Spis treści

[1. Moduły bezpieczeństwa – 1 komplet 2](#_Toc510692733#_Toc510692733)

[2. Macierze – 1 komplet 3](#_Toc510692734#_Toc510692734)

[2.1. Macierz typ I – 1 szt. 3](#_Toc510692735#_Toc510692735)

[2.2. Macierz typ II – 1 szt. 6](#_Toc510692736#_Toc510692736)

[3. Serwery – 1 komplet 9](#_Toc510692737#_Toc510692737)

[3.1.1. Serwer wirtualizacyjny – 1 szt. 9](#_Toc510692738#_Toc510692738)

[3.1.2. Oprogramowanie do wirtualizacji - 1 szt. 16](#_Toc510692739#_Toc510692739)

[3.1.3. Serwer wraz z infrastrukturą niezbędną do zabezpieczenia e-usług – 1 szt. 18](#_Toc510692740#_Toc510692740)

[3.1.4. Kontroler serwerów – 1 szt. 23](#_Toc510692741#_Toc510692741)

[3.1.5. Licencje dostępowe – 1 komplet (400 sztuk) 26](#_Toc510692742#_Toc510692742)

[3.1.6. Licencje dostępu klienta usług pulpitu zdalnego – 1 komplet (20 sztuk) 26](#_Toc510692743#_Toc510692743)

[4. Przełączniki – 1 komplet 27](#_Toc510692744#_Toc510692744)

[4.1. Przełącznik typ I – 1 komplet (2 sztuki) 27](#_Toc510692745#_Toc510692745)

[4.1.2. Przełącznik typ II – 1 komplet (2 sztuki) 32](#_Toc510692746#_Toc510692746)

[4.1.3. Przełącznik typ III – 1 komplet (14 sztuk) 36](#_Toc510692747#_Toc510692747)

[4.1.4. Przełącznik typ IV – 1 komplet (18 sztuk) 39](#_Toc510692748#_Toc510692748)

[4.1.5. Przełącznik typ V – 1 komplet (2 sztuki) 42](#_Toc510692749#_Toc510692749)

[5. Zasilacz awaryjny – 1 komplet 44](#_Toc510692750#_Toc510692750)

[5.1. Zasilacz awaryjny I – 1 szt. 44](#_Toc510692751#_Toc510692751)

[5.1.2. Zasilacz awaryjny II – 1 szt. 45](#_Toc510692752#_Toc510692752)

[6. Szafa rack - 1 szt. 46](#_Toc510692753#_Toc510692753)

[7. Serwer typu NAS – 1 szt. 47](#_Toc510692754#_Toc510692754)

[8. Oprogramowanie do backupu – 1 komplet 48](#_Toc510692755#_Toc510692755)

1. Moduły bezpieczeństwa – 1 komplet

|  |  |  |
| --- | --- | --- |
| **Lp.** | **Nazwa komponentu** | **Wymagane minimalne parametry techniczne urządzenia** |
| **1** | **2** | **3** |
| 1 | Typ urządzenia | Sieciowy moduł bezpieczeństwa |
| 2 | Obudowa | O wysokości nie większej niż 2 U, dostosowana do montażu w szafie 19” |
| 3 | Bezpieczeństwo | FIPS 140-2 poziom 3 |
| 4 | Obsługa systemów operacyjnych | Wsparcie dla systemów typu Windows Server 2008 R2 / 2012 R2 / 2016, Red Hat Enterprise Linux Server 5 i 6 |
| 5 | Porty | 2x RJ45 1000 BASE-T umożliwiające stworzenie wirtualnego numeru IP rozkładającego ruch na dwa interfejsy  1x VGA  1x USB 2.0 |
| 6 | Obsługa interfejsów | PKCS#11  MSCAPI  Java JCA/JCE API |
| 7 | Obsługa algorytmów kryptograficznych | Kryptografia symetryczna: AES, DES, Triple-DES  Kryptografia asymetryczna: DSA, ECDSA, RSA  Funkcje skrótu: SHA-1, SHA-2, SHA-3, RIPEMD |
| 8 | Integracja | Moduł musi udostępniać dodatkowe API umożliwiające integrację z:  PKCS#11  Java Cryptographic Extensions (JCE)  Microsoft Crypto API (CSP)  Cryptography Next Generation (CNG) |
| 9 | Funkcjonalności | Nielimitowana ilość aplikacji klienckich korzystających z HSM.  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 PINu karty.  Urządzenie musi 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).  Możliwość zarządzania HSM na bazie ról oraz autoryzację opartą o podział sekretu do autoryzacji w trybie “n of m” |
| 10 | Dodatkowe wyposażenie | 10 szt. dedykowanych do urządzenia kart  Dedykowany czytnik kart |
| 11 | Gwarancja | 12 miesięcy |
| 12 | Certyfikaty | FIPS 140-2 Level 3  CE, FCC Class B  UL, IEC/EN 60950-1  CB certificate  RoHS II, WEEE |
| 13 | Wdrożenie | Zamawiający wymaga wdrożenia urządzenia bezpieczeństwa które musi obejmować:  • instalację urządzenia  • inicjalizację urządzenia (procedurę bootstrap)  • integrację z Centrum Autoryzacji, dostarczanym wraz z serwerowym systemem operacyjnym dostarczanym w ramach niniejszego postępowania, za pomocą interfejsu CSP |

1. Macierze – 1 komplet
   1. Macierz typ I – 1 szt.

|  |  |  |
| --- | --- | --- |
| **Lp.** | **Nazwa komponentu** | **Wymagane minimalne parametry techniczne urządzenia** |
| **1** | **2** | **3** |
| 1 | Macierz | Macierz powinna posiadać dwa redundantne kontrolery macierzowe wraz z możliwością instalacji 24 dysków 2,5”, o maksymalnej wysokości 2U, Macierz musi umożliwiać rozbudowę o moduły 12 dysków 3,5” oraz 24 dyski 2,5”  Obsługa minimum 192 dysków SAS/NLSAS lub SSD |
| 2 | Wymagana przestrzeń | Macierz musi być wyposażona w:  7 dysków 2,5” o pojemności 480GB (SSD 12Gb/s)  12 dysków 2,5’’o pojemności 1200GB (SAS 12Gb/s, prędkość obrotowa 10K rpm) |
| 3 | Pamięć podręczna (Cache) | Pamięć podręczna (cache) – 16 GB pojemności użytkowej dla danych oraz informacji kontrolnych na każdy kontroler (sumarycznie 32 GB). Zamawiający nie dopuszcza rozwiązań rozszerzających pamięć podręczną cache dyskami SSD/Flash. |
| 4 | Interfejsy zewnętrzne | Macierz musi być wyposażenia w 4 porty FC 16Gbit/s z modułami FC 16Gbit/s, każdy kontroler macierzy w trybie Active-Active |
| 5 | Dostępność | Odporność na zanik zasilania jednej fazy lub awarię zasilacza macierzy (redundancja układu zasilania). |
| Możliwość łączenia w macierzy różnych poziomów RAID:   * 1. możliwość zastosowania RAID10,   2. możliwość zastosowania RAID5,   3. możliwość zastosowania RAID6   4. możliwość zastosowania RAID0 |
| Podwójne niezależne przyłącza SAS 6Gb/s do wewnętrznych napędów dyskowych. |
| Odporność na awarię pamięci cache – lustrzany zapis danych oraz technologia zapewniająca ochronę danych z pamięci cache w razie utraty zasilania |
| Zdublowanie pozostałych komponentów macierzy, takich jak: kontrolery, wewnętrzne szyny/przełączniki, wentylatory. |
| Możliwość wykonywania wszystkich napraw, rekonfiguracji, rozbudowy i upgrade’ów (zarówno sprzętu jak i oprogramowania macierzy) w trybie online (bez przerywania pracy systemu). |
| Możliwość zdefiniowania min. 4 dysków zapasowych dla każdego typu dysków w zaoferowanej macierzy lub odpowiednia zapasowa przestrzeń dyskowa. |
| 6 | Wspierane systemy operacyjne | Wymagane wsparcie dla różnych systemów operacyjnych, co najmniej AIX, HP-UX, MS Windows, VMware oraz Linux |
| Wymagane wsparcie dla różnych systemów klastrowych, co najmniej Veritas Cluster Server, HACMP, HP Serviceguard, Microsoft Cluster. |
| Wsparcie dla mechanizmów dynamicznego przełączania zadań I/O pomiędzy kanałami w przypadku awarii jednego z nich (path failover). Wymagane jest wsparcie min. dla odpowiednich mechanizmów oferowanych przez producentów systemów operacyjnych: AIX, HP-UX, MS Windows, Vmware, Linux. |
| Macierz musi mieć wsparcie dla automatycznego, bez agenta, odzyskiwania bloków (space reclamation) dla systemu operacyjnego Linux i systemu plików EXT4, NTFS dla Windows 2012, VMFSv5 dla ESX oraz VxFS w przypadku zastosowania technologii Thin Provisioning. |
| 7 | Skalowalność | Wykonywanie rozbudowy sprzętowej w trybie online. |
| Umożliwia rozbudowę do minimum 192 dysków 2,5”. |
| Możliwość rozbudowy macierzy za pomocą nowych dysków o większych pojemnościach oraz dysków typu SSD/Flash – zoptymalizowanych pod kątem zapisu bądź odczytu |
| Macierz musi umożliwiać mieszanie dysków o różnych prędkościach obrotowych w ramach jednej półki dyskowej. |
| 8 | Zarządzanie | Oprogramowanie do zarządzania macierzą przez administratora klienta – graficzny interfejs do monitorowania stanu i konfiguracji macierzy, diagnostyki, mapowania zasobów do serwerów (zarówno podłączanych bezpośrednio jak i przez sieć SAN – LUN Masking). |
| Monitorowanie wydajności macierzy według parametrów takich jak: przepustowość oraz liczba operacji I/O dla interfejsów zewnętrznych, wolumenów logicznych LUN, oraz kontrolerów.  Możliwość zbierania i przechowywania informacji o wydajności macierzy bez ograniczeń czasowych. |
| Możliwość konfigurowania wolumenów logicznych LUN o pojemności użytkowej 250TB. |
| Macierz musi posiadać wbudowaną funkcjonalność typu thin provisioning umożliwiającą alokację wirtualnej przestrzeni dyskowej, do której fizyczne dyski mogą być dostarczone w przyszłości. |
| 9 | Możliwość migracji danych w obrębie macierzy (licencja wymagana) | Konieczne jest posiadanie możliwości uruchomienia automatycznego, bez interwencji człowieka, rozkładania danych między dyskami poszczególnych typów (tzw. auto-tiering). Dane muszą być automatycznie przemieszczane miedzy rożnymi typami dysków oraz rożnymi poziomami RAID w zależności od stopnia obciążenia macierzy dyskowej. Dane często używane macierz powinny automatycznie przemieszczać na dyski o największej prędkości obrotowej, dane rzadko używane na dyski o prędkości obrotowej 1000 rpm. Dodatkowo funkcjonalność ta musi wspierać dyski SSD zoptymalizowane przez producenta dysków do zapisu lub do odczytu. |
| Macierz musi mieć możliwość migracji wolumenów logicznych LUN pomiędzy różnymi grupami dyskowymi RAID w obrębie macierzy. Migracja musi być wykonywana w trybie on-line. |
| Macierz musi umożliwiać tworzenie jednego wolumenu logicznego LUN w obrębie wszystkich produkcyjnych dysków macierzy. Musi również umożliwiać udostępnienie tego wolumenu logicznego LUN po protokole FC |
| 10 | Lokalna replikacja danych | Możliwość tworzenia kopii danych z poziomu macierzy i wewnątrz macierzy bez angażowania systemu operacyjnego hosta. |
| Możliwość tworzenia i utrzymywania jednocześnie minimum ośmiu lokalnych kopii danych wewnątrz macierzy dla każdego urządzenia LUN (tzw. kopie point-in-time) przez administratora. |
| Oferowana macierz dyskowa musi umożliwiać wykonanie lokalnej kopii danych na całej zaoferowanej przestrzeni dyskowej. |
| Wymaga jest również funkcjonalność wykonywania kopii wirtualnych typu snapshot. Jest wymagana licencja na pełną pojemność macierzy oraz maksymalną ilość snapshotów w obrębie macierzy. |
| Kopie migawkowe muszą być wykonywane metodą tzw. bez prealokacji przestrzeni dyskowej (ang. allocate-on-write, a.k.a redirect-on-write). Kopie migawkowe nie mogą być wykonywane metodą COW (ang. Copy On Write) |
| Kopie migawkowe muszą mieć możliwość prezentacji, jako urządzenia LUN w trybie do odczytu i zapisu. Jeżeli ta funkcjonalność wymaga dodatkowej licencji należy ja dostarczyć. |
| 11 | Zdalna replikacja danych (licencja wymagana) | Macierz musi posiadać funkcjonalność zdalnej replikacji danych do macierzy tej samej rodziny w trybie synchronicznym oraz asynchronicznym i asynchronicznym interwałowym bez użycia dodatkowych serwerów lub innych urządzeń.  Macierz musi umożliwiać zestawienie minimum 200 replik w trybie źródła oraz 800 w trybie celu. |
| Oprogramowanie musi zapewniać funkcjonalność zawieszania i ponownej przyrostowej resynchronizacji kopii z oryginałem. |
| Wymagane do replikacji jest użycie protokołu iSCSI lub FC. |
| Wymagana możliwość integracji zdalnej replikacji danych z oprogramowaniem klastrowym, co najmniej Veritas Cluster Server, HACMP, HP Serviceguard, Microsoft Cluster. |
| Oferowana macierz dyskowa musi umożliwiać wykonanie w trybie synchronicznym i asynchronicznym zdalnej kopii danych całej powierzchni użytkowej macierzy. |
| 12 | Importowanie danych | Macierz musi posiadać funkcjonalność onlinowego importu danych z macierzy innego producenta z jednoczesną konwersją wolumenu logicznego LUN do trybu „Thin Provision”. |
| 13 | Gwarancja | Min. 60 miesięcy gwarancji producenta realizowanej w miejscu instalacji sprzętu, z czasem reakcji najpóźniej do końca następnego dnia roboczego. Możliwość zgłaszania awarii w trybie 24/7. W przypadku awarii dyski twarde pozostają własnością Zamawiającego.  System zarządzania jakością w Firmie serwisującej, której wykonawca będzie powierzał serwis na rzecz Zamawiającego, musi być zgodny z normą PN-EN ISO 9001 (lub równoważną) w zakresie wykonywanych przez te firmę usług serwisowych.  Przed zawarciem umowy wybrany Wykonawca będzie zobowiązany przekazać Zamawiającemu nazwę i adres firmy, która będzie wykonywała na rzecz Zamawiającego usługi serwisowe (w zakresie przedmiotu umowy) i wystawione dla tej firmy aktualne zaświadczenie/certyfikat niezależnego podmiotu zajmującego się poświadczaniem spełniania określonych norm zapewnienia jakości, potwierdzające że system zarządzania jakością w tej firmie, w zakresie świadczenia usług serwisowych, jest zgodny z normą PN-EN ISO 9001. (lub równoważną) |
| 14. | Wdrożenie | Zamawiający wymaga wdrożenia macierzy które musi obejmować:  • montaż w szafie serwerowej zgodnie z zaleceniami producenta  • podłączenie do przełączników FC Typu V zapewniając redundancję połączeń i niezawodność całej sieci SAN  • przeprowadzenie instruktażu obsługi macierzy |

* 1. Macierz typ II – 1 szt.

|  |  |  |  |
| --- | --- | --- | --- |
| **Lp.** | | **Nazwa komponentu** | **Wymagane minimalne parametry techniczne urządzenia** |
| **1** | | **2** | **3** |
| 1 | | Macierz | Macierz powinna posiadać dwa redundantne kontrolery macierzowe wraz z możliwością instalacji 12 dysków o maksymalnej wysokość 2U, Macierz musi umożliwiać rozbudowę o moduły 12 dysków 3,5” , 24 dyski 2,5”.  Obsługa minimum 168 dysków SAS/NLSAS lub SSD. |
| 2 | | Wymagana przestrzeń | Macierz musi być wyposażona w:  12 dysków 2,5” o pojemności min. 8TB (NearLine SAS 12Gb/s, prędkość obrotowa 7.2k rpm). |
| 3 | | Pamięć podręczna (Cache) | Pamięć podręczna (cache) – 8 GB pojemności użytkowej dla danych oraz informacji kontrolnych na każdy kontroler (sumarycznie 16 GB),. Zamawiający nie dopuszcza rozwiązań rozszerzających pamięć podręczną cache dyskami SSD/Flash. |
| 4 | | Interfejsy zewnętrzne | Macierz musi być wyposażona w 2 porty FC16 Gb/s z modułami FC 16Gbit/s na pojedynczy kontroler , każdy kontroler macierzy w trybie Active-Active . |
| 5 | | Dostępność | Odporność na zanik zasilania jednej fazy lub awarię zasilacza macierzy (redundancja układu zasilania). |
| Możliwość łączenia w macierzy różnych poziomów RAID:   1. możliwość zastosowania RAID10, 2. możliwość zastosowania RAID10DM (Dual Mirror) 3. możliwość zastosowania RAID5, 4. możliwość zastosowania RAID6, |
| Podwójne niezależne przyłącza SAS 6Gb/s do wewnętrznych napędów dyskowych |
| Odporność na awarię pamięci cache – lustrzany zapis danych oraz technologia zapewniająca ochronę danych z pamięci cache w razie utraty zasilania. |
| Możliwość wykonywania wszystkich napraw, rekonfiguracji, rozbudowy i upgrade’ów (zarówno sprzętu jak i oprogramowania macierzy) w trybie online (bez przerywania pracy systemu). |
| Wymagane wsparcie dla różnych systemów operacyjnych, co najmniej MS Windows, VMware oraz Linux |
| Wykonywanie rozbudowy sprzętowej w trybie online. |
| Umożliwia rozbudowę do minimum 168 dysków 2,5” , 3,5”. |
| 6 | | Skalowalność | Możliwość rozbudowy macierzy za pomocą nowych dysków o większych pojemnościach oraz dysków typu SSD/Flash – zoptymalizowanych pod kątem zapisu bądź odczytu |
| Macierz musi umożliwiać mieszanie dysków o różnych prędkościach obrotowych w ramach jednej półki dyskowej. |
| Oprogramowanie do zarządzania macierzą przez administratora klienta – graficzny interfejs do monitorowania stanu i konfiguracji macierzy, diagnostyki, mapowania zasobów do serwerów (zarówno podłączanych bezpośrednio jak i przez sieć SAN – LUN Masking). |
| Stałe monitorowanie macierzy przez zdalne centrum serwisowe |
| 7 | | Zarządzanie | Monitorowanie wydajności macierzy według parametrów takich jak: przepustowość oraz liczba operacji I/O dla interfejsów zewnętrznych, wolumenów logicznych LUN, oraz kontrolerów.  Wymagana możliwość zbierania i przechowywania informacji o wydajności macierzy bez ograniczeń czasowych |
| Możliwość konfigurowania wolumenów logicznych LUN o pojemności użytkowej 500TB |
|  | Macierz musi posiadać wbudowaną funkcjonalność typu thin provisioning umożliwiającą alokację wirtualnej przestrzeni dyskowej, do której fizyczne dyski mogą być dostarczone w przyszłości. |
| Macierz musi posiadać funkcjonalność automatycznej konwersji bloków danych skonfigurowanych w RAID 10 na RAID 5 lub RAID 6. |
| Macierz musi mieć możliwość migracji wolumenów logicznych LUN pomiędzy różnymi grupami dyskowymi RAID w obrębie macierzy. Migracja musi być wykonywana w trybie on-line. Jeżeli funkcjonalność taka wymaga dodatkowej licencji, to należy je uwzględnić w ofercie. |
| 8 | Możliwość migracji danych w obrębie macierzy | Macierz musi umożliwiać tworzenie jednego wolumenu logicznego LUN w obrębie wszystkich produkcyjnych dysków macierzy. Jeżeli funkcjonalność taka wymaga dodatkowej licencji, to należy je uwzględnić w ofercie. |
| Możliwość tworzenia kopii danych z poziomu macierzy i wewnątrz macierzy bez angażowania systemu operacyjnego hosta. |
| Możliwość tworzenia i utrzymywania jednocześnie minimum ośmiu lokalnych kopii danych wewnątrz macierzy dla każdego urządzenia LUN (tzw. kopie point-in-time) przez administratora. |
| 9 | Lokalna replikacja danych | Oferowana macierz dyskowa musi umożliwiać wykonanie lokalnej kopii danych na całej zaoferowanej przestrzeni dyskowej. |
| Wymaga jest również funkcjonalność wykonywania kopii wirtualnych typu snapshot. Jest wymagana licencja na pełną pojemność macierzy oraz maksymalną ilość snapshotów w obrębie macierzy. |
| Kopie migawkowe muszą być wykonywane metodą tzw. bez prealokacji przestrzeni dyskowej (ang. allocate-on-write, a.k.a redirect-on-write). Kopie migawkowe nie mogą być wykonywane metodą COW (ang. Copy On Write) |
| Kopie migawkowe muszą mieć możliwość prezentacji, jako urządzenia LUN w trybie do odczytu i zapisu. Jeżeli ta funkcjonalność wymaga dodatkowej licencji należy ja dostarczyć. |
| Macierz musi posiadać możliwość zdalnej replikacji danych do macierzy tej samej rodziny w trybie asynchronicznym bez użycia dodatkowych serwerów lub innych urządzeń.  Macierz musi posiadać dedykowany port 10Gbit/s Ethernet do replikacji. |
| 10 | Współpraca z aplikacjami | Oprogramowanie musi zapewniać funkcjonalność zawieszania i ponownej przyrostowej resynchronizacji kopii z oryginałem. |
| 11 | Zdalna replikacja danych  (Zamawiający wymaga dostarczenia licencji) | Wymagane do replikacji jest użycie protokołu iSCSI. |
| 12 | Gwarancja | Min. 60 miesięcy gwarancji realizowanej w miejscu instalacji sprzętu, z czasem reakcji najpóźniej do końca następnego dnia roboczego, możliwość zgłaszania awarii w trybie 24x7x365 w języku polskim poprzez linie telefoniczną producenta.  Wymiana dysków może być dokonywana przez klienta.  System zarządzania jakością w Firmie serwisującej, której wykonawca będzie powierzał serwis na rzecz Zamawiającego, musi być zgodny z normą PN-EN ISO 9001 (lub równoważną) w zakresie wykonywanych przez te firmę usług serwisowych.  Przed zawarciem umowy wybrany Wykonawca będzie zobowiązany przekazać Zamawiającemu nazwę i adres firmy, która będzie wykonywała na rzecz Zamawiającego usługi serwisowe (w zakresie przedmiotu umowy) i wystawione dla tej firmy aktualne zaświadczenie/certyfikat niezależnego podmiotu zajmującego się poświadczaniem spełniania określonych norm zapewnienia jakości, potwierdzające że system zarządzania jakością w tej firmie, w zakresie świadczenia usług serwisowych, jest zgodny z normą PN-EN ISO 9001. (lub równoważną) |
| 13. | Wdrożenie | Zamawiający wymaga wdrożenia macierzy które musi obejmować:  • montaż w szafie serwerowej zgodnie z zaleceniami producenta  • podłączenie do przełączników FC Typu V zapewniając redundancję połączeń i niezawodność całej sieci SAN  • przeprowadzenie instruktażu obsługi macierzy |

1. Serwery – 1 komplet
   * 1. Serwer wirtualizacyjny – 1 szt.

|  |  |  |
| --- | --- | --- |
| **Lp.** | **Nazwa komponentu** | **Wymagane minimalne parametry techniczne urządzenia** |
| **1** | **2** | **3** |
| 1 | Typ serwera | Serwer wirtualizacyjny |
| 2 | Obudowa | Obudowa Rack o wysokości max 2U. Komplet wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych, wraz z ramieniem na kable. 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 (Android/ iOS) przy użyciu jednego z protokołów NFC/ BLE/ WIFI |
| 3 | Płyta główna | Płyta główna z możliwością zainstalowania minimum dwóch procesorów. |
| 4 | Chipset | Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych |
| 5 | Procesor | Zainstalowane dwa procesory ośmiordzeniowe klasy x86 dedykowany do pracy z zaoferowanym serwerem umożliwiający osiągnięcie wyniku min. 1030 punktów w teście SPECint\_rate\_base2006 dostępnym na stronie www.spec.org dla dwóch procesorów |
| 6 | RAM | 256GB DDR4 RDIMM 2667MT/s, na płycie głównej powinno znajdować się minimum 24 slotów przeznaczonych do instalacji pamięci. Płyta główna powinna obsługiwać do 1.5TB pamięci RAM |
| 7 | Zabezpieczenia pamięci RAM | Memory Rank Sparing, Memory Mirror, SDDC |
| 8 | Gniazda PCI | Min. 6 slotów x8 generacji 3 oraz 2 slot x16 generacji 3 |
| 9 | Interfejsy sieciowe | Wbudowane dwa interfejsy sieciowe 1Gb Ethernet w standardzie BaseT oraz dwa interfejsy sieciowe 10Gb Ethernet ze złączami w standardzie SFP+.  Możliwość instalacji wymiennie modułów udostępniających:  - cztery interfejsy sieciowe 10Gb Ethernet w standardzie SFP+.  - dwa interfejsy sieciowe 1Gb Ethernet w standardzie BaseT oraz dwa interfejsy sieciowe 10Gb Ethernet ze złączami w standardzie Base-T  - cztery interfejsy sieciowe 1Gb Ethernet w standardzie BaseT.  - dwa interfejsy sieciowe 25Gb Ethernet ze złączami SFP28.  Zainstalowana jedna karta czteroportowa 10GbE SFP+  - dwie karty dwuportowe FC 16Gb/s z modułami FC 16Gbit/s |
| 10 | Dyski twarde | Zainstalowane 2x120GB SSD SATA 6Gb/s fabrycznie skonfigurowane w RAID 1.  Możliwość instalacji modułu dedykowanego dla hypervisora wirtualizacyjnego, możliwość wyposażenia modułu w 2 jednakowe 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.  Możliwość instalacji dwóch dysków M.2 o pojemności min. 240, możliwość konfiguracji RAID1 |
| 11 | Kontroler RAID | Sprzętowy kontroler dyskowy, możliwe konfiguracje poziomów RAID: 0, 1, 5, 10, 50. Wsparcie dla dysków samoszyfrujących. |
| 12 | Wbudowane porty | min. 3 porty USB 3.0, 2 porty USB 2.0 oraz 1 port MicroUSB 2.0, 2 porty VGA (1 na przednim panelu obudowy, drugi na tylnym), min. 1 port RS232 |
| 13 | Karta graficzna | Zintegrowana karta graficzna umożliwiająca wyświetlanie rozdzielczości min. 1920x1200 |
| 14 | Wentylatory | Redundantne |
| 15 | Zasilacze | Redundantne zasilacze Hot Plug o mocy maksymalnej 750W każdy wraz z kablami zasilającymi o dł. min. 2m każdy |
| 16 | Bezpieczeństwo | Moduł TPM 2.0.  Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą  Dedykowany panel z przodu serwera zapobiegający przed nieuprawnionym wyjęciem dysku.  Panel LCD wyświetlający między innymi temperaturę serwera, kod serwisowy/numer seryjny, stan zasilaczy. |
| 17 | Karta Zarządzania | Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowane port RJ-45 Gigabit Ethernet 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 (SSLv3) 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, Telnet, SSH  • możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer  • możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer  • integracja z usługą katalogową,  • możliwość obsługi przez dwóch administratorów jednocześnie  • wsparcie dla dynamic DNS  • wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej  • możliwość podłączenia lokalnego poprzez złącze RS-232.  • Producent systemu musi posiadać dedykowane rozwiązanie które będzie przeciwdziałało automatycznym skryptom konfiguracyjnym działającym w sieci. Jest niedopuszczalne aby konsole zarządzające serwerów miały identyczne dane dostępowe.  • możliwość zarządzania bezpośredniego poprzez złącze USB umieszczone na froncie obudowy.  • możliwość konfiguracji przepływu powietrza na każdym slocie PCIe, jak również musi posiadać możliwość konfiguracji wyłączania lub włączania poszczególnych wentylatorów.  • możliwość zablokowania konfiguracji oraz odnowienia oprogramowania karty zarządzającej poprzez jednego z administratorów. Podczas trwania blokady musi być ona wyświetlana dla wszystkich administratorów którzy obecnie korzystają z karty.  Dodatkowe oprogramowanie umożliwiające zarządzanie poprzez sieć, spełniające minimalne wymagania:  • Wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych  • Możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta  • Wsparcie dla protokołów– WMI, SNMP, IPMI, , Linux SSH  • Możliwość oskryptowywania procesu wykrywania urządzeń  • Możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram  • Szczegółowy opis wykrytych systemów oraz ich komponentów  • Możliwość eksportu raportu do CSV, HTML, XLS  • Grupowanie urządzeń w oparciu o kryteria użytkownika  • Możliwość uruchamiania narzędzi zarządzających w poszczególnych urządzeniach  • Automatyczne skrypty CLI umożliwiające dodawanie i edycję grup urządzeń  • 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  • Automatyczne zaplanowanie akcji dla poszczególnych alertów w tym automatyczne tworzenie zgłoszeń serwisowych w oparciu o standardy przyjęte przez producentów oferowanego w tym postępowaniu sprzętu  • 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 sterowników i oprogramowania wewnętrznego serwerów  • Aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania)  • Możliwość instalacji sterowników i 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 gwarancji, adresy IP kart sieciowych  Możliwość automatycznego przywracania ustawień serwera ,kart sieciowych, BIOS, wersji firmware w przypadku awarii i wymiany któregoś z komponentów (w tym kontrolera RAID, kart sieciowych, płyty głównej) |
| 18 | System operacyjny | Licencja na oprogramowanie musi być przypisana do każdego procesora fizycznego na serwerze. Licencja na oprogramowanie musi pozwalać na zainstalowanie systemu na serwerze z 2 fizycznymi procesorami. Liczba rdzeni procesorów i ilość pamięci nie mogą mieć wpływu na liczbę wymaganych licencji. Licencja musi uprawniać do uruchamiania serwerowego systemu operacyjnego (SSO) w środowisku fizycznym i nielimitowanej liczby wirtualnych środowisk serwerowego systemu operacyjnego za pomocą wbudowanych mechanizmów wirtualizacji.  Serwerowy system operacyjny (SSO) musi posiadać następujące, wbudowane cechy.  • Możliwość wykorzystania, co najmniej 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM  w środowisku fizycznym  • Możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności min. 64TB przez każdy wirtualny serwerowy system operacyjny.  • Możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania do 8000 maszyn wirtualnych.  • 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.  • Wbudowane wsparcie instalacji i pracy na wolumenach, które:  o pozwalają na zmianę rozmiaru w czasie pracy systemu,  o umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym  i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,  o umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów,  o umożliwiają zdefiniowanie list kontroli dostępu (ACL).  • 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 zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych  i intranetowych.  • Graficzny interfejs użytkownika.  • Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe,  • Możliwość zmiany języka interfejsu po zainstalowaniu systemu, wymagane języki to min. polski i angielski.  • Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).  • Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.  • Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa.  • Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:  - Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC,  - katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji:  - Podłączenie SSO do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną,  - Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,  - Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza.  - Zdalna dystrybucja oprogramowania na stacje robocze.  - Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej  - Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:   * Dystrybucję certyfikatów poprzez http * Konsolidację CA dla wielu lasów domeny, * Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen.   -Szyfrowanie plików i folderów.  -Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec).  -Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów.  -Serwis udostępniania stron WWW.  -Wsparcie dla protokołu IP w wersji 6 (IPv6),  -Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows,  -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:   * Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych, * Obsługi ramek typu jumbo frames dla maszyn wirtualnych. * Obsługi 4-KB sektorów dysków * Nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra * Możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API.   •Możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk model)  •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.  • 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 zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF.  • Zorganizowany system szkoleń i materiały edukacyjne w języku polskim. |
| 19 | Certyfikaty | Zamawiający wymaga, aby oferowany serwer:  -był wyprodukowany zgodnie z normą ISO-9001 oraz ISO-14001(lub równoważną)  -posiadał deklarację CE |
| 20 | Warunki gwarancji | Min. 60 miesięcy gwarancji realizowanej w miejscu instalacji sprzętu, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii w trybie 365x7x24 w języku polskim poprzez linię telefoniczną producenta.  System zarządzania jakością w Firmie serwisującej, której wykonawca będzie powierzał serwis na rzecz Zamawiającego, musi być zgodny z normą PN-EN ISO 9001 (lub równoważną) w zakresie wykonywanych przez te firmę usług serwisowych.  Przed zawarciem umowy wybrany Wykonawca będzie zobowiązany przekazać Zamawiającemu nazwę i adres firmy, która będzie wykonywała na rzecz Zamawiającego usługi serwisowe (w zakresie przedmiotu umowy) i wystawione dla tej firmy aktualne zaświadczenie/certyfikat niezależnego podmiotu zajmującego się poświadczaniem spełniania określonych norm zapewnienia jakości, potwierdzające że system zarządzania jakością w tej firmie, w zakresie świadczenia usług serwisowych, jest zgodny z normą PN-EN ISO 9001. (lub równoważną) |
| 21 | Wirtualizacja | Zainstalowane oprogramowanie do wirtualizacji |
| 22 | Wdrożenie | Zamawiający w ramach wdrożenia infrastruktury serwerowej wymaga:  • montażu w/w sprzętu w szafach rack Zamawiającego w sposób zgodny z zaleceniami producenta dostarczanych serwerów.  • stworzenie klastra serwerów  • testów niezawodności środowiska serwerowego poprzez odłączanie jednej ze ścieżki/wyłączanie urządzenia oraz test redundancji zasilania  • przeprowadzenia szkolenia z zarządzania niskopoziomowego dostarczanych serwerów  • instalacji oprogramowania wirtualizacyjnego na dostarczonym sprzęcie |

* + 1. Oprogramowanie do wirtualizacji - 1 szt.

|  |  |  |
| --- | --- | --- |
| **Lp.** | **Nazwa komponentu** | **Wymagane minimalne parametry oprogramowania** |
| **1** | **2** | **3** |
| 1. | Oprogramowanie do wirtualizacji | Oprogramowanie do wirtualizacji umożliwiające zainstalowanie na min. 3 serwerach fizycznych jedno lub dwu socketowych. |
| 2. | Warstwa wirtualizacji | Zainstalowana bezpośrednio na sprzęcie fizycznym bez dodatkowych pośredniczących systemów operacyjnych. |
| 3. | Obsługa instancji systemów operacyjnych | Rozwiązanie musi zapewnić możliwość obsługi wielu instancji systemów operacyjnych na jednym serwerze fizycznym i powinno się charakteryzować maksymalnym możliwym stopniem konsolidacji sprzętowej. |
| 4. | Skalowalność klastra | Pojedynczy klaster może się skalować do 64 fizycznych hostów (serwerów) z zainstalowaną warstwą wirtualizacji. |
| 5. | Cechy oprogramowania | * Zainstalowane na serwerze fizycznym potrafi obsłużyć i wykorzystać procesory fizyczne wyposażone w 480 logicznych wątków oraz do 6TB pamięci fizycznej RAM. * Musi zapewnić możliwość skonfigurowania maszyn wirtualnych 1-128 procesorowych. * Musi zapewniać możliwość stworzenia dysku maszyny wirtualnej o wielkości do 62 TB. * Musi zapewnić możliwość skonfigurowania maszyn wirtualnych z możliwością przydzielenia do 4 TB pamięci operacyjnej RAM. * Musi zapewnić możliwość skonfigurowania maszyn wirtualnych, z których każda może mieć 1-10 wirtualnych kart sieciowych. * Musi zapewnić możliwość skonfigurowania maszyn wirtualnych, z których każda może mieć 32 porty szeregowe. |
| 6. | Platforma sprzętowa | Rozwiązanie powinno w możliwie największym stopniu być niezależne od producenta platformy sprzętowej. |
| 7. | Wsparcie dla systemów operacyjnych | Oprogramowanie musi wspierać minimum nastepujace systemy operacyjne: Windows XP, Windows Vista, Windows 7, Windows 8, Windows Server 2000, Windows Server 2003, Windows Server 2008/2008R2, Windows Server 2012/2012R2, SLES 10-12, RHEL 3-7, Solaris 10-11, OEL 4, Debian 6-8,  CentOS 4-7, FreeBSD 7-11, Asianux 3-7, Ubuntu 10-16, SCO OpenServer 5.0.6 – 5.0.7, SCO Unixware 7.1.1 – 7.1.4, Mac OS X. |
| 8. | Polityka licencjonowania | Musi umożliwiać przenoszenie licencji na oprogramowanie do wirtualizacji pomiędzy serwerami. |
| 9. | Zasoby RAM | Oprogramowanie musi umożliwiać przydzielenie większej ilości pamięci RAM dla maszyn wirtualnych niż fizyczne zasoby RAM serwera w celu osiągnięcia maksymalnego współczynnika konsolidacji. |
| 10. | Zasoby dyskowe | Oprogramowanie musi umożliwiać udostępnienie maszynie wirtualnej większej ilości zasobów dyskowych niż jest fizycznie zarezerwowane na dyskach lokalnych serwera lub na macierzy. |
| 11. | Zarządzanie maszynami wirtualnymi | * 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. * 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. * Oprogramowanie do wirtualizacji oraz oprogramowanie zarządzające musi posiadać możliwość integracji z usługami katalogowymi. |
| 12. | Kopie migawkowe | Oprogramowanie do wirtualizacji powinno zapewnić możliwość wykonywania kopii migawkowych instancji systemów operacyjnych (tzw. snapshot) na potrzeby tworzenia kopii zapasowych bez przerywania ich pracy. |
| 13. | Kopie zapasowe | Oprogramowanie musi zapewnić wbudowany, bezpieczny mechanizm do automatycznego tworzenia kopii zapasowych, odtwarzania wskazanych maszyn wirtualnych. Mechanizm ten musi umożliwiać również odtwarzanie pojedynczych plików z kopii zapasowej oraz zapewnia stosowanie deduplikacji dla kopii zapasowych. Mechanizm zapewnia możliwość wykonywania spójnych kopii zapasowych serwerów aplikacyjnych oraz replikację kopii zapasowych. |
| 14. | Aktualizacja warstwy wirtualizacyjnej | Rozwiązanie musi zapewniać mechanizm bezpiecznego uaktualniania warstwy wirtualizacyjnej (hosta) bez potrzeby wyłączania wirtualnych maszyn. |
| 15. | Funkcjonalności dodatkowe | Oprogramowanie musi 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. Pojedynczy przełącznik wirtualny powinien mieć możliwość konfiguracji do 4000 portów.  -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.  -Wirtualne przełączniki musza obsługiwać wirtualne sieci lokalne (VLAN). |
| 16. | Replikacja maszyn wirtualnych | Rozwiązanie musi zapewniać mechanizm replikacji wskazanych maszyn wirtualnych w obrębie klastra serwerów fizycznych. |
| 17. | Redundancja | -Rozwiązanie musi mieć możliwość przenoszenia maszyn wirtualnych w czasie ich pracy pomiędzy serwerami fizycznymi. Mechanizm powinien umożliwiać 4 lub więcej takich procesów przenoszenia jednocześnie.  -Oprogramowanie musi zapewnić odpowiednią redundancję i taki mechanizm (wysokiej dostępności HA), aby w przypadku awarii lub niedostępności serwera fizycznego wybrane przez administratora i uruchomione nim wirtualne maszyny zostały uruchomione na innych serwerach z zainstalowanym oprogramowaniem wirtualizacyjnym. |
| 18. | Wsparcie serwisowe | Aktualizacje i wsparcie dla oprogramowania na okres co najmniej 36 miesięcy. |
| 19. | Wdrożenie | Wdrożenie obejmie   * instalacji oprogramowania wirtualizacyjnego  na dostarczonym sprzęcie |

* + 1. Serwer wraz z infrastrukturą niezbędną do zabezpieczenia e-usług – 1 szt.

|  |  |  |
| --- | --- | --- |
| **Lp.** | **Nazwa komponentu** | **Wymagane minimalne parametry techniczne urządzenia** |
| **1** | **2** | **3** |
| **1** | Typ serwera | Serwer wraz z infrastrukturą niezbędną do zabezpieczenia e-usług |
| 2 | Obudowa | Obudowa Rack o wysokości max 2U. Komplet wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych, wraz z ramieniem na kable. Obudowa musi mieć możliwość wyposażenia w kartę umożliwiającą dostęp bezpośredni poprzez urządzenia mobilne  - serwer musi posiadac możliwość konfiguracji oraz monitoringu najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej (Android/ iOS) przy użyciu jednego z protokołów NFC/ BLE/ WIFI. |
| 3 | Płyta główna | Płyta główna z możliwością zainstalowania minimum dwóch procesorów. |
| 4 | Chipset | Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych |
| 5 | Procesor | Zainstalowane dwa procesory ośmiordzeniowe klasy x86 dedykowane do pracy z zaoferowanym serwerem umożliwiający osiągnięcie wyniku min. 1030 punktów w teście SPECint\_rate\_base2006 dostępnym na stronie www.spec.org dla dwóch procesorów |
| 6 | RAM | 256GB DDR4 RDIMM 2667MT/s, na płycie głównej powinno znajdować się minimum 24 slotów przeznaczonych do instalacji pamięci. Płyta główna powinna obsługiwać do 1.5TB pamięci RAM |
| 7 | Zabezpieczenia pamięci RAM | Memory Rank Sparing, Memory Mirror, SDDC |
| 8 | Gniazda PCI | Min. 6 slotów x8 generacji 3 oraz 2 slot x16 generacji 3 |
| 9 | Interfejsy sieciowe | Wbudowane dwa interfejsy sieciowe 1Gb Ethernet w standardzie BaseT oraz dwa interfejsy sieciowe 10Gb Ethernet ze złączami w standardzie SFP+.  Możliwość instalacji wymiennie modułów udostępniających:  - cztery interfejsy sieciowe 10Gb Ethernet w standardzie SFP+.  - dwa interfejsy sieciowe 1Gb Ethernet w standardzie BaseT oraz dwa interfejsy sieciowe 10Gb Ethernet ze złączami w standardzie Base-T  - cztery interfejsy sieciowe 1Gb Ethernet w standardzie BaseT.  - dwa interfejsy sieciowe 25Gb Ethernet ze złączami SFP28.  Zainstalowana jedna karta czteroportowa 10GbE SFP+  - dwie karty dwuportowe FC 16Gb/s z modułami FC 16Gbit/s |
| 10 | Dyski twarde | Zainstalowane 2x120GB SSD SATA 6Gb/s fabrycznie skonfigurowane w RAID 1.  Możliwość instalacji modułu dedykowanego dla hypervisora wirtualizacyjnego, możliwość wyposażenia modułu w 2 jednakowe 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.  Możliwość instalacji dwóch dysków M.2 o pojemności min. 240, możliwość konfiguracji RAID1 |
| 11 | Kontroler RAID | Sprzętowy kontroler dyskowy, możliwe konfiguracje poziomów RAID: 0, 1, 5, 10, 50. Wsparcie dla dysków samoszyfrujących. |
| 12 | Wbudowane porty | min. 3 porty USB 3.0, 2 porty USB 2.0 oraz 1 port MicroUSB, 2 porty VGA (1 na przednim panelu obudowy, drugi na tylnym), min. 1 port RS232 |
| 13 | Karta graficzna | Zintegrowana karta graficzna umożliwiająca wyświetlanie rozdzielczości min. 1920x1200 |
| 14 | Wentylatory | Redundantne |
| 15 | Zasilacze | Redundantne zasilacze Hot Plug o mocy maksymalnej 750W każdy wraz z kablami zasilającymi o dł. min. 2m każdy |
| 16 | Bezpieczeństwo | Moduł TPM 2.0.  Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą  Dedykowany panel z przodu serwera zapobiegający przed nieuprawnionym wyjęciem dysku.  Panel LCD wyświetlający między innymi temperaturę serwera, kod serwisowy/numer seryjny, stan zasilaczy. |
| 17 | Moduł bezpieczeństwa | Fabrycznie zainstalowany w serwerze na złączu PCIe v3 lub v2 sprzętowy moduł bezpieczeństwa, który umożliwia bezpieczne przechowywanie kluczy kryptograficznych oraz wspierający operacje kryptograficzne z użyciem kluczy asymetrycznych RSA długości nie mniejszej niż 8192 bitów, Diffie-Helmana oraz ECC Suite B. |
| Moduł musi posiadać wsparcie dla algorytmów symetrycznych AES o długości nie mniejszej niż 256 bit oraz 3 (Triple) DES 112 i 168 bitów |
| Musi także posiadać obsługę funkcji skrótu SHA-1 oraz SHA-2 o długości (224, 256, 284 oraz 512 bitów). |
| Moduł bezpieczeństwa musi umożliwiać pełne zarządzanie włącznie z aktualizacją firmware, oraz posiadać certyfikację FIPS 140-2 poziomu 3. |
| Ponadto moduł ten musi zezwalać na autoryzację za pomocą hasła, karty inteligentnej (musi ona zostać dostarczona wraz z urządzeniem i dedykowanym czytnikiem współpracującym tylko z kartami danego producenta) oraz klucza w postaci pliku. W zestawie z modułem kryptograficznym musi zostać dostarczone oprogramowanie producenta modułu będące odpowiednikiem zaoferowanego fizycznego modułu bezpieczeństwa. |
| Moduł bezpieczeństwa musi oferować zaawansowaną diagnostykę i logowanie zdarzeń w przynajmniej 3 poziomach (Error, Info, Warning), wykorzystując biblioteki PKCS#11. |
| 18 | Karta Zarządzania | Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowane port RJ-45 Gigabit Ethernet 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 (SSLv3) 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, Telnet, SSH  • możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer  • możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer  • integracja z usługą katalogową  • możliwość obsługi przez dwóch administratorów jednocześnie  • wsparcie dla dynamic DNS  • wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej  • możliwość podłączenia lokalnego poprzez złącze RS-232.  • Producent systemu musi posiadać dedykowane rozwiązanie które będzie przeciwdziałało automatycznym skryptom konfiguracyjnym działającym w sieci. Jest niedopuszczalne aby konsole zarządzające serwerów miały identyczne dane dostępowe.  • możliwość zarządzania bezpośredniego poprzez złącze USB umieszczone na froncie obudowy.  • możliwość konfiguracji przepływu powietrza na każdym slocie PCIe, jak również musi posiadać możliwość konfiguracji wyłączania lub włączania poszczególnych wentylatorów.  • możliwość zablokowania konfiguracji oraz odnowienia oprogramowania karty zarządzającej poprzez jednego z administratorów. Podczas trwania blokady musi być ona wyświetlana dla wszystkich administratorów którzy obecnie korzystają z karty.  Dodatkowe oprogramowanie umożliwiające zarządzanie poprzez sieć, spełniające minimalne wymagania:  • Wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych  • Możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta  • Wsparcie dla protokołów– WMI, SNMP, IPMI, , Linux SSH  • Możliwość oskryptowywania procesu wykrywania urządzeń  • Możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram  • Szczegółowy opis wykrytych systemów oraz ich komponentów  • Możliwość eksportu raportu do CSV, HTML, XLS  • Grupowanie urządzeń w oparciu o kryteria użytkownika  • Możliwość uruchamiania narzędzi zarządzających w poszczególnych urządzeniach  • Automatyczne skrypty CLI umożliwiające dodawanie i edycję grup urządzeń  • 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  • Automatyczne zaplanowanie akcji dla poszczególnych alertów w tym automatyczne tworzenie zgłoszeń serwisowych w oparciu o standardy przyjęte przez producentów oferowanego w tym postępowaniu sprzętu  • 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 sterowników i oprogramowania wewnętrznego serwerów  • Aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania)  • Możliwość instalacji sterowników i 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 gwarancji, adresy IP kart sieciowych  Możliwość automatycznego przywracania ustawień serwera ,kart sieciowych, BIOS, wersji firmware w przypadku awarii i wymiany któregoś z komponentów (w tym kontrolera RAID, kart sieciowych, płyty głównej) |
| 19 | System operacyjny | Licencja umożliwiająca podłączenie i wykorzystywanie wszystkich dostępnych funkcjonalności serwera. Minimalne wymagane funkcjonalności:   * możliwość dokonywania aktualizacji i poprawek systemu przez Internet z możliwością wyboru instalowanych poprawek; * możliwość dokonywania uaktualnień sterowników urządzeń przez Internet – witrynę producenta systemu; * darmowe aktualizacje w ramach wersji systemu operacyjnego przez Internet (niezbędne aktualizacje, poprawki, biuletyny bezpieczeństwa muszą być dostarczane bez dodatkowych opłat) - wymagane podanie nazwy strony serwera www; * internetowa aktualizacja zapewniona w języku polskim; * wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych; zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami ip v4 i v6; * zlokalizowane w języku polskim, co najmniej następujące elementy: menu, pomoc, komunikaty systemowe; * możliwość uruchomienia kontrolera domeny; * możliwość uruchomienia kontrolera domeny tylko do odczytu; * możliwość uruchomienia serwera DNS; * możliwość uruchomienia serwera usług terminalowych; * obsługa zdalnego pulpitu - RDS; * możliwość zdalnej automatycznej instalacji, konfiguracji, administrowania oraz aktualizowania systemu; * możliwość w ramach pojedynczej licencji zainstalowania min. 20 systemów wirtualnych; * obsługa certyfikatów w usłudze katalogowej; * obsługa drzewa katalogowego; * Zamawiający nie dopuszcza dostawy licencji ograniczonych czasowo. * Licencje muszą pozwalać na przenoszenie pomiędzy stacjami roboczymi/serwerami |
| 20 | Certyfikaty | Zamawiający wymaga, aby oferowany serwer:  -był wyprodukowany zgodnie z normą ISO-9001 oraz ISO-14001. (lub równoważną)  -posiadał deklarację CE |
| 21 | Gwarancja | Min. 60 miesięcy gwarancji realizowanej w miejscu instalacji sprzętu, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii w trybie 365x7x24 w języku polskim poprzez linię telefoniczną producenta.  System zarządzania jakością w Firmie serwisującej, której wykonawca będzie powierzał serwis na rzecz Zamawiającego, musi być zgodny z normą PN-EN ISO 9001 (lub równoważną) w zakresie wykonywanych przez te firmę usług serwisowych.  Przed zawarciem umowy wybrany Wykonawca będzie zobowiązany przekazać Zamawiającemu nazwę i adres firmy, która będzie wykonywała na rzecz Zamawiającego usługi serwisowe (w zakresie przedmiotu umowy) i wystawione dla tej firmy aktualne zaświadczenie/certyfikat niezależnego podmiotu zajmującego się poświadczaniem spełniania określonych norm zapewnienia jakości, potwierdzające że system zarządzania jakością w tej firmie, w zakresie świadczenia usług serwisowych, jest zgodny z normą PN-EN ISO 9001. (lub równoważną) |
| 22 | Wdrożenie | Zamawiający w ramach wdrożenia infrastruktury serwerowej wymaga:  • montażu w/w sprzętu w szafach rack Zamawiającego w sposób zgodny z zaleceniami producenta dostarczanych serwerów  • stworzenie klastra serwerów  • instalacji oprogramowania wirtualizacyjnego na dostarczonym sprzęcie wraz ze szkoleniem. |

* + 1. Kontroler serwerów – 1 szt.

|  |  |  |
| --- | --- | --- |
| **Lp.** | **Nazwa komponentu** | **Wymagane minimalne parametry techniczne urządzenia** |
| **1** | **2** | **3** |
| 1 | Obudowa | Obudowa Rack o wysokości max 1U z możliwością instalacji do 4 dysków 3.5" Hot-Plug wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych wraz z ramieniem na kable  Dodatkowo Zamawiający wymaga zabezpieczenia dysków przed nieuprawnionym fizycznym dostępem w formie ramki zabezpieczającej. |
| 2 | Płyta główna | Płyta główna z możliwością zainstalowania minimum jednego procesora. |
| 3 | Chipset | Dedykowany przez producenta procesora do pracy w serwerach jednoprocesorowych. |
| 4 | Procesor | Zainstalowany jeden procesor czterordzeniowy klasy x86 dedykowany do pracy z zaoferowanym serwerem umożliwiający osiągnięcie wyniku min.260 punktów w teście SPECint\_rate\_base2006 dostępnym na stronie www.spec.org dla jednego procesora. |
| 5 | RAM | 32GB DDR4 UDIMM, na płycie głównej powinno znajdować się minimum 3 wolne sloty przeznaczone do rozbudowy pamięci. Płyta główna powinna obsługiwać do 64GB pamięci RAM. |
| 6 | Zabezpieczenia pamięci RAM | Możliwe funkcjonalności pamięci: ODT, CKE |
| 7 | Gniazda PCI | Min. Dwa sloty PCIe Gen 3. |
| 8 | Interfejsy sieciowe | Wbudowane minimum 2 porty typu Gigabit Ethernet Base-T.  Dodatkowo zainstalowana jedna karta dwuportowa 10GbE SFP+ oraz jedna karta dwuportowa FC 8Gb/s |
| 9 | Dyski twarde | Możliwość instalacji dysków SATA, SAS, SSD. Zainstalowane 2x120GB typu HotPlug SSD SATA skonfigurowane w RAID 1.  Możliwość zainstalowania wewnętrznego modułu dedykowanego dla hypervisora wirtualizacyjnego, możliwość wyposażenia w 2 jednakowe nośniki typu flash o pojemności minimum 16GB z możliwością konfiguracji zabezpieczenia RAID 1 z poziomu BIOS serwera, rozwiązanie nie może powodować zmniejszenia ilości wnęk na dyski twarde |
| 10 | Kontroler RAID | Sprzętowy kontroler dyskowy, możliwe konfiguracje poziomów RAID: 0, 1, 5, 10, 50. |
| 11 | Wbudowane porty | min. 2 porty USB 2.0, 3 porty USB 3.0, 2 porty RJ45, 2 porty VGA (1 na przednim panelu obudowy, drugi na tylnym), min. 1 port RS232 |
| 12 | Karta graficzna | Zintegrowana karta graficzna umożliwiająca wyświetlanie rozdzielczości min. 1280x1024 |
| 13 | Wentylatory | Redundantne |
| 14 | Zasilacze | Redundantne, Hot-Plug maksymalnie 350W każdy. |
| 15 | Bezpieczeństwo | Zintegrowany z płytą główną moduł TPM 2.0  Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą |
| 16 | Diagnostyka | Panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS’u, zasilaniu oraz temperaturze. |
| 17 | Karta Zarządzania | Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowane port RJ-45 Gigabit Ethernet 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 (SSLv3) 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, Telnet, SSH * możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer * możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer * integracja z usługą katalogową * możliwość obsługi przez dwóch administratorów jednocześnie * wsparcie dla dynamic DNS * wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej * możliwość podłączenia lokalnego poprzez złącze RS-232   możliwość zarządzania bezpośredniego poprzez złącze USB umieszczone na froncie obudowy. |
| 20 | System operacyjny | Licencja umożliwiająca podłączenie i wykorzystywanie wszystkich dostępnych funkcjonalności serwera. Minimalne wymagane funkcjonalności:   * możliwość dokonywania aktualizacji i poprawek systemu przez Internet z możliwością wyboru instalowanych poprawek; * możliwość dokonywania uaktualnień sterowników urządzeń przez Internet – witrynę producenta systemu; * darmowe aktualizacje w ramach wersji systemu operacyjnego przez Internet (niezbędne aktualizacje, poprawki, biuletyny bezpieczeństwa muszą być dostarczane bez dodatkowych opłat) - wymagane podanie nazwy strony serwera www; * internetowa aktualizacja zapewniona w języku polskim; * wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych; zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami ip v4 i v6; * zlokalizowane w języku polskim, co najmniej następujące elementy: menu, pomoc, komunikaty systemowe; * możliwość uruchomienia kontrolera domeny; * możliwość uruchomienia kontrolera domeny tylko do odczytu; * możliwość uruchomienia serwera DNS; * możliwość uruchomienia serwera usług terminalowych; * obsługa zdalnego pulpitu - RDS; * możliwość zdalnej automatycznej instalacji, konfiguracji, administrowania oraz aktualizowania systemu; * możliwość w ramach pojedynczej licencji zainstalowania min. 20 systemów wirtualnych; * obsługa certyfikatów w usłudze katalogowej; * obsługa drzewa katalogowego; * Zamawiający nie dopuszcza dostawy licencji ograniczonych czasowo.   Licencje muszą pozwalać na przenoszenie pomiędzy stacjami roboczymi/serwerami |
| 21 | Certyfikaty | Zamawiający wymaga, aby oferowany serwer:  -był wyprodukowany zgodnie z normą ISO-9001 oraz ISO-14001(lub równoważną)  -posiadał deklarację CE |
| 22 | Warunki gwarancji | Min. 60 miesięcy gwarancji realizowanej w miejscu instalacji sprzętu, z dwugodzinnym czasem reakcji od przyjęcia zgłoszenia, możliwość zgłaszania awarii w trybie 365x7x24 w języku polskim poprzez linię telefoniczną producenta.  System zarządzania jakością w Firmie serwisującej, której wykonawca będzie powierzał serwis na rzecz Zamawiającego, musi być zgodny z normą PN-EN ISO 9001 (lub równoważną) w zakresie wykonywanych przez te firmę usług serwisowych.  Przed zawarciem umowy wybrany Wykonawca będzie zobowiązany przekazać Zamawiającemu nazwę i adres firmy, która będzie wykonywała na rzecz Zamawiającego usługi serwisowe (w zakresie przedmiotu umowy) i wystawione dla tej firmy aktualne zaświadczenie/certyfikat niezależnego podmiotu zajmującego się poświadczaniem spełniania określonych norm zapewnienia jakości, potwierdzające że system zarządzania jakością w tej firmie, w zakresie świadczenia usług serwisowych, jest zgodny z normą PN-EN ISO 9001. (lub równoważną) |
| 23. | **Wdrożenie** | Zamawiający w ramach wdrożenia infrastruktury serwerowej wymaga:  • montażu w/w sprzętu w szafach rack Zamawiającego w sposób zgodny z zaleceniami producenta dostarczanych serwerów |

* + 1. Licencje dostępowe – 1 komplet (400 sztuk)

|  |  |  |
| --- | --- | --- |
| **Lp.** | **Nazwa komponentu** | **Wymagane minimalne parametry oprogramowania** |
| **1** | **2** | **3** |
| 1 | Klasa produktu | Licencja wieczysta, dająca prawo korzystania z usług udostępnianych przez serwery |
| 2 | Typ licencji | komercyjna |
| 3 | Rodzaj licencji | Przeznaczona na urządzenie |
| 4 | Wersja językowa | polska |

* + 1. Licencje dostępu klienta usług pulpitu zdalnego – 1 komplet (20 sztuk)

|  |  |  |
| --- | --- | --- |
| **Lp.** | **Nazwa komponentu** | **Wymagane minimalne parametry oprogramowania** |
| **1** | **2** | **3** |
| 1 | Klasa produktu | Licencja wieczysta, dająca prawo korzystania z usług pulpitu zdalnego serwera. |
| 2 | Typ licencji | komercyjna |
| 3 | Rodzaj licencji | Przeznaczone dla użytkownika |
| 4 | Wersja językowa | polska |

1. Przełączniki – 1 komplet
   1. Przełącznik typ I – 1 komplet (2 sztuki)

|  |  |  |
| --- | --- | --- |
| **Lp.** | **Nazwa komponentu** | **Wymagane minimalne parametry techniczne urządzenia** |
| **1** | **2** | **3** |
| 1 | Porty | Przełącznik 1U wyposażony w porty:  - 48 x 10 Gigabit Ethernet SFP+  - 6 x 40 Gigabit Ethernet QSFP+  - 1 x RJ45 konsolowy/administracyjny port z RS232  - 1x USB 2.0 typu A we wsparciem zewnętrznej pamięci masowej  - 1 x Micro-USB 2.0 typu B port konsolowy  Musi umożliwiać obsługę wszystkich portów line-rate, z jednoczesną możliwością instalacji modułów SFP w miejsce portów 10 Gigabit Ethernet  Musi posiadać gniazdo dla opcjonalnego modułu łączenia w stos lub możliwość zestawienia stosu portami 40GbE (do min 6 urządzeń) |
| 2 | Komponenty dodatkowe | Wymagane jest dostarczenie komponentów kompatybilnych z przełącznikami i pochodzących od tego samego producenta co przełączniki:   1x kabel Direct Attach 40GbE QSFP+ o długości min. 3 metry do każdego przełącznika  7x kabel Direct Attach 10GbE SFP+ o długości min. 3 metry do każdego przełącznika  3x moduł nadawczo-odbiorczy SFP 1000Base-T |
| 3 | Przepustowość | Przepustowość zagregowana minimum 1080 Mpps, |
| 4 | System operacyjny | Modularny system operacyjny,  Musi umożliwiać instalacje różnych systemów operacyjnych wspieranych przez producenta w celu uzyskania dodatkowych funkcjonalności zgodnie z rekomendacją SDN |
| 5 | Zasilanie | Nadmiarowy zasilacz AC (hot-swapable),  Max. konsumpcja mocy: 250 W (AC) lub 800 W (DC) |
| 6 | RACK | Musi zapewniać instalację w szafach 19” |
| 7 | Pamięć | Moduł pamięci flash: 8 GB  Pamięć CPU: 4GB  Pojemność bufora pakietów: 12MB |
| 8 | Interfejsy | Musi istnieć możliwość zamiany interfejsów 40 Gigabit Ethernet na 4 x 10Gigabit Ethernet SFP+ lub równoważne za pomocą kabli rozszywających.  Wymagana obsługa min. 72 portów 10Gigabit Ethernet line-rate na przełącznik z wykorzystaniem kabli rozszywających. |
| 9 | Wydajność | Musi posiadać matrycę przełączającą o wydajności min. 1.44Tbps (full-duplex);  Szybkość przełączania ramki w obrębie przełącznika maksymalnie 2.5 us mikro sekund; |
| 10 | Chłodzenie | Musi posiadać możliwość chłodzenia urządzenia w trybie przód-do-tyłu  Musi być wyposażone w redundantne i wymienne w trakcie pracy (hot-swappable) 2 wiatraki |
| 11 | Funkcjonalności | Musi obsługiwać ramki „Jumbo” o długości min. 12000 bajtów.  Musi obsługiwać, co najmniej 4000 VLANów.  Pamięć, dla co najmniej 160 000 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  - implementacje dedykowanego protokołu innego niż STP, RSTP, PVST+, MSTP umożliwiający szybką konwergencję sieci w przypadku zastosowania topologii Ring.  Urządzenie musi posiadać możliwość definiowana łączy w grupy LAG (802.3ad). Obsługa min. 16 łączy w grupie LAG  Musi obsługiwać DCB (Data Center Bridging)  Musi zapewniać sprzętowe wsparcie dla VXLAN routing line rate  Musi obsługiwać protokół Resilient Ring Protocol, (FRRP) lub równoważny  **Musi obsługiwać standardy IEEE:**  802.1AB LLDP  802.1ag Connectivity Fault Management  802.1D Bridging, STP  802.1p L2 Prioritization  802.1Q VLAN Tagging, Double VLAN Tagging, GVRP  802.1X Network Access Control (Port Authentication)  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)  802.3ba 40 Gigabit Ethernet (40GBase-SR4, 40GBase-CR4)  802.3u Fast Ethernet (100BASE-FX) on management ports  802.3x Flow Control  802.3z Gigabit Ethernet (1000BASE-X)  ANSI/TIA-1057 LLDP-MED  **Musi obsługiwać, co najmniej poniższe standardy:**  768 User Datagram Protocol  793 Transmission Control Protocol  854 Telnet Protocol Specification  959 File Transfer Protocol (FTP)  1321 The MD5 Message-Digest Algorithm  1350 The TFTP Protocol (Revision 2)  2474 Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers  3164 The BSD syslog Protocol  5880 Bidirectional Forwarding Detection  **RFC w zakresie protokołu IPv4:**  791 Internet Protocol  792 Internet Control Message Protocol  826 An Ethernet Address Resolution Protocol  1027 Using ARP to Implement Transparent Subnet Gateways  1035 DOMAIN NAMES - IMPLEMENTATION AND SPECIFICATION (client)  1042 A Standard for the Transmission of IP Datagrams over IEEE 802 Networks  1305 Network Time Protocol (Version 3) Specification, Implementation and Analysis  1519 Classless Inter-Domain Routing (CIDR): an Address Assignment and Aggregation Strategy  1542 Clarifications and Extensions for the Bootstrap Protocol  1812 Requirements for IP Version 4 Routers  1858 IP Fragment Filtering  2131 Dynamic Host Configuration Protocol  2338 Virtual Router Redundancy Protocol (VRRP)  3021 Using 31-Bit Prefixes on IPv4 Point-to-Point Links  3046 DHCP Relay Agent Information Option  3069 VLAN Aggregation for Efficient IP Address Allocation  3128 Protection Against a Variant of the Tiny Fragment Attack  **Musi obsługiwać, co najmniej poniższe standardy RFC w zakresie protokołu IPv6:**  1858 IP Fragment Filtering  2460 Internet Protocol, Version 6 (IPv6) Specification  2463 Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification  2675 IPv6 Jumbograms  3587 IPv6 Global Unicast Address Format  4291 Internet Protocol Version 6 (IPv6) Addressing Architecture  **Musi obsługiwać Multicast w tym, co najmniej poniższe standardy RFC i drafty**:  1112 Host Extensions for IP Multicasting  2236 Internet Group Management Protocol, Version 2  3376 Internet Group Management Protocol, Version 3  3569 An Overview of Source-Specific Multicast (SSM)  4541 Considerations for Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) Snooping Switches  draft-ietf-pim-sm-v2-new-05 Protocol Independent Multicast - Sparse Mode (PIM-SM): Protocol Specification (Revised)  **Musi umożliwiać obsługę Statycznego i Dynamicznego Routingu:**  **W tym co najmniej poniższe standardy RFC dla OSFP:**  1587 The OSPF Not-So-Stubby Area (NSSA) Option  2154 OSPF with Digital Signatures  2328 OSPF Version 2  2370 The OSPF Opaque LSA Option  3623 Graceful OSPF Restart  4222 Prioritized Treatment of Specific OSPF Version 2 Packets and Congestion Avoidance  **W tym co najmniej poniższe standardy RFC i drafty dla BGP:**  1997 BGP Communities Attribute  2385 Protection of BGP Sessions via the TCP MD5 Signature Option  2439 BGP Route Flap Damping  2545 BGP-4 Multiprotocol Extensions for IPv6 Inter-Domain Routing  2796 BGP Route Reflection: An Alternative to Full Mesh Internal BGP (IBGP)  2842 Capabilities Advertisement with BGP-4  2858 Multiprotocol Extensions for BGP-4  2918 Route Refresh Capability for BGP-4  3065 Autonomous System Confederations for BGP  4360 BGP Extended Communities Attribute  4893 BGP Support for Four-octet AS Number Space  5396 Textual Representation of Autonomous System (AS) Numbers  draft-ietf-idr-bgp4-20 Border Gateway Protocol 4 (BGP-4)  draft-ietf-idr-restart-06 Graceful Restart Mechanism for BGP  **W tym, co najmniej poniższe standardy RFC dla IS-IS**:  1195 Routing in TCP/IP and Dual Environments  5308 Routing IPv6 with IS-IS  **W tym, co najmniej poniższe standardy RFC dla VRF**  4364 VRF-lite (IPv4 VRF with OSPF, BGP, IS-IS and V4 multicast)  **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, * 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   **Musi wspierać następujące mechanizmy związane z zarządzaniem i zapewnieniem bezpieczeństwa w sieci:**   * Co najmniej 3 poziomy dostępu administracyjnego przez konsole: * Urządzenie musi posiadać dedykowany port konsolowy do zarządzania typu RJ45 (konsola) oraz drugi wydzielony 10/100/1000BaseT * Autoryzacja użytkowników/portów w oparciu o 802.1x oraz EAP * Możliwość uzyskania dostępu do urządzenia przez SNMPv1/2/3 i SSHv2 * Implementacji listy kontroli dostępu (ACL) na poziomie co najmniej warstwy 2 * Obsługa DHCP Snooping * Obsługa dynamicznej inspekcji ARP * Obsługa walidacji adresów IP o MAC (MAC+IP Source Address Validation) * Obsługa walidacji adresów MAC (DHCP MAC Address Validation) * Obsługa, co najmniej sFlow v5 lub ekwiwalentu * Obsługa RMON * Obsługa monitorowania ruchu na porcie (Port Monitoring) * 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.   **Urządzenie musi posiadać funkcjonalność automatycznej konfiguracji poprzez ściągnięcie z serwera TFTP pliku z oprogramowaniem (firmware) i pliku konfiguracyjnego w trakcie pierwszego podłączenia do sieci Ethernet** |
| 12 | Gwarancja | Min. 60 miesięcy gwarancji realizowanej w miejscu instalacji sprzętu, z czasem reakcji do końca następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii w trybie 24x7x365 w języku polskim poprzez linię telefoniczną producenta. |
| 13 | Dokumentacja | 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. |
| 14 | Wdrożenie | Wykonawca jest zobowiązany do wdrożenia infrastruktury sieciowej, które musi obejmować:  • konfigurację nowej infrastruktury sieciowej przy wykorzystaniu istniejącego okablowania |

* + 1. Przełącznik typ II – 1 komplet (2 sztuki)

|  |  |  |
| --- | --- | --- |
| **Lp.** | **Nazwa komponentu** | **Wymagane minimalne parametry techniczne urządzenia** |
| **1** | **2** | **3** |
| 1 | Obudowa | Do montażu w szafie Rack 19", o wysokości nie większej niż 1U, Głębokość: max 48 cm wraz z kompletem odpowiednich szyn., |
| 2 | Porty | Min 24 porty 10 Gigabit Ethernet Base-T. |
|  | Możliwość instalacji wymiennie dodatkowych modułów : |
|  | - 4 porty 10Gigabit Ethernet SFP+ lub |
|  | - 4 porty 10Gigabit Ethernet 10GBaseT  - 2 porty 40GbE (QSFP+) |
|  | 1 port RJ45 umożliwiający zarządzanie poprzez konsolę, |
|  | 1 port Ethernet RJ45 dedykowany do zarządzania Out-Of-Band |
|  | 1 port USB  Wraz z przełącznikiem należy dostarczyć moduł nadawczo-odbiorczy 1x SFP 1000Base-T |
| 3 | Wydajność | Obsługa minimum 4000 wirtualnych sieci |
| Stakowalny do minimum 10 urządzeń w stosie portami 40GbE lub 10GbE (min 160Gbps) |
| Forwarding Rate min. 470 Mpps |
| Switching fabric min. 640 Gbps |
| Rozmiar tablicy routingu min.: 8 000 wpisów IPv4, 4 000 wpisów IPv6 |
| Pamięć MAC adresów min. 130 000 |
| ACL – minimum 100 list, minimum 1000 reguł na ACL, min 3000 reguł na wszystkie ACL |
| Bufor pamięci dla pakietów minimum 9 MB |
| Pamięć procesora minimum 2 GB |
| 4 | Funkcjonalność | Musi wspierać funkcjonalność wirtualnej agregacji portów umożliwoającą:  - budowę topologii sieci bez pętli z pełnym wykorzystaniem agregowanych łączy |
|  | Możliwość obsługi modułów QSFP+ 40GE-SR4 |
|  | Możliwość obsługi kabli DAC 40GbE i 10GbE (Direct Attached Cable) min długości:: min. 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 |
|  | Redundantne min. 2 zasilacze AC |
|  | Redundantne min. 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 |
| 5 | Zgodność z protokołami | 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, min.: |
| - RIP v1/2; |
| - OSPF v1/2/3 |
| - VRRP |
| - Policy Based Routing |
| - Graceful Restart |
| - BGP |
| Obsługa multicastu, min.: |
| - IGMP v1/2/3; |
| - IGMP Snooping Querier |
| - MLDv2 |
| - PIM-DM |
| - PIM-SM |
| - DHCP |
| - IGMP Proxy |
| 6 | Zarządzanie i bezpieczeństwo | 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 |
| Możliwośc 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 |
|  |
| 7 | Warunki pracy | Wydajność pracy zasilaczy na poziomie min. 80% |
| Temperatura pracy w zakresie od 0 do 45 stopni Celsjusza |
| Maksymalny pobór mocy 240W |
| Wilgotność dla trybu pracy 85% |
| 8 | Certyfikaty i standardy | Zamawiający wymaga aby oferowany przełącznik: |
|  | - został wyprodukowany zgodnie z normą  ISO-9001 oraz ISO-14001 (lub równoważną) |
|  | - posiadał deklarację CE |
|  | - jest zgodny z standardem RoHS |
| 9 | Warunki gwarancji | Min. 60 miesięcy gwarancji realizowanej w miejscu instalacji sprzętu, z czasem reakcji następnego dnia roboczego od zgłoszenia awarii możliwość zgłaszania awarii w trybie 24x7x365 w języku polskim poprzez linię telefoniczną producenta.. |
| Gwarancja czasu życia (Limited Lifetime warranty) obejmująca: |
| - przełącznik |
| - zasilacze i wiatraki |
| - moduły SFP, SFP+ i QSFP+ |
| - bezterminowy dostęp do nowych wersji oprogramowania |
| 10 | Dokumentacja użytkownika | Zamawiający wymaga dokumentacji w wersji elektronicznej i drukowanej w języku polskim |
| 11 | Wdrożenie | Wykonawca jest zobowiązany do wdrożenia infrastruktury sieciowej, które musi obejmować:  • konfigurację nowej infrastruktury sieciowej przy wykorzystaniu istniejącego okablowania |

* + 1. Przełącznik typ III – 1 komplet (14 sztuk)

|  |  |  |
| --- | --- | --- |
| **Lp.** | **Nazwa komponentu** | **Wymagane minimalne parametry techniczne urządzenia** |
| **1** | **2** | **3** |
| 1 | Obudowa | Do montażu w szafie Rack 19", o wysokości nie więcej niż 1U, wraz z zestawem montażowym rack 19”, wyposażona w zintegrowany zasilacz. |
| 2 | Porty | Minimum 48 portów GigabitEthernet w standardzie BaseT minimum 4 zintegrowane porty 10Gb Ethernet SFP+, minimum 1 port USB. |
| 3 | Wydajność przełącznika | **minimum 16000** adresów MAC switch fabric capacity min. 176Gbps forwarding rate min. 132Mpps |
| pamięć flash min. 1GB bufor pamięci dla pakietów minimum 2MB pamięć procesora minimum 1GB obsługa minimum 512 wirtualnych sieci możliwość połączenia w stos do 4 urządzeń tego samego typu  Wsparcie dla agregacji LACP (802.3ad) |
| 4 | Zgodność z protokołami | 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) |
|  |
| 5 | Zarządzanie siecią i bezpieczeństwo | 1155 SMIv1  1157 SNMPv1  1212 Concise MIB Definitions  1213 MIB-II 1215 SNMP Traps  1286 Bridge MIB 1442 SMIv2  1451 Manager-toManager 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 |
| 6 | Certyfikaty i standardy | Zamawiający wymaga aby oferowany przełącznik:  - został wyprodukowany zgodnie z normą ISO-9001 oraz ISO-14001 (lub równoważną)  - posiadał deklarację CE  - jest zgodny z standardem RoHS |
| 7 | Komponenty dodatkowe | Wymagane jest dostarczenie komponentów kompatybilnych (współpracujących) z przełącznikami:  1 x kabel Direct Attach 10GbE SFP+ o długości min. 0,5 metra do każdego przełącznika  2x moduł nadawczo-odbiorczy SFP+10GbE SR do każdego przełącznika |
| 8 | Gwarancja | Min. 60 miesięcy gwarancji realizowanej w miejscu instalacji sprzętu,  z czasem reakcji następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii w trybie 24x7x365 w języku polskim poprzez linię telefoniczną producenta. |
| **9** | Wdrożenie | Wykonawca jest zobowiązany do wdrożenia infrastruktury sieciowej, które musi obejmować:  • konfigurację nowej infrastruktury sieciowej przy wykorzystaniu istniejącego okablowania |

* + 1. Przełącznik typ IV – 1 komplet (18 sztuk)

|  |  |  |
| --- | --- | --- |
| **Lp.** | **Nazwa komponentu** | **Wymagane minimalne parametry techniczne urządzenia** |
| **1** | **2** | **3** |
| 1 | Obudowa | Do montażu w szafie Rack 19", o wysokości nie więcej niż 1U, wraz z wraz z zestawem montażowym rack 19”, wyposażona w zintegrowany zasilacz. |
| 2 | Porty | Minimum 24 portów GigabitEthernet w standardzie BaseT minimum 4 zintegrowane porty 10Gb Ethernet SFP+, minimum 1 port USB. |
| 3 | Wydajność przełącznika | minimum **16000** adresów MAC switch fabric capacity min. 128Gbps forwarding rate min. 96Mpps |
| pamięć flash min. 1GB bufor pamięci dla pakietów minimum 2MB pamięć procesora minimum 1GB obsługa minimum 512 wirtualnych sieci możliwość połączenia w stos do 4 urządzeń tego samego typu  Wsparcie dla agregacji LACP (802.3ad) |
| 4 | Zgodność z protokołami | 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) |
|  |
| 5 | Zarządzanie siecią i bezpieczeństwo | 1155 SMIv1  1157 SNMPv1  1212 Concise MIB Definitions  1213 MIB-II 1215 SNMP Traps  1286 Bridge MIB 1442 SMIv2  1451 Manager-toManager 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 |
| 6 | Certyfikaty i standardy | Zamawiający wymaga aby oferowany przełącznik:  - został wyprodukowany zgodnie z normą ISO-9001 oraz ISO-14001 (lub równoważną)  - posiadał deklarację CE  - jest zgodny z standardem RoHS |
| 7 | Komponenty dodatkowe | Wymagane jest dostarczenie komponentów kompatybilnych (współpracujących) z przełącznikami:  1 x kabel Direct Attach 10GbE SFP+ o długości min. 0,5 metra do każdego przełącznika  2x moduł nadawczo-odbiorczy SFP+10GbE SR do każdego przełącznika |
| 8 | Gwarancja | Min. 60 miesięcy gwarancji realizowanej w miejscu instalacji sprzętu, z czasem reakcji następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii w trybie 24x7x365 w języku polskim poprzez linię telefoniczną producenta. |
| 9 | Wdrożenie | Wykonawca jest zobowiązany do wdrożenia infrastruktury sieciowej, które musi obejmować:  • konfigurację nowej infrastruktury sieciowej przy wykorzystaniu istniejącego okablowania |

* + 1. Przełącznik typ V – 1 komplet (2 sztuki)

|  |  |
| --- | --- |
| **Wymagane minimalne parametry techniczne urządzeń** | |
|  | Przełącznik FC musi być wykonany w technologii FC 16 Gb/s i posiadać możliwość pracy portów FC z prędkościami 16, 8, 4, 2 Gb/s z funkcją autonegocjacji prędkości. |
|  | Przełącznik FC musi posiadać przynajmniej 1 GB RAM. |
|  | Przełącznik FC musi posiadać minimum 24 sloty na moduły FC. Wszystkie wymagane funkcje muszą być dostępne dla minimum 12 portów FC przełącznika. |
|  | Przełącznik musi posiadać całkowitą przepustowość na poziomie 384 Gb/s w pełnym dupleksie wykorzystując agregację linków. |
|  | Przełącznik musi być dostarczony wraz z minimum 12 modułami FC 16 Gb/s oraz 8 kompatybilnymi kablami światłowodowymi o długości min. 3m |
|  | Przełącznik musi obsługiwać ramki o maksymalnym rozmiarze 2112 bajtów. |
|  | Rodzaj obsługiwanych portów: E, F, M, D, EX. |
|  | Przełącznik FC musi mieć wysokość maksymalnie 1 RU (jednostka wysokości szafy montażowej) i szerokość 19” oraz zapewniać techniczną możliwość montażu w szafie 19”. |
|  | Przełącznik FC musi posiadać nadmiarowe wentylatory. |
|  | Przełącznik FC musi być wykonany w tzw. architekturze „non-blocking” uniemożliwiającej blokowanie się ruchu wewnątrz przełącznika przy pełnej prędkości pracy wszystkich portów. |
|  | Przełącznik musi posiadać mechanizm balansowania ruchu między grupami połączeń tzw. „trunk” oraz obsługiwać grupy połączeń „trunk” dla nie więcej niż niż 8 portów 16Gb |
|  | Przełącznik FC musi udostępniać usługę Name Server Zoning - tworzenia stref (zon) w oparciu bazę danych nazw serwerów. |
|  | 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. Brak szczególnego info w dwóch datasheetach |
|  | Przełącznik FC musi posiadać wsparcie dla następujących mechanizmów zwiększających poziom bezpieczeństwa:   * Listy Kontroli Dostępu definiujące urządzenia (przełączniki i urządzenia końcowe) uprawnione do pracy w sieci Fabric * Definiowanie dostępu za pomocą ról poprzez RBAC * Możliwość uwierzytelnienia (autentykacji) przełączników z listy kontroli dostępu w sieci Fabric za pomocą protokołów DH-CHAP i FCAP * Możliwość uwierzytelnienia (autentykacji) urządzeń końcowych z listy kontroli dostępu w sieci Fabric za pomocą protokołu DH-CHAP * Kontrola dostępu administracyjnego definiująca możliwość zarządzania przełącznikiem tylko z określonych urządzeń oraz portów * Szyfrowanie połączenia z konsolą administracyjną. Wsparcie dla SSHv2, * Wskazanie nadrzędnych przełączników odpowiedzialnych za bezpieczeństwo w sieci typu Fabric. * Konta użytkowników definiowane w środowisku RADIUS lub LDAP * Szyfrowanie komunikacji narzędzi administracyjnych za pomocą SSL/HTTPS * Obsługa SNMP v3 |
|  | Przełącznik FC musi posiadać możliwość konfiguracji przez komendy tekstowe w interfejsie znakowym oraz przez przeglądarkę internetową z interfejsem graficznym. |
|  | Przełącznik FC musi mieć możliwość instalacji jednomodowych SFP+ umożliwiających bezpośrednie połączenie (bez dodatkowych urządzeń pośredniczących). |
|  | Przełącznik FC musi zapewnić możliwość jego zarządzania przez zintegrowany port Ethernet, szeregowy RJ-45, port USB oraz inband IP-over-FC |
|  | Przełącznik FC musi zapewniać wsparcie dla standardu zarządzającego SMI-S. |
|  | Przełącznik FC musi zapewniać możliwość nadawania adresu IP dla zarządzającego portu Ethernet za pomocą protokołu DHCP |
|  | Maksymalny dopuszczalny pobór mocy przełącznika FC to 80W |
|  | Przełącznik FC musi zapewniać możliwość dynamicznego aktywowania portów za pomocą zakupionych kluczy licencyjnych. |
|  | Przełącznik FC musi zapewniać opóźnienie przy przesyłaniu ramek FC między lokalnymi portami nie większe niż 800ns. |
|  | Przełącznik FC musi zapewniać sprzętową obsługę zoningu na podstawie portów i adresów WWN |
|  | Możliwość wymiany w trybie „na gorąco”: minimum w odniesieniu do modułów portów Fibre Channel (SFP). |
|  | Wsparcie dla N\_Port ID Virtualization (NPIV). |
|  | Min. 60 miesięcy gwarancji na urządzenie. Gwarancja powinna być świadczona w trybie 24h/7dni w tygodniu, z czasem reakcji najpóźniej do końca następnego dnia roboczego od momentu zgłoszenia awarii. |
|  | Produkt musi być fabrycznie nowy. |
|  | Szyny do montażu w szafie rack. |
|  | Wykonawca jest zobowiązany do wdrożenia infrastruktury Fibre Channel, które musi obejmować:  • montaż przełączników FC oraz podłączenie do serwerów i macierzy  • konfigurację przełączników FC |

1. Zasilacz awaryjny – 1 komplet
   1. Zasilacz awaryjny I – 1 szt.

|  |  |  |
| --- | --- | --- |
| **Lp** | **Nazwa komponentu** | **Wymagane minimalne parametry techniczne urządzenia** |
| **1** | **2** | **3** |
| 1 | Klasa produktu | Zasilacz awaryjny |
| 2 | Typ obudowy | 4U |
| 3 | Moc pozorna | 6000 VA |
| 4 | Moc rzeczywista | 6000 Wat |
| 5 | Architektura | online z podwójną konwersją |
| 6 | Liczba i rodzaj gniazdek z utrzymaniem zasilania | 6 x IEC320 C13 (10A)  4 x IEC320 C19 (16A)  2 x IEC Jumpers  1 x połączenie stałe 3 przewody (H N+G) |
| 7 | Czas podtrzymania dla obciążenia 100% | Min. 2 min. |
| 8 | Czas podtrzymania przy obciążeniu 50% | Min. 8 min. |
| 9 | Porty komunikacji | 10/100 BaseT (RJ45)  USB  SmartSlot  RJ-45 Serial |
| 10 | Wyświetlacz | Wyświetlacz LCD |
| 11 | Dodatkowe funkcje | Awaryjny wyłącznik zasilania |
| 12 | Wyposażenie dodatkowe | Karta zarządzająca z dedykowanym portem RJ-45 umożliwiająca podłączenie za pomocą protokołu TCP/IP  3x zewnętrzny moduł bateryjny producenta UPS o wysokości maksymalnej 3U dedykowany do UPS 6000 VA |
| 13 | Gwarancja | 60 miesięcy na zasilacz, 24 miesiące na baterie |

* + 1. Zasilacz awaryjny II – 1 szt.

|  |  |  |
| --- | --- | --- |
| **Lp.** | **Nazwa komponentu** | **Wymagane minimalne parametry techniczne urządzenia** |
| **1** | **2** | **3** |
| 1 | Klasa produktu | Zasilacz awaryjny |
| 2 | Typ obudowy | 2 U |
| 3 | Moc pozorna | 750 VA |
| 4 | Moc rzeczywista | 600 Wat |
| 5 | Architektura | Line - interactive |
| 6 | Liczba i rodzaj gniazdek z utrzymaniem zasilania | 8 x IEC320 C13 |
| 7 | Czas podtrzymania dla obciążenia 100% | Min. 10 min. |
| 8 | Czas podtrzymania przy obciążeniu 50% | Min. 30 min. |
| 9 | Porty komunikacji | RS232 (DB9)  SmartSlot  USB |
| 10 | Wyświetlacz | Wyświetlacz LCD |
| 11 | Dodatkowe funkcje | Awaryjny wyłącznik zasilania |
| 12 | Wyposażenie dodatkowe | Karta zarządzająca LAN |
| 13 | Gwarancja | 24 miesiące na zasilacz |

1. Szafa rack - 1 szt.

|  |  |  |
| --- | --- | --- |
| **Lp.** | **Nazwa komponentu** | **Wymagane minimalne parametry techniczne urządzenia** |
| **1** | **2** | **3** |
| 1 | Klasa produktu | Szafa i rama krosowa |
| 2 | Wysokość | 42 U |
| 3 | Wymiary minimalne | 1990 x 600 x 1000 mm (wysokość x szerokość x głębokość) |
| 4 | Nośność | 1000 kg |
| 5 | Cechy | możliwość montażu drzwi jako lewo i prawo stronnych  - Wentylowane drzwiczki ze skalowalnymi opcjami chłodzenia  - Drzwi i panele boczne zamykane na klucz  - Odłączane drzwi tylne  - Montaż bez użycia narzędzi  - Regulowana głębokość montażowa  - Możliwość zdjęcia osłon bocznych  - dodatkowo wymagane są min. 4 listwy zasilające typu rack 16A, minimum 8 gniazd wyjściowych. Z gniazdem wejściowym typu C14 do UPS, minimalna długość przewodu zasilającego 3m |
| 6 | Gwarancja | 24 miesiące |

1. Serwer typu NAS – 1 szt.

|  |  |  |
| --- | --- | --- |
| **Lp.** | **Nazwa komponentu** | **Wymagane minimalne parametry techniczne urządzenia** |
| **1** | **2** | **3** |
| 1 | Typ serwera | Serwer sieciowy typu NAS |
| 2 | Obudowa | Obudowa montowana w szafie 19" typu rack o wysokości 2U  8 kieszeni na dyski 3,5”, zabezpieczone przed wysunięciem dysku: kluczem lub **zatrzaskiem montowanym na obudowie**  Dostarczony wraz z komplet szyn montażowych |
| 3 | Zainstalowana pojemność | Pojemność zainstalowanych dysków: 48TB  Dyski muszą posiadać rekomendację producenta do urządzeń typu NAS  Interfejs dysku nie wolniejszy niż SATA/600 |
| 4 | Złącza | **Min. 4x 1GB Ethernet**  **2 x USB 3.0**  **2 x USB 2.0** |
| 5 | Obsługa RAID | Kontroler RAID musi wspierać raid: 0, 1, 5, 6, 10, 5+0(50) |
| 6 | Płyta główna | Procesor minimum 4 rdzeniowy 2.0GHz |
| 7 | Wbudowana pamięć RAM | Musi posiadać fabrycznie zainstalowane 4096MB pamięci RAM |
| 8 | Gwarancja | 36 miesięcy |

1. Oprogramowanie do backupu – 1 komplet

|  |  |  |
| --- | --- | --- |
| **Lp.** | **Nazwa komponentu** | **Wymagane minimalne parametry techniczne oprogramowania** |
| **1** | **2** | **3** |
| 1 | Typ oprogramowania | Oprogramowanie do backupu |
| 2 | Funkcje | • Oprogramowanie musi współpracować min. z infrastrukturą VMware w wersji 4.1, 5.0, 5.1, 5.5, 6.0 oraz Microsoft Hyper-V 2012 i 2012 R2. Wszystkie funkcjonalności w specyfikacji muszą być dostępne na wszystkich wspieranych platformach wirtualizacyjnych, chyba, że wyszczególniono inaczej  • Oprogramowanie musi współpracować min. z hostami zarządzanymi przez VMware vCenter oraz pojedynczymi hostami.  • Oprogramowanie musi współpracować min. z hostami zarządzanymi przez System Center Virtual Machine Manager, klastrami hostów oraz pojedynczymi hostami.  • Oprogramowanie musi zapewniać tworzenie kopii zapasowych wszystkich systemów operacyjnych maszyn wirtualnych wspieranych przez vSphere i Hyper-V  Oprogramowanie musi być niezależne sprzętowo i umożliwiać wykorzystanie dowolnej platformy serwerowej i dyskowej  • Oprogramowanie musi tworzyć “samowystarczalne” archiwa do odzyskania których nie wymagana jest osobna baza danych z metadanymi deduplikowanych bloków  • Oprogramowanie musi mieć mechanizmy deduplikacji i kompresji w celu zmniejszenia wielkości archiwów. Włączenie tych mechanizmów nie może skutkować utratą jakichkolwiek funkcjonalności wymienionych w tej specyfikacji  • Oprogramowanie musi zapewniać warstwę abstrakcji nad poszczególnymi urządzeniami pamięci masowej, pozwalając utworzyć jedną wirtualną pulę pamięci na kopie zapasowe. Wymagane jest wsparcie dla co najmniej trzech pamięci masowych w takiej puli.  • Oprogramowanie nie może przechowywać danych o deduplikacji w centralnej bazie. Utrata bazy danych używanej przez oprogramowanie nie może prowadzić do utraty możliwości odtworzenia backupu. Metadane deduplikacji muszą być przechowywane w plikach backupu.  • Oprogramowanie nie może instalować żadnych stałych agentów wymagających wdrożenia czy upgradowania wewnątrz maszyny wirtualnej dla jakichkolwiek funkcjonalności backupu lub odtwarzania  • Oprogramowanie musi zapewniać backup jednoprzebiegowy - nawet w przypadku wymagania granularnego odtworzenia  • Oprogramowanie musi zapewniać mechanizmy informowania o wykonaniu/błędzie zadania poprzez email lub SNMP. W środowisku VMware musi mieć możliwość aktualizacji pola „notatki” na wirtualnej maszynie  • Oprogramowanie musi mieć możliwość uruchamiania dowolnych skryptów przed i po zadaniu backupowym lub przed i po wykonaniu zadania snapshota w środowisku VMware.  • Oprogramowanie musi oferować portal samoobsługowy, umożliwiający odtwarzanie użytkownikom wirtualnych maszyn, obiektów MS Exchange i baz danych MS SQL (w tym odtwarzanie point-in-time)  • Oprogramowanie musi zapewniać bezpośrednią integrację min. z VMware vCloud Director 5.1, 5.5, 5.6 i 8.0 i archiwizować również metadane vCD. Musi też umożliwiać odtwarzanie tych metadanych do vCD  • Oprogramowanie musi mieć wbudowane mechanizmy backupu konfiguracji w celu prostego odtworzenia systemu po całkowitej reinstalacji  • Oprogramowanie musi mieć wbudowane mechanizmy szyfrowania zarówno plików z backupami jak i transmisji sieciowej. Włączenie szyfrowania nie może skutkować utratą jakiejkolwiek funkcjonalności wymienionej w tej specyfikacji  • Oprogramowanie musi oferować zarządzanie kluczami w przypadku utraty podstawowego klucza  • Oprogramowanie musi wspierać min. backup maszyn wirtualnych używających współdzielonych dysków VHDX na Hyper-V (shared VHDX)  • Oprogramowanie musi posiadać architekturę klient/serwer z możliwością instalacji wielu instancji konsoli administracyjnych.  • Oprogramowanie musi wykorzystywać mechanizmy Change Block Tracking na wszystkich wspieranych platformach wirtualizacyjnych. Mechanizmy muszą być certyfikowane przez dostawcę platformy wirtualizacyjnej  • Oprogramowanie musi oferować możliwość sterowania obciążeniem storage'u produkcyjnego tak aby nie przekraczane były skonfigurowane przez administratora backupu poziomy latencji. Funkcjonalność ta musi być dostępna na wszystkich wspieranych platformach wirtualizacyjnych  • Oprogramowanie musi automatycznie wykrywać i usuwać snapshoty-sieroty (orphaned snapshots), które mogą zakłócić poprawne wykonanie backupu. Proces ten nie może wymagać interakcji administratora  • Oprogramowanie musi wspierać kopiowanie backupów na taśmy wraz z pełnym śledzeniem wirtualnych maszyn  • Oprogramowanie musi mieć możliwość wydzielenia osobnej roli typu tape server  • Oprogramowanie musi mieć możliwość kopiowania backupów do lokalizacji zdalnej  • Oprogramowanie musi mieć możliwość tworzenia retencji GFS (Grandfather-Father-Son)  • Oprogramowanie musi umieć korzystać z protokołu DDBOOST w przypadku gdy repozytorium backupów jest umiejscowione na EMC DataDomain. Funkcjonalność powinna wspierać łącze sieciowe lub FC.  • Oprogramowanie musi umieć korzystać z protokołu Catalyst w przypadku gdy repozytorium backupów jest umiejscowione na HP StoreOnce. Funkcjonalność powinna wspierać łącze sieciowe lub FC.  • Oprogramowanie musi mieć możliwość replikacji włączonych wirtualnych maszyn min. bezpośrednio z infrastruktury VMware vSphere, pomiędzy hostami ESXi, włączając asynchroniczną replikacją ciągłą. Dodatkowo oprogramowanie musi mieć możliwość użycia plików kopii zapasowych jako źródła replikacji.  • Oprogramowanie musi umożliwiać przechowywanie punktów przywracania dla replik  • Oprogramowanie musi umożliwiać wykorzystanie istniejących w infrastrukturze wirtualnych maszyn jako źródła do dalszej replikacji (replica seeding)  • Oprogramowanie musi posiadać takie same funkcjonalności replikacji dla Hyper-V  • Oprogramowanie musi wykorzystywać wszystkie oferowane przez hypervisor tryby transportu (sieć, hot-add, LAN Free-SAN)  • Oprogramowanie musi dawać możliwość tworzenia backupów ad-hoc z konsoli jak i z klienta webowego vSphere  • Oprogramowanie musi przetwarzać wiele wirtualnych dysków jednocześnie (parallel processing)  • Oprogramowanie musi umożliwić uruchomienie wielu maszyn wirtualnych bezpośrednio ze zdeduplikowanego i skompresowanego pliku backupu, z dowolnego punktu przywracania, bez potrzeby kopiowania jej na storage produkcyjny. Funkcjonalność musi być oferowana niezależnie od rodzaju storage’u użytego do przechowywania kopii zapasowych.  • Oprogramowanie musi pozwalać na migrację on-line tak uruchomionych maszyn na storage produkcyjny. Migracja powinna odbywać się mechanizmami wbudowanymi w hypervisor. Jeżeli licencja na hypervisor nie posiada takich funkcjonalności - oprogramowanie musi realizować jaką migrację swoimi mechanizmami  • Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny, plików konfiguracji i dysków  • Oprogramowanie musi umożliwić odtworzenie plików na maszynę operatora, lub na serwer produkcyjny bez potrzeby użycia agenta instalowanego wewnątrz wirtualnej maszyny. Funkcjonalność ta nie powinna być ograniczona wielkością i liczbą przywracanych plików  • Oprogramowanie musi mieć możliwość odtworzenia plików min. przy pomocy VMware VIX API  • Oprogramowanie musi wspierać odtwarzanie plików min. z następujących systemów plików:  o Linux (ext, ext2, ext3, ext4, ReiserFS (Reiser3), JFS, XFS, Btrfs)  o BSD (UFS, UFS2)  o Solaris (ZFS)  o Mac (HFS, HFS+)  o Windows (NTFS, FAT, FAT32, ReFS)  • Oprogramowanie musi wspierać przywracanie plików z partycji Linux LVM  • Oprogramowanie musi umożliwiać szybkie granularne odtwarzanie obiektów aplikacji bez użycia jakiegokolwiek agenta zainstalowanego wewnątrz maszyny wirtualnej.  • Oprogramowanie musi wspierać granularne odtwarzanie dowolnych obiektów i dowolnych atrybutów usługi katalogowej włączając hasło, obiekty Group Policy, partycja konfiguracji AD, rekordy DNS zintegrowane z AD.  • Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Exchange 2010 i nowszych (dowolny obiekt w tym obiekty w folderze "Permanently Deleted Objects"),  • Oprogramowanie musi wspierać granularne odtwarzanie Microsoft SQL 2005 i nowsze włączając bazy danych z opcją odtwarzania point-in-time, tabele, schemat  • Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Sharepoint 2010 i nowsze. Opcja odtworzenia elementów, witryn, uprawnień.  • Oprogramowanie musi wspierać granularne odtwarzanie baz danych Oracle z opcją odtwarzanie point-in-time. Funkcjonalność ta musi być dostępna dla baz uruchomionych w środowiskach Windows oraz Linux.  • Funkcjonalność ta nie może wymagać pełnego odtworzenia wirtualnej maszyny ani jej uruchomienia.  • Oprogramowanie musi indeksować pliki Windows i Linux w celu szybkiego wyszukiwania plików w plikach backupowych.  • Oprogramowanie musi używać mechanizmów VSS wbudowanych w system operacyjny Microsoft Windows  • Oprogramowanie musi wspierać także specyficzne metody odtwarzania w tym "reverse CBT" oraz odtwarzanie z wykorzystaniem sieci SAN  • Oprogramowanie musi dawać możliwość stworzenia laboratorium (izolowane środowisko) dla vSphere i Hyper-V używając wirtualnych maszyn uruchamianych bezpośrednio z plików backupu. Dla VMware’a oprogramowanie musi pozwalać na uruchomienie takiego środowiska bezpośrednio ze snapshotów macierzowych stworzonych na wspieranych urządzeniach.  • Oprogramowanie musi umożliwiać weryfikację odtwarzalności wielu wirtualnych maszyn jednocześnie z dowolnego backupu według własnego harmonogramu w izolowanym środowisku. Testy powinny uwzględniać możliwość uruchomienia dowolnego skryptu testującego również aplikację uruchomioną na wirtualnej maszynie. Testy muszą być przeprowadzone bez interakcji z administratorem |
| 3 | Licencjonowanie | Oprogramowanie musi być licencjonowanie w modelu “per-CPU” lub “per-2CPU”. |
| 4 | Wsparcie techniczne | 36 miesięcy |