***Załącznik nr 1***

*do Zapytania ofertowego nr 1/2024*

# OPIS PRZEDMIOTU ZAMÓWIENIA

## „Zakup i dostawa serwera do nowej pracowni w Ostródzie”

### 1. Serwer - 1 kpl.

| Nazwa parametru lub składnika technicznego | Minimalne parametry techniczne i wymagania |
|---|---|
| **Obudowa** | – Obudowa rack o wysokości max. 1U umożliwiającą instalację min. 2 dysków 3.5” z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych.<br>– Głębokość obudowy max. 39 cm.<br>– Zatoki dyskowe gotowe do zainstalowania 2 dyski LFF typu Hot Plug, SAS/SATA/SSD 3.5”.<br>– Czujnik otwarcia obudowy współpracujący z BIOS/UEFI.<br>– Zdejmowany panel przedni.<br>– W zestawie szyny montażowe do szafy rack |
| **Płyta główna** | – Jednoprocesorowa płyta wyprodukowana i zaprojektowana przez producenta serwera z możliwością instalacji procesorów do 8 rdzeniowych i mocy 95W.<br>– Moduł TPM min. 2.0 |
| **Procesor** | – Zainstalowany jeden procesor min. 8-rdzeniowy klasy x86 z częstotliwością bazową min. 2.8 GHz umożliwiające osiągnięcie wyniku min. 70.1 punktów w teście SPECrate2017_int_base oraz min. 57.4 punktów w teście SPECrate2017_fp_base dostępnym na stronie www.spec.org dla oferowanego modelu serwera. |
| **Pamięć operacyjna** | – Zainstalowane 96GB pamięci RAM typu DDR4 3200 MT/s w modułach dwubankowych o pojemności 32GB każdy.<br>– Wsparcie dla technologii zabezpieczania pamięci: ECC. |
| **Sloty rozszerzeń** | – Serwer musi być wyposażony w 2 aktywne gniazda PCIe Gen4 x8 (buswidth) gotowe do obsadzenia kartami w tym min. jeden slot pełnej wysokości. |
| **Dyski** | – Zainstalowane dwa dyski 480GB NVMe M.2 każdy skonfigurowane fabrycznie w RAID1 ze wsparciem ESXi.<br>– Zainstalowane min. 2 dyski HDD o pojemności co najmniej 16TB SAS 7.2k 3.5” każdy skonfigurowane fabrycznie w RAID1. |
| **Kontroler** | – Zainstalowany w dedykowanym slocie nie zajmującym slotów PCIe opisanych w punkcie „Sloty rozszerzeń” sprzętowy kontroler RAID zapewniający obsługę 8 napędów dyskowych SAS, SATA, oraz obsługujący poziomy RAID 0, 1, 5, 6, 10, 50, 60 z 2GB pamięci cache oraz podtrzymywaniem bateryjnym.<br>– Kontrolery muszą umożliwiać pracę z dyskami w trybach RAID i HBA jednocześnie. |
| **Interfejsy sieciowe** | – Zintegrowane trwale i nieusuwalnie z płytą główną 2x 1 Gbit/s BaseT. |

| | |
|---|---|
| | – Zainstalowana dwuportowa karta sieciowa 10 Gbit/s SFP+ wraz z wkładkami LC MM. Wkładki muszą występować na liście kompatybilności oferowanej karty sieciowej.<br>– Dedykowany port 1Gb RJ45 dla karty zarządzającej. |
| **Karta graficzna** | Zintegrowana karta graficzna |
| **Porty** | – VGA na tylnym panelu.<br>– Złącza USB: min. 4 portów USB 3.2 Gen1 w tym 1 szt. wewnątrz obudowy oraz 2 porty z tyłu serwera. Dodatkowy port USB z przodu obudowy umożliwiający przejęcie konsoli karty zdalnego zarządzania.<br>Możliwość rozbudowy/rekonfiguracji o:<br>- 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 |
| **Napęd DVD** | – Możliwość rozbudowy o fabrycznie wewnętrzny napęd DVD-ROM lub DVD-RW. |
| **Zasilacze, chłodzenie** | – Redundantne zasilacze typu hot plug o sprawności 96% (tzw. klasa Titanium) i mocy min. 800W każdy.<br>– Zestaw min. 3 szt. wentylatorów. |
| **Karta /moduł zarządzający** | Niezależna od system operacyjnego, zintegrowana z płytą główną serwera lub jako dodatkowa karta w gnieździe PCI posiadająca funkcjonalności:<br>– monitorowanie podzespołów serwera: temperatura, zasilacze, wentylatory, procesory, pamięć RAM, kontrolery macierzowe dyski(fizyczne i logiczne)<br>– wsparcie dla pracy w trybie bezagentowym – bez agentów zarządzania instalowanych w systemie operacyjnym z<br>– generowaniem alertów SNMP<br>– dostęp do karty zarządzającej poprzez<br>o - dedykowany port RJ45 z tyłu serwera lub przez współdzielony port zintegrowanej karty sieciowej serwera<br>– dostęp do karty możliwy<br>o - z poziomu przeglądarki webowej (GUI)<br>o z poziomu linii komend zgodnie z DMTF System Management Architecture for Server Hardware, Server Management Command Line Protocol (SM CLP)<br>- poprzez interfejs IPMI 2.0 (Intelligent Platform Management Interface)<br>– wbudowane narzędzia diagnostyczne<br>– zdalna konfiguracji serwera(BIOS) i instalacji systemu operacyjnego<br>– 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)<br>– obsługa zdalnego serwera logowania (remote syslog)<br>– wirtualna zdalna konsola, tekstowa i graficzna z dostępem do |

| | |
|---|---|
| | myszy i klawiatury i możliwością podłączenia wirtualnych napędów CD/DVD/FDD w trybie HTML5.<br>– mechanizm przechwytywania, nagrywania i odtwarzania sekwencji video dla ostatniej awarii i ostatniego startu serwera a także nagrywanie na żądanie<br>– monitorowanie zasilania oraz zużycia energii przez serwer w czasie z możliwością graficznej prezentacji<br>– konfiguracja maksymalnego poziomu pobieranej mocy przez serwer (capping)<br>– zdalna aktualizacja oprogramowania (firmware)<br>– zarządzanie grupami serwerów, w tym:<br>o - tworzenie i konfiguracja grup serwerów<br>o - sterowanie zasilaniem (wł/wył)<br>o - ograniczenie poboru mocy dla grupy (powercaping)<br>o - aktualizacja oprogramowania (firmware)<br>o - wspólne wirtualne media dla grupy<br>– możliwość równoczesnej obsługi przez min. 2 administratorów<br>– autentykacja dwuskładnikowa (Kerberos)<br>– wsparcie dla Microsoft Active Directory<br>– obsługa TLS i SSH<br>– możliwość trwałego zablokowania dokonania obniżenia wersji oprogramowania układowego (firmware) serwera<br>– wsparcie dla IPv4 oraz iPv6, obsługa SNMP v3 oraz RESTful API<br>– możliwość autokonfiguracji sieci karty zarządzającej(DNS/DHCP).<br>– Dożywotnią licencję należy dostarczyć z minimum rocznym wsparciem.<br>Dostarczony serwer musi posiadać pełne wsparcie dla funkcjonalności iLOFederation z posiadanymi serwerami HPE przez Zamawiającego. |
| **System monitorowania i analizowania konfiguracji serwerów** | – Dostęp do systemu wymagany jest dla każdego oferowanego serwera. Jeżeli wymaga to dodatkowych licencji, to należy takie licencje dostarczyć.<br>– System musi być w postaci platformy uruchomionej w chmurze i dostępnej jako usługa webowa (z przeglądarki internetowej), system niezależny od infrastruktury IT Zamawiającego. 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.<br>– System musi zapewniać:<br>o - 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.);<br>o - informacje na temat stanu gwarancji serwera – co najmniej czy jest aktywna; |

| | |
|---|---|
| | ○ - prezentację wersji zainstalowanego oprogramowania układowego na poszczególnych komponentach serwera;<br>○ - rekomendacje odnośnie optymalizacji i poprawy wydajności serwerów, przewidywanie oraz zapobieganie problemom;<br>○ - analizę danych pod kątem bezpieczeństwa serwerów np. ostrzeganie użytkownika o nieudanych próbach logowania;<br>○ - prognozy pod kątem awarii poprzez ostrzeganie użytkownika o uszkodzonych komponentach.<br>○ - zalecenia dotyczące eliminacji źródeł/przyczyn problemów wydajnościowych serwerów.<br>Dostarczony serwer musi być w pełni kompatybilny z profilami polityk bezpieczeństwa, zaimplementowanych w oprogramowaniu posiadanym przez zamawiającego tj. „HPE OneView Advanced". Jeżeli funkcjonalność zarządzania profilami serwerów wymaga dodatkowych licencji należy je dostarczyć wraz z serwerem. |
| **Wsparcie dla systemów operacyjnych i systemów wirtualizacyjnych** | – Microsoft Windows Server min. 2019, 2022<br>– Red Hat Enterprise Linux (RHEL) min. 8.x, 9.0<br>– VMware ESXi min. 7, 8<br>– CanonicalUbuntu min. 22.04 LTS<br>Oferowany serwer musi znajdować się na liście VMware HCL dla ESXi 7, 8 oraz na liście Windows Server Catalog i posiadać status „Certified for Windows" dla systemów Microsoft Windows 2019, 2022. |
| **Oprogramowanie dodatkowe** | Oprogramowanie zainstalowane w najnowszej wersji musi być instalowane bezpośrednio na sprzęcie fizycznym:<br>– Zaoferowane oprogramowanie do wirtualizacji musi być instalowane bezpośrednio na sprzęcie fizycznym i nie może być ono częścią innego systemu operacyjnego<br>– W zaoferowanym oprogramowaniu warstwa wirtualizacji nie może dla własnych celów alokować więcej niż 200MB pamięci operacyjnej RAM serwera fizycznego<br>– Zaoferowane oprogramowanie do wirtualizacji zainstalowane na serwerze fizycznym musi potrafić obsłużyć i wykorzystać procesory fizyczne tego serwera wyposażone w 768 logicznych wątków, 16TB pamięci fizycznej RAM tego serwera oraz 16 procesorów fizycznych tego serwera<br>– Zaoferowane oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych z ilością od 1 do 256 procesorów wirtualnych<br>– Zaoferowane oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych z możliwością przydzielenia do 6 TB pamięci operacyjnej RAM<br>– Zaoferowane oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych z możliwością przydzielenia od 1 do 10 wirtualnych kart sieciowych dla każdej z nich. Dodatkowo, oprogramowanie musi posiadać możliwość utworzenia maszyny wirtualnej bez przydzielonej wirtualnej karty |

| | |
|---|---|
| | sieciowej.<br>– Zaoferowane oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych, z których każda może mieć 32 porty szeregowe, 3 porty równoległe i 20 urządzeń USB<br>– Zaoferowane oprogramowanie musi wspierać następujące systemy operacyjne: Windows XP, Windows Vista, Windows 2000, Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows Server 2016, Windows Server 2019, Windows 7, Windows 8, SLES 12, SLES 11, SLES 10, SLES 9, RHEL 8, REHL 7, RHEL 6, RHEL 5, RHEL 4, RHEL 3, RHEL Atomic 7, Solaris 11, Solaris 10, Debian, CentOS, FreeBSD, Asianux, Ubuntu, SCO OpenServer, SCO Unixware, Mac OS X, Photon OS, eCommStation 1/2/2.1, Oracle Linux , CoreOS, NeoKylin, Amazon Linux 2,<br>– W celu osiągnięcia maksymalnego współczynnika konsolidacji, zaoferowane oprogramowanie musi umożliwiać przydzielenie łącznie większej ilości pamięci RAM dla maszyn wirtualnych niż fizyczne zasoby RAM serwera, na którym maszyny te są posadowione<br>– Rozwiązanie musi umożliwiać udostępnienie maszynie wirtualnej większej ilości zasobów dyskowych niż jest fizycznie dostępne na zasobach dyskowych<br>– Zaoferowane oprogramowanie musi zapewniać sprzętowe wsparcie dla wirtualizacji zagnieżdżonej, w szczególności w zakresie możliwości zastosowania trybu XP mode w Microsoft Windows 7 a także instalacji wszystkich funkcjonalności w tym Microsoft Hyper-V pakietu Microsoft Windows Server 2012 na maszynie wirtualnej<br>– Zaoferowane oprogramowanie musi umożliwiać integrację z rozwiązaniami antywirusowymi firm trzecich w zakresie skanowania maszyn wirtualnych z poziomu warstwy wirtualizacji bez ingerencji w systemy operacyjne maszyn wirtualnych (bezagentowość)<br>– Zaoferowane oprogramowanie 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”<br>– Zaoferowane oprogramowanie do wirtualizacji musi zapewnić możliwość powielania maszyn wirtualnych wraz z ich pełną konfiguracją i danymi<br>– Zaoferowane oprogramowanie do wirtualizacji musi zapewnić możliwość wykonywania kopii migawkowych instancji systemów operacyjnych na potrzeby tworzenia kopii zapasowych bez przerywania ich pracy z możliwością konieczności zachowania stanu pamięci pracującej maszyny wirtualnej.<br>– Konsola zarządzająca zaoferowanego oprogramowania musi posiadać możliwość przydzielania i konfiguracji uprawnień z możliwością integracji z usługami katalogowymi, minimalnie z: |

| | |
|---|---|
| | Microsoft Active Directory i Open LDAP oraz umozliwiać federacyjne zarządzanie tożsamością w oparciu o Microsoft Active Directory Federation Services (ADFS).<br>– Zaoferowane oprogramowanie musi zapewniać możliwość dodawania zasobów w czasie pracy maszyny wirtualnej, w szczególności w zakresie ilości procesorów, pamięci operacyjnej i przestrzeni dyskowej<br>– Zaoferowane oprogramowanie musi posiadać funkcjonalność tworzenia wirtualnego przełącznika (virtualswitch) umożliwiającego tworzenie sieci wirtualnej w obszarze hosta (hypervisora wirtualizacyjnego) i pozwalającego połączyć tym przełącznikiem maszyny wirtualne w obszarze jednego hosta, a także na zewnątrz sieci fizycznej. Pojedynczy przełącznik wirtualny powinien mieć możliwość konfiguracji minimum 4000 portów<br>– Pojedynczy wirtualny przełącznik w zaoferowanym oprogramowaniu, w celu zapewnienia bezpieczeństwa połączenia ethernetowego w razie awarii fizycznej karty sieciowej, musi posiadać możliwość przyłączania do niego minimum dwóch fizycznych kart sieciowych<br>– Wirtualne przełączniki w zaoferowane oprogramowaniu muszą posiadać funkcjonalność obsługi wirtualnych sieci lokalnych (VLAN)<br>– Zaoferowane oprogramowanie musi zapewniać możliwość konfigurowania polityk separacji sieci w warstwie trzeciej, tak aby zapewnić oddzielne grupy wzajemnej komunikacji pomiędzy maszynami wirtualnymi<br>– Zaoferowane oprogramowanie musi umożliwiać wykorzystanie technologii przepustowości sieci komputerowych do 100GbE w tym agregację połączeń fizycznych do minimalizacji czasu przenoszenia maszyny wirtualnej pomiędzy serwerami fizycznymi<br>– Zaoferowane oprogramowanie do wirtualizacji musi obsługiwać przełączenie ścieżek LAN (bez utraty komunikacji) w przypadku awarii jednej ze ścieżek<br>– Zaoferowane oprogramowanie musi zapewnić możliwość zdefiniowania alertów informujących o przekroczeniu wartości progowych<br>– Zaoferowane oprogramowanie, w przypadku działania pod zarządcą klastra VMware vCenter, 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. Replikacja musi gwarantować współczynnik RPO (angRecovery Point Objective) na poziomie minimum 5 minut<br>– Zaoferowane oprogramowanie do wirtualizacji musi obsługiwać przełączenie ścieżek SAN (bez utraty komunikacji) w przypadku awarii jednej ze ścieżek<br>– Zaoferowane oprogramowanie, w przypadku działania pod zarządcą klastra VMware vCenter, musi mieć możliwość przenoszenia maszyn wirtualnych pomiędzy serwerami fizycznymi bez przerywania pracy usług na przenoszonych maszynach |

| | |
|---|---|
| | wirtualnych. Wymaga się wsparcia natywnego szyfrowania ruchu sieciowego dla maszyn wirtualnych podczas ich przenoszenia między serwerami fizycznymi<br>– Zaoferowane oprogramowanie, w przypadku działania pod zarządcą klastra VMware vCenter, oraz w środowisku z więcej niż pojedynczym wirtualizatorem, musi umożliwiać automatyczne, ponowne uruchomienie maszyn wirtualnych w przypadku awarii jednego z wirtualizatorów na kolejnym, działającym w tym samym klastrze wirtualizatorze (funkcjonalność HA) (ang. high availability)<br>– Zaoferowane oprogramowanie, w przypadku działania pod zarządcą klastra VMware vCenter w środowisku z minimalnie dwoma wirtualizatorami oraz w przypadku potrzeby wgrania aktualizacji do warstwy wirtualizacji, musi posiadać możliwość w przypadku wywołania startu aktualizacji, automatycznego przeniesienia bezprzerwowego działających maszyn wirtualnych do innego wirtualizatora nie objętego aktualizacją, przed rozpoczęciem samej aktualizacji<br>– Zaoferowane oprogramowanie musi posiadać co najmniej 2 niezależne mechanizmy wzajemnej komunikacji między serwerami z zainstalowanym wirtualizatorem oraz z serwerem zarządzającym, gwarantujące właściwe działanie mechanizmów wysokiej dostępności na wypadek izolacji sieciowej serwerów fizycznych lub partycjonowania sieci<br>– Zaoferowane oprogramowanie, w przypadku działania pod zarządcą klastra VMware vCenter, w środowisku z minimum dwoma wirtualizatorami, musi zapewniać pracę bez przestojów dla wybranych maszyn wirtualnych (o maksymalnie dwóch procesorach wirtualnych), niezależnie od systemu operacyjnego oraz aplikacji, podczas awarii wirtualizatora, bez utraty danych i dostępności danych na maszynach wirtualnych objętych ochroną<br>– Zaoferowane oprogramowanie do wirtualizacji musi zapewniać możliwość stworzenia dysku maszyny wirtualnej o wielkości 62 TB<br>– Zaoferowane oprogramowanie musi posiadać wbudowany interfejs programistyczny (API) zapewniający pełną integrację zewnętrznych rozwiązań wykonywania kopii zapasowych z istniejącymi mechanizmami warstwy wirtualizacyjnej<br>– Producent zaoferowanego oprogramowania do wirtualizacji musi wspierać rozwiązania do automatyzacji procesów oraz wirtualizacji sieci (SDN, ang. software defined network).<br>– Zaoferowane oprogramowanie musi wspierać mechanizmy zaawansowanego uwierzytelniania do systemu operacyjnego wirtualnej maszyny za pomocą technologii Smart Card Reader<br>– Zaoferowane oprogramowanie musi wspierać TPM 2.0. Minimalne wymaganie Zamawiającego dla TPM oznacza, że TPM zapewnia mechanizm gwarantujący, że serwer fizyczny, na którym zainstalowane jest zaoferowane oprogramowanie, uruchomił się z włączoną opcją Secure Boot. Po potwierdzeniu, że Secure Boot jest włączone, system gwarantuje, poprzez weryfikację podpisu cyfrowego, że hypervisor uruchomił się w niezmienionej formie |

| | |
|---|---|
| | – Wirtualizator w zaoferowanym oprogramowaniu musi mieć możliwość włączenia funkcji “Microsoft virtualization-basedsecurity”, tzw. Microsoft VBS dla systemów operacyjnych maszyn wirtualnych opartych o system operacyjny Microsoft Windows 10 oraz Microsoft Windows Server 2016.<br>– Zaoferowane oprogramowanie musi posiadać certyfikację FIPS-140-2 min. dla modułu jądra wirtualizatora odpowiedzialnego za szyfrowanie danych<br>– Zaoferowane oprogramowanie musi posiadać funkcjonalność wirtualnego TPM 2.0 dla maszyn wirtualnych z zainstalowanym Microsoft Windows 10 oraz Microsoft Windows 2016. Zamawiający wymaga aby z punktu widzenia maszyny wirtualnej z systemem operacyjnym Microsoft Windows 10 lub Microsoft Windows 2016 wirtualny TPM widziany był jako standardowy TPM, gdzie można przechowywać bezpiecznie wrażliwe dane np. certyfikaty. Zawartość wirtualnego TPM musi być przechowywana w pliku przynależnym do maszyny wirtualnej oraz musi być szyfrowana.<br>– Zaoferowane oprogramowanie musi posiadać funkcjonalność szybkiego uruchamiania wirtualizatora po przeprowadzonym procesie jego aktualizacji. Zamawiający wymaga aby w procesie aktualizacji wirtualizatora, jeśli wymagany jest jego restart, funkcjonalność szybkiego uruchamiania powodowała eliminację czasochłonnej fazy inicjalizacji serwera fizycznego<br>– Zaoferowane oprogramowanie musi posiadać możliwość aktualizacji i kontroli wersji oprogramowania do wirtualizacji w ramach klastra serwerów z poziomu centralnej konsoli zarządzającej. Dodatkowo centralna konsola zarządzająca musi posiadać funkcjonalność aktualizacji firmware komponentów serwera fizycznego (dyski, kontrolery, karty sieciowe) z poziomu konsoli zarządzającej wirtualizatora. Konsola zarządzająca musi mieć możliwość automatycznej weryfikacji, czy zainstalowane komponenty serwera posiadają rekomendowaną wersję sterowników i firmware, eliminując ryzyko pracy na nieaktualnych wersjach. Taka funkcjonalność powinna być dostępna dla minimum dwóch producentów serwerów obecnych na rynku<br>– Zaoferowane oprogramowanie musi posiadać wsparcie dla natywnych dysków 4K<br>– Zaoferowane oprogramowanie musi wspierać protokół precyzyjnej synchronizacji czasu PTP (ang. Precision Time Protocol)<br>– Zaoferowane oprogramowanie, w przypadku działania pod zarządcą klastra VMware vCenter, 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.<br>– Zaoferowane oprogramowanie musi mieć funkcjonalność migracji w trybie rzeczywistym dysków działających maszyn wirtualnych z jednego podsystemu dyskowego do innego bez konieczności |

| | |
|---|---|
| | przerywania pracy maszyny wirtualnej, której dysk jest migrowany.<br>– Zaoferowane oprogramowanie musi być w pełni kompatybilne z posiadanym przez Zamawiającego oprogramowaniem VMware vCenter w wersji min. 8.0.<br>Dostarczone w ramach postępowania oprogramowanie w formie licencji wieczystej i objęte min. 36 miesięcznym okresem gwarancji i wsparcia w trybie 7x24. |
| **Oprogramowanie systemowe** | – Licencja na serwerowy system operacyjny musi być przypisana do każdego rdzenia procesora fizycznego na serwerze. Licencja musi uprawniać do uruchamiania serwerowego systemu operacyjnego w środowisku fizycznym i 2 wirtualnych środowisk serwerowego systemu operacyjnego za pomocą wbudowanych mechanizmów wirtualizacji. Dodatkowo musi pozwalać na uruchamianie wirtualnych środowisk serwerowego systemu operacyjnego w usłudze hostowanej platformy producenta serwerowego systemu operacyjnego.<br>– Serwerowy system operacyjny musi posiadać następujące, wbudowane cechy.<br>– Możliwość wykorzystania 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym.<br>– Możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności do 64TB przez każdy wirtualny serwerowy system operacyjny.<br>– Możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania 7000 maszyn wirtualnych.<br>– 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.<br>– Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy.<br>– Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy.<br>– Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.<br>– Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading.<br>– Wbudowane wsparcie instalacji i pracy na wolumenach, które:<br>o pozwalają na zmianę rozmiaru w czasie pracy systemu,<br>o umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,<br>o umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów,<br>o umożliwiają zdefiniowanie list kontroli dostępu (ACL). |

| | |
|---|---|
| | ○ Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.<br>– Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.<br>– Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET<br>– Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.<br>– Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.<br>– Dostępne dwa rodzaje graficznego interfejsu użytkownika:<br>– Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,<br>– Dotykowy umożliwiający sterowanie dotykiem na monitorach dotykowych.<br>– Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe,<br>– Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji.<br>– Mechanizmy logowania w oparciu o:<br>– Login i hasło,<br>– Karty z certyfikatami (smartcard),<br>– Wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM),<br>– Możliwość wymuszania wieloelementowej dynamicznej kontroli dostępu dla: określonych grup użytkowników, zastosowanej klasyfikacji danych, centralnych polityk dostępu w sieci, centralnych polityk audytowych oraz narzuconych dla grup użytkowników praw do wykorzystywania szyfrowanych danych.<br>– Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).<br>– Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.<br>– Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa.<br>– Pochodzący od producenta systemu serwis zarządzania polityką dostępu do informacji w dokumentach (Digital Rights Management).<br>– Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach.<br>– Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji: |

| | |
|---|---|
| | – Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC,<br>– 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:<br>– Podłączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną,<br>– Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,<br>– Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza.<br>– Bezpieczny mechanizm dołączania do domeny uprawnionych użytkowników prywatnych urządzeń mobilnych opartych o iOS i Windows 8.1.<br>– Zdalna dystrybucja oprogramowania na stacje robocze.<br>– Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej<br>– Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:<br>– Dystrybucję certyfikatów poprzez http<br>– Konsolidację CA dla wielu lasów domeny,<br>– Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen,<br>– Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509.<br>– Szyfrowanie plików i folderów.<br>– Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec).<br>– Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów.<br>– Serwis udostępniania stron WWW.<br>– Wsparcie dla protokołu IP w wersji 6 (IPv6),<br>– Wsparcie dla algorytmów Suite B (RFC 4869),<br>– Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows,<br>– Wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie do 1000 aktywnych środowisk wirtualnych systemów operacyjnych. Wirtualne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności. Mechanizmy wirtualizacji mają zapewnić wsparcie dla:<br>○ Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych, |

| | |
|---|---|
| | ○ Obsługi ramek typu jumbo frames dla maszyn wirtualnych.<br>○ Obsługi 4-KB sektorów dysków<br>○ Nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra<br>○ Możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API.<br>○ Możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk mode)<br>○ Możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta serwerowego systemu operacyjnego umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet.<br>○ Wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath).<br>○ Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego.<br>○ Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.<br>○ Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF.<br>○ Wymagana najnowsza dostępna wersja oprogramowania dostępna na dzień publikacji postepowania. |
| **Certyfikaty** | – Serwer musi być wyprodukowany zgodnie z normą ISO-9001 oraz ISO-14001.<br>– Serwer musi posiadać deklaracje CE lub równoważną. |
| **Kable i akcesoria** | – 2 kable zasilające z wtyczką C13-C14, min. 2m<br>– 2 kable światłowodowe LC-LC multi-mode, min. 2m |
| **Gwarancja producenta** | – Dostarczony w ramach zapytania sprzęt objęty min. 60 miesięcznym okresem gwarancji producenta, wraz z usługą serwisu gwarancyjnego świadczoną w miejscu instalacji przez inżyniera z czasem reakcji w następnym dniu rocznym (NBD).<br>– Uszkodzone nośniki danych pozostają własnością Zamawiającego.<br>– W okresie gwarancji Zamawiający ma prawo do otrzymywania poprawek oraz aktualizacji wersji oprogramowania dostarczonego wraz z urządzeniem oraz oprogramowania wewnętrznego urządzenia.<br>– Urządzenia muszą być fabrycznie nowe, pochodzić z autoryzowanego kanału sprzedaży producenta i reprezentować model bieżącej linii produkcyjnej. Nie dopuszcza się urządzeń: odnawianych, demonstracyjnych lub powystawowych.<br>– Nie dopuszcza się urządzeń posiadających wadę prawną w zakresie pochodzenia sprzętu, wsparcia technicznego i gwarancji producenta. |

| | |
|---|---|
| | – Elementy, z których zbudowane są urządzenia muszą być produktami producenta urządzeń lub być przez niego certyfikowane oraz całe muszą być objęte gwarancją producenta.<br>– Urządzenia i ich komponenty muszą być oznakowane w taki sposób, aby możliwa była identyfikacja zarówno produktu jak i producenta.<br>– Urządzenia muszą być dostarczone Zamawiającemu w oryginalnych opakowaniach producenta.<br>– Do każdego urządzenia musi być dostarczony komplet standardowej dokumentacji w dla użytkownika w języku polskim lub angielskim w formie papierowej lub elektronicznej.<br>– Gwarancja i serwis na urządzenia musi być świadczony przez firmę autoryzowaną przez producenta lub jego przedstawicielstwo w Polsce w przypadku gdy Oferent nie posiada takiej autoryzacji.<br>– Urządzenie na etapie dostawy producent a Zamawiający nie mogą podlegać modyfikacjom.<br>– Pakiet serwisowy (gwarancja) musi być składnikiem sprzętu i musi być przypisany na etapie jego produkcji bez konieczności późniejszego aktywowania, rejestrowania lub innych działań.<br>– Zamawiający wymaga możliwości sprawdzenia statusu gwarancji i pokazania szczegółowej konfiguracji oferowanego sprzętu na stronie producenta, po podaniu jego numeru seryjnego.<br>– Na min. 3dni przed dostawą sprzętu należy przesłać Zamawiającemu wykaz numerów seryjnych oferowanych urządzeń celem weryfikacji u ich producenta spełnienia w/w wymagań.<br>– Zamawiający wymaga pojedynczego punkt wsparcia serwisowego dla wszystkich serwerów dostarczonych w ramach postępowania.<br>– Wymagane jest pisemne oświadczenie producenta potwierdzające realizacje wymaganego poziomu serwisu. |