

Załącznik Nr 1 do Zapytania ofertowego:

Zakup i dostawa serwera wraz z oprogramowaniem w ramach zadania „Zwiększanie cyberbezpieczeństwa w Gminie Rokitno” finansowanego z projektu „Cyberbezpieczny Samorząd”

OPIS PRZEDMIOTU ZAMÓWIENIA

Zakup serwera wraz z oprogramowaniem w ramach projektu Cyberbezpieczny Samorząd

Serwer – 1 szt. o parametrach nie gorszych niż:

Parametr	Charakterystyka (wymagania minimalne)
Obudowa	<p>Obudowa Rack o wysokości max 2U z możliwością instalacji do 16 dysków 2.5" lub 8 dysków 3,5" Hot-Plug wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych oraz organizatorem do kabli.</p> <p><u>Zamawiający wymaga aby dostarczona była obudowa przygotowana na montaż 8 dysków o szerokości 3,5 cala wraz z ramkami na dyski twarde.</u></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 minimum dwóch procesorów Intel 3rd Gen. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym.
Chipset	Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych
Procesor	Zainstalowane dwa procesory 12 rdzeniowe o taktowaniu minimum 2,1 GHz (Turbo Speed min. 3.3 GHz), dedykowany do pracy z zaoferowanym serwerem umożliwiający osiągnięcie wyniku min. 22640 pkt w teście CPU Mark dostępnym na stronie https://www.cpubenchmark.net/ . Wynik na na dzień 14.10.2024r.
RAM	128 GB (Minimum 8 szt. po 16 GB DDR4 RDIMM 3200MT/s) na płycie głównej powinno znajdować się minimum 16 slotów przeznaczonych do instalacji pamięci. Płyta główna powinna obsługiwać do 1TB pamięci RAM.
Zabezpieczenia pamięci RAM	Advanced ECC, Memory Page Retire, Fault Resilient Memory, Memory Self-Healing lub PPR, Partial Cache Line Sparing
Gniazda PCI	Minimum 4 sloty PCIe z czego przynajmniej trzy 4 generacji.
Interfejsy sieciowe/FC/SAS	Zintegrowana karta sieciowa dwuportowa 1Gb Ethernet w standardzie BaseT oraz dodatkowa karta sieciowa OCP3.0 z dwoma portami SFP+ 10GB (porty nie mogą być osiągnięte poprzez karty w slotach PCIe). Dodatkowa karta sieciowa 4 portowa (quad

	port) 1Gb w standardzie BaseT.
Dyski twarde	<p>Możliwość instalacji dysków SAS, SATA, SSD</p> <p><u>Zainstalowane 8 dysków SATA o pojemności 10TB każdy. Poniżej specyfikacja dysków twardych ZAŁĄCZNIK nr 1.</u></p> <p><u>Zainstalowane dwa dyski M.2 SATA o pojemności min. 480GB Hot-Plug z możliwością konfiguracji RAID 1.</u></p> <p>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.</p>
Kontroler RAID	Sprzętowy kontroler dyskowy posiadający min. 8GB cache umożliwiający konfigurację poziomów RAID: 0, 1, 5, 6, 10, 50, 60.
System operacyjny/System wirtualizacji	<p>Microsoft Windows Server 2022 Standard (Na 16 rdzeni) – 1 szt. lub równoważny (warunki równoważności w ZAŁĄCZNIKU nr 2)</p> <p>Microsoft Windows Server 2022 Standard (Na 2 rdzenie) – 4 szt.</p>
Wbudowane porty	<p>Przednie: min. 1x VGA, min. 1x USB 2.0, min. 1x micro-USB dedykowane dla karty zarządzającej,</p> <p>Tylne: min. 1x VGA, min. 2x USB w tym 1x USB 3.0, 1x RJ45</p>
Video	Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1920x1200
Zasilacze	Redundantne, Hot-Plug min. 700W każdy, każdy zasilacz posiadający przewód zasilający o długości minimum 4m.
Bezpieczeństwo	<ul style="list-style-type: none"> • Zatrzask górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych. • 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	Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiającą:

	<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; • możliwość podmontowania zdalnych wirtualnych folderów; • 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 • 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

	<ul style="list-style-type: none"> • 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 aletrów, 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.
Certyfikaty	<p>Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015 oraz ISO-14001. Serwer musi posiadać deklaracja CE.</p> <p>Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów x64, Microsoft Windows Server 2016, Microsoft Windows Server 2019.</p>
Warunki gwarancji	<p>5 lat gwarancji producenta, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii 24x7x365 poprzez ogólnopolską linię telefoniczną producenta.</p> <p>Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego.</p> <p>Firma serwisująca musi posiadać ISO 9001:2008 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty.</p>

	<p>Wymagane dołączenie do oferty oświadczenia Producenta potwierdzając, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta.</p> <p>Możliwość rozszerzenia gwarancji serwera przez producenta do 7 lat.</p> <p>Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji serwera</p>
Dokumentacja użytkownika	<p>Zamawiający wymaga dokumentacji w języku polskim lub angielskim.</p> <p>Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.</p>
Montaż	<p>Wraz z serwerem wykonawca dostarczy kompatybilne z oferowanym sprzętem szyny do montażu serwera w szafie rack wraz z ruchomym ramieniem na kable umożliwiające wysunięcie serwera z szafy rack bez odłączania okablowania.</p>

Załącznik nr 1

Dyski twarde do serwera – 8 szt. o parametrach nie gorszych niż:

Form factor	3.5-inch
Interface	SATA 6 Gb/s
512n / 512e user sectors per drive ⁴	512e
Formatted capacity ¹	10TB
OptiNAND™ technology	No
RoHS compliant ⁵	Yes
Data Transfer Rate ⁶ (max Sustained)	262MB/s
RPM	7200
Cache	256MB
Power Management	
Average power requirements (W)	
Operational	9.2W
Idle	8.0W
Power efficiency index(W/TB, idle)	0.8
Reliability	
MTBF (hours, projected)	2,000,000
Annualized Failure Rate ² (AFR, %)	0.44
Limited warranty	5 years
Environmental	
Operating temperature	5°C to 60°C
Non-operating temperature	-40°C to 70°C
Shock (Read/Write)	
Operating (half-sine wave, 2ms)	70G/50G

Non-operating (half-sine wave, 2ms)	250G
Acoustics (average)	
Idle Mode	34 dBA
Seek Mode	38 dBA
Warunki gwarancji	Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wsparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego.
Okres gwarancji	Minimum 5 lat

Załącznik nr 2

WARUNKI RÓWNOWAŻNOŚCI

Warunki równoważności dla licencji systemu Microsoft Windows Server 2022 STANDARD

W przypadku zaoferowania przez Wykonawcę licencji systemu równoważnego do systemu Microsoft Windows Server 2022 STANDARD, Zamawiający wymaga dostarczenia licencji dla 1 serwera oraz instalacji. Zamawiający wymaga aby produkt równoważny spełniał niżej wymienione wymagania:

1. Współpraca z procesorami o architekturze x86 – 64bit.
2. Instalacja i użytkowanie aplikacji 32-bit. i 64-bit. na dostarczonym systemie operacyjnym.
3. Możliwość budowania klastrów składających się z 64 węzłów.
4. Pojedyncza licencja musi obsługiwać serwer fizyczny wyposażony w 16 rdzeni.
5. Licencja musi uprawniać do uruchamiania serwerowego systemu operacyjnego w środowisku fizycznym i dwóch wirtualnych środowiskach serwerowego systemu operacyjnego za pomocą wbudowanych mechanizmów wirtualizacji.
6. Możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności min. 64TB przez każdy wirtualny serwerowy system operacyjny.
7. Możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci.
8. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy.
9. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy.
10. Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.
11. Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy.
12. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading;

13. Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.
14. Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.
15. Możliwość uruchamiania aplikacji internetowych wykorzystujących technologię ASP.NET.
16. Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.
17. Wbudowana zaporę internetową (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.
18. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe.
19. Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 2 języków poprzez wybór z listy dostępnych lokalizacji.
20. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).
21. Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.
22. Wsparcie dostępu do zasobu dyskowego SSO poprzez wiele ścieżek (Multipath).
23. Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego.
24. Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.
25. Możliwość migracji konfiguracji systemu Microsoft Windows Serwer 2011/2012.
26. Praca w roli klienta domeny Microsoft Active Directory.
27. Możliwość uruchomienia roli kontrolera domeny Microsoft Active Directory na poziomie funkcjonalności Microsoft Windows Server 2012.
28. Możliwość uruchomienia roli klienta i serwera czasu (NTP).
29. Możliwość uruchomienia roli serwera plików z uwierzytelnieniem i autoryzacją dostępu w domenie Microsoft Active Directory.
30. Możliwość uruchomienia roli serwera wydruku z uwierzytelnieniem i autoryzacją dostępu w domenie Microsoft Active Directory.
31. Możliwość uruchomienia roli serwera stron WWW.
32. W ramach dostarczonej licencji zawarte prawo do pobierania poprawek systemu operacyjnego.
33. Wszystkie wymienione parametry, role, funkcje, itp. systemu operacyjnego objęte są dostarczoną licencją (licencjami) i zawarte w dostarczonej wersji oprogramowania (nie wymagają ponoszenia przez Zamawiającego dodatkowych kosztów).
34. Wbudowane wsparcie instalacji i pracy na wolumenach, które:
 - a. pozwalają na zmianę rozmiaru w czasie pracy systemu,
 - b. umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,
 - c. umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów,
 - d. umożliwiają zdefiniowanie list kontroli dostępu (ACL).
35. Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość
36. Możliwość uruchamiania aplikacji internetowych wykorzystujących technologię ASP.NET
37. Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.
38. Możliwość wykorzystania standardu http/2.
39. Mechanizmy logowania w oparciu o:

- a. login i hasło,
 - b. karty z certyfikatami (smartcard),
 - c. wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM).
40. Możliwość wymuszania wieloelementowej dynamicznej kontroli dostępu dla:
- a. określonych grup użytkowników,
 - b. zastosowanej klasyfikacji danych,
 - c. centralnych polityk dostępu w sieci,
 - d. centralnych polityk audytowych oraz narzuconych dla grup użytkowników praw do wykorzystywania szyfrowanych danych.
41. Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa.
42. Wsparcie dla środowisk Java i .NET Framework 4.x i wyższych – możliwość uruchomienia aplikacji działających we wskazanych środowiskach.
43. Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:
- a. podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC.
 - b. usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji:
 - i. podłączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną,
 - ii. ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,
 - iii. odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza,
 - iv. bezpieczny mechanizm dołączania do domeny uprawnionych użytkowników prywatnych urządzeń mobilnych opartych o iOS i Windows 8.1.,
 - c. zdalna dystrybucja oprogramowania na stacje robocze,
 - d. praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej z możliwością dostępu minimum 65 tys. Użytkowników,
 - e. Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:
 - i. Dystrybucję certyfikatów poprzez http,
 - ii. Konsolidację CA dla wielu lasów domeny,
 - iii. Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen,
 - iv. Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509.
 - f. szyfrowanie plików i folderów,
 - g. szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec),
 - h. szyfrowanie sieci wirtualnych pomiędzy maszynami wirtualnymi,
 - i. możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów,

- j. serwis udostępniania stron WWW,
- k. wsparcie dla protokołu IP w wersji 6 (IPv6),
- l. wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows,
- m. wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie uruchomienie nieograniczonej liczby aktywnych środowisk wirtualnych systemów operacyjnych (liczba ograniczona parametrami fizycznymi serwera),
- n. możliwość migracji maszyn wirtualnych między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci.
- o. możliwość przenoszenia maszyn wirtualnych pomiędzy serwerami klastra typu failoverz jednoczesnym zachowaniem pozostałej funkcjonalności.
- p. mechanizmy wirtualizacji mające wsparcie dla:
 - i. dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych,
 - ii. obsługi ramek typu jumbo frames dla maszyn wirtualnych.
 - iii. obsługi 4-KB sektorów dysków,
 - iv. nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra,
 - v. możliwość tworzenia wirtualnych maszyn chronionych, separowanych od środowiska systemu operacyjnego.
 - vi. możliwość uruchamiania kontenerów bazujących na Windows i Linux na tym samym hoście kontenerów.
- q. wsparcie dla rozwiązania Kubernetes.
- r. możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz dostępnością bezpłatnego rozwiązania producenta serwerowego systemu operacyjnego umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet.
- s. wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath).
- t. mechanizmy deduplikacji i kompresji na wolumenach.
- u. mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.
- v. mechanizm konfiguracji połączenia VPN do platformy Azure.
- w. wbudowany mechanizm wykrywania ataków na poziomie pamięci RAM i jądra systemu.
- x. mechanizmy pozwalające na blokadę dostępu nieznanym procesom do chronionych katalogów.
- y. możliwość instalacji i poprawnej pracy Systemu Bazodanowego (Microsoft SQL Server Standard).