

1 szt. – Serwer

Parametr	Charakterystyka (wymagania minimalne)
Obudowa	- Obudowa Rack o wysokości max 1U 10 slotów na dyski 2.5" - Obudowa wyposażona w panel LCD umieszczony na froncie obudowy, pozwalający jednoznacznie stwierdzić, czy system działa poprawnie i pokazujący podstawowe stany działania serwera w tym adres IP karty zarządzającej - 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/ Apple iOS) przy użyciu jednego z protokołów BLE/ WIFI.
Płyta główna	- Płyta główna z możliwością zainstalowania do dwóch procesorów. - Obsługa procesorów 56 rdzeniowych. - Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym. - Na płycie głównej powinny znajdować się minimum 32 sloty przeznaczone do instalacji pamięci. - Płyta główna powinna obsługiwać do 8TB pamięci RAM.
Chipset	Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych.
Procesor	Zainstalowane dwa procesory min. 16-rdzeniowe, min. 2.0GHz, klasy x86 dedykowane do pracy z zaoferowanym serwerem umożliwiające osiągnięcie wyniku min. 284 w teście SPECrate2017_int_base, dostępnym na stronie www.spec.org, dla oferowanego modelu serwera w konfiguracji dwuprocesorowej.
RAM	128GB DDR5 RDIMM 5600MT/s,
Kontroler RAID	- Sprzętowy kontroler dyskowy, posiadający - Min. 8GB nieulotnej pamięci cache, - Możliwość konfiguracji poziomów RAID: 0, 1, 5, 6, 10, 50, 60. - Wsparcie dla dysków samoszyfrujących - Obsługa dysków 22.5 Gbps SAS, 12 Gbps SAS, and 6 Gbps SATA/SAS

Dyski twarde	- Zainstalowane: 10x dysk SAS o pojemności min. 2.4TB, Hot-Plug - Zainstalowane dwa dyski M.2 NVMe SSD o pojemności min. 480GB Hot-Plug z możliwością konfiguracji RAID 1.
Gniazda PCI	Trzy sloty PCIe LP
Interfejsy sieciowe/FC/SAS	- Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT oraz 2 interfejsy sieciowe 25Gb Ethernet w standardzie SFP28 (porty nie mogą być osiągnięte poprzez karty w slotach PCIe) - Czteroportowa karta 12Gb SAS HBA
Wbudowane porty	4 porty USB w tym min: 1 port USB 3.0 z tyłu obudowy, 1 port micro USB z przodu obudowy 2 port VGA z czego jeden z przodu obudowy - Możliwość rozbudowy o port RS232
Video	Zintegrowana karta graficzna umożliwiającą wyświetlenie rozdzielczości min. 1920x1200
Zasilacze	Redundantne, Hot-Plug min. 1100W klasy Titanium
Elementy montażowe	- Komplet wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych - Ramię (organizer) do kabli ułatwiające wysuwanie serwera do celów serwisowych
System operacyjny/dodatkowe oprogramowanie	Windows Server 2025 Standard na wszystkie oferowane rdzenie lub system równoważny. W przypadku zaoferowania oprogramowania równoważnego do system operacyjnego Windows Server 2025 Standard, oprogramowanie musi spełniać minimalne wymagania zawarte w opisie równoważności „Kryteria stosowane w celu oceny równoważności dla systemu operacyjnego Windows Server 2025” znajdującego się pod tabelą
Bezpieczeństwo	- Zatrask górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardech. - Wbudowany w serwer mechanizm pozwalający na weryfikację niezmienności konfiguracji sprzętowej serwera od momentu produkcji do dostawy do docelowej lokalizacji. Mechanizm ma również pozwalać na kontrolę otwarcia urządzenia w trakcie transportu, niezależnie od stanu zasilania. - 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.

	• Moduł TPM 2.0 V3 • Możliwość dynamicznego włączania i wyłączania portów USB na obudowie – bez potrzeby restartu serwera • Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem • Serwer musi być wyposażony w rozwiązanie zapewniające ochronę oprogramowania układowego przed manipulacją złośliwego oprogramowania. Ochrona taka musi być zgodna z zaleceniami NIST SP 800-147B i NIST SP 800-155. Jednocześnie Zamawiający wymaga, aby dostarczony serwer posiadał zaimplementowane sprzętowo mechanizmy kryptograficzne poświadczające integralność oprogramowania BIOS (Root of Trust).
Karta Zarządzania	• Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowane port RJ-45 Gigabit Ethernet umożliwiające: ○ 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 ○ Automatyczne tworzenie kopii ustawień serwera w opraciu o harmonogram. ○ Możliwość wykrywania odchyłeń konfiguracji na poziomie konfiguracji UEFI oraz wersji firmware serwera

	○ Serwer musi posiadać możliwość uruchomienia funkcjonalności umożliwiającej dostęp bezpośredni poprzez urządzenia mobilne - serwer musi posiadać możliwość konfiguracji oraz monitoringu najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej min. (Android/ Apple iOS) przy użyciu jednego z protokołów BLE lub WIFI. Możliwość rozszerzenia funkcjonalności karty o: ○ możliwość wysyłania danych o stanie procesora, kart sieciowych, zasilaczy, kart GPU, lokalnych dysków i urządzeń NVMe, jak również dane wydajnościowe serwera do zewnętrznych narzędzi analitycznych jak Splunk, Grafana, Elasticsearch ○ kontrola stanu BIOS pod kątem naruszenia integralności oprogramowania ○ Automatyczne odświeżanie certyfikatów SSL ○ możliwość wykorzystania tokenu lub aplikacji SecurID do uwierzytelniania wielokrotnego przy logowaniu do karty zarządzającej ○ możliwość modyfikacji reguł chłodzenia kart w slotach PCIe, z możliwością własnych ustawień ○ możliwość ustawienia limitu temperatury powietrza wychodzącego z serwera ○ możliwość ustawienia dopuszczalnego wzrostu temperatury powietrza przepływającego przez serwer ○ możliwość ustawienia maksymalnej temperatury powietrza dochodzącego do slotów PCIe ○ monitorowanie przepływu powietrza na bieżąco (w CFM)
Oprogramowanie do zarządzania	● Możliwość zainstalowania oprogramowania producenta do zarządzania, spełniającego poniższe wymagania: ○ Wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych ○ integracja z Active Directory ○ Możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta ○ Wsparcie dla protokołów SNMP, IPMI, Linux SSH, Redfish ○ Możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram ○ Szczegółowy opis wykrytych systemów oraz ich komponentów ○ Możliwość eksportu raportu do CSV, HTML, XLS, PDF ○ Możliwość tworzenia własnych raportów w oparciu o wszystkie informacje zawarte w inwentarzu. ○ Grupowanie urządzeń w oparciu o kryteria użytkownika ○ Tworzenie automatycznie grup urządzeń w oparciu o dowolny element konfiguracji serwera np. Nazwa, lokalizacja, system operacyjny, obsadzenie slotów PCIe, pozostałego czasu gwarancji ○ Możliwość uruchamiania narzędzi zarządzających w poszczególnych urządzeniach ○ Szybki podgląd stanu środowiska ○ Podsumowanie stanu dla każdego urządzenia ○ Szczegółowy status urządzenia/elementu/komponentu

- Generowanie alertów przy zmianie stanu urządzenia.
- Filtry raportów umożliwiające podgląd najważniejszych zdarzeń
- Integracja z service desk producenta dostarczonej platformy sprzętowej
- Możliwość przejęcia zdalnego pulpitu
- Możliwość podmontowania wirtualnego napędu
- Kreator umożliwiający dostosowanie akcji dla wybranych alertów
- Możliwość importu plików MIB
- Przesyłanie alertów „as-is” do innych konsol firm trzecich
- Możliwość definiowania ról administratorów
- Możliwość zdalnej aktualizacji oprogramowania wewnętrznego serwerów
- Aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania)
- Możliwość instalacji oprogramowania wewnętrznego bez potrzeby instalacji agenta
- Możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów
- Moduł raportujący pozwalający na wygenerowanie następujących informacji: nr seryjne sprzętu, konfiguracja poszczególnych urządzeń, wersje oprogramowania wewnętrznego, obsadzenie slotów PCI i gniazd pamięci, informację o maszynach wirtualnych, aktualne informacje o stanie i poziomie gwarancji, adresy IP kart sieciowych, występujących alertów, MAC adresów kart sieciowych, stanie poszczególnych komponentów serwera.
- Możliwość tworzenia sprzętowej konfiguracji bazowej i na jej podstawie weryfikacji środowiska w celu wykrycia rozbieżności.
- Wdrażanie serwerów, rozwiązań modularnych oraz przełączników sieciowych w oparciu o profile
- Możliwość migracji ustawień serwera wraz z wirtualnymi adresami sieciowymi (MAC, WWN, IQN) między urządzeniami.
- Tworzenie gotowych paczek informacji umożliwiających zdiagnozowanie awarii urządzenia przez serwis producenta.
- Zdalne uruchamianie diagnostyki serwera.
- Dedykowana aplikacja na urządzenia mobilne integrująca się z wyżej opisanymi oprogramowaniem zarządzającym.
- Oprogramowanie dostarczane jako wirtualny appliance dla KVM, ESXi i Hyper-V.

Oprogramowanie do monitorowania

Oparta na chmurze aplikacja Producenta oferowanego urządzenia, która zapewnia proaktywne monitorowanie i rozwiązywanie problemów infrastruktury IT oraz integrację z posiadaną platformą wirtualizacji VMware. Zaproponowane rozwiązanie musi posiadać następujące funkcjonalności:

- Monitoring:
 - ilość podłączonych oraz rozłączonych systemów
 - stan podłączonych urządzeń
 - informacje o potencjalnych zagrożeniach związanych z cyberbezpieczeństwem w oparciu o najlepsze praktyki i szczegółową analizę posiadanych systemów

- Informacje o alertach z podziałem na minimum: krytyczne, błędy, ostrzeżenia
- informacje o statusie gwarancji dla poszczególnych urządzeń
- informacje o stanie licencji na posiadane oprogramowanie rozszerzające funkcjonalności urządzeń
- informacje w oparciu o dane historyczne umożliwiające określenie trendów krótko- i długoterminowej prognozy wykorzystania przestrzeni na pamięciach masowych.
- Wykrywanie anomalii w oparciu o analizę zajętości przestrzeni na pamięciach masowych
- Wykrywanie anomalii wydajnościowych w oparciu o uczenie maszynowe oraz porównanie parametrów historycznych i bieżących. Funkcjonalność ta musi wspierać serwery, urządzenia sieciowe oraz systemy pamięci masowych.
- Monitorowanie wydajności, przepustowości oraz opóźnień dla systemy pamięci masowych.
- Zaimplementowana analityka predykcyjna umożliwiająca określenie szacowanego czasu awarii dla optyki przełączników FC.
- Szczegółowe informacje dla serwerów o modelu, konfiguracji, wersjach firmware poszczególnych komponentów adresacji IP karty zarządzającej.
- Monitoring parametrów serwerów z informacją o minimum:
 - Obciążeniu procesora
 - Zużyciu pamięci RAM
 - Temperaturze procesorów
 - Temperaturze powietrza wlotowego
 - Zużyciu prądu
 - Zmianach w fizycznej konfiguracji serwera
 - Dla wszystkich wymienionych parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach.
- Monitoring parametrów pamięci masowych z informacją o minimum:
 - Opóźnieniach
 - IOPS
 - Przepustowości
 - Utylizacji kontrolerów
 - Pojemność całkowita i dostępna
 - Wszystkie informacje muszą być dostępne zarówno dla całej pamięci masowej jak i poszczególnych LUN-ów.
 - Dla wszystkich wymienionych powyżej parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach.
 - Dane historyczne o wykorzystaniu przestrzeni pamięci masowej muszą być przechowywane co najmniej 2 lata
 - Informacje o poziomie redukcji danych
 - Informacje o statusie replikacji oraz snapshotów
- Monitoring parametrów przełączników sieciowych z informacją o minimum:
 - Modelu, oprogramowania, adresacji IP, MAC adres, nr seryjny
 - Stanie komponentów: zasilacze, wentylatory
 - Podłączonych hostach

- Ilości i statusu portów
 - Utylizacji procesora
 - Utylizacji poszczególnych portów
 - Dla wszystkich wymienionych powyżej parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach.
- Aktualizacja firmware
 - możliwość aktualizacji firmware, oprogramowania zarządzającego dla systemów pamięci masowych, wraz z informacją o zalecanych wersjach oprogramowania
 - możliwość aktualizacji firmware, oprogramowania zarządzającego dla serwerów, wraz z informacją o zalecanych wersjach oprogramowania
 - możliwość aktualizacji firmware, oprogramowania zarządzającego dla rozwiązań HCI, wraz z informacją o zalecanych wersjach oprogramowania
 - możliwość aktualizacji firmware, dla systemów przełączników FC, wraz z informacją o zalecanych wersjach oprogramowania
 - możliwość aktualizacji firmware, dla deduplikatorów, wraz z informacją o zalecanych wersjach oprogramowania
- Raporty
 - Możliwość generowania raportów dla serwerów zawierających informację o:
 - Nazwie hosta, modelu serwera, nr serwisowym, dacie końca okresu kontraktu serwisowego, zainstalowanym systemie operacyjnym, protokole komunikacyjnym z systemem pamięci masowej
 - Średnim obciążeniu: procesorów, pamięci RAM, IO,
 - Możliwość generowania raportów dla systemów pamięci masowych zawierających informację o:
 - Nazwie, nr seryjnym, lokalizacji urządzenia, modelu urządzenia, wersji oprogramowania, zajętości systemu oraz poziomu redukcją danych, informacje o utworzonych LUN-ach i systemach pliku, status replikacji
 - Generowanie raportów do plików CSV i PDF
- Cyberbezpieczeństwo
 - Analiza środowiska w oparciu o najlepsze praktyki dotyczące cyberbezpieczeństwa sprawdzająca stan poszczególnych urządzeń w środowisku i przypisujący im odpowiedni wynik bezpieczeństwa. System musi informować administratora o wykrytych lukach bezpieczeństwa oraz sposobie ich zabezpieczenia.
 - Musi istnieć możliwość tworzenia własnych polityk bezpieczeństwa w oparciu o wzorce dla poszczególnych urządzeń.
 - Stała analiza środowiska IT umożliwiająca wykrycie ataku ransomware na podstawie analizy posiadanych danych.
 - Możliwość przypisania dedykowanych ról dla poszczególnych administratorów.
- Wspierane urządzenia
 - Urządzenie Producenta dostarczane w ramach postępowania
 - Posiadane przez Zamawiającego serwery, urządzenia pamięci masowych, przełączniki sieciowe, przełączniki SAN, rozwiązania HCI, deduplikatory Producenta oferowanego urządzenia (jeśli takie są w posiadaniu Zamawiającego)
- Wirtualny asystent

	○ Wbudowana w platformę funkcjonalność wirtualnego asystenta w oparciu o algorytmy GenAI przy dostępie do bazy wiedzy producenta urządzeń oraz analizie danych z monitoringu poszczególnych elementów infrastruktury; • Możliwość rozszerzenia funkcjonalności ○ Możliwość rozbudowy systemu o zintegrowane i dodatkowe płatne moduły do monitoringu aplikacji oraz zarządzania incydentami w ramach infrastruktury IT. • Inne ○ Oferowana platforma musi posiadać dedykowaną aplikację na urządzenia iOS oraz Android
Certyfikaty	• Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015, ISO-50001 oraz ISO-14001 • Serwer musi posiadać deklaracja CE. • Oferowane produkty muszą zawierać informacje dotyczące ponownego użycia i recyklingu, nie mogą zawierać farb i powłok na dużych plastikowych częściach, których nie da się poddać recyklingowi lub ponownie użyć. Wszystkie produkty zawierające podzespoły elektroniczne oraz niebezpieczne składniki powinny być bezpiecznie i łatwo identyfikowalne oraz usuwalne. Usunięcie materiałów i komponentów powinno odbywać się zgodnie z wymogami Dyrektywy WEEE 2002/96/EC. Produkty muszą składać się z co najmniej w 65% ze składników wielokrotnego użytku/zdatnych do recyklingu. We wszystkich produktach części tworzyw sztucznych większe niż 25-gramowe powinny zawierać nie więcej niż śladowe ilości środków zmniejszających palność sklasyfikowanych w dyrektywie RE 67/548/EEC. Potwierdzeniem spełnienia powyższego wymogu jest wydruk ze strony internetowej www.epeat.net potwierdzający spełnienie normy co najmniej Epeat Silver według normy wprowadzonej w 2019 roku - Wykonawca złoży dokument potwierdzający spełnianie wymogu.
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.
Warunki gwarancji	• Zamawiający wymaga zapewnienia gwarancji Producenta z zakresu wdrażanej technologii na okres 5 lat. • Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie i przez Internet. • Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania Producenta, w tym także sprzedanego oprogramowania. • Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy. • Certyfikowany Technik Producenta z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) powinien rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym (NBD) od zakończenia diagnostyki. • Naprawa ma się odbyć w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę. • Zamawiający oczekuje nieodpłatnego udostępnienia narzędzi serwisowych i procesów wsparcia umożliwiających: Wykrywanie usterek sprzętowych z predykcją awarii, automatyczną diagnostykę i zdalne otwieranie zgłoszeń

serwisowych, wskazówki dotyczące bezpieczeństwa produktów, samodzielne wysyłanie części, a także ocena bezpieczeństwa cybernetycznego.

- 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.
- Możliwość rozszerzenia gwarancji producenta o usługę diagnostyki sprzętu na miejscu w przypadku awarii. Charakterystyka usługi diagnostyki:
 - Możliwości utworzenia zgłaszania serwisowego w wyniku, którego proces diagnostyki odbędzie się na miejscu w siedzibie zamawiającego.
 - Po przyjeździe do siedziby Zamawiającego, pracownik serwisu przystąpi do rozwiązywania problemu. Jeśli do rozwiązania problemu będzie konieczna dodatkowa pomoc diagnostyczna lub części, pracownik serwisu może w imieniu Zamawiającego skontaktować się z producentem w celu uzyskania pomocy.
 - Reakcja na miejscu u Zamawiającego powinna nastąpić w okresie zgodnym z czasem reakcji przypisanym do urządzenia, które posiada wykupioną usługę serwisową.
 - Pracownik serwisu powinien skontaktować się z Zamawiającym przed przyjazdem na miejsce w celu sprawdzenia zgłoszenia, ustalenia harmonogramu i potwierdzenia wszelkich informacji niezbędnych do realizacji wizyty technika na miejscu.
 - Jeśli w trakcie wstępnego procesu rozwiązywania problemu na miejscu awarii zostanie ustalone, że do realizacji usługi jest niezbędna jakaś część, znajdujący się na miejscu pracownik serwisu zamówi nową część i przekaże dodatkowe zgłoszenie do działu obsługi technicznej. Technik pracujący na miejscu powróci do siedziby Klienta w celu wymiany wysłanej części w ciągu czasu reakcji ustalonego zgodnie z umową serwisową zakupionego produktu.
- Wymagane dołączenie do oferty oświadczenia Producenta potwierdzające, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta.
- Firma serwisująca musi posiadać ISO 9001:2015 oraz ISO-27001 na świadczenie usług serwisowych oraz posiadać autoryzację producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty.

Kryteria stosowane w celu oceny równoważności dla systemu operacyjnego Windows Server 2025 Standard:

Zakres Przedmiotu Zamówienia obejmuje dostarczenie Oprogramowania Systemowego zwanego dalej SSO, pokrywającego licencyjnie wszystkie rdzenie oferowanych procesorów.

Licencja musi uprawniać do uruchamiania SSO w środowisku fizycznym minimum dwóch wirtualnych środowisk SSO za pomocą wbudowanych mechanizmów wirtualizacji.

SSO musi posiadać następujące, wbudowane cechy:

- 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 minimum 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:
 - 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 zaporą 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:
 - 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:
 - 1) podłączenie 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,
 - III. zdalna dystrybucja oprogramowania na stacje robocze,

IV. praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej,

V. centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:

- 1) dystrybucję certyfikatów poprzez http,
- 2) konsolidację CA dla wielu lasów domeny,
- 3) automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen,

VI. szyfrowanie plików i folderów,

VII. szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec),

VIII. możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów,

IX. serwis udostępniania stron WWW,

X. wsparcie dla protokołu IP w wersji 6 (IPv6),

XI. wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie minimum 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:

- 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. Dodatkowo licencja pozwalająca na łączenie się z zasobami serwera dla 26 użytkowników.