

OPIS PRZEDMIOTU ZAMÓWIENIA

Przedmiotem zamówienia jest dostawa serwerów wraz z instalacją, konfiguracją i szkoleniem.

Sprzęt wchodzący w zakres dostawy musi być fabrycznie nowy, nieużywany i skalibrowany. Sprzęt musi zostać dostarczony Zamawiającemu w opakowaniu zabezpieczającym przed uszkodzeniem w czasie transportu.

SERWER - Typ I

Wymagane parametry	
Obudowa	Obudowa Rack o wysokości max. 1U umożliwiającą instalację min. 8 dysków 2,5" z kompletem wysuwanych szyn umożliwiającą montaż w szafie rack i wysuwanie serwera do celów serwisowych wraz z organizerem do kabli umożliwiającą montaż w szafie rack. Obudowa z możliwością wyposażenia w kartę umożliwiającą dostęp bezpośredni poprzez urządzenia mobilne - serwer musi posiadać możliwość konfiguracji oraz monitoringu najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej min. (Android i Apple iOS) przy użyciu jednego z protokołów BLE lub WIFI.
Płyta główna	Płyta główna z możliwością zainstalowania minimum dwóch procesorów
Chipset	Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych
Procesor	Zainstalowane dwa procesory min. szesnasto-rdzeniowe klasy x86 do pracy z zaoferowanym serwerem umożliwiające osiągnięcie wyniku min. 173 punktów w teście SPECrate2017_int_base dostępnym na stronie www.spec.org dla dwóch procesorów. Procesory muszą sprzętowo wspierać wirtualizację.
RAM	Min. 512GB DDR4 RDIMM 3200MT/s, na płycie głównej powinno znajdować się minimum 24 slotów przeznaczonych do instalacji pamięci. Płyta główna powinna obsługiwać do 3TB pamięci RAM.
Zabezpieczenia pamięci RAM	Memory Rank Sparing, Memory Mirror
Gniazda PCI	- minimum trzy sloty PCIe x16 generacji 3.
Interfejsy sieciowe/FC/SAS	Wbudowane cztery interfejsy sieciowe 1Gb Ethernet w standardzie BaseT. Możliwość instalacji wymiennie modułów udostępniających: - cztery interfejsy sieciowe 10Gb Ethernet w standardzie BaseT - cztery interfejsy sieciowe 10Gb Ethernet w standardzie SFP+ - dwa interfejsy sieciowe 1Gb Ethernet w standardzie BaseT oraz dwa interfejsy sieciowe 10Gb Ethernet ze złączami w standardzie SFP+ - dwa interfejsy sieciowe 25Gb Ethernet ze złączami SFP28. - dwa interfejsy sieciowe 1Gb Ethernet w standardzie BaseT oraz dwa interfejsy sieciowe 10Gb Ethernet ze złączami w standardzie BaseT Dodatkowo zainstalowane: - jedna karta dwuportowa 10Gb Ethernet w standardzie SFP+. - dwa interfejsy FC 16GB w standardzie SFP+.
Napęd optyczny	DVD-RW

Wymagane parametry	
Dyski twarde	Zainstalowane 2 x min. 480GB SSD SATA min. DWPD = 1, skonfigurowane fabrycznie w RAID 1. Możliwość zainstalowania modułu dla hypervisora wirtualizacyjnego, z możliwością wyposażenia w nośniki typu flash o pojemności min. 64GB, z możliwością konfiguracji zabezpieczenia synchronizacji pomiędzy nośnikami z poziomu BIOS serwera, rozwiązanie nie może powodować zmniejszenia ilości wnek na dyski twarde. Możliwość instalacji dwóch dysków M.2 SATA o pojemności min. 480GB z możliwością konfiguracji RAID 1.
Kontroler RAID	Sprzętowy kontroler dyskowy z pojemnością cache 2GB, możliwe konfiguracje poziomów RAID: 0, 1, 5, 6, 10, 50, 60.
Wbudowane porty	min. 2 porty USB 2.0 oraz 2 porty USB 3.0, 4 porty RJ45, 1 port VGA, min. 1 port RS232.
Video	Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1600x900
Wentylatory	Redundantne
Zasilacze	Min. dwa zasilacze Hot-Plug maksymalnie 750W.
Bezpieczeństwo	Zatrask górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych. Możliwość wyłączenia w BIOS funkcji przycisku zasilania. BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą TPM 2.0
Karta Zarządzania	Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowane port RJ-45 Gigabit Ethernet umożliwiające: <ul style="list-style-type: none"> • zdalny dostęp do graficznego interfejsu Web karty zarządzającej • szyfrowane połączenie (TLS) oraz autentykację i autoryzację użytkownika • możliwość podmontowania zdalnych wirtualnych napędów • wirtualną konsolę z dostępem do myszy, klawiatury • wsparcie dla IPv6 • wsparcie dla SNMP; IPMI2.0, VLAN tagging, SSH • możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer, dane historyczne powinny być dostępne przez min. 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 min. 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 urządzeń • Szybki podgląd stanu środowiska

Wymagane parametry	
	<ul style="list-style-type: none"> • 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
System Operacyjny	<p>Licencja musi uprawniać do uruchamiania SSO w środowisku fizycznym i nielimitowanej ilości wirtualnych środowisk SSO za pomocą wbudowanych mechanizmów wirtualizacji.</p> <p>SSO musi posiadać następujące, wbudowane cechy:</p> <p>a) możliwość wykorzystania, co najmniej 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym,</p> <p>b) możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności min. 64TB przez każdy wirtualny serwerowy system operacyjny,</p> <p>c) możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania do 8000 maszyn wirtualnych,</p> <p>d) 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,</p> <p>e) wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy,</p> <p>f) wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy,</p> <p>g) automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego, możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy (mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading),</p> <p>i) wbudowane wsparcie instalacji i pracy na wolumenach, które:</p> <p>I. pozwalają na zmianę rozmiaru w czasie pracy systemu,</p> <p>II. umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,</p> <p>III. umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów,</p> <p>IV. umożliwiają zdefiniowanie list kontroli dostępu (ACL),</p> <p>j) wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość,</p> <p>k) wbudowane szyfrowanie dysków</p> <p>l) możliwość uruchamiania aplikacji internetowych wykorzystujących technologię ASP.NET,</p> <p>m) możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów,</p> <p>n) wbudowana zaporą internetową (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych,</p> <p>o) graficzny interfejs użytkownika,</p> <p>p) zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe,</p> <p>r) wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play),</p> <p>s) możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu,</p> <p>t) dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa,</p> <p>u) możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:</p> <p>I. podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC,</p> <p>II. usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych</p>

Wymagane parametry	
	<p>stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji:</p> <ol style="list-style-type: none"> 1) połączenie SSO do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną, 2) ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania, 3) odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza, <p>III. zdalna dystrybucja oprogramowania na stacje robocze,</p> <p>IV. praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej,</p> <p>V. centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:</p> <ol style="list-style-type: none"> 1) dystrybucję certyfikatów poprzez http, 2) konsolidację CA dla wielu lasów domeny, 3) automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen, <p>VI. szyfrowanie plików i folderów,</p> <p>VII. szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec),</p> <p>VIII. możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów,</p> <p>IX. serwis udostępniania stron WWW,</p> <p>X. wsparcie dla protokołu IP w wersji 6 (IPv6),</p> <p>XI. wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie min. 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:</p> <ol style="list-style-type: none"> 1) dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych, 2) obsługi ramek typu jumbo frames dla maszyn wirtualnych, 3) obsługi 4-KB sektorów dysków, 4) nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra, 5) możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API, 6) możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk model), v) możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta SSO umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet, w) wsparcie dostępu do zasobu dyskowego SSO poprzez wiele ścieżek (Multipath), x) możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego, y) mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty, z) możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF.
Modułu bezpieczeństwa	<p>Serwer ma posiadać fabrycznie zamontowany moduł HSM (Hardware Security Module) spełniający poniższe wymagania:</p> <ol style="list-style-type: none"> 1. Typ zamawianego urządzenia: Sprzętowe, Kartowy Moduł Kryptograficzny (HSM). 2. Urządzenie musi umożliwiać: <ol style="list-style-type: none"> a. bezpieczne przechowywanie kluczy kryptograficznych, b. bezpieczne wykonywanie operacji z użyciem kluczy kryptograficznych c. przechowywanie wielu kluczy jednocześnie,

Wymagane parametry	
	<p>d. możliwość przechowania i backupów kluczy z wykorzystaniem mechanizmów podziału „n z k”. Do każdego urządzenia należy dostarczyć minimum 5 urządzeń przystosowanych do przechowania podzielonego klucza,</p> <p>3. Urządzenie musi obsługiwać algorytmy asymetryczne:</p> <ul style="list-style-type: none"> a. RSA (1024, 2048, 4096, 8192 bitów), b. Diffie-Helman, c. ECC Suite B; <p>4. Urządzenie musi obsługiwać algorytmy symetryczne:</p> <ul style="list-style-type: none"> a. AES (128, 192, 256 bitów), b. Triple DES (112, 168 bitów); <p>5. Urządzenie musi obsługiwać funkcję skrótu:</p> <ul style="list-style-type: none"> a. SHA-1, b. SHA-2 (224, 256, 384, 512 bitów); <p>6. Urządzenie musi zapewnić obsługę następujących interfejsów programowania:</p> <ul style="list-style-type: none"> a. PKCS#11, MSCAPI, b. Java JCE API, OpenSSL. <p>7. Urządzenie musi wykorzystywać moduły kryptograficzne posiadające Certyfikat FIPS 140-2 poziom minimum 3 – (na wezwanie zamawiającego należy dostarczyć potwierdzenie, iż oferowany moduł kryptograficzny posiada wymieniony certyfikat).</p> <p>8. urządzenie współpracuje z Urzędem Certyfikacji opartym o oprogramowanie – system operacyjny zaproponowany dla serwera w niniejszym postępowaniu;</p> <p>9. Urządzenie musi umożliwiać instalację w serwerze na złączu PCIe v2 lub v3</p> <p>10. Dostarczone urządzenia HSM muszą zapewnić interfejs do zdalnego zarządzania, umożliwiający szybką diagnostykę, konfigurację i administrację. Z możliwością zarządzania urządzeniami z poziomu linii poleceń jak i interfejsu graficznego.</p> <p>11. Urządzenia muszą posiadać obsługę protokołów umożliwiającą połączenie z istniejącą infrastrukturą telekomunikacyjną Zamawiającego.</p> <p>12. Urządzenia muszą umożliwiać przechowywanie kluczy kryptograficznych wewnątrz modułu HSM.</p> <p>13. Urządzenia muszą zapewnić kontrolę dostępu oraz bezpieczeństwo przechowywanych kluczy zgodnie z wymogami posiadanej certyfikacji.</p> <p>14. Urządzenia muszą posiadać mechanizmy wykrywania i rejestrowania nieprawidłowości działania oraz prób nieautoryzowanego dostępu.</p> <p>15. Urządzenia muszą umożliwiać archiwizację kluczy szyfrujących z zachowaniem poufności i integralności kopii bezpieczeństwa, oraz ich odtwarzanie w przypadku uszkodzenia</p> <p>16. Oprogramowanie dostarczone przez Dostawcę, wraz z urządzeniami, muszą zapewnić wsparcie min. dla systemów operacyjnych typu: Windows Server 2019, Red Hat Enterprise Linux Server 5 i 6.</p> <p>17. minimum 100 podpisów na sekundę kluczem RSA o długości 1024 bitów;</p> <p>18. wraz z urządzeniem należy dostarczyć biblioteki programowe PKCS#11, Microsoft CAPI oraz CNG dla systemu operacyjnego Microsoft Windows Server 2019;</p>
Certyfikaty	<p>Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2008 oraz ISO-14001. Serwer musi posiadać deklaracja CE.</p> <p>Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Microsoft Windows 2012, Microsoft Windows 2012 R2 x64, Microsoft Windows 2016, Microsoft Windows 2019 x64.</p>
Warunki gwarancji	<p>Pięć lat gwarancji producenta z czterogodzinnym czasem reakcji, możliwość zgłaszania awarii w trybie 365x7x24 poprzez ogólnopolską linię telefoniczną producenta.</p> <p>Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego.</p> <p>Wymagane dołączenie do oferty oświadczenia Producenta potwierdzając, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta.</p>

Wymagane parametry	
Dokumentacja użytkownika	Zamawiający wymaga dokumentacji w języku polskim lub angielskim. Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.

SERWER - Typ II

Wymagane parametry	
Obudowa	Obudowa Rack o wysokości max. 1U umożliwiającą instalację min. 8 dysków 2,5" z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych wraz z organizerem do kabli umożliwiającym montaż w szafie rack. Obudowa z możliwością wyposażenia w kartę umożliwiającą dostęp bezpośredni poprzez urządzenia mobilne - serwer musi posiadać możliwość konfiguracji oraz monitoringu najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej min. (Android i Apple iOS) przy użyciu jednego z protokołów BLE lub WIFI.
Płyta główna	Płyta główna z możliwością zainstalowania minimum dwóch procesorów.
Chipset	Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych
Procesor	Zainstalowane dwa procesory min. szesnasto- rdzeniowe klasy x86 do pracy z zaoferowanym serwerem umożliwiające osiągnięcie wyniku min. 173 punktów w teście SPECrate2017_int_base dostępnym na stronie www.spec.org dla dwóch procesorów. Procesory muszą sprzętowo wspierać wirtualizację.
RAM	Min. 512GB DDR4 RDIMM 3200MT/s, na płycie głównej powinno znajdować się minimum 24 slotów przeznaczonych do instalacji pamięci. Płyta główna powinna obsługiwać do 3TB pamięci RAM.
Zabezpieczenia pamięci RAM	Memory Rank Sparing, Memory Mirror
Gniazda PCI	- minimum trzy sloty PCIe x16 generacji 3.
Interfejsy sieciowe/FC/SAS	Wbudowane cztery interfejsy sieciowe 1Gb Ethernet w standardzie BaseT. Możliwość instalacji wymiennie modułów udostępniających: - cztery interfejsy sieciowe 10Gb Ethernet w standardzie BaseT - cztery interfejsy sieciowe 10Gb Ethernet w standardzie SFP+ - dwa interfejsy sieciowe 1Gb Ethernet w standardzie BaseT oraz dwa interfejsy sieciowe 10Gb Ethernet ze złączami w standardzie SFP+ - dwa interfejsy sieciowe 25Gb Ethernet ze złączami SFP28. - dwa interfejsy sieciowe 1Gb Ethernet w standardzie BaseT oraz dwa interfejsy sieciowe 10Gb Ethernet ze złączami w standardzie BaseT Dodatkowo zainstalowane: - jedna karta dwuportowa 10Gb Ethernet w standardzie SFP+. - dwa interfejsy FC 16GB w standardzie SFP+.
Napęd optyczny	DVD-RW
Dyski twarde	Zainstalowane 2 x min. 480GB SSD SATA min. DWPD = 1, skonfigurowane fabrycznie w RAID 1. Możliwość zainstalowania modułu dla hypervisora wirtualizacyjnego, z możliwością wyposażenia w nośniki typu flash o pojemności min. 64GB, z możliwością konfiguracji zabezpieczenia synchronizacji pomiędzy nośnikami z poziomu BIOS serwera, rozwiązanie nie może powodować zmniejszenia ilości wnek na dyski twarde. Możliwość instalacji dwóch dysków M.2 SATA o pojemności min. 480GB z możliwością konfiguracji RAID 1.

Wymagane parametry	
Kontroler RAID	Sprzętowy kontroler dyskowy z pojemnością cache 2GB, możliwe konfiguracje poziomów RAID: 0,1,5,6,10,50,60.
Wbudowane porty	min. 2 porty USB 2.0 oraz 2 porty USB 3.0, 4 porty RJ45, 1 port VGA, min. 1 port RS232.
Video	Zintegrowana karta graficzna umożliwiającą wyświetlenie rozdzielczości min. 1600x900
Wentylatory	Redundantne
Zasilacze	Min. dwa zasilacze Hot-Plug maksymalnie 750W.
Bezpieczeństwo	Zatrask górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych. Możliwość wyłączenia w BIOS funkcji przycisku zasilania. BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą TPM 2.0
Karta Zarządzania	<p>Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowane port RJ-45 Gigabit Ethernet umożliwiającą:</p> <ul style="list-style-type: none"> • zdalny dostęp do graficznego interfejsu Web karty zarządzającej • szyfrowane połączenie (TLS) oraz autentykację i autoryzację użytkownika • możliwość podmontowania zdalnych wirtualnych napędów • wirtualną konsolę z dostępem do myszy, klawiatury • wsparcie dla IPv6 • wsparcie dla SNMP; IPMI2.0, VLAN tagging, SSH • możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer, dane historyczne powinny być dostępne przez min. 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 min. 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 urządzeń • 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

Wymagane parametry	
System Operacyjny	<p>Licencja musi uprawniać do uruchamiania SSO w środowisku fizycznym i nieilimitowanej ilości wirtualnych środowisk SSO za pomocą wbudowanych mechanizmów wirtualizacji.</p> <p>SSO musi posiadać następujące, wbudowane cechy:</p> <ul style="list-style-type: none"> a) możliwość wykorzystania, co najmniej 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym, b) możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności min. 64TB przez każdy wirtualny serwerowy system operacyjny, c) możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania do 8000 maszyn wirtualnych, d) 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, e) wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy, f) wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy, g) automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego, możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy (mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading), i) wbudowane wsparcie instalacji i pracy na wolumenach, które: <ul style="list-style-type: none"> I. pozwalają na zmianę rozmiaru w czasie pracy systemu, II. umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów, III. umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów, IV. umożliwiają zdefiniowanie list kontroli dostępu (ACL), j) wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość, k) wbudowane szyfrowanie dysków l) możliwość uruchamiania aplikacji internetowych wykorzystujących technologię ASP.NET, m) możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów, n) wbudowana zaporę internetową (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych, o) graficzny interfejs użytkownika, p) zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe, r) wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play), s) możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu, t) dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa, u) możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji: <ul style="list-style-type: none"> I. podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC, II. 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: <ul style="list-style-type: none"> 1) połączenie SSO do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną, 2) ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,

Wymagane parametry	
	<p>3) odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza,</p> <p>III. zdalna dystrybucja oprogramowania na stacje robocze,</p> <p>IV. praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej,</p> <p>V. centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:</p> <p>1) dystrybucję certyfikatów poprzez http,</p> <p>2) konsolidację CA dla wielu lasów domen,</p> <p>3) automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen,</p> <p>VI. szyfrowanie plików i folderów,</p> <p>VII. szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec),</p> <p>VIII. możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów,</p> <p>IX. serwis udostępniania stron WWW,</p> <p>X. wsparcie dla protokołu IP w wersji 6 (IPv6),</p> <p>XI. wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie min. 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:</p> <p>1) dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych,</p> <p>2) obsługi ramek typu jumbo frames dla maszyn wirtualnych,</p> <p>3) obsługi 4-KB sektorów dysków,</p> <p>4) nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra,</p> <p>5) możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API,</p> <p>6) możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk model),</p> <p>v) możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta SSO umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet,</p> <p>w) wsparcie dostępu do zasobu dyskowego SSO poprzez wiele ścieżek (Multipath),</p> <p>x) możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego,</p> <p>y) mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty,</p> <p>z) możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF.</p>
Certyfikaty	<p>Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2008 oraz ISO-14001. Serwer musi posiadać deklarację CE.</p> <p>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.</p>
Warunki gwarancji	<p>Pięć lat gwarancji producenta z czterogodzinnym czasem reakcji, możliwość zgłaszania awarii w trybie 365x7x24 poprzez ogólnopolską linię telefoniczną producenta.</p> <p>Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego.</p>

Wymagane parametry	
	Wymagane dołączenie do oferty oświadczenia Producenta potwierdzając, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta.
Dokumentacja użytkownika	Zamawiający wymaga dokumentacji w języku polskim lub angielskim. Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.

MACIERZ

Wymagane parametry	
Obudowa	Do instalacji w standardowej szafie RACK 19", macierz musi zajmować maksymalnie 2U i pozwalać na instalację 24 dysków 2.5".
Kontrolery	Dwa kontrolery RAID pracujące w układzie active-active
Cache	8GB na kontroler, pamięć cache zapisu mirrorowana między kontrolerami, podtrzymywana bateryjnie przez min. 72h w razie awarii.
Dyski	Zainstalowane 12 dysów Hot-Plug o pojemności min. 1.92TB SSD interfejs SAS 12Gbps 2,5". Możliwość rozbudowy przez dokładanie kolejnych dysków/półek dyskowych do łącznie minimum 274 dysków. Możliwość mieszania typów dysków w obrębie macierzy oraz pojedynczej półki.
Interfejsy sieciowe/FC/SAS	Zainstalowane dwa interfejsy FC 16GB w standardzie SFP+ na kontroler.
Oprogramowanie/Funkcjonalności	Zarządzanie macierzą poprzez minimum przeglądarkę internetową, GUI oparte o HTML5. Powiadomianie mailem o awarii. Macierz lub oprogramowanie umożliwiające maskowanie i mapowanie dysków. Macierz powinna 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 oraz macierz musi posiadać funkcjonalność zdalnej replikacji danych do macierzy tej samej rodziny w trybie asynchronicznym bez konieczności zakupu dodatkowych licencji. Konieczne jest posiadanie automatycznego, bez interwencji człowieka, rozkładania danych między dyskami poszczególnych typów (tzw. auto-tiering). Dane muszą być automatycznie przemieszczane między różnymi typami dysków. Możliwość wykorzystania dysków SSD jako cache macierzy, możliwość rozbudowy pamięci cache do min. 4TB poprzez dyski SSD.
Wsparcie dla systemów operacyjnych	Windows Server 2012 R2, Windows Server 2016, Windows Server 2019, Red Hat Enterprise Linux (RHEL), SLES, Vmware ESXi.
Bezpieczeństwo	Ciągła praca obu kontrolerów nawet w przypadku zaniku jednej z faz zasilania. Zasilacze, wentylatory, kontrolery RAID redundantne.
Warunki gwarancji dla macierzy	Pięć lat gwarancji realizowanej w miejscu instalacji sprzętu, z czterogodzinnym czasem reakcji od przyjęcia zgłoszenia, możliwość zgłaszania awarii w trybie 365x7x24 poprzez ogólnopolską linię telefoniczną producenta. Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wsparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego. Wymagane dołączenie do oferty oświadczenia Producenta potwierdzając, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta.

Wymagane parametry	
	<p>Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia, oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji macierzy.</p> <ul style="list-style-type: none"> • Wszystkie naprawy gwarancyjne powinny być możliwe na miejscu. • Dostawca ponosi koszty napraw gwarancyjnych, włączając w to koszt części i transportu. • W czasie obowiązywania gwarancji dostawca zobowiązany jest do udostępnienia Zamawiającemu nowych wersji BIOS, firmware i sterowników (na płytach CD lub stronach internetowych).
Dokumentacja użytkownika	Zamawiający wymaga dokumentacji w języku polskim lub angielskim
Certyfikaty	Macierz musi być wyprodukowany zgodnie z normą ISO 9001:2008.

SZKOLENIE

Szkolenie	<p>Autoryzowane szkolenie Microsoft min. 35 godzin obejmujące następujące zagadnienia:</p> <ul style="list-style-type: none"> - wirtualizacja serwerów, - wirtualizacja Hyper-V, - instalowanie i konfigurowanie Virtual Machine Manager, - zarządzanie strukturą pamięci i aktualizacjami sieci szkieletowej, - konfigurowanie i zarządzanie bibliotekami Virtual Machine Manager i obiektami biblioteki, - zarządzanie strukturą sieci, - tworzenie i zarządzanie maszynami wirtualnymi za pomocą Virtual Machine Manager, - zarządzanie chmurami w programie Microsoft System Center Virtual Machine Manager, - zarządzanie usługami w Virtual Machine Manager, - monitorowanie infrastruktury wirtualizacji za pomocą System Center Operations Manager, - wdrażanie i zarządzanie repliką Hyper-V i Azure Site Recovery, - ochrona infrastruktury wirtualizacji za pomocą Data Protection Manager <p>Możliwość dostawy vouchera szkoleniowego z terminem ważności min. 1 rok.</p>
Szkolenie	<p>Szkolenie z implementacją klastra pracy awaryjnej:</p> <ul style="list-style-type: none"> - Planowanie klastra - Tworzenie nowego klastra - Konfiguracja aplikacji i usług wysokiej dostępności na klastrze - Zarządzanie i utrzymanie klastra - Rozwiązywanie problemów dotyczących klastra - Implementacja wysokiej dostępności z wieloma klastrami - Omówienie aspektów integracji Hyper-V z klastrem <p>Implementacja Hyper-V z klastrem Zarządzanie i utrzymanie maszyn wirtualnych Hyper-V na klastrach Możliwość dostawy vouchera szkoleniowego z terminem ważności min. 1 rok.</p>

INSTALACJA I KONFIGURACJA

Instalacja i konfiguracja	<ol style="list-style-type: none">1. Ustalenie z działem IT Zamawiającego prawidłowej instalacji urządzeń.2. Montaż dostarczonych urządzeń w szafach rack oraz ich instalacja zgodnie z wytycznymi Zamawiającego3. Podstawowa konfiguracja dostarczonego systemu operacyjnego4. Instalacja i konfiguracja środowiska do wirtualizacji5. Przygotowanie miejsca pod niezbędne serwery wirtualne.6. Dwutygodniowe wsparcie osoby technicznej pomagające w rozwiązaniu ewentualnych problemów z dostarczonymi urządzeniami liczone od momentu ich instalacji.7. Wykonanie klastra nowo dostarczanych serwerów oraz konfiguracja macierzy z nowym klastrem.8. Serwery i macierz wyposażone w niezbędne wkładki i kable do połączenia w sieci.
----------------------------------	---

LICENCJE DOSTĘPWE

Licencje dostępne do Windows Serwer 2019	W ramach dostawy mają zostać dostarczone licencje dostępne CAL do serwera dla 500 urządzeń
---	--