

Specyfikacja warunków zamówienia

I.Serwer:

1. Obudowa

Obudowa Rack o wysokości max 2U. Możliwość instalacji minimum 12 dysków 3.5". Komplet wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych oraz organizatorem do kabli.

Obudowa musi mieć możliwość wyposażenia w kartę umożliwiającą dostęp bezpośredni poprzez urządzenia mobilne - serwer musi posiadać możliwość konfiguracji oraz monitoringu najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej min. (Android/ Apple iOS) przy użyciu jednego z protokołów BLE/ WIFI.

2. Płyta główna

Płyta główna z możliwością zainstalowania do dwóch procesorów 3rd Generacji Intel Xeon. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym.

3. Chipset

Dedykowany przez producenta procesora do pracy w serwerach dwuprocessorowych

4. Procesor

Zainstalowane dwa procesory min. 8-rdzeniowe klasy x86, min. 3.2GHz, dedykowane do pracy z zaoferowanym serwerem umożliwiające osiągnięcie wyniku min. 139 w teście SPECrate2017_int_base, dostępnym na stronie www.spec.org dla konfiguracji dwuprocessorowej

5. RAM

Minimum 64GB DDR4 RDIMM 3200MT/s, na płycie głównej powinno znajdować się minimum 32 sloty przeznaczone do instalacji pamięci. Płyta główna powinna obsługiwać do 8TB pamięci RAM.

6. Funkcjonalność pamięci RAM

Advanced ECC, Memory Page Retire, Fault Resilient Memory, Memory Self-Healing lub PPR, Partial Cache Line Sparing

7. Gniazda PCI

Min. 8 slotów PCIe generacji 4

8. Interfejsy sieciowe/FC/SAS

Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT oraz 2 interfejsy sieciowe 10Gb Ethernet w standardzie SFP+ (porty nie mogą być osiągnięte poprzez karty w slotach PCIe)

Dodatkowa, dwuportowa karta 10Gb Ethernet w standardzie SFP+

Dodatkowa, dwuportowa karta 16Gb Fibre Channel

9. Dyski twarde

Zainstalowane 10 dysków SATA o pojemności min. 16TB, 6Gb, Hot-Plug.

Zainstalowane dwa dyski M.2 SATA SSD na dedykowanej karcie (nie zajmujące slotów na dyski twarde) o pojemności min. 240GB Hot-Plug z możliwością konfiguracji RAID 1

Możliwość zainstalowania dedykowanego modułu dla hypervisora wirtualizacyjnego, wyposażony w 2 nośniki typu flash o pojemności min. 64GB, z możliwością konfiguracji zabezpieczenia synchronizacji pomiędzy

nośnikami z poziomu BIOS serwera, rozwiązanie nie może powodować zmniejszenia ilości wnek na dyski twarde.

10. Kontroler RAID

Sprzętowy kontroler dyskowy, posiadający min. 8GB nieulotnej pamięci cache, możliwe konfiguracje poziomów RAID: 0, 1, 5, 6, 10, 50, 60. Wsparcie dla dysków samoszyfrujących.

11. Zintegrowane porty

- 4x USB, w tym min. 1 porty USB 3.0
- 2x port VGA (jeden na panelu przednim)
- Możliwość rozbudowy o Serial Port

12. Video

Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1280x1024

13. Wentylatory

Redundantne, Hot-Plug

14. Zasilanie

Redundantne, Hot-Plug min. 1400W każdy.

15. System operacyjny/System wirtualizacji

Microsoft Windows Serwer 2022 Standard

lub równoważny spełniający min. poniższe wymagania:

- Licencja musi uprawniać do uruchamiania serwerowego systemu operacyjnego w środowisku fizycznym i dwóch wirtualnych środowiskach serwerowego systemu operacyjnego za pomocą wbudowanych mechanizmów wirtualizacji.
- Możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności min. 64TB przez każdy wirtualny serwerowy system operacyjny.
- 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.
- Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy.
- Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy.
- Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.
- Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy.
- Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading;
- Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.
- Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.
- Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET.
- Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.
- Wbudowana zaporę internetową (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.

- Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe.
- Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 2 języków poprzez wybór z listy dostępnych lokalizacji.
- Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).
- Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.
- Wsparcie dostępu do zasobu dyskowego SSO poprzez wiele ścieżek (Multipath).
- Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego.
- Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.
- Możliwość migracji konfiguracji systemu Microsoft Windows Serwer 2022/2016.

16. Bezpieczeństwo

- Zatrask górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardej.
- Możliwość wyłączenia w BIOS funkcji przycisku zasilania.
- BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła
- Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą.
- Moduł TPM 2.0
- Możliwość dynamicznego włączania i wyłączania portów USB na obudowie – bez potrzeby restartu serwera
- Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem

17. Diagnostyka

Serwer wyposażony w panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS'u, zasilaniu oraz temperaturze.

18. Karta Zarządzania

Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca:

- zdalny dostęp do graficznego interfejsu Web karty zarządzającej;
- zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera);
- szyfrowane połączenie (TLS) oraz autentykację i autoryzację użytkownika;
- możliwość podmontowania zdalnych wirtualnych napędów;
- wirtualną konsolę z dostępem do myszy, klawiatury;
- wsparcie dla IPv6;
- wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish;
- możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer;
- możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer;
- integracja z Active Directory;

- możliwość obsługi przez dwóch administratorów jednocześnie;
 - wsparcie dla dynamic DNS;
 - wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej.
 - możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera
- możliwość zarządzania do 100 serwerów bezpośrednio z konsoli karty zarządzającej pojedynczego serwera

19. Oprogramowanie do zarządzania

Możliwość zainstalowania oprogramowania producenta do zarządzania, spełniającego poniższe wymagania:

- Wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych
- integracja z Active Directory
- Możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta
- Wsparcie dla protokołów SNMP, IPMI, Linux SSH, Redfish
- Możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram
- Szczegółowy opis wykrytych systemów oraz ich komponentów
- Możliwość eksportu raportu do CSV, HTML, XLS, PDF
- Możliwość tworzenia własnych raportów w oparciu o wszystkie informacje zawarte w inwentarzu.
- Grupowanie urządzeń w oparciu o kryteria użytkownika
- Tworzenie automatycznie grup urządzeń w oparciu o dowolny element konfiguracji serwera np. Nazwa, lokalizacja, system operacyjny, obsadzenie slotów PCIe, pozostałego czasu gwarancji
- Możliwość uruchamiania narzędzi zarządzających w poszczególnych urządzeniach
- Szybki podgląd stanu środowiska
- Podsumowanie stanu dla każdego urządzenia
- Szczegółowy status urządzenia/elementu/komponentu
- Generowanie alertów przy zmianie stanu urządzenia.
- Filtry raportów umożliwiające podgląd najważniejszych zdarzeń
- Integracja z service desk producenta dostarczonej platformy sprzętowej
- Możliwość przejęcia zdalnego pulpitu
- Możliwość podmontowania wirtualnego napędu
- Kreator umożliwiający dostosowanie akcji dla wybranych alertów
- Możliwość importu plików MIB
- Przesyłanie alertów „as-is” do innych konsol firm trzecich
- Możliwość definiowania ról administratorów
- Możliwość zdalnej aktualizacji oprogramowania wewnętrznego serwerów
- Aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania)

- Możliwość instalacji oprogramowania wewnętrznego bez potrzeby instalacji agenta
- Możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów
- Moduł raportujący pozwalający na wygenerowanie następujących informacji: nr seryjne sprzętu, konfiguracja poszczególnych urządzeń, wersje oprogramowania wewnętrznego, obsadzenie slotów PCI i gniazd pamięci, informację o maszynach wirtualnych, aktualne informacje o stanie i poziomie gwarancji, adresy IP kart sieciowych, występujących alertów, MAC adresów kart sieciowych, stanie poszczególnych komponentów serwera.
- Możliwość tworzenia sprzętowej konfiguracji bazowej i na jej podstawie weryfikacji środowiska w celu wykrycia rozbieżności.
- Wdrażanie serwerów, rozwiązań modularnych oraz przełączników sieciowych w oparciu o profile
- Możliwość migracji ustawień serwera wraz z wirtualnymi adresami sieciowymi (MAC, WWN, IQN) między urządzeniami.
- Tworzenie gotowych paczek informacji umożliwiających zdiagnozowanie awarii urządzenia przez serwis producenta.
- Zdalne uruchamianie diagnostyki serwera.
- Dedykowana aplikacja na urządzenia mobilne integrująca się z wyżej opisanymi oprogramowaniem zarządzającym.

Oprogramowanie dostarczane jako wirtualny appliance dla KVM, ESXi i Hyper-V.

20. Certyfikaty

Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015, ISO-50001 oraz ISO-14001

Serwer musi posiadać deklaracja CE.

Oferowane produkty muszą zawierać informacje dotyczące ponownego użycia i recyklingu, nie mogą zawierać farb i powłok na dużych plastikowych częściach, których nie da się poddać recyklingowi lub ponownie użyć. Wszystkie produkty zawierające podzespoły elektroniczne oraz niebezpieczne składniki powinny być bezpiecznie i łatwo identyfikowalne oraz usuwalne. Usunięcie materiałów i komponentów powinno odbywać się zgodnie z wymogami Dyrektywy WEEE 2002/96/EC. Produkty muszą składać się z co najmniej w 65% ze składników wielokrotnego użytku/zdatnych do recyklingu. We wszystkich produktach części tworzyw sztucznych większe niż 25-gramowe powinny zawierać nie więcej niż śladowe ilości środków zmniejszających palność sklasyfikowanych w dyrektywie RE 67/548/EEC. Potwierdzeniem spełnienia powyższego wymogu jest wydruk ze strony internetowej www.epeat.net potwierdzający spełnienie normy co najmniej Epeat Bronze według normy wprowadzonej w 2019 roku - **Wykonawca złoży dokument potwierdzający spełnienie wymogu.**

Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Microsoft Windows Server 2016, Microsoft Windows Server 2019, Microsoft Windows Server 2022.

21. Dokumentacja użytkownika

Zamawiający wymaga dokumentacji w języku polskim lub angielskim.

Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.

22. Warunki gwarancji

5 lat gwarancji producenta

Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie, przez Internet oraz z wykorzystaniem aplikacji.

Zamawiający oczekuje rozpoczęcia diagnostyki telefonicznej / internetowej już w momencie dokonania zgłoszenia. Certyfikowany Technik wykonawcy / producenta z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) ma rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym (NBD) od otrzymania zgłoszenia / zakończenia diagnostyki. Naprawa ma się odbywać w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę.

Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania producenta, w tym także sprzedanego oprogramowania.

Zgłoszenie przyjęte jest potwierdzane przez zespół pomocy technicznej (mail/telefon / aplikacja / portal) przez nadanie unikalnego numeru zgłoszenia pozwalającego na identyfikację zgłoszenia w trakcie realizacji naprawy i po jej zakończeniu.

Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy.

Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia oraz pobieranie uaktualnień mikro kodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji serwera.

Zamawiający oczekuje nieodpłatnego udostępnienia narzędzi serwisowych i procesów wsparcia umożliwiających: Wykrywanie usterek sprzętowych z predykcją awarii.

Automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych.

Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wsparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego.

Możliwość rozszerzenia gwarancji przez producenta do 7 lat.

Firma serwisująca musi posiadać ISO 9001:2015 oraz ISO-27001 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty.

Wymagane dołączenie do oferty oświadczenia Producenta potwierdzając, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta.

II.Przełącznik Fibre Channel:

1. Przełącznik FC musi być wykonany w technologii FC minimum 32 Gbs i zapewniać możliwość pracy portów FC z prędkościami 32, 16, 8, 4 Gbs w zależności od rodzaju zastosowanych wkładek SFP.
2. Dostarczony przełącznik FC musi być wyposażony w min. 16 aktywnych portów FC obsadzonych 16 wkładkami SFP+ 16Gbs SWL.
3. Przełącznik musi umożliwiać w przyszłości rozbudowę do co najmniej 24 aktywnych portów w ramach tej samej obudowy. Przyszła rozbudowa musi odbywać się za pomocą aktywacji portów za pomocą odpowiedniej licencji i instalacji dodatkowych wkładek SFP+.
4. Wszystkie zaoferowane porty przełącznika FC muszą umożliwiać działanie bez tzw. oversubskrypcji gdzie wszystkie porty w maksymalnie rozbudowanej konfiguracji przełącznika wyposażonej we wkładki 32Gbs mogą pracować równocześnie z pełną prędkością 32Gb/s.
5. Całkowita przepustowość przełącznika FC dostępna dla maksymalnie rozbudowanej konfiguracji (24 porty) wyposażonej we wkładki 32Gbs musi wynosić minimum 768 Gb/s end-to-end.
6. Oczekiwana wartość opóźnienia przy przesyłaniu ramek FC między dowolnymi portami przełącznika nie może być większa niż 900ns.

7. Rodzaj obsługiwanych portów, co najmniej: E, D oraz F.
8. Przełącznik FC powinien wydmuchiwać gorące powietrze od strony portów FC.
9. Przełącznik FC musi mieć wysokość maksymalnie 1 RU (jednostka wysokości szafy montażowej) i szerokość 19" oraz zapewniać techniczną możliwość montażu w szafie 19". Wraz z przełącznikiem należy dostarczyć odpowiedni zestaw montażowy do szafy 19".
10. Maksymalny dopuszczalny pobór mocy przełącznika FC wyposażonego w 24 aktywne porty 32Gbps to 77W.
11. Maksymalna ilość ciepła wydzielanego przez przełącznik FC wyposażony w 24 aktywne porty 32Gbps to 215 BTU na godzinę.
12. Przełącznik FC musi posiadać możliwość obsługi mechanizmu agregacji połączeń ISL między dwoma przełącznikami i tworzenia w ten sposób logicznych połączeń typu ISL Trunk o przepustowości minimum 256 Gb/s half duplex (dla wkładek 32Gbs) dla każdego logicznego połączenia. Load balancing ruchu między fizycznymi połączeniami ISL w ramach połączenia logicznego typu trunk musi być realizowany na poziomie pojedynczych ramek FC a połączenie logiczne musi zachowywać kolejność przesyłanych ramek. Nie trzeba dostarczać licencji aktywującej opisaną tu funkcjonalność.
13. Przełącznik FC musi obsługiwać mechanizm balansowania ruchu, pomiędzy co najmniej 16 różnymi połączeniami o tym samym koszcie wewnątrz wielodomenowych sieci fabric, przy czym balansowanie ruchu musi odbywać się w oparciu o 3 parametry nagłówka ramki FC: DID, SID i OXID.
14. Przełącznik FC musi posiadać możliwość jednoczesnej obsługi mechanizmów ISL Trunk oraz balansowania ruchu w oparciu o DID/SID/OXID. Nie trzeba dostarczać licencji aktywującej opisaną tu funkcjonalność.
15. Przełącznik FC musi realizować sprzętową obsługę zioningu (przez tzw. układ ASIC) na podstawie portów i adresów WWN.
16. Przełącznik FC musi mieć możliwość wymiany i aktywacji wersji firmware'u (zarówno na wersję wyższą jak i na niższą) w czasie pracy urządzenia i bez zakłócenia przesyłanego ruchu FC.
17. Przełącznik FC musi wspierać następujące mechanizmy zwiększające poziom bezpieczeństwa:
 - mechanizm tzw. Fabric Binding, który umożliwia zdefiniowanie listy kontroli dostępu regulującej prawa przełączników FC do uczestnictwa w sieci fabric
 - uwierzytelnianie (autentykacja) przełączników w sieci Fabric za pomocą protokołów DH-CHAP i FCAP
 - uwierzytelnianie (autentykacja) urządzeń końcowych w sieci Fabric za pomocą protokołu DH-CHAP
 - szyfrowanie połączenia z konsolą administracyjną. Wsparcie dla SSHv2.
 - definiowanie wielu kont administratorów z możliwością ograniczenia ich uprawnień za pomocą mechanizmu tzw. RBAC (Role Based Access Control)
 - definiowanie kont administratorów w środowisku RADIUS, LDAP w MS Active Directory, Open LDAP, TACACS+
 - szyfrowanie komunikacji narzędzi administracyjnych za pomocą SSL/HTTPS
 - obsługa SNMP v1 oraz v3
 - IP Filter dla portu administracyjnego przełącznika
 - wgrywanie nowych wersji firmware przełącznika FC z wykorzystaniem bezpiecznych protokołów SCP oraz SFTP
 - wykonywanie kopii bezpieczeństwa konfiguracji przełącznika FC z wykorzystaniem bezpiecznych protokołów SCP oraz SFTP

18. Przełącznik FC musi mieć możliwość konfiguracji przez:
- polecenia tekstowe w interfejsie znakowym konsoli terminala
 - przeglądarkę internetową z interfejsem graficznym lub dedykowane oprogramowanie.
19. Przełącznik FC musi być dostarczony z następującymi narzędziami diagnostycznymi i mechanizmami obsługi ruchu FC:
- logowanie zdarzeń poprzez mechanizm „syslog”,
 - port diagnostyczny tzw. D_port. Port diagnostyczny musi umożliwiać wykonanie testów sprawdzających komunikację portu przełącznika z wkładką SFP, połączenie optyczne pomiędzy dwoma przełącznikami, testowe obciążenie połączenia pełną przepustowością 16Gbps/32Gbps oraz pomiar opóźnienia i odległości między przełącznikami z dokładnością co najmniej do 5m dla wkładek SFP 16Gbps lub 32Gbps. Testy wykonywane przez port diagnostyczny nie mogą wpływać w żaden sposób na działanie pozostałych portów przełącznika i całej sieci fabric.
 - FCping
 - FC traceroute
 - kopiowanie danych wymienianych pomiędzy dwoma wybranymi portami na inny wybrany port przełącznika
20. Przełącznik FC musi posiadać możliwość przydzielenia, co najmniej 1700 tzw. buffer credits do wybranego portu FC przełącznika. Nie trzeba dostarczać licencji aktywującej opisaną tu funkcjonalność.
21. Przełącznik FC musi zapewnić możliwość jego zarządzania przez zintegrowany port Ethernet, RS232 oraz inband IP-over-FC.
22. Przełącznik FC musi zapewniać obsługę protokołu NVMe over FC.
23. Przełącznik FC musi zapewniać obsługę interfejsu zarządzającego REST API.
24. Przełącznik FC musi realizować kategoryzację ruchu między parami urządzeń (initiator - target) oraz przydzielenie takich par urządzeń do kategorii o wysokim, średnim lub niskim priorytecie. Konfiguracja przydziału do różnych klas priorytetów musi się odbywać za pomocą standardowych narzędzi do konfiguracji zoniingu.
25. Przełącznik FC musi realizować kategoryzację ruchu na podstawie wartości parametru CS_CTL w nagłówku ramki FC oraz odpowiednie przydzielenie ramki do kategorii o wysokim, średnim lub niskim priorytecie.
26. Wsparcie dla N_Port ID Virtualization (NPIV). Obsługa, co najmniej 255 wirtualnych urządzeń na pojedynczym porcie przełącznika.
27. Gwarancja:
- 5 lata gwarancji producenta
 - Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie, przez Internet oraz z wykorzystaniem aplikacji.
 - Zamawiający oczekuje rozpoczęcia diagnostyki telefonicznej / internetowej już w momencie dokonania zgłoszenia. Certyfikowany Technik wykonawcy / producenta z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) ma rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym (NBD) od otrzymania zgłoszenia / zakończenia diagnostyki. Naprawa ma się odbywać w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę.
 - Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania producenta, w tym także sprzedanego oprogramowania.

- Zgłoszenie przyjęte jest potwierdzane przez zespół pomocy technicznej (mail/telefon / aplikacja / portal) przez nadanie unikalnego numeru zgłoszenia pozwalającego na identyfikację zgłoszenia w trakcie realizacji naprawy i po jej zakończeniu.
- Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy.
- Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia.
- Automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych.
- Firma serwisująca musi posiadać ISO 9001:2015 oraz ISO-27001 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty.
- Wymagane dołączenie do oferty oświadczenia Producenta potwierdzając, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta.

III. W ramach dostawy należy wykonać poniższe prace w środowisku IT Zamawiającego.

1. Wykonawca zapewni w swoim zakresie okablowanie sieciowe(kable eth, patchcorty eth, światłowodowe, wkładki sfp+, sfp) i zasilające do podpięcia z istniejącym środowiskiem Zamawiającego,
2. W nowym środowisku zestawionym z posiadanych przez Zamawiającego dwóch serwerów HP DL560 G10 oraz macierzy HP 3PAR8200 należy:
 - przeprowadzić rekonfigurację polegającą na utworzeniu odpowiedniej ilości jednostek LUN, zgodnie z wymaganiami Zamawiającego, z uwzględnieniem dobrych praktyk zalecanych przez producenta
 - spiąć elementy środowiska przy użyciu dostarczonego przez Wykonawcę oraz posiadanego przez Zamawiającego switchy FC, w sposób zapewniający pełną redundancję w przypadku uszkodzeń sprzętu i awarii w sieci
 - przeprowadzić upgrade firmware urządzeń do najnowszego (zalecanego przez producenta sprzętu) na dzień instalacji
 - wykonać niezbędne testy odporności na wystąpienia przypadkowych awarii
 - zmigrować w 100% stare środowisko VMWare 6.0, złożone z dwóch serwerów HP DL980 G7 oraz macierzy HP 3PAR7200, do przekonfigurowanego przez Wykonawcę nowego środowiska. Migracji będzie podlegać ok. 70 maszyn wirtualnych (Windows, Linux). Na czas migracji Wykonawca zobowiązany jest posiadać możliwość udostępnienia z własnych zasobów przestrzeni dyskowej o wielkości min. 120TB, na którą zostaną zmigrowane maszyny wirtualne w okresie przejściowym, podczas rekonfiguracji urządzeń. Po zakończeniu prac dyski użyte podczas rekonfiguracji pozostaną u Zamawiającego.
3. Dla dostarczonego serwera backupu należy:
 - zainstalować w najnowszej wersji i skonfigurować zgodnie z zaleceniami producenta posiadane przez Zamawiającego oprogramowanie Veeam Backup
 - utworzyć zadania backupu używanych przez Zamawiającego maszyn wirtualnych
 - przeprowadzić optymalizację prędkości wykonywanych backupów zakończoną testami wydajności
 - Wymagania dodatkowe:
 - Wykonawca zagwarantuje backup i bezpieczeństwo danych w okresie przejściowym
 - prace muszą być prowadzone poza godzinami pracy urzędu. W dni robocze w godzinach 18.00 – 6.00, w weekendy bez ograniczeń
 - Zamawiający nie wyraża zgody na całkowite wyłączenie środowiska

