

MODERNIZACJA SYSTEMU HIPERKONWERGENTNEGO

Rozbudowa systemu hiperkonwergencji (HCI) – rozszerzenie istniejącego klastra.

1. Opis istniejącego środowiska.

Zamawiający posiada działający klaster HCI składający się z 4 serwerów HPE PROLIANT DL360 GEN10 (każdy wyposażony w 1 szt. procesor Intel Xenon Gold 5218R CPU @2,10 GHZ) podłączonych do przełączników klastra w architekturze 10Gb, Zamawiający posiada wolne porty na podłączenie kolejnych serwerów (węzłów) klastra. Zamawiający wymaga od Wykonawcy aby dostarczony sprzęt został przez Wykonawcę zainstalowany w szafie rack oraz podłączony do istniejącej struktury i aby Wykonawca skonfigurował prawidłowe działanie klastra przy zachowaniu ciągłości usług Zamawiającego.

Jako platformę wirtualizacyjną, Zamawiający obecnie używa oprogramowania VMware vSphere w wersji 7. Zamawiający dla realizacji funkcji klastra hiperkonwergencji wykorzystuje technologię vSan firmy VMware.

Poniżej lista zadań do wykonania przez Wykonawcę:

- a) przygotowanie harmonogramu, projektu instalacji, scenariuszy testowych rozbudowy oraz wdrożenia nowego sprzętu oraz licencji z zachowaniem ciągłości pracy Zamawiającego; Wykonawca zobowiązany jest do przekazania Zamawiającemu ww. dokumentacji wraz z harmonogramem w ciągu 21 dni od daty zawarcia umowy,
- b) dostawa sprzętu serwerowego, wyposażenia oraz licencji oprogramowania zgodnie z OPZ oraz złożoną ofertą,
- c) instalacja sprzętu oraz rozbudowa istniejącego środowiska, podłączenie do infrastruktury sieciowej i zasilającej Zamawiającego,
- d) aktualizacja oprogramowania wirtualizatorów vSphere do ostatniej dostępnej wersji, aktualizacja konsoli vCenter i vSan do zachowania spójnej i stabilnej wersji środowiska,
- e) przeprowadzenie testów działania zgodnie ze scenariuszami testowymi,
- f) uruchomienie produkcyjne środowiska,
- g) przeprowadzenie instruktażu w formie warsztatu z zakresu zaktualizowanego środowiska klastra HCI dla pracowników Wydziału Informatyki Zamawiającego,
- h) świadczenie usług wsparcia gwarancyjnego.

2. Serwery – Wykonawca dostarczy 2 sztuki dodatkowych serwerów (węzły) wg poniższej specyfikacji (węzły) klastra HCI oraz skonfiguruje je do działania.

Element konfiguracji	Wymagania minimalne
Obudowa	Maksymalnie 1U RACK 19 cali (wraz z szynami montażowymi umożliwiającymi serwisowanie serwera w szafie rack bez odłączania urządzenia).
Procesor	Nie gorszy niż obecnie zainstalowane w posiadanych przez Zamawiającego serwerach (Intel Xeon Gold 5218R CPU @2,10 GHZ). jeden procesor min. 20-rdzeniowy o taktowaniu min. 2.1 GHz klasy x86 - 64 bity, umożliwiający uzyskanie w teście wydajnościowym z dnia 27 lutego 2024 roku minimum 24 700 pkt. (kolumna CPU Mark) w benchmarku CPU zgodnie z załącznikiem nr 8 do SWZ. Płyta główna wspierająca zastosowanie procesorów od 4 do 28 rdzeniowych, o mocy maksymalnej 205W i taktowaniu CPU do min. 3.9 GHz.
Liczba procesorów	1
Pamięć operacyjna	MIN. 512GB RDIMM DDR4 2933 MT/s w modułach o pojemności 64GB każdy. Płyta główna z minimum 24 slotami na pamięć i umożliwiająca instalację do minimum 3TB. Obsługa zabezpieczeń: Advanced ECC, Online Spare, Memory Mirroring, Memory Patrol Scrubbing Serwer umożliwiający instalowanie pamięci Intel Optane DC Persistent Memory oraz NVDIMM.
Sloty rozszerzeń	2 aktywne gniazda PCI-Express Generacji 3, w tym jeden slot x16 pozwalający na instalację karty o pełnej wysokości. Możliwość rozbudowy do min. 3 slotów PCI-Express generacji 3 w tym min 2 dla kart pełnej wysokości, przy pełnej obsadzie procesorów.
Dyski twarde	Obudowa serwera na minimum 8 dysków SFF 2,5'' typu Hot Swap, SAS/SATA/SSD z przodu obudowy i opcja rozbudowy/rekonfiguracji do min. 10 dysków NVMe Zainstalowane 7 dysków o pojemności min. 1,92tb (każdy) SSD SATA SFF o minimalnej wydajności zapisu losowego 50 tys IOPS dla bloków 4KiB oraz minimalnej wydajności odczytu losowego 65 tys IOPS dla bloków 4KiB oraz współczynnika DWRPD >= 3. Dodatkowo jeden dysk o po o pojemności 1,6TB SSD SAS SFF o minimalnej wydajności zapisu losowego 120 tys IOPS dla bloków 4KiB oraz minimalnej wydajności odczytu losowego 110 tys IOPS dla bloków 4KiB oraz współczynnika DWRPD >= 3. Dyski wyposażone w oprogramowanie układowe podpisane cyfrowo. Serwer wyposażony w układ pamięci flash w postaci kart microSD/SD zapewniających minimalną pojemność 32GB i

	redundancję danych RAID-1. Zastosowane rozwiązanie musi posiadać gwarancję producenta serwera.
Kontroler	<p>Kontroler sprzętowy wyposażony w 2GB cache, z mechanizmem podtrzymywania zawartości pamięci cache w razie braku zasilania, zapewniający obsługę wszystkich napędów dyskowych SAS/SATA/SSD oraz obsługujący poziomy: RAID 0,1,10,5,50,6,60.</p> <p>Serwer umożliwiający rozbudowę o sprzętowy kontroler RAID zapewniający obsługę RAID 0/1/10/5/50/6/60 z 4GB pamięci cache z podtrzymywaniem bateryjnym.</p> <p>Kontroler umożliwiający pracę z dyskami w trybach RAID i JBOD Jednocześnie.</p> <p>Kontroler z możliwością rozbudowy o funkcjonalność szyfrowania wolumenów logicznych stworzonych na podłączonych dyskach (szyfrowanie realizowane przez kontroler RAID, a nie przez oprogramowanie zainstalowane na systemie operacyjnym) lub kontroler z funkcją współpracy z dyskami samoszyfrującymi SED. W przypadku zastosowania kontrolera RAID z funkcją współpracy z dyskami samoszyfrującymi SED wszystkie zastosowane/dostarczone dyski typu SED.</p>
Interfejsy sieciowe	<p>Minimum 4 porty Ethernet 10gb/25gb w standardzie SFP28, zapewniające stabilną pracę istniejącego klastra HCI, wszystkie porty wyposażone w moduły 10GB SFP+ w standardzie SR</p> <p>Wykonawca zapewni niezbędną ilość wkładek w celu połączenia dodatkowych serwerów wraz z posiadanymi przez Zamawiającego serwerami w celu rozszerzenia posiadanego przez Zamawiającego klastra HA (nie mniej niż 8 szt.).</p>
Karta graficzna	Zintegrowana karta graficzna
Porty	<p>Min. 5 x USB min. 3.0 (w tym min. 1 port USB min. 3.0 wewnątrz serwera)</p> <p>Min. 1x VGA</p> <p>Możliwość rekonfiguracji / rozbudowy o:</p> <p>1x USB 2.0 (z przodu obudowy)</p> <p>1x - cyfrowy port video (Display Port lub HDMI)</p> <p>1x port szeregowy typu DB9/DE-9 (9-pinowy), wyprowadzony na zewnątrz obudowy bez pośrednictwa portu USB/RJ45 oraz bez konieczności instalowania kart w slotach PCI-Express</p> <p>Nie dopuszczalne jest stosowanie przejściówek ani kart PCI w celu uzyskania wymaganej powyżej ilości portów.</p>
Zasilacz	2 szt., typu Hot-plug, redundantne, każdy o mocy minimum 900W.
Chłodzenie	Zestaw wentylatorów redundantnych typu hot-plug
Napęd	<p>Brak.</p> <p>Możliwość rozbudowy/rekonfiguracji o wewnętrzny napęd DVD-RW</p>
Diagnostyka	Możliwość instalacji elektronicznego panelu diagnostycznego dostępnego z przodu serwera, pozwalającego uzyskać informacje o stanie: procesora, pamięci, wentylatorów, zasilaczy, kartach rozszerzeń, temperaturze.
Karta/moduł zarządzający	Niezależna od systemu operacyjnego, zintegrowana z płytą główną serwera lub jako dodatkowa karta w slotcie PCI Express, jednak nie może ona powodować zmniejszenia minimalnej liczby gniazd PCIe w serwerze, posiadająca minimalną funkcjonalność:

- monitorowanie podzespołów serwera: temperatura, zasilacze, wentylatory, procesory, pamięć RAM, kontrolery macierzowe i dyski (fizyczne i logiczne), karty sieciowe
- wsparcie dla agentów zarządzających oraz możliwość pracy w trybie bezagentowym – bez agentów zarządzania instalowanych w systemie operacyjnym z generowaniem alertów SNMP
- dostęp do karty zarządzającej poprzez
 - dedykowany port RJ45
 - przez współdzielony port zintegrowanej karty sieciowej serwera
- dostęp do karty możliwy
 - z poziomu przeglądarki internetowej (GUI)
 - z poziomu linii komend zgodnie z DMTF System Management Architecture for Server Hardware, Server Management Command Line Protocol (SM CLP)
 - z poziomu skryptu (XML/Perl)
 - poprzez interfejs IPMI 2.0 (Intelligent Platform Management Interface)
- wbudowane narzędzia diagnostyczne
- zdalna konfiguracji serwera (BIOS) i instalacji systemu operacyjnego
- obsługa mechanizmu remote support - automatyczne połączenie karty z serwisem producenta sprzętu, automatyczne przesyłanie alertów, zgłoszeń serwisowych i zdalne monitorowanie
 - wbudowany mechanizm logowania zdarzeń serwera i karty zarządzającej w tym włączanie/wyłączanie serwera, restart, zmiany w konfiguracji, logowanie użytkowników
- przesyłanie alertów poprzez e-mail oraz przekierowanie SNMP (SNMP passthrough)
- obsługa zdalnego serwera logowania (remote syslog)
 - wirtualna zdalna konsola, tekstowa i graficzna, z dostępem do myszy i klawiatury i możliwością podłączenia wirtualnych napędów FDD, CD/DVD i USB i wirtualnych folderów
- mechanizm przechwytywania, nagrywania i odtwarzania sekwencji video dla ostatniej awarii i ostatniego startu serwera a także nagrywanie na żądanie
 - funkcja zdalnej konsoli szeregowej - Textcons przez SSH (wirtualny port szeregowy) z funkcją nagrywania i odtwarzania sekwencji zdarzeń i aktywności
- monitorowanie zasilania oraz zużycia energii przez serwer w czasie rzeczywistym z możliwością graficznej prezentacji
- konfiguracja maksymalnego poziomu pobieranej mocy przez serwer (capping)
- zdalna aktualizacja oprogramowania (firmware)
- zarządzanie grupami serwerów, w tym:
 - tworzenie i konfiguracja grup serwerów
 - sterowanie zasilaniem (wł/wył)
 - ograniczenie poboru mocy dla grupy (power capping)
 - aktualizacja oprogramowania (firmware)
 - wspólne wirtualne media dla grupy
- możliwość równoczesnej obsługi przez 6 administratorów
- autentykacja dwuskładnikowa (Kerberos)

	<ul style="list-style-type: none"> • wsparcie dla Microsoft Active Directory • obsługa SSL i SSH • enkrypcja AES/3DES oraz RC4 dla zdalnej konsoli • wsparcie dla IPv4 oraz IPv6, obsługa SNMP v3 oraz RESTful API • wsparcie dla Integrated Remote Console for Windows clients • możliwość autokonfiguracji sieci karty zarządzającej (DNS/DHCP) <p>Karta zdalnego zarządzania musi posiadać wbudowaną pamięć flash, minimum 4GB, w tym minimum 1GB dostępny dla użytkownika serwera.</p> <p>Rozwiązanie sprzętowe, niezależne od systemów operacyjnych, zintegrowane z płytą główną, posiadające dedykowany port RJ45.</p>
Wsparcie dla systemów operacyjnych i systemów wirtualizacyjnych	<p>Microsoft Windows Server 2016, 2019, 2022</p> <p>Red Hat Enterprise Linux (RHEL) 7, 8</p> <p>SUSE Linux Enterprise Server (SLES) 12, 15</p> <p>Canonical Ubuntu 18.x</p> <p>VMware ESXi 6.7 U3, 7.0, 7.0 U1, 8.0 U1, 8.0 U2</p>
System monitorowania i analizowania konfiguracji serwerów – wymaganie nieobligatoryjne, punktowane dodatkowo	<p>Dostęp do systemu dla każdego serwera. Licencje (jeżeli są wymagane) dożywotnie ze wsparciem technicznym na okres zgodny z wymaganą gwarancją/wsparciem serwisowym dla serwerów.</p> <p>System w postaci platformy uruchomionej w chmurze i dostępnej jako usługa webowa (z przeglądarki internetowej), system niezależny od infrastruktury IT miejsca instalacji serwerów. Platforma wspierana uczeniem maszynowym i analizą predykcyjną, zapewniająca automatyczne zbieranie i analizę danych z modułów zarządzania serwerami w celu monitorowania, analizy ich pracy i porównania zachowania serwerów z danymi z referencyjnej bazy danych wszystkich podłączonych do tego systemu serwerów.</p> <p>System zapewniający:</p> <ul style="list-style-type: none"> - scentralizowany widok parametrów monitorowanych serwerów, co najmniej: numer seryjny, stan zdrowia (Ok, Ostrzeżenie, itp), stan zasilania (Wł., Wył.), nazwa produktu (model serwera), status poszczególnych komponentów (zasilacz, pamięć, procesor, dyski, itp.); - informacje na temat stanu gwarancji serwera – co najmniej czy jest aktywna; - prezentację wersji zainstalowanego oprogramowania układowego na poszczególnych komponentach serwera; - rekomendacje odnośnie optymalizacji i poprawy wydajności serwerów, przewidywanie oraz zapobieganie problemom; - analizę danych pod kątem bezpieczeństwa serwerów np. ostrzeżenie użytkownika o nieudanych próbach logowania; - prognozy pod kątem awarii poprzez ostrzeżenie użytkownika o uszkodzonych komponentach; - zalecenia dotyczące eliminacji źródeł/przyczyn problemów np. wydajnościowych serwerów.
Integracja i aktualizacje z poziomu VMware vSphere	<p>Uproszczona administracja poprzez integrację infrastruktury fizycznej z wirtualną. Licencje (jeżeli są wymagane) na okres zgodny z wymaganą gwarancją/wsparciem serwisowym dla serwerów.</p> <p>Możliwość wykonywania kompleksowych aktualizacji serwera (ESXi, sterowników, oprogramowania firmware) z wykorzystaniem vSphere Lifecycle Manager (vLCM).</p>

Gwarancja	Minimum 5-letnia gwarancja producenta 7x24h, z gwarantowanym czasem naprawy w 6h od złożenia awarii, uszkodzone dyski pozostają u zamawiającego (keep your hard drive). Usługa wsparcia technicznego musi być świadczona przez serwis producenta oferowanych urządzeń.
Inne	Urządzenia muszą być zakupione w oficjalnym kanale dystrybucyjnym producenta. Na żądanie Zamawiającego, Wykonawca musi przedstawić oświadczenie producenta oferowanego serwera, potwierdzające pochodzenie urządzenia z oficjalnego kanału dystrybucyjnego producenta. Deklaracja zgodności CE.

3. Rozbudowa posiadanych przez Zamawiającego serwerów HPE PROLIANT DL360 GEN 10 (4SZT) o dodatkowe dyski (rozbudowa po 1 szt. dysku do każdego z serwerów).

Wykonawca dostarczy oraz zainstaluje i skonfiguruje istniejące serwery (węzły) klastra o dodatkowe dyski SSD o minimalnych poniższych parametrach:

min. 1,92tb (każdy) SSD SATA SFF o minimalnej wydajności zapisu losowego 50 tyś IOPS dla bloków 4KiB oraz minimalnej wydajności odczytu losowego 65 tyś IOPS dla bloków 4KiB oraz współczynnika DWPD >= 3.

4. Dostarczenie licencji dla systemu wirtualizacji oraz funkcji HCI.

- a) Wykonawca dostarczy dodatkowe licencje (3 letnie) zgodne z posiadaniem i użytkowanym przez Zamawiającego systemem **VMware vSphere 8 Enterprise Plus** lub równoważne wg poniższych kryteriów równoważności, ilość licencji zgodna z ilością procesorów w dostarczanych przez Wykonawcę serwerach.
- b) Wykonawca dostarczy dodatkowe licencje (3 letnie) zgodne z posiadaniem i użytkowanym przez Zamawiającego systemem **VMware vSan 8 Enterprise** lub równoważne wg poniższych kryteriów równoważności, ilość licencji zgodna z ilością procesorów w dostarczanych przez Wykonawcę serwerach.
- c) Wykonawca dostarczy dodatkowe licencje zgodne z posiadaniem i użytkowanym przez Zamawiającego systemem **Microsoft Windows 2019 Datacenter** (w przypadku niedostępności wersji 2019 dopuszczalne jest dostarczenie Microsoft Windows 2022 Datacenter) lub równoważne wg. poniższych kryteriów równoważności, ilość licencji zgodna z ilością procesorów w dostarczanych przez Wykonawcę serwerach
- d) Wykonawca dostarczy dodatkowe licencje dla posiadanych obecnie przez Zamawiającego **4 szt.** serwerów HPE na oprogramowanie służące do Integracji i aktualizacji serwerów z poziomu VMware vSphere - **HPE OneView + HPE OneView VMware vSphere plugin**.

Kryteria równoważności dla oprogramowania VMWARE z punktu a) oraz b)

Dostarczone rozwiązanie musi być rozwiązaniem systemowym tzn. musi być zainstalowana bezpośrednio na sprzęcie fizycznym, nie może być częścią innego systemu operacyjnego oraz musi spełniać poniższe warunki:

1. Warstwa wirtualizacji nie może dla własnych celów alokować więcej niż 200MB pamięci operacyjnej RAM serwera fizycznego.
2. Oprogramowanie do wirtualizacji zainstalowane na serwerze fizycznym musi potrafić obsłużyć i wykorzystać procesory fizyczne wyposażone w 576 logicznych wątków oraz do 12TB pamięci fizycznej RAM.
3. Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych 1-128 procesorowych.
4. Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych z możliwością przydzielenia do 6 TB pamięci operacyjnej RAM.
5. Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych, z których każda może mieć 1-10 wirtualnych kart sieciowych.
6. Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych, z których każda może mieć 32 porty szeregowo, 3 porty równoległe i 20 urządzeń USB.
7. Rozwiązanie musi wspierać następujące systemy operacyjne: Windows Server 2012, Windows Server 2016, Windows Server 2019, Windows 7, Windows 8, Windows 10, SLES 15 SLES 12, SLES 11, REHL 7, RHEL 6, RHEL 5, REHL Atomic 7, Solaris 11 ,Solaris 10, Solaris 9, Solaris 8, Debian, CentOS, FreeBSD, Mandriva, Ubuntu, Mac OS X, Oracle Linux.
8. Rozwiązanie musi umożliwiać przydzielenie większej ilości pamięci RAM dla maszyn wirtualnych niż fizyczne zasoby RAM serwera w celu osiągnięcia maksymalnego współczynnika konsolidacji.
9. Rozwiązanie musi umożliwiać udostępnienie maszynie wirtualnej większej ilości zasobów dyskowych niż jest fizycznie zarezerwowane na zasobach dyskowych.
10. Rozwiązanie musi umożliwiać integrację z rozwiązaniami antywirusowymi firm trzecich w zakresie skanowania maszyn wirtualnych z poziomu warstwy wirtualizacji.
11. Rozwiązanie musi zapewniać zdalny i lokalny dostęp administracyjny do wszystkich serwerów fizycznych poprzez protokół SSH, z możliwością nadawania uprawnień do takiego dostępu nazwanym użytkownikom bez konieczności wykorzystania konta root.
12. Oprogramowanie do wirtualizacji musi zapewnić możliwość klonowania systemów operacyjnych wraz z ich pełną konfiguracją i danymi.
13. Oprogramowanie do wirtualizacji musi zapewnić możliwość wykonywania kopii migawkowych instancji systemów operacyjnych na potrzeby tworzenia kopii zapasowych bez przerywania ich pracy z możliwością wskazania konieczności zachowania stanu pamięci pracującej maszyny wirtualnej.
14. Oprogramowanie zarządzające musi posiadać możliwość przydzielania i konfiguracji uprawnień z możliwością integracji z usługami katalogowymi, w szczególności: Microsoft Active Directory, Open LDAP.
15. Rozwiązanie musi zapewniać możliwość dodawania zasobów w czasie pracy maszyny wirtualnej, w szczególności w zakresie ilości procesorów, pamięci operacyjnej i przestrzeni dyskowej.
16. Rozwiązanie musi posiadać funkcjonalność wirtualnego przełącznika (virtual switch) 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.
17. 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.
18. Wirtualne przełączniki muszą obsługiwać wirtualne sieci lokalne (VLAN).
19. Rozwiązanie musi zapewniać możliwość konfigurowania polityk separacji sieci w warstwie trzeciej, tak aby zapewnić oddzielne grupy wzajemnej komunikacji pomiędzy maszynami wirtualnymi.

20. Rozwiązanie musi umożliwiać wykorzystanie technologii 10GbE w tym agregację połączeń fizycznych do minimalizacji czasu przenoszenia maszyny wirtualnej pomiędzy serwerami fizycznymi.
21. Oprogramowanie do wirtualizacji musi obsługiwać przełączenie ścieżek LAN (bez utraty komunikacji) w przypadku awarii jednej ze ścieżek.
22. Rozwiązanie musi zapewnić możliwość zdefiniowania alertów informujących o przekroczeniu wartości progowych.
23. Rozwiązanie musi zapewniać możliwość replikacji maszyn wirtualnych z dowolnej pamięci masowej w tym z dysków wewnętrznych serwerów fizycznych na dowolną pamięć masową w tym samym lub oddalonym ośrodku przetwarzania.
24. Rozwiązanie replikujące musi gwarantować współczynnik RPO na poziomie minimum 5 minut.
25. Czas planowanego przestoju usług związany z koniecznością prac serwisowych (np. rekonfiguracja serwerów, macierzy, switchy) musi być ograniczony do minimum. Konieczna jest możliwość przenoszenia maszyn wirtualnych pomiędzy serwerami fizycznymi bez przerywania pracy usług.
26. Rozwiązanie musi mieć możliwość przenoszenia maszyn wirtualnych w czasie ich pracy pomiędzy serwerami fizycznymi oraz różnymi konsolami do zarządzania wirtualizacją. Rozwiązanie musi posiadać natywne mechanizmy szyfrowania, podczas przenoszenia maszyn wirtualnych, w czasie ich pracy pomiędzy serwerami fizycznymi.
27. Musi zostać zapewniona odpowiednia redundancja i nadmiarowość zasobów tak by w przypadku awarii np. serwera fizycznego usługi na nim świadczone zostały automatycznie przełączone na inne serwery infrastruktury.
28. Rozwiązanie musi umożliwiać łatwe i szybkie ponowne uruchomienie systemów/usług w przypadku awarii poszczególnych elementów infrastruktury bez utraty danych.
29. Rozwiązanie musi zapewnić bezpieczeństwo danych mimo poważnego uszkodzenia lub utraty sprzętu lub oprogramowania.
30. Rozwiązanie musi zapewniać mechanizm bezpiecznego, bezprzerwowego i automatycznego uaktualniania warstwy wirtualizacyjnej wliczając w to zarówno poprawki bezpieczeństwa jak i zmianę jej wersji bez potrzeby wyłączenia wirtualnych maszyn.
31. 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.
32. Decyzja o próbie przywrócenia funkcjonalności maszyny wirtualnej w przypadku awarii lub niedostępności serwera fizycznego powinna być podejmowana automatycznie, jednak musi istnieć możliwość określenia przez administratora czasu po jakim taka decyzja jest wykonywana.
33. Rozwiązanie musi zapewniać pracę bez przestojów dla wybranych maszyn wirtualnych (o maksymalnie dwóch procesorach wirtualnych), niezależnie od systemu operacyjnego oraz aplikacji, podczas awarii serwerów fizycznych, bez utraty danych i dostępności danych podczas awarii serwerów fizycznych.
34. Oprogramowanie do wirtualizacji musi obsługiwać przełączenie ścieżek SAN (bez utraty komunikacji) w przypadku awarii jednej ze ścieżek.
35. Oprogramowanie do wirtualizacji musi zapewniać możliwość stworzenia dysku maszyny wirtualnej o wielkości do 62 TB.
36. Rozwiązanie musi posiadać wbudowany interfejs programistyczny (API) zapewniający pełną integrację zewnętrznych rozwiązań wykonywania kopii zapasowych z istniejącymi mechanizmami warstwy wirtualizacyjnej.
37. Rozwiązanie musi umożliwiać konfiguracje HA dla każdego swojego komponentu w celu unikania awarii pojedynczego elementu.
38. Oprogramowanie do wirtualizacji musi być wspierane przez producenta oferowanego rozwiązania do automatyzacji procesów (Automatyzacja) oraz wirtualizacji sieci (SDN) na wszystkich poziomach wsparcia (L1-L3). Wsparcie musi odbywać się poprzez jednorodny kanał serwisowy (jeden

numer telefonów dla wszystkich zgłoszeń, jeden portal www pozwalający zarządzać licencjami i zgłaszać zlecenia serwisowe).

39. System musi wspierać mechanizmy zaawansowanego uwierzytelniania do systemu operacyjnego wirtualnej maszyny za pomocą technologii Smart Card Reader.

40. Wirtualizator musi wspierać TPM 2.0 oznacza to min., że TPM zapewnia mechanizm gwarantujący, że serwer fizyczny uruchomił się z włączoną opcją Secure Boot. Po potwierdzeniu, że Secure Boot jest włączone, system gwarantuje, że wirtualizator uruchomił w prawidłowej, niezmięnionej formie poprzez weryfikację podpisu cyfrowego.

41. Wirtualizator musi mieć możliwość włączenia funkcji "Microsoft virtualization- based security", tzw. Microsoft VBS dla systemów operacyjnych maszyn wirtualnych opartych o system operacyjny Windows 10 oraz Windows Server 2019.

42. System musi posiadać certyfikację FIPS-140-2 min. dla modułu jądra wirtualizatora odpowiedzialnego za szyfrowanie danych.

43. Wirtualizator musi posiadać funkcjonalność wirtualnego TPM 2.0 dla maszyn wirtualnych Windows 10 oraz Windows 2019. Oznacza to, że punktu widzenia maszyny wirtualnej z systemem operacyjnym Windows 10 lub Windows 2019 wirtualny TPM widziany jest jako standardowy TPM, gdzie można przechowywać bezpiecznie wrażliwe dane np. certyfikaty. Zawartość wirtualnego TPM przechowywana jest w pliku przynależnym do maszyny wirtualnej oraz musi być szyfrowana. W związku z tym wszystkie standardowe funkcjonalności wirtualizatora tj. wysoka dostępność czy przenoszenie maszyn wirtualnych bez ich wyłączenia pomiędzy różnymi serwerami fizycznymi działa prawidłowo. Wirtualizator musi posiadać rolę administratora odpowiedzialnego za zarządzanie kluczami szyfrującymi. Rola ta powinna być odseparowana od roli administratora wirtualizatora. Oznacza to, że tylko administrator odpowiedzialny za szyfrowanie ma dostęp do kluczy szyfrujących oraz może zarządzać procesem szyfrowania w obrębie wirtualizatora.

44. Wirtualizator musi posiadać funkcjonalność szybkiego uruchamiania wirtualizatora po przeprowadzonym procesie jego aktualizacji. Taka funkcjonalność powoduje, że w procesie aktualizacji wirtualizatora, jeśli wymagany jest jego restart, eliminowana jest czasochłonna faza inicjalizacji serwera fizycznego – następuje skrócenia czasu wymaganego do ponownego uruchomienia serwera fizycznego podczas operacji aktualizacji.

45. Dostarczone oprogramowanie musi zapewniać możliwość wirtualizacji dla wszystkich dostarczonych w ramach postępowania serwerów.

46. Rozwiązanie musi posiadać mechanizm, który ogranicza dostęp do indywidualnego zarządzania warstwą wirtualizacji na serwerach fizycznych w ramach klastra serwerów w celu utwardzenia/hardening (maksymalnego zwiększenia bezpieczeństwa dostępu) systemu wirtualizacji. System musi umożliwiać zarządzanie całą warstwą wirtualizacji z jednego bezpiecznego systemu do zarządzania z kontrolą dostępu.

47. Rozwiązanie wirtualizatora musi posiadać mechanizmy proaktywnej wysokiej dostępności. Oznacza to, że jeśli serwer fizyczny posiada funkcję przekazania do wirtualizatora informacji o stanie serwera, to wirtualizator na podstawie tych danych, jest w stanie, proaktywnie przenieść wszystkie maszyny wirtualne na inne prawidłowo działające serwery fizyczne w klastrze, zanim dojdzie do całkowitej awarii serwera fizycznego.

48. Rozwiązanie musi umożliwiać automatyczne równoważenie obciążenia CPU/MEM serwerów fizycznych pracujących jako platforma dla infrastruktury wirtualnej.

49. Oprogramowanie do wirtualizacji musi zapewniać mechanizm pozwalający tworzyć profil (szablon konfiguracji) wybranego serwera wirtualizującego, a następnie wymuszać ten profil/konfigurację na innych serwerach lub sprawdzać zgodność konfiguracji pomiędzy zdefiniowanym wcześniej profilem a wskazanym serwerem fizycznym.

50. Rozwiązanie musi umożliwiać utworzenie jednorodnego, wirtualnego przełącznika sieciowego, rozproszonego na wszystkie serwery fizyczne platformy wirtualizacyjnej. Przełącznik taki musi zapewniać możliwość konfiguracji parametrów sieciowych maszyny wirtualnej z granulacją na

poziomie portu tego przełącznika. Pojedyncza maszyna wirtualna musi mieć możliwość wykorzystania jednego lub wielu portów przełącznika z niezależną od siebie konfiguracją.

51. Przełącznik rozproszony musi współpracować z protokołem NetFlow.

52. Platforma wirtualizacji powinna w ramach przełącznika sieciowego musi zapewniać możliwość integracji z produktami (przełącznikami wirtualnymi) firm trzecich, tak aby umożliwić granularną delegację zadań w zakresie zarządzania konfiguracją sieci do zespołów sieciowych.

53. Przełącznik rozproszony musi umożliwiać funkcjonalność duplikowania ruchu sieciowego dowolnego jego portu wirtualnego na inny port.

54. Przełącznik musi mieć wbudowane mechanizmy składowania kopii konfiguracji, przywracania tej kopii a także mechanizmy automatycznie zapobiegające niewłaściwej konfiguracji sieciowej, które w całości lub w części mogą eliminować błędy ludzkie i utratę łączności sieciowej.

55. System musi mieć wbudowany mechanizm kontrolowania i monitorowania ruchu sieciowego oraz ustalania priorytetów w zależności od jego rodzaju na poziomie konkretnych maszyn wirtualnych.

56. System musi mieć możliwość uruchamiania fizycznych serwerów z centralnie przygotowanego obrazu poprzez protokół PXE.

57. 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 z okresu co najmniej 12 ostatnich miesięcy.

58. Rozwiązanie musi mieć możliwość przenoszenia maszyn wirtualnych w czasie ich pracy pomiędzy serwerami fizycznymi, pamięciami masowymi niezależnie od dostępności współdzielonej przestrzeni dyskowej, różnymi rodzajami wirtualnych przełączników sieciowych oraz pomiędzy różnymi Centrami Przetwarzania Danych platformami wirtualnej.

59. Rozwiązanie musi zapewniać pracę bez przestoju dla wybranych maszyn wirtualnych (o maksymalnie czterech procesorach wirtualnych), niezależnie od systemu operacyjnego oraz aplikacji, podczas awarii serwerów fizycznych, bez utraty danych i dostępności danych podczas awarii serwerów fizycznych.

60. Rozwiązanie musi posiadać proaktywnie działający mechanizm, który dokona migracji wirtualnych maszyn po wykryciu potencjalnego problemu z serwerem fizycznym, zanim on ulegnie awarii.

61. System musi mieć wbudowany mechanizm kontrolowania i monitorowania ruchu do pamięci masowych oraz ustalania priorytetów dostępu do nich na poziomie konkretnych wirtualnych maszyn.

62. System musi mieć możliwość grupowania pamięci masowych o podobnych parametrach w grupy i przydzielania ich do wirtualnych maszyn zgodnie z ustaloną przez administratora polityką.

63. System musi umożliwiać udostępnianie pojedynczego urządzenia fizycznego (PCIe) jako logicznie separowane wirtualne urządzenia dedykowane dla poszczególnych maszyn wirtualnych.

64. System musi mieć możliwość równoważenia obciążenia i zajętości pamięci masowych wraz z pełną automatyką i przenoszeniem plików wirtualnych maszyn z bardziej zajętych na mniej zajęte przestrzenie dyskowe lub/i z przestrzeni dyskowych bardziej obciążonych operacjami I/O na mniej obciążone.

65. Rozwiązanie jako funkcja wirtualizatora (jądra) musi umożliwiać szyfrowanie wirtualnych maszyn oraz szyfrowanie maszyny wirtualnej podczas przenoszenia bez przerywania jej pracy na innych host lub zasób dyskowy.

66. System musi zapewniać mechanizm weryfikujący integralność komponentów systemowych i plików hosta wirtualizującego i wirtualnej maszyny podczas ich uruchamiania (ochrona systemu hypervisor i OS wirtualnej maszyny na wypadek sfałszowania lub podmiany).

Kryteria równoważności dla oprogramowania z punktu c)

1. System operacyjny musi być przeznaczony do zastosowań serwerowych w Centra danych i środowiskach chmur o wysokim stopniu wirtualizacji.

2. System operacyjny musi być najnowszą wersją rodziny systemów operacyjnych danego producenta.
3. Warunki licencjonowania systemu operacyjnego muszą zezwalać na zmianę wersji systemu operacyjnego na niższą z zachowaniem wsparcia technicznego oraz na przeniesienie licencji systemu operacyjnego na inny fizyczny serwer.
4. W ramach dostarczonej licencji na system operacyjny musi być zawarta możliwość instalacji oprogramowania na serwerze wieloprocesorowym.
5. System operacyjny musi mieć możliwość obsługi 64 procesorów fizycznych oraz co najmniej 64 procesorów logicznych (wirtualnych).
6. System operacyjny musi obsługiwać pamięć RAM w ramach jednej instancji systemu operacyjnego w wysokości przynajmniej 4TB.
7. System operacyjny musi mieć możliwość uruchomienia roli serwera DHCP, w tym funkcji klastrowania serwera DHCP (możliwość uruchomienia dwóch serwerów DHCP operujących jednocześnie na tej samej puli oferowanych adresów IP).
8. Licencja na system operacyjny musi być bez ograniczeń czasowych.
9. Licencja na system operacyjny musi pozwalać na zainstalowanie systemu przez Zamawiającego na Dostarczanych przez Wykonawcę serwerach zgodnie z polityką licencjonowania producenta oprogramowania w zakresie przypisania licencji dla procesorów oraz rdzeni fizycznych procesorów.
10. Licencja musi uprawniać do uruchamiania systemu operacyjnego w środowisku fizycznym i nielimitowaną ilość w środowiskach wirtualnych za pomocą wbudowanych mechanizmów wirtualizacji, bez konieczności zakupu dodatkowych licencji.
11. Zaimplementowanie w systemie operacyjnym środowiska wirtualizacyjnego musi umożliwiać dodawanie i usuwanie pamięci wirtualnej oraz wirtualnych kart sieciowych podczas pracy maszyny wirtualnej.
12. System operacyjny musi posiadać graficzny interfejs użytkownika.
13. System operacyjny musi być w pełni kompatybilny z usługą Active Directory w zakresie:
 - a. zarządzania użytkownikami,
 - b. zarządzania certyfikatami dla użytkowników wraz ze wsparciem możliwości logowania do domeny kartą mikroprocesorową,
 - c. możliwości przydzielania praw dostępu do zasobów sieciowych,
 - d. instalacji zdalnej oprogramowania z pakietów msi,
 - e. definiowania polityk bezpieczeństwa dla użytkowników, grup oraz stacji roboczych z systemami MS Windows.
14. System operacyjny musi wspierać pracę domenową wraz z automatyczną synchronizacją dla dodatkowych serwerów.
15. System operacyjny musi wspierać zarządzanie przez dostępne narzędzia administracji serwera dla systemu Windows 10/11 (RSAT) oraz Windows Admin Center.
16. System operacyjny musi posiadać obsługę zdalnego pulpitu zgodnie z protokołem RDP.
17. System operacyjny musi umożliwiać ustawianie relacji zaufania pomiędzy domenami.
18. Wszystkie narzędzia i usługi wykorzystywane w systemie operacyjnym powinny być rozwiązaniem jednego producenta.
19. System operacyjny musi pozwalać na obsługę pamięci USB jako monitora klastra (IJSB Witness)
20. System operacyjny musi posiadać obsługę deduplikacji na potrzeby systemu plików ReFS.
21. System operacyjny musi posiadać obsługę optymalizacji transportu w tle pod kątem opóźnień.
22. System operacyjny musi posiadać wbudowaną zaporę internetową (firewall) dla ochrony połączeń internetowych; zapora musi być zintegrowana z systemem konsoli do zarządzania ustawieniami zapory i regułami ip v4 i v6.
23. System operacyjny musi posiadać możliwość uruchomienia serwera DNS z możliwością integracji z kontrolerem domeny.
24. System operacyjny musi posiadać możliwość zdalnej automatycznej instalacji, konfiguracji, administrowania oraz aktualizowania systemu.
25. System operacyjny musi posiadać domyślną obsługę PowerShell 5 1.
26. System operacyjny musi posiadać obsługę certyfikatów Active Directory.

27. System operacyjny musi posiadać funkcję Software Defined Networking (SDN).
28. Wszystkie wymienione powyżej parametry, funkcje systemu operacyjnego objęte muszą być dostarczoną licencją (licencjami) i zawarte w dostarczonej wersji oprogramowania (nie wymagają ponoszenia przez Zamawiającego dodatkowych kosztów).

Kryteria równoważności dla oprogramowania z punktu d)

1. System umożliwiający wykonywanie kompleksowych aktualizacji serwerów (ESXi, sterowników, oprogramowania firmware) za pomocą vSphere Lifecycle Manager (vLCM).
2. System będzie sygnalizował problemy poprzez przesyłanie zdarzeń sprzętowych do konsoli zarządzania vSphere.

5. Opis wymagań w zakresie usług wdrożeniowych.

1. Usługa instalacji i konfiguracji nowych serwerów (węzłów) klastra HCI w tym:
montaż w szafach RACK,
podłączenie zasilania,
podłączenie sieci zarządzania,
podłączenie wydzielonej sieci LAN dla HCI oraz dostępu do sieci LAN produkcyjnej oraz synchronizacja czasu NTP,
aktualizacja oprogramowania mikroukładowego (firmware) wszystkich 6 serwerów i posiadanych przez Zamawiającego (w klastrze) przełączników HPE Aruba,
aktualizacja składników klastra (wirtualizatorów vSphere, konsoli vCenter i wersji vSan) do zalecanych przez producenta wersji i w celu zachowania spójnej i stabilnej wersji środowiska,
weryfikacja ustawień kont administratorów oraz ich uprawnień
2. podłączenie i wdrożenie dwóch nowych serwerów (węzłów) klastra do działania w infrastrukturze Zamawiającego,
3. instalacja i konfiguracja oprogramowania do wirtualizacji serwerów (hypervisorów) na dwóch nowych serwerach środowiska wirtualizacji,
4. zamontowanie oraz skonfigurowanie dodatkowych dysków dla czterech istniejących serwerów Zamawiającego oraz skonfigurowanie w istniejącej strukturze pamięci masowej klastra HCI
5. integracja nowych serwerów z obecnym środowiskiem wirtualizacji serwerów w tym:
konfiguracja systemu logowania zdarzeń,
konfiguracja sieci zarządzania,
konfiguracja usług vMotion,
konfiguracja klastra wysokiej dostępności,
konfiguracja systemu równoważenia obciążenia,
6. rekonfiguracja posiadanego przez Zamawiającego systemu do Integracji i aktualizacji serwerów z poziomu VMware vSphere (opartego na zwirtualizowanym w zasobach Zamawiającego „Ilo Amplifier Pack” + Hpe HSM Plugin dla VMware vCenter) do nowego wspieranego przez producenta posiadanych przez Zamawiającego serwerów systemu tj. Hpe OneView + Hpe OneView for VMware vCenter plugin.
 - a. instalacja i konfiguracja w formie maszyny wirtualnej w zasobach Zamawiającego rozwiązania Hpe OneView,
 - b. deinstalacja obecnego plugin’u HPE HCM i konfiguracja nowego plugin’u Hpe OneView dla VMware vCenter,
 - c. rekonfiguracja serwerów posiadanych przez Zamawiającego do współpracy z nowym rozwiązaniem,
7. przeprowadzenie testów niezawodności klastra HCI,

8. przeprowadzenie testów poprawności wyłączenia środowiska wirtualizacji w sytuacji zaniku zasilania,
9. zainstalowanie i skonfigurowanie systemu wirtualizacji zasobów dyskowych,
10. integracja rozwiązania do wirtualizacji zasobów dyskowych z rozwiązaniem wirtualizacji serwerów, w tym udostępnienie zasobów do klastra wirtualizacji,
11. zainstalowanie i skonfigurowanie systemu wirtualizacji sieci,
12. integracja rozwiązania do wirtualizacji sieci z rozwiązaniem wirtualizacji serwerów, w tym: konfiguracja komunikacji wdrożonych sieci i VLAN do współpracy z infrastrukturą sieciową zamawiającego, aktualizacja routingu, przełączanie sieci, NAT oraz polityk firewall,
13. aktualizacja procedur eksploatacyjnych dla klastra HCI w zakresie wykonywania operacji administracyjnych, a w szczególności instalacji, aktualizacji nowych maszyn wirtualnych, oraz instalacji poprawek dla oprogramowania wirtualizacyjnego,
14. przeprowadzenie testów procedur eksploatacyjnych i administracyjnych wdrażanego środowiska zgodnie z założeniami opracowanego przez Wykonawcę projektu wdrożenia
15. przygotowanie dokumentacji powykonawczej przedmiotu zamówienia. Dokumentacja musi zawierać przynajmniej informacje w zakresie: architektury logicznej, fizycznej i sieciowej oraz logicznej sieci LAN po wykonanych działaniach rozbudowy oraz aktualizacji środowisk, Konfiguracji klastra HCI, zasobów dyskowych i sieci.

6. Instrukcja w formie warsztatu:

Instrukcja z wdrożonego rozwiązania, dla 5-ciu (pięciu) administratorów wskazanych przez Zamawiającego, minimum trzydniowe szkolenie autorskie w języku polskim, materiały szkoleniowe w języku polskim, szkolenie przeprowadzone na infrastrukturze sprzętowej Wykonawcy, kompatybilnej z dostarczoną w niniejszym postępowaniu.