

# dodatek nr 3 do SIWZ

**SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA**

**- Specyfikacja techniczna / funkcjonalna.**

do postępowania o zamówienie publiczne w trybie przetargu nieograniczonego powyżej kwot określonych w przepisach wydanych na podstawie art. 11 ust. 8 ustawy, czyli powyżej 214 tys. euro

na zadanie pn.:

***„Rozbudowa szpitalnych systemów HIS, modernizacja infrastruktury sprzętowej i sieciowej oraz dostawę Platformy Zintegrowanych Systemów Informatycznych dla: Szpitala Międzyrzeckiego Sp. z o.o. w Międzyrzeczu, Szpitala dla Nerwowo i Psychicznie Chorych w Międzyrzeczu, Samodzielnego Publicznego Zakładu Opieki Zdrowotnej w Sulechowie, Samodzielnego Publicznego Zakładu Opieki Zdrowotnej w Sulęcinie”***

Przedmiot zamówienia dofinansowany w ramach projektu pn. „Rozwój e-usług w szpitalach powiatowych w Międzyrzeczu, Sulęcinie i Sulechowie oraz w Szpitalu dla Nerwowo i Psychicznie Chorych w Międzyrzeczu” realizowanym w ramach Regionalnego Programu Operacyjnego – Lubuskie 2020 na lata 2014-2020, Oś Priorytetowa 2 – Rozwój Cyfrowy, Działanie 2.1 Rozwój Społeczeństwa Informacyjnego

**Nr sprawy ZP/N/07/20**

Projekt współfinansowany przez Unię Europejską realizowany w ramach Regionalnego Programu Operacyjnego – Lubuskie 2020



***Informacja dla Wykonawców:***

Niniejszy dokument określa minimalne wymagania dla infrastruktury sprzętowej oraz centrum autoryzacji, które powinny zostać dostarczone dla każdego z Partnerów w ramach realizacji projektu pn.: Rozbudowa szpitalnych systemów HIS, modernizacja infrastruktury sprzętowej i sieciowej oraz dostawę Platformy Zintegrowanych Systemów Informatycznych dla: Szpitala Międzyrzeckiego Sp. z o.o. w Międzyrzeczu, Szpitala dla Nerwowo i Psychicznie Chorych w Międzyrzeczu, Samodzielnego Publicznego Zakładu Opieki Zdrowotnej w Sulechowie, Samodzielnego Publicznego Zakładu Opieki Zdrowotnej w Sulęcinie” (dalej projekt) współfinansowany jest przez Unię Europejską ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Regionalnego Programu Operacyjnego – Lubuskie 2020 oraz Regulamin Konkursu Nr RPLB.02.01.01-IZ.00-08-K01/16 w ramach Regionalnego Programu Operacyjnego – Lubuskie 2020, Osi Priorytetowej 2 – ROZWÓJ CYFROWY dla Działania 2.1 Rozwój społeczeństwa informacyjnego dla Poddziałania, 2.1.1 Rozwój społeczeństwa informacyjnego.

Urządzenia i oprogramowanie mają zostać dostarczone i wdrożone osobno dla każdego z 4 Partnerów projektu tj.:

1. Szpital Międzyrzecki Sp. z o.o. w Międzyrzeczu
2. Samodzielny Publiczny Szpital dla Nerwowo i Psychicznie Chorych w Międzyrzeczu
3. Samodzielny Publiczny Zakład Opieki Zdrowotnej w Sulęcinie
4. Samodzielny Publiczny Zakład Opieki Zdrowotnej w Sulechowie

Projekt współfinansowany przez Unię Europejską realizowany w ramach Regionalnego Programu Operacyjnego – Lubuskie 2020 na lata 2014-2020, Oś Priorytetowa 2 – Rozwój Cyfrowy, Działanie 2.1 Rozwój Społeczeństwa Informacyjnego.



**I. Infrastruktura sprzętowa wraz z Centrum Autoryzacji dla Szpitala Międzyrzeckiego Sp. z o.o.**

|  |  |  |  |
| --- | --- | --- | --- |
| **1. Szafa RACK – 2 szt.** | | | |
| **Lp.** | **Wymagane minimalne parametry techniczne** | **Wymóg do spełnienia (warunek graniczny)** | **OFEROWANE PARAMETRY TECHNICZNE - podaje**  **Wykonawca**  **Wymogi dotyczące opisu oferowanych parametrów:**  TAK – wykonawca spełnia konkretny parametr przy czym Zamawiający oczekuje by w przypadku wymagań dotyczących minimalnych parametrów opisać szczegółowo parametry oferowane przez wykonawcę  NIE – wykonawca nie spełnia konkretnego parametru |
| **OGÓLNE** | | | |
| **1.** | 42U pojemności użytecznej do instalacji urządzeń w pozycji poziomej o wymiarach nie mniejszych niż 800mmx1000mm(Szer/gł) | TAK |  |
| **2.** | wyposażona w przednie drzwi perforowane, zamykane na zamek z kluczem, jednoskrzydłowe, możliwość montażu lewa/prawa strona, możliwość zdjęcia bez użycia narzędzi\* | TAK |  |
| **3.** | wyposażona w tylne drzwi perforowane, dwuskrzydłowe dla ograniczenia przestrzeni serwisowej, zamykane na zamek z kluczem wspólny z zamkiem przednim, możliwość zdjęcia bez użycia narzędzi\* | TAK |  |
| **4.** | Minimalna klasa ochrony na poziomie IP 20\* | TAK |  |
| **5.** | wyposażona w zdejmowane panele boczne \* | TAK |  |
| **6.** | wszystkie wolne „U” zaślepione zaślepkami\* | TAK |  |
| **7.** | przystosowana do poprawnej instalacji dostarczonych serwerów rack wraz z ich fabrycznymi prowadnicami przewodów.\* | TAK |  |
| **8.** | zainstalowane 2 listwy zasilające min. 8 gniazd ,2 półki o głębokości min. 450mm | TAK |  |
| **9.** | Minimalny udźwig szafy co najmniej 900 kg | TAK |  |
| **10.** | Certyfikaty CE, RoHS | TAK |  |
| **11.** | Gwarancja 5 Lat\* | TAK |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **2. Zasilacz awaryjny UPS – 2 szt.** | | | |
| **Lp.** | **Wymagane minimalne parametry techniczne** | **Wymóg do spełnienia (warunek graniczny)** | **OFEROWANE PARAMETRY TECHNICZNE - podaje**  **Wykonawca**  **Wymogi dotyczące opisu oferowanych parametrów:**  TAK – wykonawca spełnia konkretny parametr przy czym Zamawiający oczekuje by w przypadku wymagań dotyczących minimalnych parametrów opisać szczegółowo parametry oferowane przez wykonawcę  NIE – wykonawca nie spełnia konkretnego parametru |
| **OGÓLNE** | | | |
| **1.** | Typ zasilacza: online\* | TAK |  |
| **2.** | Możliwość montażu w szafie RACK przy zajętości maksymalnie 3U | TAK |  |
| **3.** | Moc pozorna 5kVA\* | TAK |  |
| **4.** | Moc rzeczywista 4,5 kW\* | TAK |  |
| **5.** | Minimalne podtrzymanie- 3 minuty przy 100% obciążeniu | TAK |  |
| **6.** | Minimalne podtrzymanie- 10 minuty przy 50% obciążeniu | TAK |  |
| **7.** | W standardzie minimum:  - min. 6x IEC 320 C13 (10A)  - min. 2x IEC 320 C19 (16A)  - 1x RJ45 | TAK |  |
| **8.** | Aplikacja do automatycznego zamykania wspieranych systemów operacyjnych w przypadku braku zasilania\* | TAK |  |
| **9.** | Możliwość wymiany akumulatorów podczas pracy\* | TAK |  |
| **10.** | Wspierane i certyfikowane systemy operacyjne: Microsoft® Windows Server® 2012 R2, SUSE Linux Enterprise Server, Red Hat Enterprise Linux, VMware Infrastructure | TAK |  |
| **11.** | Zarządzanie przez SNMP\* | TAK |  |
| **12.** | Automatyczny wewnętrzny bypass\* | TAK |  |
| **13.** | Możliwość dołączenia baterii wydłużających czas podtrzymania zasilania\* | TAK |  |
| **14.** | Wyświetlacz LCD na froncie urządzenia, umożliwiający zarządzanie i monitoring urządzenia\* | TAK |  |
| **15.** | Certyfikaty: CE, CB | TAK |  |
| **16.** | Gwarancja 5 Lat\* | TAK |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **3. Przełącznik portowy Switch FC- 2 szt.** | | | |
| **Lp.** | **Wymagane minimalne parametry techniczne** | **Wymóg do spełnienia (warunek graniczny)** | **OFEROWANE PARAMETRY TECHNICZNE - podaje**  **Wykonawca**  **Wymogi dotyczące opisu oferowanych parametrów:**  TAK – wykonawca spełnia konkretny parametr przy czym Zamawiający oczekuje by w przypadku wymagań dotyczących minimalnych parametrów opisać szczegółowo parametry oferowane przez wykonawcę  NIE – wykonawca nie spełnia konkretnego parametru |
| **OGÓLNE** | | | |
| **1.** | Wysokość przełącznika 1U w systemie montażu w szafie typu Rack 19” | TAK |  |
| **2.** | Ilość portów SFP: 24 szt. porty uniwersalne o maksymalnej przepustowości 32GB/s, z obsługą przepustowości 16Gbit/s, 8Gbit/s i 4Gbit/s z automatycznym wyborem przepustowości (auto-sensing),  obsługa trybu full-duple | TAK |  |
| **3.** | 8 aktywnych portów | TAK |  |
| **4.** | Zainstalowane moduły optyczne 8 szt. SFP 16Gbit/s, Short Wave Length (SWL), Multi Mode Fibre (MMF) | TAK |  |
| **5.** | Obsługa trybów pracy portów FC: D\_port, F\_port, E\_port, M-Port | TAK |  |
| **6.** | Obsługa funkcji POD (Ports on Demand) przydziału licencji dla aktywnych portów FC | TAK |  |
| **7.** | Możliwość aktualizacji firmware’u switcha | TAK |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **8.** | Aktywne funkcje: Webtools, Advanced Zoning, FullFabric (z obsługą do minimum 128 przełączników FC) | TAK |  |
| **9.** | Możliwość obsługi funkcjonalności (przez zakupienie odpowiednich licencji): Trunking, Extended Fabric, Fabric Vision | TAK |  |
| **10.** | Zarządzanie min.:   * RJ-45 min 10/100 Mb/s do zarządzania poprzez sieć Ethernet * RJ-45 lub DB9 do zarządzania poprzez interfejs RS232 * USB * In-band over FC | TAK |  |
| **11.** | Sygnalizacja aktywnych i podłączonych portów na panelu przednim urządzenia | TAK |  |
| **12.** | Zarządzanie poprzez przeglądarkę WWW z obsługą połączeń szyfrowanych 128-bit SSL oraz poprzez usługę SSH | TAK |  |
| **13.** | Wsparcie dla protokołu SNMP v.3 | TAK |  |
| **14.** | Gwarancja 5 Lat\* | TAK |  |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **4. Przełącznik dystrybucyjny- 2 szt.** | | | | | | | |
| **Lp.** | | **Wymagane minimalne parametry techniczne** | | **Wymóg do spełnienia (warunek graniczny)** | | **OFEROWANE PARAMETRY TECHNICZNE - podaje**  **Wykonawca**  **Wymogi dotyczące opisu oferowanych parametrów:**  TAK – wykonawca spełnia konkretny parametr przy czym Zamawiający oczekuje by w przypadku wymagań dotyczących minimalnych parametrów opisać szczegółowo parametry oferowane przez wykonawcę  NIE – wykonawca nie spełnia konkretnego parametru | |
| **OBUDOWA** | | | | | | | |
| **1.** | | Wysokość przełącznika 1U w systemie montażu w szafie typu Rack 19” , wraz z kompletem do montażu | | TAK | |  | |
| **PORTY** | | | | | | | |
| **1.** | | - RJ-45 10/100/1000: 24 szt PoE  - SFP+ Porty Uplink: min 4 szt  - RJ-45 lub USB Port konsoli: 1szt | | TAK | |  | |
| **WYDAJNOŚĆ** | | | | | | | |
| **1.** | | - Możliwość przełączania: min. 104Gb/s  - Szybkość przekazywania: min. 77Mbps  - min. Flash: 128 MB  - min. DRAM: 256MB  - min. Tablica adresów MAC: 16K  - Jumbo Frames: min 9KB  - Auto-negocjacja, Auto- MDI/MDIX | | TAK | |  | |
| **FUNKCJONALNOŚĆ WARSTWY II** | | | | | | | |
| **1.** | | Autonegocjacja szybkości portów i trybu dupleksu  Kontrola przepływu:  - IEEE 802.3x for full duplex mode  - Back-Pressure for half duplex mode  - Protokół Spanning Tree:  - IEEE 802.1D Spanning Tree Protocol (STP)  - IEEE 802.1w Rapid Spanning Tree Protocol (RSTP)  - IEEE 802.1s Multiple Spanning Tree Protocol (MSTP)  - BPDU Guard  - BPDU filtering  - Root Guard  - Broadcast/Multicast/Unknown Unicast Storm Control  - VLANy:  - Supports 4K IEEE 802.1Q VLANs  - Active VLANs: 4K  - Port-basedGVRPI  - EEE 802.1v Protocol-based VLANs  - Mac-based VLANs  - IP based VLAN  - Link Aggregation:  - Static Trunk  - IEEE 802.3ad Link Aggregation Control Protocol  - Trunk groups: 16  - Maximum number of members per group: 8  - IGMP Snooping:  - IGMP v1/v2/v3 snooping  - IGMP proxy  - IGMP Filtering  - IGMP Throttling  - IGMP Immediate Leave  - IGMP Querier  - MVR (Multicast VLAN Registration)  - Supports QinQ | | TAK | |  | |
| **Quality of Service** | | | | | | | |
| **1.** | | - Kolejkowanie priorytetowe: 8 sprzętowe kolejki na każdym porcie  - Klasyfikacja ruchu oparta na IEEE 802.1p CoS, DSCP  - Obsługa WRR | | TAK | |  | |
| **Bezpieczeństwo** | | | | | | | |
| **1.** | | - Port security  - IEEE 802.1X port based and MAC based authentication  - MAC authentication  - Access Control List  - DHCP Snooping  - IP Source Guard  - Dynamic ARP Inspection  - RADIUS authentication  - TACACS + authorization and accounting  - SSH (v1.5/v2.0)  - SSL and HTTPS | | TAK | |  | |
| **Zarządzanie** | | | | | | | |
| **1.** | | Zarządzenie przełącznikiem:  - CLI poprzez port console port or Telnet  - WEB management  - SNMP v1, v2c, v3  Firmware & konfiguracja:  - Aktualizacja firmware z wykorzystaniem serwera TFTP  - Automatyczna aktualizacja firmware  - Dual image  - Automatyczne pobieranie konfiguracji z serwera  - Kilka plików konfiguracyjnych na jednym urządzeniu  - Wysyłanie i pobieranie konfiguracji poprzez serwer TFTP  Obsługa:  - RMON (groups 1, 2, 3 and 9)  - BOOTP, DHCP client dla przypisywania adresów IP  - SNTP (RFC 2030)  - Event/Error Log/Syslog  - Obsługa LLDP (802.1ab) | | TAK | |  | |
| **IEEE Standardy** | | | | | | | |
| **1.** | | - IEEE 802.1p Priority tags - IEEE 802.1x Port Authentication - IEEE 802.3z CSMA/CD access method and physical laye rspecifications for 1000BASE Gigabit Ethernet - IEEE 802.1q Virtual LAN - IEEE 802.1d Spanning Tree Protocol - IEEE 802.3ad Link Aggregation Control Protocol - IEEE 802.1s Rapid Spanning Tree Protocol - IEEE 802.1w Multiple Spanning Tree Protocol | | TAK | |  | |
| **Kompatybilność elektromagnetyczna** | | | | | | | |
| **1.** | | - FCC klasa A  - CE | | TAK | |  | |
| **Zasilanie** | | | | | | | |
| **1.** | | - 100-240 VAC, 50/60Hz | | TAK | |  | |
| **GWARANCJA** | | | | | | | |
| **1.** | | Gwarancja 5 Lat\* | | TAK | |  | |

|  |  |  |  |
| --- | --- | --- | --- |
| **5. Przełącznik 48 portowy- 2 szt.** | | | |
| **Lp.** | **Wymagane minimalne parametry techniczne** | **Wymóg do spełnienia (warunek graniczny)** | **OFEROWANE PARAMETRY TECHNICZNE - podaje**  **Wykonawca**  **Wymogi dotyczące opisu oferowanych parametrów:**  TAK – wykonawca spełnia konkretny parametr przy czym Zamawiający oczekuje by w przypadku wymagań dotyczących minimalnych parametrów opisać szczegółowo parametry oferowane przez wykonawcę  NIE – wykonawca nie spełnia konkretnego parametru |
| **OBUDOWA** | | | |
| **1.** | Wysokość przełącznika 1U w systemie montażu w szafie typu Rack 19” , wraz z kompletem do montażu | TAK |  |
| **PORTY** | | | |
| **1.** | - RJ-45 10/100/1000: 48 szt  - SFP+ Porty Uplink: min 4szt + wkładki niezbędne do podłączenia dostarczonych serwerów oraz switchy  - RJ-45 lub USB Port konsoli: 1szt | TAK |  |
| **WYDAJNOŚĆ** | | | |
| **1.** | - Możliwość przełączania: min. 104Gb/s  - Szybkość przekazywania: min. 77Mbps  - min. Flash: 128 MB  - min. DRAM: 256MB  - Tablica adresów min. MAC: 16K  - Jumbo Frames: min 9KB  - Auto-negocjacja, Auto- MDI/MDIX | TAK |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **FUNKCJONALNOŚĆ WARSTWY II** | | | |
| **1.** | Autonegocjacja szybkości portów i trybu dupleksu  Kontrola przepływu:  - IEEE 802.3x for full duplex mode  - Back-Pressure for half duplex mode  - Protokół Spanning Tree:  - IEEE 802.1D Spanning Tree Protocol (STP)  - IEEE 802.1w Rapid Spanning Tree Protocol (RSTP)  - IEEE 802.1s Multiple Spanning Tree Protocol (MSTP)  - BPDU Guard  - BPDU filtering  - Root Guard  - Broadcast/Multicast/Unknown Unicast Storm Control  - VLANy:  - Supports 4K IEEE 802.1Q VLANs  - Active VLANs: 4K  - Port-basedGVRPI  - EEE 802.1v Protocol-based VLANs  - Mac-based VLANs  - IP based VLAN  - Link Aggregation:  - Static Trunk  - IEEE 802.3ad Link Aggregation Control Protocol  - Trunk groups: 16  - Maximum number of members per group: 8  - IGMP Snooping:  - IGMP v1/v2/v3 snooping  - IGMP proxy  - IGMP Filtering  - IGMP Throttling  - IGMP Immediate Leave  - IGMP Querier  - MVR (Multicast VLAN Registration)  - Supports QinQ | TAK |  |
| **Quality of Service** | | | |
| **1.** | - Kolejkowanie priorytetowe: 8 sprzętowe kolejki na każdym porcie  - Klasyfikacja ruchu oparta na IEEE 802.1p CoS, DSCP  - Obsługa WRR | TAK |  |
| **Bezpieczeństwo** | | | |
| **1.** | - Port security  - IEEE 802.1X port based and MAC based authentication  - MAC authentication  - Access Control List  - DHCP Snooping  - IP Source Guard  - Dynamic ARP Inspection  - RADIUS authentication  - TACACS + authorization and accounting  - SSH (v1.5/v2.0)  - SSL and HTTPS | TAK |  |
| **Zarządzanie** | | | |
| **1.** | Zarządzenie przełącznikiem:  - CLI poprzez port console port or Telnet  - WEB management  - SNMP v1, v2c, v3  Firmware & konfiguracja:  - Aktualizacja firmware z wykorzystaniem serwera TFTP  - Automatyczna aktualizacja firmware  - Dual image  - Automatyczne pobieranie konfiguracji z serwera  - Kilka plików konfiguracyjnych na jednym urządzeniu  - Wysyłanie i pobieranie konfiguracji poprzez serwer TFTP  Obsługa:  - RMON (groups 1, 2, 3 and 9)  - BOOTP, DHCP client dla przypisywania adresów IP  - SNTP (RFC 2030)  - Event/Error Log/Syslog  - Obsługa LLDP (802.1ab) | TAK |  |
| **IEEE Standardy** | | | |
| **1.** | - IEEE 802.1p Priority tags  - IEEE 802.1x Port Authentication  - IEEE 802.3z CSMA/CD access method and physical laye rspecifications for  1000BASE Gigabit Ethernet  - IEEE 802.1q Virtual LAN  - IEEE 802.1d Spanning Tree Protocol  - IEEE 802.3ad Link Aggregation Control Protocol  - IEEE 802.1s Rapid Spanning Tree Protocol  - IEEE 802.1w Multiple Spanning Tree Protocol | TAK |  |
| **Kompatybilność elektromagnetyczna** | | | |
| **1.** | - FCC klasa A - CE | TAK |  |
| **Zasilanie** | | | |
| **1.** | - 100-240 VAC, 50/60Hz | TAK |  |
| **GWARANCJA** | | | |
| **1.** | Gwarancja 5 Lat | TAK |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **6. Serwer bazodanowy- 2 szt.** | | | |
| **Lp.** | **Wymagane minimalne parametry techniczne** | **Wymóg do spełnienia (warunek graniczny)** | **OFEROWANE PARAMETRY TECHNICZNE - podaje**  **Wykonawca**  **Wymogi dotyczące opisu oferowanych parametrów:**  TAK – wykonawca spełnia konkretny parametr przy czym Zamawiający oczekuje by w przypadku wymagań dotyczących minimalnych parametrów opisać szczegółowo parametry oferowane przez wykonawcę  NIE – wykonawca nie spełnia konkretnego parametru |
| **OBUDOWA** | | | |
| **1.** | • Typu RACK, wysokość nie więcej niż 2U;  • Szyny umożliwiające wysunięcie serwera z szafy stelażowej;  • Opcjonalne ramię porządkujące ułożenie przewodów z tyłu serwera; | TAK |  |
| **PŁYTA GŁÓWNA** | | | |
| **1.** | • Wyprodukowana i zaprojektowana przez producenta serwera  • Zainstalowany moduł TPM 2.0  • Wsparcie dla technologii:  o Advanced ECC | TAK |  |
| **Procesory** | | | |
| **1.** | • Jeden procesor 8-rdzeniowe (nie dopuszcza się większej ilości rdzeni fizycznych) o częstotliwości bazowej minimum 3,0GHz  • architektura x86\_64 | TAK |  |
| **Pamięć RAM** | | | |
| **1.** | • 192 GB pamięci RAM  • DDR4 Registered | TAK |  |
| **Dyski twarde i napędy** | | | |
| **1.** | • Minimum 8 wnęk dla dysków twardych Hotplug 2,5” ;  • Zainstalowane 2 dyski SSD Hot-Plug o pojemności min 120GB i parametrze DWPD>=3 | TAK |  |
| **Kontrolery LAN** | | | |
| **1.** | - Karta LAN 2x 10Gbit SFP+; możliwość wymiany zainstalowanych interfejsów LAN na interfejsy 2x 10Gbit Base- T bez potrzeby wymiany całego układu lub instalacji dodatkowych kart w slotach PCI Express  2 moduły SFP+ Multi Mode Fiber 10GbE LC | TAK |  |
| **Kontrolery I/O** | | | |
| **1.** | • Zainstalowana jedna karta dwuportowa FC 16Gb; | TAK |  |
| **Porty** | | | |
| **1.** | • Zintegrowana karta graficzna ze złączami VGA z tyłu oraz przodu serwera;  • Min 1 port USB 3.0 na panelu przednim;  • Min 2 porty USB 3.0 dostępne z tyłu serwera; | TAK |  |
| **Zasilanie, chłodzenie** | | | |
| **1.** | • Redundantne zasilacze hotplug mocy minimalnej 400W o sprawności 94% | TAK |  |
| **Zarządzanie** | | | |
| **1.** | • Wbudowane diody informacyjne lub wyświetlacz informujące o stanie serwera - system przewidywania, rozpoznawania awarii)  Zintegrowany z płytą główną serwera kontroler sprzętowy zdalnego zarządzania zgodny z IPMI 2.0 o funkcjonalnościach:  • Niezależny od systemu operacyjnego, sprzętowy kontroler umożliwiający pełne zarządzanie, zdalny restart serwera;  o Dedykowana karta LAN 1 Gb/s, dedykowane złącze RJ-45 do komunikacji wyłącznie z kontrolerem zdalnego zarządzania z możliwością przeniesienia tej komunikacji na inną kartę sieciową współdzieloną z systemem operacyjnym;  o Dostęp poprzez przeglądarkę Web, SSH;  o Zarządzanie mocą i jej zużyciem oraz monitoring zużycia energii;  o Zarządzanie alarmami (zdarzenia poprzez SNMP)  o Możliwość przejęcia konsoli tekstowej  o Możliwość zarządzania przez 6 administratorów jednocześnie  o Przekierowanie konsoli graficznej na poziomie sprzętowym oraz możliwość montowania zdalnych napędów i ich obrazów na poziomie sprzętowym (cyfrowy KVM)  o Obsługa serwerów proxy (autentykacja)  o Obsługa VLAN  o Możliwość konfiguracji parametru Max. Transmission Unit (MTU)  o Wsparcie dla protokołu SSDP  o Obsługa protokołów TLS 1.0, TLS 1.1, TLS 1.2, SSL v3  o Obsługa protokołu LDAP  o Synchronizacja czasu poprzez protokół NTP  o Możliwość backupu i odtworzenia ustawień bios serwera oraz ustawień karty zarządzającej  • Serwer posiada możliwość konfiguracji i wykonania aktualizacji BIOS, Firmware, sterowników serwera bezpośrednio z GUI (graficzny interfejs) | TAK |  |
| **Wspierane OS** | | | |
| **1.** | • Microsoft Windows Server 2019, 2016  • VMWare vSphere 6.7  • Suse Linux Enterprise Server 12  • Red Hat Enterprise Linux 7, 8  • Hyper-V Server | TAK |  |
| **System operacyjny** | | | |
| **1.** | System Operacyjny dedykowany do bazy danych systemu HIS\* | TAK |  |
| **Gwarancja** | | | |
| **1.** | • 5 lat gwarancji \* | TAK |  |
| **Dokumentacja, inne** | | | |
| **1.** | • Serwer musi być fabrycznie nowy i pochodzić z oficjalnego kanału dystrybucyjnego w UE. Nie dopuszcza się użycia serwerów odnawianych, demonstracyjnych lub powystawowych. \*  • Ogólnopolska, telefoniczna infolinia/linia techniczna producenta serwera\*  • Możliwość aktualizacji i pobrania sterowników do oferowanego modelu serwera w najnowszych certyfikowanych wersjach bezpośrednio z sieci Internet za pośrednictwem strony www producenta serwera;\* | TAK |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **7. Serwer do obsługi wirtualizacji- 2 szt.** | | | |
| **Lp.** | **Wymagane minimalne parametry techniczne** | **Wymóg do spełnienia (warunek graniczny)** | **OFEROWANE PARAMETRY TECHNICZNE - podaje**  **Wykonawca**  **Wymogi dotyczące opisu oferowanych parametrów:**  TAK – wykonawca spełnia konkretny parametr przy czym Zamawiający oczekuje by w przypadku wymagań dotyczących minimalnych parametrów opisać szczegółowo parametry oferowane przez wykonawcę  NIE – wykonawca nie spełnia konkretnego parametru |
| **OBUDOWA** | | | |
| **1.** | • Typu RACK, wysokość nie więcej niż 2U;  • Szyny umożliwiające wysunięcie serwera z szafy stelażowej;  • Opcjonalne ramię porządkujące ułożenie przewodów z tyłu serwera; | TAK |  |
| **Płyta główna** | | | |
| **1.** | • Dwuprocesorowa;  • Wyprodukowana i zaprojektowana przez producenta serwera  • Zainstalowany moduł TPM 2.0  • Wsparcie dla technologii:  o Advanced ECC | TAK |  |
| **Procesory** | | | |
| **1.** | • Dwa procesory 10-rdzeniowe o częstotliwości minimum 2,3 GHz  • architektura x86\_64 | TAK |  |
| **Pamięć RAM** | | | |
| **1.** | • 196 GB pamięci RAM  • DDR4 Registered | TAK |  |
| **Dyski twarde i napędy** | | | |
| **1.** | • Minimum 8 wnęk dla dysków twardych Hotplug 2,5”;  • Możliwość rozbudowy do 16 wnęk;  • Zainstalowane 2 dyski SSD o pojemności minimum 300GB | TAK |  |
| **Kontrolery LAN** | | | |
| **1.** | - Karta LAN 2x 10Gbit SFP+; możliwość wymiany zainstalowanych interfejsów LAN na interfejsy 2x 10Gbit Base- T bez potrzeby wymiany całego układu lub instalacji dodatkowych kart w slotach PCI Express  2 moduły SFP+ Multi Mode Fiber 10GbE LC | TAK |  |
| **Kontrolery I/O** | | | |
| **1.** | • Zainstalowane dwie jednoportowe karty FC 16Gb;  W jednym z serwerów Zainstalowany moduł HSM PCIe | TAK |  |
| **Porty** | | | |
| **1.** | • Zintegrowana karta graficzna ze złączami VGA z tyłu oraz przodu serwera;  • Minimum 1 port USB 3.0 na panelu przednim;  • Min 2 porty USB 3.0 dostępne z tyłu serwera;  • Możliwość instalacji jednego portu serial, możliwość wykorzystania portu do zarządzania serwerem;  • Ilość dostępnych złącz USB nie może być osiągnięta poprzez stosowanie zewnętrznych przejściówek, rozgałęziaczy czy dodatkowych kart rozszerzeń zajmujących jakikolwiek slot PCI Express i/lub USB serwera; | TAK |  |
| **Zasilanie, chłodzenie** | | | |
| **1.** | • Redundantne zasilacze hotplug o mocy minimalnej 400W o sprawności 94% | TAK |  |
| **Zarządzanie** | | | |
| **1.** | • Wbudowane diody informacyjne lub wyświetlacz informujące o stanie serwera - system przewidywania, rozpoznawania awarii)  Zintegrowany z płytą główną serwera kontroler sprzętowy zdalnego zarządzania zgodny z IPMI 2.0 o funkcjonalnościach:  • Niezależny od systemu operacyjnego, sprzętowy kontroler umożliwiający pełne zarządzanie, zdalny restart serwera;  o Dedykowana karta LAN 1 Gb/s, dedykowane złącze RJ-45 do komunikacji wyłącznie z kontrolerem zdalnego zarządzania z możliwością przeniesienia tej komunikacji na inną kartę sieciową współdzieloną z systemem operacyjnym;  o Dostęp poprzez przeglądarkę Web, SSH;  o Zarządzanie mocą i jej zużyciem oraz monitoring zużycia energii;  o Zarządzanie alarmami (zdarzenia poprzez SNMP)  o Możliwość przejęcia konsoli tekstowej  o Możliwość zarządzania przez 6 administratorów jednocześnie  o Przekierowanie konsoli graficznej na poziomie sprzętowym oraz możliwość montowania zdalnych napędów i ich obrazów na poziomie sprzętowym (cyfrowy KVM)  o Obsługa serwerów proxy (autentykacja)  o Obsługa VLAN  o Możliwość konfiguracji parametru Max. Transmission Unit (MTU)  o Wsparcie dla protokołu SSDP  o Obsługa protokołów TLS 1.0, TLS 1.1, TLS 1.2, SSL v3  o Obsługa protokołu LDAP  o Synchronizacja czasu poprzez protokół NTP  o Możliwość backupu i odtworzenia ustawień bios serwera oraz ustawień karty zarządzającej  • Oprogramowanie zarządzające i diagnostyczne wyprodukowane przez producenta serwera umożliwiające konfigurację kontrolera RAID, instalację systemów operacyjnych, zdalne zarządzanie, diagnostykę i przewidywanie awarii w oparciu o informacje dostarczane w ramach zintegrowanego w serwerze systemu umożliwiającego monitoring systemu i środowiska (m.in. temperatura, dyski, zasilacze, płyta główna, procesory, pamięć operacyjna);  • Serwer posiada możliwość konfiguracji i wykonania aktualizacji BIOS, Firmware, sterowników serwera bezpośrednio z GUI (graficzny interfejs). | TAK |  |
| **Wspierane OS** | | | |
| **1.** | • Microsoft Windows Server 2019, 2016  • VMWare vSphere 6.7  • Suse Linux Enterprise Server 12  • Red Hat Enterprise Linux 7, 8  • Hyper-V Server | TAK |  |
| **System operacyjny** | | | |
| **1.\*** | Licencje na serwerowy system operacyjny muszą uprawniać do uruchamiania serwerowego systemu operacyjnego w środowisku fizycznym i minimum 4 wirtualnych środowisk ( per serwer) serwerowego systemu operacyjnego za pomocą wbudowanych mechanizmów wirtualizacji. Serwerowy system operacyjny musi posiadać następujące, wbudowane cechy.  1) Możliwość wykorzystania 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym.  2) Możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności do 64TB przez każdy wirtualny serwerowy system operacyjny.  3) Możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania 7000 maszyn wirtualnych.  4) Możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci.  5) Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy.  6) Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy.  7) Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.  8) Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading.  9) Wbudowane wsparcie instalacji i pracy na wolumenach, które:  a) pozwalają na zmianę rozmiaru w czasie pracy systemu,  b) umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,  c) umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów,  d) umożliwiają zdefiniowanie list kontroli dostępu (ACL).  10) Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.  11) Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.  12) Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET  13) Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.  14) Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.  15) Dostępne dwa rodzaje graficznego interfejsu użytkownika:  a) Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,  b) Dotykowy umożliwiający sterowanie dotykiem na monitorach dotykowych.  16) Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe,  17) Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji.  18) Mechanizmy logowania w oparciu o:  a) Login i hasło,  b) Karty z certyfikatami (smartcard),  c) Wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM),  19) Możliwość wymuszania wieloelementowej dynamicznej kontroli dostępu dla: określonych grup użytkowników, zastosowanej klasyfikacji danych, centralnych polityk dostępu w sieci, centralnych polityk audytowych oraz narzuconych dla grup użytkowników praw do wykorzystywania szyfrowanych danych..  20) Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).  21) Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.  22) Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa.  23) Pochodzący od producenta systemu serwis zarządzania polityką dostępu do informacji w dokumentach (Digital Rights Management).  24) Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach.  25) Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:  a) Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC,  b) Usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji:  i. Podłączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną,  ii. Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,  iii. Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza.  iv. Bezpieczny mechanizm dołączania do domeny uprawnionych użytkowników prywatnych urządzeń mobilnych opartych o iOS i Windows 8.1.  c) Zdalna dystrybucja oprogramowania na stacje robocze.  d) Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej  e) Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:  i. Dystrybucję certyfikatów poprzez http  ii. Konsolidację CA dla wielu lasów domeny,  iii. Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen,  iv. Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509.  f) Szyfrowanie plików i folderów.  g) Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec).  h) Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów.  i) Serwis udostępniania stron WWW.  j) Wsparcie dla protokołu IP w wersji 6 (IPv6),  k) Wsparcie dla algorytmów Suite B (RFC 4869),  l) Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows,  m) Wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie do 1000 aktywnych środowisk wirtualnych systemów operacyjnych. Wirtualne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności. Mechanizmy wirtualizacji mają zapewnić wsparcie dla:  i. Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych,  ii. Obsługi ramek typu jumbo frames dla maszyn wirtualnych.  iii. Obsługi 4-KB sektorów dysków  iv. Nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra  v. Możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API.  vi. Możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk mode)  26) Możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta serwerowego systemu operacyjnego umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet.  27) Wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath).  28) Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego.  29) Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.  30) Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF.  31) ZORGANIZOWANY SYSTEM SZKOLEŃ I MATERIAŁY EDUKACYJNE W JEZYKU POLSKIM | TAK |  |
| **Gwarancja** | | | |
| **1.\*** | • Gwarancja 5 Lat  Gwarantowany czas reakcji do następnego dnia roboczego od przyjęcia zgłoszenia . Zgłaszanie usterek i awarii w trybie 24/7 | TAK |  |
| **Dokumentacja, inne** | | | |
| **1.\*** | • Serwer musi być fabrycznie nowy i pochodzić z oficjalnego kanału dystrybucyjnego w UE. Nie dopuszcza się użycia serwerów odnawianych, demonstracyjnych lub powystawowych.  • Ogólnopolska, telefoniczna infolinia/linia techniczna producenta serwera  • Możliwość aktualizacji i pobrania sterowników do oferowanego modelu serwera w najnowszych certyfikowanych wersjach bezpośrednio z sieci Internet za pośrednictwem strony www producenta serwera; | TAK |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **8. Licencje dostępowe serwerów- 100 szt.** | | | |
| **Lp.** | **Wymagane minimalne parametry techniczne** | **Wymóg do spełnienia (warunek graniczny)** | **OFEROWANE PARAMETRY TECHNICZNE - podaje**  **Wykonawca**  **Wymogi dotyczące opisu oferowanych parametrów:**  TAK – wykonawca spełnia konkretny parametr przy czym Zamawiający oczekuje by w przypadku wymagań dotyczących minimalnych parametrów opisać szczegółowo parametry oferowane przez wykonawcę  NIE – wykonawca nie spełnia konkretnego parametru |
| **1.\*** | Licencje dostępowe do serwera wirtualizacji z punktu 7. – 50 szt. | TAK |  |
| **2.\*** | Licencje umożliwiające podłączenie się do serwera wirtualizacji z punktu 7. poprzez zdalny dostęp – 50 szt. | TAK |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **9. System wirtualizacji** | | | |
| **Lp.** | **Wymagane minimalne parametry techniczne** | **Wymóg do spełnienia (warunek graniczny)** | **OFEROWANE PARAMETRY TECHNICZNE - podaje**  **Wykonawca**  **Wymogi dotyczące opisu oferowanych parametrów:**  TAK – wykonawca spełnia konkretny parametr przy czym Zamawiający oczekuje by w przypadku wymagań dotyczących minimalnych parametrów opisać szczegółowo parametry oferowane przez wykonawcę  NIE – wykonawca nie spełnia konkretnego parametru |
| **1.\*** | Licencja dla minimum 2 serwerów fizycznych posiadających 2 procesory | TAK |  |
| **2.\*** | Warstwa wirtualizacji zainstalowana bezpośrednio na sprzęcie fizycznym bez dodatkowych pośredniczących systemów operacyjnych | TAK |  |
| **3.\*** | Rozwiązanie zapewniające obsługę wielu instancji systemów operacyjnych  na jednym serwerze fizycznym oraz powinno się charakteryzować maksymalnym możliwym stopniem konsolidacji sprzętowej. | TAK |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **4.\*** | Pojedynczy klaster może się skalować do 3 fizycznych hostów  (serwerów) z zainstalowaną warstwą wirtualizacji. | TAK |  |
| **5.\*** | Oprogramowanie do wirtualizacji zainstalowane na serwerze fizycznym potrafiące obsłużyć i wykorzystać procesory fizyczne wyposażone w 480 logicznych wątków oraz do 6TB pamięci fizycznej RAM. | TAK |  |
| **6.\*** | Oprogramowanie do wirtualizacji ma zapewnić:   * możliwość skonfigurowania maszyn wirtualnych 1-128 procesorowych. * możliwość stworzenia dysku maszyny wirtualnej o wielkości do 62 TB. * możliwość skonfigurowania maszyn wirtualnych   z możliwością przydzielenia do 4 TB pamięci operacyjnej RAM.   * możliwość skonfigurowania maszyn wirtualnych, z których każda może mieć 1-10 wirtualnych kart sieciowych. * możliwość skonfigurowania maszyn wirtualnych, z których każda może mieć 32 porty szeregowe. | TAK |  |
| **7.\*** | Rozwiązanie musi:   * umożliwiać łatwą i szybką rozbudowę infrastruktury o nowe usługi bez spadku wydajności i dostępności pozostałych wybranych usług. * w możliwie największym stopniu być niezależne od producenta platformy sprzętowej. | TAK |  |
| **8.\*** | Polityka licencjonowania musi umożliwiać przenoszenie licencji na  oprogramowanie do wirtualizacji pomiędzy serwerami. | TAK |  |
| **11.\*** | Rozwiązanie musi wspierać następujące systemy operacyjne: MS-DOS 6.22, Windows 3.1, Windows 95, Windows 98, Windows XP, Windows Vista , Windows NT 4.0, Windows 2000, Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows 7, Windows 8, SLES 11,  SLES 10, SLES 9, SLES 8, RHEL 6, RHEL 5, RHEL 4, RHEL 3, Solaris  11 ,Solaris 10, Solaris 9, Solaris 8, OS/2 Warp 4.0, NetWare 6.5, NetWare  6, NetWare 5, OEL 4, OEL 5, Debian, CentOS, FreeBSD, Asianux, Mandriva, Ubuntu 14, Ubuntu 12, SCO OpenServer, SCO Unixware, Mac OS X. | TAK |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **12.\*** | Rozwiązanie musi:   * umożliwiać przydzielenie większej ilości pamięci RAM dla maszyn wirtualnych niż fizyczne zasoby RAM serwera w celu osiągnięcia maksymalnego współczynnika konsolidacji. * umożliwiać udostępnienie maszynie wirtualnej większej ilości zasobów dyskowych niż jest fizycznie zarezerwowane na dyskach lokalnych serwera lub na macierzy. | TAK |  |
| **13.\*** | Rozwiązanie powinno posiadać centralną konsolę graficzną do zarządzania maszynami wirtualnymi i do konfigurowania innych funkcjonalności.  Centralna konsola graficzna powinna mieć możliwość działania zarówno, jako aplikacja na maszynie fizycznej lub wirtualnej, jak i jako gotowa, wstępnie skonfigurowana maszyna wirtualna tzw. virtual appliance. | TAK |  |
| **14.\*** | Rozwiązanie musi zapewnić możliwość bieżącego monitorowania wykorzystania zasobów fizycznych infrastruktury wirtualnej (np. wykorzystanie procesorów, pamięci RAM, wykorzystanie przestrzeni na dyskach/wolumenach) oraz przechowywać i wyświetlać dane maksymalnie sprzed roku. | TAK |  |
| **15.\*** | Oprogramowanie do wirtualizacji powinno zapewnić możliwość wykonywania kopii migawkowych instancji systemów operacyjnych (tzw. snapshot) na potrzeby tworzenia kopii zapasowych bez przerywania ich  pracy. | TAK |  |
| **16.\*** | Oprogramowanie do wirtualizacji musi zapewnić możliwość klonowania systemów operacyjnych wraz z ich pełną konfiguracją i danymi. | TAK |  |
| **17.\*** | Oprogramowanie do wirtualizacji oraz oprogramowanie zarządzające musi posiadać możliwość integracji z usługami katalogowymi Microsoft Active Directory. | TAK |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **17.\*** | Rozwiązanie musi :   * zapewniać mechanizm bezpiecznego uaktualniania warstwy wirtualizacyjnej (hosta, maszyny wirtualnej) bez potrzeby wyłączania wirtualnych maszyn. * posiadać funkcjonalność wirtualnego przełącznika (virtual switch) umożliwiającego tworzenie sieci wirtualnej w obszarze hosta i   pozwalającego połączyć maszyny wirtualne w obszarze jednego hosta, a także na zewnątrz sieci fizycznej. | TAK |  |
| **18.\*** | Pojedynczy przełącznik wirtualny powinien mieć możliwość konfiguracji do minimum 4000 portów. | TAK |  |
| **19.\*** | Pojedynczy wirtualny przełącznik musi posiadać możliwość przyłączania do niego dwóch i więcej fizycznych kart sieciowych, aby zapewnić  bezpieczeństwo połączenia ethernetowego w razie awarii karty sieciowej. | TAK |  |
| **20.\*** | Wirtualne przełączniki musza obsługiwać wirtualne sieci lokalne (VLAN). | TAK |  |
| **21.\*** | Rozwiązanie musi:   * zapewniać mechanizm klonowania wskazanych maszyn wirtualnych w obrębie klastra serwerów fizycznych. * mieć możliwość przenoszenia maszyn wirtualnych pomiędzy serwerami fizycznymi. | TAK |  |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **10. Macierz dyskowa- 2 szt.** | | | | | | | |
| **Lp.** | | **Wymagane minimalne parametry techniczne** | | **Wymóg do spełnienia (warunek graniczny)** | | **OFEROWANE PARAMETRY TECHNICZNE - podaje**  **Wykonawca**  **Wymogi dotyczące opisu oferowanych parametrów:**  TAK – wykonawca spełnia konkretny parametr przy czym Zamawiający oczekuje by w przypadku wymagań dotyczących minimalnych parametrów opisać szczegółowo parametry oferowane przez wykonawcę  NIE – wykonawca nie spełnia konkretnego parametru | |
| **OGÓLNE** | | | | | | | |
| **1.** | | System musi być dostarczony ze wszystkimi komponentami do instalacji w standardowej szafie rack 19” z zajętością maks. 2U w tej szafie. Każdy skonfigurowany moduł/obudowa musi posiadać układ nadmiarowy zasilania i chłodzenia, zapewniający bezprzerwową pracę macierzy bez ograniczeń czasowych w przypadku utraty redundancji w danym układzie (zasilania lub chłodzenia). Każdy moduł/obudowa powinien posiadać widoczne elementy sygnalizacyjne do informowania o stanie poprawnej pracy lub awarii. Rozbudowa o dodatkowe moduły dla obsługiwanych dysków powinna odbywać się wyłącznie poprzez zakup takich modułów, bez konieczności zakupu dodatkowych licencji lub specjalnego oprogramowania aktywującego proces rozbudowy lub musi być dostarczona licencja na dwukrotność dostarczanej pojemności. Dostarczana macierz musi umożliwiać podłączenie półek kaskadowo , bądź w formie 2 łańcuchów. Oferowana macierz musi obsługiwać min. 260 dysków wykonanych w technologii hot-plug. Macierz musi umożliwiać rozbudowę i jednoczesne podłączenie i używanie modułów (tzw. „półek dyskowych”) w rozmiarze 2U pozwalająca umieścić do 24 dysków 2,5” typu hotplug dla dysków NL-SAS SAS i SSD oraz w rozmiarze 2U dla 12 dysków 3,5” typu hotplug SAS, NL-SAS oraz do 6U dla min 60 dysków; Wymaga się aby macierz umożliwiała jednoczesne podłączenie i użycie dowolnego rodzaju i kombinacji wyżej wymienionych półek dyskowych. Macierz musi posiadać funkcje automatycznego tieringu. | | TAK | |  | |
| **POJEMNOŚĆ DOSTARCZONEJ MACIERZY** | | | | | | | |
| **1.** | | * przestrzeń minimum 4,5 TB realizowana na dyskach SSD : * min 2 dyski SSD-SAS 12G o pojemności min. 400GB DWPD3 * min 2 dyski SSD-SAS 12G o pojemności min. 3,8TB DWPD1 * przestrzeń minimum 15,5 TB realizowana na dyskach NL :   min 8 dysków NL SAS 12G o pojemności minimum 4TB lub min 16 dysków NL SAS 12G o pojemności minimum 2TB | | TAK | |  | |
| **KONTROLERY** | | | | | | | |
| **1.** | | • Kontrolery macierzy muszą obsługiwać tryb pracy w układzie min active-active, macierz musi być dostarczona z zainstalowanymi minimum 2 kontrolerami;  • Każdy z kontrolerów macierzy musi posiadać po minimum 32 GB pamięci podręcznej Cache – kontrolery muszą obsługiwać między sobą mechanizm lustrzanej kopii danych (cache mirror) przeznaczonych do zapisu;  • W przypadku awarii zasilania dane nie zapisane na dyski, przechowywane w pamięci podręcznej Cache dla zapisów muszą być zabezpieczone metodą trwałego zapisu na dysk.  • Kontrolery muszą posiadać możliwość ich wymiany bez konieczności wyłączania zasilania całego urządzenia;  • Kontrolery macierzy obsługują funkcjonalność kompresji danych.  • Kontrolery macierzy obsługują funkcjonalność deduplikacji w trybie in-line.  • Macierz musi obsługiwać wymianę kontrolera RAID bez utraty danych zapisanych na dyskach.  • Każdy z kontrolerów RAID powinien posiadać dedykowany minimum 2 interfejsy RJ-45 Ethernet obsługujący połączenia z prędkością minimum 1Gb/s dla zdalnej komunikacji z oprogramowaniem zarządzającym i konfiguracyjnym macierzy.  • Kontrolery macierzy muszą być oparte o procesor wykonany w technologii wielordzeniowej z minimum 4 rdzeniami,  • Kontrolery macierzy muszą obsługiwać min 120 grup dyskowych w całym rozwiązaniu, bez konieczności wymiany dostarczonych kontrolerów  • Oferowana macierz musi mieć wyprowadzone 4 porty FC 16Gb/s do dołączenia serwerów bezpośrednio lub do dołączenia do sieci SAN, na każdy kontroler RAID.  • Macierz musi umożliwiać stosowanie (rozbudowa/wymiana) portów do transmisji danych:  FC 16Gb/s, iSCSI min 10Gb/s  • Stosowanie wyżej wymienionych portów nie może powodować wymiany samych kontrolerów RAID w oferowanym rozwiązaniu a w przypadku konieczność licencjonowania tej funkcjonalności macierz ma być dostarczona z aktywną licencja na instalację i obsługę każdego z wymienionych protokołów transmisji danych | | TAK | |  | |
| **Poziomy RAID** | | | | | | | |
| **1.** | | Macierz musi zapewniać poziom zabezpieczenia danych na dyskach definiowany poziomami RAID:  o Raid-0  o Raid-1  o Raid-10 lub RAID-50  o Raid-5  o Raid-6 | | TAK | |  | |
| **Dyski** | | | | | | | |
| **1.** | | Oferowana macierz musi wspierać dyski hot-plug:  o dyski elektroniczne SSD i mechaniczne HDD z interfejsami SAS12Gb/s  o dyski mechaniczne HDD o prędkości obrotowej min 7,2 krpm, 10 krpm .  • Macierz musi obsługiwać mieszaną konfigurację dysków hot-plug SSD i HDD w rozmiarach 2,5” i 3,5” zainstalowanych w dowolnym module rozwiązania;  • Wszystkie dyski wspierane przez oferowany model macierzy muszą być wykonane w technologii hot-plug i posiadać podwójne porty SAS obsługujące tryb pracy full-duplex  • Macierz musi obsługiwać min. 260 dysków SAS SSD w całym rozwiązaniu, bez konieczności dokupowania/wymiany żadnych innych elementów sprzętowych czy licencyjnych innych niż same półki dyskowe wraz z dyskami;  • Możliwość rozbudowy oferowanego modelu macierzy do minimum 500 dysków bez migracji i przenoszenia danych - jedynie poprzez wymianę modułu kontrolerów macierzy (bez konieczności wymiany posiadanych dysków, półek dyskowych, bez konieczności przenoszenia danych/ istniejącej struktury grup dyskowych/LUN, jak również z zachowaniem istniejącej gwarancji producenta na półki dyskowe i dyski;  • Macierz musi umożliwiać skonfigurowanie dysku hot-spare (dysk zapasowy)  • Macierz musi pozwalać na zaszyfrowanie danych zapisanych na wszystkich obsługiwanych dyskach SSD-SAS i HDD-SAS/NL-SAS minimum kluczem AES256-bit – jeżeli w tym celu niezbędne jest zakupienie dodatkowych licencji bądź komponentów sprzętowych to należy je dostarczyć wraz z macierzą. | | TAK | |  | |
| **Opcje programowe** | | | | | | | |
| **1.** | | • Macierz musi być wyposażona w system kopii migawkowych umożliwiających wykonanie minimum 2048 kopii migawkowych  • Macierz musi umożliwiać zdefiniowanie min. 8000 woluminów (LUN)  • Macierz powinna umożliwiać podłączenie logiczne z serwerami i stacjami poprzez min. 1024 ścieżek logicznych FC  • Macierz musi umożliwiać aktualizację oprogramowania wewnętrznego kontrolerów RAID i dysków bez konieczności wyłączania macierzy oraz bez konieczności wyłączania ścieżek logicznych FC/iSCSI dla podłączonych stacji/serwerów  • Macierz musi umożliwiać dokonywanie w trybie on-line (tj. bez wyłączania zasilania i bez przerywania przetwarzania danych w macierzy) operacje: powiększanie grup dyskowych, zwiększanie rozmiaru woluminu, migrowanie woluminu na inną grupę dyskową  • Macierz musi posiadać wsparcie dla systemów operacyjnych : Microsoft Windows Server 2012R2, 2016, 2019, SuSE Linux Enterprise Server, Red Hat Linux Enterprise Server, HP-UNIX, IBM AIX, SUN Solaris, Vmware Vsphere;  • Macierz musi być dostarczona z licencją na oprogramowanie wspierające technologię typu multipath (obsługa nadmiarowości dla ścieżek transmisji danych pomiędzy macierzą i serwerem) dla połączeń FC i iSCSI.  • Macierz musi posiadać możliwość uruchamiania mechanizmów zdalnej replikacji danych, w trybie synchronicznym i asynchronicznym, po protokołach FC lub IP lub iSCSI, bez konieczności stosowania zewnętrznych urządzeń konwersji wymienionych protokołów transmisji. Funkcjonalność replikacji danych musi być zapewniona z poziomu oprogramowania wewnętrznego macierzy. Replikacja danych musi być obsługiwana w połączeniu z każdą macierzą z tej samej rodziny urządzeń wspierającą obsługę zdalnej replikacji danych.  • Macierz musi posiadać możliwość tworzenia lokalnych tj. w obrębie zasobów macierzy, pełnych kopii danych (tzw. klony danych), kopii przyrostowych oraz kopii lustrzanych (mirror) – nie jest wymagane dostarczenie tej funkcjonalności – opcja rozbudowy  • Macierz musi obsługiwać mechanizm ochrony priorytetów obsługi wybranych zasobów – za taki mechanizm uznaje się funkcję typu ‘cache partitioning’ lub ‘storage partitioning’.  • Macierz musi obsługiwać adresację IP v.4 i IP v.6  • Macierz musi wspierać obsługę mechanizmów Vmware  • Macierz musi obsługiwać mechanizmy Thin Provisioning, czyli przydziału dla obsługiwanych środowisk woluminów logicznych o sumarycznej pojemności większej od sumy pojemności dysków fizycznych zainstalowanych w macierzy.  • Macierz musi obsługiwać mechanizmy typu AST (Automated Storage Tiering) tj. automatycznego migrowania i realokacji bloków danych pomiędzy różnymi technologiami dyskowymi na podstawie analizy częstotliwości operacji I/O dla tych bloków oraz wg potrzeb wydajnościowych serwerów, środowisk i aplikacji korzystających z zasobów macierzy. Mechanizm AST musi być obsługiwany przy korzystaniu zarówno z trzech jak z dwóch dostarczonych technologii dyskowych: SSD, SSAS, NLSAS.  • Macierz musi wspierać usługi VSS (Volume ShadowCopy Services) w systemach klasy Microsoft Windows Sever – wymagane jest dostarczenie niezbędnego oprogramowania / sterowników VSS pozwalających na obsługę VSS przy maksymalnej pojemności i liczbie dysków obsługiwanych przez oferowaną. W czasie trwania gwarancji wymaga się bezpłatnego dostępu do nowych wersji oprogramowania i sterowników  • Macierz musi obsługiwać mechanizmy migracji danych w trybie online z innej macierzy .  • Macierz wspiera rozwiązania klasy ‘klastra macierzowego’ tj. zapewnienia wysokiej dostępności zasobów dyskowych macierzy dla podłączonych platform software’owych i sprzętowych z wykorzystaniem synchronicznej replikacji danych pomiędzy minimum 2 macierzami protokołami FC. Mechanizm klastra macierzowego musi być obsługiwany dla protokołów FC, zarówno w zakresie replikacji danych jak i w zakresie sposobu podłączenia serwerów do zasobów macierzy. Pod użytym pojęciem ‘wysoka dostępność zasobów dyskowych’ należy rozumieć zapewnienie bezprzerwowego działania środowiska (aplikacja/ system operacyjny/ serwer) podłączonego do macierzy (macierz podstawowa) w przypadku wystąpienia awarii logicznego połączenia z tą macierzy bądź awarii samej macierzy, powodujących dla danego środowiska brak dostępu do zasobów macierzy podstawowej. Funkcjonalność ‘klastra macierzowego’ musi pozwalać na automatyczne i ręczne przełączanie obsługi środowisk produkcyjnych z macierzy podstawowej na zapasową w przypadku awarii macierzy podstawowej (tzw. Automated/manual failover). – nie jest wymagane dostarczenie tej funkcjonalności – opcja rozbudowy | | TAK | |  | |
| **Zarządzanie** | | | | | | | |
| **1.** | | • Oprogramowanie do zarządzania musi być zintegrowane z systemem operacyjnym systemu pamięci masowej  • Komunikacja z wbudowanym oprogramowaniem zarządzającym macierzą musi być możliwa w trybie graficznym np. poprzez przeglądarkę WWW oraz w trybie tekstowym.  • Musi być możliwe zdalne zarządzanie macierzą z wykorzystaniem standardowej przeglądarki internetowej (np. Internet Explorer, Google Chrome, Mozilla Firefox) bez konieczności instalacji żadnych dodatkowych aplikacji na stacji administratora  • Wbudowane oprogramowanie macierzy musi obsługiwać połączenia z modułem zarządzania macierzy poprzez szyfrowanie komunikacji protokołami: SSL dla komunikacji poprzez przeglądarkę WWW i protokołem SSH dla komunikacji poprzez CLI | | TAK | |  | |
| **Gwarancja i serwis** | | | | | | | |
| **1.** | | Gwarancja 5 Lat  • Macierz musi pochodzić z oficjalnego kanału sprzedaży producenta w UE. Nie dopuszcza się użycia macierzy odnawianych, demonstracyjnych lub powystawowych  • Producent oferowanej macierzy musi posiadać dedykowaną, ogólnie dostępną stronę internetową | | TAK | |  | |

|  |  |  |  |
| --- | --- | --- | --- |
| **11. Centrum Autoryzacji – 1 szt. składające się z:**  **A. *Oprogramowanie umożliwiające szyfrowanie wrażliwych danych*** | | | |
| **Lp.** | **Wymagane minimalne parametry techniczne** | **Wymóg do spełnienia (warunek graniczny)** | **OFEROWANE PARAMETRY TECHNICZNE - podaje**  **Wykonawca**  **Wymogi dotyczące opisu oferowanych parametrów: TAK –**  TAK – wykonawca spełnia konkretny parametr przy czym Zamawiający oczekuje by w przypadku wymagań dotyczących minimalnych parametrów opisać szczegółowo parametry oferowane przez wykonawcę  NIE – wykonawca nie spełnia konkretnego parametru |
| **FUNKCJONALNOŚCI** | | | |
| **1.\*** | Tworzenie głównego drzewa Root CA | TAK |  |
| **2.\*** | Tworzenie podrzędnych drzew do wystawiania certyfikatów na dane danej  jednostki organizacyjnej w danym przedsiębiorstwie | TAK |  |
| **3.\*** | Tworzenie klastra awaryjnego (fail-over) | TAK |  |
| **4.\*** | Nielimitowane czasowo działanie oprogramowania bez dokupowania licencji przedłużających | TAK |  |
| **5.\*** | Nielimitowane wydawanie, zawieszanie, zastrzeganie i odwoływanie  Certyfikatów | TAK |  |
| **6.\*** | Instalacje oraz tworzenie nowych szablonów certyfikatów | TAK |  |
| **7.\*** | Automatyczne generowanie i wystawianie certyfikatów dla urządzeń  mobilnych korzystających z sieci wireless | TAK |  |
| **8.\*** | Konfiguracja list crl oraz wyrywkowej kontroli ważności certyfikatu za  pomocą usługi ocsp | TAK |  |
| **9.\*** | Odwoływanie wystawionych już certyfikatów z możliwością czasowego ich  zawieszenia na dany okres czasu | TAK |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **10.** | Generowanie certyfikatów na podstawie istniejących już domyślnie szablonów certyfikatów minimum takich jak:   * administrator * Authenticated Session * Basic EFS * CA Exchange * CEP Encryption * Code Signing * Computer * Cross-Certification Authority * Directory E-mail Replication * Domain Controller * Domain Controller Authentication * EFS Recovery Agent * Enrollment Agent * Enrollment Agent (Computer) * Exchange Enrollment Agent (Offline request) * Exchange Signature Only * Exchange User * IPSec * IPSec (Offline request) * Kerberos Authentication * Key Recovery Agent (KRA) * OCSP Response Signing * Remote Access Service (RAS) and Internet Authentication Service (IAS) Server * Root CA * Router (Offline request) * Smart Card Logon * Smart Card User * Subordinate CA * Trust List Signing * User * User Signature Only * Web Server * Workstation Authentication | TAK |  |
| **WSPIERANE ALGORYTMY** | | | |
| **1.\*** | SHA1, SHA2 (SHA256, SHA384, SHA512) | TAK |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **2.\*** | RSA o długości 1024, 2048 oraz 4096 | TAK |  |
| **3.\*** | ECC/ECDSA NIST P-256, P-384, P-521 | TAK |  |
| **WYMAGANIA TECHNICZNE** | | | |
| **1.\*** | Interfejs graficzny GUI do obsługi oprogramowania | TAK |  |
| **2.\*** | Wsparcie dla systemów operacyjnych dostarczanych w ramach postępowania. | TAK |  |
| **B. *Sieciowy moduł bezpieczeństwa umożliwiający przechowywanie newralgicznego materiału kryptograficznego*** | | | |
| **OBUDOWA** | | | |
| **1.** | Wysokość nie większa niż 2U, dostosowana do montażu w szafie 19” | TAK |  |
| **BEZPIECZEŃSTWO** | | | |
| **1.** | FIPS 140- 2 poziom 3 | TAK |  |
| **OBSŁUGA SYSTEMÓW OPERACYJNYCH** | | | |
| **1.\*** | Wsparcie minimum dla systemów typu Windows Server 2008 R2 / 2012 R2  / 2016, Red Hat Enterprise Linux Server 5 i 6 | TAK |  |
| **PORTY** | | | |
| **1.\*** | 2x RJ45 1000 BASE-T umożliwiające stworzenie wirtualnego numeru IP rozkładającego ruch na dwa interfejsy | TAK |  |
| **2.\*** | 1x VGA | TAK |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **3.\*** | 1x USB 2.0 | TAK |  |
| **OBSŁUGA INTERFEJSÓW** | | | |
| **1.\*** | PKCS#11 | TAK |  |
| **2.\*** | MSCAPI | TAK |  |
| **3.\*** | Java JCA/JCE API | TAK |  |
| **OBSŁUGA ALGORYTMÓW KRYPTOGRAFICZNYCH** | | | |
| **1.\*** | Kryptografia symetryczna: AES, DES, Triple-DES | TAK |  |
| **2.\*** | Kryptografia asymetryczna: DSA, ECDSA, RSA | TAK |  |
| **3.\*** | Funkcje skrótu: SHA-1, SHA-2, SHA-3, RIPEMD | TAK |  |
| **INTEGRACJA** | | | |
| **1.\*** | Moduł musi udostępniać dodatkowe API umożliwiające integrację z:   * PKCS#11 * Java Cryptographic Extensions (JCE) * Microsoft Crypto API (CSP) * Cryptography Next Generation (CNG) | TAK |  |
| **FUNKCJONALNOŚCI** | | | |
| **1.\*** | Nielimitowana ilość aplikacji klienckich korzystających z modułu. | TAK |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **2\*** | Urządzenie musi :   * wspierać silną autoryzacje użytkownika w celach administracyjnych, do autoryzacji wymaga się dwóch dedykowanych kart producenta wraz z certyfikowanym czytnikiem posiadającym PIN pad do wprowadzania PIN-u karty. * wspierać backup głównego klucza (Master Backup Key) i mieć możliwość jego zapisu do pliku, oraz na dedykowane karty   producenta z dedykowaną przestrzenią na Główny klucz szyfrujący  (Master Backup Key). | TAK |  |
| **3.\*** | Możliwość zarządzania modułem na bazie ról oraz autoryzację opartą o podział sekretu do autoryzacji w trybie “n of m” | TAK |  |
| **CERTYFIKATY** | | | |
| **1.\*** | FIPS 140-2 Level 3 | TAK |  |
| **2.\*** | CE, FCC Class B | TAK |  |
| **3.\*** | UL, IEC/EN 60950-1 | TAK |  |
| **4.\*** | CB certificate | TAK |  |
| **5.\*** | RoHS II, WEEE | TAK |  |
| **WYPOSAŻENIE DODATKOWE** | | | |
| **1.\*** | Minimum 10 szt. dedykowanych do urządzenia kart | TAK |  |
| **2.\*** | Dedykowany czytnik kart | TAK |  |
| **GWARANCJA** | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **1.\*** | Gwarancja 5 Lat | TAK |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **12. Wymagania wdrożeniowe** | | | |
| **Lp.** | **Minimalne wymagania wdrożeniowe** | **Wymóg do spełnienia (warunek graniczny)** | **POTWIERDZENIE ZAOFEROWANIA MINIMALNYCH**  **WYMAGAŃ WZDROŻENIOWYCH - podaje Wykonawca**  **Wymogi dotyczące opisu oferowanych parametrów:**  TAK – wykonawca spełnia konkretny parametr przy czym Zamawiający oczekuje by w przypadku wymagań dotyczących minimalnych parametrów opisać szczegółowo parametry oferowane przez wykonawcę  NIE – wykonawca nie spełnia konkretnego parametru |
| **OGÓLNE** | | | |
| **1.\*** | Montaż opisanego w pkt. 1-8 przedmiotu zamówienia w szafach typu Rack Zamawiającego w sposób zgodny z zaleceniami producenta dostarczanych urządzeń oraz prowadzenie kabli nie może powodować  zaburzeń w cyrkulacji gorącego powietrza wydmuchiwanego z serwerów. | TAK |  |
| **2. \*** | Stworzenie klastra serwerów w oparciu o oprogramowanie wirtualizacyjne dostarczane w ramach postępowania.  Fizyczne serwery mają zostać skonfigurowane w trybie wysokiej dostępności (awaria jednego serwera nie może powodować niedostępności usług uruchomionych na dostarczanych w postępowaniu serwerach).  Dane serwerów będą przechowywane na dostarczanych macierzach. | TAK |  |
| **3.\*** | Testy niezawodności środowiska serwerowego poprzez odłączanie jednej ze ścieżki/wyłączanie urządzenia oraz test redundancji zasilania | TAK |  |
| **4.\*** | Centrum autoryzacji (CA) musi zostać skonfigurowane w sposób zgodny z zaleceniami producenta sprzętowego modułu bezpieczeństwa. | TAK |  |
| **5\*** | Minimalne wymagania do wykonania w ramach uruchomienia Centrum Autoryzacji przeprowadzone przez Wykonawcę:   * instalacja urządzenia LAN w miejscu wskazanym przez zamawiającego * inicjalizacja urządzenia (procedurę bootstrap) * integracja z Centrum Autoryzacji za pomocą interfejsu CSP * konfiguracja głównego Urzędu Certyfikacyjnego * integracja z wbudowanym (wymaganym) w serwer modułem | TAK |  |

|  |  |  |  |
| --- | --- | --- | --- |
|  | bezpieczeństwa umożliwiając tworzenie backupów – z urządzenia LAN na kartę PCI-e   * instruktaż z obsługi urządzenia bezpieczeństwa obejmujący min.:   + Pierwsze uruchomienie i rozruch - procedura BootStrap.   + Inicjalizacja Sprzętowego Modułu Bezpieczeństwa - wygenerowanie kart administracyjnych dla głównych administratorów.   + Zarządzanie użytkownikami i autoryzacją.   + Konfiguracja dostępu do LAN Sprzętowego Modułu   Bezpieczeństwa po protokole SSH do zarządzania poprzez sieć LAN   * + Dołączanie dodatkowego magazynu danych na klucze kryptograficzne z HSM   + Administracja poprzez Comand Line Interface VS Graphic User Interface   + Tworzenie kopi bezpieczeństwa i odzyskiwanie.   + Inicjalizacja komunikacji z Sprzętowym Modułem Bezpieczeństwa po PCS#11, CSP. * podział kluczy kryptograficznych szyfrujących cały materiał   krypograficzny znajdujący się w pamięci urządzenia na minimum 4 karty inteligentne   * PIN do każdej karty powinien zostać zmieniony po przeprowadzonym wdrożeniu. * użytkownik administracyjny Sprzętowego Modułu Bezpieczeństwa musi logować się na „dwie ręce” – procedura logowania musi wymagać dwóch użytkowników/kart. * miejscem składowania materiały kryptograficznego powinna być pamięć wewnętrzna Sprzętowego Modułu Bezpieczeństwa. |  |  |
| **6.\*** | Proces konfiguracji Centrum Autoryzacji zakłada wydanie certyfikatu Root CA w jednostce lidera projektu (Szpital Międzyrzecki Sp. z o.o.)  oraz musi zostać wydany certyfikat SubCA z kluczem na urządzeniu HSM dostarczanym do Szpitala Międzyrzeckiego Sp z o.o.  Finalnie SubCA musi wydawać certyfikaty dla użytkowników Szpitala Zamawiającego. | TAK |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **7.\*** | Wymaga konfiguracja akcji shutdown na zasilaczach awaryjnych dostarczanych w ramach postępowania w przypadku braku zasilania z sieci dla klastra serwerów jak i pojedynczych urządzeń wspierających tę  funkcję. | TAK |  |
| **8.\*** | Aktualizacja sterowników do najnowszych na dzień wdrożenia. | TAK |  |
| **9.\*** | Do macierzy należy podłączyć wszystkie serwery fizyczne w taki sposób, aby fizyczne i wirtualne maszyny uruchomione na serwerach fizycznych mogły korzystać z dysków macierzy w możliwie najszybszy sposób. | TAK |  |
| **10.\*** | Instalacja systemów operacyjnych na 3 serwerach fizycznych, podstawowa konfiguracja serwerów, w tym kart sieciowych. | TAK |  |
| **11.\*** | Konfiguracja macierzy dyskowej, w tym skonfigurowanie RAID na poszczególnych grupach dyskowych. | TAK |  |
| **12.\*** | Instruktaż Zespołu Informatycznego odnośnie przeprowadzonego wdrożenia systemu informatycznego na dostarczanym sprzęcie. | TAK |  |

II. **Infrastruktura sprzętowa wraz z Centrum Autoryzacji dla Samodzielnego Publicznego Szpitala dla Nerwowo i Psychicznie Chorych w Międzyrzeczu**

|  |  |  |  |
| --- | --- | --- | --- |
| **1. Serwer do obsługi wirtualizacji- 2 szt.** | | | |
| **Lp.** | **Wymagane minimalne parametry techniczne** | **Wymóg do spełnienia (warunek graniczny)** | **OFEROWANE PARAMETRY TECHNICZNE - podaje**  **Wykonawca**  **Wymogi dotyczące opisu oferowanych parametrów:**  TAK – wykonawca spełnia konkretny parametr przy czym Zamawiający oczekuje by w przypadku wymagań dotyczących minimalnych parametrów opisać szczegółowo parametry oferowane przez wykonawcę  NIE – wykonawca nie spełnia konkretnego parametru |
| **OBUDOWA** | | | |
| **1.** | • Typu RACK, wysokość nie więcej niż 2U;  • Szyny umożliwiające wysunięcie serwera z szafy stelażowej;  • Opcjonalne ramię porządkujące ułożenie przewodów z tyłu serwera; | TAK |  |
| **Płyta główna** | | | |
| **1.** | • Dwuprocesorowa;  • Wyprodukowana i zaprojektowana przez producenta serwera  • Zainstalowany moduł TPM 2.0  • Wsparcie dla technologii:  o Memory Scrubbing  o Advanced ECC | TAK |  |
| **Procesory** | | | |
| **1.** | • Dwa procesory 10-rdzeniowe o częstotliwości minimum 2,3GHz  • architektura x86\_64 | TAK |  |
| **Pamięć RAM** | | | |
| **1.** | • 256 GB pamięci RAM  • DDR4 Registered | TAK |  |
| **Dyski twarde i napędy** | | | |
| **1.** | • Minimum 8 wnęk dla dysków twardych Hotplug 2,5” lub 3,5”;  • Zainstalowane 2 dyski o pojemności minimum 250GB SAS 10k RPM | TAK |  |
| **Kontrolery LAN** | | | |
| **1.** | • Karta LAN 2x 10Gbit SFP; możliwość wymiany zainstalowanych interfejsów LAN na interfejsy 2x 10Gbit Base- T bez potrzeby wymiany całego układu lub instalacji dodatkowych kart w slotach PCI Express  2 moduły SFP+ Multi Mode Fiber 10GbE LC | TAK |  |
| **Kontrolery I/O** | | | |
| **1.** | • Zainstalowane jedna dwuportowa karta FC 16Gb; | TAK |  |
| **Porty** | | | |
| **1.** | • Zintegrowana karta graficzna ze złączami VGA z tyłu oraz przodu serwera;  • Minimum 1 port USB 3.0 na panelu przednim;  • Min 2 porty USB 3.0 dostępne z tyłu serwera;  • Możliwość instalacji jednego portu serial, możliwość wykorzystania portu do zarządzania serwerem;  • Ilość dostępnych złącz USB nie może być osiągnięta poprzez stosowanie zewnętrznych przejściówek, rozgałęziaczy czy dodatkowych kart rozszerzeń zajmujących jakikolwiek slot PCI Express i/lub USB serwera; | TAK |  |
| **Zasilanie, chłodzenie** | | | |
| **1.** | • Redundantne zasilacze hotplug o mocy minimalnej 400W o sprawności min. 94%; | TAK |  |
| **Zarządzanie** | | | |
| **1.\*** | • Wbudowane diody informacyjne lub wyświetlacz informujące o stanie serwera - system przewidywania, rozpoznawania awarii)  Zintegrowany z płytą główną serwera kontroler sprzętowy zdalnego zarządzania zgodny z IPMI 2.0 o funkcjonalnościach:  • Niezależny od systemu operacyjnego, sprzętowy kontroler umożliwiający pełne zarządzanie, zdalny restart serwera;  o Dedykowana karta LAN 1 Gb/s, dedykowane złącze RJ-45 do komunikacji wyłącznie z kontrolerem zdalnego zarządzania z możliwością przeniesienia tej komunikacji na inną kartę sieciową współdzieloną z systemem operacyjnym;  o Dostęp poprzez przeglądarkę Web, SSH;  o Zarządzanie mocą i jej zużyciem oraz monitoring zużycia energii;  o Zarządzanie alarmami (zdarzenia poprzez SNMP)  o Możliwość przejęcia konsoli tekstowej  o Możliwość zarządzania przez 6 administratorów jednocześnie  o Przekierowanie konsoli graficznej na poziomie sprzętowym oraz możliwość montowania zdalnych napędów i ich obrazów na poziomie sprzętowym (cyfrowy KVM)  o Obsługa serwerów proxy (autentykacja)  o Obsługa VLAN  o Możliwość konfiguracji parametru Max. Transmission Unit (MTU)  o Wsparcie dla protokołu SSDP  o Obsługa protokołów TLS 1.0, TLS 1.1, TLS 1.2, SSL v3  o Obsługa protokołu LDAP  o Synchronizacja czasu poprzez protokół NTP  o Możliwość backupu i odtworzenia ustawień bios serwera oraz ustawień karty zarządzającej  • Oprogramowanie zarządzające i diagnostyczne wyprodukowane przez producenta serwera umożliwiające konfigurację kontrolera RAID, instalację systemów operacyjnych, zdalne zarządzanie, diagnostykę i przewidywanie awarii w oparciu o informacje dostarczane w ramach zintegrowanego w serwerze systemu umożliwiającego monitoring systemu i środowiska (m.in. temperatura, dyski, zasilacze, płyta główna, procesory, pamięć operacyjna);  • Serwer posiada możliwość konfiguracji i wykonania aktualizacji BIOS, Firmware, sterowników serwera bezpośrednio z GUI (graficzny interfejs). | TAK |  |
| **Wspierane OS** | | | |
| **1.\*** | • Microsoft Windows Server 2019, 2016  • VMWare vSphere 6.7  • Suse Linux Enterprise Server 12  • Red Hat Enterprise Linux 7, 8  • Hyper-V Server | TAK |  |
| **System operacyjny** | | | |
| **1.\*** | Licencje na serwerowy system operacyjny muszą uprawniać do uruchamiania serwerowego systemu operacyjnego w środowisku fizycznym i minimum 4 wirtualnych środowisk(per serwer) serwerowego systemu operacyjnego za pomocą wbudowanych mechanizmów wirtualizacji .Serwerowy system operacyjny musi posiadać następujące, wbudowane cechy.  1) Możliwość wykorzystania 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym.  2) Możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności do 64TB przez każdy wirtualny serwerowy system operacyjny.  3) Możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania 7000 maszyn wirtualnych.  4) Możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci.  5) Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy.  6) Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy.  7) Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.  8) Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading.  9) Wbudowane wsparcie instalacji i pracy na wolumenach, które:  a) pozwalają na zmianę rozmiaru w czasie pracy systemu,  b) umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,  c) umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów,  d) umożliwiają zdefiniowanie list kontroli dostępu (ACL).  10) Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.  11) Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.  12) Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET  13) Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.  14) Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.  15) Dostępne dwa rodzaje graficznego interfejsu użytkownika:  a) Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,  b) Dotykowy umożliwiający sterowanie dotykiem na monitorach dotykowych.  16) Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe,  17) Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji.  18) Mechanizmy logowania w oparciu o:  a) Login i hasło,  b) Karty z certyfikatami (smartcard),  c) Wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM),  19) Możliwość wymuszania wieloelementowej dynamicznej kontroli dostępu dla: określonych grup użytkowników, zastosowanej klasyfikacji danych, centralnych polityk dostępu w sieci, centralnych polityk audytowych oraz narzuconych dla grup użytkowników praw do wykorzystywania szyfrowanych danych..  20) Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).  21) Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.  22) Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa.  23) Pochodzący od producenta systemu serwis zarządzania polityką dostępu do informacji w dokumentach (Digital Rights Management).  24) Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach.  25) Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:  a) Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC,  b) Usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji:  i. Podłączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną,  ii. Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,  iii. Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza.  iv. Bezpieczny mechanizm dołączania do domeny uprawnionych użytkowników prywatnych urządzeń mobilnych opartych o iOS i Windows 8.1.  c) Zdalna dystrybucja oprogramowania na stacje robocze.  d) Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej  e) Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:  i. Dystrybucję certyfikatów poprzez http  ii. Konsolidację CA dla wielu lasów domeny,  iii. Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen,  iv. Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509.  f) Szyfrowanie plików i folderów.  g) Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec).  h) Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów.  i) Serwis udostępniania stron WWW.  j) Wsparcie dla protokołu IP w wersji 6 (IPv6),  k) Wsparcie dla algorytmów Suite B (RFC 4869),  l) Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows,  m) Wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie do 1000 aktywnych środowisk wirtualnych systemów operacyjnych. Wirtualne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności. Mechanizmy wirtualizacji mają zapewnić wsparcie dla:  i. Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych,  ii. Obsługi ramek typu jumbo frames dla maszyn wirtualnych.  iii. Obsługi 4-KB sektorów dysków  iv. Nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra  v. Możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API.  vi. Możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk mode)  26) Możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta serwerowego systemu operacyjnego umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet.  27) Wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath).  28) Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego.  29) Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.  30) Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF. | TAK |  |
| **Gwarancja** | | | |
| **1.** | • Gwarancja 5 Lat  . | TAK |  |
| **Dokumentacja, inne** | | | |
| **1.** | • Serwer musi być fabrycznie nowy i pochodzić z oficjalnego kanału dystrybucyjnego w UE. Nie dopuszcza się użycia serwerów odnawianych, demonstracyjnych lub powystawowych.  • Ogólnopolska, telefoniczna infolinia/linia techniczna producenta serwera  • Możliwość aktualizacji i pobrania sterowników do oferowanego modelu serwera w najnowszych certyfikowanych wersjach bezpośrednio z sieci Internet za pośrednictwem strony www producenta serwera; | TAK |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **2. System wirtualizacji** | | | |
| **Lp.** | **Wymagane minimalne parametry techniczne** | **Wymóg do spełnienia (warunek graniczny)** | **OFEROWANE PARAMETRY TECHNICZNE - podaje**  **Wykonawca**  **Wymogi dotyczące opisu oferowanych parametrów:**  TAK – wykonawca spełnia konkretny parametr przy czym Zamawiający oczekuje by w przypadku wymagań dotyczących minimalnych parametrów opisać szczegółowo parametry oferowane przez wykonawcę  NIE – wykonawca nie spełnia konkretnego parametru |
| **1.** | Licencja dla minimum 2 serwerów fizycznych posiadających 2 procesory | TAK |  |
| **2.** | Warstwa wirtualizacji zainstalowana bezpośrednio na sprzęcie fizycznym bez dodatkowych pośredniczących systemów operacyjnych | TAK |  |
| **3.** | Rozwiązanie zapewniające obsługę wielu instancji systemów operacyjnych  na jednym serwerze fizycznym oraz powinno się charakteryzować maksymalnym możliwym stopniem konsolidacji sprzętowej. | TAK |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **4.** | Pojedynczy klaster może się skalować do 3 fizycznych hostów  (serwerów) z zainstalowaną warstwą wirtualizacji. | TAK |  |
| **5.** | Oprogramowanie do wirtualizacji zainstalowane na serwerze fizycznym potrafiące obsłużyć i wykorzystać procesory fizyczne wyposażone w 480 logicznych wątków oraz do 6TB pamięci fizycznej RAM. | TAK |  |
| **6.** | Oprogramowanie do wirtualizacji ma zapewnić:   * możliwość skonfigurowania maszyn wirtualnych 1-128 procesorowych. * możliwość stworzenia dysku maszyny wirtualnej o wielkości do 62 TB. * możliwość skonfigurowania maszyn wirtualnych   z możliwością przydzielenia do 4 TB pamięci operacyjnej RAM.   * możliwość skonfigurowania maszyn wirtualnych, z których każda może mieć 1-10 wirtualnych kart sieciowych. * możliwość skonfigurowania maszyn wirtualnych, z których każda może mieć 32 porty szeregowe. | TAK |  |
| **7.** | Rozwiązanie musi:   * umożliwiać łatwą i szybką rozbudowę infrastruktury o nowe usługi bez spadku wydajności i dostępności pozostałych wybranych usług. * w możliwie największym stopniu być niezależne od producenta platformy sprzętowej. | TAK |  |
| **8.** | Polityka licencjonowania musi umożliwiać przenoszenie licencji na  oprogramowanie do wirtualizacji pomiędzy serwerami. | TAK |  |
| **9.** | Rozwiązanie musi wspierać następujące systemy operacyjne: MS-DOS 6.22, Windows 3.1, Windows 95, Windows 98, Windows XP, Windows Vista , Windows NT 4.0, Windows 2000, Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows 7, Windows 8, SLES 11,  SLES 10, SLES 9, SLES 8, RHEL 6, RHEL 5, RHEL 4, RHEL 3, Solaris  11 ,Solaris 10, Solaris 9, Solaris 8, OS/2 Warp 4.0, NetWare 6.5, NetWare  6, NetWare 5, OEL 4, OEL 5, Debian, CentOS, FreeBSD, Asianux, Mandriva, Ubuntu 14, Ubuntu 12, SCO OpenServer, SCO Unixware, Mac OS X. | TAK |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **10.** | Rozwiązanie musi:   * umożliwiać przydzielenie większej ilości pamięci RAM dla maszyn wirtualnych niż fizyczne zasoby RAM serwera w celu osiągnięcia maksymalnego współczynnika konsolidacji. * umożliwiać udostępnienie maszynie wirtualnej większej ilości zasobów dyskowych niż jest fizycznie zarezerwowane na dyskach lokalnych serwera lub na macierzy. | TAK |  |
| **11.** | Rozwiązanie powinno posiadać centralną konsolę graficzną do zarządzania maszynami wirtualnymi i do konfigurowania innych funkcjonalności.  Centralna konsola graficzna powinna mieć możliwość działania zarówno, jako aplikacja na maszynie fizycznej lub wirtualnej, jak i jako gotowa, wstępnie skonfigurowana maszyna wirtualna tzw. virtual appliance. | TAK |  |
| **12.** | Rozwiązanie musi zapewnić możliwość bieżącego monitorowania wykorzystania zasobów fizycznych infrastruktury wirtualnej (np. wykorzystanie procesorów, pamięci RAM, wykorzystanie przestrzeni na dyskach/wolumenach) oraz przechowywać i wyświetlać dane maksymalnie sprzed roku. | TAK |  |
| **13.** | Oprogramowanie do wirtualizacji powinno zapewnić możliwość wykonywania kopii migawkowych instancji systemów operacyjnych (tzw. snapshot) na potrzeby tworzenia kopii zapasowych bez przerywania ich  pracy. | TAK |  |
| **14.** | Oprogramowanie do wirtualizacji musi zapewnić możliwość klonowania systemów operacyjnych wraz z ich pełną konfiguracją i danymi. | TAK |  |
| **15.** | Oprogramowanie do wirtualizacji oraz oprogramowanie zarządzające musi posiadać możliwość integracji z usługami katalogowymi Microsoft Active Directory. | TAK |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **16.** | Rozwiązanie musi :   * zapewniać mechanizm bezpiecznego uaktualniania warstwy wirtualizacyjnej (hosta, maszyny wirtualnej) bez potrzeby wyłączania wirtualnych maszyn. * posiadać funkcjonalność wirtualnego przełącznika (virtual switch) umożliwiającego tworzenie sieci wirtualnej w obszarze hosta i   pozwalającego połączyć maszyny wirtualne w obszarze jednego hosta, a także na zewnątrz sieci fizycznej. | TAK |  |
| **17.** | Pojedynczy przełącznik wirtualny powinien mieć możliwość konfiguracji do minimum 4000 portów. | TAK |  |
| **18.** | Pojedynczy wirtualny przełącznik musi posiadać możliwość przyłączania do niego dwóch i więcej fizycznych kart sieciowych, aby zapewnić  bezpieczeństwo połączenia ethernetowego w razie awarii karty sieciowej. | TAK |  |
| **19.** | Wirtualne przełączniki musza obsługiwać wirtualne sieci lokalne (VLAN). | TAK |  |
| **20.** | Rozwiązanie musi:   * zapewniać mechanizm klonowania wskazanych maszyn wirtualnych w obrębie klastra serwerów fizycznych. * mieć możliwość przenoszenia maszyn wirtualnych pomiędzy serwerami fizycznymi. | TAK |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **3. Serwer backup-u- 1 szt.** | | | |
| **Lp.** | **Wymagane minimalne parametry techniczne** | **Wymóg do spełnienia (warunek graniczny)** | **OFEROWANE PARAMETRY TECHNICZNE - podaje**  **Wykonawca**  **Wymogi dotyczące opisu oferowanych parametrów:**  TAK – wykonawca spełnia konkretny parametr przy czym Zamawiający oczekuje by w przypadku wymagań dotyczących minimalnych parametrów opisać szczegółowo parametry oferowane przez wykonawcę  NIE – wykonawca nie spełnia konkretnego parametru |
| **OBUDOWA** | | | |
| **1.** | • Typu RACK, wysokość nie więcej niż 2U;  • Szyny umożliwiające wysunięcie serwera z szafy stelażowej;  • Opcjonalne ramię porządkujące ułożenie przewodów z tyłu serwera; | TAK |  |
| **PŁYTA GŁÓWNA** | | | |
| **1.** | • Wyprodukowana i zaprojektowana przez producenta serwera  • Zainstalowany moduł TPM 2.0  • Wsparcie dla technologii:  o Advanced ECC | TAK |  |
| **Procesory** | | | |
| **1.** | • jeden procesor 8-rdzeniowy  • architektura x86\_64 Taktowanie min. 2,2 GHz | TAK |  |
| **Pamięć RAM** | | | |
| **1.** | • min 32 GB pamięci RAM  • DDR4 Registered | TAK |  |
| **Dyski twarde i napędy** | | | |
| **1.** | • Minimum 8 wnęk dla dysków twardych Hotplug 3,5”;  • Zainstalowane 4 dyski SATA 4TB; | TAK |  |
| **Kontrolery LAN** | | | |
| **1.** | • Karta LAN 2x 10Gbit SFP; możliwość wymiany zainstalowanych interfejsów LAN na interfejsy 2x 10Gbit Base- T bez potrzeby wymiany całego układu lub instalacji dodatkowych kart w slotach PCI Express  2 moduły SFP+ Multi Mode Fiber 10GbE LC | TAK |  |
| **Kontrolery I/O** | | | |
| **1.** | Kontroler pamięci z modułem potrzymania pamięci/nieulotną pamięcią, obsługujący poziomy RAID: 0,1,10,5,50,6,60  • Zainstalowana karta dwuportowa FC 16Gb;  Zainstalowany Kontroler HSM PCIe | TAK |  |
| **Porty** | | | |
| **1.** | • Zintegrowana karta graficzna ze złączami VGA z tyłu oraz przodu serwera;  • Minimum 1 port USB 3.0 na panelu przednim;  • Min 2 porty USB 3.0 dostępne z tyłu serwera;  • Możliwość instalacji jednego portu serial, możliwość wykorzystania portu do zarządzania serwerem;  • Ilość dostępnych złącz USB nie może być osiągnięta poprzez stosowanie zewnętrznych przejściówek, rozgałęziaczy czy dodatkowych kart rozszerzeń zajmujących jakikolwiek slot PCI Express i/lub USB serwera; | TAK |  |
| **Zasilanie, chłodzenie** | | | |
| **1.** | • Redundantne zasilacze hotplug o mocy minimalnej 400W o sprawności min. 94%; | TAK |  |
| **Zarządzanie** | | | |
| **1.\*** | • Wbudowane diody informacyjne lub wyświetlacz informujące o stanie serwera  Zintegrowany z płytą główną serwera kontroler sprzętowy zdalnego zarządzania zgodny z IPMI 2.0 o funkcjonalnościach:  • Niezależny od systemu operacyjnego, sprzętowy kontroler umożliwiający pełne zarządzanie, zdalny restart serwera;  o Dedykowana karta LAN 1 Gb/s, dedykowane złącze RJ-45 do komunikacji wyłącznie z kontrolerem zdalnego zarządzania z możliwością przeniesienia tej komunikacji na inną kartę sieciową współdzieloną z systemem operacyjnym;  o Dostęp poprzez przeglądarkę Web, SSH;  o Zarządzanie mocą i jej zużyciem oraz monitoring zużycia energii;  o Zarządzanie alarmami (zdarzenia poprzez SNMP)  o Możliwość przejęcia konsoli tekstowej  o Możliwość zarządzania przez 6 administratorów jednocześnie  o Przekierowanie konsoli graficznej na poziomie sprzętowym oraz możliwość montowania zdalnych napędów i ich obrazów na poziomie sprzętowym (cyfrowy KVM)  o Obsługa serwerów proxy (autentykacja)  o Obsługa VLAN  o Możliwość konfiguracji parametru Max. Transmission Unit (MTU)  o Wsparcie dla protokołu SSDP  o Obsługa protokołów TLS 1.0, TLS 1.1, TLS 1.2, SSL v3  o Obsługa protokołu LDAP  o Synchronizacja czasu poprzez protokół NTP  o Możliwość backupu i odtworzenia ustawień bios serwera oraz ustawień karty zarządzającej  • Serwer posiada możliwość konfiguracji i wykonania aktualizacji BIOS, Firmware, sterowników serwera bezpośrednio z GUI (graficzny interfejs) . | TAK |  |
| **Wspierane OS** | | | |
| **1.\*** | • Microsoft Windows Server 2019, 2016  • VMWare vSphere 6.7  • Suse Linux Enterprise Server 12  • Red Hat Enterprise Linux 7, 8  • Hyper-V Server | TAK |  |
| **System operacyjny** | | | |
| **1.\*** | Licencja na serwerowy system operacyjny musi uprawniać do uruchamiania dwóch wirtualnych środowisk serwerowego systemu operacyjnego na jednym serwerze fizycznym.  Serwerowy system operacyjny musi posiadać następujące, wbudowane cechy.  1. Możliwość wykorzystania 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym.  2. Możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności do 64TB przez każdy wirtualny serwerowy system operacyjny.  3. Możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania 7000 maszyn wirtualnych.  4. Możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci.  5. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy.  6. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy.  7. Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.  8. Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading.  9. Wbudowane wsparcie instalacji i pracy na wolumenach, które:  a. pozwalają na zmianę rozmiaru w czasie pracy systemu,  b. umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,  c. umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów,  d. umożliwiają zdefiniowanie list kontroli dostępu (ACL).  10. Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.  11. Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.  12. Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET  13. Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.  14. Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.  15. Dostępne dwa rodzaje graficznego interfejsu użytkownika:  a. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,  b. Dotykowy umożliwiający sterowanie dotykiem na monitorach dotykowych.  16. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe,  17. Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji.  18. Mechanizmy logowania w oparciu o:  a. Login i hasło,  b. Karty z certyfikatami (smartcard),  c. Wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM),  19. Możliwość wymuszania wieloelementowej dynamicznej kontroli dostępu dla: określonych grup użytkowników, zastosowanej klasyfikacji danych, centralnych polityk dostępu w sieci, centralnych polityk audytowych oraz narzuconych dla grup użytkowników praw do wykorzystywania szyfrowanych danych..  20. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).  21. Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.  22. Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa.  23. Pochodzący od producenta systemu serwis zarządzania polityką dostępu do informacji w dokumentach (Digital Rights Management).  24. Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach.  25. Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:  a. Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC,  b. Usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji:  i. Podłączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną,  ii. Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,  iii. Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza.  iv. Bezpieczny mechanizm dołączania do domeny uprawnionych użytkowników prywatnych urządzeń mobilnych opartych o iOS i Windows 8.1.  c. Zdalna dystrybucja oprogramowania na stacje robocze.  d. Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej  e. Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:  i. Dystrybucję certyfikatów poprzez http  ii. Konsolidację CA dla wielu lasów domeny,  iii. Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen,  iv. Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509.  f. Szyfrowanie plików i folderów.  g. Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec).  h. Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów.  i. Serwis udostępniania stron WWW.  j. Wsparcie dla protokołu IP w wersji 6 (IPv6),  k. Wsparcie dla algorytmów Suite B (RFC 4869),  l. Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows,  m. Wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie do 1000 aktywnych środowisk wirtualnych systemów operacyjnych. Wirtualne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności. Mechanizmy wirtualizacji mają zapewnić wsparcie dla:  i. Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych,  ii. Obsługi ramek typu jumbo frames dla maszyn wirtualnych.  iii. Obsługi 4-KB sektorów dysków  iv. Nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra  v. Możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API.  vi. Możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk mode)  26. Możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta serwerowego systemu operacyjnego umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet.  27. Wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath).  28. Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego.  29. Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.  30. Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF.  31. Nośnik i klucz produktu pochodzący od producenta sprzętu | TAK |  |
| **Gwarancja** | | | |
| **1.\*** | Gwarancja 5 Lat | TAK |  |
| **Dokumentacja, inne** | | | |
| **1.\*** | • Serwer musi być fabrycznie nowy i pochodzić z oficjalnego kanału dystrybucyjnego w UE. Nie dopuszcza się użycia serwerów odnawianych, demonstracyjnych lub powystawowych.  • Ogólnopolska, telefoniczna infolinia/linia techniczna producenta serwera  • Możliwość aktualizacji i pobrania sterowników do oferowanego modelu serwera w najnowszych certyfikowanych wersjach bezpośrednio z sieci Internet za pośrednictwem strony www producenta serwera; | TAK |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **4. Serwer bazodanowy- 2 szt.** | | | |
| **Lp.** | **Wymagane minimalne parametry techniczne** | **Wymóg do spełnienia (warunek graniczny)** | **OFEROWANE PARAMETRY TECHNICZNE - podaje**  **Wykonawca**  **Wymogi dotyczące opisu oferowanych parametrów:**  TAK – wykonawca spełnia konkretny parametr przy czym Zamawiający oczekuje by w przypadku wymagań dotyczących minimalnych parametrów opisać szczegółowo parametry oferowane przez wykonawcę  NIE – wykonawca nie spełnia konkretnego parametru |
| **OBUDOWA** | | | |
| **1.** | • Typu RACK, wysokość nie więcej niż 2U;  • Szyny umożliwiające wysunięcie serwera z szafy stelażowej;  • Opcjonalne ramię porządkujące ułożenie przewodów z tyłu serwera; | TAK |  |
| **PŁYTA GŁÓWNA** | | | |
| **1.** | • Wyprodukowana i zaprojektowana przez producenta serwera  • Zainstalowany moduł TPM 2.0  • Wsparcie dla technologii:  o Memory Scrubbing  o Advanced ECC | TAK |  |
| **Procesory** | | | |
| **1.** | • Jeden procesor 8-rdzeniowy (nie dopuszcza się większej ilości rdzeni fizycznych) o częstotliwości bazowej min. 3,0GHz  • architektura x86\_64 | TAK |  |
| **Pamięć RAM** | | | |
| **1.** | • min 64 GB pamięci RAM  • DDR4 Registered  • | TAK |  |
| **Dyski twarde i napędy** | | | |
| **1.** | • Minimum 4 wnęki dla dysków twardych Hotplug 2,5” lub 3,5”;  • Zainstalowane 2 dyski SSD Hot-Plug o pojemności min 120GB i parametrze DWPD>=3 | TAK |  |
| **Kontrolery LAN** | | | |
| **1.** | • Karta LAN 2x 10Gbit SFP; możliwość wymiany zainstalowanych interfejsów LAN na interfejsy 2x 10Gbit Base- T bez potrzeby wymiany całego układu lub instalacji dodatkowych kart w slotach PCI Express  2 moduły SFP+ Multi Mode Fiber 10GbE LC, | TAK |  |
| **Kontrolery I/O** | | | |
| **1.** | • Zainstalowana jedna dwuportowa karta FC 16Gb; | TAK |  |
| **Porty** | | | |
| **1.** | • Zintegrowana karta graficzna ze złączami VGA z tyłu oraz przodu serwera;  • Min 1 port USB 3.0 na panelu przednim;  • Min 2 porty USB 3.0 dostępne z tyłu serwera;  • Możliwość instalacji jednego portu serial, możliwość wykorzystania portu do zarządzania serwerem;  • Ilość dostępnych złącz USB nie może być osiągnięta poprzez stosowanie zewnętrznych przejściówek, rozgałęziaczy czy dodatkowych kart rozszerzeń zajmujących jakikolwiek slot PCI Express i/lub USB serwera;; | TAK |  |
| **Zasilanie, chłodzenie** | | | |
| **1.** | • Redundantne zasilacze hotplug o mocy minimalnej 400W o sprawności min. 94% | TAK |  |
| **Zarządzanie** | | | |
| **1.\*** | • Wbudowane diody informacyjne lub wyświetlacz informujące o stanie serwera - system przewidywania, rozpoznawania awarii)  Zintegrowany z płytą główną serwera kontroler sprzętowy zdalnego zarządzania zgodny z IPMI 2.0 o funkcjonalnościach:  • Niezależny od systemu operacyjnego, sprzętowy kontroler umożliwiający pełne zarządzanie, zdalny restart serwera;  o Dedykowana karta LAN 1 Gb/s, dedykowane złącze RJ-45 do komunikacji wyłącznie z kontrolerem zdalnego zarządzania z możliwością przeniesienia tej komunikacji na inną kartę sieciową współdzieloną z systemem operacyjnym;  o Dostęp poprzez przeglądarkę Web, SSH;  o Zarządzanie mocą i jej zużyciem oraz monitoring zużycia energii;  o Zarządzanie alarmami (zdarzenia poprzez SNMP)  o Możliwość przejęcia konsoli tekstowej  o Możliwość zarządzania przez 6 administratorów jednocześnie  o Przekierowanie konsoli graficznej na poziomie sprzętowym oraz możliwość montowania zdalnych napędów i ich obrazów na poziomie sprzętowym (cyfrowy KVM)  o Obsługa serwerów proxy (autentykacja)  o Obsługa VLAN  o Możliwość konfiguracji parametru Max. Transmission Unit (MTU)  o Wsparcie dla protokołu SSDP  o Obsługa protokołów TLS 1.0, TLS 1.1, TLS 1.2, SSL v3  o Obsługa protokołu LDAP  o Synchronizacja czasu poprzez protokół NTP  o Możliwość backupu i odtworzenia ustawień bios serwera oraz ustawień karty zarządzającej  Serwer posiada możliwość konfiguracji i wykonania aktualizacji BIOS, Firmware, sterowników serwera bezpośrednio z GUI (graficzny interfejs) . | TAK |  |
| **Wspierane OS** | | | |
| **1.** | • Microsoft Windows Server 2019, 2016  • VMWare vSphere 6.7  • Suse Linux Enterprise Server 12  • Red Hat Enterprise Linux 7, 8  • Hyper-V Server | TAK |  |
| **System operacyjny** | | | |
| **1.** | System Operacyjny dedykowany do bazy danych systemu his. | TAK |  |
| **Gwarancja** | | | |
| **1.\*** | Gwarancja 5 Lat | TAK |  |
| **Dokumentacja, inne** | | | |
| **1.\*** | • Serwer musi być fabrycznie nowy i pochodzić z oficjalnego kanału dystrybucyjnego w UE. Nie dopuszcza się użycia serwerów odnawianych, demonstracyjnych lub powystawowych.  • Ogólnopolska, telefoniczna infolinia/linia techniczna producenta serwera  • Możliwość aktualizacji i pobrania sterowników do oferowanego modelu serwera w najnowszych certyfikowanych wersjach bezpośrednio z sieci Internet za pośrednictwem strony www producenta serwera; | TAK |  |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **5. Macierz dyskowa- 2 szt.** | | | | | | | |
| **Lp.** | | **Wymagane minimalne parametry techniczne** | | **Wymóg do spełnienia (warunek graniczny)** | | **OFEROWANE PARAMETRY TECHNICZNE - podaje**  **Wykonawca**  **Wymogi dotyczące opisu oferowanych parametrów:**  TAK – wykonawca spełnia konkretny parametr przy czym Zamawiający oczekuje by w przypadku wymagań dotyczących minimalnych parametrów opisać szczegółowo parametry oferowane przez wykonawcę  NIE – wykonawca nie spełnia konkretnego parametru | |
| **OGÓLNE** | | | | | | | |
| **1.** | | System musi być dostarczony ze wszystkimi komponentami do instalacji w standardowej szafie rack 19” z zajętością maks. 2U w tej szafie. Każdy skonfigurowany moduł/obudowa musi posiadać układ nadmiarowy zasilania i chłodzenia, zapewniający bezprzerwową pracę macierzy bez ograniczeń czasowych w przypadku utraty redundancji w danym układzie (zasilania lub chłodzenia). Każdy moduł/obudowa powinien posiadać widoczne elementy sygnalizacyjne do informowania o stanie poprawnej pracy lub awarii. Rozbudowa o dodatkowe moduły dla obsługiwanych dysków powinna odbywać się wyłącznie poprzez zakup takich modułów, bez konieczności zakupu dodatkowych licencji lub specjalnego oprogramowania aktywującego proces rozbudowy lub musi być dostarczona licencja na dwukrotność dostarczanej pojemności. Dostarczana macierz musi umożliwiać podłączenie półek kaskadowo , bądź w formie 2 łańcuchów. Oferowana macierz musi obsługiwać min. 260 dysków wykonanych w technologii hot-plug. Macierz musi umożliwiać rozbudowę i jednoczesne podłączenie i używanie modułów (tzw. „półek dyskowych”) w rozmiarze 2U pozwalająca umieścić do 24 dysków 2,5” typu hotplug dla dysków NL-SAS SAS i SSD oraz w rozmiarze 2U dla 12 dysków 3,5” typu hotplug SAS, NL-SAS oraz do 6U dla min 60 dysków; Wymaga się aby macierz umożliwiała jednoczesne podłączenie i użycie dowolnego rodzaju i kombinacji wyżej wymienionych półek dyskowych Macierz musi posiadać funkcje automatycznego tieringu | | TAK | |  | |
| **POJEMNOŚĆ DOSTARCZONEJ MACIERZY** | | | | | | | |
| **1.** | | * przestrzeń minimum 4,5 TB realizowana na dyskach SSD : * min 2 dyski SSD-SAS 12G o pojemności min. 400GB DWPD3 * min 2 dyski SSD-SAS 12G o pojemności min. 3,8TB DWPD1 * przestrzeń minimum 15,5 TB realizowana na dyskach NL : * min 8 dysków NL SAS 12G o pojemności minimum 4TB lub min 16 dysków NL SAS 12G o pojemności minimum 2TB | | TAK | |  | |
| **KONTROLERY** | | | | | | | |
| **1.** | | • Kontrolery macierzy muszą obsługiwać tryb pracy w układzie min active-active, macierz musi być dostarczona z zainstalowanymi minimum 2 kontrolerami;  • Każdy z kontrolerów macierzy musi posiadać po minimum 32 GB pamięci podręcznej Cache – kontrolery muszą obsługiwać między sobą mechanizm lustrzanej kopii danych (cache mirror) przeznaczonych do zapisu;  • W przypadku awarii zasilania dane nie zapisane na dyski, przechowywane w pamięci podręcznej Cache dla zapisów muszą być zabezpieczone metodą trwałego zapisu na dysk.  • Kontrolery muszą posiadać możliwość ich wymiany bez konieczności wyłączania zasilania całego urządzenia;  • Kontrolery macierzy obsługują funkcjonalność kompresji danych.  • Kontrolery macierzy obsługują funkcjonalność deduplikacji w trybie in-line.  • Macierz musi obsługiwać wymianę kontrolera RAID bez utraty danych zapisanych na dyskach.  • Każdy z kontrolerów RAID powinien posiadać dedykowany minimum 2 interfejsy RJ-45 Ethernet obsługujący połączenia z prędkością minimum 1Gb/s dla zdalnej komunikacji z oprogramowaniem zarządzającym i konfiguracyjnym macierzy.  • Kontrolery macierzy muszą być oparte o procesor wykonany w technologii wielordzeniowej z minimum 4 rdzeniami,  • Kontrolery macierzy muszą obsługiwać min 120 grup dyskowych w całym rozwiązaniu, bez konieczności wymiany dostarczonych kontrolerów  • Oferowana macierz musi mieć wyprowadzone 4 porty FC 16Gb/s do dołączenia serwerów bezpośrednio lub do dołączenia do sieci SAN, na każdy kontroler RAID.  • Macierz musi umożliwiać stosowanie (rozbudowa/wymiana) portów do transmisji danych:  FC 16Gb/s, iSCSI min 10Gb/s  • Stosowanie wyżej wymienionych portów nie może powodować wymiany samych kontrolerów RAID w oferowanym rozwiązaniu a w przypadku konieczność licencjonowania tej funkcjonalności macierz ma być dostarczona z aktywną licencja na instalację i obsługę każdego z wymienionych protokołów transmisji danych | | TAK | |  | |
| **Poziomy RAID** | | | | | | | |
| **1.** | | Macierz musi zapewniać poziom zabezpieczenia danych na dyskach definiowany poziomami RAID:  o Raid-0  o Raid-1  o Raid-10 lub Raid-50  o Raid-5  o Raid-6 | | TAK | |  | |
| **Dyski** | | | | | | | |
| **1.** | | Oferowana macierz musi wspierać dyski hot-plug:  o dyski elektroniczne SSD i mechaniczne HDD z interfejsami SAS12Gb/s  o dyski mechaniczne HDD o prędkości obrotowej min 7,2 krpm, 10 krpm .  • Macierz musi obsługiwać mieszaną konfigurację dysków hot-plug SSD i HDD w rozmiarach 2,5” i 3,5” zainstalowanych w dowolnym module rozwiązania;  • Wszystkie dyski wspierane przez oferowany model macierzy muszą być wykonane w technologii hot-plug i posiadać podwójne porty SAS obsługujące tryb pracy full-duplex  • Macierz musi obsługiwać min. 260 dysków SAS SSD w całym rozwiązaniu, bez konieczności dokupowania/wymiany żadnych innych elementów sprzętowych czy licencyjnych innych niż same półki dyskowe wraz z dyskami;  • Możliwość rozbudowy oferowanego modelu macierzy do minimum 500 dysków bez migracji i przenoszenia danych - jedynie poprzez wymianę modułu kontrolerów macierzy (bez konieczności wymiany posiadanych dysków, półek dyskowych, bez konieczności przenoszenia danych/ istniejącej struktury grup dyskowych/LUN, jak również z zachowaniem istniejącej gwarancji producenta na półki dyskowe i dyski;  • Macierz musi umożliwiać skonfigurowanie dysku hot-spare (dysk zapasowy)  • Macierz musi pozwalać na zaszyfrowanie danych zapisanych na wszystkich obsługiwanych dyskach SSD-SAS i HDD-SAS/NL-SAS minimum kluczem AES256-bit – jeżeli w tym celu niezbędne jest zakupienie dodatkowych licencji bądź komponentów sprzętowych to należy je dostarczyć wraz z macierzą. | | TAK | |  | |
| **Opcje programowe** | | | | | | | |
| **1.** | | • Macierz musi być wyposażona w system kopii migawkowych umożliwiających wykonanie minimum 2048 kopii migawkowych  • Macierz musi umożliwiać zdefiniowanie min. 8000 woluminów (LUN)  • Macierz powinna umożliwiać podłączenie logiczne z serwerami i stacjami poprzez min. 1024 ścieżek logicznych FC  • Macierz musi umożliwiać aktualizację oprogramowania wewnętrznego kontrolerów RAID i dysków bez konieczności wyłączania macierzy oraz bez konieczności wyłączania ścieżek logicznych FC/iSCSI dla podłączonych stacji/serwerów  • Macierz musi umożliwiać dokonywanie w trybie on-line (tj. bez wyłączania zasilania i bez przerywania przetwarzania danych w macierzy) operacje: powiększanie grup dyskowych, zwiększanie rozmiaru woluminu, migrowanie woluminu na inną grupę dyskową  • Macierz musi posiadać wsparcie dla systemów operacyjnych : Microsoft Windows Server 2012R2, 2016, 2019, SuSE Linux Enterprise Server, Red Hat Linux Enterprise Server, HP-UNIX, IBM AIX, SUN Solaris, Vmware Vsphere;  • Macierz musi być dostarczona z licencją na oprogramowanie wspierające technologię typu multipath (obsługa nadmiarowości dla ścieżek transmisji danych pomiędzy macierzą i serwerem) dla połączeń FC i iSCSI.  • Macierz musi posiadać możliwość uruchamiania mechanizmów zdalnej replikacji danych, w trybie synchronicznym i asynchronicznym, po protokołach FC lub IP lub iSCSI, bez konieczności stosowania zewnętrznych urządzeń konwersji wymienionych protokołów transmisji. Funkcjonalność replikacji danych musi być zapewniona z poziomu oprogramowania wewnętrznego macierzy. Replikacja danych musi być obsługiwana w połączeniu z każdą macierzą z tej samej rodziny urządzeń wspierającą obsługę zdalnej replikacji danych.  • Macierz musi posiadać możliwość tworzenia lokalnych tj. w obrębie zasobów macierzy, pełnych kopii danych (tzw. klony danych), kopii przyrostowych oraz kopii lustrzanych (mirror) – nie jest wymagane dostarczenie tej funkcjonalności – opcja rozbudowy  • Macierz musi obsługiwać mechanizm ochrony priorytetów obsługi wybranych zasobów – za taki mechanizm uznaje się funkcję typu ‘cache partitioning’ lub ‘storage partitioning’.  • Macierz musi obsługiwać adresację IP v.4 i IP v.6  • Macierz musi wspierać obsługę mechanizmów Vmware  • Macierz musi obsługiwać mechanizmy Thin Provisioning, czyli przydziału dla obsługiwanych środowisk woluminów logicznych o sumarycznej pojemności większej od sumy pojemności dysków fizycznych zainstalowanych w macierzy.  • Macierz musi obsługiwać mechanizmy typu AST (Automated Storage Tiering) tj. automatycznego migrowania i realokacji bloków danych pomiędzy różnymi technologiami dyskowymi na podstawie analizy częstotliwości operacji I/O dla tych bloków oraz wg potrzeb wydajnościowych serwerów, środowisk i aplikacji korzystających z zasobów macierzy. Mechanizm AST musi być obsługiwany przy korzystaniu zarówno z trzech jak z dwóch dostarczonych technologii dyskowych: SSD, SSAS, NLSAS.  • Macierz musi wspierać usługi VSS (Volume ShadowCopy Services) w systemach klasy Microsoft Windows Sever – wymagane jest dostarczenie niezbędnego oprogramowania / sterowników VSS pozwalających na obsługę VSS przy maksymalnej pojemności i liczbie dysków obsługiwanych przez oferowaną. W czasie trwania gwarancji wymaga się bezpłatnego dostępu do nowych wersji oprogramowania i sterowników  • Macierz musi obsługiwać mechanizmy migracji danych w trybie online z innej macierzy .  • Macierz wspiera rozwiązania klasy ‘klastra macierzowego’ tj. zapewnienia wysokiej dostępności zasobów dyskowych macierzy dla podłączonych platform software’owych i sprzętowych z wykorzystaniem synchronicznej replikacji danych pomiędzy minimum 2 macierzami protokołami FC. Mechanizm klastra macierzowego musi być obsługiwany dla protokołów FC, zarówno w zakresie replikacji danych jak i w zakresie sposobu podłączenia serwerów do zasobów macierzy. Pod użytym pojęciem ‘wysoka dostępność zasobów dyskowych’ należy rozumieć zapewnienie bezprzerwowego działania środowiska (aplikacja/ system operacyjny/ serwer) podłączonego do macierzy (macierz podstawowa) w przypadku wystąpienia awarii logicznego połączenia z tą macierzy bądź awarii samej macierzy, powodujących dla danego środowiska brak dostępu do zasobów macierzy podstawowej. Funkcjonalność ‘klastra macierzowego’ musi pozwalać na automatyczne i ręczne przełączanie obsługi środowisk produkcyjnych z macierzy podstawowej na zapasową w przypadku awarii macierzy podstawowej (tzw. Automated/manual failover). – nie jest wymagane dostarczenie tej funkcjonalności – opcja rozbudowy | | TAK | |  | |
| **Zarządzanie** | | | | | | | |
| **1.** | | • Oprogramowanie do zarządzania musi być zintegrowane z systemem operacyjnym systemu pamięci masowej  • Komunikacja z wbudowanym oprogramowaniem zarządzającym macierzą musi być możliwa w trybie graficznym np. poprzez przeglądarkę WWW oraz w trybie tekstowym.  • Musi być możliwe zdalne zarządzanie macierzą z wykorzystaniem standardowej przeglądarki internetowej (np. Internet Explorer, Google Chrome, Mozilla Firefox) bez konieczności instalacji żadnych dodatkowych aplikacji na stacji administratora  • Wbudowane oprogramowanie macierzy musi obsługiwać połączenia z modułem zarządzania macierzy poprzez szyfrowanie komunikacji protokołami: SSL dla komunikacji poprzez przeglądarkę WWW i protokołem SSH dla komunikacji poprzez CLI | | TAK | |  | |
| **Gwarancja i serwis** | | | | | | | |
| **1.\*** | | Gwarancja 5 Lat  • Macierz musi pochodzić z oficjalnego kanału sprzedaży producenta w UE. Nie dopuszcza się użycia macierzy odnawianych, demonstracyjnych lub powystawowych  • Producent oferowanej macierzy musi posiadać dedykowaną, ogólnie dostępną stronę internetową | | TAK | |  | |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **6. Przełącznik rdzeniowy- 2 szt. wraz oprogramowania do zarządzania infrastrukturą LAN** | | | | | | | |
| **Lp.** | | **Wymagane minimalne parametry techniczne** | | **Wymóg do spełnienia (warunek graniczny)** | | **OFEROWANE PARAMETRY TECHNICZNE - podaje**  **Wykonawca**  **Wymogi dotyczące opisu oferowanych parametrów:**  TAK – wykonawca spełnia konkretny parametr przy czym Zamawiający oczekuje by w przypadku wymagań dotyczących minimalnych parametrów opisać szczegółowo parametry oferowane przez wykonawcę  NIE – wykonawca nie spełnia konkretnego parametru | |
| **OBUDOWA** | | | | | | | |
| **1.** | | Wysokość przełącznika 1U w systemie montażu w szafie typu Rack 19” | | TAK | |  | |
| **2.\*** | | Głębokość: Do montażu w szafie wraz z kompletem odpowiednich szyn. | | TAK | |  | |
| **PORTY** | | | | | | | |
| **1.** | | - min. 24 portów SFP+ 10GE + , oraz wkładki niezbędne do podłączenia dostarczonych serwerów oraz switchy  - min. 2 porty 40GE + kabel Stack  - 1 x RJ-45 lub USB : port konsolowy  - 1 x RJ-45 10/100/ BASE-T management port ( out of the band )  - 1 x USB Type A storage port | | TAK | |  | |
| **Usługi warstwy 2** | | | | | | | |
| **1.** | | • Non-blocking wire speed L2 switching  • Jumbo frames up to 9,216 bytes  • Flow control - IEEE 802.3x for full-duplex mode - Back-pressure flow  control in half-duplex mode  • Broadcast, unicast, and multicast storm protection  • IGMP snooping  • VLAN support - IEEE 802.1Q VLANs - 4,094 VLANs - Port-based  VLANs  • Spanning Tree - IEEE 802.1D STP - IEEE 802.1w RSTP - IEEE 802.1s  MSTP - Per-VLAN Spanning Tree (PVST)  • Link aggregation –  trunk groups – min 16  IEEE 802.3ad Link Aggregation & LACP  • Port mirroring (many-to-one)  • Port security  • LLDP  • Multi-chassis Link Aggregation (MLAG)  • MLAG with Spanning Tree support  • VXLAN Tunnel Endpoint (VTEP) support  • 802.1X support | | TAK | |  | |
| **Usługi warstwy 3** | | | | | | | |
| **1.** | | funkcje routingu:  • ECMP  • RIPv2  • OSPFv2  • MP-BGP (IPv4, IPv6) - Static • VRRP  • DHCP-relay including DHCP option-82 and ARP inspection Layer 3  Multicast  • PIM-SM  • IGMPv1/v2/v3  • VXLAN Tunnel Endpoint (VTEP) - VxLAN over mLAG  • 802.1X support  IPv6:  • OSPFv3   * • IPv6 routing | | TAK | |  | |
| **Bezpieczeństwo** | | | | | | | |
| **1.** | | • Hasło użytkownika ( dostęp do zarządzania )  • L2/L3/L4 ACLs  • TACACS+ AAA  • SSHv1/v2 | | TAK | |  | |
| **Quality of Service** | | | | | | | |
| **1.** | | • IEEE 802.1p-based CoS  • 8 priority queues per port | | TAK | |  | |
| **Zarządzanie** | | | | | | | |
| **1.** | | • Command line interface (CLI) • Telnet and SSH remote login  • Web-Management • SNMPv1/v2c | | TAK | |  | |
| **Środowisko Programowe** | | | | | | | |
| **1.** | | • CLI ze skryptami | | TAK | |  | |
| **Zgodność ze Standardami** | | | | | | | |
| **1.** | | • 802.1D Bridging and Spanning Tree Protocol  • 802.1s Multiple Spanning Tree Protocol  • 802.1w Rapid Spanning Tree Protocol  • 802.1p QOS/COS  • 802.1Q VLAN Tagging  • 802.1X Port-based Network Access Control (PNAC))  • 802.3ad Link Aggregation with LACP  • 802.3ae 10 Gigabit Ethernet  sygnalizacja błędu linku 10G/40G | | TAK | |  | |
| **Kompatybilność Elektromagnetyczna** | | | | | | | |
| **1.** | | - CE Mark (EN55022 Class A)  - FCC Part 15 Class A  - VCCI | | TAK | |  | |
| **Zasilanie** | | | | | | | |
| **1.** | | - Zasilacze PSU (Power Supply Unit): 2 redundantne zasilacze, load-sharing,  hot-swappable,  - AC lub 48VDC | | TAK | |  | |
| **GWARANCJA** | | | | | | | |
| **1.\*** | | Gwarancja 5 Lat | | TAK | |  | |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **7. Przełącznik dystrybucyjny- 2 szt.** | | | | | | | |
| **Lp.** | | **Wymagane minimalne parametry techniczne** | | **Wymóg do spełnienia (warunek graniczny)** | | **OFEROWANE PARAMETRY TECHNICZNE - podaje**  **Wykonawca**  **Wymogi dotyczące opisu oferowanych parametrów:**  TAK – wykonawca spełnia konkretny parametr przy czym Zamawiający oczekuje by w przypadku wymagań dotyczących minimalnych parametrów opisać szczegółowo parametry oferowane przez wykonawcę  NIE – wykonawca nie spełnia konkretnego parametru | |
| **OBUDOWA** | | | | | | | |
| **1.** | | Wysokość przełącznika 1U w systemie montażu w szafie typu Rack 19” , wraz z kompletem odpowiednich szyn | | TAK | |  | |
| **PORTY** | | | | | | | |
| **1.** | | - RJ-45 10/100/1000: 24 szt PoE  - SFP+ 10 GE Porty Uplink: 4szt  - RJ-45 lub USB Port konsoli: 1szt | | TAK | |  | |
| **WYDAJNOŚĆ** | | | | | | | |
| **1.** | | - Możliwość przełączania: min. 104Gb/s  - Szybkość przekazywania: min. 77Mbps  - min. Flash: 128 MB  - min. DRAM: 256MB  - min. Tablica adresów MAC: 16K  - Jumbo Frames: min 9KB  - Auto-negocjacja, Auto- MDI/MDIX | | TAK | |  | |
| **FUNKCJONALNOŚĆ WARSTWY II** | | | | | | | |
| **1.** | | Autonegocjacja szybkości portów i trybu dupleksu  Kontrola przepływu:  - IEEE 802.3x for full duplex mode  - Back-Pressure for half duplex mode  - Protokół Spanning Tree:  - IEEE 802.1D Spanning Tree Protocol (STP)  - IEEE 802.1w Rapid Spanning Tree Protocol (RSTP)  - IEEE 802.1s Multiple Spanning Tree Protocol (MSTP)  - BPDU Guard  - BPDU filtering  - Root Guard  - Broadcast/Multicast/Unknown Unicast Storm Control  - VLANy:  - Supports 4K IEEE 802.1Q VLANs  - Active VLANs: 4K  - GVRP  - EEE 802.1v Protocol-based VLANs  - Mac-based VLANs  - IP based VLAN  - Link Aggregation:  - Static Trunk  - IEEE 802.3ad Link Aggregation Control Protocol  - Trunk groups: 16  - Maximum number of members per group: 8  - IGMP Snooping:  - IGMP v1/v2/v3 snooping  - IGMP proxy  - IGMP Filtering  - IGMP Immediate Leave  - IGMP Querier  - MVR (Multicast VLAN Registration)  - Supports QinQ | | TAK | |  | |
| **Quality of Service** | | | | | | | |
| **1.** | | - Kolejkowanie priorytetowe: 8 sprzętowe kolejki na każdym porcie  - Klasyfikacja ruchu oparta na IEEE 802.1p CoS, DSCP  - Obsługa WRR | | TAK | |  | |
| **Bezpieczeństwo** | | | | | | | |
| **1.** | | - Port security  - IEEE 802.1X port based and MAC based authentication  - MAC authentication  - Access Control List  - DHCP Snooping  - IP Source Guard  - Dynamic ARP Inspection  - RADIUS authentication  - TACACS + authorization and accounting  - SSH (v1.5/v2.0)  - SSL and HTTPS | | TAK | |  | |
| **Zarządzanie** | | | | | | | |
| **1.** | | Zarządzenie przełącznikiem:  - CLI poprzez port console port lub Telnet  - WEB management  - SNMP v1, v2c, v3  Firmware & konfiguracja:  - Aktualizacja firmware z wykorzystaniem serwera TFTP  - Kilka plików konfiguracyjnych na jednym urządzeniu  - Wysyłanie i pobieranie konfiguracji poprzez serwer TFTP  Obsługa:  - RMON (groups 1, 2, 3 and 9)  - BOOTP, DHCP client dla przypisywania adresów IP  - SNTP (RFC 2030)  - Event/Error Log/Syslog  - Obsługa LLDP (802.1ab) | | TAK | |  | |
| **IEEE Standardy** | | | | | | | |
| **1.** | | - IEEE 802.1p Priority tags - IEEE 802.1x Port Authentication - IEEE 802.3z CSMA/CD access method and physical laye rspecifications for 1000BASE Gigabit Ethernet - IEEE 802.1q Virtual LAN - IEEE 802.1d Spanning Tree Protocol - IEEE 802.3ad Link Aggregation Control Protocol - IEEE 802.1s Rapid Spanning Tree Protocol - IEEE 802.1w Multiple Spanning Tree Protocol | | TAK | |  | |
| **Kompatybilność elektromagnetyczna** | | | | | | | |
| **1.** | | - FCC klasa A  - CE | | TAK | |  | |
| **Zasilanie** | | | | | | | |
| **1.** | | - 100-240 VAC, 50/60Hz | | TAK | |  | |
| **GWARANCJA** | | | | | | | |
| **1.\*** | | Gwarancja 5 Lat | | TAK | |  | |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **8. Przełącznik portowy Switch FC- 2 szt.** | | | | | | | |
| **Lp.** | | **Wymagane minimalne parametry techniczne** | | **Wymóg do spełnienia (warunek graniczny)** | | **OFEROWANE PARAMETRY TECHNICZNE - podaje**  **Wykonawca**  **Wymogi dotyczące opisu oferowanych parametrów:**  TAK – wykonawca spełnia konkretny parametr przy czym Zamawiający oczekuje by w przypadku wymagań dotyczących minimalnych parametrów opisać szczegółowo parametry oferowane przez wykonawcę  NIE – wykonawca nie spełnia konkretnego parametru | |
| **OGÓLNE** | | | | | | | |
| **1.** | | Wysokość przełącznika 1U w systemie montażu w szafie typu Rack 19” | | TAK | |  | |
| **2.** | | Ilość portów SFP: 24 szt. porty uniwersalne o maksymalnej przepustowości 32GB/s, z obsługą przepustowości 16Gbit/s, 8Gbit/s i 4Gbit/s z automatycznym wyborem przepustowości (auto-sensing),  obsługa trybu full-duple | | TAK | |  | |
| **3.** | | 12 aktywnych portów | | TAK | |  | |
| **4.** | | Zainstalowane moduły optyczne 12 szt. SFP 16Gbit/s, Short Wave Length (SWL), Multi Mode Fibre (MMF) | | TAK | |  | |
| **5.\*** | | Obsługa trybów pracy portów FC: D\_port, F\_port, E\_port, M-Port | | TAK | |  | |
| **6.\*** | | Obsługa funkcji POD (Ports on Demand) przydziału licencji dla aktywnych portów FC | | TAK | |  | |
| **7.\*** | | Możliwość aktualizacji firmware’u switcha | | TAK | |  | |
| **8.\*** | | Aktywne funkcje: Webtools, Advanced Zoning, FullFabric (z obsługą do minimum 128 przełączników FC) | | TAK | |  | |
| **9.\*** | | Możliwość obsługi funkcjonalności (przez zakupienie odpowiednich licencji): Trunking, Extended Fabric, Fabric Vision | | TAK | |  | |
| **10.\*** | | Zarządzanie min.:   * RJ-45 min 10/100 Mb/s do zarządzania poprzez sieć Ethernet * RJ-45 lub DB9 do zarządzania poprzez interfejs RS232 * USB * In-band over FC | | TAK | |  | |
| **11.\*** | | Sygnalizacja aktywnych i podłączonych portów na panelu przednim urządzenia | | TAK | |  | |
| **12.** | | Zarządzanie poprzez przeglądarkę WWW z obsługą połączeń szyfrowanych 128-bit SSL oraz poprzez usługę SSH | | TAK | |  | |
| **13.** | | Wsparcie dla protokołu SNMP v.3 | | TAK | |  | |
| **14.\*** | | Gwarancja 5 Lat | | TAK | |  | |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **9. Szafa RACK – 1 szt.** | | | | | | | |
| **Lp.** | **Wymagane minimalne parametry techniczne** | | | **Wymóg do spełnienia (warunek graniczny)** | | **OFEROWANE PARAMETRY TECHNICZNE - podaje**  **Wykonawca**  **Wymogi dotyczące opisu oferowanych parametrów:**  TAK – wykonawca spełnia konkretny parametr przy czym Zamawiający oczekuje by w przypadku wymagań dotyczących minimalnych parametrów opisać szczegółowo parametry oferowane przez wykonawcę  NIE – wykonawca nie spełnia konkretnego parametru | |
| **OGÓLNE** | | | | | | | |
| **1.** | 42U pojemności użytecznej do instalacji urządzeń w pozycji poziomej o wymiarach nie mniejszych niż 800mmx1000mm(Szer/gł) | | | TAK | |  | |
| **2.\*** | wyposażona w przednie drzwi perforowane, zamykane na zamek z kluczem, jednoskrzydłowe, możliwość montażu lewa/prawa strona, możliwość zdjęcia bez użycia narzędzi | | | TAK | |  | |
| **3.\*** | wyposażona w tylne drzwi perforowane, dwuskrzydłowe dla ograniczenia przestrzeni serwisowej, zamykane na zamek z kluczem wspólny z zamkiem przednim, możliwość zdjęcia bez użycia narzędzi | | | TAK | |  | |
| **4.\*** | Minimalna klasa ochrony na poziomie IP 20 | | | TAK | |  | |
| **5.\*** | wyposażona w zdejmowane panele boczne | | | TAK | |  | |
| **6.\*** | | wszystkie wolne „U” zaślepione zaślepkami | TAK | |  | |
| **7.\*** | | przystosowana do poprawnej instalacji dostarczonych serwerów rack wraz z ich fabrycznymi prowadnicami przewodów. | TAK | |  | |
| **8.** | | zainstalowane 2 listwy zasilające min. 8 gniazd ,2 półki o głębokości min. 450mm | TAK | |  | |
| **9.** | | Minimalny udźwig szafy co najmniej 900 kg | TAK | |  | |
| **10.** | | Certyfikaty CE, RoHS | TAK | |  | |

|  |  |  |  |
| --- | --- | --- | --- |
| **10. Licencje dostępowe serwerów- 100 szt.** | | | |
| **Lp.** | **Wymagane minimalne parametry techniczne** | **Wymóg do spełnienia (warunek graniczny)** | **OFEROWANE PARAMETRY TECHNICZNE - podaje**  **Wykonawca**  **Wymogi dotyczące opisu oferowanych parametrów:**  TAK – wykonawca spełnia konkretny parametr przy czym Zamawiający oczekuje by w przypadku wymagań dotyczących minimalnych parametrów opisać szczegółowo parametry oferowane przez wykonawcę  NIE – wykonawca nie spełnia konkretnego parametru |
| **1.** | Licencje dostępowe do serwera wirtualizacji z punktu 1.– 50 szt. | TAK |  |
| **2.** | Licencje umożliwiające podłączenie się do serwera wirtualizacji z punktu 1. poprzez zdalny dostęp – 50 szt. | TAK |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **11. Centrum Autoryzacji – 1 szt. składające się z:**  ***A. Oprogramowanie umożliwiające szyfrowanie wrażliwych danych*** | | | |
| **Lp.** | **Wymagane minimalne parametry techniczne** | **Wymóg do spełnienia (warunek graniczny)** | **OFEROWANE PARAMETRY TECHNICZNE - podaje**  **Wykonawca**  **Wymogi dotyczące opisu oferowanych parametrów:**  TAK – wykonawca spełnia konkretny parametr przy czym Zamawiający oczekuje by w przypadku wymagań dotyczących minimalnych parametrów opisać szczegółowo parametry oferowane przez wykonawcę  NIE – wykonawca nie spełnia konkretnego parametru |
| **FUNKCJONALNOŚCI** | | | |
| **1.\*** | Tworzenie głównego drzewa Root CA | TAK |  |
| **2.\*** | Tworzenie podrzędnych drzew do wystawiania certyfikatów na  dane danej jednostki organizacyjnej w danym przedsiębiorstwie | TAK |  |
| **3.\*** | Tworzenie klastra awaryjnego (fail-over) | TAK |  |
| **4.\*** | Nielimitowane czasowo działanie oprogramowania bez dokupowania licencji przedłużających | TAK |  |
| **5.\*** | Nielimitowane wydawanie, zawieszanie, zastrzeganie i  odwoływanie certyfikatów | TAK |  |
| **6.\*** | Instalacje oraz tworzenie nowych szablonów certyfikatów | TAK |  |
| **7.\*** | Automatyczne generowanie i wystawianie certyfikatów dla  urządzeń mobilnych korzystających z sieci wireless | TAK |  |
| **8.\*** | Konfiguracja list crl oraz wyrywkowej kontroli ważności certyfikatu  za pomocą usługi ocsp | TAK |  |
| **9.\*** | Odwoływanie wystawionych już certyfikatów z możliwością  czasowego ich zawieszenia na dany okres czasu | TAK |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **10.\*** | Generowanie certyfikatów na podstawie istniejących już domyślnie szablonów certyfikatów minimum takich jak:   * administrator * Authenticated Session * Basic EFS * CA Exchange * CEP Encryption * Code Signing * Computer * Cross-Certification Authority * Directory E-mail Replication * Domain Controller * Domain Controller Authentication * EFS Recovery Agent * Enrollment Agent * Enrollment Agent (Computer) * Exchange Enrollment Agent (Offline request) * Exchange Signature Only * Exchange User * IPSec * IPSec (Offline request) * Kerberos Authentication * Key Recovery Agent (KRA) * OCSP Response Signing * Remote Access Service (RAS) and Internet Authentication Service   (IAS) Server   * Root CA * Router (Offline request) * Smart Card Logon * Smart Card User * Subordinate CA * Trust List Signing * User * User Signature Only * Web Server * Workstation Authentication | TAK |  |
| **WSPIERANE ALGORYTMY** | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **1.\*** | SHA1, SHA2 (SHA256, SHA384, SHA512) | TAK |  |
| **2.\*** | RSA o długości 1024, 2048 oraz 4096 | TAK |  |
| **3.\*** | ECC/ECDSA NIST P-256, P-384, P-521 | TAK |  |
| **WYMAGANIA TECHNICZNE** | | | |
| **1.** | Interfejs graficzny GUI do obsługi oprogramowania | TAK |  |
| **2.** | Wsparcie dla systemów operacyjnych dostarczanych w ramach postępowania. | TAK |  |
| ***B. Sieciowy moduł bezpieczeństwa umożliwiający przechowywanie newralgicznego materiału kryptograficznego*** | | | |
| **OBUDOWA** | | | |
| **1.\*** | Wysokość nie większa niż 2U, dostosowana do montażu w szafie 19” | TAK |  |
| **BEZPIECZEŃSTWO** | | | |
| **1.** | FIPS 140- 2 poziom 3 | TAK |  |
| **OBSŁUGA SYSTEMÓW OPERACYJNYCH** | | | |
| **1.\*** | Wsparcie minimum dla systemów typu Windows Server 2008 R2 / 2012 R2 / 2016, Red Hat Enterprise Linux Server 5 i 6 | TAK |  |
| **PORTY** | | | |
| **1.** | 2x RJ45 1000 BASE-T umożliwiające stworzenie wirtualnego numeru IP rozkładającego ruch na dwa interfejsy | TAK |  |
| **2.** | 1x VGA | TAK |  |
| **3.** | 1x USB 2.0 | TAK |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **OBSŁUGA INTERFEJSÓW** | | | |
| **1.** | PKCS#11 | TAK |  |
| **2.** | MSCAPI | TAK |  |
| **3.** | Java JCA/JCE API | TAK |  |
| **OBSŁUGA ALGORYTMÓW KRYPTOGRAFICZNYCH** | | | |
| **1.** | Kryptografia symetryczna: AES, DES, Triple-DES | TAK |  |
| **2.** | Kryptografia asymetryczna: DSA, ECDSA, RSA | TAK |  |
| **3.** | Funkcje skrótu: SHA-1, SHA-2, SHA-3, RIPEMD | TAK |  |
| **INTEGRACJA** | | | |
| **1.** | Moduł musi udostępniać dodatkowe API umożliwiające integrację z:   * PKCS#11 * Java Cryptographic Extensions (JCE) * Microsoft Crypto API (CSP) * Cryptography Next Generation (CNG) | TAK |  |
| **FUNKCJONALNOŚCI** | | | |
| **1.\*** | Nielimitowana ilość aplikacji klienckich korzystających z modułu. | TAK |  |
| **2\*** | Urządzenie musi :   * wspierać silną autoryzacje użytkownika w celach administracyjnych, do autoryzacji wymaga się dwóch dedykowanych kart producenta wraz z certyfikowanym czytnikiem posiadającym PIN pad do wprowadzania PIN-u karty. * wspierać backup głównego klucza (Master Backup Key) i mieć możliwość jego zapisu do pliku, oraz na dedykowane karty   producenta z dedykowaną przestrzenią na Główny klucz szyfrujący  (Master Backup Key). | TAK |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **3.\*** | Możliwość zarządzania modułem na bazie ról oraz autoryzację opartą o podział sekretu do autoryzacji w trybie “n of m” | TAK |  |
| **CERTYFIKATY** | | | |
| **1.\*** | FIPS 140-2 Level 3 | TAK |  |
| **2.\*** | CE, FCC Class B | TAK |  |
| **3.\*** | UL, IEC/EN 60950-1 | TAK |  |
| **4.\*** | CB certificate | TAK |  |
| **5.\*** | RoHS II, WEEE | TAK |  |
| **WYPOSAŻENIE DODATKOWE** | | | |
| **1.\*** | Minimum 10 szt. dedykowanych do urządzenia kart | TAK |  |
| **2.\*** | Dedykowany czytnik kart | TAK |  |
| **GWARANCJA** | | | |
| **1.\*** | Gwarancja 5 Lat | TAK |  |

|  |  |  |
| --- | --- | --- |
| **12. Oprogramowanie do zarządzania infrastrukturą – 1 szt. składające się z:** | | |
| **Wymagane minimalne parametry techniczne** | **Wymóg do spełnienia (warunek graniczny)** | **OFEROWANE PARAMETRY TECHNICZNE - podaje**  **Wykonawca**  **Wymogi dotyczące opisu oferowanych parametrów:**  TAK – wykonawca spełnia konkretny parametr przy czym Zamawiający oczekuje by w przypadku wymagań dotyczących minimalnych parametrów opisać szczegółowo parametry oferowane przez wykonawcę  NIE – wykonawca nie spełnia konkretnego parametru |
| **FUNKCJONALNOŚCI** | | |
| System umożliwia bezproblemową i stabilną obsługę co najmniej 250 agentów jednocześnie.  System posiada następującą architekturę:  Agent – komponent odpowiedzialny za zarządzanie komputerem, zbieranie danych oraz przesyłanie danych do serwera z wykorzystaniem bezpiecznego połączenia, pracujący w trybie usługi systemowej.  Konsola administracyjna – przeznaczona do zarządzania całym systemem, w formie w pełni funkcjonalnej aplikacji internetowej (webowej). Pozwala na realizację pełnego zarządzania systemem oraz zasobami, wyposażona w mechanizmy do edycji/modyfikacji/usuwania i analizy danych, zawierająca mechanizmy raportowania (nie jest dopuszczalne stosowanie aplikacji webowej do przeglądania danych oraz innej aplikacji do wprowadzania/edycji danych).  Serwer – oprogramowanie odpowiadające za utrzymywanie komunikacji i wymianę danych z agentami.  Baza danych pracująca na silniku Microsoft SQL Server w wersjach wyspecyfikowanych poniżej. Jako równoważną Zamawiający dopuszcza inne bazy danych pod warunkiem dostarczenia kompleksowego rozwiązania z bazą bez znaczących ograniczeń i licencją bezterminową.  Wszystkie komponenty systemu muszą się aktualizować samodzielnie za pośrednictwem bezpiecznego połączenia z serwerami aktualizacji producenta systemu. Czas aktualizacji wszystkich komponentów systemu: serwer, konsola administracyjna, baza danych, agenci - nie może przekroczyć 24h od wydania przez producenta nowej wersji dowolnego komponentu. Agenci na komputerach muszą się zaktualizować samodzielnie w czasie nie dłuższym niż 1h od pobrania aktualizacji od producenta, przy czym aktualizacja agentów przebiegać w pełni automatycznie  z wykorzystaniem funkcjonalności wbudowanej w system (bez użycia zewnętrznych narzędzi, np. MS Active Directory). W przypadku, gdy połączenie pomiędzy systemem a serwerem aktualizacji producenta nie jest dostępne być możliwość dokonania aktualizacji manualnie poprzez pobranie ze strony producenta paczki aktualizacyjnej w postaci jednego pliku z kompletną aktualizacją.  System w sposób w pełni automatyczny z wykorzystaniem serwera aktualizacji producenta aktualizuje wzorce aplikacji, pakietów, pomoc i inne wbudowane bazy wiedzy.  Agent do działania nie może wymagać instalacji komponentów pomocniczych typu.NET Framework lub innych z wyłączeniem komponentów WMI.  Agent jest dostępny dla administratora z poziomu webowej interfejsu konsoli administracyjnej zawsze w najnowszej wersji wydanej przez producenta (bez konieczności pobierania go od producenta), w postaci pliku msi gotowego do zainstalowania (bez konieczności dodatkowego wykonywania zmian/ustalania parametrów) w pliku msi.  Agent jest możliwy do zainstalowania za pośrednictwem MS Active Directory, za pomocą skryptów lub manualnie, poprzez uruchomienie na danej stacji roboczej.  Agent pracuje w trybie niewidocznym dla użytkownika (usługa systemowa).  System umożliwia generowanie unikatowego identyfikatora agenta – wygenerowanego losowo i unikatowo (np. za pomocą mechanizmu typu GUID) lub  w sposób powtarzalny dla danego komputera) na podstawie kombinacji parametrów wybranych przez użytkownika systemu spośród następujących: nazwy producenta BIOS, numeru seryjnego komputera, system UUID, nazwy komputera, dowolnego oraz losowego ciągu znaków.  Agent posiada definiowalny priorytet pracy (ABOVE\_NORMAL, NORMAL, BELOW\_NORMAL, IDLE), przy czym w każdym momencie administrator może automatycznie z poziomu konsoli administracyjnej systemu wydać polecenie zmiany tej konfiguracji na dowolnej grupie komputerów.  Agent wspiera do sześciu różnych adresów serwera rozumianych jako adresy w sieci lokalnej, rozległej (VPN) oraz za NATem i potrafić wykorzystać adres dostępny (na którym następuje połączenie z serwerem) w dowolnym momencie działania, bez konieczności restartu agenta.  System umożliwia komunikację pomiędzy agentami a serwerem w sieciach lokalnych, rozległych, także gdy komputery znajdują się za NATem.  System ma możliwość współpracy komponentów agent i serwer w taki sposób, aby serwer mógł współpracować ze wszystkimi poprzednimi wersjami agentów.  System ma wbudowane mechanizmy automatycznej konserwacji/utrzymania zgodnie ze zdefiniowanym harmonogramem realizujące co najmniej: usuwanie zbędnych danych z systemu (dane z monitoringu uruchamianych aplikacji, uruchamianych procesów, odwiedzonych stron www, wydrukowanych dokumentów, indeksowanie bazy danych, kopie bezpieczeństwa przyrostowe i nieprzyrostowe, zmniejszanie bazy danych. Harmonogram posiada możliwość ustalenia częstotliwości wykonywania zadania (godzina, dzień, tydzień, miesiąc), możliwość zmiany wartość parametrów wejściowych do wykonania danej konserwacji, a także zatrzymania/uruchomienia wybranych pozycji harmonogramu w dowolnym momencie. System prezentować historię przeprowadzonych konserwacji/utrzymania. | TAK\* |  |
| Konsola administracyjna działa na dowolnej przeglądarce stron WWW zgodnej  z HTML5 (np. Internet Explorer 11, Firefox, Chrome, Opera).  Agent działa na systemach 32 i 64 bitowych: Windows 2003 Server, Windows 2008 Server, Windows 2012 Server, Windows 2016 Server, Windows XP SP3, Windows Vista, Windows 7, Windows 8, Windows 10, MacOS 10.7, MacOS 10.8, Linux dla wersji: Ubuntu v.11.04 lub wyższa, Debian v.6.0 lub wyższa, RedHat v.6.0 lub wyższa, CentOS v.6.0 lub wyższa, Fedora v.16 lub wyższa.  Serwer działa na systemach 32 i 64 bitowych: Windows 2000, Windows 2000 Server, Windows 2003 Server, Windows 2008 Server, Windows 2012 Server, Windows 2016 Server, Windows XP SP3, Windows Vista, Windows 7, Windows 8.  Serwer www jest oparty o platformę: MS Windows 64-bit (Windows XP SP3, Windows Server 2003 lub nowsze) oraz Java 7 (JRE lub JDK), Apache Tomcat 7.  Baza danych działa na silniku Microsoft SQL Server 2005/2008/2012/2014/2016  w wersjach 32 lub 64 bitowych zarówno komercyjnych jak i bezpłatnych (np. Microsoft SQL Server Express Edition).  System posiada możliwość pracy w środowisku wirtualnym Microsoft Hyper-V oraz VMWare. | TAK\* |  |
| System umożliwia wielokrotny, zgodny z harmonogramem lub na życzenie, import użytkowników, komputerów, struktury organizacyjnej (całości bądź wybranego kontenera) z usługi MS Active Directory, przy czym import struktury organizacyjnej następować we wskazane miejsce struktury organizacyjnej zdefiniowanej w systemie.  Import obiektów z MS Active Directory być odporny na zmianę nazw obiektów (nazwy użytkownika, struktury organizacyjnej itp.) – podczas import zmienione dane muszą zostać odpowiednio zaktualizowane wg klucza UUID.  System umożliwia import użytkowników z zewnętrznego pliku CSV.  System posiada wbudowany, w pełni definiowalny przez administratora interfejs do importu innych niż komputery urządzeń (np. pendrive, monitory, switche itp.) wraz  z danymi o kosztach zakupu, nr dokumentu zakupowego, dostawcy, daty zakupu, gwarancji. Import umożliwia pobieranie danych z dowolnego źródła danych  o dowolnej strukturze danych z wykorzystaniem sterownika ODBC (np. z pliku tekstowego, pliku xls, pliku xml) w sposób jednorazowy lub zgodnie ze zdefiniowanym harmonogramem. Import aktualizuje te same dane wcześniej zaimportowane.  System umożliwia pobieranie danych z komputerów (wyników skanowania) metodą bezpośredniego połączenia, za pośrednictwem serwera pocztowego (MAIL), za pośrednictwem serwera HTTP/HTTPS. | TAK\* |  |
| Funkcjonalność agenta  System umożliwia pełne zdalne zarządzanie agentami (w sposób masowy  i jednostkowy) w zakresie: uruchamiania i wyłączania agenta, zmiany konfiguracji, uruchamiania skanowania, przekazania dowolnych zadań do wykonania (poleceń systemu operacyjnego), uruchamiania i wyłączania polityk w obszarze bezpieczeństwa (DLP).  Agent posiada możliwość konfiguracji zakresu skanowania plików w oparciu o nazwę plików (z uwzględnieniem znaków wieloznacznych), lokalizację na konkretnym dysku, datę utworzenia pliku oraz wielkość.  Agent posiada możliwość wyświetlenia dowolnego komunikatu w postaci HTML wysłanego z poziomu konsoli administracyjnej a konsola udostępnić dane o dacie  i godzinie wyświetlenia komunikatu oraz użytkowniku, który go wyświetlił.  Agent posiada budowę modułową – uniemożliwienie pracy jednego z modułów (np. w wyniku niekompatybilnego systemu operacyjnego, pracy programów firm trzecich, awarii sprzętowej) nie może blokować pracy całego Agenta.  Po wykryciu nieprawidłowości w pracy dowolnego z modułów Agent powinien podjąć samoczynną próbę jego naprawy i przywrócenia do działania. | TAK\* |  |
| Konsola jest w pełni polskojęzyczna.  Interfejs konsoli musi być wyposażony w intuicyjne mechanizmy obsługi, zapewnia pełną obsługę funkcjonalną (dodawanie/modyfikacja/usuwanie).  Konsola administracyjna musi być wyposażona w panel zawierający graficzne widgety prezentujące dane w postaci wykresu kołowego i słupkowego bądź w formie tabeli z danymi.  Dane na widgetach muszą być aktualizowane automatycznie nie rzadziej niż 1 raz/ godzinę lub w każdym czasie na życzenia użytkownika.  Widgety muszą być skojarzone dziedzinowo ze wszystkimi obszarami zarządzania infrastrukturą, a każdy obszar powinien być reprezentowany przez min. 5 widgetów (np. w obszarze zarządzania komputerami system powinien być wyposażony  w widgety zawierające: ilość komputerów w ramach danego typu, ilość komputerów on/off-line, strukturę komputerów wg ilości pamięci RAM, ilość komputerów wg ilości wolnego miejsca na dysku, ilość komputerów wg dat ostatnich połączeń).  Z każdego widgetu można uzyskać szczegółową informację analityczną (listę z danymi składającymi się na wybraną wartość na widgecie).  System umożliwia i zapamiętuje w profilu użytkownika indywidualną personalizację interfejsu konsoli administracyjnej (wybór wyświetlanych kolumn, ich kolejność, język, definiowanie filtrów, kolejność sortowania, wyświetlane widgety, ich konfigurację i kolejność).  Dane prezentowane na wszystkich widokach/zakładkach w systemie muszą być dynamicznie filtrowane w oparciu o reguły utworzone przez dowolnego użytkownika systemu. Reguły muszą być zapamiętywane i dostępne w kolejnych sesjach oraz oparte co najmniej o: nazwę komputera, IP, rodzaj systemu operacyjnego, identyfikator agenta, strukturę organizacyjną, stan agenta (włączony/wyłączony), nazwę użytkownika zalogowanego, producenta sprzętu, dostawcę sprzętu, lokalizację komputera, dowolnie zdefiniowaną przez użytkownika wartość (np. kolor obudowy komputera). Użytkownik może wybrać za jednym razem więcej niż jedną regułę. Zmiana wybranej reguły powoduje aktualizację wyświetlonego widoku.  System umożliwia definiowanie poziomu uprawnień dla grupy oraz użytkownika (odczyt, dodawanie, usuwanie, modyfikowanie, wydruk) do wszystkich widoków danych oraz wybranych elementów struktury organizacyjnej, być wyposażony  w opcję dziedziczenia uprawnień. Odebranie praw do widoku lub zakładki na widoku powoduje ukrycie opcji.  Lista użytkowników/administratorów systemu musi być importowana  i aktualizowana zgodnie z harmonogramem w oparciu o mechanizm RBAC (Role Base Access Control) z wybranego obiektu Active Directory. Użytkownik wyłączony/usunięty/zablokowany w Active Directory automatycznie traci prawa do korzystania z konsoli administracyjnej systemu.  Konsola umożliwia wykonywanie poszczególnych poleceń na wielu rekordach,  w szczególności na wszystkich rekordach, również tych, które nie są widoczne  w konsoli w ramach jednej strony (zaznacz wszystko).  Konsola administracyjna zawiera szczegółowe informacje dotyczące pracy wszystkich komputerów: wersja agenta, stanu agenta (włączony/wyłączony), zalogowanego użytkownika, historii czasu włączenia i wyłączenia komputera.  Konsola umożliwia bezpośrednie przejście do witryny internetowej producenta  z poziomu repozytorium producentów (o ile taka jest dostępna, np. DELL).  Konsola umożliwia bezpośrednie przejście do strony producenta zawierającej dodatkowe dane konfiguracyjne na temat konkretnego komputera w oparciu  o Service Tag lub inny unikatowy identyfikator (np. Dell).  Konsola zawiera w sobie pełną dokumentację systemu, dokumentacja być na bieżąco aktualizowana poprzez automatyczne mechanizmy aktualizacji z serwera aktualizacji producenta. | TAK\* |  |
| System umożliwia zarządzanie licencjami w ramach dowolnego elementu struktury organizacyjnej (dla wybranej struktury organizacyjnej pokazuje liczbę instalacji i liczbę licencji w danym modelu licencjonowania wraz z listą komputerów).  System posiada możliwość wykonywania (historia) wielu audytów legalności  i zapamiętuje wyniki tych audytów w odniesieniu do systemów operacyjnych jak  i aplikacji/pakietów, z uwzględnieniem segmentu struktury organizacyjnej.  Zarządzanie oprogramowaniem następuje z podziałem na aplikacje i pakiety oprogramowania.  System pozwala na zdefiniowanie dowolnej ilości tzw. „standardów oprogramowania”, które definiują 3 kategorie oprogramowania: „oprogramowanie standardowe” – pozycje z tej listy są wymagane do zainstalowania obowiązkowo na każdym komputerze, „oprogramowanie dodatkowe” - pozycje z tej listy mogą być zainstalowane (nie jest to wymagane) a instalacja odbywa się na wniosek samego użytkownika lub jego przełożonego, „oprogramowanie nieokreślone” – oprogramowanie nie należące do żadnej z dwóch powyżej zdefiniowanych kategorii, a zidentyfikowane na komputerze.  System umożliwia zdefiniowanie listy aplikacji zabronionych.  System umożliwia utworzenie schematów (kolekcji) oprogramowania zabronionego  i w momencie pojawienia się ich na komputerze przystępuje do automatycznego odinstalowania w trybie cichym (bez interfejsu).  System umożliwia zdefiniowanie dowolnej kategorii oprogramowania/pliku/procesu i samodzielnej przydzielenie oprogramowania/pliku/procesu do kategorii.  System zbiera szczegółowe informacje o systemie operacyjnym (wersja, edycja, service pack, poprawki, data instalacji).  System umożliwia odczytywanie identyfikatorów i kluczy produktowych dla systemu operacyjnego oraz dowolnego oprogramowania, tam gdzie jest to tylko technicznie możliwe.  System wspiera następujące typy licencji: Enterprise, Licensed concurrent, Licensed Name, Licensed per Processor, Licensed per Seat, Licensed per Server, OEM, OEM Downgrade, Open, Select, MOLP Open Value (Company wide), MOLP Open Value (non-Company wide), MOLP Open Value Subscription, CAL, SAAS, Trial, Shareware.  System automatycznie klasyfikuje i rozlicza licencje OEM dla systemów operacyjnych oraz licencje typu freeware dla aplikacji.  System pomija w rozliczeniu licencje wygasłe (po terminie ważności) i informuje administratora o wygasaniu licencji.  System umożliwia wyróżnianie licencji zabezpieczonych kluczami sprzętowymi.  System automatycznie wskazuje liczbę posiadanych licencji oraz liczbę używanego oprogramowania (pokazuje braki oraz nadwyżki).  System automatycznie uwzględnia i rozlicza licencje typu Upgrade i Downgrade wg zdefiniowanych przez użytkownika reguł.  System prezentuje datę instalacji oprogramowania.  System umożliwia ewidencję licencji (data zakupu, cena, dostawca, nr faktury, typ licencji, klucz produktowy, identyfikator produktowy, data wygaśnięcia, nr dokumentu OT, nr zapotrzebowania) poprzez rejestrację dokumentów źródłowych (faktur zakupu) z możliwością dołączenia dowolnych załączników z repozytorium.  System umożliwia przypisanie licencji do użytkownika i/lub komputera oraz udostępnia informację o licencjach zarejestrowanych i jednocześnie wolnych (nieprzypisanych).  System umożliwia zbieranie informacji na temat uruchamianych aplikacji na inwentaryzowanych komputerach (m.in. czas uruchomienia, nazwa zalogowanego użytkownika, nazwa aplikacji). System posiada mechanizm zabezpieczający przed powstaniem niekompletnych lub niewłaściwych zapisów w wyniku braku zasilania lub innych awarii inwentaryzowanego systemu/sprzętu).  System udostępnia informację o uruchamianych aplikacjach w okresie 3/6/12 miesięcy oraz udostępnia datę ostatniego uruchomienia.  System automatycznie wyliczać przybliżone oszczędności z zakupionych a nie zainstalowanych aplikacji, przybliżone oszczędności z zainstalowanych  a niewykorzystanych licencji oraz przybliżone nakłady konieczne na uzyskanie pełnej legalności.  System umożliwia podgląd historii zmian aplikacji i pakietów na komputerach.  System umożliwia zdalne odinstalowanie oprogramowania na jednym bądź wybranych komputerach.  System udostępnia informacje o stopniu wykorzystania aplikacji / pakietów dla modeli licencjonowania oprogramowania typu CAL w podziale na analizę godzinową/dzienną/miesięczną w zadanym okresie czasu. W/w informacja winna być przedstawiona również w postaci graficznej.  System udostępnia informacje o stopniu wykorzystania oprogramowania typu web dla modeli licencjonowania oprogramowania typu CAL w podziale na analizę godzinową/dzienną/miesięczną w zadanym okresie czasu. W/w informacja winna być przedstawiona również w postaci graficznej. | TAK\* |  |
| System ma posiada wbudowaną bazę wzorców dostawcy oprogramowania posiadającą co najmniej 3,5 tys. wzorców aplikacji, 1,3 tys. producentów, 21 tys. plików, 1,5 tys. wbudowanych treści umów licencyjnych różnych producentów oprogramowania.  System udostępnia informacje dotyczące plików, na podstawie których zidentyfikowana została dana aplikacja.  System musi prezentować informacje o ilości i dacie publikacji posiadanej bazy wzorców oprogramowania.  System posiada możliwość definiowania własnych wzorców aplikacji i pakietów (składających się z aplikacji) w oparciu o definiowalne reguły rozpoznawania.  Własne wzorce aplikacji i pakietów muszą posiada pierwszeństwo w procesie rozpoznawania aplikacji i pakietów.  System posiada możliwość zamawiania bezpośrednio z poziomu konsoli administracyjnej u producenta systemu wzorców oprogramowania z możliwością wskazania dla jakiego komputera/komputerów wzorce mają być utworzone. Zamówione i utworzone przez Producenta wzorce muszą automatycznie (bez ingerencji administratora systemu) zostać zaimportowane do systemu.  System musi rozpoznawać wersję i edycję zainstalowanych pakietów Microsoft Office (tam gdzie jest to technicznie możliwe (np. Microsoft Office 2007 Professional, Microsoft Office 2007 Standard, Microsoft Office 2003 Standard itd.). | TAK\* |  |
| System umożliwia: automatyczną inwentaryzację komputerów znajdujących się  w sieci lokalnej oraz komputerów znajdujących się poza siecią lokalną (za NATem).  System zbiera szczegółowe informacje o sprzęcie (producent, model, data produkcji, numer seryjny) w oparciu o klasy WMI (Windows Management Instrumentation). Szczegółowość odczytywania danych musi być parametryzowana za pomocą definiowanego zapytania w standardzie WMI Query Language.  System umożliwia skanowanie kości pamięci RAM (z podaniem jednoznacznej specyfikacji kości, typu, numeru seryjnego oraz informacji o taktowaniu).  System ma odczytywać informacje o zainstalowanych kościach pamięci: producent, numer seryjny (Serial Number), numer części (Part Number), rozmiar, częstotliwość, taktowania.  System posiada możliwość odczytywania danych z dowolnego miejsca rejestru systemowego. Musi istnieć możliwość łączenia (konkatenacji) kilku pozycji z różnych miejsc rejestru oraz możliwość automatycznego, rekurencyjnego wyszukiwania wartości podanego klucza począwszy od wskazanego miejsca w hierarchii kluczy rejestru.  System umożliwia automatyczne skanowanie monitorów podłączonych do komputera (ze wskazaniem producenta, modelu, numeru seryjnego, przekątnej ekranu).  System ma możliwość skanowania dysków twardych (z podaniem typu interfejsu, numeru seryjnego oraz informacji SMART).  System umożliwia budowanie powiadomień administracyjnych w oparciu o dowolne atrybuty tabeli SMART dysku.  System umożliwia skanowanie uprawnień użytkowników oraz grup użytkowników wraz z informacją o uprawnieniach, czy konto jest włączone, zablokowane, czy wymagana jest zmiana hasła, czy hasło wygasa, czy hasło jest wymagane).  System prowadzi szczegółową ewidencję zmian konfiguracji sprzętu.  System udostępnia informacje o występowaniu plików na komputerach (nazwa, rozmiar, rodzaj, wielkość, lokalizacja, w przypadku plików wykonywalnych: wersja, producent).  System umożliwia dokonanie klasyfikacji pliku wg dowolnie zdefiniowanych kategorii (np. audio, wideo, graficzne, erotyczne/pornograficzne, archiwa, wykonywalne.  System pozwala na zdalne trwałe (bez możliwości odzyskania) usunięcie dowolnego pliku/plików na dowolnie zdefiniowanej grupie komputerów.  System udostępnia informacje o zmianach w systemie plików (dodano plik, usunięto plik).  System umożliwia dodawanie notatek do każdej pozycji sprzętu.  System umożliwia ewidencję zdarzeń serwisowych dowolnego typu (np. naprawy sprzętu, wymiany części).  System pozwala na dołączanie do urządzeń dokumentów z repozytorium.  System umożliwia samodzielną definicję, ewidencję oraz wydruk wszelkiego typu protokołów (przyjęcie, przekazanie do użytkowania, likwidacja). | TAK\* |  |
| System automatycznie identyfikuje i klasyfikuje urządzenia podłączane do komputera (pendrive, kamera, aparat, monitor zewnętrzny, pamięć masowa, telefon, urządzenie multimedialne itp.  System pozwala na automatycznie lub ręczne przypisanie podłączonego urządzenia do komputera oraz użytkownika.  System ewidencjonuje historię podłączanych urządzeń zewnętrznych w zakresie: komputer, data, godzina, kto podłączył, czy urządzenia było podłączane na innym komputerze, czy urządzenie było podłączane przez innego użytkownika). | TAK\* |  |
| System umożliwia inwentaryzację manualną (ewidencję) sprzętu innego niż komputery: np. drukarki, switche, routery, monitory, pamięci masowe itp.  System musi być wyposażony we wbudowany, konfigurowalny w zakresie IP oraz portów, pracujący zgodnie z harmonogramem skaner SNMP. Skaner musi wykryć typ urządzenia na danym IP/porcie i zwracać podstawowe informacje o tym urządzeniu (nazwa, producent, opis).  Skaner SNMP musi kojarzyć (łączyć) zinwentaryzowane urządzenia (np. komputery, drukarki) z danymi uzyskanymi w procesie skanowania IP/port.  System musi być wyposażony we wbudowany, konfigurowalny skaner sieci, pozwalający na zweryfikowanie czy znalezione skanerem komputery posiadają agenta a w przypadku, gdy takiego agenta nie posiadają powinien umożliwia zdalną instalację agenta.  System umożliwia wprowadzanie dowolnych notatek oraz zdarzeń serwisowych.  System monitoruje zmiany ewidencyjne i ruchy sprzętu.  System umożliwia przypisanie urządzenia do użytkownika, ewidencję napraw, gwarancji.  System posiada możliwość przypominania o upływającym terminie gwarancji.  System pozwala na dołączanie do urządzeń dokumentów z repozytorium wewnętrznego systemu.  System udostępnia informację o wartości wprowadzonego sprzętu.  System umożliwia samodzielną definicję, ewidencję oraz wydruk wszelkiego typu protokołów oraz zapewnia automatyczną numerację tych dokumentów zapewniającą unikatowość.  System pozwala na kopiowanie (duplikację) dowolnego urządzenia dowolną ilość razy.  System pozwala na ewidencję umów utrzymaniowych (SLA) w odniesieniu do zaewidencjonowanych licencji oraz urządzeń w zakresie co najmniej: nazwa, okres, data dokumentu, numer dokumentu, dostawca, osoba kontaktowa, wartość, opis, warunki oraz umożliwia dołączenie dowolnej ilości załączników z repozytorium  i powiązanie umowy utrzymaniowej z dowolną ilością zasobów (urządzenia, licencje). | TAK\* |  |
| System automatycznie tworzy bazę danych podpinanych do komputerów urządzeń USB.  System automatycznie klasyfikuje podłączane urządzenia (pamięć masowa, pendrive, aparat fotograficzny, urządzenie multimedialne itp.)  System umożliwia uzyskanie informacji kto, kiedy i na jakim komputerze posługiwał się urządzeniem zewnętrznym, pozwalając na jego jednoznaczne zidentyfikowanie.  System umożliwia utworzenie listy urządzeń USB dozwolonych do stosowania - tzw. białej listy urządzeń USB.  System ma możliwość zidentyfikowania urządzenia USB i wprowadzenia go do systemu za pośrednictwem konsoli administracyjnej oraz wbudowanego do konsoli oprogramowania/skryptu, pozwalając na zidentyfikowanie jednocześnie wielu urządzeń USB (multiplekser USB).  System umożliwia zdefiniowanie reguł stanowiących podstawę użytkowania urządzeń USB (dozwolone/niedozwolone) na inwentaryzowanych komputerach wg kryteriów: użytkownik, dzień tygodnia, okres (data od, godzina od, data do, godzina do), urządzenie USB, komputer, data obowiązywania reguły. | TAK\* |  |
| System ma automatyczne wykonywać dowolne polecenia na dowolnych komputerach: wykonywanie poleceń powłoki, uruchamianie aplikacji, instalacja/deinstalacja oprogramowania, zmiany w rejestrach systemowych (dodawanie, usuwanie, modyfikowanie), usuwanie oraz kopiowanie plików  i folderów, dostarczanie wyników zwróconych przez wykonane zadanie do bazy danych i prezentowanie ich w konsoli zarządzającej, możliwość wykonywania zadań  z uprawnieniami dowolnego użytkownika.  System posiada wbudowany skaner wyposażony w harmonogram skanowania umożliwiający wykrywanie (rozpoznawanie) komputerów z technologią Intel VPro/AMT wraz z identyfikacją IP technologii Vpro, portu VPro oraz wersji Vpro.  System umożliwia zarządzanie komputerami z technologią Intel vPro, w tym: Serial Over LAN, zdalne włączanie, wyłączanie komputera, zdalna konfiguracja BIOS, uruchomienie zdalnie komputera przy użyciu obrazu ISO lub IMG znajdującego się  w dowolnej lokalizacji.  System ma umożliwia połączenie się z wybranym komputerem w trybie graficznym (od VPro v.6).  System umożliwia za pomocą technologii Ultra VNC: przejęcie ekranu, klawiatury  i myszki użytkownika, zdalne uruchamianie aplikacji, zarządzanie usługami i restart komputera, zdalną instalacja oprogramowania, poprawek i aktualizacji (service pack, patch).  System posiada predefiniowane zadania (polecenia) możliwe do wykonania zdalnie – niezwłocznie lub zgodnie z harmonogramem o funkcjonalnościach typowego harmonogramu windows; zadania powinny być podzielone na typy: administracyjne, bezpieczeństwo, konserwacyjne, a użytkownik może utworzyć dowolny nowy typ zadania.  Minimalne zadania predefiniowane: wyświetlanie aktywnych połączeń sieciowych, czyszczenie buforu DNS, pobranie listy zalogowanych użytkowników, ping, tracert, pobranie listy procesów, wyłączenie/włączenie komputera, wyłączenie/włączenie usługi, wyłączenie/włączenie/restart zapory windows, włączenie usługi Windows Update, pobranie zmiennych środowiskowych, opróżnienie kosza, usunięcie plików tymczasowych, wymuszenie sprawdzenia dostępności aktualizacji Windows Update, wymuszenie aktualizacji zasad grup (AD), konserwację dysku twardego.  Każde wykonanie zadania posiada odzwierciedlenie w statusie wykonania zadania (poprawne, z błędem) oraz udostępnia informację zwrotną o przebiegu wykonania (godzina, data, status).  System umożliwia zdefiniowanie dowolnego własnego zadania z poziomu konsoli administracyjnej z wykorzystaniem poleceń cmd, windows powershell. | TAK\* |  |
| System ma posiadać możliwość ustalania harmonogramu, zgodnie z którym uruchamiane są czynności konserwacyjne, naprawcze, porządkujące.  Harmonogram posiada możliwość ustalenia częstotliwości wykonywania danej czynności (godzina, dzień, tydzień, miesiąc), możliwość zmiany wartość parametrów wejściowych, a także zatrzymania/uruchomienia harmonogramu uruchomienia dla każdej z czynności.  System posiada możliwość definiowania czynności wykonywanych automatycznie.  System musi być wyposażony w następujące mechanizmy automatyzacji: wykonywanie kopii bezpieczeństwa bazy danych, identyfikacja aplikacji i pakietów, porządkowanie bazy danych / odbudowa indeksów, usuwanie nadmiarowych danych w bazie danych, usuwanie zewnętrznych plików (logów).  System musi być wyposażony w mechanizmy informowania - wysyłania komunikatów (alerty) o: zasobach zakazanych (pliki erotyczne i pornograficzne), zasobach multimedialnych (pliki multimedialne), nowych komputerach w bazie danych, braku skanowania komputerów, brakach w licencjach, niewłaściwych datach systemowych komputerów, urządzeniach bez użytkowników, zdublowanych systemach operacyjnych, zakazanych procesach/stronach www/aplikacjach, wygasaniu serwisu lub licencji, przekroczeniu wielkości bazy danych, nadmiernym obciążeniu dysków twardych, nadmiernym obciążeniu sieci, nadmiernym obciążeniu sieci na komputerze, nadmiernym obciążeniu procesora, nadmiernym obciążeniu pamięci RAM, małej ilości wolnego miejsca na dysku, upływającej gwarancji.  System musi wspierać obsługę dowolnych poleceń powłoki na stacjach roboczych (kopiowanie plików, usuwanie plików, przenoszenie plików, zmiana ustawień systemu, wykonywanie programów, instalacja oprogramowania, instalacja poprawek itp.).  System umożliwia wykonanie poleceń z uprawnieniami dowolnego użytkownika (Uruchom jako)  System umożliwia tworzenie zadań cyklicznych dla komputerów.  Obsługa zadań cyklicznych następować w cyklu dziennym: co n dni, w każdy dzień powszedni, nowe zadanie n dni od wykonania, tygodniowym: w wybrane dni co  n tygodni, nowe zadanie n tygodni od wykonania, miesięcznym: co x miesięcy n-tego dnia, pierwszy/drugi/trzeci/czwarty/ostatni poniedziałek/ wtorek/środa/czwartek/ piątek/sobota/niedziela/dzień wolny/dzień powszedni co n miesięcy, nowe zadanie  n miesięcy od wykonania, rocznym: n dzień w wybranym miesiącu,  w pierwszy/drugi/trzeci/czwarty/ostatni, w dowolny dzień tygodnia, dzień wolny/dzień powszedni wybranego miesiąca, nowe zadanie n lat od wykonania.  System musi obsługiwać zadania cykliczne: bez daty końcowej, z końcem cyklu po  n wystąpieniach, z końcem cyklu w określonej dacie. | TAK\* |  |
| System umożliwia obsługę magazynu IT.  System umożliwia obsługę dowolnej ilości magazynów w różnych lokalizacjach.  System umożliwia obsługę dokumentów PZ, WZ, MM+, MM-, LI.  System prowadzi ewidencję materiałów w magazynach w oparciu o metodę FIFO (pierwsze przyszło pierwsze wyszło).  System umożliwia obsługę kodów kreskowych dla materiałów w magazynach.  System udostępnia informację o wartościach materiałów w poszczególnych magazynach, stanach materiałów w magazynach, dokumentach dotyczących danego materiału w dowolnym magazynie. | TAK\* |  |
| Konsola administracyjna być wyposażona w repozytorium dokumentów dowolnego typu.  Repozytorium umożliwia: dodawanie nowych dokumentów dowolnego typu, przeszukiwanie, oznaczanie dokumentów (znaczniki TAG) więcej niż jednym znacznikiem, podgląd dokumentów, dołączanie dokumentów z repozytorium  w dowolnym miejscu systemu, uzyskanie informacji w jakich miejscach systemu dany dokument repozytorium występuje. | TAK\* |  |
| System wspiera obsługę kodów kreskowych jedno i dwuwymiarowych.  System wspiera parametryzację kodu w zakresie wielkości graficznej kodu.  System pozwala w każdym momencie na zmianę typu i atrybutów kodu.  System informuje o błędzie generacji kodu, np. na skutek niewłaściwej długości wprowadzonego ciągu znaków w stosunku do danego standardu kodu.  Istnieje możliwość podglądu kodu oraz jednostkowego i masowego wydruku kodu/kodów.  System powinien generować kody kreskowe (jedno i dwuwymiarowe) dla każdego zaewidencjonowanego urządzenia w standardzie wybranym przez użytkownika: aztec, codabar, code128, code39, dataMatrix, EAN128, EAN13, EAN8, interleaved2of5, ITF14, PDF417, POSTNET, qrcode, royalMailCBC, UPCA, UPCE, USPSIntelligentMail.  Obsługa kodów kreskowych nie może wymagać instalacji czcionek.  Parametry kodu kreskowego (wymiary, wielkość i typ czcionki) muszą być definiowalne.  System umożliwia współpracę z zewnętrznymi czytnikami kodów. |  |  |
| System posiada możliwość zdefiniowania pakietów tekstowych (kontent) celem automatycznego wysyłania do urządzeń i użytkowników komputerów.  System posiada predefiniowane szkolenia: „Klasyfikowanie informacji stanowiących tajemnicę przedsiębiorstwa”, „Kontrola zabezpieczeń i obiegu informacji stanowiących tajemnicę przedsiębiorstwa”, „Postępowanie w przypadku naruszenia tajemnicy”, „Udostępnienie informacji stanowiących tajemnicę”.  Formatowanie treści musi być zgodne z HTML.  System posiada możliwość edycji treści (zmiana kolejności, usuwanie, dodawanie nowych).  System posiada programowalny harmonogram wysyłania treści do dowolnej grupy odbiorców.  Użytkownik otrzymujący wiadomość musi być powiadamiany wizualne i dźwiękowo  o otrzymaniu nowej wiadomości.  Użytkownik posiada możliwość natychmiastowego odczytania wiadomości lub jej odłożenia (na 10 minut, 1, 2 lub 4 godziny) celem późniejszego odczytania.  System posiada zabezpieczenie (np. synchronizowany z serwerem znacznik czasowy) odporne na zmiany czasu na lokalnym komputerze (użytkownika) a pozwalające na jednoznaczne ustalenie daty i godziny dostarczenia i odczytania wiadomości.  System udostępnia historię przesyłania wiadomości i odczytywania wiadomości przez użytkowników.  System musi generować elektroniczną listę uczestników przeszkolonych  (z odczytanym całym szkoleniem).  System posiada możliwość eksportu/importu treści. | TAK\* |  |
| System posiada możliwość ewidencji wszystkich generowanych wydruków niezależnie od miejsca ich generowania oraz typu drukarki (lokalna, sieciowa).  Ewidencja wydruków obejmuje: nazwę i wielkość dokumentu, datę i godzinę wydruku, nazwę użytkownika drukującego, IP i nazwę komputera, z którego dokonano wydruku, format dokumentu, informację i jedno bądź dwustronnym wydruku, informację o wydruku mono/kolor.  System dla każdego wydruku, dla każdej drukarki obliczać rzeczywisty koszt wydruku w oparciu o wbudowany cennik wydruków obejmujący cenę papieru (w zależności od formatu) oraz cenę materiałów eksploatacyjnych (toner, tusz) dla danej drukarki, typu wydruku, rozmiaru papieru.  System musi generować zestawienia pozwalające ustalić miejsca powstawania kosztów wydruków (komórki organizacyjne, użytkownicy) oraz stopień obciążenia poszczególnych urządzeń drukujących.  System musi prognozować ilość i koszt wydruków na wszystkich drukarkach w okresie kolejnych 3, 6, 12 miesięcy.  System pozwala na grupowanie (kojarzenie) drukarek wg sterowników. |  |  |
| System posiada możliwość monitorowania odwiedzanych stron www niezależnie od typu używanej przeglądarki internetowej.  Ewidencja otwieranych stron dotyczyć wielu jednocześnie otwartych zakładek.  Ewidencja otwieranych stron działa również, gdy otwierana jest strona z połączeniem szyfrowanym (https).  Ewidencja obejmuje co najmniej: nazwę i adres IP komputera, nazwę użytkownika, datę i godzinę, adres strony. | TAK\* |  |
| System posiada możliwość monitorowania dziennika zdarzeń wszystkich komputerów.  Ewidencja zdarzeń następować w oparciu o definiowalną kategorię zdarzenia: critical, error, warning, info, audit failure, audit success, debug oraz typ dziennika: aplikacja, bezpieczeństwo, system.  System pozwala na zdefiniowanie ewidencji zdarzeń z komputerów na podstawie kategorii zdarzenia.  Ewidencja zawiera: datę i godzinę zdarzenia, nazwę i adres IP komputera, typ zdarzenia, opis zdarzenia.  System posiada możliwość monitorowania daty włączenia i wyłączenia komputera niezależnie czy znajduje się w sieci lokalnej czy też poza nią i prezentować czas pracy komputera w układzie graficznym.  System posiada ewidencję daty i godziny przyłączenia i odłączenia komputera od systemu monitorującego.  System musi ewidencjonować zdarzenia związane z logowaniem się użytkowników do danego komputera, również w przypadku podłączania się wielu użytkowników jednocześnie. | TAK\* |  |
| System prowadzi ewidencję sesji zdalnych połączeń na każdym komputerze.  Informacja o nawiązanej sesji zawiera co najmniej: nazwę i adres IP komputera  z którego nastąpiło połączenia, nazwę użytkownika nawiązującego połączenie, nazwę i adres IP komputera docelowego, adres portu połączenia. | TAK\* |  |
| System umożliwia wyeksportowanie wybranych lub wszystkich danych do formatu xls, csv, OpenOffice calc, html, mht, xml, jpeg, png, gif, bmp.  System posiada możliwość kategoryzowania raportów (spośród wszystkich raportów) oraz dodawania raportów użytkownika (zaprojektowanych przez użytkownika).  System umożliwia generowanie raportów bezpośrednio z każdego widoku w aplikacji z zastosowaniem bieżących filtrów.  Generowanie raportu powinno odbywać się po stronie serwera a nie klienta.  System umożliwia wieloinstancyjność raportowania (wiele otwartych raportów jednocześnie z wielu widoków).  System posiada możliwość generowania i wyświetlania dowolnych wieloparametrycznych raportów w standardzie SAP Crystal Reports (rpt).  System umożliwia eksport danych z raportu do formatów: RPT, PDF, XLS, DOC, RTF.  System powinien obsługiwać raporty parametryczne z parametrami statycznymi (wprowadzanymi w momencie generowania raportów) oraz dynamicznymi (pobieranymi z bazy danych w momencie generowania raportu).  System posiada co najmniej 100 zdefiniowanych raportów dotyczących wszystkich obszarów funkcjonalnych. | TAK\* |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **13. Wymagania wdrożeniowe** | | | |
| **Lp.** | **Minimalne wymagania wdrożeniowe** | **Wymóg do spełnienia (warunek graniczny)** | **POTWIERDZENIE ZAOFEROWANIA MINIMALNYCH**  **WYMAGAŃ WZDROŻENIOWYCH - podaje Wykonawca**  **Wymogi dotyczące opisu oferowanych parametrów:**  TAK – wykonawca spełnia konkretny parametr przy czym Zamawiający oczekuje by w przypadku wymagań dotyczących minimalnych parametrów opisać szczegółowo parametry oferowane przez wykonawcę  NIE – wykonawca nie spełnia konkretnego parametru |
| **OGÓLNE** | | | |
| **1.** | Montaż przedmiotu zamówienia w szafach typu Rack Zamawiającego w sposób zgodny z zaleceniami producenta dostarczanych urządzeń oraz prowadzenie kabli nie może powodować zaburzeń w cyrkulacji gorącego powietrza  wydmuchiwanego z serwerów. | TAK\* |  |
| **2.** | Stworzenie klastra serwerów w oparciu o oprogramowanie wirtualizacyjne dostarczane w ramach postępowania.  Fizyczne serwery mają zostać skonfigurowane w trybie wysokiej dostępności (awaria jednego serwera nie może powodować  niedostępności usług uruchomionych na dostarczanych w postępowaniu serwerach).  Dane serwerów będą przechowywane na dostarczanych macierzach. | TAK\* |  |
| **3.** | Testy niezawodności środowiska serwerowego poprzez odłączanie jednej ze ścieżki/wyłączanie urządzenia oraz test redundancji  Zasilania | TAK\* |  |
| **4.** | Centrum autoryzacji (CA) musi zostać skonfigurowane w sposób zgodny z zaleceniami producenta sprzętowego modułu  bezpieczeństwa. | TAK\* |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **5** | Minimalne wymagania do wykonania w ramach uruchomienia Centrum Autoryzacji przeprowadzone przez Wykonawcę:   * instalacja urządzenia LAN w miejscu wskazanym przez zamawiającego * inicjalizacja urządzenia (procedurę bootstrap) * integracja z Centrum Autoryzacji za pomocą interfejsu CSP * konfiguracja głównego Urzędu Certyfikacyjnego * integracja z wbudowanym (wymaganym) w serwer modułem   bezpieczeństwa umożliwiając tworzenie backupów – z urządzenia LAN na kartę PCI-e   * instruktaż z obsługi urządzenia bezpieczeństwa obejmujący min.:   + Pierwsze uruchomienie i rozruch - procedura BootStrap.   + Inicjalizacja Sprzętowego Modułu Bezpieczeństwa - wygenerowanie kart administracyjnych dla głównych administratorów.   + Zarządzanie użytkownikami i autoryzacją.   + Konfiguracja dostępu do LAN Sprzętowego Modułu   Bezpieczeństwa po protokole SSH do zarządzania poprzez sieć LAN   * + Dołączanie dodatkowego magazynu danych na klucze kryptograficzne z HSM   + Administracja poprzez Comand Line Interface VS Graphic User Interface   + Tworzenie kopi bezpieczeństwa i odzyskiwanie.   + Inicjalizacja komunikacji z Sprzętowym Modułem Bezpieczeństwa po PCS#11, CSP. * podział kluczy kryptograficznych szyfrujących cały materiał krypograficzny znajdujący się w pamięci urządzenia na minimum 4 karty inteligentne * PIN do każdej karty powinien zostać zmieniony po przeprowadzonym wdrożeniu. * użytkownik administracyjny Sprzętowego Modułu   Bezpieczeństwa musi logować się na „dwie ręce” – procedura logowania musi wymagać dwóch użytkowników/kart.   * miejscem składowania materiały kryptograficznego powinna być pamięć wewnętrzna Sprzętowego Modułu Bezpieczeństwa. | TAK\* |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **6.** | Proces konfiguracji Centrum Autoryzacji zakłada wydanie certyfikatu Root CA w jednostce lidera projektu (Szpital Międzyrzecki Sp. z o.o.) oraz musi zostać wydany certyfikat SubCA z kluczem na urządzeniu HSM dostarczanym do Samodzielnego Szpitala Publicznego dla Nerwowo i Psychicznie Chorych w Międzyrzeczu.  Finalnie SubCA musi wydawać certyfikaty dla użytkowników Szpitala Zamawiającego. | TAK\* |  |
| **7.** | Wymaga konfiguracja akcji shutdown na zasilaczach awaryjnych dostarczanych w ramach postępowania w przypadku braku  zasilania z sieci dla klastra serwerów jak i pojedynczych urządzeń wspierających tę funkcję. | TAK\* |  |
| **8.** | Aktualizacja sterowników do najnowszych na dzień wdrożenia. | TAK\* |  |
| **9.** | Do macierzy należy podłączyć wszystkie serwery fizyczne w taki sposób, aby fizyczne i wirtualne maszyny uruchomione na serwerach fizycznych mogły korzystać z dysków macierzy w możliwie najszybszy sposób. | TAK\* |  |
| **10.** | Instalacja systemów operacyjnych na 3 serwerach fizycznych,  podstawowa konfiguracja serwerów, w tym kart sieciowych. | TAK\* |  |
| **11.** | Konfiguracja macierzy dyskowej, w tym skonfigurowanie RAID  na poszczególnych grupach dyskowych. | TAK\* |  |
| **12.** | Instruktaż Zespołu Informatycznego odnośnie przeprowadzonego wdrożenia systemu informatycznego na dostarczanym sprzęcie. | TAK\* |  |

**III. Infrastruktura sprzętowa wraz z Centrum Autoryzacji dla Samodzielnego Publicznego Zakładu Opieki Zdrowotnej w Sulechowie**

|  |  |  |  |
| --- | --- | --- | --- |
| **1. Serwer do obsługi wirtualizacji- 2 szt.** | | | |
| **Lp.** | **Wymagane minimalne parametry techniczne** | **Wymóg do spełnienia (warunek graniczny)** | **OFEROWANE PARAMETRY TECHNICZNE - podaje**  **Wykonawca**  **Wymogi dotyczące opisu oferowanych parametrów:**  TAK – wykonawca spełnia konkretny parametr przy czym Zamawiający oczekuje by w przypadku wymagań dotyczących minimalnych parametrów opisać szczegółowo parametry oferowane przez wykonawcę  NIE – wykonawca nie spełnia konkretnego parametru |
| **OBUDOWA** | | | |
| **1.** | • Typu RACK, wysokość nie więcej niż 2U;  • Szyny umożliwiające wysunięcie serwera z szafy stelażowej;  • Opcjonalne ramię porządkujące ułożenie przewodów z tyłu serwera; | TAK |  |
| **Płyta główna** | | | |
| **1.** | • Dwuprocesorowa;  • Wyprodukowana i zaprojektowana przez producenta serwera  • Zainstalowany moduł TPM 2.0  • Wsparcie dla technologii:  o Advanced ECC | TAK |  |
| **Procesory** | | | |
| **1.** | • Dwa procesory 10-rdzeniowe o częstotliwości minimum 2,3GHz  • architektura x86\_64  • | TAK |  |
| **Pamięć RAM** | | | |
| **1.** | • 256 GB pamięci RAM  • DDR4 Registered  • | TAK |  |
| **Dyski twarde i napędy** | | | |
| **1.** | • Minimum 8 wnęk dla dysków twardych Hotplug 2,5”lub 3,5”;  • Zainstalowane 2 dyski o pojemności minimum 300GB SSD | TAK |  |
| **Kontrolery LAN** | | | |
| **1.** | - Karta LAN 2x 10Gbit SFP; możliwość wymiany zainstalowanych interfejsów LAN na interfejsy 2x 10Gbit Base- T bez potrzeby wymiany całego układu lub instalacji dodatkowych kart w slotach PCI Express  2 moduły SFP+ Multi Mode Fiber 10GbE LC | TAK |  |
| **Kontrolery I/O** | | | |
| **1.** | • Zainstalowana jedna dwuportowa karta FC 16Gb; | TAK |  |
| **Porty** | | | |
| **1.** | • Zintegrowana karta graficzna ze złączami VGA z tyłu oraz przodu serwera;  • Minimum 1 port USB 3.0 na panelu przednim;  • Min 2 porty USB 3.0 dostępne z tyłu serwera;  • Możliwość instalacji jednego portu serial, możliwość wykorzystania portu do zarządzania serwerem;  • Ilość dostępnych złącz USB nie może być osiągnięta poprzez stosowanie zewnętrznych przejściówek, rozgałęziaczy czy dodatkowych kart rozszerzeń zajmujących jakikolwiek slot PCI Express i/lub USB serwera; | TAK |  |
| **Zasilanie, chłodzenie** | | | |
| **1.** | • Redundantne zasilacze hotplug o mocy minimalnej 400W o sprawności minimum 94%; | TAK |  |
| **Zarządzanie** | | | |
| **1.** | • Wbudowane diody informacyjne lub wyświetlacz informujące o stanie serwera - system przewidywania, rozpoznawania awarii)  Zintegrowany z płytą główną serwera kontroler sprzętowy zdalnego zarządzania zgodny z IPMI 2.0 o funkcjonalnościach:  • Niezależny od systemu operacyjnego, sprzętowy kontroler umożliwiający pełne zarządzanie, zdalny restart serwera;  o Dedykowana karta LAN 1 Gb/s, dedykowane złącze RJ-45 do komunikacji wyłącznie z kontrolerem zdalnego zarządzania z możliwością przeniesienia tej komunikacji na inną kartę sieciową współdzieloną z systemem operacyjnym;  o Dostęp poprzez przeglądarkę Web, SSH;  o Zarządzanie mocą i jej zużyciem oraz monitoring zużycia energii;  o Zarządzanie alarmami (zdarzenia poprzez SNMP)  o Możliwość przejęcia konsoli tekstowej  o Możliwość zarządzania przez 6 administratorów jednocześnie  o Przekierowanie konsoli graficznej na poziomie sprzętowym oraz możliwość montowania zdalnych napędów i ich obrazów na poziomie sprzętowym (cyfrowy KVM)  o Obsługa serwerów proxy (autentykacja)  o Obsługa VLAN  o Możliwość konfiguracji parametru Max. Transmission Unit (MTU)  o Wsparcie dla protokołu SSDP  o Obsługa protokołów TLS 1.0, TLS 1.1, TLS 1.2, SSL v3  o Obsługa protokołu LDAP  o Synchronizacja czasu poprzez protokół NTP  o Możliwość backupu i odtworzenia ustawień bios serwera oraz ustawień karty zarządzającej  • Oprogramowanie zarządzające i diagnostyczne wyprodukowane przez producenta serwera umożliwiające konfigurację kontrolera RAID, instalację systemów operacyjnych, zdalne zarządzanie, diagnostykę i przewidywanie awarii w oparciu o informacje dostarczane w ramach zintegrowanego w serwerze systemu umożliwiającego monitoring systemu i środowiska (m.in. temperatura, dyski, zasilacze, płyta główna, procesory, pamięć operacyjna);  • Serwer posiada możliwość konfiguracji i wykonania aktualizacji BIOS, Firmware, sterowników serwera bezpośrednio z GUI (graficzny interfejs). | TAK\* |  |
| **Wspierane OS** | | | |
| **1.** | • Microsoft Windows Server 2019, 2016  • VMWare vSphere 6.7  • Suse Linux Enterprise Server 12  • Red Hat Enterprise Linux 7, 8  • Hyper-V Server | TAK |  |
| **System operacyjny** | | | |
| **1.** | Licencje na serwerowy system operacyjny muszą uprawniać do uruchamiania serwerowego systemu operacyjnego w środowisku fizycznym i minimum 4 wirtualnych środowisk( per server) serwerowego systemu operacyjnego za pomocą wbudowanych mechanizmów wirtualizacji.  Serwerowy system operacyjny musi posiadać następujące, wbudowane cechy.  1) Możliwość wykorzystania 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym.  2) Możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności do 64TB przez każdy wirtualny serwerowy system operacyjny.  3) Możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania 7000 maszyn wirtualnych.  4) Możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci.  5) Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy.  6) Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy.  7) Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.  8) Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading.  9) Wbudowane wsparcie instalacji i pracy na wolumenach, które:  a) pozwalają na zmianę rozmiaru w czasie pracy systemu,  b) umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,  c) umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów,  d) umożliwiają zdefiniowanie list kontroli dostępu (ACL).  10) Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.  11) Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.  12) Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET  13) Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.  14) Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.  15) Dostępne dwa rodzaje graficznego interfejsu użytkownika:  a) Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,  b) Dotykowy umożliwiający sterowanie dotykiem na monitorach dotykowych.  16) Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe,  17) Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji.  18) Mechanizmy logowania w oparciu o:  a) Login i hasło,  b) Karty z certyfikatami (smartcard),  c) Wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM),  19) Możliwość wymuszania wieloelementowej dynamicznej kontroli dostępu dla: określonych grup użytkowników, zastosowanej klasyfikacji danych, centralnych polityk dostępu w sieci, centralnych polityk audytowych oraz narzuconych dla grup użytkowników praw do wykorzystywania szyfrowanych danych..  20) Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).  21) Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.  22) Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa.  23) Pochodzący od producenta systemu serwis zarządzania polityką dostępu do informacji w dokumentach (Digital Rights Management).  24) Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach.  25) Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:  a) Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC,  b) Usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji:  i. Podłączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną,  ii. Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,  iii. Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza.  iv. Bezpieczny mechanizm dołączania do domeny uprawnionych użytkowników prywatnych urządzeń mobilnych opartych o iOS i Windows 8.1.  c) Zdalna dystrybucja oprogramowania na stacje robocze.  d) Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej  e) Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:  i. Dystrybucję certyfikatów poprzez http  ii. Konsolidację CA dla wielu lasów domeny,  iii. Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen,  iv. Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509.  f) Szyfrowanie plików i folderów.  g) Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec).  h) Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów.  i) Serwis udostępniania stron WWW.  j) Wsparcie dla protokołu IP w wersji 6 (IPv6),  k) Wsparcie dla algorytmów Suite B (RFC 4869),  l) Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows,  m) Wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie do 1000 aktywnych środowisk wirtualnych systemów operacyjnych. Wirtualne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności. Mechanizmy wirtualizacji mają zapewnić wsparcie dla:  i. Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych,  ii. Obsługi ramek typu jumbo frames dla maszyn wirtualnych.  iii. Obsługi 4-KB sektorów dysków  iv. Nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra  v. Możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API.  vi. Możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk mode)  26) Możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta serwerowego systemu operacyjnego umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet.  27) Wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath).  28) Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego.  29) Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.  30) Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF.  31) Zorganizowany system szkoleń i materiały edukacyjne w języku polskim. | TAK\* |  |
| **Gwarancja** | | | |
| **1.** | Gwarancja 5 Lat  Gwarantowany czas reakcji do następnego dnia roboczego od przyjęcia zgłoszenia .  Zgłaszanie usterek i awarii w trybie 24/7 | TAK\* |  |
| **Dokumentacja, inne** | | | |
| **1.** | • Serwer musi być fabrycznie nowy i pochodzić z oficjalnego kanału dystrybucyjnego w UE. Nie dopuszcza się użycia serwerów odnawianych, demonstracyjnych lub powystawowych.  • Ogólnopolska, telefoniczna infolinia/linia techniczna producenta serwera  • Możliwość aktualizacji i pobrania sterowników do oferowanego modelu serwera w najnowszych certyfikowanych wersjach bezpośrednio z sieci Internet za pośrednictwem strony www producenta serwera; | TAK\* |  |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **2. System wirtualizacji** | | | | | | | |
| **Lp.** | | **Wymagane minimalne parametry techniczne** | | **Wymóg do spełnienia (warunek graniczny)** | | **OFEROWANE PARAMETRY TECHNICZNE - podaje**  **Wykonawca**  **Wymogi dotyczące opisu oferowanych parametrów:**  TAK – wykonawca spełnia konkretny parametr przy czym Zamawiający oczekuje by w przypadku wymagań dotyczących minimalnych parametrów opisać szczegółowo parametry oferowane przez wykonawcę  NIE – wykonawca nie spełnia konkretnego parametru | |
| **1.** | | Licencja dla minimum 2 serwerów fizycznych posiadających 2 procesory | | TAK\* | |  | |
| **2.** | | Warstwa wirtualizacji zainstalowana bezpośrednio na sprzęcie fizycznym bez dodatkowych pośredniczących systemów operacyjnych | | TAK\* | |  | |
| **3.** | | Rozwiązanie zapewniające obsługę wielu instancji systemów operacyjnych  na jednym serwerze fizycznym oraz powinno się charakteryzować maksymalnym możliwym stopniem konsolidacji sprzętowej. | | TAK\* | |  | |
| **4.** | | Pojedynczy klaster może się skalować do 3 fizycznych hostów  (serwerów) z zainstalowaną warstwą wirtualizacji. | | TAK\* | |  | |
| **5.** | | Oprogramowanie do wirtualizacji zainstalowane na serwerze fizycznym potrafiące obsłużyć i wykorzystać procesory fizyczne wyposażone w 480 logicznych wątków oraz do 6TB pamięci fizycznej RAM. | | TAK\* | |  | |
| **6.** | | Oprogramowanie do wirtualizacji ma zapewnić:   * możliwość skonfigurowania maszyn wirtualnych 1-128 procesorowych. * możliwość stworzenia dysku maszyny wirtualnej o wielkości do 62 TB. * możliwość skonfigurowania maszyn wirtualnych   z możliwością przydzielenia do 4 TB pamięci operacyjnej RAM.   * możliwość skonfigurowania maszyn wirtualnych, z których każda może mieć 1-10 wirtualnych kart sieciowych. * możliwość skonfigurowania maszyn wirtualnych, z których każda może mieć 32 porty szeregowe. | | TAK\* | |  | |
| **7.** | | Rozwiązanie musi:   * umożliwiać łatwą i szybką rozbudowę infrastruktury o nowe usługi bez spadku wydajności i dostępności pozostałych wybranych usług. * w możliwie największym stopniu być niezależne od producenta platformy sprzętowej. | | TAK\* | |  | |
| **8.** | | Polityka licencjonowania musi umożliwiać przenoszenie licencji na  oprogramowanie do wirtualizacji pomiędzy serwerami. | | TAK\* | |  | |
| **9.** | | Rozwiązanie musi wspierać następujące systemy operacyjne: MS-DOS 6.22, Windows 3.1, Windows 95, Windows 98, Windows XP, Windows Vista , Windows NT 4.0, Windows 2000, Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows 7, Windows 8, SLES 11,  SLES 10, SLES 9, SLES 8, RHEL 6, RHEL 5, RHEL 4, RHEL 3, Solaris  11 ,Solaris 10, Solaris 9, Solaris 8, OS/2 Warp 4.0, NetWare 6.5, NetWare  6, NetWare 5, OEL 4, OEL 5, Debian, CentOS, FreeBSD, Asianux, Mandriva, Ubuntu 14, Ubuntu 12, SCO OpenServer, SCO Unixware, Mac OS X. | | TAK\* | |  | |
| **10.** | | Rozwiązanie musi:   * umożliwiać przydzielenie większej ilości pamięci RAM dla maszyn wirtualnych niż fizyczne zasoby RAM serwera w celu osiągnięcia maksymalnego współczynnika konsolidacji. * umożliwiać udostępnienie maszynie wirtualnej większej ilości zasobów dyskowych niż jest fizycznie zarezerwowane na dyskach lokalnych serwera lub na macierzy. | | TAK\* | |  | |
| **11.** | | Rozwiązanie powinno posiadać centralną konsolę graficzną do zarządzania maszynami wirtualnymi i do konfigurowania innych funkcjonalności.  Centralna konsola graficzna powinna mieć możliwość działania zarówno, jako aplikacja na maszynie fizycznej lub wirtualnej, jak i jako gotowa, wstępnie skonfigurowana maszyna wirtualna tzw. virtual appliance. | | TAK\* | |  | |
| **13.** | | Rozwiązanie musi zapewnić możliwość bieżącego monitorowania wykorzystania zasobów fizycznych infrastruktury wirtualnej (np. wykorzystanie procesorów, pamięci RAM, wykorzystanie przestrzeni na dyskach/wolumenach) oraz przechowywać i wyświetlać dane maksymalnie sprzed roku. | | TAK\* | |  | |
| **14.** | | Oprogramowanie do wirtualizacji powinno zapewnić możliwość wykonywania kopii migawkowych instancji systemów operacyjnych (tzw. snapshot) na potrzeby tworzenia kopii zapasowych bez przerywania ich  pracy. | | TAK\* | |  | |
| **15.** | | Oprogramowanie do wirtualizacji musi zapewnić możliwość klonowania systemów operacyjnych wraz z ich pełną konfiguracją i danymi. | | TAK\* | |  | |
| **16.** | | Oprogramowanie do wirtualizacji oraz oprogramowanie zarządzające musi posiadać możliwość integracji z usługami katalogowymi Microsoft Active Directory. | | TAK\* | |  | |

|  |  |  |  |
| --- | --- | --- | --- |
| **17.** | Rozwiązanie musi :   * zapewniać mechanizm bezpiecznego uaktualniania warstwy wirtualizacyjnej (hosta, maszyny wirtualnej) bez potrzeby wyłączania wirtualnych maszyn. * posiadać funkcjonalność wirtualnego przełącznika (virtual switch) umożliwiającego tworzenie sieci wirtualnej w obszarze hosta i   pozwalającego połączyć maszyny wirtualne w obszarze jednego hosta, a także na zewnątrz sieci fizycznej. | TAK\* |  |
| **18.** | Pojedynczy przełącznik wirtualny powinien mieć możliwość konfiguracji do minimum 4000 portów. | TAK\* |  |
| **19.** | Pojedynczy wirtualny przełącznik musi posiadać możliwość przyłączania do niego dwóch i więcej fizycznych kart sieciowych, aby zapewnić  bezpieczeństwo połączenia ethernetowego w razie awarii karty sieciowej. | TAK\* |  |
| **20.** | Wirtualne przełączniki musza obsługiwać wirtualne sieci lokalne (VLAN). | TAK\* |  |
| **21.** | Rozwiązanie musi:   * zapewniać mechanizm klonowania wskazanych maszyn wirtualnych w obrębie klastra serwerów fizycznych. * mieć możliwość przenoszenia maszyn wirtualnych pomiędzy serwerami fizycznymi. | TAK\* |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **3.** **Serwer backup-u- 1 szt.** | | | |
| **Lp.** | **Wymagane minimalne parametry techniczne** | **Wymóg do spełnienia (warunek graniczny)** | **OFEROWANE PARAMETRY TECHNICZNE - podaje**  **Wykonawca**  **Wymogi dotyczące opisu oferowanych parametrów:**  TAK – wykonawca spełnia konkretny parametr przy czym Zamawiający oczekuje by w przypadku wymagań dotyczących minimalnych parametrów opisać szczegółowo parametry oferowane przez wykonawcę  NIE – wykonawca nie spełnia konkretnego parametru |
| **OBUDOWA** | | | |
| **1.** | • Typu RACK, wysokość nie więcej niż 2U;  • Szyny umożliwiające wysunięcie serwera z szafy stelażowej;  • Opcjonalne ramię porządkujące ułożenie przewodów z tyłu serwera; | TAK |  |
| **PŁYTA GŁÓWNA** | | | |
| **1.** | • Wyprodukowana i zaprojektowana przez producenta serwera  • Zainstalowany moduł TPM 2.0  • Wsparcie dla technologii:  o Advanced ECC | TAK |  |
| **Procesory** | | | |
| **1.** | • jeden procesor 8-rdzeniowy Taktowanie minimum 2,2 GHz  • architektura x86\_64 | TAK |  |
| **Pamięć RAM** | | | |
| **1.** | • min 32 GB pamięci RAM  • DDR4 Registered  • | TAK |  |
| **Dyski twarde i napędy** | | | |
| **1.** | • Minimum 8 wnęk dla dysków twardych Hotplug 3,5”;  • Zainstalowane 4 dyski SATA 4TB; | TAK |  |
| **Kontrolery LAN** | | | |
| **1.** | • Karta LAN 2x 10Gbit SFP; możliwość wymiany zainstalowanych interfejsów LAN na interfejsy 2x 10Gbit Base- T bez potrzeby wymiany całego układu lub instalacji dodatkowych kart w slotach PCI Express  2 moduły SFP+ Multi Mode Fiber 10GbE LC | TAK |  |
| **Kontrolery I/O** | | | |
| **1.** | • Zainstalowany moduł HSM PCIe.  • Zainstalowany kontroler RAID dla wewnętrznych dysków twardych posiadający 2GB pamięci z modułem potrzymania pamięci/nieulotną pamięcią, obsługujący poziomy RAID: 0,1,10,5,50,6,60  • Zainstalowana karta dwuportowa FC 16Gb; | TAK |  |
| **Porty** | | | |
| **1.** | • Zintegrowana karta graficzna ze złączami VGA z tyłu oraz przodu serwera;  • Minimum 1 port USB 3.0 na panelu przednim;  • Min 2 porty USB 3.0 dostępne z tyłu serwera;  • Możliwość instalacji jednego portu serial, możliwość wykorzystania portu do zarządzania serwerem;  • Ilość dostępnych złącz USB nie może być osiągnięta poprzez stosowanie zewnętrznych przejściówek, rozgałęziaczy czy dodatkowych kart rozszerzeń zajmujących jakikolwiek slot PCI Express i/lub USB serwera; | TAK\* |  |
| **Zasilanie, chłodzenie** | | | |
| **1.** | • Redundantne zasilacze hotplug o mocy minimalnej 400W o sprawności minimum 94%; | TAK |  |
| **Zarządzanie** | | | |
| **1.** | • Wbudowane diody informacyjne lub wyświetlacz informujące o stanie serwera - system przewidywania, rozpoznawania awarii)  Zintegrowany z płytą główną serwera kontroler sprzętowy zdalnego zarządzania zgodny z IPMI 2.0 o funkcjonalnościach:  • Niezależny od systemu operacyjnego, sprzętowy kontroler umożliwiający pełne zarządzanie, zdalny restart serwera;  o Dedykowana karta LAN 1 Gb/s, dedykowane złącze RJ-45 do komunikacji wyłącznie z kontrolerem zdalnego zarządzania z możliwością przeniesienia tej komunikacji na inną kartę sieciową współdzieloną z systemem operacyjnym;  o Dostęp poprzez przeglądarkę Web, SSH;  o Zarządzanie mocą i jej zużyciem oraz monitoring zużycia energii;  o Zarządzanie alarmami (zdarzenia poprzez SNMP)  o Możliwość przejęcia konsoli tekstowej  o Możliwość zarządzania przez 6 administratorów jednocześnie  o Przekierowanie konsoli graficznej na poziomie sprzętowym oraz możliwość montowania zdalnych napędów i ich obrazów na poziomie sprzętowym (cyfrowy KVM)  o Obsługa serwerów proxy (autentykacja)  o Obsługa VLAN  o Możliwość konfiguracji parametru Max. Transmission Unit (MTU)  o Wsparcie dla protokołu SSDP  o Obsługa protokołów TLS 1.0, TLS 1.1, TLS 1.2, SSL v3  o Obsługa protokołu LDAP  o Synchronizacja czasu poprzez protokół NTP  o Możliwość backupu i odtworzenia ustawień bios serwera oraz ustawień karty zarządzającej  • Serwer posiada możliwość konfiguracji i wykonania aktualizacji BIOS, Firmware, sterowników serwera bezpośrednio z GUI (graficzny interfejs) . | TAK\* |  |
| **Wspierane OS** | | | |
| **1.** | • Microsoft Windows Server 2019, 2016  • VMWare vSphere 6.7  • Suse Linux Enterprise Server 12  • Red Hat Enterprise Linux 7, 8  • Hyper-V Server | TAK\* |  |
| **System operacyjny** | | | |
| **1.** | Licencja na serwerowy system operacyjny musi uprawniać do uruchamiania dwóch wirtualnych środowisk serwerowego systemu operacyjnego na jednym serwerze fizycznym.  Serwerowy system operacyjny musi posiadać następujące, wbudowane cechy.  1. Możliwość wykorzystania 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym.  2. Możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności do 64TB przez każdy wirtualny serwerowy system operacyjny.  3. Możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania 7000 maszyn wirtualnych.  4. Możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci.  5. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy.  6. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy.  7. Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.  8. Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading.  9. Wbudowane wsparcie instalacji i pracy na wolumenach, które:  a. pozwalają na zmianę rozmiaru w czasie pracy systemu,  b. umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,  c. umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów,  d. umożliwiają zdefiniowanie list kontroli dostępu (ACL).  10. Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.  11. Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.  12. Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET  13. Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.  14. Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.  15. Dostępne dwa rodzaje graficznego interfejsu użytkownika:  a. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,  b. Dotykowy umożliwiający sterowanie dotykiem na monitorach dotykowych.  16. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe,  17. Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji.  18. Mechanizmy logowania w oparciu o:  a. Login i hasło,  b. Karty z certyfikatami (smartcard),  c. Wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM),  19. Możliwość wymuszania wieloelementowej dynamicznej kontroli dostępu dla: określonych grup użytkowników, zastosowanej klasyfikacji danych, centralnych polityk dostępu w sieci, centralnych polityk audytowych oraz narzuconych dla grup użytkowników praw do wykorzystywania szyfrowanych danych..  20. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).  21. Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.  22. Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa.  23. Pochodzący od producenta systemu serwis zarządzania polityką dostępu do informacji w dokumentach (Digital Rights Management).  24. Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach.  25. Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:  a. Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC,  b. Usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji:  i. Podłączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną,  ii. Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,  iii. Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza.  iv. Bezpieczny mechanizm dołączania do domeny uprawnionych użytkowników prywatnych urządzeń mobilnych opartych o iOS i Windows 8.1.  c. Zdalna dystrybucja oprogramowania na stacje robocze.  d. Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej  e. Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:  i. Dystrybucję certyfikatów poprzez http  ii. Konsolidację CA dla wielu lasów domeny,  iii. Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen,  iv. Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509.  f. Szyfrowanie plików i folderów.  g. Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec).  h. Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów.  i. Serwis udostępniania stron WWW.  j. Wsparcie dla protokołu IP w wersji 6 (IPv6),  k. Wsparcie dla algorytmów Suite B (RFC 4869),  l. Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows,  m. Wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie do 1000 aktywnych środowisk wirtualnych systemów operacyjnych. Wirtualne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności. Mechanizmy wirtualizacji mają zapewnić wsparcie dla:  i. Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych,  ii. Obsługi ramek typu jumbo frames dla maszyn wirtualnych.  iii. Obsługi 4-KB sektorów dysków  iv. Nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra  v. Możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API.  vi. Możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk mode)  26. Możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta serwerowego systemu operacyjnego umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet.  27. Wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath).  28. Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego.  29. Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.  30. Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF.  31. Nośnik i klucz produktu pochodzący od producenta sprzętu | TAK\* |  |
| **Gwarancja** | | | |
| **1.** | Gwarancja 5 Lat  Gwarantowany czas reakcji do następnego dnia roboczego od przyjęcia zgłoszenia .  Zgłaszanie usterek i awarii w trybie 24/7 | TAK\* |  |
| **Dokumentacja, inne** | | | |
| **1.** | • Serwer musi być fabrycznie nowy i pochodzić z oficjalnego kanału dystrybucyjnego w UE. Nie dopuszcza się użycia serwerów odnawianych, demonstracyjnych lub powystawowych.  • Ogólnopolska, telefoniczna infolinia/linia techniczna producenta serwera  • Możliwość aktualizacji i pobrania sterowników do oferowanego modelu serwera w najnowszych certyfikowanych wersjach bezpośrednio z sieci Internet za pośrednictwem strony www producenta serwera; | TAK\* |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **4. Serwer bazodanowy- 2 szt.** | | | |
| **Lp.** | **Wymagane minimalne parametry techniczne** | **Wymóg do spełnienia (warunek graniczny)** | **OFEROWANE PARAMETRY TECHNICZNE - podaje**  **Wykonawca**  **Wymogi dotyczące opisu oferowanych parametrów:**  TAK – wykonawca spełnia konkretny parametr przy czym Zamawiający oczekuje by w przypadku wymagań dotyczących minimalnych parametrów opisać szczegółowo parametry oferowane przez wykonawcę  NIE – wykonawca nie spełnia konkretnego parametru |
| **OBUDOWA** | | | |
| **1.** | • Typu RACK, wysokość nie więcej niż 2U;  • Szyny umożliwiające wysunięcie serwera z szafy stelażowej;  • Opcjonalne ramię porządkujące ułożenie przewodów z tyłu serwera; | TAK |  |
| **PŁYTA GŁÓWNA** | | | |
| **1.** | • Wyprodukowana i zaprojektowana przez producenta serwera  • Zainstalowany moduł TPM 2.0  • Wsparcie dla technologii:  o Advanced ECC | TAK |  |
| **Procesory** | | | |
| **1.** | • Jeden procesor 8-rdzeniowe (nie dopuszcza się większej ilości rdzeni fizycznych) o częstotliwości minimum 3,0 GHz  • architektura x86\_64 | TAK |  |
| **Pamięć RAM** | | | |
| **1.** | • min. 64 GB pamięci RAM  • DDR4 Registered  • | TAK |  |
| **Dyski twarde i napędy** | | | |
| **1.** | • Minimum 4 wnęki dla dysków twardych Hotplug 2,5” lub 3,5”;  • Zainstalowane 2 dyski SSD Hot-Plug o pojemności min 120GB i parametrze DWPD>=3 | TAK |  |
| **Kontrolery LAN** | | | |
| **1.** | - Karta LAN 2x 10Gbit SFP+; możliwość wymiany zainstalowanych interfejsów LAN na interfejsy 2x 10Gbit Base- T bez potrzeby wymiany całego układu lub instalacji dodatkowych kart w slotach PCI Express  2 moduły SFP+ Multi Mode Fiber 10GbE LC | TAK |  |
| **Kontrolery I/O** | | | |
| **1.** | • Zainstalowane jedna karta dwuportowa FC 16Gb; | TAK |  |
| **Porty** | | | |
| **1.** | • Zintegrowana karta graficzna ze złączami VGA z tyłu oraz przodu serwera;  • Min 1 port USB 3.0 na panelu przednim;  • Min 2 porty USB 3.0 dostępne z tyłu serwera;  • Możliwość instalacji jednego portu serial, możliwość wykorzystania portu do zarządzania serwerem;  • Ilość dostępnych złącz USB nie może być osiągnięta poprzez stosowanie zewnętrznych przejściówek, rozgałęziaczy czy dodatkowych kart rozszerzeń zajmujących jakikolwiek slot PCI Express i/lub USB serwera;; | TAK\* |  |
| **Zasilanie, chłodzenie** | | | |
| **1.** | • Redundantne zasilacze hotplug o mocy minimalnej 400W o sprawności minimum 94%; | TAK |  |
| **Zarządzanie** | | | |
| **1.** | • Wbudowane diody informacyjne lub wyświetlacz informujące o stanie serwera - system przewidywania, rozpoznawania awarii)  Zintegrowany z płytą główną serwera kontroler sprzętowy zdalnego zarządzania zgodny z IPMI 2.0 o funkcjonalnościach:  • Niezależny od systemu operacyjnego, sprzętowy kontroler umożliwiający pełne zarządzanie, zdalny restart serwera;  o Dedykowana karta LAN 1 Gb/s, dedykowane złącze RJ-45 do komunikacji wyłącznie z kontrolerem zdalnego zarządzania z możliwością przeniesienia tej komunikacji na inną kartę sieciową współdzieloną z systemem operacyjnym;  o Dostęp poprzez przeglądarkę Web, SSH;  o Zarządzanie mocą i jej zużyciem oraz monitoring zużycia energii;  o Zarządzanie alarmami (zdarzenia poprzez SNMP)  o Możliwość przejęcia konsoli tekstowej  o Możliwość zarządzania przez 6 administratorów jednocześnie  o Przekierowanie konsoli graficznej na poziomie sprzętowym oraz możliwość montowania zdalnych napędów i ich obrazów na poziomie sprzętowym (cyfrowy KVM)  o Obsługa serwerów proxy (autentykacja)  o Obsługa VLAN  o Możliwość konfiguracji parametru Max. Transmission Unit (MTU)  o Wsparcie dla protokołu SSDP  o Obsługa protokołów TLS 1.0, TLS 1.1, TLS 1.2, SSL v3  o Obsługa protokołu LDAP  o Synchronizacja czasu poprzez protokół NTP  o Możliwość backupu i odtworzenia ustawień bios serwera oraz ustawień karty zarządzającej  • Serwer posiada możliwość konfiguracji i wykonania aktualizacji BIOS, Firmware, sterowników serwera bezpośrednio z GUI (graficzny interfejs) . | TAK\* |  |
| **Wspierane OS** | | | |
| **1.** | • Microsoft Windows Server 2019, 2016  • VMWare vSphere 6.7  • Suse Linux Enterprise Server 12  • Red Hat Enterprise Linux 7, 8  • Hyper-V Server | TAK\* |  |
| **System operacyjny** | | | |
| **1.** | System Operacyjny dedykowany do bazy danych systemu his. | TAK\* |  |
| **Gwarancja** | | | |
| **1.** | Gwarancja 5 Lat  Gwarantowany czas reakcji do następnego dnia roboczego od przyjęcia zgłoszenia .  Zgłaszanie usterek i awarii w trybie 24/7 | TAK\* |  |
| **Dokumentacja, inne** | | | |
| **1.** | • Serwer musi być fabrycznie nowy i pochodzić z oficjalnego kanału dystrybucyjnego w UE. Nie dopuszcza się użycia serwerów odnawianych, demonstracyjnych lub powystawowych.  • Ogólnopolska, telefoniczna infolinia/linia techniczna producenta serwera  • Możliwość aktualizacji i pobrania sterowników do oferowanego modelu serwera w najnowszych certyfikowanych wersjach bezpośrednio z sieci Internet za pośrednictwem strony www producenta serwera; | TAK\* |  |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **5. Macierz dyskowa- 2 szt.** | | | | | | | |
| **Lp.** | | **Wymagane minimalne parametry techniczne** | | **Wymóg do spełnienia (warunek graniczny)** | | **OFEROWANE PARAMETRY TECHNICZNE - podaje**  **Wykonawca**  **Wymogi dotyczące opisu oferowanych parametrów:**  TAK – wykonawca spełnia konkretny parametr przy czym Zamawiający oczekuje by w przypadku wymagań dotyczących minimalnych parametrów opisać szczegółowo parametry oferowane przez wykonawcę  NIE – wykonawca nie spełnia konkretnego parametru | |
| **OGÓLNE** | | | | | | | |
| **1.** | | System musi być dostarczony ze wszystkimi komponentami do instalacji w standardowej szafie rack 19” z zajętością maks. 2U w tej szafie. Każdy skonfigurowany moduł/obudowa musi posiadać układ nadmiarowy zasilania i chłodzenia, zapewniający bezprzerwową pracę macierzy bez ograniczeń czasowych w przypadku utraty redundancji w danym układzie (zasilania lub chłodzenia). Każdy moduł/obudowa powinien posiadać widoczne elementy sygnalizacyjne do informowania o stanie poprawnej pracy lub awarii. Rozbudowa o dodatkowe moduły dla obsługiwanych dysków powinna odbywać się wyłącznie poprzez zakup takich modułów, bez konieczności zakupu dodatkowych licencji lub specjalnego oprogramowania aktywującego proces rozbudowy lub musi być dostarczona licencja na dwukrotność dostarczanej pojemności. Dostarczana macierz musi umożliwiać podłączenie półek kaskadowo , bądź w formie 2 łańcuchów. Oferowana macierz musi obsługiwać min. 260 dysków wykonanych w technologii hot-plug. Macierz musi umożliwiać rozbudowę i jednoczesne podłączenie i używanie modułów (tzw. „półek dyskowych”) w rozmiarze 2U pozwalająca umieścić do 24 dysków 2,5” typu hotplug dla dysków NL-SAS SAS i SSD oraz w rozmiarze 2U dla 12 dysków 3,5” typu hotplug SAS, NL-SAS oraz do 6U dla min 60 dysków; Wymaga się aby macierz umożliwiała jednoczesne podłączenie i użycie dowolnego rodzaju i kombinacji wyżej wymienionych półek dyskowych Macierz musi posiadać funkcje automatycznego tieringu | | TAK\* | |  | |
| **POJEMNOŚĆ DOSTARCZONEJ MACIERZY** | | | | | | | |
| **1.** | | * przestrzeń minimum 4,5 TB realizowana na dyskach SSD : * min 2 dyski SSD-SAS 12G o pojemności min. 400GB DWPD3 * min 2 dyski SSD-SAS 12G o pojemności min. 3,8TB DWPD1 * przestrzeń minimum 15,5 TB realizowana na dyskach NL : * min 8 dysków NL SAS 12G o pojemności minimum 4TB lub min 16 dysków NL SAS 12G o pojemności minimum 2TB | | TAK | |  | |
| **KONTROLERY** | | | | | | | |
| **1.** | | • Kontrolery macierzy muszą obsługiwać tryb pracy w układzie min active-active, macierz musi być dostarczona z zainstalowanymi minimum 2 kontrolerami;  • Każdy z kontrolerów macierzy musi posiadać po minimum 32 GB pamięci podręcznej Cache – kontrolery muszą obsługiwać między sobą mechanizm lustrzanej kopii danych (cache mirror) przeznaczonych do zapisu;  • W przypadku awarii zasilania dane nie zapisane na dyski, przechowywane w pamięci podręcznej Cache dla zapisów muszą być zabezpieczone metodą trwałego zapisu na dysk.  • Kontrolery muszą posiadać możliwość ich wymiany bez konieczności wyłączania zasilania całego urządzenia;  • Kontrolery macierzy obsługują funkcjonalność kompresji danych.  • Kontrolery macierzy obsługują funkcjonalność deduplikacji w trybie in-line.  • Macierz musi obsługiwać wymianę kontrolera RAID bez utraty danych zapisanych na dyskach.  • Każdy z kontrolerów RAID powinien posiadać dedykowany minimum 2 interfejsy RJ-45 Ethernet obsługujący połączenia z prędkością minimum 1Gb/s dla zdalnej komunikacji z oprogramowaniem zarządzającym i konfiguracyjnym macierzy.  • Kontrolery macierzy muszą być oparte o procesor wykonany w technologii wielordzeniowej z minimum 4 rdzeniami,  • Kontrolery macierzy muszą obsługiwać min 120 grup dyskowych w całym rozwiązaniu, bez konieczności wymiany dostarczonych kontrolerów  • Oferowana macierz musi mieć wyprowadzone 4 porty FC 16Gb/s do dołączenia serwerów bezpośrednio lub do dołączenia do sieci SAN, na każdy kontroler RAID.  • Macierz musi umożliwiać stosowanie (rozbudowa/wymiana) portów do transmisji danych:  FC 16Gb/s, iSCSI min 10Gb/s  • Stosowanie wyżej wymienionych portów nie może powodować wymiany samych kontrolerów RAID w oferowanym rozwiązaniu a w przypadku konieczność licencjonowania tej funkcjonalności macierz ma być dostarczona z aktywną licencja na instalację i obsługę każdego z wymienionych protokołów transmisji danych | | TAK\* | |  | |
| **Poziomy RAID** | | | | | | | |
| **1.** | | Macierz musi zapewniać poziom zabezpieczenia danych na dyskach definiowany poziomami RAID:  o Raid-0  o Raid-1  o Raid-10 lub Raid-50  o Raid-5  o Raid-6 | | TAK | |  | |
| **Dyski** | | | | | | | |
| **1.** | | Oferowana macierz musi wspierać dyski hot-plug:  o dyski elektroniczne SSD i mechaniczne HDD z interfejsami SAS12Gb/s  o dyski mechaniczne HDD o prędkości obrotowej min 7,2 krpm, 10 krpm .  • Macierz musi obsługiwać mieszaną konfigurację dysków hot-plug SSD i HDD w rozmiarach 2,5” i 3,5” zainstalowanych w dowolnym module rozwiązania;  • Wszystkie dyski wspierane przez oferowany model macierzy muszą być wykonane w technologii hot-plug i posiadać podwójne porty SAS obsługujące tryb pracy full-duplex  • Macierz musi obsługiwać min. 260 dysków SAS SSD w całym rozwiązaniu, bez konieczności dokupowania/wymiany żadnych innych elementów sprzętowych czy licencyjnych innych niż same półki dyskowe wraz z dyskami;  • Możliwość rozbudowy oferowanego modelu macierzy do minimum 500 dysków bez migracji i przenoszenia danych - jedynie poprzez wymianę modułu kontrolerów macierzy (bez konieczności wymiany posiadanych dysków, półek dyskowych, bez konieczności przenoszenia danych/ istniejącej struktury grup dyskowych/LUN, jak również z zachowaniem istniejącej gwarancji producenta na półki dyskowe i dyski;  • Macierz musi umożliwiać skonfigurowanie dysku hot-spare (dysk zapasowy)  • Macierz musi pozwalać na zaszyfrowanie danych zapisanych na wszystkich obsługiwanych dyskach SSD-SAS i HDD-SAS/NL-SAS minimum kluczem AES256-bit – jeżeli w tym celu niezbędne jest zakupienie dodatkowych licencji bądź komponentów sprzętowych to należy je dostarczyć wraz z macierzą. | | TAK | |  | |
| **Opcje programowe** | | | | | | | |
| **1.** | | • Macierz musi być wyposażona w system kopii migawkowych umożliwiających wykonanie minimum 2048 kopii migawkowych  • Macierz musi umożliwiać zdefiniowanie min. 8000 woluminów (LUN)  • Macierz powinna umożliwiać podłączenie logiczne z serwerami i stacjami poprzez min. 1024 ścieżek logicznych FC  • Macierz musi umożliwiać aktualizację oprogramowania wewnętrznego kontrolerów RAID i dysków bez konieczności wyłączania macierzy oraz bez konieczności wyłączania ścieżek logicznych FC/iSCSI dla podłączonych stacji/serwerów  • Macierz musi umożliwiać dokonywanie w trybie on-line (tj. bez wyłączania zasilania i bez przerywania przetwarzania danych w macierzy) operacje: powiększanie grup dyskowych, zwiększanie rozmiaru woluminu, migrowanie woluminu na inną grupę dyskową  • Macierz musi posiadać wsparcie dla systemów operacyjnych : Microsoft Windows Server 2012R2, 2016, 2019, SuSE Linux Enterprise Server, Red Hat Linux Enterprise Server, HP-UNIX, IBM AIX, SUN Solaris, Vmware Vsphere;  • Macierz musi być dostarczona z licencją na oprogramowanie wspierające technologię typu multipath (obsługa nadmiarowości dla ścieżek transmisji danych pomiędzy macierzą i serwerem) dla połączeń FC i iSCSI.  • Macierz musi posiadać możliwość uruchamiania mechanizmów zdalnej replikacji danych, w trybie synchronicznym i asynchronicznym, po protokołach FC lub IP lub iSCSI, bez konieczności stosowania zewnętrznych urządzeń konwersji wymienionych protokołów transmisji. Funkcjonalność replikacji danych musi być zapewniona z poziomu oprogramowania wewnętrznego macierzy. Replikacja danych musi być obsługiwana w połączeniu z każdą macierzą z tej samej rodziny urządzeń wspierającą obsługę zdalnej replikacji danych.  • Macierz musi posiadać możliwość tworzenia lokalnych tj. w obrębie zasobów macierzy, pełnych kopii danych (tzw. klony danych), kopii przyrostowych oraz kopii lustrzanych (mirror) – nie jest wymagane dostarczenie tej funkcjonalności – opcja rozbudowy  • Macierz musi obsługiwać mechanizm ochrony priorytetów obsługi wybranych zasobów – za taki mechanizm uznaje się funkcję typu ‘cache partitioning’ lub ‘storage partitioning’.  • Macierz musi obsługiwać adresację IP v.4 i IP v.6  • Macierz musi wspierać obsługę mechanizmów Vmware  • Macierz musi obsługiwać mechanizmy Thin Provisioning, czyli przydziału dla obsługiwanych środowisk woluminów logicznych o sumarycznej pojemności większej od sumy pojemności dysków fizycznych zainstalowanych w macierzy.  • Macierz musi obsługiwać mechanizmy typu AST (Automated Storage Tiering) tj. automatycznego migrowania i realokacji bloków danych pomiędzy różnymi technologiami dyskowymi na podstawie analizy częstotliwości operacji I/O dla tych bloków oraz wg potrzeb wydajnościowych serwerów, środowisk i aplikacji korzystających z zasobów macierzy. Mechanizm AST musi być obsługiwany przy korzystaniu zarówno z trzech jak z dwóch dostarczonych technologii dyskowych: SSD, SSAS, NLSAS.  • Macierz musi wspierać usługi VSS (Volume ShadowCopy Services) w systemach klasy Microsoft Windows Sever – wymagane jest dostarczenie niezbędnego oprogramowania / sterowników VSS pozwalających na obsługę VSS przy maksymalnej pojemności i liczbie dysków obsługiwanych przez oferowaną. W czasie trwania gwarancji wymaga się bezpłatnego dostępu do nowych wersji oprogramowania i sterowników  • Macierz musi obsługiwać mechanizmy migracji danych w trybie online z innej macierzy .  • Macierz wspiera rozwiązania klasy ‘klastra macierzowego’ tj. zapewnienia wysokiej dostępności zasobów dyskowych macierzy dla podłączonych platform software’owych i sprzętowych z wykorzystaniem synchronicznej replikacji danych pomiędzy minimum 2 macierzami protokołami FC. Mechanizm klastra macierzowego musi być obsługiwany dla protokołów FC, zarówno w zakresie replikacji danych jak i w zakresie sposobu podłączenia serwerów do zasobów macierzy. Pod użytym pojęciem ‘wysoka dostępność zasobów dyskowych’ należy rozumieć zapewnienie bezprzerwowego działania środowiska (aplikacja/ system operacyjny/ serwer) podłączonego do macierzy (macierz podstawowa) w przypadku wystąpienia awarii logicznego połączenia z tą macierzy bądź awarii samej macierzy, powodujących dla danego środowiska brak dostępu do zasobów macierzy podstawowej. Funkcjonalność ‘klastra macierzowego’ musi pozwalać na automatyczne i ręczne przełączanie obsługi środowisk produkcyjnych z macierzy podstawowej na zapasową w przypadku awarii macierzy podstawowej (tzw. Automated/manual failover). – nie jest wymagane dostarczenie tej funkcjonalności – opcja rozbudowy | | TAK | |  | |
| **Zarządzanie** | | | | | | | |
| **1.** | | • Oprogramowanie do zarządzania musi być zintegrowane z systemem operacyjnym systemu pamięci masowej  • Komunikacja z wbudowanym oprogramowaniem zarządzającym macierzą musi być możliwa w trybie graficznym np. poprzez przeglądarkę WWW oraz w trybie tekstowym.  • Musi być możliwe zdalne zarządzanie macierzą z wykorzystaniem standardowej przeglądarki internetowej (np. Internet Explorer, Google Chrome, Mozilla Firefox) bez konieczności instalacji żadnych dodatkowych aplikacji na stacji administratora  • Wbudowane oprogramowanie macierzy musi obsługiwać połączenia z modułem zarządzania macierzy poprzez szyfrowanie komunikacji protokołami: SSL dla komunikacji poprzez przeglądarkę WWW i protokołem SSH dla komunikacji poprzez CLI | | TAK\* | |  | |
| **Gwarancja i serwis** | | | | | | | |
| **1.** | | Gwarancja 5 Lat  • Macierz musi pochodzić z oficjalnego kanału sprzedaży producenta w UE. Nie dopuszcza się użycia macierzy odnawianych, demonstracyjnych lub powystawowych  • Producent oferowanej macierzy musi posiadać dedykowaną, ogólnie dostępną stronę internetową. | | TAK\* | |  | |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **6. Przełącznik rdzeniowy- 2 szt.** | | | | | | | |
| **Lp.** | | **Wymagane minimalne parametry techniczne** | | **Wymóg do spełnienia (warunek graniczny)** | | **OFEROWANE PARAMETRY TECHNICZNE - podaje**  **Wykonawca**  **Wymogi dotyczące opisu oferowanych parametrów:**  TAK – wykonawca spełnia konkretny parametr przy czym Zamawiający oczekuje by w przypadku wymagań dotyczących minimalnych parametrów opisać szczegółowo parametry oferowane przez wykonawcę  NIE – wykonawca nie spełnia konkretnego parametru | |
| **OBUDOWA** | | | | | | | |
| **1.** | | Wysokość przełącznika 1U w systemie montażu w szafie typu Rack 19” | | TAK | |  | |
| **2.** | | Głębokość: do montażu w szafie rack z kompletem odpowiednich szyn. | | TAK | |  | |
| **PORTY** | | | | | | | |
| **1.** | | - min. 24 portów SFP+ 10GE oraz wkładki niezbędne do podłączenia dostarczonych serwerów oraz switchy  - min. 2 porty 40GbE (QSFP+) - dodatkowy moduł  - 1 x RJ-45 lub USB : port konsolowy  - 1 x RJ-45 management port ( out of the band )  - 1 x USB  - redundantne wentylatory | | TAK | |  | |
| **Wydajność** | | | | | | | |
| **1.** | | Obsługa minimum 4000 wirtualnych sieci  Stakowalny do minimum 10 urządzeń w stosie portami 40GbE lub 10GbE (min 160Gbps)  Forwarding Rate minimum 470 Mpps  Switching fabric minimum 640 Gbps  Rozmiar tablicy routingu minimum: 8 000 wpisów IPv4, 4 000 wpisów IPv6  Pamięć MAC adresów minimum 130 000  ACL – minimum 100 list, minimum 1000 reguł na ACL, minimum 3000 reguł na wszystkie ACL  Bufor pamięci dla pakietów minimum 9 MB  Pamięć procesora minimum 2 GB | | TAK | |  | |
| **Funkcjonalność** | | | | | | | |
| **1.** | | Przełącznik musi wspierać funkcjonalność wirtualnej agregacji portów umożliwiającą:  - terminowanie pojedynczej wiązki EtherChannel/LACP wyprowadzonej z  urządzenia zewnętrznego (serwera, przełącznika) na 2 niezależnych  opisywanych urządzeniach  - budowę topologii sieci bez pętli z pełnym wykorzystaniem agregowanych  łączy  - umożliwiać wysokodostępny mechanizm kontroli dla 2 niezależnych  opisywanych urządzeń  Możliwość obsługi modułów QSFP+ 40GE-SR4  Możliwość obsługi kabli DAC 40GbE i 10GbE (Direct Attached Cable) minimalna długości: 0,5 - 7 m  Możliwość obsługi kabli rozszywających DAC (Direct Attached Cable) 1 x 40GbE na 4 x 10GbE min długości: min. 0,5 - 7 m  Musi posiadać redundantne minimum 2 zasilacze AC  Redundantne wiatraki  Chłodzenie przełącznika od portów Eth w kierunku zasilaczy (od przodu do tyłu urządzenia)   * Wsparcie dla agregacji LACP (802.3ad) - minimum 128 grup do 8 portów na grupę | | TAK\* | |  | |
| **Zgodność z protokołami** | | | | | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **1.** | Zgodność z:   * IEEE 802.1D Spanning Tree, GARP i GVRP * IEEE 802.1p Traffic Prioritization * IEEE 802.1Q VLAN Trunking * IEEE 802.1w Rapid Spanning Tree Protocol * IEEE 802.1S Multiple Spanning Tree Protocol * IEEE 802.1t IEEE802.1D maintenance * IEEE 802.1v VLAN Classification by Protocol & Port * IEEE 802.1x Port Based Network Access Control * IEEE 802.3ac Frame extension for VLAN tags * IEEE 802.3x Flow Control * IEEE 802.3I * IEEE 802.1v VLAN Classification by Protocol & Port   IEEE 802.1ab LLDP  Obsługa routingu, minimum:  - RIP v1/2;  - OSPF v1/2/3  - VRRP  - Policy Based Routing  - Graceful Restart  - BGP  Obsługa multicastu, minimum:  - IGMP v1/2/3;  - IGMP Snooping Querier  - MLDv2  - PIM-DM  - PIM-SM  - DHCP  - IGMP Proxy | TAK |  |
| **Zarządzanie** | | | |
| **1.** | Połączenie szyfrowane: SSL/SSH,  Autentykacja dostępu do przełącznika w oparciu o Radius lub TACACS+  Listy dostępu (ACL) warstwy 2/3/4  Listy dostępu (ACL) konfigurowalne dla fizycznego portu, łącza zagregowanego LAG i VLAN  Obsługa RMON,  Obsługa SNMP v2 i v3,  Obsługa sFlow,  Możliwość przechowywania dwóch wersji oprogramowania na przełączniku,  Obsługa DHCP Server i Relay Agent,  Obsługa 802.1x w tym:  - MAC-based authentication  - MAC authentication bypass  - Guest VLAN  Zarządzenie przez CLI i przez przeglądarkę internetową,  Radius  Radius Accounting  RADIUS Tunnel Authentication  DHCP options oraz BOOTP vendor extensions  Dynamic Host Configuration Protocol (DHCP) klient  Bootstrap Protocol  DNS Client  Form-based File Upload in HTML  Simple Network Time Protocol (SNTP)  Wsparcie dla IPv6  TLS protocol, version 1.0  PPP Extensible Authentication Protocol, EAP  Hypertext Transfer Protocol -- HTTP/1.1  BSD Syslog Protocol  Port mirroring  Wsparcie dla ramek typu Jumbo 9,000 bajtów  Broadcast storm control  Możliwość wgrywania oprogramowania przez USB  Trivial File Transfer Protocol (TFTP) Rev. 2  Honorowanie wartości 802.1p oraz IP DSCP  Wsparcie kolejkowania Strict priority oraz algorytmu weighted round robin (WRR)  wsparcie dla VLAN ID w ilości 4096  Private VLAN  Guest VLAN  Locked Port | TAK |  |
| **Pozostałe** | | | |
| **1.** | Przełącznik musi posiadać deklaracja CE.  Przełącznik musi być zgodny ze standardem RoHS. | TAK\* |  |
| **Zasilanie** | | | |
| **1.** | - Zasilacze PSU (Power Supply Unit): 2 redundantne zasilacze,  hot-swappable, | TAK |  |
| **GWARANCJA** | | | |
| **1.** | Gwarancja 5 Lat | TAK\* |  |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **7. Przełącznik dystrybucyjny- 3 szt.** | | | | | | | |
| **Lp.** | | **Wymagane minimalne parametry techniczne** | | **Wymóg do spełnienia (warunek graniczny)** | | **OFEROWANE PARAMETRY TECHNICZNE - podaje**  **Wykonawca**  **Wymogi dotyczące opisu oferowanych parametrów:**  TAK – wykonawca spełnia konkretny parametr przy czym Zamawiający oczekuje by w przypadku wymagań dotyczących minimalnych parametrów opisać szczegółowo parametry oferowane przez wykonawcę  NIE – wykonawca nie spełnia konkretnego parametru | |
| **OBUDOWA** | | | | | | | |
| **1.** | | Wysokość przełącznika 1U w systemie montażu w szafie typu Rack 19” , wraz z kompletem do montażu | | TAK | |  | |
| **PORTY** | | | | | | | |
| **1.** | | - RJ-45 10/100/1000: min 24 szt PoE  - SFP+ Porty Uplink: min 4szt  1 port konsolowy mikro-USB .  1 port USB umożliwiający załadowanie konfiguracji dla przełącznika z pamięci flash USB | | TAK | |  | |
| **WYDAJNOŚĆ** | | | | | | | |
| **1.** | | Minimum 16000 adresów MAC  Switch fabric capacity minimum 128Gbps  Forwarding rate minimum 96Mpps  Pamięć flash minimum 1GB  Pamięć RAM minimum 1GB  Bufor pamięci dla pakietów minimum 2MB | | TAK | |  | |
| **FUNKCJONALNOŚĆ WARSTWY II** | | | | | | | |
| **1.** | | Obsługa minimum 512 wirtualnych sieci  Obsługa 64 grup LACP i 8 portów fizycznych per grupa  Możliwość połączenia w stos do 4 urządzeń tego samego typu  Wydajność połączenia pomiędzy przełącznikami w stosie minimum 40Gbps  Obsługa Multicast Snooping w wersji v1/v2/v3  Wsparcie dla agregacji LACP (802.3ad)  Zgodność ze standardami wyspecyfikowanymi poniżej:  802.1AB LLDP  802.1D Bridging, Spanning Tree  802.1p Ethernet Priority (User Provisioning and Mapping)  802.1Q VLAN Tagging, Double VLAN Tagging, GVRP  802.1S Multiple Spanning Tree (MSTP)  802.1v Protocol-based VLANs  802.1W Rapid Spanning Tree (RSTP) RSTP-Per VLAN  802.1X Network Access Control, Auto VLAN  802.2 Logical Link Control  802.3 10BASE-T  802.3ab Gigabit Ethernet (1000BASE-T)  802.3ac Frame Extensions for VLAN Tagging  802.3ad Link Aggregation with LACP  802.3ae 10 Gigabit Ethernet (10GBASE-X) | | TAK | |  | |
| **Obsługa PoE** | | | | | | | |
| **1.** | | Możliwość podłączenia urządzenia zgodnie ze standardem PoE/PoE+  Budżet mocy w wysokości nie mniejszej niż 190W dla urządzeń PoE | | TAK | |  | |
| **Bezpieczeństwo i zarządzanie** | | | | | | | |
| **1.** | | Obsługa 802.1x, Guest vlan i Mac Authentication Bypass  Obsługa mechanizmu Private VLAN  Obsługa technologii port mirroring oraz remote port mirroring  Obsługa list kontroli dostępu opartych o adresy MAC i IP  Obsługa minimum 100 list kontroli dostępu i 4000 reguł sumarycznie dla wszystkich list  Obsługa czasowych list kontroli dostępu  Obsługa minimum 8 kolejek QoS na port fizyczny  Obsługa protokołu sflow  Obsługa SNMP v1/2/3  Zarządzanie przez interfejs WWW  Obsługa Openflow 1.3  Obsługa skryptów Python  Możliwość konfiguracji makr uproszczających zarządzanie systemem  Zgodność ze standardami wyspecyfikowanymi poniżej:  • 1155 SMIv1  • 1157 SNMPv1  • 1212 Concise MIB Definitions  • 1213 MIB-II  • 1215 SNMP Traps  • 1286 Bridge MIB  • 1442 SMIv2  • 1451 Manager-to- Manager MIB  • 1492 TACACS+  • 1493 Managed Objects for Bridges MIB  • 1573 Evolution of Interfaces  • 1612 DNS Resolver MIB Extensions  • 1643 Ethernet-like MIB  • 1757 RMON MIB  • 1867 HTML/2.0 Forms with File Upload Extensions  • 1901 Community-based SNMPv2  • 1907 SNMPv2 MIB  • 1908 Coexistence Between SNMPv1/v2  • 2011 IP MIB  • 2012 TCP MIB  • 2013 UDP MIB  • 2068 HTTP/1.1  • 2096 IP Forwarding Table MIB  • 2233 Interfaces Group using SMIv2  • 2246 TLS v1  • 2271 SNMP Framework MIB  • 2295 Transport Content Negotiation  • 2296 Remote Variant Selection  • 2346 AES Ciphersuites for TLS  • 2576 Coexistence Between SNMPv1/v2/v3  • 2578 SMIv2  • 2579 Textual Conventions for SMIv2  • 2580 Conformance Statements  • for SMIv2  • 2613 RMON MIB  • 2618 RADIUS Authentication MIB  • 2620 RADIUS Accounting MIB  • 2665 Ethernet-like Interfaces MIB  • 2674 Extended Bridge MIB  • 2737 ENTITY MIB  • 2818 HTTP over TLS  • 2819 RMON MIB (groups 1, 2, 3, 9)  • 2863 Interfaces MIB  • 2865 RADIUS  • 2866 RADIUS Accounting  • 2868 RADIUS Attributes for Tunnel Prot.  • 2869 RADIUS Extensions  • 3410 Internet Standard Mgmt. Framework  • 3411 SNMP Management Framework  • 3412 Message Processing and Dispatching  • 3413 SNMP Applications  • 3414 User-based security model  • 3415 View-based control model  • 3416 SNMPv2  • 3418 SNMP MIB  • 3577 RMON MIB  • 3580 802.1X with RADIUS  • 3737 Registry of RMOM MIB  • 4086 Randomness Requirements  • 4113 UDP MIB  • 4251 SSHv2 Protocol  • 4252 SSHv2 Authentication  • 4253 SSHv2 Transport  • 4254 SSHv2 Connection Protocol  • 4419 SSHv2 Transport Layer Protocol  • 4521 LDAP Extensions  • 4716 SECSH Public Key File Format  • 6101 SSL | | TAK | |  | |
| **Warunki Pracy** | | | | | | | |
| **1.** | | Przełącznik zgodny ze standardem ONIE i umożliwiać instalacje systemów operacyjnych innych producentów, w celu uzyskania dodatkowych funkcjonalności | | TAK\* | |  | |
| **Pozostałe** | | | | | | | |
| **1.** | | Przełącznik musi posiadać deklaracja CE.  Przełącznik musi być zgodny ze standardem RoHS. | | TAK | |  | |
| **Kompatybilność elektromagnetyczna** | | | | | | | |
| **1.** | | Przełącznik z redudantnymi modułami wentylatorów | | TAK | |  | |
| **Zasilanie** | | | | | | | |
| **1.** | | - 100-240 VAC, 50/60Hz  - zintegrowany zasilacz o mocy co najmniej 250W | | TAK | |  | |
| **GWARANCJA** | | | | | | | |
| **1.** | | Gwarancja 5 Lat | | TAK | |  | |

|  |  |  |  |
| --- | --- | --- | --- |
| **8. Przełącznik portowy Switch FC- 2 szt.** | | | |
| **Lp.** | **Wymagane minimalne parametry techniczne** | **Wymóg do spełnienia (warunek graniczny)** | **OFEROWANE PARAMETRY TECHNICZNE - podaje**  **Wykonawca**  **Wymogi dotyczące opisu oferowanych parametrów:**  TAK – wykonawca spełnia konkretny parametr przy czym Zamawiający oczekuje by w przypadku wymagań dotyczących minimalnych parametrów opisać szczegółowo parametry oferowane przez wykonawcę  NIE – wykonawca nie spełnia konkretnego parametru |
| **OGÓLNE** | | | |
| **1.** | Wysokość przełącznika 1U w systemie montażu w szafie typu Rack 19” | TAK |  |
| **2.** | Ilość portów SFP: 24 szt. porty uniwersalne o maksymalnej przepustowości 32GB/s, z obsługą przepustowości 16Gbit/s, 8Gbit/s i 4Gbit/s z automatycznym wyborem przepustowości (auto-sensing),  obsługa trybu full-duple | TAK\* |  |
| **3.** | 12 aktywnych portów | TAK\* |  |
| **4.** | Zainstalowane moduły optyczne 12 szt. SFP 16Gbit/s, Short Wave Length (SWL), Multi Mode Fibre (MMF) | TAK\* |  |
| **5.** | Obsługa trybów pracy portów FC: D\_port, F\_port, E\_port, M-Port | TAK\* |  |
| **6.** | Obsługa funkcji POD (Ports on Demand) przydziału licencji dla aktywnych portów FC | TAK\* |  |
| **7.** | Możliwość aktualizacji firmware’u switcha | TAK\* |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **8.** | Aktywne funkcje: Webtools, Advanced Zoning, FullFabric (z obsługą do minimum 128 przełączników FC) | TAK\* |  |
| **9.** | Możliwość obsługi funkcjonalności (przez zakupienie odpowiednich licencji): Trunking, Extended Fabric, Fabric Vision | TAK\* |  |
| **10.** | Zarządzanie min.:   * RJ-45 min 10/100 Mb/s do zarządzania poprzez sieć Ethernet * RJ-45 lub DB9 do zarządzania poprzez interfejs RS232 * USB * In-band over FC | TAK\* |  |
| **11.** | Sygnalizacja aktywnych i podłączonych portów na panelu przednim urządzenia | TAK\* |  |
| **12.** | Zarządzanie poprzez przeglądarkę WWW z obsługą połączeń szyfrowanych 128-bit SSL oraz poprzez usługę SSH | TAK\* |  |
| **13.** | Wsparcie dla protokołu SNMP v.3 | TAK\* |  |
| **14.** | Gwarancja 5 Lat | TAK\* |  |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **9. Szafa RACK – 1 szt.** | | | | | | | |
| **Lp.** | **Wymagane minimalne parametry techniczne** | | | **Wymóg do spełnienia (warunek graniczny)** | | **OFEROWANE PARAMETRY TECHNICZNE - podaje**  **Wykonawca**  **Wymogi dotyczące opisu oferowanych parametrów:**  TAK – wykonawca spełnia konkretny parametr przy czym Zamawiający oczekuje by w przypadku wymagań dotyczących minimalnych parametrów opisać szczegółowo parametry oferowane przez wykonawcę  NIE – wykonawca nie spełnia konkretnego parametru | |
| **OGÓLNE** | | | | | | | |
| **1.** | 42U pojemności użytecznej do instalacji urządzeń w pozycji poziomej o wymiarach nie mniejszych niż 800mmx1000mm(Szer/gł) | | | TAK\* | |  | |
| **2.** | wyposażona w przednie drzwi perforowane, zamykane na zamek z kluczem, jednoskrzydłowe, możliwość montażu lewa/prawa strona, możliwość zdjęcia bez użycia narzędzi | | | TAK \* | |  | |
| **3.** | wyposażona w tylne drzwi perforowane, dwuskrzydłowe dla ograniczenia przestrzeni serwisowej, zamykane na zamek z kluczem wspólny z zamkiem przednim, możliwość zdjęcia bez użycia narzędzi | | | TAK \* | |  | |
| **4.** | Minimalna klasa ochrony na poziomie IP 20 | | | TAK \* | |  | |
| **5.** | wyposażona w zdejmowane panele boczne | | | TAK\* | |  | |
| **6.** | | | wszystkie wolne „U” zaślepione zaślepkami | TAK\* | |  | |
| **7.** | | | przystosowana do poprawnej instalacji dostarczonych serwerów rack wraz z ich fabrycznymi prowadnicami przewodów. | TAK\* | |  | |
| **8.** | | | zainstalowane 2 listwy zasilające min. 8 gniazd ,2 półki o głębokości min. 450mm | TAK\* | |  | |
| **9.** | | | Minimalny udźwig szafy co najmniej 900 kg | TAK \* | |  | |
| **10.** | | | Certyfikaty CE, RoHS | TAK\* | |  | |

|  |  |  |  |
| --- | --- | --- | --- |
| **10. Zasilacz awaryjny UPS – 2 szt.** | | | |
| **Lp.** | **Wymagane minimalne parametry techniczne** | **Wymóg do spełnienia (warunek graniczny)** | **OFEROWANE PARAMETRY TECHNICZNE - podaje**  **Wykonawca**  **Wymogi dotyczące opisu oferowanych parametrów:**  **TAK -** *wystarczy potwierdzić spełnianie wymogu wpisując: TAK* **TAK -** *należy spełnić wymóg oraz dokładnie opisać dany parametr oferowanego urządzenia*  **TAK/ NIE-** *należy podać czy wykonawca spełnia wymóg, czy nie*  *spełnia* |
| **OGÓLNE** | | | |
| **1.** | Typ zasilacza: online | TAK\* |  |
| **2.** | Możliwość montażu w szafie RACK przy zajętości maksymalnie 3U | TAK\* |  |
| **3.** | Moc pozorna 5kVA | TAK\* |  |
| **4.** | Moc rzeczywista 4,5 kW | TAK\* |  |
| **5.** | Minimalne podtrzymanie- 3 minuty przy 100% obciążeniu | TAK\* |  |
| **6.** | Minimalne podtrzymanie- 10 minuty przy 50% obciążeniu | TAK\* |  |
| **7.** | W standardzie minimum:  - min. 6x IEC 320 C13 (10A)  - min. 2x IEC 320 C19 (16A)  - 1x RJ45 | TAK\* |  |
| **8.** | Aplikacja do automatycznego zamykania wspieranych systemów operacyjnych w przypadku braku zasilania | TAK\* |  |
| **9.** | Możliwość wymiany akumulatorów podczas pracy | TAK\* |  |
| **10.** | Wspierane i certyfikowane systemy operacyjne: Microsoft® Windows Server® 2012 R2, SUSE Linux Enterprise Server, Red Hat Enterprise Linux, VMware Infrastructure | TAK\* |  |
| **11.** | Zarządzanie przez SNMP | TAK\* |  |
| **12.** | Automatyczny wewnętrzny bypass | TAK\* |  |
| **13.** | Możliwość dołączenia baterii wydłużających czas podtrzymania zasilania | TAK\* |  |
| **14.** | Wyświetlacz LCD na froncie urządzenia, umożliwiający zarządzanie i monitoring urządzenia | TAK\* |  |
| **15.** | Certyfikaty: CE, CB | TAK\* |  |
| **16.** | Gwarancja 5 Lat | TAK\*  . |  |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **11. Punkty dostępowe WiFi (30 szt. ) wraz z kontrolerem (1 szt. )** | | | | | | | |
| **Lp.** | | **Wymagane minimalne parametry techniczne** | | **Wymóg do spełnienia (warunek graniczny)** | | **OFEROWANE PARAMETRY TECHNICZNE - podaje**  **Wykonawca**  **Wymogi dotyczące opisu oferowanych parametrów:**  TAK – wykonawca spełnia konkretny parametr przy czym Zamawiający oczekuje by w przypadku wymagań dotyczących minimalnych parametrów opisać szczegółowo parametry oferowane przez wykonawcę  NIE – wykonawca nie spełnia konkretnego parametru | |
| **Antena** | | | | | | | |
| **1.** | | Typ: min. 6 x wbudowany PIFA (3 x 2,4 GHz i 3 x 5 GHz)  • Wzmocnienie: min. 3 dBi (2,4 GHz), min. 5 dBi (5 GHz) | | TAK | |  | |
| **Standardy** | | | | | | | |
| **1.** | | 802.11a / b / g / n / ac  • Jednoczesne dwuzakresowe 2,4 GHz i 5 GHz  Obsługiwane transmisje danych:  • 802.11b: 1, 2, 5,5, 11 Mb / s  • 802.11a / g: 6, 9, 12, 18, 24, 36, 48, 54 Mb / s  • 802.11n: 6,5 - 216,7 Mbps (20 MHz)  • 802.11n: 13,5 - 450 Mbps (40 MHz)  • 802.11ac: 6,5 - 260,1 Mbps (20 MHz)  • 802.11ac: 13,5 - 600 Mbps (40 MHz)  • 802.11ac: 29,3 - 1300 Mbps (80 MHz) | | TAK | |  | |
| **Moc wyjściowa** | | | | | | | |
| **1.** | | • 2,4 GHz: min 10 dBm  • 5 GHz: min 10 dBm | | TAK | |  | |
| **Kanalizacja** | | | | | | | |
| **1.** | | 20 MHz, 40 MHz, 80 MHz | | TAK | |  | |
| **Pasmo częstotliwości** | | | | | | | |
| **1.** | | 2,412 - 2,472 GHz, 5,180 - 5,825 GHz | | TAK | |  | |
| **Kanały operacyjne** | | | | | | | |
| **1.** | | • 2,4 GHz: 1-11 (USA), 1-13 (Europa), 1-13 (Japonia)  • 5 GHz : 36 - 165 (USA), 36 - 140 (Europa), 36 - 140 (Japonia)  ESSID: do 16 na radio (łącznie 32)  Certyfikaty: FCC (Stany Zjednoczone), CE (Europa), NCC (Tajwan) | | TAK | |  | |
| **Wydajność** | | | | | | | |
| **1.** | | Szybkość danych fizycznych:  • Do 450 Mbps (2,4 GHz)  • Do 1,3 Gb / s (5 GHz)  Równocześni użytkownicy: do 384 (256 dla 2,4 GHz, 128 dla 5 GHz) | | TAK | |  | |
| **Jakość usługi** | | | | | | | |
| **1.** | | Bezprzewodowa QoS (802.11e / WMM)  DSCP (802.1p)  Sterowanie pasmem  Konwersja multiemisji do emisji pojedynczej  Optymalne filtrowanie klientów | | TAK | |  | |
| **Zarządzanie** | | | | | | | |
| **1.** | | Rozlokowanie:  • Samodzielny  • Zarządzanie tunelowane przez kontrolera  • Kompatybilny z IPv4 i IPv6  Konfiguracja:  • Internetowy interfejs użytkownika (HTTP / HTTPS)  • SNMP v1, v2c, v3 | | TAK | |  | |
| **Bezpieczeństwo** | | | | | | | |
| **1.** | | Ochrona bezprzewodowa:  • WEP  • WPA / WPA2 Mixed  • WPA2-Personal  • WPA2-Enterprise (802.1X)  • Szyfrowanie TKIP i AES  Tagowanie VLAN (802.1Q)  Izolacja stacji  DHCP snooping  Zapora ogniowa warstwy 2 | | TAK | |  | |
| **Mobilność / roaming** | | | | | | | |
| **1.** | | Wstępne uwierzytelnianie 802.1X  Szybki roaming w warstwie 2 / warstwie 3 | | TAK | |  | |
| **Interfejsy** | | | | | | | |
| **1.** | | Uplink: 1 x 10/100 / 1000BASE-T Ethernet, Auto MDIX, RJ-45 z 802.3at PoE | | TAK | |  | |
| **Montowanie** | | | | | | | |
| **1.** | | Uchwyt ścienny (panel montażowy w zestawie)  • Montaż sufitowy (zestaw do montażu sufitowego w zestawie) | | TAK | |  | |
| **Moc** | | | | | | | |
| **1.** | | • Zasilanie DC: 12 V / 2,5 A (opcjonalny zasilacz)  • PoE: zgodny z 802.3at  • Pobór mocy: 17,0 W maks  . | | TAK | |  | |
| **Warunki środowiska** | | | | | | | |
| **1.** | | • Temperatura pracy: od -10 ° C (14 ° F) do 40 ° C (104 ° F)  • Wilgotność podczas pracy: 10% do 90% bez kondensacji  • Klasa UL94-5VB. | | TAK | |  | |
| **GWARANCJA** | | | | | | | |
| **1.** | | Gwarancja 5 Lat | | TAK | |  | |
| **Kontroler** | | | | | | | |
| **Obudowa i zasilanie** | | | | | | | |
| **1.** | | • 19” (1U) do montażu w szafie rack (dołączone elementy montażowe)  • 100-240 VAC, 50/60 Hz | | TAK | |  | |
| **Porty** | | | | | | | |
| **1.** | | • min. WAN: 1 x 10/100/1000BASE-T Ethernet, Auto-MDIX, RJ-45  • min. LAN: 4 x 10/100/1000BASE-T Ethernet, Auto-MDIX, RJ-45  • min. Console: 1 x RJ-45  • min. USB: 1 x USB 3.0 LED | | TAK | |  | |
| **Parametry system** | | | | | | | |
| **1.** | | Zarządzane punkty dostępowe: do 150  Konta lokalne: do 10 000  Konta na żądanie: do 10 000  Przełączniki zarządzane: 10  Limit równoczesnych użytkowników: 400, przełączalny | | TAK | |  | |
| **Status systemu i sieci** | | | | | | | |
| **1.** | | Deska rozdzielcza systemu  Graficzne raporty wydajności systemu  Raporty o natężeniu ruchu  Monitor procesu systemowego  Monitorowanie urządzeń online  Lista aktywnych sesji  Konfigurowalny poziom ważności syslog  Powiadomienia SMTP (e-mail)  Wiele jednoczesnych odbiorców powiadomień e-mail | | TAK | |  | |
| **Dzienniki aktywności sieci** | | | | | | | |
| **1.** | | Log systemu (Syslog)  Log CAPWAP  Log zmian konfiguracji  Log serwera RADIUS  Log zdarzeń użytkownika  Log użytkownika HTTP  Log zapory  Serwer DHCP / log dzierżawy  Log interfejsu PMS  Raport rozliczeniowy na żądanie  Powiadomienie e-mail o statusie AP  Logowanie do zewnętrznego FTP  Konfigurowalne dzienniki i interwały raportowania | | TAK | |  | |
| **Bezpieczeństwo** | | | | | | | |
| **1.** | | Rodzaje uwierzytelnienia:  • 802.1X  • UAM (oparty na przeglądarce)  • Na podstawie adresu IP lub MAC  Serwery uwierzytelniające:  • Lokalny  • Na żądanie  • Gość  • RADIUS  • LDAP  • Domena NT  • SIP  • POP3  Konfigurowalny Captive Portal  Konfigurowalny wild card  Czarna lista użytkowników | | TAK | |  | |
| **Zarządzanie systemem** | | | | | | | |
| **1.** | | Konfiguracja oparta na przeglądarce  Konta administratora:  • Wiele wielopoziomowych uprawnień dostępu  Czas systemu:  • Synchronizacja NTP  • Ręczna konfiguracja  Tworzenie kopii zapasowych i przywracanie systemu  SNMP v2c  Narzędzia sieciowe: wbudowane przechwytywanie pakietów | | TAK | |  | |
| **Zarządzanie AP** | | | | | | | |
| **1.** | | Automatyczne wykrywanie AP  Automatyczne przydzielanie AP: na podstawie szablonu  Tworzenie kopii zapasowych i przywracanie konfiguracji AP  Zarządzanie tunelowanymi AP: zarówno AP L2, jak i L3  Równoważenie obciążenia AP | | TAK | |  | |
| **Zarządzanie przełącznikami** | | | | | | | |
| **1.** | | Automatyczne wykrywanie przełączników  Automatyczne udostępnianie przełączników: oparte na szablonach  Tworzenie kopii zapasowych i przywracanie konfiguracji przełączników  Harmonogram zasilania przełączników | | TAK | |  | |
| **Zarządzanie użytkownikami** | | | | | | | |
| **1.** | | Przypisanie zasad użytkownika:  • Oparte na rolach  • Zależy od czasu i lokalizacji  Ograniczenie przepustowości  • Oparte na użytkownikach  • Na bazie grupy  • Ograniczanie przepustowości  Klasyfikacja / uwagi ruchu: 802.1p / DSCP  Statefl Firewall: Każda reguła z indywidualnymi harmonogramami egzekwowania  Przypisywanie statycznych tras  Limit równoczesnych sesji  Zmiana przypisania adresu IP: Zezwalanie klientom na uzyskanie innego adresu IP  po uwierzytelnieniu | | TAK | |  | |
| **GWARANCJA** | | | | | | | |
| **1.** | | Gwarancja 5 Lat | | TAK | |  | |

|  |  |  |  |
| --- | --- | --- | --- |
| **12. Licencje dostępowe serwerów 110 szt.** | | | |
| **Lp.** | **Wymagane minimalne parametry techniczne** | **Wymóg do spełnienia (warunek graniczny)** | **OFEROWANE PARAMETRY TECHNICZNE - podaje**  **Wykonawca**  **Wymogi dotyczące opisu oferowanych parametrów:**  TAK – wykonawca spełnia konkretny parametr przy czym Zamawiający oczekuje by w przypadku wymagań dotyczących minimalnych parametrów opisać szczegółowo parametry oferowane przez wykonawcę  NIE – wykonawca nie spełnia konkretnego parametru |
| **1.** | Licencje dostępowe do serwera wirtualizacji z punktu 1. – 55 szt. | TAK |  |
| **2.** | Licencje umożliwiające podłączenie się do serwera wirtualizacji z punktu 1. poprzez zdalny dostęp – 55 szt. | TAK |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **13. Centrum Autoryzacji – 1 szt. składające się z:**  ***A. Oprogramowanie umożliwiające szyfrowanie wrażliwych danych*** | | | | | | |
| **Lp.** | **Wymagane minimalne parametry techniczne** | | **Wymóg do spełnienia (warunek graniczny)** | | **OFEROWANE PARAMETRY TECHNICZNE - podaje**  **Wykonawca**  **Wymogi dotyczące opisu oferowanych parametrów:**  TAK – wykonawca spełnia konkretny parametr przy czym Zamawiający oczekuje by w przypadku wymagań dotyczących minimalnych parametrów opisać szczegółowo parametry oferowane przez wykonawcę  NIE – wykonawca nie spełnia konkretnego parametru | |
| **FUNKCJONALNOŚCI** | | | | | | |
| **1.** | | Tworzenie głównego drzewa Root CA | TAK | |  | |
| **2.** | | Tworzenie podrzędnych drzew do wystawiania certyfikatów na  dane danej jednostki organizacyjnej w danym przedsiębiorstwie | TAK | |  | |
| **3.** | | Tworzenie klastra awaryjnego (fail-over) | TAK | |  | |
| **4.** | | Nielimitowane czasowo działanie oprogramowania bez dokupowania licencji przedłużających | TAK | |  | |
| **5.** | | Nielimitowane wydawanie, zawieszanie, zastrzeganie i  odwoływanie certyfikatów | TAK | |  | |
| **6.** | | Instalacje oraz tworzenie nowych szablonów certyfikatów | TAK | |  | |
| **7.** | | Automatyczne generowanie i wystawianie certyfikatów dla  urządzeń mobilnych korzystających z sieci wireless | TAK | |  | |
| **8.** | | Konfiguracja list crl oraz wyrywkowej kontroli ważności certyfikatu  za pomocą usługi ocsp | TAK | |  | |
| **9.** | | Odwoływanie wystawionych już certyfikatów z możliwością  czasowego ich zawieszenia na dany okres czasu | TAK | |  | |
| **10.** | | Generowanie certyfikatów na podstawie istniejących już domyślnie szablonów certyfikatów minimum takich jak:   * administrator * Authenticated Session * Basic EFS * CA Exchange * CEP Encryption * Code Signing * Computer * Cross-Certification Authority * Directory E-mail Replication * Domain Controller * Domain Controller Authentication * EFS Recovery Agent | TAK | |  | |

|  |  |  |  |
| --- | --- | --- | --- |
|  | * Enrollment Agent * Enrollment Agent (Computer) * Exchange Enrollment Agent (Offline request) * Exchange Signature Only * Exchange User * IPSec * IPSec (Offline request) * Kerberos Authentication * Key Recovery Agent (KRA) * OCSP Response Signing * Remote Access Service (RAS) and Internet Authentication Service   (IAS) Server   * Root CA * Router (Offline request) * Smart Card Logon * Smart Card User * Subordinate CA * Trust List Signing * User * User Signature Only * Web Server * Workstation Authentication |  |  |
| **WSPIERANE ALGORYTMY** | | | |
| **1.** | SHA1, SHA2 (SHA256, SHA384, SHA512) | TAK |  |
| **2.** | RSA o długości 1024, 2048 oraz 4096 | TAK |  |
| **3.** | ECC/ECDSA NIST P-256, P-384, P-521 | TAK |  |
| **WYMAGANIA TECHNICZNE** | | | |
| **1.** | Interfejs graficzny GUI do obsługi oprogramowania | TAK |  |
| **2.** | Wsparcie dla systemów operacyjnych dostarczanych w ramach postępowania. | TAK |  |

|  |  |  |  |
| --- | --- | --- | --- |
| ***B. Sieciowy moduł bezpieczeństwa umożliwiający przechowywanie newralgicznego materiału kryptograficznego*** | | | |
| **OBUDOWA** | | | |
| **1.** | Wysokość nie większa niż 2U, dostosowana do montażu w szafie 19” | TAK |  |
| **BEZPIECZEŃSTWO** | | | |
| **1.** | FIPS 140- 2 poziom 3 | TAK |  |
| **OBSŁUGA SYSTEMÓW OPERACYJNYCH** | | | |
| **1.** | Wsparcie minimum dla systemów typu Windows Server 2008 R2 / 2012 R2 / 2016, Red Hat Enterprise Linux Server 5 i 6 | TAK |  |
| **PORTY** | | | |
| **1.** | 2x RJ45 1000 BASE-T umożliwiające stworzenie wirtualnego numeru IP rozkładającego ruch na dwa interfejsy | TAK |  |
| **2.** | 1x VGA | TAK |  |
| **3.** | 1x USB 2.0 | TAK |  |
| **OBSŁUGA INTERFEJSÓW** | | | |
| **1.** | PKCS#11 | TAK |  |
| **2.** | MSCAPI | TAK |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **3.** | Java JCA/JCE API | TAK |  |
| **OBSŁUGA ALGORYTMÓW KRYPTOGRAFICZNYCH** | | | |
| **1.** | Kryptografia symetryczna: AES, DES, Triple-DES | TAK |  |
| **2.** | Kryptografia asymetryczna: DSA, ECDSA, RSA | TAK |  |
| **3.** | Funkcje skrótu: SHA-1, SHA-2, SHA-3, RIPEMD | TAK |  |
| **INTEGRACJA** | | | |
| **1.** | Moduł musi udostępniać dodatkowe API umożliwiające integrację z:   * PKCS#11 * Java Cryptographic Extensions (JCE) * Microsoft Crypto API (CSP) * Cryptography Next Generation (CNG) | TAK |  |
| **FUNKCJONALNOŚCI** | | | |
| **1.** | Nielimitowana ilość aplikacji klienckich korzystających z modułu. | TAK |  |
| **2** | Urządzenie musi :   * wspierać silną autoryzacje użytkownika w celach administracyjnych, do autoryzacji wymaga się dwóch dedykowanych kart producenta wraz z certyfikowanym czytnikiem posiadającym PIN pad do wprowadzania PIN-u karty. * wspierać backup głównego klucza (Master Backup Key) i mieć możliwość jego zapisu do pliku, oraz na dedykowane karty producenta z dedykowaną przestrzenią na Główny klucz szyfrujący   (Master Backup Key). | TAK |  |
| **3.** | Możliwość zarządzania modułem na bazie ról oraz autoryzację opartą o podział sekretu do autoryzacji w trybie “n of m” | TAK |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **CERTYFIKATY** | | | |
| **1.** | FIPS 140-2 Level 3 | TAK |  |
| **2.** | CE, FCC Class B | TAK |  |
| **3.** | UL, IEC/EN 60950-1 | TAK |  |
| **4.** | CB certificate | TAK |  |
| **5.** | RoHS II, WEEE | TAK |  |
| **WYPOSAŻENIE DODATKOWE** | | | |
| **1.** | Minimum 10 szt. dedykowanych do urządzenia kart | TAK |  |
| **2.** | Dedykowany czytnik kart | TAK |  |
| **GWARANCJA** | | | |
| **1.** | Gwarancja 5 Lat | TAK |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **14. Wymagania wdrożeniowe** | | | |
| **Lp.** | **Minimalne wymagania wdrożeniowe** | **Wymóg do spełnienia (warunek graniczny)** | **POTWIERDZENIE ZAOFEROWANIA MINIMALNYCH**  **WYMAGAŃ WZDROŻENIOWYCH - podaje Wykonawca**  **Wymogi dotyczące opisu oferowanych parametrów:**  TAK – wykonawca spełnia konkretny parametr przy czym Zamawiający oczekuje by w przypadku wymagań dotyczących minimalnych parametrów opisać szczegółowo parametry oferowane przez wykonawcę  NIE – wykonawca nie spełnia konkretnego parametru |

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  | *spełnia* |
| **OGÓLNE** | | | |
| **1.** | Montaż opisanego przedmiotu zamówienia w szafach typu Rack Zamawiającego w sposób zgodny z zaleceniami producenta  dostarczanych urządzeń oraz prowadzenie kabli nie może powodować zaburzeń w cyrkulacji gorącego powietrza  wydmuchiwanego z serwerów. | TAK |  |
| **2.** | Stworzenie klastra serwerów w oparciu o oprogramowanie wirtualizacyjne dostarczane w ramach postępowania.  Fizyczne serwery mają zostać skonfigurowane w trybie wysokiej dostępności (awaria jednego serwera nie może powodować  niedostępności usług uruchomionych na dostarczanych w postępowaniu serwerach).  Dane serwerów będą przechowywane na dostarczanych macierzach. | TAK |  |
| **3.** | Testy niezawodności środowiska serwerowego poprzez odłączanie jednej ze ścieżki/wyłączanie urządzenia oraz test redundancji  Zasilania | TAK |  |
| **4.** | Centrum autoryzacji (CA) musi zostać skonfigurowane w sposób zgodny z zaleceniami producenta sprzętowego modułu  bezpieczeństwa. | TAK |  |
| **5** | Minimalne wymagania do wykonania w ramach uruchomienia Centrum Autoryzacji przeprowadzone przez Wykonawcę:   * instalacja urządzenia LAN w miejscu wskazanym przez zamawiającego * inicjalizacja urządzenia (procedurę bootstrap) * integracja z Centrum Autoryzacji za pomocą interfejsu CSP * konfiguracja głównego Urzędu Certyfikacyjnego * integracja z wbudowanym (wymaganym) w serwer modułem   bezpieczeństwa umożliwiając tworzenie backupów – z urządzenia LAN na kartę PCI-e   * instruktaż z obsługi urządzenia bezpieczeństwa obejmujący min.:   + Pierwsze uruchomienie i rozruch - procedura BootStrap.   + Inicjalizacja Sprzętowego Modułu Bezpieczeństwa - wygenerowanie kart administracyjnych dla głównych administratorów. | TAK |  |

|  |  |  |  |
| --- | --- | --- | --- |
|  | * Zarządzanie użytkownikami i autoryzacją. * Konfiguracja dostępu do LAN Sprzętowego Modułu   Bezpieczeństwa po protokole SSH do zarządzania poprzez sieć LAN   * Dołączanie dodatkowego magazynu danych na klucze kryptograficzne z HSM * Administracja poprzez Comand Line Interface VS Graphic User Interface * Tworzenie kopi bezpieczeństwa i odzyskiwanie. * Inicjalizacja komunikacji z Sprzętowym Modułem Bezpieczeństwa po PCS#11, CSP. * podział kluczy kryptograficznych szyfrujących cały materiał krypograficzny znajdujący się w pamięci urządzenia na minimum 4 karty inteligentne * PIN do każdej karty powinien zostać zmieniony po przeprowadzonym wdrożeniu. * użytkownik administracyjny Sprzętowego Modułu   Bezpieczeństwa musi logować się na „dwie ręce” – procedura logowania musi wymagać dwóch użytkowników/kart.   * miejscem składowania materiały kryptograficznego powinna być pamięć wewnętrzna Sprzętowego Modułu Bezpieczeństwa. |  |  |
| **6.** | Proces konfiguracji Centrum Autoryzacji zakłada wydanie certyfikatu Root CA w jednostce lidera projektu (Szpital Międzyrzecki Sp. z o.o.) oraz musi zostać wydany certyfikat SubCA z kluczem na urządzeniu HSM dostarczanym do Samodzielnego Publicznego Zakładu Opieki Zdrowotnej w Sulechowie.  Finalnie SubCA musi wydawać certyfikaty dla użytkowników Szpitala Zamawiającego. | TAK |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **7.** | Wymaga konfiguracja akcji shutdown na zasilaczach awaryjnych dostarczanych w ramach postępowania w przypadku braku zasilania z sieci dla klastra serwerów jak i pojedynczych urządzeń  wspierających tę funkcję. | TAK |  |
| **8.** | Aktualizacja sterowników do najnowszych na dzień wdrożenia. | TAK |  |
| **9.** | Do macierzy należy podłączyć wszystkie serwery fizyczne w taki sposób, aby fizyczne i wirtualne maszyny uruchomione na serwerach fizycznych mogły korzystać z dysków macierzy w możliwie najszybszy sposób. | TAK |  |
| **10.** | Instalacja systemów operacyjnych na 3 serwerach fizycznych,  podstawowa konfiguracja serwerów, w tym kart sieciowych. | TAK |  |
| **11.** | Konfiguracja macierzy dyskowej, w tym skonfigurowanie RAID na poszczególnych grupach dyskowych. | TAK |  |
| **12.** | Instruktaż Zespołu Informatycznego odnośnie przeprowadzonego wdrożenia systemu informatycznego na dostarczanym sprzęcie. | TAK |  |

**IV. Infrastruktura sprzętowa wraz z Centrum Autoryzacji dla Samodzielnego Publicznego Zakładu Opieki Zdrowotnej w Sulęcinie**

|  |  |  |  |
| --- | --- | --- | --- |
| **1. Serwer do obsługi wirtualizacji- 2 szt.** | | | |
| **Lp.** | **Wymagane minimalne parametry techniczne** | **Wymóg do spełnienia (warunek graniczny)** | **OFEROWANE PARAMETRY TECHNICZNE - podaje**  **Wykonawca**  **Wymogi dotyczące opisu oferowanych parametrów:**  TAK – wykonawca spełnia konkretny parametr przy czym Zamawiający oczekuje by w przypadku wymagań dotyczących minimalnych parametrów opisać szczegółowo parametry oferowane przez wykonawcę  NIE – wykonawca nie spełnia konkretnego parametru |
| **OBUDOWA** | | | |
| **1.** | • Typu RACK, wysokość nie więcej niż 2U;  • Szyny umożliwiające wysunięcie serwera z szafy stelażowej;  • Opcjonalne ramię porządkujące ułożenie przewodów z tyłu serwera; | TAK |  |
| **Płyta główna** | | | |
| **1.** | • Dwuprocesorowa;  • Wyprodukowana i zaprojektowana przez producenta serwera  • Zainstalowany moduł TPM 2.0  • Wsparcie dla technologii:  o Advanced ECC | TAK |  |
| **Procesory** | | | |
| **1.** | • Dwa procesory 8-rdzeniowe o taktowaniu procesora nie mniejszym niż 2,5GHz  • architektura x86\_64 | TAK |  |
| **Pamięć RAM** | | | |
| **1.** | • 256 GB pamięci RAM (16 wolnych slotów do dalszej rozbudowy pamięci)  • DDR4 Registered | TAK |  |
| **Dyski twarde i napędy** | | | |
| **1.** | • Minimum 8 wnęk dla dysków twardych Hotplug 2,5”;  • Możliwość rozbudowy do 16 wnęk;  • Zainstalowane 2 dyski o pojemności minimum 120GB . | TAK |  |
| **Kontrolery LAN** | | | |
| **1.** | • Karta LAN 2x 10Gbit SFP+; możliwość wymiany zainstalowanych interfejsów LAN na interfejsy 2x 10Gbit Base- T bez potrzeby wymiany całego układu lub instalacji dodatkowych kart w slotach PCI Express  2 moduły SFP+ Multi Mode Fiber 10GbE LC | TAK |  |
| **Kontrolery I/O** | | | |
| **1.** | • Zainstalowane dwie jednoportowe karty FC 16Gb;  W jednym z serwerów zainstalowany Moduł HSM PCIe | TAK |  |
| **Porty** | | | |
| **1.** | • Zintegrowana karta graficzna ze złączami VGA z tyłu oraz przodu serwera;  • Minimum 1 port USB 3.0 na panelu przednim;  • Min 2 porty USB 3.0 dostępne z tyłu serwera;  • Możliwość instalacji jednego portu serial, możliwość wykorzystania portu do zarządzania serwerem;  • Ilość dostępnych złącz USB nie może być osiągnięta poprzez stosowanie zewnętrznych przejściówek, rozgałęziaczy czy dodatkowych kart rozszerzeń zajmujących jakikolwiek slot PCI Express i/lub USB serwera; | TAK |  |
| **Zasilanie, chłodzenie** | | | |
| **1.** | • Redundantne zasilacze hotplug o mocy minimalnej 400W o sprawności min. 94%; | TAK |  |
| **Zarządzanie** | | | |
| **1.** | • Wbudowane diody informacyjne lub wyświetlacz informujące o stanie serwera - system przewidywania, rozpoznawania awarii)  Zintegrowany z płytą główną serwera kontroler sprzętowy zdalnego zarządzania zgodny z IPMI 2.0 o funkcjonalnościach:  • Niezależny od systemu operacyjnego, sprzętowy kontroler umożliwiający pełne zarządzanie, zdalny restart serwera;  o Dedykowana karta LAN 1 Gb/s, dedykowane złącze RJ-45 do komunikacji wyłącznie z kontrolerem zdalnego zarządzania z możliwością przeniesienia tej komunikacji na inną kartę sieciową współdzieloną z systemem operacyjnym;  o Dostęp poprzez przeglądarkę Web, SSH;  o Zarządzanie mocą i jej zużyciem oraz monitoring zużycia energii;  o Zarządzanie alarmami (zdarzenia poprzez SNMP)  o Możliwość przejęcia konsoli tekstowej  o Możliwość zarządzania przez 6 administratorów jednocześnie  o Przekierowanie konsoli graficznej na poziomie sprzętowym oraz możliwość montowania zdalnych napędów i ich obrazów na poziomie sprzętowym (cyfrowy KVM)  o Obsługa serwerów proxy (autentykacja)  o Obsługa VLAN  o Możliwość konfiguracji parametru Max. Transmission Unit (MTU)  o Wsparcie dla protokołu SSDP  o Obsługa protokołów TLS 1.0, TLS 1.1, TLS 1.2, SSL v3  o Obsługa protokołu LDAP  o Synchronizacja czasu poprzez protokół NTP  o Możliwość backupu i odtworzenia ustawień bios serwera oraz ustawień karty zarządzającej  • Oprogramowanie zarządzające i diagnostyczne wyprodukowane przez producenta serwera umożliwiające konfigurację kontrolera RAID, instalację systemów operacyjnych, zdalne zarządzanie, diagnostykę i przewidywanie awarii w oparciu o informacje dostarczane w ramach zintegrowanego w serwerze systemu umożliwiającego monitoring systemu i środowiska (m.in. temperatura, dyski, zasilacze, płyta główna, procesory, pamięć operacyjna);  • Serwer posiada możliwość konfiguracji i wykonania aktualizacji BIOS, Firmware, sterowników serwera bezpośrednio z GUI (graficzny interfejs). | TAK |  |
| **Wspierane OS** | | | |
| **1.** | • Microsoft Windows Server 2019, 2016  • VMWare vSphere 6.7  • Suse Linux Enterprise Server 12  • Red Hat Enterprise Linux 7, 8  • Hyper-V Server | TAK |  |
| **System operacyjny** | | | |
| **1.** | Licencje na serwerowy system operacyjny muszą uprawniać do uruchamiania serwerowego systemu operacyjnego w środowisku fizycznym i minimum 4 wirtualnych środowisk ( per serwer)serwerowego systemu operacyjnego za pomocą wbudowanych mechanizmów wirtualizacji.  Serwerowy system operacyjny musi posiadać następujące, wbudowane cechy.  1) Możliwość wykorzystania 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym.  2) Możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności do 64TB przez każdy wirtualny serwerowy system operacyjny.  3) Możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania 7000 maszyn wirtualnych.  4) Możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci.  5) Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy.  6) Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy.  7) Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.  8) Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading.  9) Wbudowane wsparcie instalacji i pracy na wolumenach, które:  a) pozwalają na zmianę rozmiaru w czasie pracy systemu,  b) umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,  c) umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów,  d) umożliwiają zdefiniowanie list kontroli dostępu (ACL).  10) Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.  11) Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.  12) Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET  13) Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.  14) Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.  15) Dostępne dwa rodzaje graficznego interfejsu użytkownika:  a) Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,  b) Dotykowy umożliwiający sterowanie dotykiem na monitorach dotykowych.  16) Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe,  17) Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji.  18) Mechanizmy logowania w oparciu o:  a) Login i hasło,  b) Karty z certyfikatami (smartcard),  c) Wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM),  19) Możliwość wymuszania wieloelementowej dynamicznej kontroli dostępu dla: określonych grup użytkowników, zastosowanej klasyfikacji danych, centralnych polityk dostępu w sieci, centralnych polityk audytowych oraz narzuconych dla grup użytkowników praw do wykorzystywania szyfrowanych danych..  20) Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).  21) Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.  22) Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa.  23) Pochodzący od producenta systemu serwis zarządzania polityką dostępu do informacji w dokumentach (Digital Rights Management).  24) Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach.  25) Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:  a) Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC,  b) Usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji:  i. Podłączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną,  ii. Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,  iii. Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza.  iv. Bezpieczny mechanizm dołączania do domeny uprawnionych użytkowników prywatnych urządzeń mobilnych opartych o iOS i Windows 8.1.  c) Zdalna dystrybucja oprogramowania na stacje robocze.  d) Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej  e) Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:  i. Dystrybucję certyfikatów poprzez http  ii. Konsolidację CA dla wielu lasów domeny,  iii. Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen,  iv. Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509.  f) Szyfrowanie plików i folderów.  g) Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec).  h) Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów.  i) Serwis udostępniania stron WWW.  j) Wsparcie dla protokołu IP w wersji 6 (IPv6),  k) Wsparcie dla algorytmów Suite B (RFC 4869),  l) Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows,  m) Wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie do 1000 aktywnych środowisk wirtualnych systemów operacyjnych. Wirtualne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności. Mechanizmy wirtualizacji mają zapewnić wsparcie dla:  i. Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych,  ii. Obsługi ramek typu jumbo frames dla maszyn wirtualnych.  iii. Obsługi 4-KB sektorów dysków  iv. Nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra  v. Możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API.  vi. Możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk mode)  26) Możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta serwerowego systemu operacyjnego umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet.  27) Wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath).  28) Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego.  29) Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.  30) Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF. | TAK |  |
| **Gwarancja** | | | |
| **1.** | Gwarancja 5 Lat | TAK |  |
| **Dokumentacja, inne** | | | |
| **1.** | • Serwer musi być fabrycznie nowy i pochodzić z oficjalnego kanału dystrybucyjnego w UE. Nie dopuszcza się użycia serwerów odnawianych, demonstracyjnych lub powystawowych.  • Ogólnopolska, telefoniczna infolinia/linia techniczna producenta serwera  • Możliwość aktualizacji i pobrania sterowników do oferowanego modelu serwera w najnowszych certyfikowanych wersjach bezpośrednio z sieci Internet za pośrednictwem strony www producenta serwera; | TAK |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **2. Serwer bazodanowy- 2 szt.** | | | |
| **Lp.** | **Wymagane minimalne parametry techniczne** | **Wymóg do spełnienia (warunek graniczny)** | **OFEROWANE PARAMETRY TECHNICZNE - podaje**  **Wykonawca**  **Wymogi dotyczące opisu oferowanych parametrów:**  TAK – wykonawca spełnia konkretny parametr przy czym Zamawiający oczekuje by w przypadku wymagań dotyczących minimalnych parametrów opisać szczegółowo parametry oferowane przez wykonawcę  NIE – wykonawca nie spełnia konkretnego parametru |
| **OBUDOWA** | | | |
| **1.** | • Typu RACK, wysokość nie więcej niż 2U;  • Szyny umożliwiające wysunięcie serwera z szafy stelażowej;  • Opcjonalne ramię porządkujące ułożenie przewodów z tyłu serwera; | TAK |  |
| **PŁYTA GŁÓWNA** | | | |
| **1.** | • Wyprodukowana i zaprojektowana przez producenta serwera  • Zainstalowany moduł TPM 2.0  • Wsparcie dla technologii:  o Memory Scrubbing  o Advanced ECC | TAK |  |
| **Procesory** | | | |
| **1.** | • Jeden procesor 8-rdzeniowy (nie dopuszcza się większej ilości rdzeni fizycznych) o taktowaniu nie mniejszym niż 3,0 GHz  • architektura x86\_64 | TAK |  |
| **Pamięć RAM** | | | |
| **1.** | • min 64 GB pamięci RAM  • DDR4 Registered  • | TAK |  |
| **Dyski twarde i napędy** | | | |
| **1.** | • Minimum 8 wnęk dla dysków twardych Hotplug 2,5”;  • Zainstalowane 2 dyski SSD Hot-Plug o pojemności 120GB i parametrze DWPD>=3 | TAK |  |
| **Kontrolery LAN** | | | |
| **1.** | • Karta LAN 2x 10Gbit SFP+; możliwość wymiany zainstalowanych interfejsów LAN na interfejsy 2x 10Gbit Base- T bez potrzeby wymiany całego układu lub instalacji dodatkowych kart w slotach PCI Express  2 moduły SFP+ Multi Mode Fiber 10GbE LC | TAK |  |
| **Kontrolery I/O** | | | |
| **1.** | • Zainstalowane jedna karta dwuportowe karty FC 16Gb; | TAK |  |
| **Porty** | | | |
| **1.** | • Zintegrowana karta graficzna ze złączami VGA z tyłu oraz przodu serwera;  • Min 1 port USB 3.0 na panelu przednim;  • Min 2 porty USB 3.0 dostępne z tyłu serwera;  • Możliwość instalacji jednego portu serial, możliwość wykorzystania portu do zarządzania serwerem;  • Ilość dostępnych złącz USB nie może być osiągnięta poprzez stosowanie zewnętrznych przejściówek, rozgałęziaczy czy dodatkowych kart rozszerzeń zajmujących jakikolwiek slot PCI Express i/lub USB serwera;; | TAK |  |
| **Zasilanie, chłodzenie** | | | |
| **1.** | • Redundantne zasilacze hotplug o mocy minimalnej 400W o sprawności min. 94%; | TAK |  |
| **Zarządzanie** | | | |
| **1.** | • Wbudowane diody informacyjne lub wyświetlacz informujące o stanie serwera - system przewidywania, rozpoznawania awarii)  Zintegrowany z płytą główną serwera kontroler sprzętowy zdalnego zarządzania zgodny z IPMI 2.0 o funkcjonalnościach:  • Niezależny od systemu operacyjnego, sprzętowy kontroler umożliwiający pełne zarządzanie, zdalny restart serwera;  o Dedykowana karta LAN 1 Gb/s, dedykowane złącze RJ-45 do komunikacji wyłącznie z kontrolerem zdalnego zarządzania z możliwością przeniesienia tej komunikacji na inną kartę sieciową współdzieloną z systemem operacyjnym;  o Dostęp poprzez przeglądarkę Web, SSH;  o Zarządzanie mocą i jej zużyciem oraz monitoring zużycia energii;  o Zarządzanie alarmami (zdarzenia poprzez SNMP)  o Możliwość przejęcia konsoli tekstowej  o Możliwość zarządzania przez 6 administratorów jednocześnie  o Przekierowanie konsoli graficznej na poziomie sprzętowym oraz możliwość montowania zdalnych napędów i ich obrazów na poziomie sprzętowym (cyfrowy KVM)  o Obsługa serwerów proxy (autentykacja)  o Obsługa VLAN  o Możliwość konfiguracji parametru Max. Transmission Unit (MTU)  o Wsparcie dla protokołu SSDP  o Obsługa protokołów TLS 1.0, TLS 1.1, TLS 1.2, SSL v3  o Obsługa protokołu LDAP  o Synchronizacja czasu poprzez protokół NTP  o Możliwość backupu i odtworzenia ustawień bios serwera oraz ustawień karty zarządzającej  • Serwer posiada możliwość konfiguracji i wykonania aktualizacji BIOS, Firmware, sterowników serwera bezpośrednio z GUI (graficzny interfejs) . | TAK |  |
| **Wspierane OS** | | | |
| **1.** | • Microsoft Windows Server 2019, 2016  • VMWare vSphere 6.7  • Suse Linux Enterprise Server 12  • Red Hat Enterprise Linux 7, 8  • Hyper-V Server | TAK |  |
| **System operacyjny** | | | |
| **1.** | System Operacyjny dedykowany do bazy danych systemu his. | TAK |  |
| **Gwarancja** | | | |
| **1.** | Gwarancja 5 Lat | TAK |  |
| **Dokumentacja, inne** | | | |
| **1.** | • Serwer musi być fabrycznie nowy i pochodzić z oficjalnego kanału dystrybucyjnego w UE. Nie dopuszcza się użycia serwerów odnawianych, demonstracyjnych lub powystawowych.  • Ogólnopolska, telefoniczna infolinia/linia techniczna producenta serwera  • Możliwość aktualizacji i pobrania sterowników do oferowanego modelu serwera w najnowszych certyfikowanych wersjach bezpośrednio z sieci Internet za pośrednictwem strony www producenta serwera; | TAK |  |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **3. Macierz dyskowa- 1 szt.** | | | | | | | |
| **Lp.** | | **Wymagane minimalne parametry techniczne** | | **Wymóg do spełnienia (warunek graniczny)** | | **OFEROWANE PARAMETRY TECHNICZNE - podaje**  **Wykonawca**  **Wymogi dotyczące opisu oferowanych parametrów:**  TAK – wykonawca spełnia konkretny parametr przy czym Zamawiający oczekuje by w przypadku wymagań dotyczących minimalnych parametrów opisać szczegółowo parametry oferowane przez wykonawcę  NIE – wykonawca nie spełnia konkretnego parametru | |
| **OGÓLNE** | | | | | | | |
| **1.** | | System musi być dostarczony ze wszystkimi komponentami do instalacji w standardowej szafie rack 19” z zajętością maks. 2U w tej szafie. Każdy skonfigurowany moduł/obudowa musi posiadać układ nadmiarowy zasilania i chłodzenia, zapewniający bezprzerwową pracę macierzy bez ograniczeń czasowych w przypadku utraty redundancji w danym układzie (zasilania lub chłodzenia). Każdy moduł/obudowa powinien posiadać widoczne elementy sygnalizacyjne do informowania o stanie poprawnej pracy lub awarii. Rozbudowa o dodatkowe moduły dla obsługiwanych dysków powinna odbywać się wyłącznie poprzez zakup takich modułów, bez konieczności zakupu dodatkowych licencji lub specjalnego oprogramowania aktywującego proces rozbudowy lub musi być dostarczona licencja na dwukrotność dostarczanej pojemności. Dostarczana macierz musi umożliwiać podłączenie półek kaskadowo , bądź w formie 2 łańcuchów. Oferowana macierz musi obsługiwać min. 260 dysków wykonanych w technologii hot-plug. Macierz musi umożliwiać rozbudowę i jednoczesne podłączenie i używanie modułów (tzw. „półek dyskowych”) w rozmiarze 2U pozwalająca umieścić do 24 dysków 2,5” typu hotplug dla dysków NL-SAS SAS i SSD oraz w rozmiarze 2U dla 12 dysków 3,5” typu hotplug SAS, NL-SAS oraz do 6U dla min 60 dysków; Wymaga się aby macierz umożliwiała jednoczesne podłączenie i użycie dowolnego rodzaju i kombinacji wyżej wymienionych półek dyskowych Macierz musi posiadać funkcje automatycznego tieringu | | TAK | |  | |
| **POJEMNOŚĆ DOSTARCZONEJ MACIERZY** | | | | | | | |
| **1.** | | * przestrzeń minimum 12TB realizowana na dyskach : * min 4 dyski SSD-SAS o pojemności minimum 1,8TB * min 6 dysków 10k SAS o pojemności minimum 1,8TB | | TAK | |  | |
| **KONTROLERY** | | | | | | | |
| **1.** | | • Kontrolery macierzy muszą obsługiwać tryb pracy w układzie min active-active, macierz musi być dostarczona z zainstalowanymi minimum 2 kontrolerami;  • Każdy z kontrolerów macierzy musi posiadać po minimum 32 GB pamięci podręcznej Cache – kontrolery muszą obsługiwać między sobą mechanizm lustrzanej kopii danych (cache mirror) przeznaczonych do zapisu;  • W przypadku awarii zasilania dane nie zapisane na dyski, przechowywane w pamięci podręcznej Cache dla zapisów muszą być zabezpieczone metodą trwałego zapisu na dysk.  • Kontrolery muszą posiadać możliwość ich wymiany bez konieczności wyłączania zasilania całego urządzenia;  • Kontrolery macierzy obsługują funkcjonalność kompresji danych.  • Kontrolery macierzy obsługują funkcjonalność deduplikacji w trybie in-line.  • Macierz musi obsługiwać wymianę kontrolera RAID bez utraty danych zapisanych na dyskach.  • Każdy z kontrolerów RAID powinien posiadać dedykowany minimum 2 interfejsy RJ-45 Ethernet obsługujący połączenia z prędkością minimum 1Gb/s dla zdalnej komunikacji z oprogramowaniem zarządzającym i konfiguracyjnym macierzy.  • Kontrolery macierzy muszą być oparte o procesor wykonany w technologii wielordzeniowej z minimum 4 rdzeniami,  • Kontrolery macierzy muszą obsługiwać min 120 grup dyskowych w całym rozwiązaniu, bez konieczności wymiany dostarczonych kontrolerów  • Oferowana macierz musi mieć wyprowadzone 4 porty FC 16Gb/s do dołączenia serwerów bezpośrednio lub do dołączenia do sieci SAN, na każdy kontroler RAID.  • Macierz musi umożliwiać stosowanie (rozbudowa/wymiana) portów do transmisji danych:  FC 16Gb/s, iSCSI min 10Gb/s  • Stosowanie wyżej wymienionych portów nie może powodować wymiany samych kontrolerów RAID w oferowanym rozwiązaniu a w przypadku konieczność licencjonowania tej funkcjonalności macierz ma być dostarczona z aktywną licencja na instalację i obsługę każdego z wymienionych protokołów transmisji danych | | TAK | |  | |
| **Poziomy RAID** | | | | | | | |
| **1.** | | Macierz musi zapewniać poziom zabezpieczenia danych na dyskach definiowany poziomami RAID:  o Raid-0  o Raid-1  o Raid-10  o Raid-5  o Raid-6 | | TAK | |  | |
| **Dyski** | | | | | | | |
| **1.** | | Oferowana macierz musi wspierać dyski hot-plug:  o dyski elektroniczne SSD i mechaniczne HDD z interfejsami SAS12Gb/s  o dyski mechaniczne HDD o prędkości obrotowej min 7,2 krpm, 10 krpm .  • Macierz musi obsługiwać mieszaną konfigurację dysków hot-plug SSD i HDD w rozmiarach 2,5” i 3,5” zainstalowanych w dowolnym module rozwiązania;  • Wszystkie dyski wspierane przez oferowany model macierzy muszą być wykonane w technologii hot-plug i posiadać podwójne porty SAS obsługujące tryb pracy full-duplex  • Macierz musi obsługiwać min. 260 dysków SAS SSD w całym rozwiązaniu, bez konieczności dokupowania/wymiany żadnych innych elementów sprzętowych czy licencyjnych innych niż same półki dyskowe wraz z dyskami;  • Możliwość rozbudowy oferowanego modelu macierzy do minimum 500 dysków bez migracji i przenoszenia danych - jedynie poprzez wymianę modułu kontrolerów macierzy (bez konieczności wymiany posiadanych dysków, półek dyskowych, bez konieczności przenoszenia danych/ istniejącej struktury grup dyskowych/LUN, jak również z zachowaniem istniejącej gwarancji producenta na półki dyskowe i dyski;  • Macierz musi umożliwiać skonfigurowanie dysku hot-spare (dysk zapasowy)  • Macierz musi pozwalać na zaszyfrowanie danych zapisanych na wszystkich obsługiwanych dyskach SSD-SAS i HDD-SAS/NL-SAS minimum kluczem AES256-bit – jeżeli w tym celu niezbędne jest zakupienie dodatkowych licencji bądź komponentów sprzętowych to należy je dostarczyć wraz z macierzą. | | TAK | |  | |
| **Opcje programowe** | | | | | | | |
| **1.** | | • Macierz musi być wyposażona w system kopii migawkowych umożliwiających wykonanie minimum 2048 kopii migawkowych  • Macierz musi umożliwiać zdefiniowanie min. 8000 woluminów (LUN)  • Macierz powinna umożliwiać podłączenie logiczne z serwerami i stacjami poprzez min. 1024 ścieżek logicznych FC  • Macierz musi umożliwiać aktualizację oprogramowania wewnętrznego kontrolerów RAID i dysków bez konieczności wyłączania macierzy oraz bez konieczności wyłączania ścieżek logicznych FC/iSCSI dla podłączonych stacji/serwerów  • Macierz musi umożliwiać dokonywanie w trybie on-line (tj. bez wyłączania zasilania i bez przerywania przetwarzania danych w macierzy) operacje: powiększanie grup dyskowych, zwiększanie rozmiaru woluminu, migrowanie woluminu na inną grupę dyskową  • Macierz musi posiadać wsparcie dla systemów operacyjnych : Microsoft Windows Server 2012R2, 2016, 2019, SuSE Linux Enterprise Server, Red Hat Linux Enterprise Server, HP-UNIX, IBM AIX, SUN Solaris, Vmware Vsphere;  • Macierz musi być dostarczona z licencją na oprogramowanie wspierające technologię typu multipath (obsługa nadmiarowości dla ścieżek transmisji danych pomiędzy macierzą i serwerem) dla połączeń FC i iSCSI.  • Macierz musi posiadać możliwość uruchamiania mechanizmów zdalnej replikacji danych, w trybie synchronicznym i asynchronicznym, po protokołach FC lub IP lub iSCSI, bez konieczności stosowania zewnętrznych urządzeń konwersji wymienionych protokołów transmisji. Funkcjonalność replikacji danych musi być zapewniona z poziomu oprogramowania wewnętrznego macierzy. Replikacja danych musi być obsługiwana w połączeniu z każdą macierzą z tej samej rodziny urządzeń wspierającą obsługę zdalnej replikacji danych. – nie jest wymagane dostarczenie tej funkcjonalności – opcja rozbudowy  • Macierz musi posiadać możliwość tworzenia lokalnych tj. w obrębie zasobów macierzy, pełnych kopii danych (tzw. klony danych), kopii przyrostowych oraz kopii lustrzanych (mirror) – nie jest wymagane dostarczenie tej funkcjonalności – opcja rozbudowy  • Macierz musi obsługiwać mechanizm ochrony priorytetów obsługi wybranych zasobów – za taki mechanizm uznaje się funkcję typu ‘cache partitioning’ lub ‘storage partitioning’.  • Macierz musi obsługiwać adresację IP v.4 i IP v.6  • Macierz musi wspierać obsługę mechanizmów Vmware  • Macierz musi obsługiwać mechanizmy Thin Provisioning, czyli przydziału dla obsługiwanych środowisk woluminów logicznych o sumarycznej pojemności większej od sumy pojemności dysków fizycznych zainstalowanych w macierzy.  • Macierz musi obsługiwać mechanizmy typu AST (Automated Storage Tiering) tj. automatycznego migrowania i realokacji bloków danych pomiędzy różnymi technologiami dyskowymi na podstawie analizy częstotliwości operacji I/O dla tych bloków oraz wg potrzeb wydajnościowych serwerów, środowisk i aplikacji korzystających z zasobów macierzy. Mechanizm AST musi być obsługiwany przy korzystaniu zarówno z trzech jak z dwóch dostarczonych technologii dyskowych: SSD, SSAS, NLSAS.  • Macierz musi wspierać usługi VSS (Volume ShadowCopy Services) w systemach klasy Microsoft Windows Sever – wymagane jest dostarczenie niezbędnego oprogramowania / sterowników VSS pozwalających na obsługę VSS przy maksymalnej pojemności i liczbie dysków obsługiwanych przez oferowaną. W czasie trwania gwarancji wymaga się bezpłatnego dostępu do nowych wersji oprogramowania i sterowników  • Macierz musi obsługiwać mechanizmy migracji danych w trybie online z innej macierzy .  • Macierz wspiera rozwiązania klasy ‘klastra macierzowego’ tj. zapewnienia wysokiej dostępności zasobów dyskowych macierzy dla podłączonych platform software’owych i sprzętowych z wykorzystaniem synchronicznej replikacji danych pomiędzy minimum 2 macierzami protokołami FC. Mechanizm klastra macierzowego musi być obsługiwany dla protokołów FC, zarówno w zakresie replikacji danych jak i w zakresie sposobu podłączenia serwerów do zasobów macierzy. Pod użytym pojęciem ‘wysoka dostępność zasobów dyskowych’ należy rozumieć zapewnienie bezprzerwowego działania środowiska (aplikacja/ system operacyjny/ serwer) podłączonego do macierzy (macierz podstawowa) w przypadku wystąpienia awarii logicznego połączenia z tą macierzy bądź awarii samej macierzy, powodujących dla danego środowiska brak dostępu do zasobów macierzy podstawowej. Funkcjonalność ‘klastra macierzowego’ musi pozwalać na automatyczne i ręczne przełączanie obsługi środowisk produkcyjnych z macierzy podstawowej na zapasową w przypadku awarii macierzy podstawowej (tzw. Automated/manual failover). – nie jest wymagane dostarczenie tej funkcjonalności – opcja rozbudowy | | TAK | |  | |
| **Zarządzanie** | | | | | | | |
| **1.** | | • Oprogramowanie do zarządzania musi być zintegrowane z systemem operacyjnym systemu pamięci masowej  • Komunikacja z wbudowanym oprogramowaniem zarządzającym macierzą musi być możliwa w trybie graficznym np. poprzez przeglądarkę WWW oraz w trybie tekstowym.  • Musi być możliwe zdalne zarządzanie macierzą z wykorzystaniem standardowej przeglądarki internetowej (np. Internet Explorer, Google Chrome, Mozilla Firefox) bez konieczności instalacji żadnych dodatkowych aplikacji na stacji administratora  • Wbudowane oprogramowanie macierzy musi obsługiwać połączenia z modułem zarządzania macierzy poprzez szyfrowanie komunikacji protokołami: SSL dla komunikacji poprzez przeglądarkę WWW i protokołem SSH dla komunikacji poprzez CLI | | TAK | |  | |
| **Gwarancja i serwis** | | | | | | | |
| **1.** | | Gwarancja 5 Lat  • Macierz musi pochodzić z oficjalnego kanału sprzedaży producenta w UE. Nie dopuszcza się użycia macierzy odnawianych, demonstracyjnych lub powystawowych  • Producent oferowanej macierzy musi posiadać dedykowaną, ogólnie dostępną stronę internetową | | TAK | |  | |

|  |  |  |  |
| --- | --- | --- | --- |
| **4. Przełącznik dystrybucyjny- 10 szt.** | | | |
| **Lp.** | **Wymagane minimalne parametry techniczne** | **Wymóg do spełnienia (warunek graniczny)** | **OFEROWANE PARAMETRY TECHNICZNE - podaje**  **Wykonawca**  **Wymogi dotyczące opisu oferowanych parametrów:**  TAK – wykonawca spełnia konkretny parametr przy czym Zamawiający oczekuje by w przypadku wymagań dotyczących minimalnych parametrów opisać szczegółowo parametry oferowane przez wykonawcę  NIE – wykonawca nie spełnia konkretnego parametru |
| **OBUDOWA** | | | |
| **1.** | Wysokość przełącznika 1U w systemie montażu w szafie typu Rack 19” , wraz z kompletem odpowiednich szyn | TAK |  |
| **PORTY** | | | |
| **1.** | - RJ-45 10/100/1000: 24 szt PoE  - SFP+ Porty Uplink: 4szt  - RJ-45 lub USB Port konsoli: 1szt | TAK |  |
| **WYDAJNOŚĆ** | | | |
| **1.** | - Możliwość przełączania: min. 104Gb/s  - Szybkość przekazywania: min. 77Mbps  - min. Flash: 128 MB  - min. DRAM: 256MB  - min. Tablica adresów MAC: 16K  - Jumbo Frames: min 9KB  - Auto-negocjacja, Auto- MDI/MDIX | TAK |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **FUNKCJONALNOŚĆ WARSTWY II** | | | |
| **1.** | Autonegocjacja szybkości portów i trybu dupleksu  Kontrola przepływu:  - IEEE 802.3x for full duplex mode  - Back-Pressure for half duplex mode  - Protokół Spanning Tree:  - IEEE 802.1D Spanning Tree Protocol (STP)  - IEEE 802.1w Rapid Spanning Tree Protocol (RSTP)  - IEEE 802.1s Multiple Spanning Tree Protocol (MSTP)  - BPDU Guard  - BPDU filtering  - Root Guard  - Broadcast/Multicast/Unknown Unicast Storm Control  - VLANy:  - Supports 4K IEEE 802.1Q VLANs  - Active VLANs: 4K  - Port-basedGVRPI  - EEE 802.1v Protocol-based VLANs  - Mac-based VLANs  - IP based VLAN  - Link Aggregation:  - Static Trunk  - IEEE 802.3ad Link Aggregation Control Protocol  - Trunk groups: 16  - Maximum number of members per group: 8  - IGMP Snooping:  - IGMP v1/v2/v3 snooping  - IGMP proxy  - IGMP Filtering  - IGMP Throttling  - IGMP Immediate Leave  - IGMP Querier  - MVR (Multicast VLAN Registration)  - Supports QinQ | TAK |  |
| **Quality of Service** | | | |
| **1.** | - Kolejkowanie priorytetowe: 8 sprzętowe kolejki na każdym porcie  - Klasyfikacja ruchu oparta na IEEE 802.1p CoS, DSCP  - Obsługa WRR | TAK |  |
| **Bezpieczeństwo** | | | |
| **1.** | - Port security  - IEEE 802.1X port based and MAC based authentication  - MAC authentication  - Access Control List  - DHCP Snooping  - IP Source Guard  - Dynamic ARP Inspection  - RADIUS authentication  - TACACS + authorization and accounting  - SSH (v1.5/v2.0)  - SSL and HTTPS | TAK |  |
| **Zarządzanie** | | | |
| **1.** | Zarządzenie przełącznikiem:  - CLI poprzez port console port or Telnet  - WEB management  - SNMP v1, v2c, v3  Firmware & konfiguracja:  - Aktualizacja firmware z wykorzystaniem serwera TFTP  - Automatyczna aktualizacja firmware  - Dual image  - Automatyczne pobieranie konfiguracji z serwera  - Kilka plików konfiguracyjnych na jednym urządzeniu  - Wysyłanie i pobieranie konfiguracji poprzez serwer TFTP  Obsługa:  - RMON (groups 1, 2, 3 and 9)  - BOOTP, DHCP client dla przypisywania adresów IP  - SNTP (RFC 2030)  - Event/Error Log/Syslog  - Obsługa LLDP (802.1ab) | TAK |  |
| **IEEE Standardy** | | | |
| **1.** | - IEEE 802.1p Priority tags - IEEE 802.1x Port Authentication - IEEE 802.3z CSMA/CD access method and physical laye rspecifications for 1000BASE Gigabit Ethernet - IEEE 802.1q Virtual LAN - IEEE 802.1d Spanning Tree Protocol - IEEE 802.3ad Link Aggregation Control Protocol - IEEE 802.1s Rapid Spanning Tree Protocol - IEEE 802.1w Multiple Spanning Tree Protocol | TAK |  |
| **Kompatybilność elektromagnetyczna** | | | |
| **1.** | - FCC klasa A  - CE | TAK |  |
| **Zasilanie** | | | |
| **1.** | - 100-240 VAC, 50/60Hz | TAK |  |
| **GWARANCJA** | | | |
| **1.** | Gwarancja 5 Lat | TAK |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **5. Przełącznik 48 portowy- 1 szt.** | | | |
| **Lp.** | **Wymagane minimalne parametry techniczne** | **Wymóg do spełnienia (warunek graniczny)** | **OFEROWANE PARAMETRY TECHNICZNE - podaje**  **Wykonawca**  **Wymogi dotyczące opisu oferowanych parametrów:**  TAK – wykonawca spełnia konkretny parametr przy czym Zamawiający oczekuje by w przypadku wymagań dotyczących minimalnych parametrów opisać szczegółowo parametry oferowane przez wykonawcę  NIE – wykonawca nie spełnia konkretnego parametru |
| **OBUDOWA** | | | |
| **1.** | Wysokość przełącznika 1U w systemie montażu w szafie typu Rack 19” , wraz z kompletem odpowiednich szyn | TAK |  |
| **PORTY** | | | |
| **1.** | - RJ-45 10/100/1000: 48 szt  - SFP+ Porty Uplink: 4szt  - RJ-45 lub USB Port konsoli: 1szt | TAK |  |
| **WYDAJNOŚĆ** | | | |
| **1.** | - Możliwość przełączania: min. 104Gb/s  - Szybkość przekazywania: min. 77Mbps  - min. Flash: 128 MB  - min. DRAM: 256MB  - Tablica adresów min. MAC: 16K  - Jumbo Frames: min 9KB  - Auto-negocjacja, Auto- MDI/MDIX | TAK |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **FUNKCJONALNOŚĆ WARSTWY II** | | | |
| **1.** | Autonegocjacja szybkości portów i trybu dupleksu  Kontrola przepływu:  - IEEE 802.3x for full duplex mode  - Back-Pressure for half duplex mode  - Protokół Spanning Tree:  - IEEE 802.1D Spanning Tree Protocol (STP)  - IEEE 802.1w Rapid Spanning Tree Protocol (RSTP)  - IEEE 802.1s Multiple Spanning Tree Protocol (MSTP)  - BPDU Guard  - BPDU filtering  - Root Guard  - Broadcast/Multicast/Unknown Unicast Storm Control  - VLANy:  - Supports 4K IEEE 802.1Q VLANs  - Active VLANs: 4K  - Port-basedGVRPI  - EEE 802.1v Protocol-based VLANs  - Mac-based VLANs  - IP based VLAN  - Link Aggregation:  - Static Trunk  - IEEE 802.3ad Link Aggregation Control Protocol  - Trunk groups: 16  - Maximum number of members per group: 8  - IGMP Snooping:  - IGMP v1/v2/v3 snooping  - IGMP proxy  - IGMP Filtering  - IGMP Throttling  - IGMP Immediate Leave  - IGMP Querier  - MVR (Multicast VLAN Registration)  - Supports QinQ | TAK |  |
| **Quality of Service** | | | |
| **1.** | - Kolejkowanie priorytetowe: 8 sprzętowe kolejki na każdym porcie  - Klasyfikacja ruchu oparta na IEEE 802.1p CoS, DSCP  - Obsługa WRR | TAK |  |
| **Bezpieczeństwo** | | | |
| **1.** | - Port security  - IEEE 802.1X port based and MAC based authentication  - MAC authentication  - Access Control List  - DHCP Snooping  - IP Source Guard  - Dynamic ARP Inspection  - RADIUS authentication  - TACACS + authorization and accounting  - SSH (v1.5/v2.0)  - SSL and HTTPS | TAK |  |
| **Zarządzanie** | | | |
| **1.** | Zarządzenie przełącznikiem:  - CLI poprzez port console port or Telnet  - WEB management  - SNMP v1, v2c, v3  Firmware & konfiguracja:  - Aktualizacja firmware z wykorzystaniem serwera TFTP  - Automatyczna aktualizacja firmware  - Dual image  - Automatyczne pobieranie konfiguracji z serwera  - Kilka plików konfiguracyjnych na jednym urządzeniu  - Wysyłanie i pobieranie konfiguracji poprzez serwer TFTP  Obsługa:  - RMON (groups 1, 2, 3 and 9)  - BOOTP, DHCP client dla przypisywania adresów IP  - SNTP (RFC 2030)  - Event/Error Log/Syslog  - Obsługa LLDP (802.1ab) | TAK |  |
| **IEEE Standardy** | | | |
| **1.** | - IEEE 802.1p Priority tags  - IEEE 802.1x Port Authentication  - IEEE 802.3z CSMA/CD access method and physical laye rspecifications for  1000BASE Gigabit Ethernet  - IEEE 802.1q Virtual LAN  - IEEE 802.1d Spanning Tree Protocol  - IEEE 802.3ad Link Aggregation Control Protocol  - IEEE 802.1s Rapid Spanning Tree Protocol  - IEEE 802.1w Multiple Spanning Tree Protocol | TAK |  |
| **Kompatybilność elektromagnetyczna** | | | |
| **1.** | - FCC klasa A - CE | TAK |  |
| **Zasilanie** | | | |
| **1.** | - 100-240 VAC, 50/60Hz | TAK |  |
| **GWARANCJA** | | | |
| **1.** | Gwarancja 5 Lat | TAK |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **6. Przełącznik portowy Switch FC- 2 szt.** | | | |
| **Lp.** | **Wymagane minimalne parametry techniczne** | **Wymóg do spełnienia (warunek graniczny)** | **OFEROWANE PARAMETRY TECHNICZNE - podaje**  **Wykonawca**  **Wymogi dotyczące opisu oferowanych parametrów:**  TAK – wykonawca spełnia konkretny parametr przy czym Zamawiający oczekuje by w przypadku wymagań dotyczących minimalnych parametrów opisać szczegółowo parametry oferowane przez wykonawcę  NIE – wykonawca nie spełnia konkretnego parametru |
| **OGÓLNE** | | | |
| **1.** | Wysokość przełącznika 1U w systemie montażu w szafie typu Rack 19” | TAK |  |
| **2.** | Ilość portów SFP: 24 szt. porty uniwersalne o maksymalnej przepustowości 32GB/s, z obsługą przepustowości 16Gbit/s, 8Gbit/s i 4Gbit/s z automatycznym wyborem przepustowości (auto-sensing),  obsługa trybu full-duple | TAK |  |
| **3.** | 8 aktywnych portów | TAK |  |
| **4.** | Zainstalowane moduły optyczne 8 szt. SFP 16Gbit/s, Short Wave Length (SWL), Multi Mode Fibre (MMF) | TAK |  |
| **5.** | Obsługa trybów pracy portów FC: D\_port, F\_port, E\_port, M-Port | TAK |  |
| **6.** | Obsługa funkcji POD (Ports on Demand) przydziału licencji dla aktywnych portów FC | TAK |  |
| **7.** | Możliwość aktualizacji firmware’u switcha | TAK |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **8.** | Aktywne funkcje: Webtools, Advanced Zoning, FullFabric (z obsługą do minimum 128 przełączników FC) | TAK |  |
| **9.** | Możliwość obsługi funkcjonalności (przez zakupienie odpowiednich licencji): Trunking, Extended Fabric, Fabric Vision | TAK |  |
| **10.** | Zarządzanie min.:   * RJ-45 min 10/100 Mb/s do zarządzania poprzez sieć Ethernet * RJ-45 lub DB9 do zarządzania poprzez interfejs RS232 * USB * In-band over FC | TAK |  |
| **11.** | Sygnalizacja aktywnych i podłączonych portów na panelu przednim urządzenia | TAK |  |
| **12.** | Zarządzanie poprzez przeglądarkę WWW z obsługą połączeń szyfrowanych 128-bit SSL oraz poprzez usługę SSH | TAK |  |
| **13.** | Wsparcie dla protokołu SNMP v.3 | TAK |  |
| **14.** | Gwarancja 5 Lat | TAK |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **7. Licencje dostępowe serwerów- 100 szt.** | | | |
| **Lp.** | **Wymagane minimalne parametry techniczne** | **Wymóg do spełnienia (warunek graniczny)** | **OFEROWANE PARAMETRY TECHNICZNE - podaje**  **Wykonawca**  **Wymogi dotyczące opisu oferowanych parametrów:**  TAK – wykonawca spełnia konkretny parametr przy czym Zamawiający oczekuje by w przypadku wymagań dotyczących minimalnych parametrów opisać szczegółowo parametry oferowane przez wykonawcę  NIE – wykonawca nie spełnia konkretnego parametru |
| **1.** | Licencje dostępowe do serwera wirtualizacji z punktu 1. – 50 szt. | TAK |  |
| **2.** | Licencje umożliwiające podłączenie się do serwera wirtualizacji z punktu 1. poprzez zdalny dostęp – 50 szt. | TAK |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **8. Szafa RACK – 1 szt.** | | | | | |
| **Lp.** | **Wymagane minimalne parametry techniczne** | **Wymóg do spełnienia (warunek graniczny)** | | **OFEROWANE PARAMETRY TECHNICZNE - podaje**  **Wykonawca**  **Wymogi dotyczące opisu oferowanych parametrów:**  TAK – wykonawca spełnia konkretny parametr przy czym Zamawiający oczekuje by w przypadku wymagań dotyczących minimalnych parametrów opisać szczegółowo parametry oferowane przez wykonawcę  NIE – wykonawca nie spełnia konkretnego parametru | |
| **OGÓLNE** | | | | | |
| **1.** | 42U pojemności użytecznej do instalacji urządzeń w pozycji poziomej o wymiarach nie mniejszych niż 600mmx1000mm(Szer/gł) | TAK | |  | |
| **2.** | wyposażona w przednie drzwi perforowane, zamykane na zamek z kluczem, jednoskrzydłowe, możliwość montażu lewa/prawa strona, możliwość zdjęcia bez użycia narzędzi | TAK | |  | |
| **3.** | wyposażona w tylne drzwi perforowane, dwuskrzydłowe dla ograniczenia przestrzeni serwisowej, zamykane na zamek z kluczem wspólny z zamkiem przednim, możliwość zdjęcia bez użycia narzędzi | TAK | |  | |
| **4.** | Minimalna klasa ochrony na poziomie IP 20 | TAK | |  | |
| **5.** | wyposażona w zdejmowane panele boczne | TAK | |  | |
| **6.** | wszystkie wolne „U” zaślepione zaślepkami | TAK |  | |
| **7.** | przystosowana do poprawnej instalacji dostarczonych serwerów rack wraz z ich fabrycznymi prowadnicami przewodów. | TAK |  | |
| **8.** | zainstalowane 2 listwy zasilające min. 8 gniazd ,2 półki o głębokości min. 450mm | TAK |  | |
| **9.** | Minimalny udźwig szafy co najmniej 900 kg | TAK |  | |
| **10.** | Certyfikaty CE, RoHS | TAK |  | |

|  |  |  |  |
| --- | --- | --- | --- |
| **9. Zasilacz awaryjny UPS – 1 szt.** | | | |
| **Lp.** | **Wymagane minimalne parametry techniczne** | **Wymóg do spełnienia (warunek graniczny)** | **OFEROWANE PARAMETRY TECHNICZNE - podaje**  **Wykonawca**  **Wymogi dotyczące opisu oferowanych parametrów:**  TAK – wykonawca spełnia konkretny parametr przy czym Zamawiający oczekuje by w przypadku wymagań dotyczących minimalnych parametrów opisać szczegółowo parametry oferowane przez wykonawcę  NIE – wykonawca nie spełnia konkretnego parametru |
| **OGÓLNE** | | | |
| **1.** | Typ zasilacza: online | TAK |  |
| **2.** | Możliwość montażu w szafie RACK przy zajętości maksymalnie 3U | TAK |  |
| **3.** | Moc pozorna 5kVA | TAK |  |
| **4.** | Moc rzeczywista 4,5 kW | TAK |  |
| **5.** | Minimalne podtrzymanie- 3 minuty przy 100% obciążeniu | TAK |  |
| **6.** | Minimalne podtrzymanie- 10 minuty przy 50% obciążeniu | TAK |  |
| **7.** | W standardzie minimum:  - min. 6x IEC 320 C13 (10A)  - min. 2x IEC 320 C19 (16A)  - 1x RJ45 | TAK |  |
| **8.** | Aplikacja do automatycznego zamykania wspieranych systemów operacyjnych w przypadku braku zasilania | TAK |  |
| **9.** | Możliwość wymiany akumulatorów podczas pracy | TAK |  |
| **10.** | Wspierane i certyfikowane systemy operacyjne: Microsoft® Windows Server® 2012 R2, SUSE Linux Enterprise Server, Red Hat Enterprise Linux, VMware Infrastructure | TAK |  |
| **11.** | Zarządzanie przez SNMP | TAK |  |
| **12.** | Automatyczny wewnętrzny bypass | TAK |  |
| **13.** | Możliwość dołączenia baterii wydłużających czas podtrzymania zasilania | TAK |  |
| **14.** | Wyświetlacz LCD na froncie urządzenia, umożliwiający zarządzanie i monitoring urządzenia | TAK |  |
| **15.** | Certyfikaty: CE, CB | TAK |  |
| **16.** | Gwarancja 5 Lat | TAK |  |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **10. Centrum Autoryzacji – 1 szt. składające się z:**  ***A. Oprogramowanie umożliwiające szyfrowanie wrażliwych danych*** | | | | | | | |
| **Lp.** | | **Wymagane minimalne parametry techniczne** | | **Wymóg do spełnienia (warunek graniczny)** | | **OFEROWANE PARAMETRY TECHNICZNE - podaje**  **Wykonawca**  **Wymogi dotyczące opisu oferowanych parametrów:**  TAK – wykonawca spełnia konkretny parametr przy czym Zamawiający oczekuje by w przypadku wymagań dotyczących minimalnych parametrów opisać szczegółowo parametry oferowane przez wykonawcę  NIE – wykonawca nie spełnia konkretnego parametru | |
| **FUNKCJONALNOŚCI** | | | | | | | |
| **1.** | | Tworzenie głównego drzewa Root CA | | TAK | |  | |
| **2.** | | Tworzenie podrzędnych drzew do wystawiania certyfikatów na  dane danej jednostki organizacyjnej w danym przedsiębiorstwie | | TAK | |  | |
| **3.** | | Tworzenie klastra awaryjnego (fail-over) | | TAK | |  | |
| **4.** | | Nielimitowane czasowo działanie oprogramowania bez dokupowania licencji przedłużających | | TAK | |  | |
| **5.** | | Nielimitowane wydawanie, zawieszanie, zastrzeganie i  odwoływanie certyfikatów | | TAK | |  | |
| **6.** | | Instalacje oraz tworzenie nowych szablonów certyfikatów | | TAK | |  | |
| **7.** | | Automatyczne generowanie i wystawianie certyfikatów dla  urządzeń mobilnych korzystających z sieci wireless | | TAK | |  | |
| **8.** | | Konfiguracja list crl oraz wyrywkowej kontroli ważności certyfikatu  za pomocą usługi ocsp | | TAK | |  | |
| **9.** | | Odwoływanie wystawionych już certyfikatów z możliwością  czasowego ich zawieszenia na dany okres czasu | | TAK | |  | |
| **10.** | | Generowanie certyfikatów na podstawie istniejących już domyślnie szablonów certyfikatów minimum takich jak:   * administrator * Authenticated Session * Basic EFS * CA Exchange | | TAK | |  | |
|  | | * CEP Encryption * Code Signing * Computer * Cross-Certification Authority * Directory E-mail Replication * Domain Controller * Domain Controller Authentication * EFS Recovery Agent * Enrollment Agent * Enrollment Agent (Computer) * Exchange Enrollment Agent (Offline request) * Exchange Signature Only * Exchange User * IPSec * IPSec (Offline request) * Kerberos Authentication * Key Recovery Agent (KRA) * OCSP Response Signing * Remote Access Service (RAS) and Internet Authentication Service   (IAS) Server   * Root CA * Router (Offline request) * Smart Card Logon * Smart Card User * Subordinate CA * Trust List Signing * User * User Signature Only * Web Server * Workstation Authentication | |  | |  | |
| **WSPIERANE ALGORYTMY** | | | | | | | |
| **1.** | | SHA1, SHA2 (SHA256, SHA384, SHA512) | | TAK | |  | |
| **2.** | | RSA o długości 1024, 2048 oraz 4096 | | TAK | |  | |
| **3.** | | ECC/ECDSA NIST P-256, P-384, P-521 | | TAK | |  | |

|  |  |  |  |
| --- | --- | --- | --- |
| **WYMAGANIA TECHNICZNE** | | | |
| **1.** | Interfejs graficzny GUI do obsługi oprogramowania | TAK |  |
| **2.** | Wsparcie dla systemów operacyjnych dostarczanych w ramach postępowania. | TAK |  |
| ***B. Sieciowy moduł bezpieczeństwa umożliwiający przechowywanie newralgicznego materiału kryptograficznego*** | | | |
| **OBUDOWA** | | | |
| **1.** | Wysokość nie większa niż 2U, dostosowana do montażu w szafie 19” | TAK |  |
| **BEZPIECZEŃSTWO** | | | |
| **1.** | FIPS 140- 2 poziom 3 | TAK |  |
| **OBSŁUGA SYSTEMÓW OPERACYJNYCH** | | | |
| **1.** | Wsparcie minimum dla systemów typu Windows Server 2008 R2 / 2012 R2 / 2016, Red Hat Enterprise Linux Server 5 i 6 | TAK |  |
| **PORTY** | | | |
| **1.** | 2x RJ45 1000 BASE-T umożliwiające stworzenie wirtualnego numeru IP rozkładającego ruch na dwa interfejsy | TAK |  |
| **2.** | 1x VGA | TAK |  |
| **3.** | 1x USB 2.0 | TAK |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **OBSŁUGA INTERFEJSÓW** | | | |
| **1.** | PKCS#11 | TAK |  |
| **2.** | MSCAPI | TAK |  |
| **3.** | Java JCA/JCE API | TAK |  |
| **OBSŁUGA ALGORYTMÓW KRYPTOGRAFICZNYCH** | | | |
| **1.** | Kryptografia symetryczna: AES, DES, Triple-DES | TAK |  |
| **2.** | Kryptografia asymetryczna: DSA, ECDSA, RSA | TAK |  |
| **3.** | Funkcje skrótu: SHA-1, SHA-2, SHA-3, RIPEMD | TAK |  |
| **INTEGRACJA** | | | |
| **1.** | Moduł musi udostępniać dodatkowe API umożliwiające integrację z:   * PKCS#11 * Java Cryptographic Extensions (JCE) * Microsoft Crypto API (CSP) * Cryptography Next Generation (CNG) | TAK |  |
| **FUNKCJONALNOŚCI** | | | |
| **1.** | Nielimitowana ilość aplikacji klienckich korzystających z modułu. | TAK |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **2** | Urządzenie musi :   * wspierać silną autoryzacje użytkownika w celach administracyjnych, do autoryzacji wymaga się dwóch dedykowanych kart producenta wraz z certyfikowanym czytnikiem posiadającym PIN pad do wprowadzania PIN-u karty. * wspierać backup głównego klucza (Master Backup Key) i mieć możliwość jego zapisu do pliku, oraz na dedykowane karty   producenta z dedykowaną przestrzenią na Główny klucz szyfrujący  (Master Backup Key). | TAK |  |
| **3.** | Możliwość zarządzania modułem na bazie ról oraz autoryzację opartą o podział sekretu do autoryzacji w trybie “n of m” | TAK |  |
| **CERTYFIKATY** | | | |
| **1.** | FIPS 140-2 Level 3 | TAK |  |
| **2.** | CE, FCC Class B | TAK |  |
| **3.** | UL, IEC/EN 60950-1 | TAK |  |
| **4.** | CB certificate | TAK |  |
| **5.** | RoHS II, WEEE | TAK |  |
| **WYPOSAŻENIE DODATKOWE** | | | |
| **1.** | Minimum 10 szt. dedykowanych do urządzenia kart | TAK |  |
| **2.** | Dedykowany czytnik kart | TAK |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **GWARANCJA** | | | |
| **1.** | Gwarancja 5 Lat | TAK |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **7. Wymagania wdrożeniowe** | | | |
| **Lp.** | **Minimalne wymagania wdrożeniowe** | **Wymóg do spełnienia (warunek graniczny)** | **POTWIERDZENIE ZAOFEROWANIA MINIMALNYCH**  **WYMAGAŃ WZDROŻENIOWYCH - podaje Wykonawca**  **Wymogi dotyczące opisu oferowanych parametrów:**  TAK – wykonawca spełnia konkretny parametr przy czym Zamawiający oczekuje by w przypadku wymagań dotyczących minimalnych parametrów opisać szczegółowo parametry oferowane przez wykonawcę  NIE – wykonawca nie spełnia konkretnego parametru |
| **OGÓLNE** | | | |
| **1.** | Montaż opisanego przedmiotu zamówienia w szafach typu Rack Zamawiającego w sposób zgodny z zaleceniami producenta  dostarczanych urządzeń oraz prowadzenie kabli nie może powodować zaburzeń w cyrkulacji gorącego powietrza wydmuchiwanego z serwerów. | TAK |  |
| **2.** | Stworzenie klastra serwerów w oparciu o oprogramowanie wirtualizacyjne dostarczane w ramach postępowania.  Fizyczne serwery mają zostać skonfigurowane w trybie wysokiej dostępności (awaria jednego serwera nie może powodować  niedostępności usług uruchomionych na dostarczanych w postępowaniu serwerach).  Dane serwerów będą przechowywane na dostarczanych macierzach. | TAK |  |
| **3.** | Testy niezawodności środowiska serwerowego poprzez odłączanie jednej ze ścieżki/wyłączanie urządzenia oraz test redundancji  Zasilania | TAK |  |
| **4.** | Centrum autoryzacji (CA) musi zostać skonfigurowane w sposób zgodny z zaleceniami producenta sprzętowego modułu  bezpieczeństwa. | TAK |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **5** | Minimalne wymagania do wykonania w ramach uruchomienia Centrum Autoryzacji przeprowadzone przez Wykonawcę:   * instalacja urządzenia LAN w miejscu wskazanym przez zamawiającego * inicjalizacja urządzenia (procedurę bootstrap) * integracja z Centrum Autoryzacji za pomocą interfejsu CSP * konfiguracja głównego Urzędu Certyfikacyjnego * integracja z wbudowanym (wymaganym) w serwer modułem bezpieczeństwa umożliwiając tworzenie backupów – z urządzenia LAN na kartę PCI-e * instruktaż z obsługi urządzenia bezpieczeństwa obejmujący min.:   + Pierwsze uruchomienie i rozruch - procedura BootStrap.   + Inicjalizacja Sprzętowego Modułu Bezpieczeństwa - wygenerowanie kart administracyjnych dla głównych administratorów.   + Zarządzanie użytkownikami i autoryzacją.   + Konfiguracja dostępu do LAN Sprzętowego Modułu   Bezpieczeństwa po protokole SSH do zarządzania poprzez sieć LAN   * + Dołączanie dodatkowego magazynu danych na klucze kryptograficzne z HSM   + Administracja poprzez Comand Line Interface VS Graphic User Interface   + Tworzenie kopi bezpieczeństwa i odzyskiwanie.   + Inicjalizacja komunikacji z Sprzętowym Modułem Bezpieczeństwa po PCS#11, CSP. * podział kluczy kryptograficznych szyfrujących cały materiał krypograficzny znajdujący się w pamięci urządzenia na minimum 4 karty inteligentne * PIN do każdej karty powinien zostać zmieniony po przeprowadzonym wdrożeniu. * użytkownik administracyjny Sprzętowego Modułu   Bezpieczeństwa musi logować się na „dwie ręce” – procedura logowania musi wymagać dwóch użytkowników/kart.   * miejscem składowania materiały kryptograficznego powinna być pamięć wewnętrzna Sprzętowego Modułu Bezpieczeństwa. | TAK |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **6.** | Proces konfiguracji Centrum Autoryzacji zakłada wydanie certyfikatu Root CA w jednostce lidera projektu (Szpital Międzyrzecki Sp. z o.o.) oraz musi zostać wydany certyfikat SubCA z kluczem na urządzeniu HSM dostarczanym do Samodzielnego Publicznego Zakładu Opieki Zdrowotnej w Sulęcinie.  Finalnie SubCA musi wydawać certyfikaty dla użytkowników Szpitala Zamawiającego. | TAK |  |
| **7.** | Wymaga konfiguracja akcji shutdown na zasilaczach awaryjnych dostarczanych w ramach postępowania w przypadku braku  zasilania z sieci dla klastra serwerów jak i pojedynczych urządzeń wspierających tę funkcję. | TAK |  |
| **8.** | Aktualizacja sterowników do najnowszych na dzień wdrożenia. | TAK |  |
| **9.** | Do macierzy należy podłączyć wszystkie serwery fizyczne w taki sposób, aby fizyczne i wirtualne maszyny uruchomione na serwerach fizycznych mogły korzystać z dysków macierzy w możliwie najszybszy sposób. | TAK |  |
| **10.** | Instalacja systemów operacyjnych na 3 serwerach fizycznych,  podstawowa konfiguracja serwerów, w tym kart sieciowych. | TAK |  |
| **11.** | Konfiguracja macierzy dyskowej, w tym skonfigurowanie RAID  na poszczególnych grupach dyskowych. | TAK |  |
| **12.** | Instruktaż Zespołu Informatycznego odnośnie przeprowadzonego wdrożenia systemu informatycznego na dostarczanym sprzęcie. | TAK |  |

**Uwaga! Dokument wymaga kwalifikowanego podpisu elektronicznego osób uprawnionych do reprezentacji wykonawcy, a w przypadku oferty wspólnej - pełnomocnika wykonawców.**