaniem
- 4.4.2.94.2. Przegląd funkcjonalności
- 4.4.2.94.3. Konfiguracja przestrzeni dla backup 'u danych
- 4.4.2.94.4. Konfiguracja źródeł backup 'u (VM, bazy danych, zasoby plikowe, S3, itp)
- 4.4.2.94.5. Konfiguracja backupu dla elementów wchodzących w skład kompleksowego rozwiązania platformy konteneryzacyjnej (Urządzeń i Oprogramowania, środowisk wirtualnych oraz kontenerów aplikacyjnych)
- 4.4.2.94.6. Retencja danych backupu i archiwizacji
- 4.4.2.94.7. Zarządzanie harmonogramem wykonywania kopii
- 4.4.2.94.8. Raporty i statystyki
- 4.4.2.94.9. Replikacja danych
- 4.4.2.94.10. Odzyskiwanie danych
- 4.4.2.94.11. Inne niezbędne podstawowe funkcjonalności administracyjne
- 4.4.2.94.12. Praktyczne wykorzystanie pozostałych funkcjonalności rozwiązania

Pozostałe zasady realizacji niniejszego zamówienia określone zostały w rozdziale III SWZ – Projektowane postanowienia umowy.

[3] Stanowi kryterium oceny ofert