

Załącznik nr 1 do SWZ – Opis przedmiotu zamówienia dla Części 1.

Część 1. Dostawa i uruchomienie serwerów wirtualizacyjnych z repozytorium backupu.

3X SERWER WIRTUALIZACYJNY

Parametr	Charakterystyka (wymagania minimalne)
Obudowa	<p>Obudowa Rack o wysokości max 1U wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych oraz organizatorem do kabli.</p> <p>Obudowa z możliwością wyposażenia w kartę umożliwiającą dostęp bezpośredni poprzez urządzenia mobilne - serwer musi posiadać możliwość konfiguracji oraz monitoringu najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej min. (Android/ Apple iOS) przy użyciu jednego z protokołów BLE/ WIFI.</p>
Płyta główna	Płyta główna z możliwością zainstalowania do dwóch procesorów. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym.
Chipset	Dedykowany przez producenta procesora do pracy w serwerach dwuprocessorowych.
Procesor	Zainstalowane dwa procesory min. 8-rdzeniowe, min. 2.6GHz, klasy x86 dedykowane do pracy z zaferowanym serwerem umożliwiające osiągnięcie wyniku min. 169 w teście SPECrate2017_int_base, dostępnym na stronie www.spec.org dla konfiguracji dwuprocessorowej.
RAM	Minimum 128GB DDR4 RDIMM 3200MT/s, na płycie głównej powinno znajdować się minimum 16 slotów przeznaczone do instalacji pamięci. Płyta główna powinna obsługiwać do 1TB pamięci RAM.
Funkcjonalność pamięci RAM	Memory Rank Sparing, Memory Mirror, Failed DIMM isolation, Memory Address Parity Protection, Memory Thermal Throttling
Gniazda PCI	- minimum dwa sloty PCIe x16 generacji 4
Interfejsy sieciowe/FC/SAS	Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT oraz minimum 2 interfejsy sieciowe 10Gb/25Gb Ethernet w standardzie SFP28 (porty nie mogą być osiągnięte poprzez karty w slotach PCIe) Dodatkowo zainstalowana w jednym slotcie PCIe dwuportowa karta SAS 12Gb
Dyski twarde	Zainstalowane dwa dyski min. M.2 SATA o pojemności min. 480GB z możliwością konfiguracji RAID 1. Możliwość zainstalowania dedykowanego modułu dla hypervisora wirtualizacyjnego, wyposażony w 2 nośniki typu flash o pojemności min. 64GB, z możliwością konfiguracji zabezpieczenia synchronizacji pomiędzy nośnikami z poziomu BIOS serwera, rozwiązanie nie może powodować zmniejszenia ilości wnek na dyski twarde.
Kontroler RAID	Sprzętowy kontroler dyskowy, posiadający min. 8GB nieulotnej pamięci cache, możliwe konfiguracje poziomów RAID: 0, 1, 5, 6, 10, 50, 60. Wsparcie dla dysków samoszyfrujących.
Wbudowane porty	Przynajmniej 4 x USB z czego nie mniej niż 1x USB 3.0, 1xVGA z czego jeden na panelu przednim.
Video	Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1920x1200

Zasilacze	Redundantne, Hot-Plug min. 1100W każdy.
Bezpieczeństwo	<ul style="list-style-type: none"> • Zatrzaszk górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardej. • Możliwość wyłączenia w BIOS funkcji przycisku zasilania. • BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła • Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą. • Moduł TPM 2.0 • Możliwość dynamicznego włączania i wyłączania portów USB na obudowie – bez potrzeby restartu serwera • Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem
Diagnostyka	Serwer wyposażony w panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS'u, zasilaniu oraz temperaturze.
Karta Zarządzania	<p>Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca:</p> <ul style="list-style-type: none"> • zdalny dostęp do graficznego interfejsu Web karty zarządzającej; • zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera); • szyfrowane połączenie (TLS) oraz autentykację i autoryzację użytkownika; • możliwość podmontowania zdalnych wirtualnych napędów; • wirtualną konsolę z dostępem do myszy, klawiatury; • wsparcie dla IPv6; • wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish; • możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer; • możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer; • integracja z Active Directory; • możliwość obsługi przez dwóch administratorów jednocześnie; • wsparcie dla dynamic DNS; • wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej. • możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera • możliwość zarządzania do 100 serwerów bezpośrednio z konsoli karty zarządzającej pojedynczego serwera
Oprogramowanie do zarządzania	<ul style="list-style-type: none"> • Wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych • integracja z Active Directory • Możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta • Wsparcie dla protokołów SNMP, IPMI, Linux SSH, Redfish • Możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram • Szczegółowy opis wykrytych systemów oraz ich komponentów • Możliwość eksportu raportu do CSV, HTML, XLS, PDF

	<ul style="list-style-type: none"> • Możliwość tworzenia własnych raportów w oparciu o wszystkie informacje zawarte w inwentarzu. • Grupowanie urządzeń w oparciu o kryteria użytkownika • Tworzenie automatycznie grup urządzeń w oparciu o dowolny element konfiguracji serwera np. Nazwa, lokalizacja, system operacyjny, obsadzenie slotów PCIe, pozostałego czasu gwarancji • Możliwość uruchamiania narzędzi zarządzających w poszczególnych urządzeniach • Szybki podgląd stanu środowiska • Podsumowanie stanu dla każdego urządzenia • Szczegółowy status urządzenia/elementu/komponentu • Generowanie alertów przy zmianie stanu urządzenia. • Filtry raportów umożliwiające podgląd najważniejszych zdarzeń • Integracja z service desk producenta dostarczonej platformy sprzętowej • Możliwość przejęcia zdalnego pulpitu • Możliwość podmontowania wirtualnego napędu • Kreator umożliwiający dostosowanie akcji dla wybranych alertów • Możliwość importu plików MIB • Przesyłanie alertów „as-is” do innych konsol firm trzecich • Możliwość definiowania ról administratorów • Możliwość zdalnej aktualizacji oprogramowania wewnętrznego serwerów • Aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania) • Możliwość instalacji oprogramowania wewnętrznego bez potrzeby instalacji agenta • Możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów • Moduł raportujący pozwalający na wygenerowanie następujących informacji: nr seryjne sprzętu, konfiguracja poszczególnych urządzeń, wersje oprogramowania wewnętrznego, obsadzenie slotów PCI i gniazd pamięci, informację o maszynach wirtualnych, aktualne informacje o stanie i poziomie gwarancji, adresy IP kart sieciowych, występujących alertów, MAC adresów kart sieciowych, stanie poszczególnych komponentów serwera. • Możliwość tworzenia sprzętowej konfiguracji bazowej i na jej podstawie weryfikacji środowiska w celu wykrycia rozbieżności. • Wdrażanie serwerów, rozwiązań modularnych oraz przełączników sieciowych w oparciu o profile. • Możliwość migracji ustawień serwera wraz z wirtualnymi adresami sieciowymi (MAC, WWN, IQN) między urządzeniami. • Tworzenie gotowych paczek informacji umożliwiających zdiagnozowanie awarii urządzenia przez serwis producenta. • Zdalne uruchamianie diagnostyki serwera. • Dedykowana aplikacja na urządzenia mobilne integrująca się z wyżej opisanymi oprogramowaniem zarządzającym. • Oprogramowanie dostarczane jako wirtualny appliance dla KVM, ESXi i Hyper-V.
<p>Certyfikaty</p>	<p>Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015 oraz ISO-14001. Serwer musi posiadać deklarację CE. Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać</p>

	status „Certified for Windows” dla systemów Microsoft Windows 2016, Microsoft Windows 2019.
Warunki gwarancji	Minimum 5 lat gwarancji producenta, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii 24x7x365 poprzez ogólnopolską linię telefoniczną producenta. Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia oraz pobieranie uaktualnień mikro kodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji serwera
Dokumentacja użytkownika	Zamawiający wymaga dokumentacji w języku polskim lub angielskim. Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.

REPOZYTORIUM BACKUPU

PARAMETR	CHARAKTERYSTYKA (WYMAGANIA MINIMALNE)
Obudowa	Obudowa do montażu w szafie rack 19” za pomocą dostarczonych dedykowanych elementów.
Kontrolery	Deduplikator musi być wyposażony w minimum 2 kontrolery pracujące w trybie active-passive lub active-active. Deduplikator nie może posiadać pojedynczego punktu awarii, który powodowałby brak dostępu do danych. W przypadku awarii kontrolera wszystkie procesy musi przejąć drugi kontroler.
Wymagana przestrzeń	Przestrzeń użytkowa po zbudowaniu RAID 6 z min. 1 dyskiem hot-spare lub przestrzenią hot-spare równą pojemności min. 1 dysku musi wynosić min 17TB. Rozmiar RAW pojedynczego dysku nie może być większy niż 4 TB. Dodatkowo wymagane jest zastosowanie co najmniej 4 dysków SSD SAS o pojemności RAW min 480 GB jako cache pod zapis backupu. Wymagana pojemność użytkowa rozumiana jest jako pojemność dostępna po konfiguracji RAID i odliczeniu rezerwy na dyski/przestrzeń <i>spare</i> i dostępna dla hostów bez uwzględnienia jakichkolwiek mechanizmów kompresji, czy deduplikacji.
Zabezpieczenia RAID	Dane przechowywane w obrębie podsystemu dyskowego urządzenia muszą być chronione za pomocą technologii RAID 6 lub równoważnej, tolerującej jednoczesną awarię 2 dysków bez utraty danych. Urządzenie musi umożliwiać bezpieczne usuwanie danych zgodnie ze standardem DoD 5220.22-M poprzez mechanizm nadpisywania danych.
Pamięć Cache	Co najmniej 256GB pamięci cache na cały deduplikator (dwa kontrolery). Pamięć cache musi być zabezpieczona przed utratą danych w przypadku awarii zasilania.
Dostępne interfejsy	Urządzenie musi posiadać minimum: 4 porty Ethernet 10 Gb/s z możliwością obsługi każdym portem Ethernet protokołów CIFS, NFS, wszystkie porty wyposażone we wkładki optyczne.
Obsługiwane protokoły	Wymagane wsparcie dla FC, iSCSI, NFS, CIFS.
Zarządzanie	Zarządzanie deduplikatorem (wszystkimi kontrolerami) z poziomu pojedynczego interfejsu graficznego. Wymagane jest stałe monitorowanie stanu deduplikatora w tym monitorowanie wydajności obiektów takich jak: - cały deduplikator - kontrolery - CPU

PARAMETR	CHARAKTERYSTYKA (WYMAGANIA MINIMALNE)
	<ul style="list-style-type: none"> - porty front-end - porty logiczne - dyski - file systemy <p>Pod kątem parametrów takich jak:</p> <ul style="list-style-type: none"> - operacje wejścia/wyjścia IOPS - przepustowość (KB/s lub MB/s) - czas odpowiedzi (latency) - średnie użycie (w % dla CPU) <p>Wymagana możliwość dostępu do historycznych danych wydajnościowych z poziomu GUI urządzenia do co najmniej 2 lat wstecz lub jako równoważne dostarczenie fizycznego serwera z oprogramowaniem umożliwiającym zbieranie i przeglądanie danych historycznych.</p> <p>Wymagany dostęp do informacji o wykorzystanej przestrzeni.</p> <p>Wymagana możliwość tworzenia wielu użytkowników deduplikatora w oparciu o wbudowane role. Rozwiązanie musi umożliwiać tworzenie własnych ról.</p> <p>Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje to ich dostarczenie jest wymagane na tym etapie postępowania oraz należy je uwzględnić w cenie ofertowej.</p>
Redukcja danych	<p>Urządzenie musi deduplikować dane inline przed zapisem na nośnik dyskowy. Technologia deduplikacji musi wykorzystywać algorytm bazujący na zmiennym bloku. Algorytm ten musi samoczynnie i automatycznie dopasowywać się do otrzymywanego strumienia danych. Proces deduplikacji musi odbywać się inline – w pamięci urządzenia, przed zapisem danych na nośnik dyskowy. Dane muszą być poddane także procesowi kompresji. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia oraz należy je uwzględnić w cenie ofertowej.</p> <p>Wymagana także obsługa deduplikacji na źródle, co pozwala ograniczyć zużycie sieci.</p>
Kontrola zasobów plikowych	<p>Wymagana możliwość skonfigurowania tzw. quoty ograniczającej wystawione zasoby plikowe. Wymagana możliwość ograniczenia użytkownikom przestrzeni, z której mogą korzystać lub liczby plików jakie mogą być przechowywane na udostępnionej przestrzeni.</p> <p>Wymagana możliwość skonfigurowania polityki filtrowania zapisywanych plików poprzez wykluczenie ich konkretnych rozszerzeń.</p> <p>Wymagana możliwość ograniczenia dostępu do udostępnionych udziałów CIFS/NFS poprzez zdefiniowanie adresów IP lub ich przedziałów, które będą miały do nich dostęp.</p> <p>Dostarczenie powyższych funkcjonalności jest wymagane na tym etapie postępowania oraz należy je uwzględnić w cenie ofertowej.</p>
Ochrona zasobów plikowych	<p>Tworzenie na żądanie tzw. migawkowej kopii danych (ang. snapshot) file systemów w ramach deduplikatora do wykorzystania w celu np. wykonywania kopii zapasowych. Wymagana jest możliwość utworzenia harmonogramu snapshotów, które będą zabezpieczone przed modyfikacją oraz usunięciem przez wybrany okres czasu bez odpowiednich uprawnień celem przywrócenia danych w przypadku ataku ransomware. Musi być możliwość odtworzenia danych z dowolnej kopii (snapshot) wykonanej w ramach harmonogramu. Odtworzenie danych z jednej kopii nie może uniemożliwiać odtworzenia danych z innej kopii z innego punktu w czasie. Dostarczenie tej funkcjonalności jest wymagane na tym etapie</p>

PARAMETR	CHARAKTERYSTYKA (WYMAGANIA MINIMALNE)
	<p>postępowania na całą przestrzeń dyskową i na maksymalną liczbę snapshotów obsługiwanych przez oferowany model deduplikatora oraz należy je uwzględnić w cenie ofertowej.</p> <p>Wymagana możliwość zablokowania plików przed modyfikacją lub usunięciem (WORM). Dostarczenie licencji na tą funkcjonalność jest wymagane na tym etapie postępowania oraz należy je uwzględnić w cenie ofertowej.</p>
Replikacja danych	<p>Urządzenie musi umożliwiać replikację danych do drugiego urządzenia w ramach tej samej rodziny oferowanego deduplikatora. Replikacja musi się odbywać w trybie asynchronicznym. Wymagana możliwość ograniczenia ilości przesyłanych danych poprzez ich deduplikację oraz kompresję.</p> <p>Deduplikator musi umożliwiać konfigurację harmonogramu replikacji poprzez określenie interwału (np. replikacja co 60 min) lub konkretnych okien czasowych (np. w każdą sobotę o godz. 20:00).</p> <p>Dostarczenie powyższych funkcjonalności jest wymagane na tym etapie postępowania oraz należy je uwzględnić w cenie ofertowej.</p> <p>Wymagana możliwość zastosowania funkcjonalności typu AirGap czyli fizyczne wyłączenie portów dedykowanych do replikacji w czasie kiedy replikacja nie jest wykonywana. Dopuszcza się realizację tej funkcjonalności poprzez zastosowanie dodatkowego oprogramowania.</p> <p>Dostarczenie funkcjonalności typu AirGap nie jest wymagane na tym etapie postępowania.</p>
Wspierane systemy backup	<p>Urządzenie musi wspierać co najmniej następujące aplikacje do backupu: Commvault, Veritas NetBackup, Veeam Backup&Replication.</p>
Obsługa serwisowa	<p>Deduplikator musi posiadać możliwość upgrade'u firmware-u kontrolerów bez przerywania dostępu do danych.</p> <p>Urządzenie przystosowane do napraw w miejscu instalacji oraz wymiany elementów bez konieczności jego wyłączenia.</p> <p>Urządzenie musi umożliwiać zdalne zarządzanie.</p> <p>Urządzenie musi być fabrycznie nowe, wyprodukowane nie wcześniej niż 6 miesięcy przed datą dostarczenia do Zamawiającego i pochodzić z autoryzowanego kanału dystrybucji producenta, a także musi być objęte serwisem producenta lub autoryzowanego partnera serwisowego na terenie RP.</p> <p>Deduplikator musi zostać objęty minimum 5 letnim okresem gwarancji producenta z gwarantowanym czasem reakcji najpóźniej w następnym dniu roboczym od momentu zgłoszenia usterki. Zamawiający dopuszcza realizację gwarancji przez autoryzowanego partnera serwisowego producenta.</p>

Vmware:

1. Warstwa wirtualizacji musi być zainstalowana bezpośrednio na sprzęcie fizycznym bez dodatkowych pośredniczących systemów operacyjnych.
2. Rozwiązanie musi zapewnić możliwość obsługi wielu instancji systemów operacyjnych na jednym serwerze fizycznym i powinno się charakteryzować maksymalnym możliwym stopniem konsolidacji sprzętowej.
3. Pojedynczy klaster może się skalować do maksymalnie 3 dwuprocessorowych fizycznych hostów (serwerów) z zainstalowaną warstwą wirtualizacji.
4. Pojedynczy fizyczny procesor wymaga przypisania do niego licencji w ilości minimum 16 rdzeni.
5. Pojedyncza licencja pokrywa maksymalnie do 96 rdzeni łącznie w całym klastrze. W przypadku przekroczenia tej wartości (96 rdzeni) wymagana jest kolejna licencja zwiększająca ilość obsługiwanych rdzeni do 192.
6. Oprogramowanie do wirtualizacji musi zapewniać możliwość stworzenia dysku maszyny wirtualnej o wielkości 62 TB.

7. Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych z możliwością przydzielenia 24 TB pamięci operacyjnej RAM.
8. Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych, z których każda może mieć 1-10 wirtualnych kart sieciowych.
9. Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych, z których każda może mieć 32 porty szeregowo.
10. Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych, z których każda może mieć 20 portów USB.
11. Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych, z których każda może mieć 4 GB pamięci graficznej.
12. Rozwiązanie musi umożliwiać łatwą i szybką rozbudowę infrastruktury o nowe usługi bez spadku wydajności i dostępności pozostałych wybranych usług.
13. Rozwiązanie powinno w możliwie największym stopniu być niezależne od producenta platformy sprzętowej.
14. Rozwiązanie musi wspierać następujące systemy operacyjne: Windows 7/8/10/11, Windows Server, Amazon Linux 2, macOS, OS X, Asianux, Ubuntu, CentOS, NeoKylin, Debian, FreeBSD, Oracle Linux, RHEL, SUSE, Photon OS.
15. Rozwiązanie musi umożliwiać przydzielenie większej ilości pamięci RAM dla maszyn wirtualnych niż fizyczne zasoby RAM serwera w celu osiągnięcia maksymalnego współczynnika konsolidacji.
16. Oprogramowanie do wirtualizacji powinno zapewnić możliwość wykonywania kopii migawkowych instancji systemów operacyjnych (tzw. snapshot) na potrzeby tworzenia kopii zapasowych bez przerywania ich pracy.
17. Rozwiązanie musi umożliwiać udostępnienie maszynie wirtualnej większej ilości zasobów dyskowych niż jest fizycznie zarezerwowane na dyskach lokalnych serwera lub na macierzy.
18. System musi posiadać funkcjonalność wirtualnego przełącznika sieciowego umożliwiającego tworzenie sieci wirtualnej w obszarze hosta i pozwalającego połączyć maszyny wirtualne w obszarze jednego hosta, a także na zewnątrz sieci fizycznej. Pojedynczy przełącznik wirtualny powinien mieć możliwość konfiguracji do 4000 portów.
19. Pojedynczy wirtualny przełącznik musi posiadać możliwość przyłączania do niego dwóch i więcej fizycznych kart sieciowych, aby zapewnić bezpieczeństwo połączenia ethernetowego w razie awarii karty sieciowej.
20. Wirtualne przełączniki muszą obsługiwać wirtualne sieci lokalne (VLAN).
21. Polityka licencjonowania musi umożliwiać przenoszenie licencji na oprogramowanie do wirtualizacji pomiędzy serwerami różnych producentów z zachowaniem wsparcia technicznego i zmianą wersji oprogramowania na niższą (downgrade). Wsparcie techniczne musi być świadczone bezpośrednio przez producenta oprogramowania. Licencjonowanie nie może odbywać się w trybie OEM.
22. Rozwiązanie musi zawierać zintegrowaną funkcjonalność do zarządzania poprawkami i podnoszenia wersji wirtualizatora.
23. Oprogramowanie do wirtualizacji musi zapewnić możliwość klonowania systemów operacyjnych wraz z ich pełną konfiguracją i danymi.
24. Oprogramowanie do wirtualizacji musi posiadać możliwość integracji z usługami katalogowymi Microsoft Active Directory.
25. Rozwiązanie musi posiadać wbudowany interfejs programistyczny (API) zapewniający pełną integrację zewnętrznych rozwiązań wykonywania kopii zapasowych z istniejącymi mechanizmami warstwy wirtualizacyjnej.
26. Rozwiązanie musi posiadać centralną konsolę graficzną do zarządzania maszynami wirtualnymi i do konfigurowania innych funkcjonalności. Centralna konsola graficzna dostarczana jest w postaci gotowej, wstępnie skonfigurowanej maszyny wirtualnej tzw. virtual appliance. Dostęp do konsoli może być realizowany z poziomu przeglądarki internetowej z wykorzystaniem protokołu HTML5.
27. Rozwiązanie musi zapewnić możliwość bieżącego monitorowania wykorzystania zasobów fizycznych infrastruktury wirtualnej (np. wykorzystanie procesorów, pamięci RAM, wykorzystanie przestrzeni na dyskach/wolumenach) oraz przechowywać i wyświetlać dane historyczne.
28. Rozwiązanie musi zawierać wsparcie dla TPM 2.0 oraz wirtualnego TPM.
29. Rozwiązanie musi zapewniać mechanizm replikacji wskazanych maszyn wirtualnych pomiędzy różnymi systemami pamięci masowych.
30. Rozwiązanie musi zawierać funkcjonalność pozwalającą na ominięcie testów inicjalizacyjnych sprzętu fizycznego w celu szybkiego startu wirtualizatora.
31. Rozwiązanie musi zawierać możliwość zabezpieczania maszyn wirtualnych przez rozwiązania antywirusowe firm trzecich bez konieczności instalacji agenta wewnątrz maszyny wirtualnej.

32. Rozwiązanie musi mieć możliwość przenoszenia maszyn wirtualnych w czasie ich pracy pomiędzy serwerami fizycznymi. Mechanizm powinien umożliwiać 8 takich procesów przenoszenia jednocześnie.
33. Musi zostać zapewniona odpowiednia redundancja i taki mechanizm (wysokiej dostępności HA), aby w przypadku awarii lub niedostępności serwera fizycznego wybrane przez administratora i uruchomione nim wirtualne maszyny zostały uruchomione na innych serwerach z zainstalowanym oprogramowaniem wirtualizacyjnym. Rozwiązanie musi posiadać co najmniej 2 niezależne mechanizmy wzajemnej komunikacji między serwerami oraz z serwerem zarządzającym, gwarantujące właściwe działanie mechanizmów wysokiej dostępności na wypadek izolacji sieciowej serwerów fizycznych lub partycjonowania sieci.
34. Wymagane jest dostarczenie minimum trzyletniej subskrypcji na licencji.

Lp.	Charakterystyka
1.	Instalacja trzech hostów wirtualizacyjnych
	<ol style="list-style-type: none"> 1. Montaż w szafie Rack 2. Podłączenie do zasilania 3. Konfiguracja konsoli zdalnego dostępu 4. Aktualizacja mikrokodu (firmware) komponentów do najnowszej i zalecanej przez producenta wersji. 5. Podłączenie do infrastruktury sieci LAN/SAN
2.	Wirtualizacja środowiska serwerowego
	<ol style="list-style-type: none"> 1. Instalacja systemu wirtualizacji 2. Konfiguracja parametrów serwerów wirtualizacyjnych: adresacja IP, routing, DNS, synchronizacja czasu 3. Rejestracja hostów wirtualizacyjnych w macierzy dyskowej 4. Konfiguracja wirtualnych przełączników sieciowych 5. Konfiguracja wirtualnych sieci 6. Prezentacja przestrzeni macierzy dyskowej dla wszystkich hostów 7. Definicja mechanizmów wielościeżkowego dostępu do danych (tzw. multipathing) 8. Organizacja systemu plików na wydzielonych zasobach macierzy dyskowej dedykowanych do składowania plików maszyn wirtualnych 9. Konfiguracja sieci wirtualnych dedykowanych dla maszyn wirtualnych oraz mechanizmów migracji maszyn wirtualnych pomiędzy maszynami fizycznymi, w trybie on-line 10. Instalacja oprogramowania służącego do centralnego zarządzania, monitorowania i konfiguracji środowiskiem wirtualizacji serwerowej 11. Konfiguracja klastra wysokiej dostępności HA (High Availability) 12. Konfiguracja mechanizmu migracji maszyn wirtualnych pomiędzy maszynami fizycznymi w trybie on-line 13. Konfiguracja mechanizmu powiadamiania (tzw. notyfikacje) poprzez protokoły SNMP, SMTP. 14. Konfiguracja praw dostępu do systemu zarządzania środowiskiem wirtualizacji serwerowej, zgodnie z założeniami Zamawiającego, z uwzględnieniem wskazanych użytkowników, grup użytkowników oraz odpowiednich ról (typu: administrator, operator maszyn wirtualnych, itp.) 15. Instalacja mechanizmu automatyzacji aktualizacji środowiska 16. Aktualizacja środowiska wirtualnego do najnowszej stabilnej wersji 17. Testy mechanizmów migracji maszyn wirtualnych pomiędzy maszynami fizycznymi 18. Testy mechanizmów klastra wysokiej dostępności
3.	Migracja maszyn VM
	<ol style="list-style-type: none"> 1. Migracja wszystkich maszyn wirtualnych ze starych serwerów na nowe hosty przy jednoczesnym zachowaniu ciągłości działania całego środowiska wirtualnego.
4.	Montaż deduplikatora dyskowego

	<ul style="list-style-type: none"> a. Instalacja deduplikatora dyskowego w szafie rack b. Inicjalizacja wirtualnego deduplikatora dyskowego (zapewnienie maszynie wirtualnej wymaganych zasobów CPU, pamięci RAM i przestrzeni dyskowej) c. Konfiguracja parametrów sieciowych d. Konfiguracja protokołów dostępowych do urządzenia e. Konfiguracja przestrzeni dyskowej dedykowanej dla składowania unikatowych bloków f. Prezentacja danych dla systemu backupu
5.	Rekonfiguracja systemu backupowego
	<ul style="list-style-type: none"> 1. Rejestracja deduplikatora dyskowego w systemie backupu 2. Rekonfiguracja polityk ochrony dla wskazanych maszyn wirtualnych/fizycznych: <ul style="list-style-type: none"> a. Definicje typów kopii zapasowych (obraz maszyny, dane plikowe, dane aplikacyjne w trybie online, dane aplikacyjne w trybie offline) b. Definicja harmonogramów c. Definicja miejsc składowania kopii zapasowych d. Definicja polityk retencji e. Testy odtwarzania danych