**Załącznik Nr 1 do SWZ**

**Opis przedmiotu zamówienia:**

Przedmiotem zamówienia jest dostawa i uruchomienie fabrycznie nowych serwerów wraz macierzami oraz systemem operacyjnym.

1. **Ogólne warunki realizacji zamówienia**:
2. Przedmiot zamówienia obejmuje dostarczenie do siedziby Zamawiającego, instalację oraz uruchomienie niżej wymienionych elementów w ilościach wskazanych w zestawieniu rzeczowo - ilościowym poniżej.
3. Dostarczany sprzęt i oprogramowanie muszą być fabrycznie nowe, nieużywane, nieuszkodzone i nieobciążone prawami osób trzecich.
4. Wykonawca zapewni takie opakowanie sprzętu jakie jest wymagane, żeby nie dopuścić do jego uszkodzenia lub pogorszenia jego jakości w trakcie transportu do miejsca dostawy.
5. Sprzęt będzie oznaczony zgodnie z obowiązującymi przepisami, a w szczególności znakami bezpieczeństwa.
6. **Wymagania ogólne dla urządzeń i oprogramowania**:
7. Wszystkie urządzenia muszą być ze sobą kompatybilne.
8. Wszystkie serwery, macierz oraz przełączniku FC muszą pochodzić od tego samego producenta w celu zapewnienia centralnego zarządzania.
9. Dostarczony sprzęt musi pochodzić z oficjalnego kanału sprzedaży producenta na rynek polski.
10. Elementy, z których zbudowane są serwery oraz macierz muszą być produktami producenta tych urządzeń lub być przez niego certyfikowane oraz muszą być objęte gwarancją producenta. Na żądanie Zamawiającego, Wykonawca dostarczy wraz ze sprzętem oświadczenia producenta potwierdzające, że oferowany sprzęt spełnia te wymogi.
11. Nie dopuszcza się urządzeń posiadających wadę prawną w zakresie pochodzenia sprzętu, wsparcia technicznego i gwarancji producenta. Urządzenia i ich komponenty muszą być oznakowane w taki sposób, aby możliwa była identyfikacja zarówno produktu jak i producenta.
12. Urządzenia muszą być dostarczone Zamawiającemu w oryginalnych opakowaniach producenta. Do każdego urządzenia musi być dostarczony komplet standardowej dokumentacji dla użytkownika w języku polskim lub angielskim w formie papierowej lub elektronicznej.
13. Wykonawca wyda Zamawiającemu instrukcje obsługi sprzętu lub – jeśli są one udostępniane przez producenta w formie elektronicznej – przekaże adresy stron internetowych, pod którymi można je pobrać.
14. Dla oprogramowania Wykonawca zobowiązany jest do udzielenia niewyłącznej licencji Zamawiającemu lub przeniesienia na Zamawiającego niewyłącznego uprawnienia licencyjnego zgodnego z zasadami licencjonowania określonymi przez producenta.

1. Główne serwery komunikacyjne – 2 szt. spełniające poniższe wymagania.

|  |  |
| --- | --- |
| **Nazwa elementu,** **parametru lub cechy**  | **Opis wymagań serwerów**  |
| **Obudowa**  | Do instalacji w szafie Rack 19”, wysokość nie więcej niż 2U, z zestawem szyn do mocowania w szafie i wysuwania do celów serwisowych.  |
| **Procesor**  | Architektura x86, maksymalny TDP dla procesora – 185W. Wymagana ilość rdzeni dla procesora – min. 16, taktowanie procesora nie niższe niż 2.5GHz. Ilość linków UPI min. 3. Wynik wydajności procesorów zainstalowanych w oferowanym serwerze nie może być niższy niż 320 punktów 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. Do oferty należy załączyć wydruk z wynikiem testu.Procesor musi zapewniać obsługę pamięci DDR5. |
| **Liczba zainstalowanych procesorów**  | Min. 2 szt. |
| **Płyta główna**  | Płyta główna dedykowana do pracy w serwerach, wyprodukowana przez producenta serwera z możliwością zainstalowania do dwóch procesorów Intel Xeon wykonujących 64-bitowe instrukcje  |
| **Pamięć operacyjna**  | Zainstalowane minimum 256GB pamięci RAM o częstotliwości 4800MHz. Zainstalowana pamięć musi być sygnowana i zoptymalizowana do użycia przez producenta serwera. Minimum 32 sloty na pamięć. Serwer musi posiadać możliwość rozbudowy pamięci do 8TB RAM.  |
| **Zabezpieczenie pamięci**  | Memory mirroring, ECC, SDDC, ADDDC  |
| **Procesor Graficzny**  | Zintegrowana karta graficzna z minimum 16MB pamięci osiągająca rozdzielczość 1920x1200 przy 60 Hz.  |
| **Dyski** | Zainstalowane min. 3 szt. dysków SSD o pojemności min. 480GB typu Read Intensive. |
| **Rozbudowa dysków**  | Serwer musi posiadać możliwość rozbudowy na potrzeby zainstalowania minimum 24 dysków SAS/SATA 2,5” z przodu serwera oraz 8 dysków SAS/SATA 2,5” z tyłu serwera. Dodatkowo wymaga się, aby serwer posiadał możliwość rozbudowy umożliwiającą instalację dysków NVMe. Wymaga się możliwości wyposażenia serwera w zatoki umożliwiające wymiennie instalację dysków SAS/SATA oraz dysków NVMe (ta sama zatoka). W momencie dostawy serwer musi posiadać elementy umożliwiające instalacje 8 dysków SAS/SATA hot plug.Serwer musi posiadać możliwość instalacji napędu Flash w wewnętrznym porcie USB serwera.  |
| **Kontroler dyskowy**  | Zainstalowany kontroler 12 Gb SAS/SATA z obsługą RAID 0, 1, 10, 5.Serwer musi posiadać możliwość rozbudowy na potrzeby zainstalowania kontrolera dyskowego z 8GB Cache wykorzystującego pamięć flash NAND będącego w ofercie producenta serwera. Kontroler powinien posiadać funkcjonalność podtrzymania napięcia w przypadku utraty głównego zasilania w technologii nie wykorzystującej jakiegokolwiek rozwiązania bateryjnego. Kontroler taki dedykowany do ofertowanego serwera powinien być w ofercie producenta serwera. Kontroler powinien obsługiwać następujące poziomy zabezpieczeń RAID 0/1/10/5/50/6/60. 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. Kontroler powinien mieć możliwość jednoczesnej obsługi dysków SAS/SATA oraz dysków NVMe.  |
| **Zasilacz**  | Minimum dwa redundantne zasilacze o mocy minimum 1100W z certyfikatem minimum Titanium. Moc pojedynczego zasilacza musi być wystarczająca do zasilenia serwera w oferowanej konfiguracji. Zasilacze wyposażone w kable zasilające posiadające wtyk typu C14. |
| **Interfejsy sieciowe**  | 4 porty 10Gbs RJ45. Interfejsy te nie mogą wpływać na ilość dostępnych slotów PCIe wymienionych w sekcji dodatkowe sloty I/O.Zainstalowana jedna dwuportowa karta FC 16Gbs.Jeden port RJ-45 o przepustowości 1GbE dedykowany dla karty zarządzającej.  |
| **Sloty I/O PCIe**  | Serwer musi posiadać min. 3 sloty PCIe generacji 4, w tym min, 1 slot x16. Wszystkie sloty muszą być aktywne. Możliwość rozbudowy do 8 slotów PCIe generacji 4. |
| **Dodatkowe porty**  | Serwer musi posiadać:1. z przodu obudowy: min. 1x USB 3.2, 1x USB 2.0 (współdzielony z systemem zarządzania), Możliwość instalacji portu VGA.
2. z tyłu obudowy: 3x USB 3.2, 1x VGA. Możliwość instalacji portu DB9
3. wewnątrz: 1x USB 3.2
 |
| **Chłodzenie**  | Serwer wyposażony w wentylatory wspierające wymianę Hot-Swap, zamontowane nadmiarowo minimum N+1  |
| **Zarządzanie**  | Zintegrowany z płytą główną serwera, niezależny od systemu operacyjnego, sprzętowy kontroler zdalnego zarzadzania umożliwiający: 1. Monitoring stanu systemu (komponenty objęte monitoringiem to przynajmniej: CPU, pamięć RAM, dyski, karty PCI, zasilacze, wentylatory, płyta główna
2. 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
3. Logowanie zdarzeń systemowych oraz związanych z działaniami użytkownika. Każdy dziennik zdarzeń powinien mieć możliwość zapisu co najmniej 1024 rekordów.
 |
| **Wspierane systemy operacyjne** | Serwer powinien wspierać przynajmniej poniższe systemy operacyjne:1. Microsoft Windows Server 2019, 2022
2. Red Hat Enterprise Linux 8.6, 8.7, 8.8, 8.9, 9.0, 9.1, 9.2, 9.3
3. SUSE Linux Enterprise Server 15 SP4, 15 SP5, 15 Xen SP4, 15 Xen SP5
4. VMware vSphere (ESXi) 7.0 U3, 8.0, 8.0 U1, 8.0 U2
5. Ubuntu 22
 |
| **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.W przypadku braku funkcjonalności przewidywania awarii dla wszystkich komponentów wymienionych w punkcie Diagnostyka wymagane jest dostarczenie serwera nadmiarowego, mogącego zastąpić funkcjonalnie jak i wydajnościowo wymagane w opisie parametry. |
| **Gwarancja** | 3 lata gwarancji producenta serwera w trybie on-site z gwarantowanym czasem reakcji serwisu do końca następnego dnia od zgłoszenia. Naprawa realizowana przez producenta serwera lub autoryzowany przez producenta serwis. |
| **Dokumentacja, inne** | Elementy, z których zbudowane są serwery muszą być produktami producenta tych serwerów lub być przez niego certyfikowane oraz całe muszą być objęte gwarancją producenta, o wymaganym w specyfikacji poziomie SLA Serwer musi być fabrycznie nowy i pochodzić z oficjalnego kanału dystrybucyjnego w UE.Możliwość aktualizacji i pobrania sterowników do oferowanego modelu serwera w najnowszych certyfikowanych wersjach bezpośrednio z sieci Internet za pośrednictwem strony www producenta serwera |
| **Serwerowy system operacyjny** | Licencja na serwerowy system operacyjny musi uprawniać do zainstalowania serwerowego systemu operacyjnego w środowisku fizycznym oraz nielimitowanej ilości maszyn wirtualnych tego serwerowego systemu operacyjnego. Licencja musi zostać tak dobrana aby była zgodna z zasadami licencjonowania producenta oraz pozwalała na legalne używanie na oferowanym serwerze. 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:
	1. pozwalają na zmianę rozmiaru w czasie pracy systemu,
	2. umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,
	3. umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów,
	4. 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:
	1. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,
	2. 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:
	1. Login i hasło,
	2. Karty z certyfikatami (smartcard),
	3. 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.
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:
	1. Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC,
	2. 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:
		* Podłączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną,
		* Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,
		* Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza.
		* Bezpieczny mechanizm dołączania do domeny uprawnionych użytkowników prywatnych urządzeń mobilnych opartych o iOS i Windows 8.1.
	3. Zdalna dystrybucja oprogramowania na stacje robocze.
	4. Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej
	5. Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:
		* Dystrybucję certyfikatów poprzez http
		* Konsolidację CA dla wielu lasów domeny,
		* Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen,
		* Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509.
	6. Szyfrowanie plików i folderów.
	7. Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec).
	8. Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów.
	9. Serwis udostępniania stron WWW.
	10. Wsparcie dla protokołu IP w wersji 6 (IPv6),
	11. Wsparcie dla algorytmów Suite B (RFC 4869),
	12. Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows,
	13. 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:
		* Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych,
		* Obsługi ramek typu jumbo frames dla maszyn wirtualnych.
		* Obsługi 4-KB sektorów dysków
		* Nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra
		* Możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API.
		* 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.
 |

2. Serwer kontroler domeny – 1 szt. spełniający poniższe wymagania.

|  |  |
| --- | --- |
| **Nazwa elementu,** **parametru lub cechy**  | **Opis wymagań serwera** |
| **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 – 150W. Wymagana ilość rdzeni dla procesora – min. 16, taktowanie bazowe procesora nie niższe niż 2 GHz. Możliwość uzyskania częstotliwości min. 3.4 GHz w trybie Turbo. Wielkość pamięci cache min. 30 MB. Ilość linków UPI min. 2. Obsługa minimum dwóch procesorów. Procesor musi zapewniać obsługę pamięci DDR5.  |
| **Liczba zainstalowanych procesorów**  | Min. 1 szt. |
| **Płyta główna**  | Płyta główna dedykowana do pracy w serwerach, wyprodukowana przez producenta serwera z możliwością zainstalowania do dwóch procesorów Intel Xeon wykonujących 64-bitowe instrukcje  |
| **Pamięć operacyjna**  | Zainstalowane minimum 128GB pamięci RAM o częstotliwości 5600MHz. Zainstalowana pamięć musi być sygnowana i zoptymalizowana do użycia przez producenta serwera. Minimum 32 sloty na pamięć. Możliwość rozbudowy do 8TB RAM.  |
| **Zabezpieczenie pamięci**  | Memory mirroring, ECC, SDDC, ADDDC  |
| **Procesor Graficzny**  | Zintegrowana karta graficzna z minimum 16MB pamięci osiągająca rozdzielczość 1920x1200 przy 60 Hz.  |
| **Dyski** | Zainstalowane min. 3 szt. dysków SSD o pojemności min. 480GB typu Read Intensive. |
| **Rozbudowa dysków**  | Serwer musi posiadać możliwość rozbudowy na potrzeby zainstalowania minimum 10 dysków SAS/SATA 2,5” z przodu serwera, oraz 2 dysków SAS/SATA 2,5” z tyłu serwera. Dodatkowo wymaga się, aby serwer posiadał możliwość rozbudowy do instalacji dysków NVMe. Wymaga się możliwości wyposażenia serwera w przynajmniej 4 zatoki umożliwiające wymiennie instalację dysków SAS/SATA oraz dysków NVMe (ta sama zatoka). W momencie dostawy serwer musi posiadać elementy umożliwiające instalacje 8 dysków SAS/SATA hot plug.Serwer powinien posiadać możliwość instalacji napędu Flash w wewnętrznym porcie USB serwera. |
| **Kontroler dyskowy**  | Zainstalowany kontroler 12 Gb SAS/SATA z obsługą RAID 0, 1, 10, 5.Serwer musi posiadać możliwość rozbudowy na potrzeby zainstalowania kontrolera dyskowego z 8GB Cache wykorzystującego pamięć flash NAND będącego w ofercie producenta serwera. Kontroler powinien posiadać funkcjonalność podtrzymania napięcia w przypadku utraty głównego zasilania w technologii nie wykorzystującej jakiegokolwiek rozwiązania bateryjnego. Kontroler taki dedykowany do ofertowanego serwera powinien być w ofercie producenta serwera. Kontroler powinien obsługiwać następujące poziomy zabezpieczeń RAID 0/1/10/5/50/6/60. 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. Kontroler powinien mieć możliwość jednoczesnej obsługi dysków SAS/SATA oraz dysków NVMe.  |
| **Zasilacz**  | Minimum dwa redundantne zasilacze o mocy minimum 750W z certyfikatem minimum Titanium. Moc pojedynczego zasilacza musi być wystarczająca do zasilenia serwera w oferowanej konfiguracji. Zasilacze wyposażone w kable zasilające posiadające wtyk typu C14. |
| **Interfejsy sieciowe**  | 4 porty 1Gbs RJ45. Interfejsy te nie mogą wpływać na ilość dostępnych slotów PCIe wymienionych w sekcji Dodatkowe sloty I/O.Zainstalowana jedna dwuportowa karta FC 16Gbs.Jeden port RJ-45 o przepustowości 1GbE dedykowany dla karty zarządzającej.  |
| **Sloty I/O PCIe**  | Serwer musi posiadać min. 2 sloty PCIe x16 generacji 4. Wszystkie sloty muszą być aktywne. Możliwość rozbudowy do 3 slotów PCIe generacji 4. |
| **Dodatkowe porty**  | Serwer musi posiadać:1. z przodu obudowy: 1x USB 3.2, 1x USB 2.0 (współdzielony z systemem zarządzania), Możliwość instalacji portu VGA.
2. z tyłu obudowy: 3x USB 3.2, 1x VGA. Możliwość instalacji portu DB9
3. wewnątrz: 1x USB 3.2
 |
| **Chłodzenie**  | Serwer wyposażony w wentylatory wspierające wymianę Hot-Swap, zamontowane nadmiarowo minimum N+1  |
| **Zarządzanie**  | Zintegrowany z płytą główną serwera, niezależny od systemu operacyjnego, sprzętowy kontroler zdalnego zarzadzania umożliwiający: 1. Monitoring stanu systemu (komponenty objęte monitoringiem to przynajmniej: CPU, pamięć RAM, dyski, karty PCI, zasilacze, wentylatory, płyta główna
2. 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
3. Logowanie zdarzeń systemowych oraz związanych z działaniami użytkownika. Każdy dziennik zdarzeń powinien mieć możliwość zapisu co najmniej 1024 rekordów.
 |
| **Wspierane systemy operacyjne** | Serwer powinien wspierać przynajmniej poniższe systemy operacyjne:1. Microsoft Windows Server 2019, 2022
2. Red Hat Enterprise Linux 8.6, 8.7, 8.8, 8.9, 9.0, 9.1, 9.2, 9.3
3. SUSE Linux Enterprise Server 15 SP4, 15 SP5, 15 Xen SP4, 15 Xen SP5
4. VMware vSphere (ESXi) 7.0 U3, 8.0, 8.0 U1, 8.0 U2
5. Ubuntu 22
 |
| **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.W przypadku braku funkcjonalności przewidywania awarii dla wszystkich komponentów wymienionych w punkcie Diagnostyka wymagane jest dostarczenie serwera nadmiarowego, mogącego zastąpić funkcjonalnie jak i wydajnościowo wymagane w opisie parametry. |
| **Gwarancja** | 3 lata gwarancji producenta serwera w trybie on-site z gwarantowanym czasem reakcji serwisu do końca następnego dnia od zgłoszenia. Naprawa realizowana przez producenta serwera lub autoryzowany przez producenta serwis. |
| **Dokumentacja, inne** | Elementy, z których zbudowane są serwery muszą być produktami producenta tych serwerów lub być przez niego certyfikowane oraz całe muszą być objęte gwarancją producenta, o wymaganym w specyfikacji poziomie SLA.Serwer musi być fabrycznie nowy i pochodzić z oficjalnego kanału dystrybucyjnego w UE.Możliwość aktualizacji i pobrania sterowników do oferowanego modelu serwera w najnowszych certyfikowanych wersjach bezpośrednio z sieci Internet za pośrednictwem strony www producenta serwera. |
| **Serwerowy system operacyjny** | Licencja na serwerowy system operacyjny musi uprawniać do zainstalowania serwerowego systemu operacyjnego w środowisku fizycznym oraz dwóch maszyn wirtualnych tego serwerowego systemu operacyjnego. Licencja musi zostać tak dobrana aby była zgodna z zasadami licencjonowania producenta oraz pozwalała na legalne używanie na oferowanym serwerze. 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:
	1. pozwalają na zmianę rozmiaru w czasie pracy systemu,
	2. umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,
	3. umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów,
	4. 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:
	1. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,
	2. 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:
	1. Login i hasło,
	2. Karty z certyfikatami (smartcard),
	3. 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.
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:
	1. Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC,
	2. 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:
		* Podłączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną,
		* Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,
		* Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza.
		* Bezpieczny mechanizm dołączania do domeny uprawnionych użytkowników prywatnych urządzeń mobilnych opartych o iOS i Windows 8.1.
	3. Zdalna dystrybucja oprogramowania na stacje robocze.
	4. Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej
	5. Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:
		* Dystrybucję certyfikatów poprzez http
		* Konsolidację CA dla wielu lasów domeny,
		* Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen,
		* Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509.
	6. Szyfrowanie plików i folderów.
	7. Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec).
	8. Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów.
	9. Serwis udostępniania stron WWW.
	10. Wsparcie dla protokołu IP w wersji 6 (IPv6),
	11. Wsparcie dla algorytmów Suite B (RFC 4869),
	12. Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows,
	13. 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:
		* Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych,
		* Obsługi ramek typu jumbo frames dla maszyn wirtualnych.
		* Obsługi 4-KB sektorów dysków
		* Nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra
		* Możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API.
		* 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.
 |

3. Macierz – 1 szt. spełniająca poniższe wymagania.

|  |  |
| --- | --- |
| **Nazwa elementu,** **parametru lub cechy**  | **Opis wymagań macierzy**  |
| **Typ obudowy** | Macierz musi być przystosowana do montażu w szafie rack 19”, o wysokość maksymalnie 2U. |
| **Przestrzeń dyskowa** | Macierz musi udostępniać przestrzeń zbudowaną w oparciu o minimum 16 dysków 1.92TB SSD o parametrze 1DWD |
| **Możliwość rozbudowy** | Macierz musi umożliwiać rozbudowę (bez wymiany kontrolerów macierzy), o dodatkowe co najmniej 72 dysków twardych 2,5”, lub dodatkowe co najmniej 36 dysków twardych 3,5”. |
| **Obsługa dysków** | Macierz musi obsługiwać dyski SSD, SAS i Nearline SAS. Macierz musi umożliwiać mieszanie napędów dyskowych SSD, SAS i NL-SAS w obrębie pojedynczej półki dyskowej i macierzy. Macierz musi obsługiwać dyski 2,5” jak również 3,5”. |
| **Sposób zabezpieczenia danych** | Macierz musi obsługiwać mechanizmy RAID zgodne z RAID1, RAID10, RAID3, RAID5 oraz RAID6 realizowane sprzętowo za pomocą dedykowanego układu, z możliwością dowolnej ich kombinacji w obrębie oferowanej macierzy i z wykorzystaniem wszystkich dysków twardych.Macierz musi umożliwiać definiowanie dysków hot-spare. |
| **Tryb pracy kontrolerów macierzowych** | Macierz musi posiadać minimum 2 kontrolery macierzowe pracujące w trybie active-active i udostępniające dane blokowe w sieci iSCSI 10/25Gb, FC 16/32Gb lub SAS 12Gb, w zależności od wybranego interfejsu. Wszystkie kontrolery muszą komunikować się między sobą bez stosowania dodatkowych przełączników. |
| **Pamięć cache** | Każdy kontroler macierzowy musi być wyposażony w minimum 8GB pamięci cache, 16GB sumarycznie w macierzy. Pamięć cache musi być zbudowana w oparciu o wydajną pamięć typu RAM.Pamięć zapisu musi być mirrorowana (kopie lustrzane) pomiędzy kontrolerami dyskowymi.Dane niezapisane na dyskach (np. zawartość pamięci kontrolera) muszą zostać zabezpieczone w przypadku awarii zasilania za pomocą podtrzymania bateryjnego lub z zastosowaniem innej technologii przez okres minimum 72 godziny. |
| **Rozbudowa pamięci cache** | Macierz musi umożliwiać zwiększenie pojemności pamięci cache dla odczytów do minimum 4 TB z wykorzystaniem dysków SSD lub kart pamięci flash. Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć wraz z rozwiązaniem. |
| **Interfejsy** | Macierz musi posiadać, co najmniej 8 portów FC 32 Gb/s.Wszystkie porty muszą być wyposażone w odpowiednie wkładki min. 16 Gb/s oraz kable światłowodowe długości min. 3m. |
| **Zarządzanie** | Zarządzanie macierzą musi być możliwe z poziomu interfejsu graficznego i interfejsu znakowego. Zarządzanie macierzą musi odbywać się bezpośrednio na kontrolerach macierzy z poziomu przeglądarki internetowej. |
| **Zarządzanie grupami dyskowymi oraz dyskami logicznymi** | Macierz musi umożliwiać zdefiniowanie, co najmniej 500 wolumenów logicznych w ramach oferowanej macierzy dyskowej. Musi istnieć możliwość rozłożenia pojedynczego wolumenu logicznego na wszystkie dyski fizyczne macierzy bez konieczności łączenia wielu różnych dysków logicznych w jeden większy.Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia. |
| **Thin Provisioning** | Macierz musi umożliwiać udostępnianie zasobów dyskowych do serwerów w trybie tradycyjnym, jak i w trybie typu Thin Provisioning.Macierz musi umożliwiać odzyskiwanie przestrzeni dyskowych po usuniętych danych w ramach wolumenów typu Thin. Proces odzyskiwania danych musi być automatyczny bez konieczności uruchamiania dodatkowych procesów na kontrolerach macierzowych (wymagana obsługa standardu T10 SCSI UNMAP).Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia. |
| **Wewnętrzne kopie migawkowe** | Macierz musi umożliwiać dokonywania na żądanie tzw. migawkowej kopii danych (snapshot, point-in-time) w ramach macierzy za pomocą wewnętrznych kontrolerów macierzowych. Kopia migawkowa wykonuje się bez alokowania dodatkowej przestrzeni dyskowej na potrzeby kopii. Zajmowanie dodatkowej przestrzeni dyskowej następuje w momencie zmiany danych na dysku źródłowym lub na jego kopii. Macierz musi wspierać minimum 128 kopii migawkowych, z możliwością jej rozbudowy w przyszłości do 512 kopii migawkowych. |
| **Wewnętrzne kopie pełne** | Macierz musi umożliwiać dokonywanie na żądanie pełnej fizycznej kopii danych (clone) w ramach macierzy za pomocą wewnętrznych kontrolerów macierzowych. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia. |
| **Zdalna replikacja danych** | Macierz musi umożliwiać co najmniej asynchroniczną replikację danych do innej macierzy z tej samej rodziny. Replikacja musi być wykonywana na poziomie kontrolerów, bez użycia dodatkowych serwerów lub innych urządzeń i bez obciążania serwerów podłączonych do macierzy. Aktualnie nie jest konieczne dostarczenie licencji dla tej funkcjonalności. Możliwość aktywowania takiej funkcjonalności w przyszłości dla całej pojemności macierzy. |
| **Podłączanie zewnętrznych systemów operacyjnych** | Macierz musi umożliwiać jednoczesne podłączenie wielu serwerów w trybie wysokiej dostępności (co najmniej dwoma ścieżkami). Macierz musi wspierać podłączenie następujących systemów operacyjnych: Windows, Linux, VMware. Wsparcie dla wymienionych systemów operacyjnych i klastrowych musi być potwierdzone wpisem na ogólnodostępnej liście kompatybilności producentów. |
| **Redundancja** | Macierz nie może posiadać pojedynczego punktu awarii, który powodowałby brak dostępu do danych. Musi być zapewniona pełna redundancja komponentów, w szczególności zdublowanie kontrolerów, zasilaczy i wentylatorów.Macierz musi umożliwiać wymianę elementów systemu w trybie „hot-swap”, a w szczególności takich, jak: dyski, kontrolery, zasilacze, wentylatory. |
| **Dodatkowe wymagania** | Oferowany system dyskowy musi się składać z pojedynczej macierzy dyskowej. Niedopuszczalna jest realizacja zamówienia poprzez dostarczenie wielu macierzy dyskowych. Za pojedynczą macierz nie uznaje się rozwiązania opartego o wiele macierzy dyskowych (par kontrolerów macierzowych) połączonych przełącznikami SAN lub tzw. wirtualizatorem sieci SAN czy wirtualizatorem macierzy dyskowych.Macierz musi umożliwiać szyfrowanie z wykorzystaniem dysków SED.Możliwość ograniczania poboru zasilania przez dyski, które nie obsługują operacji we/wy, poprzez ich zatrzymanie. |
| **Gwarancja** | 3-letnia gwarancja producenta w miejscu instalacji z czasem reakcji w następnym dniu roboczym.W okresie gwarancji Zamawiający ma prawo do otrzymywania poprawek oraz aktualizacji wersji oprogramowania dostarczonego wraz z macierzą oraz oprogramowania wewnętrznego macierzy. |

4. Przełączniki FC – 2 szt. spełniająca poniższe wymagania.

|  |  |
| --- | --- |
| **Nazwa elementu,** **parametru lub cechy**  | **Opis wymagań przełączników FC**  |
| **Obudowa**  | Typu Rack o wysokości maksymalnej 1U, wraz z kompletem elementów umożliwiających montaż w standardowej szafie Rack.Kierunek przepływu powietrza od tyłu do frontu. |
| **Porty** | Przynajmniej 24 miejsca na porty Fibre Channel zdolne do osiągnięcia przepustowości 32Gb/s każdy. Min. 16 lub więcej aktywnych portów ze złączami SFP+. Wsparcie dla portów SFP+ 32Gb/s Hot-Plug.Moduły do transmisji światłowodowej z prędkością min. 16Gb/s poprzez kabel światłowodowy wielomodowy (Short-Wavelenght) z interfejsem LC, liczba modułów dostosowana do liczby aktywnych portów. |
| **Łączna możliwa przepustowość** | Całkowita przepustowość przełącznika FC dostępna dla maksymalnie rozbudowanej konfiguracji (24 porty) wyposażonej we wkładki 32Gbs musi wynosić minimum 768 Gb/s end-to-end.Oczekiwana wartość opóźnienia przy przesyłaniu ramek FC między dowolnymi portami przełącznika nie może być większa niż 900ns. |
| **Typy portów** | Przynajmniej D\_PORT, E\_PORT, F\_PORT |
| **Klasy usług (CoS)** | Wspierane klasy usług: 2, 3, F |
| **Funkcjonalność** | 1. automatyczne monitorowanie sieci SAN pod kątem potencjalnych usterek oraz przeciążeń i ostrzeganie na podstawie definiowalnych polityk alertów.
2. zapewnienie QoS ze zdolnością do rozpoznawania priorytetu ramki.
3. adaptacyjne ograniczanie prędkości wybranych portów z uwzględnieniem priorytetów zadań.
4. możliwość definiowalnej izolacji ruchu na określonych łączach między przełącznikami, gwarantującej dedykowane zasoby sieciowe dla danej aplikacji.
5. identyfikacja urządzeń hamujących przepływ danych i automatyczna redukcja efektu backpressure.
6. Fibre Channel zoning. R
7. CS (Reliable Commit Service).
8. IPoFC. FSPF. NPIV.
9. Serwer czasu NTP. RSCN. FDMI. Buffer-to-Buffer Credit Recovery.
10. dynamiczne obieranie ścieżki routingu na podstawie identyfikatorów SID, DID i OXID, w celu proporcjonalnego rozłożenia zużycia pasma i zoptymalizowania wydajności.
11. serwer nazw dostępny pod standardowym adresem WKA FFFFFC
12. usługi zarządzania dostępne pod standardowym adresem WKA FFFFFA.
 |
| **Bezpieczeństwo** | 1. DH-CHAP,
2. Fibre Channel Authentication Protocol,
3. HTTPS,
4. IPsec,
5. filtrowanie IP,
6. LDAP ze wsparciem IPv6,
7. OpenLDAR,
8. przydzielanie portów,
9. RADIUS,
10. TACACS+,
11. kontrola dostępu oparta na rolach definiowanych przez użytkownika (RBAC),
12. SCP,
13. Secure RPC, s
14. szyfrowany syslog, SSH v2, SSL, przypisywanie zaufanych przełączników.
 |
| **Diagnostyka** | 1. cyfrowe możliwości diagnostyczne zapewniające wykonanie elektrycznego/optycznego testu pętli zwrotnej (loopback), zbadanie ruchu/opóźnień/długości łącza, diagnostyka POST i wbudowane narzędzia diagnostyki online/offline, w tym monitorowanie środowiskowe,
2. FC ping i Pathinfo (FC traceroute),
3. przeglądarka ramek,
4. niezakłócający pracy restart daemonów,
5. monitorowanie kondycji łączy optycznych,
6. monitorowanie zasilania,
7. rejestrowanie RAStrace.
 |
| **Zasilanie** | Wbudowany zasilacz. Zasilanie z sieci prądu przemiennego o napięciu w zakresie 100- 240V/50-60HzMaksymalne zużycie mocy 77W przy wykorzystaniu 24 portów. |
| **Zarządzanie** | 1. dostęp poprzez 10/100/1000 Mb/s Ethernet RJ-45, wewnątrzpasmowo po Fibre Channel, Serial port RJ-45 oraz USB.
2. pobieranie i aktywacja aktualizacji firmware'u bez przerywania pracy urządzenia.
3. pulpit zarządzania dostępny z przeglądarki internetowej oraz możliwość łączenia przez SSH.
4. zgodność ze standardami SMI-S oraz SNMP.
5. oprogramowanie przedstawiające w czytelny i przejrzysty sposób wizualizację sieci SAN wraz ze statystykami i informacjami dotyczącymi statusu, żywotności, wydajności i bezpieczeństwa.
 |
| **Gwarancja** | 3 lata gwarancji producenta realizowanej w miejscu instalacji sprzętu, z czasem reakcji serwisu do następnego dnia roboczego od przyjęcia zgłoszenia.Diagnostyka awarii przeprowadzana przez autoryzowany serwis producenta w miejscu użytkowania sprzętu w godzinach pracy zamawiającego. |

5. Urządzenie NAS – 1 szt. spełniające poniższe wymagania.

|  |  |
| --- | --- |
| **Nazwa elementu,** **parametru lub cechy**  | **Opis wymagań urządzenia NAS**  |
| **Procesor** | Jeden 8-rdzeniowy/16-wątkowy procesor osiągający w testach PassMark - CPU Mark wynik nie gorszy niż 10000 pkt. |
| **Obudowa** | Rack 2U o wymiarach max. 89 mm x 483 mm x 725 mm; w zestawie szyny wysuwane do instalacji w szafie RACK |
| **Pamięć RAM** | 8GB DDR4 ECC RAM z możliwością rozszerzenia do 64GB |
| **Ilość obsługiwanych dysków** | 12 dysków 3,5”/2,5” SATAIII/II;możliwość rozszerzenia do 36 dysków poprzez dołożenie dodatkowych półek rozszerzających |
| **Ilość zainstalowanych dysków** | 10 dysków w formacie 3,5” znajdujących się na liście kompatybilności producenta macierzy NAS o min. pojemności 8TB każdy. |
| **Interfejsy sieciowe** | 4 x Gigabit (10/100/1000)2 x 10GbE RJ-45 |
| **Porty** | 2 x USB3.2, 2 x Infiniband |
| **Gniazda PCIe** | 2 gniazda PCIe Gen3 x8 (minimum 1 gniazdo wolne) |
| **Wskaźniki LED** | Status, LAN, HDD1 -12 |
| **Obsługa RAID** | Basic, JBOD, RAID F1,0,1,5,6,10 + Hot Spare 1,5,6,10.  |
| **Funkcje RAID** | Możliwość zwiększania pojemności i migracja między poziomami RAID online. |
| **Szyfrowanie** | Możliwość szyfrowania wybranych udziałów sieciowych, kluczem AES-256bitów |
| **Licencja na Kamery IP** | W zestawie licencja na dwie kamery z możliwością rozszerzenia do 90. Funkcja CMS. |
| **Obsługa SSD Cache** | Wymagane wsparcie dla SSD Cache  |
| **Protokoły** | AFP, NFS, FTP, WebDAV, iSCSI, Telnet, SSH, SNMP, VPN, CalDAV, SMB, |
| **Usługi** | Wsparcie dla High AvailabilitySerwer VPNSerwer pocztowy dla kilku domenStacja monitoringuWindows ACLIntegracja z Windows ADSFirewall z kontrolą ruchuSerwer WWWSerwer plikówManager plików przez WWWSzyfrowana replikacja zdalna na kilka serwerów w tym samym czasieAntyvirusKlient VPNUsługa DDNSOprogramownie do backup stacji roboczych, serwerów fizycznych i środowiska wirtualizacji VMware |
| **Zarządzanie dyskami** | SMART, sprawdzanie złych sektorów, dynamiczne mapowanie uszkodzonych sektorów, |
| **Język GUI** | Polski |
| **Waga** | Do 15 KG |
| **Certyfikaty**  | CE |
| **System plików** | Dyski wewnętrzne Btrfs, EXT4. Dyski zewnętrzne Btfrs, FAT, NTFS, EXT4, EXT3, HFS+, exFAT |
| **Liczba wolumenów** | 256 |
| **Liczba iSCSI Targetów** | 256 |
| **Liczba iSCSI LUN** | Do 512 |
| **Liczba kont użytkowników** | 16000 |
| **Liczba grup** | 512 |
| **Liczba folderów udostępnionych** | 512 |
| **Ilość jednoczesnych połączeń** | 2000 dla CIFS, FTP, AFP |
| **Zasilanie** | Max. 2 x 550W  |
| **Chłodzenie** | FAN x 4 80 x 80 mm |
| **Gwarancja i serwis** | 5 lat gwarancji 5 lat gwarancji na dyski |

6. Serwery administracyjne – 2 szt. spełniające poniższe wymagania.

|  |  |
| --- | --- |
| **Nazwa elementu,** **parametru lub cechy**  | **Opis wymagań serwera** |
| **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 – 150W. Wymagana ilość rdzeni dla procesora – min. 16, taktowanie bazowe procesora nie niższe niż 2 GHz. Możliwość uzyskania częstotliwości min. 3.4 GHz w trybie Turbo. Wielkość pamięci cache min. 30 MB. Ilość linków UPI min. 2. Obsługa minimum dwóch procesorów. Procesor musi zapewniać obsługę pamięci DDR5.  |
| **Liczba zainstalowanych procesorów**  | Min. 1 szt. |
| **Płyta główna**  | Płyta główna dedykowana do pracy w serwerach, wyprodukowana przez producenta serwera z możliwością zainstalowania do dwóch procesorów Intel Xeon wykonujących 64-bitowe instrukcje  |
| **Pamięć operacyjna**  | Zainstalowane minimum 128GB pamięci RAM o częstotliwości 5600MHz. Zainstalowana pamięć musi być sygnowana i zoptymalizowana do użycia przez producenta serwera. Minimum 32 sloty na pamięć. Możliwość rozbudowy do 8TB RAM.  |
| **Zabezpieczenie pamięci**  | Memory mirroring, ECC, SDDC, ADDDC  |
| **Procesor Graficzny**  | Zintegrowana karta graficzna z minimum 16MB pamięci osiągająca rozdzielczość 1920x1200 przy 60 Hz.  |
| **Dyski** | Zainstalowane min. 3 szt. dysków SSD o pojemności min. 480GB typu Read Intensive. |
| **Rozbudowa dysków**  | Serwer musi posiadać możliwość rozbudowy na potrzeby zainstalowania minimum 10 dysków SAS/SATA 2,5” z przodu serwera, oraz 2 dysków SAS/SATA 2,5” z tyłu serwera. Dodatkowo wymaga się, aby serwer posiadał możliwość rozbudowy do instalacji dysków NVMe. Wymaga się możliwości wyposażenia serwera w przynajmniej 4 zatoki umożliwiające wymiennie instalację dysków SAS/SATA oraz dysków NVMe (ta sama zatoka). W momencie dostawy serwer musi posiadać elementy umożliwiające instalacje 8 dysków SAS/SATA hot plug.Serwer powinien posiadać możliwość instalacji napędu Flash w wewnętrznym porcie USB serwera. |
| **Kontroler dyskowy**  | Zainstalowany kontroler 12 Gb SAS/SATA z obsługą RAID 0, 1, 10, 5.Serwer musi posiadać możliwość rozbudowy na potrzeby zainstalowania kontrolera dyskowego z 8GB Cache wykorzystującego pamięć flash NAND będącego w ofercie producenta serwera. Kontroler powinien posiadać funkcjonalność podtrzymania napięcia w przypadku utraty głównego zasilania w technologii nie wykorzystującej jakiegokolwiek rozwiązania bateryjnego. Kontroler taki dedykowany do ofertowanego serwera powinien być w ofercie producenta serwera. Kontroler powinien obsługiwać następujące poziomy zabezpieczeń RAID 0/1/10/5/50/6/60. 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. Kontroler powinien mieć możliwość jednoczesnej obsługi dysków SAS/SATA oraz dysków NVMe.  |
| **Zasilacz**  | Minimum dwa redundantne zasilacze o mocy minimum 750W z certyfikatem minimum Titanium. Moc pojedynczego zasilacza musi być wystarczająca do zasilenia serwera w oferowanej konfiguracji. Zasilacze wyposażone w kable zasilające posiadające wtyk typu C14. |
| **Interfejsy sieciowe**  | 4 porty 10Gbs RJ45. Interfejsy te nie mogą wpływać na ilość dostępnych slotów PCIe wymienionych w sekcji Dodatkowe sloty I/O.Zainstalowana jedna dwuportowa karta FC 16Gbs.Jeden port RJ-45 o przepustowości 1GbE dedykowany dla karty zarządzającej.  |
| **Sloty I/O PCIe**  | Serwer musi posiadać min. 2 sloty PCIe x16 generacji 4. Wszystkie sloty muszą być aktywne. Możliwość rozbudowy do 3 slotów PCIe generacji 4. |
| **Dodatkowe porty**  | Serwer musi posiadać:1. z przodu obudowy: 1x USB 3.2, 1x USB 2.0 (współdzielony z systemem zarządzania), Możliwość instalacji portu VGA.
2. z tyłu obudowy: 3x USB 3.2, 1x VGA. Możliwość instalacji portu DB9
3. wewnątrz: 1x USB 3.2
 |
| **Chłodzenie**  | Serwer wyposażony w wentylatory wspierające wymianę Hot-Swap, zamontowane nadmiarowo minimum N+1  |
| **Zarządzanie**  | Zintegrowany z płytą główną serwera, niezależny od systemu operacyjnego, sprzętowy kontroler zdalnego zarzadzania umożliwiający: 1. Monitoring stanu systemu (komponenty objęte monitoringiem to przynajmniej: CPU, pamięć RAM, dyski, karty PCI, zasilacze, wentylatory, płyta główna
2. 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
3. Logowanie zdarzeń systemowych oraz związanych z działaniami użytkownika. Każdy dziennik zdarzeń powinien mieć możliwość zapisu co najmniej 1024 rekordów.
 |
| **Wspierane systemy operacyjne** | Serwer powinien wspierać przynajmniej poniższe systemy operacyjne:1. Microsoft Windows Server 2019, 2022
2. Red Hat Enterprise Linux 8.6, 8.7, 8.8, 8.9, 9.0, 9.1, 9.2, 9.3
3. SUSE Linux Enterprise Server 15 SP4, 15 SP5, 15 Xen SP4, 15 Xen SP5
4. VMware vSphere (ESXi) 7.0 U3, 8.0, 8.0 U1, 8.0 U2
5. Ubuntu 22
 |
| **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.W przypadku braku funkcjonalności przewidywania awarii dla wszystkich komponentów wymienionych w punkcie Diagnostyka wymagane jest dostarczenie serwera nadmiarowego, mogącego zastąpić funkcjonalnie jak i wydajnościowo wymagane w opisie parametry. |
| **Gwarancja** | 3 lata gwarancji producenta serwera w trybie on-site z gwarantowanym czasem reakcji serwisu do końca następnego dnia od zgłoszenia. Naprawa realizowana przez producenta serwera lub autoryzowany przez producenta serwis. |
| **Dokumentacja, inne** | Elementy, z których zbudowane są serwery muszą być produktami producenta tych serwerów lub być przez niego certyfikowane oraz całe muszą być objęte gwarancją producenta, o wymaganym w specyfikacji poziomie SLA.Serwer musi być fabrycznie nowy i pochodzić z oficjalnego kanału dystrybucyjnego w UE.Możliwość aktualizacji i pobrania sterowników do oferowanego modelu serwera w najnowszych certyfikowanych wersjach bezpośrednio z sieci Internet za pośrednictwem strony www producenta serwera. |
| **Serwerowy system operacyjny** | Licencja na serwerowy system operacyjny musi uprawniać do zainstalowania serwerowego systemu operacyjnego w środowisku fizycznym oraz czterech maszyn wirtualnych tego serwerowego systemu operacyjnego. Licencja musi zostać tak dobrana aby była zgodna z zasadami licencjonowania producenta oraz pozwalała na legalne używanie na oferowanym serwerze. 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:
	1. pozwalają na zmianę rozmiaru w czasie pracy systemu,
	2. umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,
	3. umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów,
	4. 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:
	1. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,
	2. 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:
	1. Login i hasło,
	2. Karty z certyfikatami (smartcard),
	3. 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.
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:
	1. Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC,
	2. 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:
		* Podłączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną,
		* Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,
		* Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza.
		* Bezpieczny mechanizm dołączania do domeny uprawnionych użytkowników prywatnych urządzeń mobilnych opartych o iOS i Windows 8.1.
	3. Zdalna dystrybucja oprogramowania na stacje robocze.
	4. Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej
	5. Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:
		* Dystrybucję certyfikatów poprzez http
		* Konsolidację CA dla wielu lasów domeny,
		* Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen,
		* Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509.
	6. Szyfrowanie plików i folderów.
	7. Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec).
	8. Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów.
	9. Serwis udostępniania stron WWW.
	10. Wsparcie dla protokołu IP w wersji 6 (IPv6),
	11. Wsparcie dla algorytmów Suite B (RFC 4869),
	12. Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows,
	13. 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:
		* Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych,
		* Obsługi ramek typu jumbo frames dla maszyn wirtualnych.
		* Obsługi 4-KB sektorów dysków
		* Nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra
		* Możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API.
		* 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.
 |

7. Serwery administracyjne – 2 szt. spełniające poniższe wymagania.

|  |  |
| --- | --- |
| **Nazwa elementu,** **parametru lub cechy**  | **Opis wymagań serwera** |
| **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 – 150W. Wymagana ilość rdzeni dla procesora – min. 16, taktowanie bazowe procesora nie niższe niż 2 GHz. Możliwość uzyskania częstotliwości min. 3.4 GHz w trybie Turbo. Wielkość pamięci cache min. 30 MB. Ilość linków UPI min. 2. Obsługa minimum dwóch procesorów. Procesor musi zapewniać obsługę pamięci DDR5.  |
| **Liczba zainstalowanych procesorów**  | Min. 1 szt. |
| **Płyta główna**  | Płyta główna dedykowana do pracy w serwerach, wyprodukowana przez producenta serwera z możliwością zainstalowania do dwóch procesorów Intel Xeon wykonujących 64-bitowe instrukcje  |
| **Pamięć operacyjna**  | Zainstalowane minimum 128GB pamięci RAM o częstotliwości 5600MHz. Zainstalowana pamięć musi być sygnowana i zoptymalizowana do użycia przez producenta serwera. Minimum 32 sloty na pamięć. Możliwość rozbudowy do 8TB RAM.  |
| **Zabezpieczenie pamięci**  | Memory mirroring, ECC, SDDC, ADDDC  |
| **Procesor Graficzny**  | Zintegrowana karta graficzna z minimum 16MB pamięci osiągająca rozdzielczość 1920x1200 przy 60 Hz.  |
| **Dyski** | Zainstalowane min. 3 szt. dysków SSD o pojemności min. 480GB typu Read Intensive. |
| **Rozbudowa dysków**  | Serwer musi posiadać możliwość rozbudowy na potrzeby zainstalowania minimum 10 dysków SAS/SATA 2,5” z przodu serwera, oraz 2 dysków SAS/SATA 2,5” z tyłu serwera. Dodatkowo wymaga się, aby serwer posiadał możliwość rozbudowy do instalacji dysków NVMe. Wymaga się możliwości wyposażenia serwera w przynajmniej 4 zatoki umożliwiające wymiennie instalację dysków SAS/SATA oraz dysków NVMe (ta sama zatoka). W momencie dostawy serwer musi posiadać elementy umożliwiające instalacje 8 dysków SAS/SATA hot plug.Serwer powinien posiadać możliwość instalacji napędu Flash w wewnętrznym porcie USB serwera. |
| **Kontroler dyskowy**  | Zainstalowany kontroler 12 Gb SAS/SATA z obsługą RAID 0, 1, 10, 5.Serwer musi posiadać możliwość rozbudowy na potrzeby zainstalowania kontrolera dyskowego z 8GB Cache wykorzystującego pamięć flash NAND będącego w ofercie producenta serwera. Kontroler powinien posiadać funkcjonalność podtrzymania napięcia w przypadku utraty głównego zasilania w technologii nie wykorzystującej jakiegokolwiek rozwiązania bateryjnego. Kontroler taki dedykowany do ofertowanego serwera powinien być w ofercie producenta serwera. Kontroler powinien obsługiwać następujące poziomy zabezpieczeń RAID 0/1/10/5/50/6/60. 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. Kontroler powinien mieć możliwość jednoczesnej obsługi dysków SAS/SATA oraz dysków NVMe.  |
| **Zasilacz**  | Minimum dwa redundantne zasilacze o mocy minimum 750W z certyfikatem minimum Titanium. Moc pojedynczego zasilacza musi być wystarczająca do zasilenia serwera w oferowanej konfiguracji. Zasilacze wyposażone w kable zasilające posiadające wtyk typu C14. |
| **Interfejsy sieciowe**  | 4 porty 1Gbs RJ45. Interfejsy te nie mogą wpływać na ilość dostępnych slotów PCIe wymienionych w sekcji Dodatkowe sloty I/O.Zainstalowana jedna dwuportowa karta FC 16Gbs.Jeden port RJ-45 o przepustowości 1GbE dedykowany dla karty zarządzającej.  |
| **Sloty I/O PCIe**  | Serwer musi posiadać min. 2 sloty PCIe x16 generacji 4. Wszystkie sloty muszą być aktywne. Możliwość rozbudowy do 3 slotów PCIe generacji 4. |
| **Dodatkowe porty**  | Serwer musi posiadać:1. z przodu obudowy: 1x USB 3.2, 1x USB 2.0 (współdzielony z systemem zarządzania), Możliwość instalacji portu VGA.
2. z tyłu obudowy: 3x USB 3.2, 1x VGA. Możliwość instalacji portu DB9
3. wewnątrz: 1x USB 3.2
 |
| **Chłodzenie**  | Serwer wyposażony w wentylatory wspierające wymianę Hot-Swap, zamontowane nadmiarowo minimum N+1  |
| **Zarządzanie**  | Zintegrowany z płytą główną serwera, niezależny od systemu operacyjnego, sprzętowy kontroler zdalnego zarzadzania umożliwiający: 1. Monitoring stanu systemu (komponenty objęte monitoringiem to przynajmniej: CPU, pamięć RAM, dyski, karty PCI, zasilacze, wentylatory, płyta główna
2. 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
3. Logowanie zdarzeń systemowych oraz związanych z działaniami użytkownika. Każdy dziennik zdarzeń powinien mieć możliwość zapisu co najmniej 1024 rekordów.
 |
| **Wspierane systemy operacyjne** | Serwer powinien wspierać przynajmniej poniższe systemy operacyjne:1. Microsoft Windows Server 2019, 2022
2. Red Hat Enterprise Linux 8.6, 8.7, 8.8, 8.9, 9.0, 9.1, 9.2, 9.3
3. SUSE Linux Enterprise Server 15 SP4, 15 SP5, 15 Xen SP4, 15 Xen SP5
4. VMware vSphere (ESXi) 7.0 U3, 8.0, 8.0 U1, 8.0 U2
5. Ubuntu 22
 |
| **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.W przypadku braku funkcjonalności przewidywania awarii dla wszystkich komponentów wymienionych w punkcie Diagnostyka wymagane jest dostarczenie serwera nadmiarowego, mogącego zastąpić funkcjonalnie jak i wydajnościowo wymagane w opisie parametry. |
| **Gwarancja** | 3 lata gwarancji producenta serwera w trybie on-site z gwarantowanym czasem reakcji serwisu do końca następnego dnia od zgłoszenia. Naprawa realizowana przez producenta serwera lub autoryzowany przez producenta serwis. |
| **Dokumentacja, inne** | Elementy, z których zbudowane są serwery muszą być produktami producenta tych serwerów lub być przez niego certyfikowane oraz całe muszą być objęte gwarancją producenta, o wymaganym w specyfikacji poziomie SLA.Serwer musi być fabrycznie nowy i pochodzić z oficjalnego kanału dystrybucyjnego w UE.Możliwość aktualizacji i pobrania sterowników do oferowanego modelu serwera w najnowszych certyfikowanych wersjach bezpośrednio z sieci Internet za pośrednictwem strony www producenta serwera. |
| **Serwerowy system operacyjny** | Licencja na serwerowy system operacyjny musi uprawniać do zainstalowania serwerowego systemu operacyjnego w środowisku fizycznym oraz dwóch maszyn wirtualnych tego serwerowego systemu operacyjnego. Licencja musi zostać tak dobrana aby była zgodna z zasadami licencjonowania producenta oraz pozwalała na legalne używanie na oferowanym serwerze. 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:
	1. pozwalają na zmianę rozmiaru w czasie pracy systemu,
	2. umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,
	3. umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów,
	4. 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:
	1. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,
	2. 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:
	1. Login i hasło,
	2. Karty z certyfikatami (smartcard),
	3. 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.
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:
	1. Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC,
	2. 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:
		* Podłączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną,
		* Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,
		* Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza.
		* Bezpieczny mechanizm dołączania do domeny uprawnionych użytkowników prywatnych urządzeń mobilnych opartych o iOS i Windows 8.1.
	3. Zdalna dystrybucja oprogramowania na stacje robocze.
	4. Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej
	5. Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:
		* Dystrybucję certyfikatów poprzez http
		* Konsolidację CA dla wielu lasów domeny,
		* Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen,
		* Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509.
	6. Szyfrowanie plików i folderów.
	7. Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec).
	8. Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów.
	9. Serwis udostępniania stron WWW.
	10. Wsparcie dla protokołu IP w wersji 6 (IPv6),
	11. Wsparcie dla algorytmów Suite B (RFC 4869),
	12. Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows,
	13. 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:
		* Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych,
		* Obsługi ramek typu jumbo frames dla maszyn wirtualnych.
		* Obsługi 4-KB sektorów dysków
		* Nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra
		* Możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API.
		* 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.
 |

8. Licencja na serwerowy system operacyjny.

|  |
| --- |
| **Opis wymagań licencji**  |
| Licencja na serwerowy system operacyjny dla posiadanego serwera wyposażonego w 18-rdzeniowy procesor. Licencja musi uprawniać do zainstalowania serwerowego systemu operacyjnego w środowisku fizycznym oraz dwóch maszyn wirtualnych tego serwerowego systemu operacyjnego. Licencja musi zostać tak dobrana aby była zgodna z zasadami licencjonowania producenta oraz pozwalała na legalne używanie na posiadanym przez Zamawiającego serwerze. 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:
	1. pozwalają na zmianę rozmiaru w czasie pracy systemu,
	2. umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,
	3. umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów,
	4. 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:
	1. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,
	2. 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:
	1. Login i hasło,
	2. Karty z certyfikatami (smartcard),
	3. 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.
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:
	1. Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC,
	2. 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:
		* Podłączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną,
		* Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,
		* Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza.
		* Bezpieczny mechanizm dołączania do domeny uprawnionych użytkowników prywatnych urządzeń mobilnych opartych o iOS i Windows 8.1.
	3. Zdalna dystrybucja oprogramowania na stacje robocze.
	4. Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej
	5. Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:
		* Dystrybucję certyfikatów poprzez http
		* Konsolidację CA dla wielu lasów domeny,
		* Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen,
		* Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509.
	6. Szyfrowanie plików i folderów.
	7. Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec).
	8. Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów.
	9. Serwis udostępniania stron WWW.
	10. Wsparcie dla protokołu IP w wersji 6 (IPv6),
	11. Wsparcie dla algorytmów Suite B (RFC 4869),
	12. Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows,
	13. 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:
		* Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych,
		* Obsługi ramek typu jumbo frames dla maszyn wirtualnych.
		* Obsługi 4-KB sektorów dysków
		* Nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra
		* Możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API.
		* 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.

Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF. |

9. Licencje dostępowe spełniające poniższe wymagania.

|  |
| --- |
| **Opis wymagań licencji**  |
| 1. Licencja dostępowa dla użytkownika umożliwiająca połączenie i wykorzystywanie wszystkich dostępnych funkcjonalności serwera Microsoft Windows Server 2022 z wdrożoną rolą Active Directory. Licencja dla 50 użytkowników.
2. Licencja dostępowa dla użytkownika umożliwiająca połączenie do pulpitu zdalnego serwera Microsoft Windows Server 2022. Licencja dla 50 użytkowników.
3. Licencje umożliwiające użytkownikowi na dostęp z dowolnego urządzenia do zasobów serwera.
4. Licencje pochodzące z legalnego kanału sprzedaży i wolne od wszelkich wad prawnych oraz w szczególności spełniające następujące wymagania:
	1. pozwalają na swobodne przenoszenie pomiędzy serwerami (np. w przypadku wymiany sprzętu);
	2. licencjonowanie uwzględnia prawo do bezpłatnej instalacji udostępnianych przez producenta oprogramowania uaktualnień, poprawek krytycznych i opcjonalnych;
	3. zapewniają możliwość korzystania z wcześniejszych wersji oprogramowania i korzystania z kopii zamiennych (możliwość kopiowania oprogramowania na wiele urządzeń przy wykorzystaniu jednego standardowego obrazu uzyskanego z nośników dostępnych w programach licencji zbiorowych), z prawem do wielokrotnego użycia jednego obrazu dysku w procesie instalacji i tworzenia kopii zapasowych;
	4. są nieograniczone w czasie;
	5. zapewniają możliwość kopiowania oprogramowania na wiele urządzeń przy wykorzystaniu jednego standardowego obrazu uzyskanego z nośników;
	6. są potwierdzone dokumentami, które umożliwiają stwierdzenie legalności oprogramowania dla celów inwentaryzacyjnych i audytowych.
 |

10. Licencja dostępowe dla użytkowników zewnętrznych spełniające poniższe wymagania.

|  |
| --- |
| **Opis wymagań licencji**  |
| 1. Licencja dla jednego serwera, do którego użytkownicy zewnętrzni mają uzyskiwać dostęp. Użytkownik zewnętrzny to osoba, która nie ma typowego dla pracowników dostępu do sieci danej firmy lub sieci jej podmiotów stowarzyszonych i nie korzysta z usług hostowanych, świadczonych przez daną organizację. Licencja przypisana do serwera umożliwia uzyskanie dostępu do niego dowolnej liczbie użytkowników zewnętrznych, o ile beneficjentem tego dostępu jest licencjobiorca, a nie użytkownik zewnętrzny.
2. Licencje pochodzące z legalnego kanału sprzedaży i wolne od wszelkich wad prawnych oraz w szczególności spełniające następujące wymagania:
	1. pozwalają na swobodne przenoszenie pomiędzy serwerami (np. w przypadku wymiany sprzętu);
	2. licencjonowanie uwzględnia prawo do bezpłatnej instalacji udostępnianych przez producenta oprogramowania uaktualnień, poprawek krytycznych i opcjonalnych;
	3. zapewniają możliwość korzystania z wcześniejszych wersji oprogramowania;
	4. są nieograniczone w czasie;
	5. są potwierdzone dokumentami, które umożliwiają stwierdzenie legalności oprogramowania dla celów inwentaryzacyjnych i audytowych.
 |

11. Szafa serwerowa – 2 szt. spełniające poniższe wymagania.

|  |  |
| --- | --- |
| **Nazwa elementu,** **parametru lub cechy**  | **Opis wymagań szafy**  |
| **Wymiary** | 600x1000, wysokość 42U |
| **Parametry** | 1. Szkielet (płyta dolna, płyta górna, cztery słupy).
2. Drzwi przednie i tylne blaszane perforowane (prześwit
3. 80%) z zamkiem trzypunktowym z klamką.
4. Dwie osłony boczne pełne z zamkami jednopunktowymi.
5. Dwie pary belek nośnych 19" o płynnej regulacji położenia.
6. Otwory kablowe o szerokości min. 71 mm w płycie dolnej
7. i górnej.
8. Wszystkie otwory w płycie dolnej i górnej zamknięte
9. wyłamywanymi zaślepkami.
10. Numeracja jednostek U na belkach nośnych.
11. Maksymalny kąt otwarcia drzwi przednich i tylnych min. 180°.
12. Możliwość zmiany kierunku otwierania drzwi.
13. Możliwość ustawienia szafy bez stopek bezpośrednio na podłodze (brak wystających elementów pod szafą).
14. Przystosowania do łączenia szaf w układy szeregowe oraz zabudowy typu Data Box (zimny/gorący korytarz).
 |
| **Wyposażenie** | Listwa uziemieniaLinki uziemienia drzwi i osłonStopki poziomujące |
| **Materiał** | Szkielet, osłony, drzwi, belki nośne, ceowniki - blacha stalowaWysięgniki - odlew znalowy |
| **Stopień ochrony** | IP 20 zgodnie z normą PN-EN 60529 |
| **Wykończenie powierzchni** | Szkielet, osłony, drzwi - malowane farbą proszkową w kolorze RAL 7035 (jasnoszary)Belki nośne, ceowniki - alucynk |
| **Dopuszczalne obciążenie** | 1300 kg  |

12. Przełączniki sieciowe – 2 szt. spełniające poniższe wymagania.

|  |  |
| --- | --- |
| **Nazwa elementu,** **parametru lub cechy**  | **Opis wymagań przełączników**  |
| **Właściwości fizyczne** | 1. Wysokość mak. 1RU, możliwość montażu w szafie 19”
2. Przełącznik sieciowy wyposażony w min. 48 portów 10/100/1000BaseT RJ-45 i min. 4x10G SFP+,
3. Urządzenie musi być wyposażone w redundantne zasilania, zasilacze wymienne typu hot-plug,
4. Urządzenie wyposażone w wymienne moduły wentylatorów,
 |
| **Parametry** | 1. Urządzenie musi obsługiwać minimum 4094 etykiet (ID) VLAN,
2. Urządzenie musi obsługiwać minimum 500 aktywnych sieci VLAN,
3. Urządzenie musi obsługiwać minimum 32 000 adresów MAC,
4. Urządzenie musi obsługiwać minimum 4 000 tras IPv4 i 2000 tras IPv6
5. Urządzenie musi obsługiwać minimum 1 000 wpisów w listach kontroli dostępu Security ACL,
6. Urządzenie musi obsługiwać minimum 1 000 wpisów w listach kontroli QoS ACL,
7. Urządzenie musi obsługiwać minimum 1000 interfejsów SVI,
8. Urządzenie musi obsługiwać co najmniej 48 zagregowanych połączeń typu port-channel,
9. Urządzenia muszą mieć możliwość stackowania do co najmniej 8 urządzeń w pojedynczym stosie,
10. Urządzenie musi obsługiwać co najmniej 16 linków w ramach jednego połączenia zagregowanego typu port-channel LACP,
11. Urządzenie musi posiadać min. 4GB pamięci DRAM i 4GB pamięci flash,
12. Wydajność przełączania minimum 176 Gbps (bez podłączenia do stosu) i min. 336 Gbps (z podłączeniem w stosie),
13. Minimalna wydajność przesyłania pakietów ang. forwarding rate min. 130 Mpps),
14. Urządzenie musi umożliwiać obsługę ramek jumbo o wielkości min. 9198 bajtów
15. Obsługa protokołu NTP
16. Obsługa protokołu DHCP i możliwość uruchomienia serwera DHCP,
17. Obsługa IGMPv1/2/3 i MLDv1/2 Snooping,
18. Obsługa standardu IEEE 802.1ae (MACSec) w tym możliwość szyfrowania ruchu zgodnie z IEEE 802.1ae (MACSec) dla wszystkich portów przełącznika (dla połączeń switch-switch) kluczami o długości 128-bitów (gcm-aes-128) z mechanizmem MACsec Key Agreement (MKA),
19. System operacyjny przełącznika musi umożliwiać wgrywanie poprawek bez konieczności restartowania platformy,
20. Urządzenie powinno być wyposażone w dwa porty konsoli USB Typ B, oraz Ethernet RJ-45
21. Przełącznik musi posiadać makra lub wzorce konfiguracji portów zawierające prekonfigurowane ustawienie rekomendowane przez producenta sprzętu zależnie od typu urządzenia dołączonego do portu,
22. Obsługa protokołu LLDP IEEE 802.1ab i LLDP-MED,
23. Urządzenie musi mieć możliwość zarządzania poprzez interfejs CLI z poziomu portu konsoli,
24. Urządzenie musi mieć możliwość zarządzania poprzez interfejs Web,
25. Przełącznik musi wspierać protokół RESTCONF,
26. Przełącznik musi mieć możliwość lokalną i zdalną obserwację ruchu na określonym porcie, polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego – mechanizmy SPAN, RSPAN,
27. Urządzenie musi mieć zaimplementowaną funkcjonalność sondy IP SLA Responder,
28. Urządzenie musi umożliwiać modyfikację programową takich parametrów urządzenia jak: ilości pozycji w tablicy MAC, ilości tras routingowych unicast i multicast,
29. Plik konfiguracyjny urządzenia musi być możliwy do edycji w trybie off-line (tzn. konieczna jest możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC). Po zapisaniu konfiguracji w pamięci nieulotnej musi być możliwe uruchomienie urządzenia z nową konfiguracją. W pamięci nieulotnej musi być możliwość przechowywania przynajmniej 5 plików konfiguracyjnych,
30. Przełącznik musi obsługiwać protokoły SNMPv3, SSHv2, SCP, sftp (SSH File Transfer Protocol), https, syslog,
31. Urządzenie musi mieć możliwość konfiguracji za pomocą protokołu NETCONF (RFC 6241) i modelowania YANGa (RFC 6020) oraz eksportowania zdefiniowanych według potrzeb danych do zewnętrznych systemów,
32. Przełącznik musi posiadać wbudowany tag RFID w celu łatwiejszego zarządzania infrastrukturą,
33. Urządzenie musi mieć wbudowany port USB umożliwiający podłączenie zewnętrznego nośnika danych. Urządzenie ma możliwość uruchomienia z nośnika danych umieszczonego w porcie USB,
 |
| **Możliwość łączenia w stos** | Urządzenie musi być wyposażone w elementy umożliwiające łączenie w stosy z zachowaniem następujących parametrów:1. Urządzenie musi posiadać możliwość łączenia w klaster z minimum drugim takim samym urządzeniem i urządzenia w klastrze będą się zachowywać jak jedno urządzenie z punktu widzenia warstw L2 i L3,
2. Technologia StackWise Virtual (połączenie kablami StackWise) o przepustowości min. 160 Gbps lub funkcjonalnie taka sama,
3. Możliwość tworzenia połączeń EtherChannel zgodnie z 802.3ad dla portów należących do różnych jednostek w stosie (Cross-stack Link Aggregation)
 |
| **Ciągłość pracy** | Przełącznik musi wspierać następujące mechanizmy związane z zapewnieniem ciągłości pracy:1. IEEE 802.1w Rapid Spanning Tree,
2. Per-VLAN Rapid Spanning Tree (PVRST+),
3. IEEE 802.1s Multi-Instance Spanning Tree,
4. Obsługa 64 instancji protokołu STP;
 |
| **Mechanizmy związane z bezpieczeństwem sieci** | Przełącznik musi wspierać następujące mechanizmy związane z bezpieczeństwem sieci:1. Wiele poziomów dostępu administracyjnego poprzez konsolę. Przełącznik umożliwia zalogowanie się administratora z konkretnym poziomem dostępu zgodnie z odpowiedzią serwera autoryzacji (privilege-level),
2. Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania użytkownika do określonej sieci VLAN,
3. Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania listy ACL,
4. Obsługa funkcji Guest VLAN umożliwiająca uzyskanie gościnnego dostępu do sieci dla użytkowników bez suplikanta 802.1X,
5. Możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC,
6. Możliwość uwierzytelniania użytkowników w oparciu o portal www dla klientów bez suplikanta 802.1X,
7. Możliwość obsługi żądań Change of Authorization (CoA) zgodnie z RFC 5176,
8. Funkcjonalność flexible authentication (możliwość wyboru kolejności uwierzytelniania – 802.1X/uwierzytelnianie w oparciu o MAC adres/uwierzytelnianie oparciu o portal www),
9. Obsługa funkcji Port Security, DHCP Snooping, Dynamic ARP Inspection i IP Source Guard,
10. Zapewnienie podstawowych mechanizmów bezpieczeństwa IPv6 na brzegu sieci (IPv6 FHS) – w tym minimum ochronę przed rozgłaszaniem fałszywych komunikatów Router Advertisement (RA Guard) i ochronę przed dołączeniem nieuprawnionych serwerów DHCPv6 do sieci (DHCPv6 Guard),
11. Możliwość autoryzacji prób logowania do urządzenia (dostęp administracyjny) do serwerów RADIUS i TACACS+,
12. Obsługa list kontroli dostępu (ACL) następujących typów:
	* Port ACL umożliwiające kontrolę ruchu wchodzącego (inbound) na poziomie portów L2 przełącznika,
	* VLAN ACL umożliwiające kontrolę ruchu pomiędzy stacjami znajdującymi się w tej samej sieci VLAN w obrębie przełącznika,
	* Routed ACL umożliwiające kontrolę ruchu routowanego pomiędzy sieciami VLAN,
	* Możliwość konfiguracji tzw. czasowych list ACL (aktywnych w określonych godzinach i dniach tygodnia);
13. Możliwość szyfrowania ruchu zgodnie z IEEE 802.1ae (MACSec) dla wszystkich portów przełącznika (dla połączeń switch-switch) kluczami o długości 128-bitów (gcm-aes-128) z mechanizmem MACsec Key Agreement (MKA),
14. Wbudowane mechanizmy ochrony warstwy kontrolnej przełącznika (CoPP – Control Plane Policing),
15. Funkcja Private VLAN;
 |
| **Routing** | Urządzenie musi wspierać routing statyczny i dynamiczny dla IPv4 i IPv6 w zakresie:1. Routing statyczny dla IPv4 i IPv6,
2. Routing dynamiczny – RIP, OSPF PIM Stub
3. Policy-based routing (PBR),
4. Obsługa protokołu redundancji bramy (VRRP) z obsługą 64 grup,
5. Obsługa 10 tuneli GRE (Generic Routing Encapsulation),
 |
| **Jakość usług** | Przełącznik musi wspierać następujące mechanizmy związane z zapewnieniem jakości usług w sieci:1. Implementacja 8 kolejek dla ruchu wyjściowego na każdym porcie dla obsługi ruchu o różnej klasie obsługi,
2. Implementacja algorytmu Shaped Round Robin dla obsługi kolejek,
3. Możliwość obsługi jednej z powyżej wspomnianych kolejek z bezwzględnym priorytetem w stosunku do innych (Strict Priority),
4. Klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy/docelowy adres MAC, źródłowy/docelowy adres IP, źródłowy/docelowy port TCP,
5. Możliwość ograniczania pasma dostępnego na danym porcie dla ruchu o danej klasie obsługi z dokładnością do 8 Kbps (policing, rate limiting),
6. Kontrola sztormów dla ruchu broadcast/multicast/unicast,
7. Możliwość zmiany przez urządzenie kodu wartości QoS zawartego w ramce Ethernet lub pakiecie IP – poprzez zmianę pola 802.1p (CoS) oraz IP ToS/DSCP;
 |
| **Oprogramowanie** | Przełącznik powinien być zgodny z oprogramowaniem spełniającym poniższe parametry:1. Możliwość próbkowania (bez samplowania) i eksportu statystyk ruchu do zewnętrznych kolektorów danych ze wsparciem sprzętowym dla protokołu NetFlow – obsługa 16000 strumieni (flow),
2. Realizacja rozszerzenia protokołu NetFlow w postaci tzw. Flexible NetFlow, który umożliwia monitorowanie większej ilości informacji zawartej w pakiecie danych od warstw 2 do 7, bardziej granularne monitorowanie ruchu i definiowanie monitorowanych przepływów (flow) poprzez elastyczne definiowanie pól kluczowych,
3. Możliwość tworzenia skryptów celem obsługi zdarzeń, które mogą pojawić się w systemie,
 |
| **Pozostałe wymagania** | Oferowany sprzęt musi spełniać wymagania:1. musi być fabrycznie nowy,
2. nie może być refabrykowany lub ponownie wprowadzony na rynek,
3. musi pochodzić z oficjalnego kanału sprzedaży polskiej dystrybucji producenta,
4. będzie dostarczony w oryginalnych i nienaruszonych opakowaniach producenta,
5. będzie oznakowany w taki sposób, aby była możliwa jednoznaczna identyfikacja producenta i produktu,
6. wszystkie oferowane urządzenia muszą posiadać numer seryjny producenta umieszczony na obudowie,
7. będzie dostarczony wraz z instrukcją obsługi w języku polskim lub angielskim,
8. musi posiadać wsparcie producenta na danego typu sprzęt poprzez:
	1. udostępnienie na witrynie producenta pełnej dokumentacji użytkowej i technicznej sprzętu, co najmniej w języku polskim lub angielskim,
	2. udostępnienie w witrynie producenta wszystkich sterowników oprogramowania i uaktualnień. System udostępniony użytkownikom w witrynie producenta musi automatycznie wyszukiwać i udostępniać do ściągnięcia komplet oprogramowania i dokumentacji właściwych tylko dla konkretnego sprzętu, zidentyfikowanego przez numer fabryczny lub numer modelu. Do oferty należy dołączyć bezpośredni adres strony potwierdzającej spełnienie ww. wymagania,
 |
| **Gwarancja** | Oferowany sprzęt musi być objęty gwarancją producenta na okres 36 miesięcy i wsparciem Wykonawcy na okres 36 miesięcy określonym jako 8x5xNBD (8 - zgłoszenie w godzinach pracy 8:00-16:00, 5 - zgłoszenia w dni robocze, NBD - z wymianą na następny dzień roboczy) z opcją wymiany urządzenia na następny dzień roboczy po przyjęciu zgłoszenia przez Wykonawcę w przypadku przełączników sieciowych oraz 12 miesięcy gwarancji w przypadku akcesoriów służących do skompletowania i podłączenia urządzeń (między innymi kable, moduły i wkładki).Zamawiający będzie miał możliwość dokonywania zgłoszeń poprzez:1. polskojęzyczny punkt serwisowy Wykonawcy oraz serwis telefoniczny Wykonawcy, pracujący co najmniej w godzinach 8-16 we wszystkie dni robocze, bezpłatnie lub w cenie połączenia lokalnego w całej Polsce

lub 1. pocztę elektroniczną e-mail zapewniającą przyjmowanie zgłoszeń serwisowych przez 24h na dobę,

Naprawy będą dokonywane w miejscu użytkowania sprzętu lub poza nim, jeżeli dokonanie naprawy w miejscu użytkowania sprzętu okaże się niemożliwe,W przypadku przyjęcia sprzętu do naprawy Wykonawca zobligowany jest dostarczyć sprzęt zastępczy (urządzenia zastępcze), o parametrach nie gorszych niż naprawiany, w terminie do końca bieżącego dnia roboczego od momentu przekazania sprzętu do naprawy.Zamawiający nie ponosi kosztów napraw i związanych z naprawami, w tym odbioru i dostawy sprzętu oraz sprzętu zastępczego. Rozbudowa przełącznika macierzystego o dostarczone akcesoria nie spowoduje utraty gwarancji na pozostałe elementy, w tym na przełącznik. |
| **Certyfikaty** | Wszystkie oferowane urządzenia muszą posiadać widoczne i czytelne oznaczenie znakiem CE oraz dostarczaną wraz z urządzeniem, ważną deklarację zgodności z normami zharmonizowanymi CE. |

13. Zasilacz awaryjny – 1 szt. spełniający poniższe wymagania.

|  |  |
| --- | --- |
| **Nazwa elementu,** **parametru lub cechy**  | **Opis wymagań zasilacza awaryjnego**  |
| **Minimalne wymagania techniczne dla jednostki UPS** | 1. Moc znamionowa jednostki nie mniej niż 8000VA / 8000W
2. Montaż w szafie rack
3. Technologia Podwójnej konwersji (online)
4. Klasa VFI-SS-111 zgodnie z PN-EN62040-1
5. Temperatura eksploatacji 0 - 40 °C
6. Wilgotność względna podczas pracy 0 - 95 %
7. Wysokość n.p.m. podczas pracy 0-10000metrów
8. Hałas słyszalny w odległości 1 m od powierzchni urządzenia 55,0dBA
9. Rozpraszanie ciepła w trybie online ≤1497,00 BTU/h
10. Sprawność:
11. Praca on-line ≥ 94% przy pełnym obciążeniu
12. Klasa ochrony IP 20
13. Klasa energetyczna sprzętu przeciwprzepięciowego 480J
 |
| **Parametry wejściowe** | 1. Nominalne napięcie wejściowe 220 V/380 V, 230 V/400 V, 240 V/ 415 V
2. Częstotliwość wejściowa 40–70 Hz (wykrywanie automatyczne)
3. Typ gniazda wejściowego: Hard Wire 3 wire (1PH+N+G), Hard Wire 5-wire (3PH + N + G)
4. Zmienny zakres napięcia wejściowego w trybie podstawowym 160 – 476 VAC połowa obciążenia 100/173 – 275/476 VAC
5. Inne napięcia wejściowe 220, 240, 380, 415 (nastawa z wyświetlacza)
6. Możliwość podłączenia dwóch niezależnych źródeł zasilania
 |
| **Parametry wyjściowe** | 1. Napięcie wyjściowe 230VAC
2. Zniekształcenia napięcia wyjściowego ≤0,01%
3. Częstotliwość na wyjściu (zsynchronizowana z siecią zasilającą) 50/60Hz ±0.1Hz
4. Inne napięcia wyjściowe 220, 240
5. Współczynnik szczytu 3: 1
6. Typ przebiegu sinusoida
7. Złącza/gniazda wyjściowe
8. (6) IEC 320 C13
9. (4) IEC 320 C19
10. Hard wire 3-wire (H N + E)
11. Układ obejściowy (bypass) wewnętrzny tor obejściowy (automatyczny lub ręczny)
 |
| **Akumulatory i czas podtrzymania** | 1. Typ akumulatora bezobsługowy szczelny akumulator kwasowo-ołowiowy z elektrolitem w postaci żelu szczelny
2. Zasilacz awaryjny w dostarczonej konfiguracji misi zapewniać czas podtrzymania:
	* Min.24 minuty dla pełnego obciążenia
	* Min.55 minut dla połowy obciążenia
3. Typowy czas ładowania ≤1,5 godziny
4. Oczekiwana żywotność akumulatora (lata) 3 – 5
5. Rozszerzalny czas podtrzymania za pomocą dodatkowych modułów
6. Baterie wymieniane na gorąco
7. Opcje przedłużonego podtrzymania zasilania: do 10 zewnętrznych modułów akumulatorowych
 |
| **Komunikacja i zarządzanie** | 1. Gniazdo do montażu karty WEB/SNMP- Smart Slot x1
2. Moduł WEB/SNMP obsługiwane protokoły komunikacyjne:

IP v.4 i v.6SNMP v.3HTTPS/SSL, SSH z kluczem do 2048 bitTLSSMTP, NTP, FTP, TelnetModbus TCP1. Port uniwersalny do podłączenia np. czujnika temperatury (jeden czujnik temperatury dostarczyć w komplecie z UPS)
2. Porty komunikacyjne: RJ-45 10/100 Base-T, RJ-45 Serial, Smart-Slot, USB
3. Panel sterowania: Wielofunkcyjna konsola sterownicza i informacyjna LCD
4. Alarm dźwiękowy: Alarmy dźwiękowe i wizualne według priorytetu ważności zdarzenia
5. Awaryjny wyłącznik zasilania (EPO) : Tak
 |
| **Certyfikaty zgodności**  | CE, EAC, EN/IEC 62040-1, EN/IEC 62040-2, RCM, VDE |
| **Gwarancja** | 3 lata gwarancji naprawy lub wymiany (bez akumulatora) i 2 lata na akumulatory, z możliwością przedłużenia o 3 lata. |
| **Oprogramowanie** | Dostępne oprogramowanie do zarządzania/monitorigu (niektóre wersje odpłatne) z VMware® ESXi (VMware® ESXi Server 6.5 Update 3 (vMA 6.5), VMware® ESXi Server 6.5 Update 2 (vMA 6.5)); Microsoft® Hyper-V (Windows® Hyper-V Server 2019, 2012 R2); Windows® Server 2019, 2016, 2012; Windows® 10, 7; Red Hat® Enterprise Linux; SuSE® Linux®. |
| **Inne** | Zasilacz UPS mus być wyposażony w sterowane programowo gniazda wyjściowe (co najmniej dwie grupy gniazd). |

14. Konsola KVM – 1 szt. spełniająca poniższe wymagania.

|  |  |
| --- | --- |
| **Nazwa elementu,** **parametru lub cechy**  | **Opis wymagań konsoli KVM**  |
| **Funkcjonalność** | 1. Obsługa 16 komputerów/serwerów poprzez dedykowane porty SPHD
2. Interfejs obsługujący porty PS/2 oraz USB
3. Wsparcie dla klawiatur USB PC, Mac oraz Sun
4. Automatyczne wykrywanie rodzaju podłączonego interfejsu
5. Emulacja klawiatury i myszy umożliwiająca start podłączonego serwera mimo iż konsola przełączona jest na inny port
6. Możliwość przełączania między zarządzanymi serwerami za pomocą przycisków na panelu, kombinacji klawiszy lub menu ekranowego
7. Wsparcie dla platform Windows/Linux/Mac oraz Sun
 |
| **Porty** | 16 x SPHD porty KVM, 1 x port konsolowy SPHD (męski), 1 x port RJ45 (port LAN do zdalnego zarządzania), 1 x port RJ11 dla aktualizacji oprogramowania urządzenia, 1 x port zasilania , 2 x porty USB typu A, 1 x port DB-25 (do podłączenia kolejnych przełączników KVM) |
| **Grafika** | Wbudowany ekran 19 cali z podświetleniem LED o rozdzielczości 1280x1024 75Hz, kąt widzenia min: 170° (w poziomie), 160° (w pionie), współczynnik kontrastu: 1000:1 , Luminancja: 250 cd/m², przy dostępie zdalnym maksymalna rozdzielczość 1920x1200 60Hz. |
| **Rozmiar** | 1U z możliwością montażu w szafie RACK 19”; do urządzenia należy dostarczyć komplet wyposażenia montażowego.Głębokość nie może przekraczać 69 cm. |
| **Obudowa** | Podświetlana klawiatura za pomocą diody LED.Wbudowane urządzenie wskazujące (trackball lub touchpad). |
| **Zarządzanie** | 1. Dwupoziomowe zabezpieczenie hasłem
2. Możliwość kontroli do 256 komputerów/serwerów (przy połączeniu łańcuchowym kolejnych przełączników KVM)
3. Możliwość aktualizacji oprogramowania wbudowanego – kabel w zestawie
4. Możliwość odłączania oraz podłączania serwerów/komputerów bez konieczności wyłączania urządzenia
5. Funkcja duplikowania sygnałów z klawiatury i myszy na wszystkich serwerach jednocześnie
6. Obsługa multimedialnych klawiatur USB dla Windows, Mac i SUN
7. Obsługa zewnętrznej myszy USB
8. Aktualizacja oprogramowania dla wszystkich połączonych łańcuchowo przełączników KVM w tym samym czasie poprzez kabel daisy-chain
9. Obsługa uwierzytelniania: RADIUS, LDAP, LDAPS, MS Active Directory
10. Zdalne zarządzanie po TCP/IP
11. Możliwość wybrania dowolnej kombinacji metod szyfrowania: DES, 3DES, AES, RC4 lub losowy w celu niezależnego szyfrowania komunikacji z klawiaturą/myszą i sygnałem wizyjnym,
12. Obsługa protokołów TLS 1.2 / RSA 2048-bit
13. Dostęp na poziomie BIOS
 |
| **Gwarancja** | 24 miesiące. |
| **Akcesoria** | Komplet 14 szt. przewodów do podłączenia serwerów USB/VGA: 2 kable o długości min. 1,8m, 10 kabli KVM o długości min. 3m, 1 przewód do zasilania, 1 kabel do aktualizacji firmware, 1 kabel konsolowy VGA/USB/PS2 |

15. Przełącznik sieciowy – 1 szt. spełniający poniższe wymagania.

|  |  |
| --- | --- |
| **Nazwa elementu,** **parametru lub cechy**  | **Opis wymagań przełączników**  |
| **Właściwości fizyczne** | 1. Wysokość mak. 1RU, możliwość montażu w szafie 19”
2. Przełącznik sieciowy wyposażony w min. 12 portów 100M/1G/2,5G/5G/10G RJ-45 oraz 2 współdzielone porty SFP+
3. 2 wentylatory aktywne
4. Wewnętrzny zasilacz
 |
| **Pamięć buforowania pakietów** | Min. 3MB |
| **Rozmiar tablicy adresów MAC** | Min. 32 tys. |
| **Obsługiwana liczba VLAN** | Min. 64 |
| **Obsługa grup transmisji Multicast** | Min. 128 |
| **Rozmiar ramki Jumbo**  | 9 KB |
| **Przepustowość** | Min. 240 Gb/s |
| **Prędkość przekazywania** | 178 Mpps (64 byte) |
| **Opóźnienie** | Max. 4.3us (10G)Max. 3.76us (1G) |
| **QoS** | Port-based QoS, IEEE 802.1p COS, IPv4 DSCP, IPv4 ToS, Weighted Round Robin (WRR) |
| **Protokół routingu** | IGMP, IGMPv2, IGMPv3 |
| **Grupy multicast IGMP** | Min. 128 |
| **Protokół zdalnego zarządzania** | HTTP, TFTP, graficzny interfejs użytkownika oparty na przeglądarce internetowej |
| **Obsługiwane protokoły i standardy** | IEEE 802.3, IEEE 802.3u, IEEE 802.3z, IEEE 802.1Q, IEEE 802.3ab, IEEE 802.1p, IEEE 802.3x, IEEE 802.3ae, IEEE 802.3an, IEEE 802.3az, IEEE 802.3bz |
| **Temperatura robocza** | 0–50°C |
| **Waga** | Max. 2,55 kg |
| **Zużycie energii** | Max. 77W |
| **Poziom hałasu** | Max. dBA (25°C) |
| **Certyfikaty** | ANSI C63.4:2014, EN 55024:2010, EN 61000-3-2:2014, Class A, EN 60950-1: 2006 + A11:2009 + A1:2010 + A12:2011 + A2:2013, IEC 60950-1:2005 (ed.2)+A1:2009+A2:2013 |
| **Gwarancja** | Dożywotnia ograniczona gwarancja producenta |

1. Wykonawca wdroży, zintegruje całość sprzętu i oprogramowania będącego przedmiotem zamówienia oraz przeprowadzi migrację i integrację wskazanych niżej elementów środowiska informatycznego na przedmiotową infrastrukturę.

Wykonawca zobligowany jest do podziału prac i realizacji zgodnie z niżej ustalonymi etapami:

1. Analiza i inwentaryzacja obecnie wykorzystywanej infrastruktury pod kątem dalszych prac migracyjnych.
2. Fizyczny montaż i okablowanie sprzętu w miejscu wskazanym przez zamawiającego.
3. Przygotowanie planu wdrożenia.
4. Konfiguracja dostarczonego sprzętu i oprogramowania zgodnie z przygotowanym i zaakceptowanym planem wdrożenia o którym mowa w punkcie 3.
5. Migracja środowiska do nowo zainstalowanej infrastruktury zgodnie z przygotowanym i zaakceptowanym planem wdrożenia o którym mowa w punkcie 3. Przygotowanie dokumentacji powdrożeniowej oraz szkolenia personelu w zakresie dostarczonego sprzętu.

Ad. 1. Analiza i inwentaryzacja obecnie wykorzystywanej infrastruktury pod kątem dalszych prac migracyjnych.

Zamawiający korzysta w tej chwili z następującego oprogramowania będącego przedmiotem migracji:

W części KKM i SIP klaster HA Microsoft obejmujący następujące funkcjonalności:

1. Aplikacja KKM - Kieleckiej Karty Miejskiej, dostawca R&G Mielec, serwer wirtualny Windows Server 2008 R2
2. Aplikacja CNR – Centrum Nadzoru Ruchu, dostawca R&G Mielec, serwer wirtualny Windows Server 2008 R2
3. Aplikacja SIP - Systemu Informacji Pasażerskiej, dostawca R&G Mielec, serwer wirtualny Windows Server 2008 R2
4. Serwer komunikacyjny - oprogramowanie do komunikacji z pojazdami oraz integracji z aplikacją SIP, dostawca R&G Mielec, Windows Server 2008 R2
5. Serwer WWW KKM – serwis WWW Kieleckiej Karty Miejskiej, dostawca R&G Mielec, serwer wirtualny Windows Server 2008 R2
6. Serwer WWW SIP – serwis WWW Systemu Informacji Pasażerskiej, dostawca R&G Mielec, serwer wirtualny Windows Server 2008 R2
7. Serwer Bazodanowy dla SIP i KKM – baza danych IBM DB2, integrator R&G Mielec, serwer wirtualny Windows Server 2008 R2
8. System do monitorowania automatów biletowych stacjonarnych , dostawca Trapeze Niemcy, serwer wirtualny Windows Server 2008 R2
9. Kontroler domeny (SIP i KKM) , Windows Server 2008 R2, serwer fizyczny
10. Serwer kopii zapasowej Veeam Backup, Windows Server 2008 R2, serwer fizyczny

W części Administracyjnej klaster HA Microsoft obejmujący następujące funkcjonalności:

1. System do planowania komunikacji BUSMAN, dostawca AGC – serwer wirtualny Windows Server 2012 R2
2. Serwer systemu Eset NOD32, – serwer wirtualny Windows Server 2012
3. System do monitorowania automatów biletowych mobilnych, dostawca Trapeze Niemcy, serwer wirtualny Windows Server 2012 R2
4. Kontroler domeny (część biurowa) , Windows Server 2008 R2, serwer fizyczny
5. Serwer kopii zapasowej Veeam Backup, Windows Server 2008 R2, serwer fizyczny

Klaster HA obejmujący dwa serwery fizyczne z systemem Linux pełniących rolę serwera komunikacyjnego do komunikacji systemu SIP z tablicami informacyjnymi na terenie miasta, dostawca R&G Mielec oraz NiT

Zamawiający wymaga na tym etapie przygotowania inwentaryzacji wszystkich w/w systemów, opracowania zależności, tak aby Wykonawca mógł zrozumieć w pełni mechanizmy działania aplikacji, co pozwoli na opracowanie optymalnego planu wdrożenia.

Wynikiem prac tego etapu będzie zaakceptowana przez Zamawiającego plan projektu uwzględniający m.in.:

1. Koncepcję wdrożenia
2. Grupowanie zadań
3. Zakres oraz kolejność prowadzenia prac;
4. Opis przewidywanych do zastosowania mechanizmów;
5. Przewidywane godziny pracy oraz wymagane okna serwisowe. Z uwagi na specyfikę działalności Zamawiającego większość prac będzie musiało odbywać się poza aktywnymi godzinami pracy lub w dni wole od pracy. Należy uwzględnić również, że z uwagi na publiczny charakter świadczonych usług Zamawiający musi odpowiednio wcześniej komunikować ograniczenie dostępu do usług.

Ad. 2. Fizyczny montaż i okablowanie sprzętu w miejscu wskazanym przez zamawiającego.

Etap obejmuje montaż wszystkich dostarczonych elementów w serwerowni wskazanej przez Zamawiającego, oraz ewentualną relokację i konfigurację wyposażenia dotychczas użytkowanej serwerowni w zakresie wskazanym przez Zamawiającego. Zamawiający przed przystąpieniem do realizacji projektu przekaże Wykonawcy wszystkie wymagane do jego realizacji informacje o dotychczas eksploatowanej infrastrukturze. W szczególności należy uwzględnić migrację urządzeń brzegowych UTM które m.in. pełnią rolę punktu końcowego dla transmisji danych z pojazdów których autokomputery pracują w prywatnym APNie. Wykonawca musi zadbać o pełną koordynację w trakcie zmiany lokalizacji serwerów współpracujących z urządzeniami w APN.

Ad. 3. Przygotowanie planu wdrożenia

Przed przystąpieniem do dalszych prac Wykonawca przedstawi do akceptacji plan wdrożenia obejmujący harmonogram oraz kompletną ścieżkę migracji poszczególnych elementów systemu.

Zamawiający dopuszcza przeprowadzenie migracji testowej umożliwiającej opracowanie w pełni powtarzalnej, skutecznej ścieżki migracyjnej. Testy będą mogła odbyć się tylko i wyłącznie pod nadzorem i w siedzibie Zamawiającego.

Zamawiający zastrzega sobie możliwość weryfikacji oraz wykonania testów funkcjonalnych poszczególnych elementów systemu na każdym etapie wdrożenia przed wydaniem zgody na finalną migrację.

Zakres prac wymagany do uwzględnienia w projekcie oraz dalszej realizacji:

1. Budowa klastra pracy awaryjnej w systemie Windows Server
2. Migracja aktualnie użytkowanego systemu Active Directory(część SIP i KKM) do najnowszej wersji (Windows Server 2022) wraz z podniesieniem funkcjonalności domeny oraz wycofaniem z eksploatacji dotychczas użytkowanych kontrolerów domeny
3. Migracja aplikacji KKM - Kieleckiej Karty Miejskiej do Windows Server 2022 oraz nowo utworzonego klastra pracy awaryjnej a w szczególności:
4. Aplikacja MUNICOM
5. Aplikacja MUNICOM.premium (wystawienia faktur)
6. Aplikacja WPF (Common, Analizy, Dyspozytor, Rejestry, Rozkład Jazdy)
7. Usługa XmlDiagnostic
8. Usługa McDiag
9. GTFS Standard i Real time export
10. Podkład mapowy Openstreet
11. Serwis do obsługiwania aplikacji MyBus
12. Strona rozkładowa / strona administracyjna
13. Webserwis SMS
14. Webserwis WSEBILET
15. Webserwis Wshectronic
16. Webserwis WSEBILET
17. Strona biletowa KKM
18. Migracja aplikacji CNR – Centrum nadzoru ruchu do Windows Server 2022 oraz nowo utworzonego klastra pracy awaryjnej, w szczególności:
19. CNR dla WebService Dyspozytor
20. Api Udostępniające dane
21. Big Brother
22. CNr
23. Cnr dla Webserwis
24. Jakość powietrza
25. Kasowanie stanu pojazdów
26. Odczyt statusów z serwera komunikacyjnego
27. Rozsyłanie linii informacyjnych
28. Rozsyłanie RJ dla tablic TIP
29. Stan pojazdów CNR do DN2
30. Tworzenie SQL RJ dla CNR
31. Migracja Systemu Informacji Pasażerskiej do Windows Server 2022 oraz nowo utworzonego klastra pracy awaryjnej
32. Migracja serwera komunikacyjnego GSM/WIFI/URVE R&G do Windows Server 2022 oraz nowo utworzonego klastra pracy awaryjnej
33. Migracja Serwerów WWW KKM i SIP do Windows Server 2022 oraz nowo utworzonego klastra pracy awaryjnej, w szczególności:
34. Instalacja i konfiguracja komponentów serwera IIS
35. konfiguracja zapory Windows (wyjątki komunikacyjne dla usług)
36. Instalacja i konfiguracja klienta Db2 dla usług WWW
37. Instalacja i konfiguracja usług dla aplikacji MyBus
38. Instalacja i konfiguracja strony rozkładowej
39. Instalacja i konfiguracja podkładu mapowego
40. Instalacja i konfiguracja strony www
41. Webserwis SMS
42. Webserwis Wshectronic
43. Webserwis WSEBILET
44. Aktualizacja Bazy danych IBM DB2, aktualnie użytkowana jest baza w wersji 9.7, Zamawiający wymaga przeprowadzenie procesu konwersji oraz migracji do najnowszej wersji DB2 Community Edition. Wykonawca odpowiada za przeprowadzenie prac developerskich dostosowujących dotychczasowe oprogramowanie bazy danych do nowej wersji silnika praz korekty w w/w systemach opartych o przedmiotową bazę danych. Wykonawca uruchomi nowe środowisko w systemie Windows Server 2022
45. Migracja Systemu do planowania komunikacji BUSMAN z opcją aktualizacji do Windows Server 2022 oraz nowo utworzonego klastra pracy awaryjnej
46. Migracja systemu zarządzania Serwer systemu Eset NOD32 do Windows Server 2022 oraz nowo utworzonego klastra pracy awaryjnej
47. Migracja aktualnie użytkowanego systemu Active Directory (część biurowa) do najnowszej wersji (Windows Server 2022) wraz z podniesieniem funkcjonalności domeny oraz wycofaniem z eksploatacji dotychczas użytkowanych kontrolerów domeny
48. Migracja Systemu do monitorowania automatów biletowych mobilnych z opcją aktualizacji do Windows Server 2022 oraz nowo utworzonego klastra pracy awaryjnej,
49. Migracja do środowiska wirtualnego oraz integracja z nowo utworzonym klastrem pracy awaryjnej serwera komunikacyjnego NiT/R&G
50. Wdrożenie systemu kopii zapasowej
51. Wszelkie inne prace wskazane na etapie analizy przez Zamawiającego.

Ad. 4. Konfiguracja dostarczonego sprzętu i oprogramowania zgodnie z przygotowanym i zaakceptowanym planem wdrożenia o którym mowa w punkcie 3, a w szczególności:

1. Aktualizacja oprogramowania układowego we wszystkich dostarczonych urządzeniach do najnowszej, stabilnej wersji zalecanej przez producenta
2. Instalacja/konfiguracja systemów operacyjnych
3. Konfiguracja modułów zarządzania serwerów
4. Konfiguracja przełączników SAN w oparciu o wymagania projektu, w szczególności skrupulatne oznaczenie portów (aliasy) oraz zoning.
5. Konfiguracja macierzy dyskowej w oparciu o wymagania projektu

Ad. 5. Migracja środowiska do nowo zainstalowanej infrastruktury zgodnie z przygotowanym i zaakceptowanym planem wdrożenia – wykonawca zrealizuje migrację zgodnie z harmonogramem oraz planem wdrożenia przedstawionym i zaakceptowanym przez Zamawiającego w toku wcześniejszych etapów projektu.

Ad. 6. Przygotowanie dokumentacji powdrożeniowej oraz szkolenia personelu w zakresie dostarczonego sprzętu oraz oprogramowania

Wykonawca przygotuje dokumentację powykonawczą obejmującą szczegółową konfigurację dostarczonego sprzętu a w szczególności:

1. Opis przeprowadzonych prac
2. Zestawienie danych inwentarzowych
3. Opis konfiguracji serwerów
4. Poglądowy schemat wdrożonej infrastruktury sprzętowej
5. Opis konfiguracji klastra pracy awaryjnej
6. Opis konfiguracji urządzeń sieci SAN
7. Opis konfiguracji zasilaczy awaryjnych
8. Inne, istotne z punktu widzenia bezproblemowej eksploatacji dostarczonego sprzętu

Wykonawca w terminie uzgodnionym z Zamawiającym przeprowadzi szkolenie w wymiarze minimum 6 h dla pracowników obejmujące wdrożone mechanizmy oraz eksploatację dostarczonych urządzeń. Szkolenie musi odbyć się w siedzibie Zamawiającego przy sprzęcie, nie dopuszcza się formy zdalnej.