Załącznik nr 2 do siwz po zmianie

Serwery aplikacyjne	Opis wymagań Serwerów
Ilość sztuk	3
Obudowa	Do instalacji w szafie Rack 19", wysokość nie więcej niż 1U, z zestawem szyn do mocowania w szafie i wysuwania do celów serwisowych.
Procesor	Architektura x86, maksymalny TDP dla procesora – 165W. Minimalna ilość rdzeni dla procesora – 12, taktowanie procesora nie niższe niż 3.3GHz. Wynik wydajności procesora instalowanego w oferowanym serwerze nie powinien być niższy niż 183 punky base w teście SPECrate 2017 Integer, opublikowanym przez SPEC.org (www.spec.org) dla konfiguracji dwuprocesorowej. Test przeprowadzony przez producenta serwera musi być zamieszczony na stronie spec.org. Obsługa minimum dwóch procesorów.
Liczba procesorów	Min. 2
Płyta główna	Płyta główna dedykowana do pracy w serwerach, wyprodukowana przez producenta serwera z możliwością zainstalowania do dwóch procesorów wykonujących 64-bitowe instrukcje AMD64 lub EM64T (np. AMD Opteron albo Intel Xeon)
Pamięć operacyjna	Zainstalowane minimum 256GB pamięci RAM o częstotliwości 2933MHz. Minimum 24 sloty na pamięć. Możliwość rozbudowy do 7.5TB RAM.
Zabezpieczenie pamięci	memory mirroring, demand scrubing, patrol scrubing, memory rank sparing, ECC, SDDC, ADDDC
Procesor Graficzny	Zintegrowana karta graficzna z minimum 16MB pamięci osiągająca rozdzielczość 1920x1200 przy 60 Hz. 1 port VGA na tylnym panelu serwera. Wymagana możliwość instalacji portu VGA na panelu przednim.
Rozbudowa dysków	W chwili dostawy serwer musi posiadać możliwość zainstalowania minimum 8 dysków SAS/SATA bez konieczności instalacji jakichkolwiek dodatkowych komponentów, przy czym zainstalowane powinny być minimum 4 dyski ssd 3D TLC NAND o pojemności przynajmniej 480GB . Dyski powinny być zorientowane na intensywny odczyt i wydajność odczytu sekwencyjnego dla bloku 128KB nie powinna być mniejsza niż 540MBps dla każdego dysku. Wymaga się, aby serwer posiadał możliwość instalacji dysków SED.
Kontroler dyskowy	Zainstalowany sprzętowy kontroler SAS obsługujący następujące poziomy zabezpieczeń raid 0/1/10/5/50. Wymagana obsługa następującego formatowania dysków: 512e, 512n, 4K. Kontroler musi umożliwiać tworzenie globalnych dysków hot-spare. Wymaga się, aby kontroler posiadał funkcjonalność kontynuowania procesu odbudowy macierzy raid przerwanego na skutek awarii zasilania. Zmiana pojemności zdefiniowanych dysków wirtualnych powinna odbywać się online. Wymaga się także możliwości zmiany typu raid grupy dyskowej w trybie online.
Zasilacz	Minimum dwa redundantne zasilacze o mocy minimum 750W z certyfikatem minimum Platinum.
Interfejsy sieciowe	Zintegrowane na płycie 2 porty 10Gb SFP+ wyposażone we wkładki typu SR. Interfejsy te nie mogą wpływać na ilość dostępnych slotów PCIe wymienionych w punkcie Dodatkowe sloty I/O . Wymagana funkcjonalność wbudowanych portów: NIC teaming, możliwość realizacji bezpośredniego dostępu do pamięci iWARP, SR-IOV, offload sumy kontrolnej stosu TCP/IP, wsparcie dla DCB, obsługa ramek Jumbo do 9.5Kb, Jeden port RJ-45 o przepustowości 1GbE dedykowany dla karty zarządzającej. Dodatkowo serwer powinien posiadać zainstalowane minimum dwa porty FC 16GBs.
Dodatkowe sloty I/O	Serwer powinien umożliwiać instalacje do 4 kart PCIe. W chwili dostawy serwer powinien umożliwiać obsługę przynajmniej 3 kart PCIe bez instalacji jakichkolwiek dodatkowych
Dodatkowe porty	· z przodu obudowy: 1x USB 3.0, 1x USB 2.0, Możliwość instalacji portu VGA. · z tyłu obudowy: 2x USB 3.0, , 1x DB-15 . Możliwość instalacji portu DB9
Chłodzenie	Wentylatory wspierające wymianę Hot-Swap, zamontowane nadmiarowo minimum N+1
	Zintegrowany z płytą główną serwera, niezależny od systemu operacyjnego, sprzętowy kontroler zdalnego zarzadzania umożliwiający:

Monitoring statusu i zdrowia systemu (komponenty objęte monitoringiem to przynajmniej: CPU, pamięć RAM, dyski, karty PCI, zasilacze, wentylatory, płyta główna
Pozyskanie następujących informacji o serwerze: nazwa, typ i model, numer seryjny, nazwa systemu, wersja UEFI oraz BMC, adres IP karty zarządzającej, utylizacja CPU, utylizacja pamięci oraz komponentów I/O
Logowanie zdarzeń
Wysyłanie określonych zdarzeń poprzez SMTP SNMPv3
Logowanie aktywności użytkowników
Umożliwiający Update systemowego firmware
Monitoring i możliwość ograniczenia poboru prądu
Zdalne włączanie/wyłączanie/restart
Zapis video zdalnych sesji
Podmontowanie lokalnych mediów z wykorzystaniem Java client
Przekierowanie konsoli szeregowej przez IPMI
Zrzut ekranu w momencie zawieszenia systemu
Możliwość przejęcia zdalnego ekranu
Możliwość zdalnej instalacji systemu operacyjnego
Alerty Syslog
Przekierowanie konsoli szeregowej przez SSH
Wyświetlanie danych aktualnych I historycznych dla użycia energii I temperatury serwera
Możliwość mapowania obrazów ISO z lokalnego dysku operatora
Możliwość mapowania obrazów ISO przez HTTPS, SFTP, CIFS oraz NFS
Możliwość jednoczesnej pracy do 6 użytkowników przez wirtualną konsolę
Wspierane protokoły/interfejsy: IPMI v2.0, SNMP v3, CIM, DCMI v1.5, REST API
Wymaga się możliwości wykorzystania frontowego portu USB do celów serwisowych (komunikacja portu z karta zarządzającą) bez możliwości uzyskania jakiejkolwiek funkcjonalności na poziomie zainstalowanego systemu operacyjnego. Funkcjonalność ta musi być realizowana na poziomie sprzętowym i musi być niezależna od zainstalowanego systemu operacyjnego.
Wraz z serwerem powinno zostać dostarczone dodatkowe oprogramowanie zarządzające umożliwiające :
- zarządzenie infrastruktura serwerów, przełączników i storage bez udziału dedykowanego agenta
- przedstawianie graficznej reprezentacji zarządzanych urządzeń
- możliwość skalowania do minimum 560 urządzeń
- udostępnianie szybkiego podgląd stanu środowiska
- udostępnianie podsumowania stanu dla każdego urządzenia
- tworzenie alertów przy zmianie stanu urządzenia
- monitorowanie oraz tracking zużycia energii przez monitorowane urządzenie, możliwość ustalania granicy zużycia energii,
- konsola zarzadzania oparta o HTML 5
- dostępność konsoli monitorującej na urządzeniach przenośnych ze wsparciem dla systemu Android oraz iOS
- automatyczne wykrywanie dołączanych systemów oraz szczegółowa inwentaryzacja
- możliwość podnoszenia wersji oprogramowania dla komponentów zarządzanych serwerów w oparciu o repozytorium lokalne jak i zdalne dostępne na stronie producenta oferowanego rozwiązania
- definiowanie polityk zgodności wersji firmware komponentów zarządzanych urządzeń
- definiowanie roli użytkowników oprogramowania
- obsługa REST API oraz Windows PowerShell
- obsługa SNMP, SYSLOG, Email Forwarding
- autentykacja użytkowników: centralna (możliwość definiowania wymaganego poziomu skomplikowania danych autentykacyjnych) oraz integracja z MS AD oraz obsługa single sign on oraz SAML
- wsparcie dla NIST 800-131A oraz FIPS 140-2
- obsługa tzw. Forward Secrecy w komunikacji z zarządzanymi urządzeniami
- przedstawianie historycznych aktywności użytkowników
- wsparcie dla certyfikatów SSL tzw. self-signed oraz zewnętrznych

	-blokowanie możliwości podłączenia innego systemu zarzadzania do urządzeń zarządzanych
	- tworzenie dziennika zdarzeń ukończonych sukcesem lub bledem, oraz zdarzeń będących w trakcie. Możliwość definiowania filtrów wyświetlanych zdarzeń z dziennika. Możliwość eksportu dziennika zdarzeń do pliku csv
	- Obsługa NTP
	- możliwość automatycznego tworzenia zgłoszeń w centrum serwisowym producenta dla określonych zdarzeń wraz z przesyłem plików diagnostycznych,
	- przesyłanie alertów do konsoli firm trzecich
	- tworzenie wzorców konfiguracji zarządzanych urządzeń (definiowanie przez konsole albo kopiowanie konfiguracji z już zaimplementowanych urządzeń)
	- instalowanie systemów operacyjnych oraz witalizatorów Vmware i Hyper-V. Wymagana jest integracja konsoli zarządzania z konsolą witalizatora tak, aby zarządzanie środowiskiem sprzętowym mogło odbywać się z konsoli witalizatora
Zarządzanie	
Funkcje zabezpieczeń	Hasło włączania, hasło administratora, moduł TPM. Wymagana możliwość zainstalowania przedniego panelu zabezpieczającego zamykanego na klucz.
Urządzenia hot swap	Dyski twarde, zasilacze, wentylatory.
Obsługa	Możliwość instalacji serwera oraz wymiany procesora, radiatora oraz tzw. Backplane'y dysków twardych do celów serwisowych bez użycia dodatkowych narzędzi mechanicznych.
	Możliwość przewidywania awarii dla procesorów, regulatorów napięcia, pamięci, dysków wewnętrznych, wentylatorów, zasilaczy, kontrolerów RAID
Diagnostyka	Możliwość użycia aplikacji mobilnej na telefonie, do przeglądania awarii, konfiguracji i włączenia/wyłączenia serwera.
Systemy operacyjne obsługiwane	Microsoft Windows Server 2012 R2, 2016, 2019, Red Hat Enterprise Linux 6 oraz 7, SUSE Linux Enterprise Server 12 oraz 15, VMware vSphere (ESXi) 6.5 oraz 6.7.
Waga	maximum: 18.8kg
Gwarancja	36 miesięcy wsparcia producenta w trybie pełnego serwisu on-site z gwarantowanym czasem naprawy 24h
Serwery bazodanowe	
Ilość sztuk	2
Obudowa	Do instalacji w szafie Rack 19", wysokość nie więcej niż 1U, z zestawem szyn do mocowania w szafie i wysuwania do celów serwisowych.
Procesor	Architektura x86, maksymalny TDP dla procesora – 125W. Ilość rdzeni dla procesora – 8. Wynik wydajności procesora instalowanego w oferowanym serwerze nie powinien być niższy niż 120 punky base w teście SPECrate 2017 Integer, opublikowanym przez SPEC.org (www.spec.org) dla konfiguracji dwuprocesorowej. Test przeprowadzony przez producenta serwera musi być zamieszczony na stronie spec.org. Obsługa minimum dwóch procesorów.
Liczba procesorów	1
Płyta główna	Płyta główna dedykowana do pracy w serwerach, wyprodukowana przez producenta serwera z możliwością zainstalowania do dwóch procesorów wykonujących 64-bitowe instrukcje AMD64 lub EM64T (np. AMD Opteron albo Intel Xeon)
	Zainstalowane minimum 128GB pamięci RAM.
Pamięć operacyjna	Minimum 16 slotów na pamięć. Możliwość rozbudowy do 2.75TB RAM.
Zabezpieczenie pamięci	memory mirroring, demand scrubing, patrol scrubing, memory rank sparing, ECC, SDDC, ADDDC
	Zintegrowana karta graficzna z minimum 16MB pamięci osiągająca rozdzielczość 1920x1200 przy 60 Hz.
Procesor Graficzny	1 port VGA na tylnym panelu serwera. Wymagana możliwość instalacji portu VGA na panelu przednim.
Rozbudowa dysków	W chwili dostawy serwer musi posiadać możliwość zainstalowania minimum 8 dysków SAS/SATA bez konieczności instalacji jakichkolwiek dodatkowych komponentów, przy czym zainstalowane powinny być minimum 4 dyski 900GB SAS 15k. Wymaga się, aby serwer posiadał możliwość instalacji dysków SED.

Kontroler dyskowy	Zainstalowany kontroler SAS posiadający przynajmniej 2GB nieulotnej pamięci cache. Podtrzymanie pamięci kontrolera powinno być zrealizowane w technologii nie wymagającej baterii. Wymagana obsługa następującego formatowania dysków: 512e, 512n, 4K. Kontroler musi umożliwiać tworzenie globalnych dysków hot-spare. Wymaga się, aby kontroler posiadał funkcjonalność kontynuowania procesu odbudowy macierzy raid przerwanego na skutek awarii zasilania.
	Zmiana pojemności zdefiniowanych dysków wirtualnych powinna odbywać się online. Wymaga się także możliwości zmiany typu raid grupy dyskowej w trybie online.
Zasilacz	Minimum dwa redundantne zasilacze o mocy minimum 750W z certyfikatem minimum Platinum.
Interfejsy sieciowe	Zintegrowane na płycie 2 porty 10Gb Base-T. Interfejsy te nie mogą wpływać na ilość dostępnych slotów PCIe wymienionych w punkcie Dodatkowe sloty I/O .
	Wymagana funkcjonalność wbudowanych portów:
	NIC teaming, możliwość realizacji bezpośredniego dostępu do pamięci iWARP, SR-IOV, offload sumy kontrolnej stosu TCP/IP, wsparcie dla DCB, obsługa ramek Jumbo do 9.5Kb,
	Jeden port RJ-45 o przepustowości 1GbE dedykowany dla karty zarządzającej.
	Dodatkowo serwer powinien posiadać zainstalowane minimum dwa porty 1Gb Base-t oraz dwa porty 10Gb SFP+ . Wymagana funkcjonalność portów SFP: możliwość realizacji bezpośredniego dostępu do pamięci RDMA (RoCE, TCP/IP stack By-Pass), offload sumy kontrolnej stosu TCP/IP, wsparcie dla DCB, obsługa ramek Jumbo, możliwość całkowitego sprzętowego wsparcia dla protokołów iSCSI oraz FCoE.
Dodatkowe sloty I/O	W chwili dostawy serwer powinien umożliwiać obsługę przynajmniej 3 kart PCIe bez instalacji jakichkolwiek dodatkowych komponentów serwera.
Dodatkowe porty	· z przodu obudowy: 1x USB 3.0, 1x USB 2.0, Możliwość instalacji portu VGA.
	· z tyłu obudowy: 2x USB 3.0, , 1x DB-15 . Możliwość instalacji portu DB9
Chłodzenie	Wentylatory wspierające wymianę Hot-Swap, zamontowane nadmiarowo minimum N+1
	Zintegrowany z płytą główną serwera, niezależny od systemu operacyjnego, sprzętowy kontroler zdalnego zarzadzania umożliwiający:
	Monitoring statusu i zdrowia systemu (komponenty objęte monitoringiem to przynajmniej: CPU, pamięć RAM, dyski, karty PCI, zasilacze, wentylatory, płyta główna
	Pozyskanie następujących informacji o serwerze: nazwa, typ i model, numer seryjny, nazwa systemu, wersja UEFI oraz BMC, adres iIP karty zarządzającej, utylizacja CPU, utylizacja pamięci oraz komponentów I/O
	Logowanie zdarzeń
	Wysyłanie określonych zdarzeń poprzez SMTP SNMPv3
	Logowanie aktywności użytkowników
	Umożliwiający Update systemowego firmware
	Monitoring i możliwość ograniczenia poboru prądu
	Zdalne włączanie/wyłączanie/restart
	Zapis video zdalnych sesji
	Podmontowanie lokalnych mediów z wykorzystaniem Java client
	Przekierowanie konsoli szeregowej przez IPMI
	Zrzut ekranu w momencie zawieszenia systemu
	Możliwość przejęcia zdalnego ekranu
	Możliwość zdalnej instalacji systemu operacyjnego
	Alerty Syslog
	Przekierowanie konsoli szeregowej przez SSH
	Wyświetlanie danych aktualnych I historycznych dla użycia energii I temperatury serwera
	Możliwość mapowania obrazów ISO z lokalnego dysku operatora
	Możliwość mapowania obrazów ISO przez HTTPS, SFTP, CIFS oraz NFS
	Możliwość jednoczesnej pracy do 6 użytkowników przez wirtualną konsolę
	Wspierane protokoły/interfejsy: IPMI v2.0, SNMP v3, CIM, DCMI v1.5, REST API

	Wymaga się możliwości wykorzystania frontowego portu USB do celów serwisowych (komunikacja portu z karta zarządzającą) bez możliwości uzyskania jakiejkolwiek funkcjonalności na poziomie zainstalowanego systemu operacyjnego. Funkcjonalność ta musi być realizowana na poziomie sprzętowym i musi być niezależna od zainstalowanego systemu operacyjnego.
	Wraz z serwerem powinno zostać dostarczone dodatkowe oprogramowanie zarządzające umożliwiające :
	- zarządzenie infrastruktura serwerów, przełączników i storage bez udziału dedykowanego agenta
	- przedstawianie graficznej reprezentacji zarządzanych urządzeń
	- możliwość skalowania do minimum 560 urządzeń
	- udostępnianie szybkiego podgląd stanu środowiska
	- udostępnianie podsumowania stanu dla każdego urządzenia
	- tworzenie alertów przy zmianie stanu urządzenia
	- monitorowanie oraz tracking zużycia energii przez monitorowane urządzenie, możliwość ustalania granicy zużycia energii,
	- konsola zarzadzania oparta o HTML 5
	- dostępność konsoli monitorującej na urządzeniach przenośnych ze wsparciem dla systemu Android oraz iOS
	- automatyczne wykrywanie dołączanych systemów oraz szczegółowa inwentaryzacja
	- możliwość podnoszenia wersji oprogramowania dla komponentów zarządzanych serwerów w oparciu o repozytorium lokalne jak i zdalne dostępne na stronie producenta oferowanego rozwiązania
	- definiowanie polityk zgodności wersji firmware komponentów zarządzanych urządzeń
	- definiowanie roli użytkowników oprogramowania
	- obsługa REST API oraz Windows PowerShell
	- obsługa SNMP, SYSLOG, Email Forwarding
	- autentykacja użytkowników: centralna (możliwość definiowania wymaganego poziomu skomplikowania danych autentykacyjnych) oraz integracja z MS AD oraz obsługa single sign on oraz SAML
	- wsparcie dla NIST 800-131A oraz FIPS 140-2
	- obsługa tzw. Forward Secrecy w komunikacji z zarządzanymi urządzeniami
	- przedstawianie historycznych aktywności użytkowników
	- wsparcie dla certyfikatów SSL tzw self-signed oraz zewnętrznych
	-blokowanie możliwości podłączenia innego systemu zarzadzania do urządzeń zarządzanych
	- tworzenie dziennika zdarzeń ukończonych sukcesem lub bledem, oraz zdarzeń będących w trakcie. Możliwość definiowania filtrów wyświetlanych zdarzeń z dziennika. Możliwość eksportu dziennika zdarzeń do pliku csv
	- obsługa NTP
	- możliwość automatycznego tworzenia zgłoszeń w centrum serwisowym producenta dla określonych zdarzeń wraz z przesyłem plików diagnostycznych,
	- przesyłanie alertów do konsoli firm trzecich
	- tworzenie wzorców konfiguracji zarządzanych urządzeń (definiowanie przez konsole albo kopiowanie konfiguracji z już zaimplementowanych urządzeń)
	- instalowanie systemów operacyjnych oraz witalizatorów Vmware i Hyper-V. Wymagana jest integracja konsoli zarządzania z konsolą witalizatora tak, aby zarządzanie środowiskiem sprzętowym mogło odbywać się z konsoli witalizatora
Zarządzanie	
Funkcje zabezpieczeń	Hasło włączania, hasło administratora, moduł TPM. Wymagana możliwość zainstalowania przedniego panelu zabezpieczającego zamykanego na klucz.
Urządzenia hot swap	Dyski twarde, zasilacze, wentylatory.
Obsługa	Możliwość instalacji serwera oraz wymiany procesora, radiatora oraz tzw. Backplane'y dysków twardych do celów serwisowych bez użycia dodatkowych narzędzi mechanicznych.
Diagnostyka	Możliwość przewidywania awarii dla procesorów, regulatorów napięcia, pamięci, dysków wewnętrznych, wentylatorów, zasilaczy, kontrolerów RAID
	Możliwość użycia aplikacji mobilnej na telefonie, do przeglądania awarii, konfiguracji i włączenia/wyłączenia serwera.

Systemy operacyjne obsługiwane	Microsoft Windows Server 2012 R2, 2016, 2019, Red Hat Enterprise Linux 6 oraz 7, SUSE Linux Enterprise Server 12 oraz 15, VMware vSphere (ESXi) 6.5 oraz 6.7.
Inne	Wykonawca wraz z serwerem dostarczy komplet wkładek światłowodowych 10GbE.
Waga	maximum: 16kg
Gwarancja	36 miesięcy wsparcia producenta w trybie pełnego serwisu on-site z gwarantowanym czasem naprawy 24h
Komputery	**Opis wymagań Komputerów**
Ilość sztuk	50
Opis rozwiązania	Przedmiotem zamówienia jest komputer zintegrowany z monitorem i niewystający poza jego obrys.
	Zamawiający nie dopuszcza rozwiązań polegających na podczepieniu komputera w malej obudowie z pomocą uniwersalnych uchwytów do monitora lub jego podstawy.
	Zestaw powinien umożliwiać elastyczną rekonfiguracje w zakresie:
	-RAM
	-Pamięci masowe (talerzowy / ssd)
	-CPU
	W ofercie należy podać nazwę producenta, typ, model, oraz numer katalogowy oferowanego sprzętu umożliwiający jednoznaczną identyfikację oferowanej konfiguracji. W przypadku rozwiązania składającego się z kilku komponentów należy podać nazwę producenta, typ, model, oraz numer katalogowy wszystkich elementów składowych rozwiązania.
	Połączenie jednostki centralnej z wyświetlaczem/monitorem za pomocą portów dokujących zintegrowanych w obudowie wyświetlacza/monitora.
Wyświetlacz	Matryca matowa z podświetleniem LED wykonana w technologii IPS, PLS lub innej spełniającej poniższe parametry.
	Rozmiar matrycy min. 23”
	Rozmiar pojedynczego pixela nie większy niż 0,260 mm
	Minimalna rozdzielczość 1920x1080
	Kąty widzenia pion/poziom co najmniej 178/178 stopni
	Czas reakcji matrycy min. 6ms
	Wyświetlanie zakresu barw min. 72%
	Ergonomiczna regulacja podstawy w zakresie min:
	- Pochylenia przód/tył min.-5 do 30 stopni
	- Wysokość min. 110mm
	Demontaż podstawy musi odbywać się beznarzędziowo.
Wydajność systemu	Procesor wielordzeniowy, min.6-rdzeniowy, zaprojektowany do pracy w komputerach stacjonarnych klasy x86, taktowany bazowym zegarem co najmniej 2.90GHz, pamięcią cache CPU co najmniej 9MB, osiągający wynik min. 11900 punktow Average CPU Mark na podstawie PassMark CPU Benchmark , wynik zaproponowanego procesora musi być opublikowany na stronie http://www.cpubenchmark.net . Wykonawca w składanej ofercie winien podać dokładny model oferowanego podzespołu.
Chipset	Dostosowany do zaoferowanego procesora.
Pamięć operacyjna	8 GB SoDIMM, min. 2600MHz DDR4,
	2 sloty SoDIMM dual-channel umożliwiające instalację RAM max. do 32 GB w tym jeden slot wolny
Parametry pamięci masowej	256GB SSD PCIe wspierający sprzętowe szyfrowanie dysku
	Możliwość konfiguracji RAID (0/1) dla dysków PCIe
	Możliwość rozbudowy o dysk 2,5”
Karta graficzna	Zintegrowana karta graficzna wykorzystująca pamięć RAM systemu dynamicznie przydzielaną na potrzeby grafiki w trybie UMA (Unified Memory Access) – z możliwością dynamicznego przydzielenia pamięci.
Wyposażenie multimedialne	Karta dźwiękowa zintegrowana z płytą główną, zgodna z High Definition.
	Wbudowane głośniki stereo min 2x2W
	Wbudowane dwa mikrofony.
	Możliwość elastycznego podłączenia dodatkowych zewnętrznych wyświetlaczy za pomocą wbudowanych portów HDMI i VGA.
Połączenia, porty i karty sieciowe	Port sieci LAN 10/100/1000 Ethernet RJ 45 zintegrowany z płytą główną obsługujący technologię WoL, PXE.
	WiFi 2x2 AC + Bluetooth 5.0
	Min. 8xUSB 3.0, 1xDisplayPort, 1xHDMI, 1x wyjście combo,

	Wymagana ilość i rozmieszczenie (na zewnątrz obudowy komputera) portów USB nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek itp.
System operacyjny	System operacyjny klasy PC musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji:
	1. Dostępne graficzny interfejs użytkownika, umożliwiający obsługę przy pomocy klawiatury i myszy.
	2. Funkcje związane z obsługą komputerów typu tablet, z wbudowanym modułem „uczenia się” pisma użytkownika – obsługa języka polskiego
	3. Interfejs użytkownika dostępny w wielu językach do wyboru – w tym polskim i angielskim
	4. Możliwość tworzenia pulpitów wirtualnych, przenoszenia aplikacji pomiędzy pulpitami i przełączanie się pomiędzy pulpitami za pomocą skrótów klawiaturowych lub GUI.
	5. Wbudowane w system operacyjny minimum dwie przeglądarki Internetowe
	6. Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu, tekstów, metadanych) dostępny z kilku poziomów: poziom menu, poziom otwartego okna systemu operacyjnego; system wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych,
	7. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, pomoc, komunikaty systemowe, menedżer plików.
	8. Graficzne środowisko instalacji i konfiguracji dostępne w języku polskim
	9. Wbudowany system pomocy w języku polskim.
	10. Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących).
	11. Możliwość dokonywania aktualizacji i poprawek systemu poprzez mechanizm zarządzany przez administratora systemu Zamawiającego.
	12. Możliwość dostarczania poprawek do systemu operacyjnego w modelu peer-to-peer.
	13. Możliwość sterowania czasem dostarczania nowych wersji systemu operacyjnego, możliwość centralnego opóźniania dostarczania nowej wersji o minimum 4 miesiące.
	14. Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników.
	15. Możliwość dołączenia systemu do usługi katalogowej on-premise lub w chmurze.
	16. Umożliwienie zablokowania urządzenia w ramach danego konta tylko do uruchamiania wybranej aplikacji - tryb "kiosk".
	17. Możliwość automatycznej synchronizacji plików i folderów roboczych znajdujących się na firmowym serwerze plików w centrum danych z prywatnym urządzeniem, bez konieczności łączenia się z siecią VPN z poziomu folderu użytkownika zlokalizowanego w centrum danych firmy.
	18. Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem.
	19. Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe.
	20. Oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej.
	21. Możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci.
	22. Możliwość przywracania systemu operacyjnego do stanu początkowego z pozostawieniem plików użytkownika.
	23. Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu)."
	24. Wbudowany mechanizm wirtualizacji typu hypervisor."
	25. Wbudowana możliwość zdalnego dostępu do systemu i pracy zdalnej z wykorzystaniem pełnego interfejsu graficznego.
	26. Dostępność bezpłatnych biuletynów bezpieczeństwa związanych z działaniem systemu operacyjnego.
	27. Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych, zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6.

	28. Identyfikacja sieci komputerowych, do których jest podłączony system operacyjny, zapamiętywanie ustawień i przypisywanie do min. 3 kategorii bezpieczeństwa (z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej, udostępniania plików itp.).
	29. Możliwość zdefiniowania zarządzanych aplikacji w taki sposób aby automatycznie szyfrowały pliki na poziomie systemu plików. Blokowanie bezpośredniego kopiowania treści między aplikacjami zarządzanymi a niezarządzanymi.
	30. Wbudowany system uwierzytelnienia dwuskładnikowego oparty o certyfikat lub klucz prywatny oraz PIN lub uwierzytelnienie biometryczne.
	31. Wbudowane mechanizmy ochrony antywirusowej i przeciw złośliwemu oprogramowaniu z zapewnionymi bezpłatnymi aktualizacjami.
	32. Wbudowany system szyfrowania dysku twardego ze wsparciem modułu TPM
	33. Możliwość tworzenia i przechowywania kopii zapasowych kluczy odzyskiwania do szyfrowania dysku w usługach katalogowych.
	34. Możliwość tworzenia wirtualnych kart inteligentnych.
	35. Wsparcie dla firmware UEFI i funkcji bezpiecznego rozruchu (Secure Boot)
	36. Wbudowany w system, wykorzystywany automatycznie przez wbudowane przeglądarki filtr reputacyjny URL.
	37. Wsparcie dla IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny.
	38. Mechanizmy logowania w oparciu o:
	a. Login i hasło,
	b. Karty inteligentne i certyfikaty (smartcard),
	c. Wirtualne karty inteligentne i certyfikaty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM),
	d. Certyfikat/Klucz i PIN
	e. Certyfikat/Klucz i uwierzytelnienie biometryczne
	39. Wsparcie dla uwierzytelniania na bazie Kerberos v. 5
	40. Wbudowany agent do zbierania danych na temat zagrożeń na stacji roboczej.
	41. Wsparcie .NET Framework 2.x, 3.x i 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach
	42. Wsparcie dla VBScript – możliwość uruchamiania interpretera poleceń
	43. Wsparcie dla PowerShell 5.x – możliwość uruchamiania interpretera poleceń
Dodatkowe oprogramowanie	Dedykowane oprogramowanie producenta sprzętu umożliwiające automatyczna weryfikacje i instalację sterowników oraz oprogramowania użytkowego producenta w tym również wgranie najnowszej wersji BIOS. Oprogramowanie musi automatycznie łączyć się z centralna bazą sterowników i oprogramowania użytkowego producenta, sprawdzać dostępne aktualizacje i zapewniać zbiorczą instalację wszystkich sterowników i aplikacji bez ingerencji użytkownika. Oprogramowanie musi być wyposażone w moduł rejestru zdarzeń, w którym znajdują się informacje o tym kiedy i jakie sterowniki zostały zainstalowane na danej maszynie. Oprogramowanie musi zapewniać również ustawienie automatycznego uaktualnienia wszystkich sterowników we wskazanym dniu miesiąca.
BIOS	BIOS zgodny ze specyfikacją UEFI
	- Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych podłączonych do niego urządzeń zewnętrznych informacji o:
	- modelu komputera,
	- numerze konfiguracji,
	- numerze seryjnym,
	- AssetTag (numerze inwentarzowym),
	- MAC Adres karty sieciowej,
	- wersja Biosu wraz z datą produkcji,
	- zainstalowanym procesorze, jego taktowaniu i ilości rdzeni
	- ilości pamięci RAM wraz z taktowaniem,
	- stanie pracy wentylatora na procesorze
	- dyskach podłączonych do portów SATA/M.2 (model dysku twardego)
	Możliwość z poziomu BIOS:
	- wyłączenia/włączenia portów USB
	- wyłączenia karty sieciowej, karty audio, portu szeregowego,
	- możliwość ustawienia portów USB w jednym z dwóch trybów:

	1. użytkownik może kopiować dane z urządzenia pamięci masowej podłączonego do pamięci USB na komputer ale nie może kopiować danych z komputera na urządzenia pamięci masowej podłączone do portu USB
	2. użytkownik nie może kopiować danych z urządzenia pamięci masowej podłączonego do portu USB na komputer oraz nie może kopiować danych z komputera na urządzenia pamięci masowej
	- ustawienia hasła: administratora, Power-On, HDD,
	- blokady aktualizacji BIOS bez podania hasła administratora
	- wglądu w system zbierania logów (min. Informacja o update Bios, błędzie wentylatora na procesorze, wyczyszczeniu logów) z możliwością czyszczenia logów
	- alertowania zmiany konfiguracji sprzętowej komputera
	- wyboru trybu uruchomienia komputera po utracie zasilania (włącz, wyłącz, poprzedni stan)
	- ustawienia trybu wyłączenia komputera w stan niskiego poboru energii
	- zdefiniowania trzech sekwencji bootujących (podstawowa, WOL, po awarii)
	- załadowania optymalnych ustawień Bios
	- obsługa Bios za pomocą klawiatury i myszy bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego, urządzeń zewnętrznych.
Zintegrowany System Diagnostyczny	Wizualny system diagnostyczny producenta działający nawet w przypadku uszkodzenia dysku twardego z systemem operacyjnym komputera umożliwiający na wykonanie diagnostyki następujących podzespołów:
	· test pamięci RAM
	· test dysku twardego
	· test monitora
	· test magistrali PCI-e
	· test portów USB
	· test płyty głównej
	· test procesora
	Wizualna lub dźwiękowa sygnalizacja w przypadku błędów któregokolwiek z powyższych podzespołów komputera.
	Ponadto system powinien umożliwiać identyfikacje testowanej jednostki i jej komponentów w następującym zakresie:
	· PC: Producent, model
	· BIOS: Wersja oraz data wydania Bios
	· Procesor : Nazwa, taktowanie
	· Pamięć RAM : Ilość zainstalowanej pamięci RAM, producent oraz numer seryjny poszczególnych kości pamięci
	· Dysk twardy: model, numer seryjny, wersja firmware, pojemność, temperatura pracy
	System Diagnostyczny działający nawet w przypadku uszkodzenia dysku twardego z systemem operacyjnym komputera.
Zabezpieczenia i zarządzanie	- Obudowa musi umożliwiać zastosowanie zabezpieczenia fizycznego w postaci linki metalowej (złącze blokady Kensingtona)
	- TPM sprzętowy 2.0
	- Czujnik otwarcia obudowy komputera sygnalizujący nieautoryzowany dostęp do takich komponentów jak HDD, RAM, CPU
	- zdalne przejęcie konsoli tekstowej systemu;
Wirtualizacja	Sprzętowe wsparcie technologii wirtualizacji procesorów w BIOS.
Certyfikaty i standardy	
	Deklaracja zgodności
	Certyfikat TCO dla monitora
	Certyfikat zgodności Microsoft, potwierdzający poprawną współpracę oferowanych komputerów z oferowanym systemem operacyjnym
	Głośność jednostki mierzona z pozycji operatora w trybie IDLE max. 20 dB - certyfikat akredytowanej jednostki potwierdzający głośność jednostki
	Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia producenta jednostki
Waga	Waga urządzenia max. 7kg
Wymagania dodatkowe	Suma wymiarów komputera nie powinna być większa nić 115 cm.

	Zasilacz o mocy maksymalnej 140W o sprawności min 88%. Dopuszcza się zastosowanie zasilacza zewnętrznego.
	Klawiatura USB w układzie polskim programisty rozszerzona o możliwość włączenia komputera za pomocą dedykowanego przycisku lub skrótu klawiszowego.
	Mysz optyczna (laserowa) USB z klawiszami oraz rolką (scroll).
	Wbudowany port szeregowy (RS232)
Gwarancja	Minimum 36 miesięcy. Serwis świadczony w miejscu instalacji sprzętu, czas reakcji serwisu w następnym dniu roboczym od zgłoszenia.
	W przypadku awarii, dyski twarde pozostają u Zamawiającego.
	Serwis sprzętu musi być realizowany przez Autoryzowanego Partnera Serwisowego Producenta, posiadającego certyfikat ISO 9001 na świadczenie usług serwisowych - dokumenty potwierdzające załączyć do oferty.
	Oświadczenie producenta komputera, że w przypadku nie wywiązywania się z obowiązków gwarancyjnych oferenta lub firmy serwisującej, przejmie na siebie wszelkie zobowiązania związane z serwisem.
Informacje dodatkowe	Zamawiający zastrzega sobie prawo sprawdzenia pełnej zgodności parametrów oferowanego sprzętu z wymogami niniejszej SIWZ. W tym celu Wykonawcy na wezwanie Zamawiającego dostarczą do siedziby Zamawiającego w terminie 10 dni od daty otrzymania wezwania, próbkę oferowanego sprzętu. . W odniesieniu do programowania mogą zostać dostarczone licencje tymczasowe, w pełni zgodne z oferowanymi. Ocena złożonych próbek zostanie dokonana przez Komisję Przetargową na zasadzie spełnia / nie spełnia. Z badania każdej próbki zostanie sporządzony protokół. Pozytywna ocena próbki będzie oznaczała zgodność próbki (oferty) z treścią SIWZ. Niezgodność próbki z SIWZ chociażby w zakresie jednego parametru podlegającemu badaniu bądź nieprzedłożenie wymaganej próbki w sposób i terminie wymaganym przez Zamawiającego będzie oznaczało negatywny wynik oceny próbki i będzie skutkowało odrzuceniem oferty na podstawie art. 89 ust. 1 pkt 2 ustawy z dnia 29 stycznia 2004 r. Prawo zamówień publicznych (Dz. U. z 2015 r. poz. 2164 ze zm.), tj. z uwagi na fakt, że treść oferty nie odpowiada treści specyfikacji istotnych warunków zamówienia. Szczegółowy sposób przygotowania i złożenia próbek zostanie dostarczony wykonawcom wraz z wezwaniem do złożenia próbek
Systemy operacyjne	**Opis wymagań Systemu operacyjnego**
	Licencje na serwerowy system operacyjny muszą być przypisane do każdego rdzenia procesora fizycznego na serwerze. Licencja musi uprawniać do uruchamiania serwerowego systemu operacyjnego w środowisku fizycznym i nielimitowanej liczbie 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.
	Licencja dostępowa dla 500 urządzeń
	Serwerowy system operacyjny musi posiadać następujące, wbudowane cechy.
	1. Możliwość wykorzystania 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym.
	2. Możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności do 64TB przez każdy wirtualny serwerowy system operacyjny.
	3. Możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania 7000 maszyn wirtualnych.
	4. 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.
	5. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy.

	6. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy.
	7. Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.
	8. Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading.
	9. Wbudowane wsparcie instalacji i pracy na wolumenach, które:
	a) pozwalają na zmianę rozmiaru w czasie pracy systemu,
	b) umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,
	c) umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów,
	d) umożliwiają zdefiniowanie list kontroli dostępu (ACL).
	10. Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.
	11. Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.
	12. Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET
	13. Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.
	14. Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.
	15. Dostępne dwa rodzaje graficznego interfejsu użytkownika:
	a) Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,
	b) Dotykowy umożliwiający sterowanie dotykiem na monitorach dotykowych.
	16. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe,
	17. Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji.
	18. Mechanizmy logowania w oparciu o:
	a) Login i hasło,
	b) Karty z certyfikatami (smartcard),
	c) Wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM),
	19. 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..
	20. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).
	21. Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.
Paramerty	22. Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa.
	23. Pochodzący od producenta systemu serwis zarządzania polityką dostępu do informacji w dokumentach (Digital Rights Management).
	24. Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach.
	25. Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:
	a) Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC,
	b) Usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji:
	i. Podłączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną,
	ii. Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,

	iii. Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza,
	iv. Bezpieczny mechanizm dołączania do domeny uprawnionych użytkowników prywatnych urządzeń mobilnych opartych o iOS i Windows 8.1.
	c) Zdalna dystrybucja oprogramowania na stacje robocze.
	d) Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej
	e) Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:
	i. Dystrybucję certyfikatów poprzez http,
	ii. Konsolidację CA dla wielu lasów domeny,
	iii. Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen,
	iv. Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509.
	f) Szyfrowanie plików i folderów.
	g) Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec).
	h) Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów.
	i) Serwis udostępniania stron WWW.
	j) Wsparcie dla protokołu IP w wersji 6 (IPv6),
	k) Wsparcie dla algorytmów Suite B (RFC 4869),
	l) Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows,
	m) Wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie 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:
	i. Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych,
	ii. Obsługi ramek typu jumbo frames dla maszyn wirtualnych,
	iii. Obsługi 4-KB sektorów dysków,
	iv. Nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra,
	v. Możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API,
	vi. Możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk mode).
	26. 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.
	27. Wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath).
	28. Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego.
	29. Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.
	30. Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF.
	31. Zorganizowany system szkoleń i materiały edukacyjne w języku polskim.
Oprogramowanie do wirtualizacji	
Oprogramowanie do wirtualizacji	Licencje muszą umożliwiać uruchamianie wirtualizacji na oferowanych serwerach fizycznych oraz jednej konsoli do zarządzania całym środowiskiem.
	Wszystkie licencje powinny być dostarczone wraz z 3-letnim wsparciem, świadczonym przez producenta lub dostawcy będącego licencjodawcą oprogramowania.
Konsolidacja	1. Warstwa wirtualizacji musi być rozwiązaniem systemowym tzn. musi być zainstalowana bezpośrednio na sprzęcie fizycznym i nie może być częścią innego systemu operacyjnego.

2. Warstwa wirtualizacji nie może dla własnych celów alokować więcej niż 200MB pamięci operacyjnej RAM serwera fizycznego.
3. Rozwiązanie musi zapewnić Wymóg obsługi wielu instancji systemów operacyjnych na jednym serwerze fizycznym. Wymagana jest Wymóg przydzielenia maszynie większej ilości wirtualnej pamięci operacyjnej niż jest zainstalowana w serwerze fizycznym oraz większej ilości przestrzeni dyskowej niż jest fizycznie dostępna.
4. Oprogramowanie do wirtualizacji musi zapewnić Wymóg skonfigurowania maszyn wirtualnych z możliwością dostępu do 4TB pamięci operacyjnej.
5. Oprogramowanie do wirtualizacji musi zapewnić Wymóg przydzielenia maszynom wirtualnym do 128 procesorów wirtualnych.
6. Rozwiązanie musi umożliwiać łatwą i szybką rozbudowę infrastruktury o nowe usługi bez spadku wydajności i dostępności pozostałych wybranych usług.
7. Rozwiązanie musi w możliwie największym stopniu być niezależne od producenta platformy sprzętowej.
8. Rozwiązanie musi wspierać następujące systemy operacyjne: Windows Server 2012, Windows Server 2012R2, SLES, Ubuntu, RHEL, Solaris dla platformy x86 Debian, CentOS, FreeBSD, ,.
9. Rozwiązanie musi posiadać centralną konsolę graficzną do zarządzania środowiskiem serwerów wirtualnych. Konsola graficzna musi być dostępna poprzez dedykowanego klienta i za pomocą przeglądarek internetowych.
10. Dostęp przez przeglądarkę do konsoli graficznej musi być skalowalny tj. powinien umożliwiać rozdzielenie komponentów na wiele instancji w przypadku zapotrzebowania na dużą liczbę jednoczesnych dostępów administracyjnych do środowiska.
11. Rozwiązanie musi zapewniać zdalny i lokalny dostęp administracyjny do wszystkich serwerów fizycznych poprzez protokół SSH, z możliwością nadawania uprawnień do takiego dostępu nazwanym użytkownikom bez konieczności wykorzystania konta root.
12. Rozwiązanie musi umożliwiać składowanie logów ze wszystkich serwerów fizycznych i konsoli zarządzającej na serwerze Syslog. Serwer Syslog w dowolnej implementacji musi stanowić integralną część rozwiązania.
13. Rozwiązanie musi zapewnić Wymóg monitorowania wykorzystania zasobów fizycznych infrastruktury wirtualnej i zdefiniowania alertów informujących o przekroczeniu wartości progowych.
14. Rozwiązanie musi umożliwiać integrację z rozwiązaniami antywirusowymi firm trzecich w zakresie skanowania maszyn wirtualnych z poziomu warstwy wirtualizacji.
15. Rozwiązanie musi zapewniać Wymóg konfigurowania polityk separacji sieci w warstwie trzeciej, tak aby zapewnić oddzielne grupy wzajemnej komunikacji pomiędzy maszynami wirtualnymi.
16. Oprogramowanie do wirtualizacji musi zapewnić Wymóg wykonywania kopii zapasowych instancji systemów operacyjnych oraz ich odtworzenia w możliwie najkrótszym czasie.
17. Kopie zapasowe muszą być składowane z wykorzystaniem technik de-duplikacji danych.
18. Musi istnieć Wymóg odtworzenia pojedynczych plików z kopii zapasowej maszyny wirtualnej przez osoby do tego upoważnione bez konieczności nadawania takim osobom bezpośredniego dostępu do głównej konsoli zarządzającej całym środowiskiem.
19. Mechanizm zapewniający kopie zapasowe musi być wyposażony w system cyklicznej kontroli integralności danych. Ponadto musi istnieć Wymóg przywrócenia stanu repozytorium kopii zapasowych do punktu w czasie, kiedy wszystkie dane były integralne w przypadku jego awarii.
20. Oprogramowanie do wirtualizacji musi zapewnić Wymóg 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.
21. Oprogramowanie do wirtualizacji musi zapewnić Wymóg klonowania systemów operacyjnych wraz z ich pełną konfiguracją i danymi.
22. Oprogramowanie zarządzające musi posiadać Wymóg przydzielania i konfiguracji uprawnień z możliwością integracji z usługami katalogowymi, w szczególności: Active Directory, Open LDAP.

	23. Platforma wirtualizacyjna musi umożliwiać zastosowanie w serwerach fizycznych procesorów o dowolnej ilości rdzeni.
	24. Rozwiązanie musi umożliwiać tworzenie jednorodnych wolumenów logicznych o wielkości do 62TB.
	25. Rozwiązanie musi zapewniać Wymóg dodawania zasobów w czasie pracy maszyny wirtualnej, w szczególności w zakresie przestrzeni dyskowej.
	26. Rozwiązanie musi posiadać wbudowany interfejs programistyczny (API) zapewniający pełną integrację zewnętrznych rozwiązań wykonywania kopii zapasowych z istniejącymi mechanizmami warstwy wirtualizacyjnej.
	27. Rozwiązanie musi umożliwiać wykorzystanie technologii 10GbE w tym agregację połączeń fizycznych do minimalizacji czasu przenoszenia maszyny wirtualnej pomiędzy serwerami fizycznymi.
	28. Rozwiązanie musi zapewniać Wymóg 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.
	29. Rozwiązanie musi gwarantować współczynnik RPO na poziomie minimum 5 minut
	30. Czas planowanego przestoju usług związany z koniecznością prac serwisowych (np. rekonfiguracja serwerów, macierzy, switchy) musi być ograniczony do minimum.
	31. Oprogramowanie do wirtualizacji musi obsługiwać przełączenie ścieżek SAN (bez utraty komunikacji) w przypadku awarii jednej ze ścieżek.
	32. Oprogramowanie do wirtualizacji musi obsługiwać przełączenie ścieżek LAN (bez utraty komunikacji) w przypadku awarii jednej ze ścieżek.
	33. System musi umożliwiać udostępnianie pojedynczego urządzenia fizycznego (PCIe) jako logicznie separowane wirtualne urządzenia dedykowane dla poszczególnych maszyn wirtualnych.
Wysoka dostępność	34. Rozwiązanie musi mieć Wymóg przenoszenia maszyn wirtualnych w czasie ich pracy pomiędzy serwerami fizycznymi, niezależnie od dostępności współdzielonej przestrzeni dyskowej, różnymi rodzajami wirtualnych przełączników sieciowych.
	35. 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.
	36. Rozwiązanie musi umożliwiać łatwe i szybkie ponowne uruchomienie systemów/usług w przypadku awarii poszczególnych elementów infrastruktury.
	37. Rozwiązanie musi zapewnić bezpieczeństwo danych mimo poważnego uszkodzenia lub utraty sprzętu lub oprogramowania.
	38. Rozwiązanie musi zapewniać mechanizm bezpiecznego, bezprzerwowego i automatycznego uaktualniania warstwy wirtualizacyjnej wliczając w to zarówno poprawki bezpieczeństwa jaki zmianę jej wersji.
	39. 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.
	40. Decyzja o próbie przywrócenia funkcjonalności maszyny wirtualnej w przypadku awarii lub niedostępności serwera fizycznego powinna być podejmowana automatycznie, jednak musi istnieć Wymóg określenia przez administratora czasu po jakim taka decyzja jest wykonywana
Sposób instalacji	41. System musi być jednorodnym środowiskiem, pozwalającym na przerzucanie maszyn wirtualnych pomiędzy maszynami fizycznymi w tzw „locie” online.
	42. System musi zostać wyposażony we wszystkie licencje związane z odtwarzaniem automatycznym środowiska po awarii.
	43. System LDAP/Active Directory domeny dla komputerów PC Windows, musi być sklastrowany jako dwie niezależne maszyny wirtualne. Nie dopuszcza się stosowania zewnętrznych niezwirtualizowanych kontrolerów domeny.
	44. W obszarze wirtualnym musi zostać zainstalowany serwer zwirtualizowany w klastrze active-active, który będzie odpowiadał za centrum certyfikacji wewnętrznej dla podpisów niekwalifikowanych, służących do podpisywania dokumentacji EDM. Certyfikaty musza spływać na komputer podpisującego dokumentację w trakcie logowania do domeny AD. Podpisujący w systemie HIS musi mieć Wymóg wyboru metody podpisywania dokumentu poprzez wewnętrzny podpis, własny podpis kwalifikowany lub e-PUAP.

ważenie obciążenia i przestoje serw	45. Czas planowanego przestoju usług związany z koniecznością prac serwisowych (np. rekonfiguracja serwerów, macierzy, switchy) musi być ograniczony do minimum. Konieczna jest Wymóg przenoszenia usług pomiędzy serwerami fizycznymi, bez przerywania pracy usług.
	46. System musi mieć wbudowany mechanizm kontrolowania i monitorowania ruchu do pamięci masowych oraz ustalania priorytetów dostępu do nich na poziomie konkretnych wirtualnych maszyn.
Usługi konfiguracyjne, instalacyjne	
Wymagania konfiguracyjne i instalacyjne	1. Instalacja i konfiguracja oprogramowania do wirtualizacji serwerów.
	2. Instalacja i konfiguracja do sześciu maszyn wirtualnych.
	3. Przygotowanie templates do wdrożenia kolejnychmaszyn wirtualnych
	4. Podłączenie serwerów i konfiguracja środowiska do współpracy z istniejącymi macierzami dyskowymi EMC vnx 5200.
	5. Rekonfiguracja przestrzeni dyskowej na macierzy EMC vnx 5200.
	6. Rekonfiguracja systemu kopii bezpieczeństwa Networker.
	7. Instalacja środowiska produkcyjnego Active Directory złożonego z dwóch kontrolerów domeny ,serwerów DHCP, serwera aktualizacji WSUS oraz serwera plików.
	8. Konfiguracja serwera czasu korzystającego z zewnętrznego serwera atomowego
	9. Dołączenie do domeny 20 komputerów i zmigrowanie profilu użytkownika do konta domenowego.
	10. Stworzenie topologii drzewa AD dla lokalizacji klienta , podsieci oraz konfiguracja usług DNS.
	11. Konfiguracja do 100 jednostek organizacyjnych, zgodnie z wytycznymi Zamawiającego.
	12. Konfiguracja do 100 grup zabezpieczeń zgodnie z wytycznymi Zamawiającego.
	13. Przygotowanie do szablonów użytkowników.
	14. Przygotowanie do polityk haseł (PSO)
	15. Przygotowanie zasad grupy (instalacja aplikacji, dystrybucja drukarek, mapowanie dysków, Bitlocker)
	16. Konfiguracja i dystrybucja elementów systemu do cyklicznej zmiany haseł lokalnych administratorów komputerów (LAPS)
	17. Konfiguracja usługi certyfikatów (ADCS)
	18. Projekt usługi DHCP w trybie przełączania (failover)
	19. Testy przełączania
	20. Konfiguracja systemu MDT
	21. Przygotowanie do dwóch obrazów systemów
	22. Testy instalacji ZTI oraz LTI na wybranych stacjach roboczych
	23. Konfiguracja usługi katalogowej Active Directory do odzyskiwania usuniętych obiektów
	24. Założenie kont AD dla wszystkich użytkowników na podstawie danych dostarczonych przez zamawiającego w postaci plików Excel-owych.
	25. Opracowanie struktury grup zabezpieczeń i ustalenie praw dostępu do zasobów sieciowych (katalogi na serwerze plików).
	26. Przypisanie kont użytkowników do odpowiednich grup zabezpieczeń.
	27. Konfiguracja obiektów zasad grupy dotyczących automatycznej aktualizacji stacji roboczych.
	28. Instalacja i konfiguracja serwera plików : przygotowanie struktury folderów oraz nadanie odpowiednich uprawnień (dla 10 przykładowych grup),
	29. Opracowanie i wdrożenie skryptów logowania użytkowników mapujących zasoby serwera plików.
	30. Przygotowanie procedury podłączania stacji roboczych do domeny wraz z opracowaniem metody migracji profilu lokalnego roboczych do domeny.
Zakres szkolenie	
Ilość osób	4
Sposób prowadzenia szkolenia	Szkolenie podczas wdrożenia na środowisku, serwerach i komputerach Zamawiającego
	1. Instalacja, uaktualnienie i migracja serwerów i obciążenia roboczego

	1.1.1.Wstęp do oferowanego systemu operacyjnego
	1.1.2.Przygotowanie oraz instalacja serwera w wersji Nano i Core
	1.1.3.Przygotowanie do uaktualnienia i migracji
	1.1.4.Migracja ról serwera i obciążenia roboczego
	1.1.5.Modele aktywacji serwera Windows
	2. Konfiguracja lokalnego magazynu danych
	2.1.1.Zarządzanie dyskami w oferowanym OS
	2.1.2.Zarządzanie wolumenami w oferowanym OS
	3. Wdrażanie rozwiązań magazynu danych typu „Enterprise”
	3.1.1.Przegląd rozwiązań dyskowych typu DAS, NAS i SAN
	3.1.2.Porównanie rozwiązań Fibre Channel, iSCSI oraz FCoE
	3.1.3.Zrozumienie rozwiązań iSNS, DCP (Data Center Bridging) oraz MPIO
	3.1.4.Konfiguracja udostępnień zasobów w oferowanym OS
	4. Wdrażanie rozwiązań „Storage Spaces” oraz deduplikacji danych
	4.1.1.Wdrażanie przestrzeni magazynu dancyh „Storage Spaces”
	4.1.2.Zarządzanie przestrzeniami dyskowymi
	4.1.3.Wdrażanie deduplikacji danych
	5. Instalacja i konfiguracja środowiska maszyn wirtualnych
	5.1.1.Przegląd funkcjonalności środowiska maszyn wirtualnych
	5.1.2.Instalacja środowiska maszyn wirtualnych
	5.1.3.Konfiguracja magazynu danych na środowiska maszyn wirtualnych
	5.1.4.Konfiguracja usług sieciowych na środowisku maszyn wirtualnych
	5.1.5.Konfiguracja maszyn wirtualnych środowiska maszyn wirtualnych
	5.1.6.Zarządzanie maszynami wirtualnymi środowiska maszyn wirtualnych
	6. Instalacja i zarządzanie kontenerami Windows Server
	6.1.1.Przegląd kontenerów w oferowanym OS
	6.1.2.Instalacja kontenerów w oferowanym OS
	6.1.3.Konfiguracja i zarządzanie kontenerami
	7. Przegląd rozwiązań wysokodostępnych oraz odtwarzania danych
	7.1.1.Definiowanie poziomów dostępności
	7.1.2.Planowanie rozwiązań wysokodostępnych oraz odtwarzania danych dotyczących maszyn wirtualnych
	7.1.3.Tworzenie kopii zapasowych i odtwarzanie systemu oraz danych w oferowanym OS
	7.1.4.Wysoka dostępność przy wykorzystaniu klastrów w oferowanym OS
	8. Wdrożenie i zarządzanie klastrami
	8.1.1.Planowanie usługi klastrów
	8.1.2.Tworzenie i konfigurowania klastrów
	8.1.3.Utrzymywanie klastrów
	8.1.4.Rozwiązywanie problemów z usługą klastrów
	8.1.5.Wdrażanie wysokiej dostępności lokacji za pomocą funkcjonalności „Strech clustering”
	9. Wdrażanie usług klastrowych maszyn wirtualnych
	9.1.1.Wdrażanie i zarządzanie wirtualnymi maszynami w klastrze
	9.1.2.Kluczowe cechy maszyn wirtualnych w środowisku klastrowym
Wymagania dotyczące szkolenia	10. Wdrażanie usługi równoważenia obciążenia sieciowego NLB
	10.1.1. Przegląd klastrów NLB
	10.1.2. Konfigurowanie klastra NLB
	10.1.3. Planowanie wdrożenia NLB
	11. Tworzenie i zarządzanie instalacją opartą na obrazach dyskowych
	11.1.1. Wprowadzenie do instalacji opartej na obrazach dyskowych
	11.1.2. Tworzenie i zarządzanie instalacją opartą na obrazach dyskowych przy użyciu MDT
	11.1.3. Środowisko maszyn wirtualnych dla różnych obciążeń roboczych
	12. Zarządzanie, monitorowanie i utrzymanie wdrożeń opartych na maszynach wirtualnych
	12.1.1. Przegląd usługi WSUS i możliwości instalacji
	12.1.2. Zarządzanie procesem uaktualnień za pomocą WSUS
	12.1.3. Przegląd funkcjonalności PowerShell DSC
	12.1.4. Przegląd narzędzi monitorowanie oferowanego OS
	12.1.5. Wykorzystanie monitora wydajności
	12.1.6. Monitorowanie logów wydarzeń

	13. Pojęcia związane Active Directory: domena, drzewo, las, site, LDAP, kerberos, schemat.
	14. Relacje zaufania pomiędzy domenami (podstawy teoretyczne)
	15. Role FSMO kontrolera domeny.
	16. Poziomy funkcjonalności domeny.
	17. Strefy (site) i replikacje.
	18. Konfigurowanie usługi DNS (podstawy)
	19. Podłączanie i odłączanie komputera od domeny .
	20. Automatyczne tworzenie obiektów AD i rekordów w DNS.
	21. Zasady grupy - Group Policy Object (GPO)
	22. Zasady grupy lokalne i domenowe
	23. Zapoznanie z Group Policy Management Console (GPMC)
	24. Tworzenie i zarządzanie Group Policy Object (GPO) : dziedziczenie, wymuszanie polityk, filtrowanie zabezpieczeń, delegowanie uprawnień, wyniki zasad grupy.
	25. Stworzenie polityk GPO wykonujących następujące czynności: - wykonanie skryptu podczas logowania - mapowanie dysków (przez skrypt oraz preferencje) - przekierowanie folderów pulpit i moje dokumenty - stworzenie profili mobilnych - zmiana lokalnych grup zabezpieczeń (dodanie grupy działu IT do administratorów lokalnych) - instalacja aplikacji z paczek MSI na przykładzie np: Acrobat Reader lub Google Chrome - skopiowanie plików na wybrane komputery - usunięcie/dodanie klucza rejestru na wybranych komputerach
	26. Diagnozowanie problemów z politykami (narzędzia gpresult, gpudapte, rsop.msc)
	27. Filtry WMI
	28. Wykorzystanie szablonów administracyjnych ADM/ADMX na przykładzie
	29. Tworzenie i odtwarzanie kopii zapasowych GPO
	30. Zarządzanie usługą DHCP
	31. Zarządzanie serwerem plików
	32. Materiały szkoleniowe obejmujące cały zakres szkolenia powinny zawierać zrzuty z ekranu , filmy instruktarzowe , całość powinna być dostępna w postaci elektronicznej w języku polskim .

Wymagania dodatkowe	
	Okablowanie do serwerów, komputerów niezbędne do pracy i podłączenia do istniejącej infrastruktury leży po stronie Wykonawcy
Wsparcie powdrożeniowe	Zamawiający wymaga wsparcia powdrożeniowego, dla serwerów, oprogramowania wirtualizacyjnego, systemu operacyjnego serwerów oraz wdrożonych usług w tym :
	Wsparcia w okresie gwarancji w wymiarze 32h roboczych w postaci wizyt w siedzibie Zamawiającego
	Wsparcia zdalnego w okresie gearancji w wymiarze 32h roboczych świadczonego drogą elektroniczną lub telefoniczną.