



Załącznik nr 1 do szacowania

Spis treści

1. Zakup serwera dla Urzędu Gminy w Radkowie wraz z wdrożeniem i konfiguracją.....	1
2. Zakup serwera NAS wraz z instalacją i konfiguracją.....	12

1. Zakup serwera dla Urzędu Gminy w Radkowie wraz z wdrożeniem i konfiguracją

Komponent	Minimalne wymagania
Obudowa	Obudowa typu Tower z możliwością instalacji do 8 dysków twardych 3.5”.
Płyta główna	- Płyta główna z możliwością instalacji jednego fizycznego procesora, - Płyta główna posiadająca minimum 4 sloty na pamięć RAM UDIMM, z możliwością zainstalowania do minimum 128GB pamięci RAM. - Płyta główna zaprojektowana przez producenta serwera i oznaczona trwale jego znakiem firmowym.
Procesor	Zainstalowany jeden procesor 6-rdzeniowy, 3.3GHz, klasy x86 dedykowany do pracy z zaoferowanym serwerem umożliwiający osiągnięcie wyniku min. 68.5 w teście SPECrate2017_int_base w konfiguracji jedno procesorowej, dostępnym na stronie www.spec.org.
Pamięć RAM	1x 32GB UDIMM 5600MT
Kontroler RAID	Sprzętowy kontroler dyskowy, posiadający możliwość konfiguracji poziomów RAID: 0, 1, 10
Dyski twarde	- Zainstalowane: 4x dysk SSD SATA o pojemności 960GB, Hot-Plug - Możliwość zainstalowania dwóch dysków M.2 NVMe o pojemności min. 960GB Hot-Plug z możliwością konfiguracji RAID 1.
Sloty PCI Express	Cztery sloty PCIe
Interfejsy sieciowe/FC/SAS	Minimum dwa interfejsy sieciowe 1Gb Ethernet w standardzie BaseT
Wbudowane porty	- Minimum 8 portów USB z czego min. 4 w technologii 3.0 1x RS-232 1x VGA
Video	Zintegrowana karta graficzna, umożliwiająca wyświetlanie obrazu w rozdzielczości minimum 1280x1024 pikseli
Zasilanie	Redundantne zasilacze o mocy 700W klasy Titanium



**System
operacyjny/dodatkowe
oprogramowanie**

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

Licencja musi uprawniać do uruchamiania SSO w środowisku fizycznym nielimitowanej ilości 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 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:
 - 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 zapora internetowa (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, udział 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 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: 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. Zamawiający wymaga dostarczenia dodatkowo licencji dostępowych dla minimum 10 użytkowników.
Diagnostyka i Bezpieczeństwo	• zintegrowany z płytą główną moduł TPM 2.0 • 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 • 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). Wymagane dołączenie do oferty oświadczenia Producenta potwierdzającego spełnienie powyższych zaleceń.
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 wewnętrznych 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 modułarnych 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 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
 - Pojemności 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 ○ Oferowana platforma musi być zaprojektowana zgodnie ze standardami: ▪ ISO 27001 ▪ NIST Security and Privacy Controls for Federal Information Systems and Organization ▪ CSA Cloud Control Matrix
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 4 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. • Zgłoszenie przyjęte jest potwierdzane przez zespół pomocy technicznej (mail/telefon / portal) przez nadanie unikalnego numeru zgłoszenia pozwalającego na identyfikację zgłoszenia w trakcie realizacji naprawy i po jej zakończeniu. • 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 otrzymania zgłoszenia / zakończenia diagnostyki. Naprawa ma się odbyć w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę. • 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. • 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 rozwiązywania 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. • Firma serwisująca musi posiadać ISO 9001:2015 oraz ISO-27001 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty.
Wymagania dodatkowe	Zamawiający wymaga wdrożenia w zakresie minimum: - instalacji w miejscu wskazanym przez Zamawiającego -konfiguracji podstawowej oraz aktualizacji oprogramowania.
Ilość	1 szt

2. Zakup serwera NAS wraz z instalacją i konfiguracją

Komponent	Minimalne wymagania
Procesor	Procesor 64 bit x86 o taktowaniu nie mniejszym niż 2.2 GHz
Procesor liczba rdzeni	Nie mniej niż 4
Pamięć RAM	Nie mniej niż 8GB
Pamięć RAM liczba slotów	Minimum 2 sloty
Pamięć RAM - możliwość rozszerzenia	Nie mniej niż do 64GB
Pamięć Flash	Nie mniej niż 5 GB
Liczba zatok na dyski	Minimum 8 zatok 3,5"
Obsługiwane dyski twarde	3.5" SATA oraz 2.5" SATA oraz 2.5" SATA SSD
Możliwość stosowania dysków twardych o pojemnościach	do 22TB
Zainstalowane dyski	Minimum 4 dyski o parametrach minimum 10TB SATA III 7200 obr./min
Możliwość podłączenia modułu rozszerzającego	Tak, co najmniej 2
Porty LAN 2,5 GbE	Minimum 2 RJ-45
Diody LED	Minimum Status, LAN, HDD,
Porty USB	Minimum 3 x typu A USB 3.2 Gen 2 10 Gb/s Minimum 1 x typu C USB 3.2 Gen 1 5 Gb/s
Port PCIe	Tak, minimum 2xGen 3x4
Przyciski	Reset, Zasilanie
Typ obudowy	Tower



Fundusze Europejskie
na Rozwój Cyfrowy



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



CENTRUM
PROJEKTÓW
POLISA
CYFROWA

Dopuszczalna temperatura pracy	od 0 do 40°C
Wilgotność względna podczas pracy	5-95% R.H.
Zasilanie	Max. 250 W
Typ obudowy	Tower
Dopuszczalna temperatura pracy	od 0 do 40°C
Wilgotność względna podczas pracy	5-95% R.H.
Zasilanie	Max. 250 W
Agregacja łącz	Tak
Obsługiwane systemy plików	Dyski wewnętrzne: EXT4 Dyski zewnętrzne: EXT3, EXT4, NTFS, FAT32, HFS+, exFAT
Możliwość podłączenia karty WLAN na USB	Tak
Szyfrowanie udziałów	Tak, min AES 256
Szyfrowanie dysków zewnętrznych	Tak
Zarządzanie dyskami	Pojedynczy Dysk, 0, 1, 5, 6, 10, JBOD, Obsługa Hot Spare per grupa RAID oraz global hot spare Rozszerzanie pojemności Online RAID Migracja poziomów Online RAID HDD S.M.A.R.T. Skanowanie uszkodzonych bloków Przywracanie macierzy RAID Obsługa map bitowych Pula pamięci masowej Obsługa migawek Obsługa replikacji migawek
Wbudowana obsługa iSCSI	Multi-LUNs na Target Obsługa LUN Mapping & Masking Obsługa SPC-3 Persistent Reservation Obsługa MPIO & MC/S, Migawka / kopia zapasowa iSCSI LUN



Fundusze Europejskie
na Rozwój Cyfrowy



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



CENTRUM
PROJEKTÓW
POLSEA
CYFROWA

Zarządzanie prawami dostępu	Ograniczenie dostępnej pojemności dysku dla użytkownika Importowanie listy użytkowników Zarządzanie kontami użytkowników Zarządzanie grupą użytkowników Zarządzanie współdzieleniem w sieci Tworzenie użytkowników za pomocą makr Obsługa zaawansowanych uprawnień dla podfolderów, Windows ACL
Obsługa Windows AD	Logowanie użytkowników poprzez CIFS/SMB, AFP, FTP oraz menadżera plików sieci Web Funkcja serwera LDAP
Funkcje backup	Oprogramowanie do tworzenia kopii bezpieczeństwa plików producenta urządzenia dla systemów Windows, backup na zewnętrzne dyski twarde,
Współpraca z zewnętrznymi dostawcami usług chmury	Przynajmniej: Google Drive, Dropbox, Microsoft OneDrive, Microsoft OneDrive for Business i Box
Darmowe aplikacje na urządzenia mobilne	Monitoring / Zarządzanie / Współdzielenie plików / obsługa kamer Dostępne na systemy iOS oraz Android
Minimum obsługiwane serwery	Serwer plików Serwer FTP Serwer WEB Serwer kopii zapasowych Serwer multimediiów UPnP Serwer pobierania (Bittorrent / HTTP / FTP) Serwer Monitoringu
VPN	VPN client / VPN server Obsługa PPTP, OpenVPN
Administracja systemu	Połączenia HTTP/HTTPS Powiadamianie przez e-mail (uwierzytelnianie SMTP) Powiadamianie przez SMS Ustawienia inteligentnego chłodzenia DDNS oraz zdalny dostęp w chmurze SNMP (v2 & v3) Obsługa UPS z zarządzaniem SNMP (USB) Obsługa sieciowej jednostki UPS Monitor zasobów Kosz sieciowy dla CIFS/SMB oraz AFP Monitor zasobów systemu w czasie rzeczywistym Rejestr zdarzeń System plików dziennika Całkowity rejestr systemowy (poziom pliku) Zarządzanie zdarzeniami systemowymi, rejestr, bieżące połączenie użytkowników on-line Aktualizacja oprogramowania automatyczna



Fundusze Europejskie
na Rozwój Cyfrowy



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



CENTRUM
PROJEKTÓW
POLSEA
CYFROWA

	Możliwość aktualizacji oprogramowania ręcznie Ustawienia systemu: Kopia, Przywracanie, Resetowanie
Wirtualizacja	Wbudowana aplikacja umożliwiająca tworzenie środowiska wirtualnego wraz z instalacją maszyn wirtualnych na systemach Windows, Linux i Android. Dostęp do konsoli maszyn za pośrednictwem przeglądarki z HTML5 Funkcjonalności importu, eksportu, klonowania i wykonywania migawek maszyn wirtualnych.
Konteneryzacja	Możliwość uruchomienia wirtualnych kontenerów dla LXD i Docker
Zabezpieczenia	Filtracja IP Ochrona dostępu do sieci z automatycznym blokowaniem Połączenie HTTPS FTP z SSL/TLS (Explicit) Obsługa SFTP (tylko admin) Szyfrowanie AES 256-bit Szyfrowana zdalna replikacja (Rsync poprzez SSH) Import certyfikatu SSL Powiadomienia o zdarzeniach za pośrednictwem Email i SMS
Możliwość instalacji dodatkowego oprogramowania	Tak, sklep z aplikacjami; możliwość instalacji z paczek
Gwarancja	Minimum 3 lata
Agregacja łączy	Tak
Obsługiwane systemy plików	Dyski wewnętrzne: EXT4 Dyski zewnętrzne: EXT3, EXT4, NTFS, FAT32, HFS+, exFAT
Możliwość podłączenia karty WLAN na USB	Tak
Szyfrowanie udziałów	Tak, min AES 256
Ilość	1 szt.