Załącznik nr 1 do SWZ TP 76/2023

Celem projektu jest aktualizacja i rozbudowa posiadanych przez Zamawiającego platform przetwarzania o mechanizmy podnoszące poziom cyberbezpieczeństwa i niezawodności procesów medycznych i biznesowych. Projekt zakłada implementację i konfigurację w środowisku IT Zamawiającego szeregu systemów i technologii umożliwiających zapewnienie ciągłości przetwarzania   
i dostępności danych poprzez wprowadzenie odporności wybranych elementów środowisk produkcyjnych lokalizacji Konstancin-Jeziorna (lokalizacja KJ) i Pruszków (lokalizacja P) na brak dostępu do danych i systemów IT spowodowany między innymi:

* awarią sprzętową, zniszczeniem lub czasową niedostępnością produkcyjnego sprzętu warstwy wirtualizacji (serwery, przełączniki, macierze dyskowe),
* uszkodzeniem danych produkcyjnych poprzez utratę urządzeń i/lub nośników, na których się one znajdują lub ich skasowanie, nieuprawnioną modyfikację czy zaszyfrowanie,
* uszkodzeniem lub utratą lokalnych kopii zapasowych,
* niedostępnością całej serwerowni – pojedynczej lokalizacji.

Zakłada się wdrożenie mechanizmów minimalizujących zablokowanie pracy organizacji Zamawiającego spowodowane wymienionymi powyżej czynnikami, poprzez wprowadzenie redundancji danych (w szczególności serwerów wirtualnych) w postaci ich okresowej replikacji do ośrodka zapasowego (z lokalizacji KJ do lokalizacji P oraz z lokalizacji P do lokalizacji KJ) z możliwością ich produkcyjnego uruchomienia w razie zaistnienia takiej potrzeby.

Na aktualną infrastrukturę serwerową warstwy wirtualizacji Zamawiającego składają się niżej wymienione elementy (obie lokalizacje):

• Klaster serwerów VMware wraz z macierzą dyskową hostujący maszyny wirtualne z krytycznymi systemami biznesowymi i medycznymi. Klaster posiada zdolność odporności na awarię pojedynczego serwera fizycznego i redundancję w zakresie elementów składowych macierzy (dyski, kontrolery, zasilacze).

• System kopii zapasowych z oprogramowaniem do wykonywania kopii zapasowych (Veeam Backup & Replication) na dyski repozytoriów backupu. Dodatkowo wybrane dane zabezpieczane są na taśmy i wynoszone okresowo poza pomieszczenie, w którym przetwarzane są dane.

• Redundantne przełączniki sieci LAN i SAN.

Zamawiający wymaga dostarczenia następującego sprzętu oraz licencji:

1. Serwer replikacji – 2 szt.

|  |  |  |
| --- | --- | --- |
| **Parametr** | **Charakterystyka (wymagania minimalne)** | **TAK** |
| **Obudowa** | Obudowa rack o wysokości max. 2U umożliwiającą instalację min. 26 dysków 2,5” z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych oraz organizatorem kabli.  Możliwość wyposażenia obudowy w kartę dostępu bezpośredniego poprzez urządzenia mobilne w celu konfiguracji oraz monitoringu najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej (Android/ Apple iOS) przy użyciu jednego z protokołów BLE/ WIFI. |  |
| **Płyta główna** | Płyta główna z możliwością zainstalowania dwóch procesorów. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym. |  |
| **Chipset** | Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych. |  |
| **Procesor** | Zainstalowane dwa procesory min. ośmiordzeniowe klasy x86 do pracy z zaoferowanym serwerem umożliwiające osiągnięcie wyniku min. 128 punktów w teście SPECrate2017\_int\_base dostępnym na stronie www.spec.org dla dwóch procesorów. |  |
| **RAM** | Min. 512GB DDR4 RDIMM 3200MT/s, na płycie głównej powinno znajdować się minimum 32 slotów przeznaczonych do instalacji pamięci, w tym 16 slotów wolnych/niezajętych. Płyta główna powinna obsługiwać do 8TB pamięci RAM. |  |
| **Zabezpieczenia pamięci RAM** | Memory Health Check, Memory Page Retire. |  |
| **Gniazda PCIe** | Min. cztery sloty PCIe x8 generacji 4 oraz minimum dwa sloty PCIe x16 generacji 4. |  |
| **Interfejsy sieciowe/FC/SAS** | Wbudowane dwa interfejsy sieciowe 1Gb Ethernet w standardzie BaseT.  Dwa interfejsy sieciowe 10Gb Ethernet w standardzie BaseT.  Dwa interfejsy sieciowe 10Gb Ethernet w standardzie SFP+.  Dla każdego portu SFP+ należy dostarczyć kabel direct-attach 10GbE SFP+ o długości min. 3 metrów.  Możliwość instalacji wymiennie modułów udostępniających:   * cztery interfejsy sieciowe 10Gb Ethernet w standardzie SFP+ , * cztery interfejsy sieciowe 1Gb Ethernet w standardzie BaseT, * dwa interfejsy sieciowe 25Gb Ethernet ze złączami SFP28 , * cztery interfejsy sieciowe 25Gb Ethernet ze złączami SFP28.   Dodatkowo zainstalowane:   * dwa interfejsy FC 16Gb/s, * dwa interfejsy SAS 12Gb/s. |  |
| **Dyski twarde** | Zainstalowane min. 18 dysków min. 960GB SSD hot-swap. Min. 6 slotów na dyski z przodu obudowy powinny pozostawać nieobsadzone dyskami w celu umożliwienia dalszej rozbudowy powierzchni dyskowej serwera.  Zainstalowane min. 2 dyski 960GB SSD w sposób nie powodujący zmniejszenia ilości wnęk (na dyski twarde) umieszczonych na przodzie obudowy, skonfigurowane fabrycznie w RAID1.  Możliwość zainstalowania dedykowanego modułu dla hypervisora wirtualizacyjnego, wyposażonego w nośniki typu flash o pojemności min. 64GB, z możliwością konfiguracji zabezpieczenia synchronizacji pomiędzy nośnikami z poziomu BIOS serwera - rozwiązanie nie może powodować zmniejszenia ilości wnęk na dyski twarde. |  |
| **Kontroler RAID** | Sprzętowy kontroler z pojemnością cache min. 8GB, możliwe konfiguracje poziomów RAID: 0, 1, 5, 6, 10, 50, 60. |  |
| **Wbudowane porty** | min. 2x port USB 2.0 oraz port USB 3.0, 2 porty VGA – z przodu i z tyłu obudowy serwera. |  |
| **Video** | Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1920x1200. |  |
| **Wentylatory** | Redundantne Hot-Plug. |  |
| **Zasilacze** | Min. dwa zasilacze Hot-Plug maksymalnie 800W. |  |
| **Bezpieczeństwo** | Zatrzask górnej pokrywy oraz blokada na ramce panelu zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych.  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.  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.  Możliwość integracji z RSA SecurID. |  |
| **Diagnostyka** | Panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS’u, zasilaniu oraz temperaturze. |  |
| **Karta Zarządzania** | Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port RJ-45 Gigabit Ethernet umożliwiająca:   * zdalny dostęp do graficznego interfejsu Web karty zarządzającej, * szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika, * możliwość podmontowania zdalnych wirtualnych napędów, * wirtualną konsolę z dostępem do myszy, klawiatury, * wsparcie dla IPv6, * wsparcie dla SNMP; IPMI2.0, VLAN tagging, SSH, * możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer, dane historyczne powinny być dostępne przez min. 7 dni wstecz, * możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer, * integracja z Active Directory, * możliwość obsługi przez min. czterech administratorów jednocześnie, * wsparcie dla automatycznej rejestracji DNS, * wsparcie dla LLDP, * wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej, * możliwość zarządzania bezpośredniego poprzez złącze microUSB umieszczone na froncie obudowy, * monitorowanie zużycia dysków SSD, * możliwość monitorowania z jednej konsoli min. 100 serwerami fizycznymi, * automatyczne zgłaszanie alertów do centrum serwisowego producenta, * automatyczne update firmware dla wszystkich komponentów serwera, * możliwość przywrócenia poprzednich wersji firmware, * możliwość eksportu eksportu/importu konfiguracji (ustawienie karty zarządzającej, BIOSu, kart sieciowych, HBA oraz konfiguracji kontrolera RAID) serwera do pliku XML lub JSON, * możliwość zaimportowania ustawień, poprzez bezpośrednie podłączenie plików konfiguracyjnych , * automatyczne tworzenie kopii ustawień serwera w oparciu o harmonogram, * możliwość wykrywania odchyleń konfiguracji na poziomie konfiguracji UEFI oraz wersji firmware serwera. |  |
| **System Operacyjny** | Zakres Przedmiotu Zamówienia obejmuje dostarczenie Oprogramowania Systemowego zwanego dalej SSO.  Licencja musi być w wersji najnowszej dostępnej na rynku, nigdy wcześniej nie użytkowana i nieaktywowana na innym urządzeniu.  Licencja ma obejmować wszystkie procesory/rdzenie (i/lub inne elementy sprzętowe) zainstalowane w serwerze - zgodnie z polityką licencjonowania producenta SSO.  SSO ma być fabrycznie zainstalowane przez producenta serwera.  Licencja musi uprawniać do uruchamiania SSO w środowisku fizycznym i dwóch wirtualnych środowisk SSO za pomocą wbudowanych mechanizmów wirtualizacji.  SSO musi posiadać następujące, wbudowane cechy:   1. możliwość wykorzystania, co najmniej 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 min. 64TB przez każdy wirtualny serwerowy system operacyjny, 3. możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania do 8000 maszyn wirtualnych, 4. możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci, 5. wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy, 6. wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy, 7. automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego, 8. możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy (mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading), 9. wbudowane wsparcie instalacji i pracy na wolumenach, które:    1. pozwalają na zmianę rozmiaru w czasie pracy systemu,    2. umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,    3. umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów,    4. umożliwiają zdefiniowanie list kontroli dostępu (ACL), 10. wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość, 11. wbudowane szyfrowanie dysków, 12. możliwość uruchamiania 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. graficzny interfejs użytkownika, 16. zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe, 17. wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play), 18. możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu, 19. dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa, 20. możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:     1. podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC,     2. usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji:        1. podłączenie SSO do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną,        2. ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,        3. odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza,     3. zdalna dystrybucja oprogramowania na stacje robocze,     4. praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej,     5. centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:        1. dystrybucję certyfikatów poprzez http,        2. konsolidację CA dla wielu lasów domeny,        3. automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen,     6. szyfrowanie plików i folderów,     7. szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec),     8. możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów,     9. serwis udostępniania stron WWW,     10. wsparcie dla protokołu IP w wersji 6 (IPv6),     11. wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie min. 1000 aktywnych środowisk wirtualnych systemów operacyjnych. Wirtualne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności. Mechanizmy wirtualizacji mają zapewnić wsparcie dla:         1. dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych,         2. obsługi ramek typu jumbo frames dla maszyn wirtualnych,         3. obsługi 4-KB sektorów dysków,         4. nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra,         5. możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API,         6. możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk model), 21. możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta SSO umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet, 22. wsparcie dostępu do zasobu dyskowego SSO poprzez wiele ścieżek (Multipath), 23. możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego, 24. mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty, 25. możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF.   Wraz z licencją SSO należy dostarczyć właściwą dla SSO licencję dostępową per urządzenie – 1 szt. |  |
| **Certyfikaty** | Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015 oraz ISO-14001.  Serwer musi posiadać deklaracja CE.  Urządzenia wyprodukowane są przez producenta, zgodnie z normą PN-EN ISO 50001.  Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Microsoft Windows 2019 x64, Microsoft Windows 2022 x64. |  |
| **Warunki gwarancji** | Min.5 lat gwarancji producenta czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii w trybie 365x7x24 poprzez ogólnopolską linię telefoniczną producenta.  Zamawiający wymaga od wykonawcy dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego.  Wymagane dołączenie do oferty oświadczenia potwierdzającego, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta.  Sprzęt musi być fabrycznie nowy i pochodzić z oficjalnego kanału dystrybucyjnego producenta.  Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia, oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji systemu.  Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela. |  |
| **Dokumentacja użytkownika** | Zamawiający wymaga dokumentacji w języku polskim lub angi*e*lskim. |  |

1. Przełącznik sieci SAN FC – 2 szt.

|  |  |  |
| --- | --- | --- |
| **Parametr** | **Charakterystyka (wymagania minimalne)** | **TAK** |
| **Obudowa** | Przełącznik FC musi mieć wysokość maksymalnie 1 RU (jednostka wysokości szafy montażowej)  i szerokość 19” oraz zapewniać techniczną możliwość montażu w szafie 19”. |  |
| **Technologia** | Przełącznik FC musi być wykonany w technologii FC 32Gb/s i posiadać możliwość pracy portów FC z prędkościami 16, 8, 4 Gb/s z funkcją autonegocjacji prędkości. |  |
| **Porty** | Przełącznik FC musi posiadać minimum 24 sloty na moduły FC.  Wszystkie wymagane funkcje muszą być dostępne dla min. 16 portów FC przełącznika (min. 16 aktywnych/licencjonowanych portów).  Przełącznik FC musi zapewniać możliwość dynamicznego aktywowania portów za pomocą zakupionych kluczy licencyjnych.  Możliwość wymiany w trybie „na gorąco”: minimum w odniesieniu do modułów portów Fibre Channel (SFP+). |  |
| **Wyposażenie** | Przełącznik musi być dostarczony wraz z:   * 16 szt. modułów SFP+ FC 16 Gb/s, * 8 szt. patchcordów LC-LC OM4 min. 3m, * szyny do montażu w szafie rack. |  |
| **Rodzaj portów** | Rodzaj obsługiwanych portów: D\_Port (ClearLink Diagnostic Port), E\_Port, F\_Port, M\_Port. |  |
| **Obudowa i montaż** | Przełącznik FC musi mieć wysokość maksymalnie 1 RU (jednostka wysokości szafy montażowej) i szerokość 19” oraz zapewniać techniczną możliwość montażu w szafie 19”. |  |
| **Architektura ruchu** | Przełącznik FC musi być wykonany w tzw. architekturze „non-blocking” uniemożliwiającej blokowanie się ruchu wewnątrz przełącznika przy pełnej prędkości pracy wszystkich portów. |  |
| **Grupowanie połączeń** | Przełącznik musi posiadać mechanizm balansowania ruchu między grupami połączeń tzw. „trunk” oraz obsługiwać grupy połączeń „trunk” o różnych długościach. |  |
| **Strefy (zoninng)** | Przełącznik FC musi udostępniać usługę Name Server Zoning - tworzenia stref (zon) w oparciu bazę danych nazw serwerów, na podstawie portów i adresów WWN |  |
| **Firmware** | Przełącznik FC musi posiadać możliwość wymiany i aktywacji wersji firmware’u (zarówno na wersję wyższą jak i na niższą) w czasie pracy urządzenia, bez wymogu ponownego uruchomienia urządzeń w sieci SAN. |  |
| **Bezpieczeństwo** | Przełącznik FC musi posiadać wsparcie dla następujących mechanizmów zwiększających poziom bezpieczeństwa:   * Możliwość uwierzytelnienia (autentykacji) przełączników z listy kontroli dostępu w sieci Fabric za pomocą protokołów DH-CHAP i FCAP, * Szyfrowanie komunikacji narzędzi administracyjnych za pomocą SSL/HTTPS, * IPsec, * Kontrola dostępu administracyjnego definiująca możliwość zarządzania przełącznikiem tylko z określonych urządzeń oraz portów - IP filtering, * Wsparcie dla autentykacji LDAP z IPv6, * Open LDAR, * Port Binding, * Konta użytkowników definiowane w środowisku RADIUS, * TACACS+, * Listy Kontroli Dostępu definiujące urządzenia (przełączniki i urządzenia końcowe) uprawnione do pracy w sieci Fabric - Role-based Access Control (RBAC), * Secure Copy (SCP), * Secure RPC, * Secure Syslog, * Szyfrowanie połączenia z konsolą administracyjną. Wsparcie dla SSH v2, * Switch Binding, * Trusted Switch. |  |
| **Diagnostyka** | Przełącznik FC musi posiadać wsparcie dla następujących mechanizmów:   * elektryczny/optyczny loopback, * ruch/opóźnienia/odległość na linku, * flow mirroring, * wbudowany generator przepływu, * diagnostyka POST and wbudowana online/offline z monitoringiem środowiskowym, * FC ping and Pathinfo (FC traceroute), * Podgląd ramek, * Monitorowanie stanu optyki, * Monitorowanie zasilania, * Logowanie RAS trace, * Rolling Reboot Detection (RRD). |  |
| **Zarządzanie** | Przełącznik FC musi posiadać możliwość konfiguracji przez komendy tekstowe w interfejsie znakowym oraz przez przeglądarkę internetową z interfejsem graficznym.  Przełącznik FC musi zapewnić możliwość jego zarządzania przez zintegrowany port Ethernet, RS232 oraz inband IP-over-FC.  Przełącznik FC musi zapewniać wsparcie dla standardu zarządzającego SMI-S v1.1 (powinien zawierać agenta SMI-S zgodnego z wersją standardu v1.1).  Przełącznik FC musi zapewniać możliwość nadawania adresu IP dla zarządzającego portu Ethernet za pomocą protokołu DHCP.  Obsługa SNMP v3. |  |
| **Obsługa wkładek SFP+** | Przełącznik FC musi mieć możliwość instalacji jednomodowych SFP+ umożliwiających bezpośrednie połączenie (bez dodatkowych urządzeń pośredniczących) z innymi przełącznikami na odległość minimum 10km. |  |
| **Zasilacz** | Przełącznik musi posiadać wbudowany zasilacz. Maksymalny dopuszczalny pobór mocy przełącznika FC to 77W. |  |
| **Wirtualizacja portów** | Wsparcie dla N\_Port ID Virtualization (NPIV). Obsługa co najmniej 255 wirtualnych urządzeń na pojedynczym porcie przełącznika. |  |
| **Warunki gwarancji** | Min. 5 lat gwarancji realizowanej w miejscu instalacji sprzętu, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii poprzez ogólnopolską linię telefoniczną producenta.  Wymagane dołączenie do oferty oświadczenia potwierdzającego, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta.  Sprzęt musi pochodzić z oficjalnego kanału dystrybucyjnego producenta.  Możliwość telefonicznego sprawdzenia statusu gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela. |  |
| **Dokumentacja użytkownika** | Zamawiający wymaga dokumentacji w języku polskim lub angielskim. |  |

1. Przełącznik sieci LAN – 2 szt.

|  |  |  |
| --- | --- | --- |
| **Parametr** | **Charakterystyka (wymagania minimalne)** | **TAK** |
| **Porty** | Przełącznik wyposażony w porty:   * 12 x 10 Gigabit Ethernet BaseT * 3 x 100 Gigabit Ethernet QSFP28 * 1 port konsolowy RJ45 * 1 port ethernet RJ-45, out-of-band management * 1 port USB |  |
| **System operacyjny** | Modularny system operacyjny.  Przełącznik musi być zgodny ze standardem ONIE i umożliwiać instalacje systemów operacyjnych innych producentów, w celu uzyskania dodatkowych funkcjonalności. |  |
| **Zasilanie** | 2 redundantne zasilacze AC |  |
| **Obudowa** | Obudowa 1U do instalacji w szafie rack 19’’ |  |
| **Pamięć** | Pamięć CPU: 4GB  Pojemność bufora pakietów: 12MB |  |
| **Wydajność** | Musi posiadać matrycę przełączającą o wydajności min. 840Gbps (full-duplex), przepustowość 625 Mpps. |  |
| **Chłodzenie** | Musi posiadać możliwość chłodzenia urządzenia w trybie przód-do-tyłu (ustawienia fabryczne).  Temperatura pracy w przedziale 5-40 stopni Celcjusza |  |
| **Funkcjonalności warstwy II** | Musi obsługiwać, co najmniej 4000 VLANów.  Obsługa min. 270 000 adresów MAC.  Musi obsługiwać, co najmniej protokoły: STP, RSTP, PVST+, MSTP.  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.   Urządzenie musi posiadać możliwość definiowana łączy w grupy LAG (802.3ad). Obsługa min. 16 łączy w grupie LAG.  Musi obsługiwać DCB (Data Center Bridging), 802.1Qbb Priority-Based Flow Control, funkcjonalność DCB oraz PFC i ECN.  Musi zapewniać sprzętowe wsparcie dla L3 VXLAN routing.  Musi być zgodny z następującymi standardami IEEE:  802.1AB LLDP  TIA-1057 LLDP-MED  802.1s MSTP  802.1w RSTP  802.3ab Gigabit Ethernet (1000Base-T)  802.3ad Link Aggregation with LACP  802.3ae 10 Gigabit Ethernet (10GBase-X)  802.3ba 40 Gigabit Ethernet (40GBase-X)  802.3i Ethernet (10Base-T)  802.3u Fast Ethernet (100Base-TX)  802.3z Gigabit Ethernet (1000BaseX)  802.1D Bridging, STP  802.1p L2 Prioritization  802.1Q VLAN Tagging, Double VLAN Tagging, GVRP  802.1Qbb PFC  802.1Qaz ETS  802.1s MSTP  802.1w RSTP PVST+  802.1X Network Access Control  802.3ab Gigabit Ethernet (1000BASE-T) or breakout  802.3ac Frame Extensions for VLAN Tagging  802.3ad Link Aggregation with LACP  802.3ae 10 Gigabit Ethernet (10GBase-X)  802.3ba 40 Gigabit Ethernet (40GBase- SR4, 40GBase-CR4, 40GBase-LR4, 100GBase-SR10, 100GBase-LR4, 100GBase-ER4) on optical ports  802.3bj 100 Gigabit Ethernet  802.3u Fast Ethernet (100Base-TX) na porcie zarządzania  802.3x Flow Control |  |
| **Funkcjonalności warstwy III** | Musi obsługiwać protokoły dynamicznego routing dla IPv4 i dla IPv6: OSPF, BGP.  Musi obsługiwać protokół BFD, przynajmniej dla protokłu OSPF i OSFP v3.  Musi przechowywać minimum 200 000 wpisów rotingu IPv4 i minimum 130 000 wpisów routigu IPv6.  Musi wspierać mechanizm L3 ECMP Load Balancing.  Musi wspierać protokół redundancji VRRP.  Wsparcie dla DHCP server i DHCP Relay.  Obsługa Policy Based Routing.  Musi obsługiwać funkcjonalność VxLAN, Static VxLan, BGP eVPN oraz BGP eVPN Layer2 Vxlan Gateway.  Musi obsługiwać poniższe standardy w zakresie protokołów routingu:  791 IPv4  792 ICMP  826 ARP  1027 Proxy ARP  1035 DNS (client)  1042 Ethernet Transmission  1191 Path MTU Discovery  1305 NTPv4  1519 CIDR  1812 Routers  1858 IP Fragment Filtering  2131 DHCP (server and relay)  5798 VRRP  3021 31-bit Prefixes  3046 DHCP Option 82 (Relay)  1812 Requirements for IPv4 Routers  1918 Address Allocation for Private Internets  2474 Diffserv Field in IPv4 and Ipv6 Headers  2596 Assured Forwarding PHB Group  3195 Reliable Delivery for Syslog  3246 Expedited Assured Forwarding  COPP: Control Plane Policing  Policy Based Routing  2460 IPv6  2462 Stateless Address AutoConfig  2463 ICMPv6  2464 Ethernet Transmission  2675 Jumbo grams  3587 Global Unicast Address Format  4291 IPv6 Addressing  2464 Transmission of IPv6 Packets over Ethernet Networks  2711 IPv6 Router Alert Option  4007 IPv6 Scoped Address Architecture  4213 Basic Transition Mechanisms for IPv6 Hosts and Routers  Dla protokołu OSPF:  1587 NSSA  1745 OSPF/BGP interaction  1765 OSPF Database overflow  2154 MD5  2328 OSPFv2  2370 Opaque LSA  3101 OSPF NSSA  Dla protokołu BGP:  1997 BGP Communities  2385 MD5  2439 Route Flap Damping  2796 Route Reflection  2842 Capabilities  2918 Route Refresh  3065 Confederations  4271 BGP-4 |  |
| **Mechanizmy bezpieczeństwa i QoS** | Musi wspierać następujące mechanizmy związane z zapewnieniem, jakości obsługi (QoS) w sieci:   * Klasyfikacja ruchu dla klas różnej, jakości obsługi QoS poprzez wykorzystanie, co najmniej następujących paramentów: źródłowy/docelowy adres MAC, źródłowy/docelowy adres IP, vlan, wartość DSCP. * Implementacja, co najmniej 8 kolejek sprzętowych na każdym porcie wyjściowym dla obsługi ruchu o różnej klasie obsługi. * Możliwość obsługi jednej z powyższych kolejek z bezwzględnym priorytetem w stosunku do innych (Strict Priority). * Implementacja mechanizmu Weighted Random Early Detection (WRED). * Obsługa IP Precedence i DSCP. * Obsługa Control-Plane-Policing (ochrona systemu operacyjnego przd atakami DoS).   Musi wspierać następujące mechanizmy związane z zarządzaniem i zapewnieniem bezpieczeństwa w sieci:   * Co najmniej 3 poziomy dostępu administracyjnego przez konsole, * Autoryzacja użytkowników/portów w oparciu o 802.1x, * Obsługa List dostępu ACL dla adresów MAC i adresów IPv4 i IPv6. |  |
| **Mechanizmy zarządzania** | Musi wspierać następujące mechanizmy zarządzania:   * Możliwość uzyskania dostępu do urządzenia przez SNMPv1/2/3 i SSHv2, * Obsługa monitorowania ruchu na porcie (Port Monitoring), ACL-Based Monitoring oraz RSPAN, * Urządzenie musi posiadać dedykowany port konsolowy do zarządzania typu RJ45 (konsola) oraz drugi wydzielony 10/100/1000BaseT, * Plik konfiguracyjny urządzenia musi być możliwy do edycji ‘off-line’. Tzn. konieczna jest możliwość przeglądania zmian konfiguracji w pliku tekstowym na dowolnym PC. Po zapisaniu konfiguracji w pamięci nieulotnej musi być możliwe uruchomienie urządzenia z nową konfiguracją. Zmiany aktywnej konfiguracji muszą być widoczne bez częściowych restartów urządzania po dokonaniu zmian. * Wsparcie dla mechanizmu Beacon LED control – włączenie diody danego interfejsu celem identyfikacji, * Urządzenie musi posiadać funkcjonalność automatycznej instalacji oprogramowania poprzez ściągnięcie z serwera TFTP pliku z oprogramowaniem (firmware), w trakcie pierwszego podłączenia do sieci Ethernet. |  |
| **Wyposażenie dodatkowe** | Pasywny kabel miedziany DAC QSDP+ do QSFP+ 40GbE min. 0.5m  Wkładka 40GbE QSFP+ SR4 850nm MPO MMF zainstalowana w porcie 100Gb QSFP28 umożliwiająca zastosowanie kabla breakout rozdzielającego port na 4 złącza LC.  Kabel światłowodowy rozdzielający (breakout) MPO na 4 złącza LC, MM, OM4, min. 3m  2 szt. wkładek SFP+ 10GbE i 2 szt. patchcord światłowodowy MM LC-LC OM4 min. 3 m do połączenia switcha z istniejącymi przełącznikami zamawiającego HP 5130. |  |
| **Warunki gwarancji** | Min. 5 lat gwarancji realizowanej w miejscu instalacji sprzętu, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii poprzez ogólnopolską linię telefoniczną producenta.  Wymagane dołączenie do oferty oświadczenia potwierdzającego, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta.  Sprzęt musi pochodzić z oficjalnego kanału dystrybucyjnego producenta.  Możliwość telefonicznego sprawdzenia statusu gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela. |  |
| **Dokumentacja użytkownika** | Zamawiający wymaga dokumentacji w języku polskim lub angielskim. |  |

1. Licencje systemu kopii zapasowej – 1 komplet

Zamawiający wymaga dostarczenia kompletu licencji pozwalających migrację posiadanych przez Zamawiającego licencji wieczystych Veeam Data Platform Essentials Standard Socket-Based, w ilości 5 paczek po 2 CPU (dwie instancje Veeam; 2 kontrakty serwisowe odpowiednio: 3 paczki po 2 CPU i 2 paczki po 2 CPU), do wersji Veeam Data Platform Essentials Subscription Universal License, w ilości 2x 45 obciążeń, w celu dostarczenia funkcjonalności pozwalających na:

* Zabezpieczanie kopią zapasową po 45 szt. obciążeń (w tym: maszyn wirtualnych, serwerów fizycznych) w obu instancjach Veeam w każdej z lokalizacji (KJ i P).
* wykonywanie aplikacyjnie konsystentnych kopii zapasowych z granularnym odzyskiwaniem i backupem logów transakcyjnych SQ/ Oracle,
* szyfrowanie przesyłanych pomiędzy lokalizacjami danych,
* kontrolę opóźnień systemów dyskowych w celu minimalizacji wpływu procesów backupu na wydajność dyskowych macierzy produkcyjnych,
* użycie wbudowanej akceleracja WAN w celu przyspieszenia procesów replikacji pomiędzy lokalizacjami i minimalizacji wykorzystania/obciążenia łącza podczas przesyłania danych replik,
* wykorzystanie wtyczek umożliwiających aplikacyjny backup Oracle RMAN i SAP HANA,
* bezpośredni backup SQL na repozytoria Veeam,
* tworzenie repozytoriów Scale-out (pojedyncze repozytorium złożone z wielu oddzielnych repozytoriów),
* integrację z deduplikatorami (np. DataDomain),
* natywne wsparcie kopii zapasowej na taśmy (backup NAS, retencja GFS, pule taśmowe),
* wykorzystanie funkcjonalności „one-click” failover – plany odtworzenia uruchamiane jednym kliknięciem myszy,
* natychmiastowe odtwarzanie baz SQL i Oracle do danego punktu w czasie,
* porównywanie kopii zapasowych z danymi z produkcji w celu odzyskiwania tylko zmienionych plików,
* granularne odtwarzanie Microsoft Active Directory, Exchange, SQL, SharePoint, Oracle,
* indeksowanie plików w kopii zapasowej,
* automatyczną weryfikację kopii zapasowej po jej wykonaniu,
* automatyczną weryfikację repliki po jej wykonaniu,
* odtwarzanie do wydzielonej „piaskownicy” w celu bezpiecznej analizy/weryfikacji kopii zapasowej.

Wraz z licencjami wymaga się dostarczenia wsparcia producenta na okres min. 3 lat od daty końca aktualnego kontraktu wsparcia posiadanych przez Zamawiającego licencji tj. 16 września 2023 r.

1. Odnowienie na kolejne 5 lat wygasającego w dniu 17 listopada 2023 r. wsparcia typu Basic producenta posiadanych przez Zamawiającego licencji VMware Essentials Plus Kit for 3 hosts, w celu umożliwienia zamawiającemu dostępu do wydawanych przez producenta poprawek związanych z bezpieczeństwem i nowych wersji oraz funkcjonalności systemu zwiększających bezpieczeństwo całego środowiska przetwarzania Zamawiającego.
2. Taśma LTO-6 WORM – 24 szt. wraz z etykietami umożliwiającymi identyfikację taśm przez bibliotekę taśmową i system kopii zapasowej Zamawiającego.
3. Zamawiający wymaga wykonania następujących prac:

* Instalacja dostarczonych urządzeń w szafach rack zamawiającego, podłączenie do istniejących gniazd zasilania i sieci LAN oraz SAN, okablowanie i uruchomienie – w obu lokalizacjach (KJ i P). Dostarczenie niezbędnego okablowania leży po stronie Wykonawcy.
* Upgrade firmware/BIOS/iDRAC dostarczanych urządzeń oraz serwerów Dell użytkowanych przez zamawiającego (w obu lokalizacjach).
* Rozszerzenie sieci SAN FC w lokalizacji KJ zamawiającego o nowe przełączniki FC – rekonfiguracja fabric-ów i zoningu.
* Rozszerzenie sieci LAN o dostarczane przełączniki LAN jako przełączniki rdzeniowe, rekonfiguracja sieci, spięcie dostarczanych przełączników z serwerami i przełącznikami HP Zamawiającego.
* Podniesienie do możliwie najnowszych i wyrównanie wersji środowisk wirtualizacyjnych VMware i kopii zapasowych Veeam w obu lokalizacjach (KJ i P) w oparciu o kontrakty wsparcia i licencje producentów posiadane przez Zamawiającego oraz odnowienia kontraktów wsparcia dostarczane przez Wykonawcę (dotyczy Veeam i VMware).
* Instalacja wirtualizatora VMware na dostarczonych serwerach replikacji w oparciu o licencje posiadane przez zamawiającego i podpięcie ich do istniejących vCenter oraz macierzy w ten sposób, by oprócz funkcji repozytoriów zreplikowanych maszyn wirtualnych, mogły pełnić także funkcję serwerów produkcyjnych w przypadku awarii aktualnie działającego węzła klastrów wysokiej dostępności w każdej z lokalizacji.
* Instalacja i konfiguracja niezbędnych komponentów Veeam jako maszyny wirtualne z dostarczanym wraz z serwerami replikacji Systemem operacyjnym pod obsługę replikacji zgodnie z zaleceniami i dobrymi praktykami producenta systemu kopii zapasowej Veeam.
* Migracja licencji systemu kopii zapasowej Veeam per CPU do Veeam VUL za pomocą dostarczonej licencji.
* Konfiguracja procesów replikacji wskazanych serwerów wirtualnych z jednej lokalizacji do drugiej (i na odwrót) na repozytoria położone na dyskach lokalnych dostarczonych serwerów replikacji w celu implementacji możliwości ich uruchomienia w przypadku awarii czy niedostępności lokalizacji oryginalnej.
* Uporządkowanie procesów kopii zapasowej na zasoby dyskowe i taśmowe w obrębie zasobów posiadanych przez zamawiającego.
* Testy zaimplementowanych rozwiązań.
* Dokumentacja powdrożeniowa.
* Szkolenie stanowiskowe personelu IT zamawiającego z zakresu wdrożonych technologii i mechanizmów pod kątem codziennej administracji i użytkowania zaimplementowanych rozwiązań.