**(nazwa i adres Wykonawcy)**

Dostawa **serwerów wraz z oprogramowaniem do wirtualizacji serwerów oraz dostawa i wdrożenie macierzy dyskowej do Głównego Inspektoratu Jakości Handlowej Artykułów Rolno-Spożywczych, (nr sprawy GI-BAD-231-6/20)** do Głównego Inspektoratu Jakości Handlowej Artykułów Rolno-Spożywczych  
ul. Wspólna 30, 00-930 Warszawa.

**Serwer – 3 sztuki**

Producent (marka)

model     

**Oprogramowanie na 6 procesorów**

Producent (marka)      

model     

**Macierz – 1 sztuka**

Producent (marka)      

model

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Lp.** | **Opis parametrów** | | **Wymagane parametry techniczne** | |
| ***1*** | ***2*** | | ***3*** | |
|  | **Serwer wraz z oprogramowaniem** | |  | |
|  | Obudowa Rack o wysokości maksymalnej 1U z możliwością instalacji co najmniej 10 dysków 2.5" Hot-Plug, kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych.  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 (Android/ Apple iOS) przy użyciu jednego z protokołów BLE/ WIFI.  **Zamawiający dopuszcza zamiast obudowy wyposażonej w kartę umożliwiającą dostęp bezpośredni poprzez urządzenia mobilne, dostarczenie oprogramowania zarządzającego dołączonego do serwera, a umożliwiającego zarządzanie serwerem poprzez aplikację mobilną udostępnioną przez producenta serwera, którą można zainstalować na urządzeniach mobilnych z systemem operacyjnym Android lub iOS.** | | wymagane | |
|  | Płyta główna z możliwością zainstalowania minimum dwóch procesorów. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym. Chipset dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych. Zainstalowany moduł Trusted Platform Module 2.0. | | wymagane | |
|  | Dwa zainstalowane procesory. | | wymagane | |
|  | Każdy procesor minimum dziesięcio-rdzeniowy klasy x86 do pracy z zaoferowanym serwerem umożliwiające osiągnięcie wyniku minimum 120 punktów w teście SPECrate2017\_int\_base dostępnym na stronie www.spec.org dla dwóch procesorów. | | wymagane | |
|  | Zainstalowany moduł dedykowany dla hypervisora wirtualizacyjnego, wyposażony w co najmniej w dwa nośniki typu flash o pojemności minimum 32GB z możliwoscią konfiguracji zabezpieczenia synchronizacji pomiędzy nośnikami z poziomu BIOS serwera, rozwiązanie nie może powodować zmiejszenia ilości wnęk na dyski twarde. Pamięć flash musi pochodzić bezpośrednio od producenta serwera.  Możliwość instalacji co najmniej dwóch dysków M.2 SATA o pojemności minimum 480GB z możliością konfiguracji RAID 1. | | wymagane | |
|  | Pojemność zainstalowanej pamięci typu RAM  192GB DDR4 RDIMM 2933MT/s | | wymagane | |
|  | Na płycie głównej powinny znajdować się co najmniej 24 sloty przeznaczonych do instalacji pamięci. Płyta główna powinna obsługiwać co najmniej 3TB pamięci RAM. | | wymagane | |
|  | Zabezpieczenia pamięci RAM - Memory Rank Sparing, Memory Mirror | | wymagane | |
|  | Karta graficzna - zintegrowana umożliwiająca wyświetlenie rozdzielczości co najmniej 1600x900 | | wymagane | |
|  | Wbudowane co najmniej dwa interfejsy sieciowe 1Gb Ethernet w standardzie BaseT oraz w co najmniej dwa interfejsy sieciowe 10Gb Ethernet ze złączami w standardzie BaseT.  Możliwość instalacji wymiennie modułów udostępniających:  - dwa interfejsy sieciowe 1Gb Ethernet w standardzie BaseT oraz dwa interfejsy sieciowe 10Gb Ethernet ze złączami w standardzie SFP+,  - cztery interfejsy sieciowe 10Gb Ethernet w standardzie BaseT,  - cztery interfejsy sieciowe 1Gb Ethernet w standardzie BaseT,  - cztery interfejsy sieciowe 10Gb Ethernet w standardzie SFP+,  - dwa interfejsy sieciowe 25Gb Ethernet ze złączami SFP28.  Dodatkowo zainstalowana co najmniej jedna karta czteroportowa 1 Gb Ethernet ze złączami BaseT. | | wymagane | |
|  | Karta niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port RJ-45 Gigabit Ethernet umożliwiająca:  - zdalny dostęp do graficznego interfejsu Web karty zarządzającej,  - szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika,  - możliwość podmontowania zdalnych wirtualnych napędów,  - wirtualną konsolę z dostępem do myszy, klawiatury,  - wsparcie dla Ipv6,  - wsparcie dla SNMP; IPMI2.0, VLAN tagging, SSH,  - możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer, dane historyczne powinny być dostępne przez 7 dni wstecz,  - możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer,  - integracja z Active Directory,  - możliwość obsługi przez ośmiu administratorów jednocześnie,  - wsparcie dla automatycznej rejestracji DNS,  - wsparcie dla LLDP,  - wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej,  - możliwość podłączenia lokalnego poprzez złącze RS-232,  - możliwość zarządzania bezpośredniego poprzez złącze microUSB umieszczone na froncie obudowy,  - monitorowanie zużycia dysków SSD,  - możliwość monitorowania z jednej konsoli co najmniej 100 serwerami fizycznymi,  - automatyczne zgłaszanie alertów do centrum serwisowego producenta,  - automatyczne update firmware dla wszystkich komponentów serwera,  - możliwość przywrócenia poprzednich wersji firmware,  - możliwość eksportu/importu konfiguracji (ustawienie karty zarządzającej, BIOSu, kart sieciowych, HBA oraz konfiguracji kontrolera RAID) serwera do pliku XML lub JSON,  - możliwość zaimportowania ustawień, poprzez bezpośrednie podłączenie plików konfiguracyjnych,  - automatyczne tworzenie kopii ustawień serwera w opraciu o harmonogram.  Dodatkowe oprogramowanie umożliwiające zarządzanie poprzez sieć, spełniające wymagania:  - 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 opraciu o wszystkie informacje zawarte w inwentarzu,  - grupowanie urządzeń w oparciu o kryteria użytkownika,  - tworzenie automatycznie grup urządzeń w opraciu o dowolny element konfiguracji serwera np. Nazwa, lokalizacja, system operacyjny, obsadzenie slotów PCIe, pozostałego czasu gwarancji,  - możliwość uruchamiania narzędzi zarządzających w poszczególnych urządzeniach,  - szybki podgląd stanu środowiska,  - podsumowanie stanu dla każdego urządzenia,  - szczegółowy status urządzenia/elementu/komponentu,  - generowanie alertów przy zmianie stanu urządzenia,  - filtry raportów umożliwiające podgląd najważniejszych zdarzeń,  - integracja z service desk producenta dostarczonej platformy sprzętowej,  - możliwość przejęcia zdalnego pulpitu,  - możliwość podmontowania wirtualnego napędu,  - kreator umożliwiający dostosowanie akcji dla wybranych alertów,  - możliwość importu plików MIB,  - przesyłanie alertów „as-is” do innych konsol firm trzecich,  - możliwość definiowania ról administratorów,  - możliwość zdalnej aktualizacji oprogramowania wewnętrznego serwerów,  - aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania),  - możliwość instalacji oprogramowania wewnętrznego bez potrzeby instalacji agenta,  - możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów,  - moduł raportujący pozwalający na wygenerowanie następujących informacji: nr seryjne sprzętu, konfiguracja poszczególnych urządzeń, wersje oprogramowania wewnętrznego, obsadzenie slotów PCI i gniazd pamięci, informację o maszynach wirtualnych, aktualne informacje o stanie i poziomie gwarancji, adresy IP kart sieciowych, występujących aletrów, MAC adresów kart sieciowych, stanie poszczególnych komponentów serwera,  - możliwość tworzenia sprzętowej konfiguracji bazowej i na jej podstwie weryfikacji środowiska w celu wykrycia rozbieżności,  - wdrażanie serwerów, rozwiązań modularnych oraz przełączników sieciowych w opraciu o profile,  - możliwość migracji ustawień serwera wraz z wirtualnymi adresami sieciowymi (MAC, WWN, IQN) między urządzeniami,  - zainstalowana karta Flash co najmniej 16GB,  - 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 zarzadzającym,  - oprogramowanie dostarczane jako wirtualny appliance dla KVM, ESXi i Hyper-V | | wymagane | |
|  | Minimum trzy sloty PCIe x16 generacji 3. | | wymagane | |
|  | Wspierane systemy operacyjne - Canonical Ubuntu LTS, Citrix XenServer, Microsoft Windows Server with Hyper-V, Red Hat Enterprise Linux, SUSE Linux Enterprise Server, VMware ESXi | | wymagane | |
|  | Napięcie zasilania 230V 50/60Hz | | wymagane | |
|  | Co najmniej 2 zasilacze Hot-Plug maksymalnie 750W. | | wymagane | |
|  | Co najmniej 2 porty USB 2.0 oraz 2 porty USB 3.0, 1 port VGA,1 port RS232. | | wymagane | |
|  | - redundantne wentylatory,  - wbudowany czujnik otwarcia obudowy,  - dokumentacja w języku polskim lub angielskim,  - możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela,  - wsparcie dla funkcjonalności vSphere Quick Boot | | wymagane | |
|  | Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2008 oraz ISO-14001. Serwer musi posiadać deklaracja CE.  Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Microsoft Windows 2012, Microsoft Windows 2012 R2 x64, Microsoft Windows 2016, Microsoft Windows 2019 x64. | | wymagane | |
|  | **Gwarancja -**  Minimum 36 miesięcy gwarancji podstawowej producenta realizowanej w miejscu instalacji sprzętu, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania w trybie 365x7x24 awarii poprzez ogólnopolską linię telefoniczną producenta. Gwarancja producenta musi obejmować sprzęt jak i oprogramowanie do wirtualizacji. | | należy podać | |
|  | **Oprogramowanie do wirtualizacji** | |  | |
|  | Oferowana warstwa wirtualizacji musi być rozwiązaniem systemowym tzn. musi być zainstalowana bezpośrednio na sprzęcie fizycznym, nie może być częścią innego systemu operacyjnego. | | wymagane | |
|  | Warstwa wirtualizacji nie może dla własnych celów alokować więcej niż 200MB pamięci operacyjnej RAM serwera fizycznego. | | wymagane | |
|  | Oprogramowanie do wirtualizacji zainstalowane na serwerze fizycznym musi potrafić obsłużyć i wykorzystać procesory fizyczne wyposażone w co najmniej 576 logicznych wątków oraz do co najmniej 12TB pamięci fizycznej RAM. | | wymagane | |
|  | Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych co najmniej 1-128 procesorowych. | | wymagane | |
|  | Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych z możliwością przydzielenia co najmniej 6 TB pamięci operacyjnej RAM. | | wymagane | |
|  | Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych, z których każda może mieć co najmniej 1-10 wirtualnych kart sieciowych. | | wymagane | |
|  | Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych, z których każda może mieć co najmniej 32 porty szeregowe, 3 porty równoległe i 20 urządzeń USB. | | wymagane | |
|  | Rozwiązanie musi wspierać następujące systemy operacyjne: MS-DOS 6.22, Windows XP, Windows Vista, Windows 2000, Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows Server 2016, Windows 7, Windows 8, SLES 12, SLES 11, SLES 10, SLES 9, SLES 8, REHL 7, RHEL 6, RHEL 5, RHEL 4, RHEL 3, REHL Atomic 7, Solaris 11 ,Solaris 10, Solaris 9, Solaris 8, OS/2 Warp 4.0, Debian, CentOS, FreeBSD, Asianux, Mandriva, Ubuntu, SCO OpenServer, SCO Unixware, Mac OS X, Photon OS, eCommStation 1/2/2.1, Oracle Linux , CoreOS, NeoKylin. | | wymagane | |
|  | Rozwiązanie musi umożliwiać przydzielenie większej ilości pamięci RAM dla maszyn wirtualnych niż fizyczne zasoby RAM serwera w celu osiągnięcia maksymalnego współczynnika konsolidacji. | | wymagane | |
|  | Rozwiązanie musi umożliwiać udostępnienie maszynie wirtualnej większej ilości zasobów dyskowych niż jest fizycznie zarezerwowane na zasobach dyskowych. | | wymagane | |
|  | Rozwiązanie musi zapewniać sprzętowe wsparcie dla wirtualizacji zagnieżdżonej, w szczególności w zakresie możliwości zastosowania trybu XP mode w Windows 7 a także instalacji wszystkich funkcjonalności w tym Hyper-V pakietu Windows Server 2012 na maszynie wirtualnej. | | wymagane | |
|  | Rozwiązanie musi umożliwiać integrację z rozwiązaniami antywirusowymi firm trzecich w zakresie skanowania maszyn wirtualnych z poziomu warstwy wirtualizacji. | | wymagane | |
|  | 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. | | wymagane | |
|  | Oprogramowanie do wirtualizacji musi zapewnić możliwość klonowania systemów operacyjnych wraz z ich pełną konfiguracją i danymi. | | wymagane | |
|  | 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. | | wymagane | |
|  | Oprogramowanie zarządzające musi posiadać możliwość przydzielania i konfiguracji uprawnień z możliwością integracji z usługami katalogowymi, w szczególności: Microsoft Active Directory i Open LDAP. | | wymagane | |
|  | Rozwiązanie musi zapewniać możliwość dodawania zasobów w czasie pracy maszyny wirtualnej, w szczególności w zakresie ilości procesorów, pamięci operacyjnej i przestrzeni dyskowej. | | wymagane | |
|  | System 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 co najmniej 4000 portów. | | wymagane | |
|  | 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. | | wymagane | |
|  | Wirtualne przełączniki musza obsługiwać wirtualne sieci lokalne (VLAN). | | wymagane | |
|  | Rozwiązanie musi zapewniać możliwość konfigurowania polityk separacji sieci w warstwie trzeciej, tak aby zapewnić oddzielne grupy wzajemnej komunikacji pomiędzy maszynami wirtualnymi. | | wymagane | |
|  | Rozwiązanie musi umożliwiać wykorzystanie technologii 10GbE w tym agregację połączeń fizycznych do minimalizacji czasu przenoszenia maszyny wirtualnej pomiędzy serwerami fizycznymi. | | wymagane | |
|  | Oprogramowanie do wirtualizacji musi obsługiwać przełączenie ścieżek LAN (bez utraty komunikacji) w przypadku awarii jednej ze ścieżek. | | wymagane | |
|  | Rozwiązanie musi zapewnić możliwość zdefiniowania alertów informujących o przekroczeniu wartości progowych. | | wymagane | |
|  | 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. | | wymagane | |
|  | Rozwiązanie replikujące musi gwarantować współczynnik RPO na poziomie minimum 5 minut. | | wymagane | |
|  | 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. | | wymagane | |
|  | 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. | | wymagane | |
|  | 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. | | wymagane | |
|  | Rozwiązanie musi umożliwiać łatwe i szybkie ponowne uruchomienie systemów/usług w przypadku awarii poszczególnych elementów infrastruktury bez utraty danych. | | wymagane | |
|  | Rozwiązanie musi zapewnić bezpieczeństwo danych mimo poważnego uszkodzenia lub utraty sprzętu lub oprogramowania. | | wymagane | |
|  | Rozwiązanie musi zapewniać mechanizm bezpiecznego, bezprzerwowego i automatycznego uaktualniania warstwy wirtualizacyjnej wliczając w to zarówno poprawki bezpieczeństwa jaki zmianę jej wersji bez potrzeby wyłączania wirtualnych maszyn. | | wymagane | |
|  | 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. | | wymagane | |
|  | 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. | | wymagane | |
|  | 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. | | wymagane | |
|  | Oprogramowanie do wirtualizacji musi obsługiwać przełączenie ścieżek SAN (bez utraty komunikacji) w przypadku awarii jednej ze ścieżek. | | wymagane | |
|  | Oprogramowanie do wirtualizacji musi zapewniać możliwość stworzenia dysku maszyny wirtualnej o wielkości co najmniej 62 TB. | | wymagane | |
|  | Rozwiązanie musi posiadać wbudowany interfejs programistyczny (API) zapewniający pełną integrację zewnętrznych rozwiązań wykonywania kopii zapasowych z istniejącymi mechanizmami warstwy wirtualizacyjnej. | | wymagane | |
|  | Rozwiązanie musi umożliwiać konfiguracje HA dla każdego swojego komponentu w celu unikania awarii pojedynczego elementu. | | wymagane | |
|  | 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). | | wymagane | |
|  | System musi wspierać mechanizmy zaawansowanego uwierzytelniania do systemu operacyjnego wirtualnej maszyny za pomocą technologii Smart Card Reader. | | wymagane | |
|  | Wirtualizator musi wspierać TPM 2.0 oznacza to, 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 się w prawidłowej, niezmienionej formie poprzez weryfikację podpisu cyfrowego. | | wymagane | |
|  | Wirtualizator musi mieć możliwość włączenia funkcji „Microsoft virtualization-based security”, tzw. Microsoft VBS dla systemów operacyjnych maszyn wirtualnych opatrych o system operacyjny Windows 10 oraz Windows Server 2016. | | wymagane | |
|  | System musi posiadać certyfikację FIPS-140-2 minimum dla modułu jądra wirtualizatora odpowiedzialnego za szyfrowanie danych. | | wymagane | |
|  | Wirtualizator musi posiadać funkcjonalność wirtualnego TPM 2.0 dla maszyn wirtualnych Windows 10 oraz Windows 2016. Oznacza to, że z punktu widzenia maszyny wirtualnej z systemem operacyjnym Windows 10 lub Windows 2016 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 wyłączania 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 odpowiedziany za szyfrowanie ma dostęp do kluczy szyfrujących oraz może zarządzać procesem szyfrowania w obrębie wirtualizoatora. | | wymagane | |
|  | Wirtualizatora 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 skrócenie czasu wymaganego do ponownego uruchomienia serwera fizycznego podczas operacji aktualizacji. | | wymagane | |
|  | Dostarczone oprogramowanie musi zapewniać możliwość wirtualizacji (zgodnej z licencją) dla wszystkich dostarczonych w ramach postępowania serwerów. | | wymagane | |
|  | Rozwiązanie musi posiadać wsparcie dla natywnych dysków 4K. | | wymagane | |
|  | 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. | | wymagane | |
|  | Wsparcie techniczne - minimum 12 miesięcy | | należy podać | |
|  | **Cechy Macierzy** |  | |  |
|  | Macierz musi być przeznaczona do instalacji w standardowej szafie rack 19” i może zajmować maksymalnie 2U. | wymagane | |  |
|  | Macierz musi zostać dostarczona w konfiguracji:  - posiadającej minimum 6 dysków Hot-Plug 960GB SSD SAS 12Gb/s i 6 dysków Hot-Plug 4TB NearLine SAS 12Gb/s 7.2k,  - umożliwiającej instalację minimum 12 dysków 3.5”,  - zapewniającej możliwość instalacji dysków SAS minimum - 900GB, 1.2TB, 2.4TB,  - zapewniającej możliwość instalacji dysków NLSAS minimum - 4TB, 8TB,12TB,  - zapewniającej możliwość instalacji dysków SSD SAS minimum - 960GB, 1.92TB, 3.84TB,  - zapewniającej możliwość rozbudowy przez dodawanie kolejnych dysków lub półek dyskowych do łącznie minimum 264 dysków,  - zapewniającej możliwość mieszania typów dysków w obrębie macierzy oraz pojedynczej półki. | wymagane | |  |
|  | - dwa kontrolery wyposażone w przynajmniej 8 GB cache każdy,  - kontrolery muszą działać w układzie active-active,  - w przypadku awarii zasilania dane nie zapisane na dyski, powinny być przechowywane w pamięci cache zabezpieczonej za pomocą podtrzymania bateryjnego przez minimum 72 godziny,  - pamięć cache zapisu musi być mirrorowana pomiędzy kontrolerami,  - obsługa następujących poziomów RAID - 0, 1, 5, 5, 6, 10, 50. | wymagane | |  |
|  | Oferowana macierz musi posiadać minimum 8 portów iSCSI 1/10 Gb/s BaseT. | wymagane | |  |
|  | - zarządzanie macierzą poprzez co najmniej przeglądarkę internetową, interfejs graficzny oparty o HTML5,  - powiadamianie mailem o awarii, umożliwiające maskowanie i mapowanie dysków,  - macierz musi zostać dostarczona z licencją umożliwiającą utworzenie minimum 512 LUN’ów oraz 1024 kopii migawkowych na całą macierz,  - licencja zaoferowanej macierzy powinna umożliwiać podłączanie minimum 8 hostów bez konieczności zakupu dodatkowych licencji,  - automatyczne, bez interwencji człowieka, rozkładania danych między dyskami poszczególnych typów (tzw. auto-tiering).  - dane muszą być automatycznie przemieszczane między rożnymi typami dysków,  - możliwość wykorzystania dysków SSD jako cache macierzy, możliwość rozbudowy pamięci cache do min. 4TB poprzez dyski SSD,  - funkcjonalność zdalnej replikacji danych do macierzy tej samej rodziny w trybie asynchronicznym, licencje należy dostarczyć wraz z macierzą | wymagane | |  |
|  | Windows Server 2012 R2, Windows Server 2016, Windows Server 2019, Red Hat Enterprise Linux (RHEL), SLES, Vmware ESXi. | wymagane | |  |
|  | - Zamawiający wymaga dokumentacji w języku polskim lub angielskim,  - macierz musi być wyprodukowana zgodnie z normą ISO 9001:2008,  - zasilacze i wentylatory muszą być redundantne. | wymagane | |  |
|  | **Gwarancja -**  36 miesięcy gwarancji podstawowej producenta realizowanej w miejscu instalacji sprzętu, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania w trybie 365x7x24 awarii poprzez ogólnopolską linię telefoniczną producenta. | należy podać | |  |

**Przyjmujemy do wiadomości, że niewypełnienie pozycji określonych w kolumnie 3 (parametry techniczne oferowane) spowoduje odrzucenie oferty, o ile z treści innych dokumentów stanowiących załączniki do oferty nie będzie wynikało, iż oferowany sprzęt spełnia wymagania określone w ww. tabeli.**

data podpisania formularza

(pieczęć imienna i podpis/kwalifikowany podpis elektroniczny Wykonawcy lub osoby/osób upoważnionej /ych do reprezentowania Wykonawcy)