# **Serwer typu rack Ilość sztuk: 4**

**Oferowany model \* …………………….. Producent \* …………………..**

|  |  |
| --- | --- |
| **L.p.** | **Opis wymagań minimalnych** |
| 1 | Obudowa | 1. Serwer przeznaczony do montażu w szafie rack 19”;
2. Maksymalna wysokość max. 3U;
3. Serwer dostarczony z elementami umożliwiającymi montaż w szafie rack ( w tym komplet kabli zasilających, ramię umożliwiające swobodne wysuwanie serwera z szafy bez potrzeby odłączania kabli);
4. Wnęki dyskowe umożliwiające zamontowanie minimum 24 dysków 2,5” typu „hot- plug” od zewnątrz obudowy;
5. Wentylatory redundantne typu „hot-plug”;
6. Minimum 2 zasilacze typu „hot-plug” (1 redundantny);
7. Znajdująca/-y się na froncie obudowy panel LCD lub sygnalizacja diodami LED, umożliwiająca/-y wyświetlanie informacji o stanie co najmniej: pamięci RAM, dysków, slotów PCIe.
8. Wbudowany czujnik otwarcia obudowy współpracujący z kartą zarządzającą
 |
| 2 | Procesor | 1. Serwer osiągający wynik SPECint\_rate2006base minimum 3280 pkt. lub SPECrate2017\_int\_base minimum 348 pkt.
2. Testy dla oferowanego modelu serwera w oferowanej konfiguracji (model serwera/procesory) muszą być opublikowane i ogólnie dostępne na stronie [www.spec.org.](http://www.spec.org/)
 |
| 3 | Płyta główna | 1. Przystosowana do pracy ciągłej,
2. Minimum 13 slotów PCIe trzeciej generacji, z czego minimum 6 slotów PCIe x16. Wszystkie sloty powinny umożliwiać instalację kart pełnej wysokości.
3. W każdym przypadku opis slotu dotyczy jego przepustowości, a nie tylko długości.
4. Minimum 9 slotów pozostaje dostępne pod przyszłe potrzeby.
5. Płyta główna obsługująca minimum 6 TB pamięci RAM.
6. Na płycie głównej powinno znajdować się minimum 48 slotów przeznaczonych dla pamięci RAM.
 |
| 4 | Pamięć | Pamięć RAM minimum 3072 GB DDR4. |
| 5 | Karta graficzna | Umożliwiająca poprawne wyświetlenie obrazu w rozdzielczości 1600x900. |
| 6 | Kontroler macierzowy | Dedykowany kontroler SAS 12Gbps obsługujący RAID 0, 1, 5, 10, 50 |
| 7 | Dyski HDD | 1. 2 dyski SSD o pojemności nie mniej niż 480 GB SAS/SATA każdy, kompatybilne z technologią VMware Flash Read Cache.
2. Możliwość instalacji dysków SATA, SAS, NL-SAS i SSD.
3. Wymagany jeden dodatkowy dysk niezamontowany, takiego samego modelu i typu jak zainstalowane w obudowie.
 |
| 8 | Oprogramowanie | Komplet sterowników na CD lub DVD.  |
| 9 | Zarządzanie serwerem | 1. Karta zarządzająca niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca:
2. zdalny dostęp do graficznego interfejsu Web karty zarządzającej;
3. zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera);
4. szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika;
5. możliwość podmontowania zdalnych wirtualnych napędów;
6. wirtualną konsolę z dostępem do myszy, klawiatury;
7. wsparcie dla IPv6;
8. wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish;
9. możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer;
10. możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer;
11. integracja z Active Directory;
12. możliwość obsługi przez dwóch administratorów jednocześnie;
13. wsparcie dla dynamic DNS;
14. wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej.
15. możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera
16. możliwość zarządzania do 50 serwerów bezpośrednio z konsoli karty zarządzającej pojedynczego serwera
17. Karta powinna posiadać wbudowaną wewnętrzną pamięć SD lub USB o pojemności 16GB do przechowywania sterowników i firmware'ów komponentów serwera, umożliwiająca szybką instalację wspieranych systemów operacyjnych.
18. Dodatkowe oprogramowanie umożliwiające zarządzanie poprzez sieć, spełniające minimalne wymagania:
19. możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta;
20. wsparcie dla protokołów – WMI, SNMP, IPMI, WSMan, SSH;
21. możliwość oskryptowywania procesu wykrywania urządzeń;
22. możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram;
23. opis wykrytych systemów oraz ich komponentów;
24. możliwość eksportu raportu do CSV, HTML, XLS;
25. grupowanie urządzeń w oparciu o kryteria użytkownika;
26. automatyczne skrypty CLI umożliwiające dodawanie i edycję grup urządzeń;
27. podgląd stanu środowiska;
28. podsumowanie stanu dla każdego urządzenia;
29. szczegółowy status urządzenia/elementu/komponentu;
30. generowanie alertów przy zmianie stanu urządzenia;
31. filtry raportów umożliwiające podgląd najważniejszych zdarzeń;
32. integracja z service desk producenta dostarczonej platformy sprzętowej;
33. możliwość przejęcia zdalnego pulpitu;
34. możliwość podmontowania wirtualnego napędu;
35. automatyczne zaplanowanie akcji dla poszczególnych alertów w tym automatyczne tworzenie zgłoszeń serwisowych w oparciu o standardy przyjęte przez producentów oferowanego w tym postępowaniu serwerów;
36. kreator umożliwiający dostosowanie akcji dla wybranych alertów;
37. możliwość importu plików MIB;
38. przesyłanie alertów „as-is” do innych konsol firm trzecich;
39. aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania);
40. możliwość instalacji sterowników i oprogramowania wewnętrznego bez potrzeby instalacji agenta;
41. możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów; moduł raportujący pozwalający na wygenerowanie następujących informacji: nr seryjny sprzętu, konfiguracja poszczególnych urządzeń, wersje oprogramowania wewnętrznego, obsadzenie slotów PCIe i gniazd pamięci, aktualne informacje o stanie gwarancji, adresy IP kart sieciowych.
 |
| 10 | Karty sieciowe | 1. Minimum 4 porty typu 1 Gigabit Ethernet wbudowane na płycie głównej ze wsparciem dla protokołu IPv6.
2. Dwie dwuportowe karty konwergentne PCIe posiadające 2 porty typu 10 Gigabit Ethernet.
3. Pojedyncza karta powinna umożliwiać wirtualizację do minimum 16 kart sieciowych oraz zapewniać wsparcie dla protokołu iSCSI i FCoE (tym uruchamiania systemu z zasobów dyskowych udostępnianych tymi protokołami).
4. Dwie karty jednoportowe FC o prędkości minimalnej 16 Gb/s umożliwiające uruchamianie systemu z zasobów udostępnianych po FC.
5. Wszystkie karty muszą być obsadzone odpowiednimi wkładkami.
 |
| 11 | Porty | 1. 5 x USB 3.0 z czego nie mniej niż 2 na przednim panelu obudowy i jeden wewnętrzny, 6 x RJ-45, 2xVGA z czego jeden na panelu przednim.
2. Nie dopuszcza się stosowania konwerterów/przejściówek.
 |
| 12 | Inne wymagania | 1. Dokumentacja użytkownika.
2. Do serwera dołączona musi być szczegółowa informacja o konfiguracji sprzętowej urządzenia i jego pełnej funkcjonalności oraz lista wszystkich nieulotnych nośników danych (również wbudowanych)..
 |
| 13 | Certyfikaty | 1. **Certyfikat IS09001 dla Producenta sprzętu obejmujący proces projektowania i produkcji.**
2. **ISO 14001 dla Producenta sprzętu. Deklaracja zgodności CE.**
3. **Oferowany model serwera musi znajdować się na liście kompatybilności sprzętowej dla serwerowych systemów operacyjnych VmWare dla najnowszej wersji tych systemów operacyjnych przed dniem składania ofert.**
4. **Oferowany model serwera musi znajdować się na liście kompatybilności sprzętowej dla serwerowych systemów operacyjnych Microsoft, dla najnowszej wersji tych systemów operacyjnych przed dniem składania ofert.**
 |

# **Oprogramowanie wirtualizacyjne Ilość sztuk: 1**

**Oferowany model \* …………………….. Producent \* …………………..**

|  |  |
| --- | --- |
| **Lp.** | **Opis wymagań minimalnych** |
| 1. | Licencje | 1) Licencje muszą umożliwiać uruchamianie oprogramowania do wirtualizacji na dostarczanych serwerach fizycznych o łącznej liczbie 16 procesorów oraz jednej konsoli do zarządzania całym środowiskiem.1. Wszystkie licencje powinny być dostarczone wraz ze wsparciem, świadczonym przez producenta oprogramowania na pierwszym, drugim i trzecim poziomie, które powinno umożliwiać zgłaszanie problemów 7 dni w tygodniu przez 24h/dobę. Po zakończeniu okresu wsparcia Zamawiający musi mieć możliwość dalszego korzystania z dostarczonego rozwiązania bez aktywnej umowy serwisowej lub przedłużyć wsparcie na kolejny okres. Wsparcie musi obejmować co najmniej:
	1. dostęp do aktualizacji oprogramowania w ramach dostarczonych licencji,
	2. możliwość podnoszenia wersji dostarczonych licencji,
	3. nielimitowany dostępu do wsparcia producenta za pomocą przynajmniej zgłoszenia telefonicznego, formularza na stronie internetowej, z czasem reakcji maksymalnie następnego dnia roboczego,
	4. wsparcie nie może mieć limitu ilości zgłoszeń,
	5. dostęp do zasobów wiedzy producenta i forum technicznych - na stronie producenta.
2. Dostarczona licencja na powyższe oprogramowanie musi posiadać możliwość swobodnego przeniesienia na dowolny serwer fizyczny będący w posiadaniu Zamawiającego (bez ograniczeń licencji OEM). Licencje dostępne w modelu licencjonowania na sztuki. Każda sztuka może zarządzać dowolną ilością serwerów fizycznych na której zainstalowanej jest oprogramowanie do wirtualizacji.
3. Dostarczone licencje oprogramowania muszą wspierać posiadane przez Zamawiającego rozwiązanie VmWare vCenter.
4. Dostarczone licencje oprogramowania wirtualizacyjnego muszą wspierać oprogramowanie do migracji i zarządzania maszynami wirtualnymi w ośrodku Podstawowym oraz Zapasowym opisanie w pkt VI.
 |
| 2 | Wymagania techniczne dotyczące oprogramowania | 1. Warstwa wirtualizacji musi być rozwiązaniem dedykowanym do tego celu, niewymagającym istnienia jakiegokolwiek systemu operacyjnego do pracy hypervisor'a.
2. W ramach rozwiązania musi istnieć możliwość podłączenia i zarządzania każdym, pojedynczym serwerem fizycznym za pomocą graficznej konsoli (klienta) z pominięciem centralnego serwera zarządzającego środowiskiem wirtualnym
3. Rozwiązanie musi zapewnić możliwość obsługi wielu instancji systemów operacyjnych na jednym serwerze fizycznym i musi się charakteryzować maksymalnym możliwym stopniem konsolidacji sprzętowej.
4. Oprogramowanie do wirtualizacji musi działać na serwerach fizycznych posiadających do 320 procesorów logicznych.
5. Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych z możliwością dostępu do 1TB pamięci operacyjnej.
6. Oprogramowanie do wirtualizacji musi zapewnić możliwość przydzielenia maszynom wirtualnym co najmniej 64 procesorów wirtualnych.
7. Oprogramowanie do wirtualizacji musi zapewnić obsługę 16 węzłów NUMA na pojedynczym serwerze fizycznym.
8. Oprogramowanie do wirtualizacji musi zapewnić obsługę co najmniej 4TB pamięci RAM na pojedynczym serwerze fizycznym.
9. Oprogramowanie do wirtualizacji musi zapewnić obsługę serwisowania dysków SSD poprzez ich podłączanie i odłączanie od serwera bez konieczności jego wyłączenia.
10. Rozwiązanie musi umożliwiać łatwą i szybką rozbudowę infrastruktury o nowe usługi bez spadku wydajności i dostępności pozostałych wybranych usług.
11. Rozwiązanie musi w możliwie największym stopniu być niezależne od producenta platformy sprzętowej.
12. Rozwiązanie musi wspierać następujące systemy operacyjne: Windows Server 2012R2, RedHat Enterprise, CentOS.
13. Rozwiązanie musi umożliwiać przydzielenie większej ilości pamięci RAM dla maszyn wirtualnych niż fizyczne zasoby RAM serwera w celu osiągniecia maksymalnego współczynnika konsolidacji.
14. Rozwiązanie musi posiadać centralną konsolę graficzną do zarządzania maszynami wirtualnymi, zasobami macierzowymi i zwirtualizowanymi hostami fizycznymi. Musi pozwalać na stworzenie klastra wysokiej dostępności przy wykorzystaniu przynajmniej czterech zwirtualizowanych hostów.
15. Centralna graficzna konsola administracyjna musi być dostępna co najmniej na system operacyjny Windows 7.
16. Rozwiązanie musi zapewnić możliwość monitorowania wykorzystania zasobów fizycznych infrastruktury wirtualnej.
17. Oprogramowanie do wirtualizacji musi zapewnić możliwość wykonywania kopii zapasowych z instancji systemów operacyjnych oraz ich odtworzenia w możliwie najkrótszym czasie.
18. Mechanizm wykonywania kopii zapasowych musi posiadać wbudowane algorytmy de-duplikacji danych zmienną długością bloku danych oraz wbudowaną możliwość replikacji kopii zapasowych do rozwiązań sprzętowych firm trzecich.
19. Oprogramowanie do wirtualizacji musi zapewnić możliwość wykonywania kopii migawkowych instancji systemów operacyjnych na potrzeby tworzenia kopii zapasowych bez przerywania ich pracy.
20. Oprogramowanie do wirtualizacji musi zapewnić możliwość klonowania systemów operacyjnych wraz z ich pełną konfiguracją i danymi.
21. Oprogramowanie zarządzające musi posiadać możliwość przydzielania i konfiguracji uprawnień z możliwością integracji z usługami katalogowymi Microsoft Active Directory.
22. Oprogramowanie do wirtualizacji musi obsługiwać przełączenie ścieżek SAN (bez utraty komunikacji) w przypadku awarii jednej z dwóch ścieżek.
23. Platforma wirtualizacyjna musi umożliwiać zastosowanie w serwerach fizycznych procesorów o dowolnej ilości rdzeni.
24. Rozwiązanie musi umożliwiać udostepnienie maszynie wirtualnej większej ilości zasobów dyskowych niż fizycznie zarezerwowane.
25. Rozwiązanie musi umożliwiać tworzenie jednorodnych wolumenów logicznych o wielkości do 64TB
26. Oprogramowanie musi umożliwiać tworzenie wirtualnych dysków dla maszyn wirtualnych o pojemności do 62 TB.
27. Oprogramowanie do wirtualizacji musi wspierać uruchamianie maszyn wirtualnych z systemem Windows Server 2012 w konfiguracji klastra Failover.
28. System musi w pełni wykorzystywać 8 Gb/s lub 16Gb/s połączenia FC w obrębie sieci SAN.
29. System musi posiadać funkcjonalność wirtualnego przełącznika (switch) umożliwiającego tworzenie sieci wirtualnej w obszarze hosta i pozwalającego połączyć maszyny wirtualne w obszarze jednego hosta, a także na zewnątrz sieci fizycznej.
30. Rozwiązanie musi mieć możliwość przenoszenia maszyn wirtualnych w czasie ich pracy pomiędzy serwerami fizycznymi.
31. Rozwiązanie musi zapewnić ciągłą pracę usług. Usługi krytyczne biznesowo muszą działać bez przestoju, czas niedostępności innych usług nie powinien przekraczać kilkunastu minut.
32. Mechanizmy wysokiej dostępności muszą funkcjonować prawidłowo niezależnie od skali awarii (np. awaria większości środowiska) jak jej zaistnienia w czasie (jednoczesne wyłączenie całej platformy)
33. Musi zostać zapewniona odpowiednia redundancja i nadmiarowość zasobów tak by w przypadku awarii np. serwera fizycznego usługi na nim świadczone zostały przełączone na inne serwery infrastruktury.
34. Rozwiązanie musi umożliwiać łatwe i szybkie ponowne uruchomienie systemów/usług w przypadku awarii poszczególnych elementów infrastruktury.
35. Rozwiązanie musi zapewniać mechanizm bezpiecznego uaktualniania warstwy wirtualizacyjnej, (np. wgrywania patch-y) tak, aby zminimalizować ryzyko awarii systemu na skutek wprowadzenia zamiany.
36. Rozwiązanie musi zapewniać pracę bez przestojów dla wybranych maszyn wirtualnych, niezależnie od systemu operacyjnego oraz aplikacji, podczas awarii serwerów fizycznych, bez utraty danych i dostępności danych podczas awarii serwerów fizycznych.
37. Rozwiązanie musi umożliwiać dodawanie i rozszerzanie dysków wirtualnych, procesorów i pamięci RAM podczas pracy wybranych systemów.
38. Czas planowanego przestoju usług związany z koniecznością prac serwisowych (np. rekonfiguracja serwerów, macierzy, switchy) musi być ograniczony do minimum.
39. Rozwiązanie musi umożliwiać przenoszenie usług pomiędzy serwerami fizycznymi oraz wolumenami dyskowymi, bez przerywania pracy usług.
 |
| 3 | Zarządzanie  | 1. Rozwiązanie musi posiadać centralną konsolę graficzną do zarządzania maszynami wirtualnymi i do konfigurowania innych funkcjonalności. Centralna konsola graficzna powinna działania, jako aplikacja na maszynie wirtualnej, jako gotowa, wstępnie skonfigurowana maszyna wirtualna tzw. virtual appliance.
2. Konsola graficzna musi być dostępna poprzez dedykowanego klienta (za pomocą przeglądarek, minimum IE i Firefox) lub poprzez konsolę graficzną, która zbudowana jest z wykorzystaniem standardu HTML5
3. Dostęp przez przeglądarkę do konsoli graficznej musi być skalowalny tj. powinien umożliwiać rozdzielenie komponentów na wiele instancji w przypadku zapotrzebowania na dużą liczbę jednoczesnych dostępów administracyjnych do środowiska.
4. Rozwiązanie musi posiadać natywne mechanizmy do wykonywania kopii zapasowej swojej konfiguracji. Dodatkowo musi być możliwość ustawienia harmonogramu wykonywania kopii zapasowej.
5. Rozwiązanie musi posiadać interfejs graficzny do prowadzenia prac administracyjnych w zakresie swojej konfiguracji oraz monitoringu (możliwość monitorowania obciążenia min. vCPU, vRAM, vHDD, sieci, bazy danych). Interfejs graficzny powinien być wykonany w standardzie HTML5.
6. Rozwiązanie musi zapewniać natywne mechanizmy HA w niezawodnej architekturze Active-Passive-Witness dla wszystkich składowych komponentów centralnej konsoli graficznej zarządzającej platformą wirtualną.
 |

# **Oprogramowanie do automatyzacji zadań przełączania maszyn wirtualnych Ilość sztuk: 2**

**Oferowany model \* …………………….. Producent \* …………………..**

|  |  |
| --- | --- |
| **Lp.** | **Opis wymagań minimalnych** |
| 1 | Automatyzacja zadań przełączania maszyn wirtualnych pomiędzy ośrodkami | 1. Rozwiązanie musi umożliwiać zapewnienie ochrony maszyn wirtualnych niezależnie od architektury DataCenter (Active-Active, Active-Pasive).
2. Rozwiązanie musi posiadać taką architekturę, aby umożliwiać wykonanie planu awaryjnego nawet w przypadku całkowitej niedostępności pojedynczego centrum danych.
3. Rozwiązanie musi umożliwiać przełączanie maszyn wirtualnych z systemami operacyjnymi minimum: Windows Server 2012, Windows Server 2016, Windows 7, Windows 8, SLES 12, REHL 7, Debian, CentOS, FreeBSD, Ubuntu.
4. Rozwiązanie musi umożliwiać integrację z mechanizmami replikacji macierzowej (Array-Based) oraz musi integrować się z replikacją natywną wirtualizatora w ten sposób, że zarządzanie procesami DR dla obu mechanizmów musi odbywać się za pomocą jednej centralnej konsoli zarządzającej całą platformą wirtualizacyjną.
5. Rozwiązanie musi umożliwiać zapewnienie ochrony maszyn wirtualnych z dyskami wirtualnymi oraz dyskami udostępnionymi maszynom wirtualnym wprost z macierzy typu Raw Device.
6. Rozwiązanie musi umożliwiać zapewnienie ochrony maszyn wirtualnych zlokalizowanych na macierzach typu FC, iSCSI, NFS.
7. Rozwiązanie musi być niezależne od producenta zastosowanego sprzętu fizycznego.
8. Rozwiązanie musi umożliwiać wykonywanie procedur przełączania usług IT z ośrodka podstawowego do ośrodka zapasowego (fail-over) i z powrotem (fail-back) w ramach jednego narzędzia/konsoli.
9. Rozwiązanie musi umożliwiać wykonywanie tzw. planowanego przełączania pojedynczych maszyn wirtualnych lub grup wirtualnych maszyn do ośrodka zapasowego, polegające na wykonaniu scenariusza na który składają się automatycznie następujące po sobie kroki: poprawne zamkniecie wirtualnych maszyn po stronie centrum podstawowego, resynchronizacja replik danych, prezentacja replik danych po stronie odtworzeniowej, uruchomienie maszyn wirtualnych w ośrodku zapasowym.
10. Rozwiązanie musi umożliwiać wykonywanie tzw. testowego przełączania pojedynczych maszyn wirtualnych lub grup wirtualnych maszyn do ośrodka zapasowego, polegające na uruchomieniu wszystkich lub wybranych usług w lokalizacji zapasowej, w izolowanej sieci LAN. Takie testowe przełączenie, nie może mieć wpływu na działanie usług produkcyjnych oraz samo przełączenie testowe nie może mieć wpływu na relacje replikacji danych.
11. Proces przełączania usług IT pomiędzy Centrami Przetwarzania Danych musi być automatyczny tzn. – nie wymagający interwencji administratora w żadnej warstwie infrastruktury – CPU, RAM, LAN, SAN.
12. Rozwiązanie musi umożliwiać tworzenie planów przełączeniowych, konfigurowanie tych planów i przypisywanie do nich maszyn wirtualnych. Plan przełączeniowy musi umożliwiać:
13. Tworzenie więcej niż jednego planu przełączeniowego,
14. przypisanie jednej lub wielu wirtualnych maszyn,
15. Określanie kolejności uruchamiania maszyn wirtualnych w momencie przełączenia,
16. zatrzymanie wybranych wirtualnych maszyn pracujących w ośrodku zapasowym zwalniając tym samym moc obliczeniową dla przełączanych maszyn
17. Zmianę adresacji IP maszyn wirtualnych,
18. Uruchamianie skryptów konfiguracyjnych w dowolnym momencie procesu przełączenia (w tym w maszynach wirtualnych).
19. Rozwiązanie musi umożliwiać ochronę maszyn wirtualnych pracujących w Centrach Przetwarzania o następującej architekturze:
20. Jeden do Jednego,
21. Wiele do Jednego,
22. A do B do C do A.
23. Rozwiązanie musi umożliwiać automatyczne generowanie raportów z historycznych przełączeń oraz ich eksportowanie do pliku HTML, XML, CSV, MS Excel lub MS Word.
24. **Rozwiązanie musi umożliwiać ochronę powyżej 75 maszyn wirtualnych w ramach jednej licencji.**
25. Rozwiązanie musi umożliwiać zapewnienie ochrony maszyn wirtualnych niezależnie od architektury DataCenter (Active-Active, Active-Pasive, Stretched Cluster).
26. Rozwiązanie musi umożliwiać ochronę maszyn wirtualnych z wykorzystaniem funkcjonalności migracji „online” maszyn wirtualnych pomiędzy różnymi konsolami do zarządzania środowiskami wirtualnymi.
27. Rozwiązanie musi umożliwiać ochronę wirtualnych maszyn w oparciu o technologię macierzową VASA.
28. Rozwiązanie musi umożliwiać ochronę maszyn wirtualnych poprzez integrację z rozwiązaniem do wirtualizacji sieci (SDN).
 |

# **Realizacja usług wdrożeniowych**

1. W ramach realizacji umowy Wykonawca dokona:
2. Dostawa kompletu Sprzętu i licencji Oprogramowania.
3. Montaż sprzętu według Projektu Technicznego w istniejącej szafie rack.
4. Podłączenie do zasilania elektrycznego w lokalizacji Zamawiającego.
5. Aktualizacja oprogramowania wewnętrznego (firmware) elementów Sprzętu do najnowszych rekomendowanych przez producenta wersji.
6. Podłączenie Sprzętu do sieci LAN oraz SAN wraz z konfiguracją urządzeń aktywnych sieci LAN oraz SAN (niezbędne okablowanie dostarcza Wykonawca).
7. Instalacja i konfiguracja zgodnie z klastra wirtualizacyjnego w ośrodku zapasowym wraz z konfiguracją dostarczanego oprogramowania do automatyzacji zadań przełączania maszyn wirtualnych w ośrodku podstawowym i zapasowym.
8. Rekonfiguracja posiadanych przez Zamawiającego macierzy dyskowych Dell EMC Unity 600 w ośrodku podstawowym i zapasowym do współpracy z oprogramowania do automatyzacji zadań przełączania maszyn wirtualnych pomiędzy ośrodkami.
9. Relokacja maszyn wirtualnych i podział na dwa ośrodki.
10. Rekonfiguracja posiadanego przez Zamawiającego systemu wykonywania kopii zapasowych.
11. Opracowanie dokumentacji powykonawczej oraz procedur eksploatacyjnych wdrożonych komponentów warstwy fizycznej i logicznej. Jako procedurę eksploatacyjną rozumie się opis zbioru czynności eksploatacyjnych mających na celu zrealizowane określonego zadania eksploatacyjnego np. wykonanie aktualizacji oprogramowania wirtualizacyjnego, przeniesienie maszyn wirtualnych pomiędzy ośrodkami, planowanego i nieplanowanego wyłączenia danego ośrodka, . Procedury muszą obejmować wszystkie czynności, jakie należy wykonać w celu monitorowania i utrzymania dostarczonych komponentów w poprawnym działaniu i zgodności z najnowszymi wersjami komponentów.

# **Warunki gwarancji i serwisu**

1. Wykonawca będzie świadczył usługi serwisu technicznego producenta w miejscu zainstalowania Sprzętu, obejmujące co najmniej:
	1. naprawy uszkodzeń sprzętowych (tzw. RMA);
	2. dostęp do pomocy technicznej za pośrednictwem strony www producenta.
2. Wykonawca będzie świadczył usługi serwisu technicznego producenta dla wszystkich komponentów sprzętowych i programowych oferowanych serwerów.
3. Nie później niż w dniu dostarczenia urządzeń Wykonawca dostarczy szczegółowe informacje dotyczące trybu zgłaszania awarii oraz punktów serwisowych (adresy, numery telefonów i faksów oraz adresy poczty elektronicznej) w okresie gwarancji. W przypadku jakichkolwiek zmian danych o serwisie Wykonawca niezwłocznie poinformuje o tym Zamawiającego pisemnie (dopuszcza się faks).
4. Wykonawca zapewni możliwość zgłaszania nieprawidłowego działania (awarii) urządzeń 24 godziny na dobę, 7 dni w tygodniu, 365 dni  w roku do serwisu producenta przez cały okres trwania umowy.
5. Zgłoszenie może być dokonywane w postaci zgłoszenia telefonicznego, za pomocą faksu, z wykorzystaniem serwisu WWW oraz za pomocą poczty elektronicznej, w języku polskim.
6. Opis procedury śledzenia bieżącego statusu zgłoszenia awarii Wykonawca przedstawi do 30 dni kalendarzowych od podpisania umowy, ale nie później niż w dniu dostarczenia urządzeń.
7. Naprawa będzie dokonywana w miejscu eksploatowania urządzeń z możliwością naprawy w serwisie Wykonawcy. Jeżeli naprawa u Zamawiającego nie będzie możliwa, koszty dostarczenia uszkodzonego urządzenia do punktu serwisowego oraz z punktu serwisowego do miejsca eksploatacji pokrywa Wykonawca.
8. W przypadku uszkodzenia sprzętu Zamawiający dopuszcza instalację w miejsce uszkodzonego sprzętu dostarczony przez Wykonawcę sprzęt zastępczy o tych samych parametrach jakie były dostarczone w dostawie. Nie dotyczy to pamięci dyskowych oraz innych urządzeń z nośnikami informacji.
9. W przypadku awarii dysku twardego lub innego nośnika danych, powodującej konieczność jego wymiany, uszkodzony dysk lub inny nośnik danych pozostanie u Zamawiającego. Koszty dysków twardych i innych nośników danych wymienianych z powodu awarii ponosi Wykonawca.
10. Po dokonaniu zgłoszenia awarii przez Zamawiającego, Wykonawca potwierdzi w terminie do 2 godzin jej przyjęcie za pomocą faksu lub poczty elektronicznej na wskazany przez Zamawiającego numer/adres e-mail.
11. Wykonawca jest zobowiązany usunięcia awarii urządzeń w terminie do 8 godzin od zgłoszenia awarii, przy czym awarie zgłaszane w dniach wolnych od pracy traktuje się jako zgłoszone o godzinie 8:00 następnego dnia roboczego.
12. W przypadku problemów technicznych, których nie można rozwiązać zdalnie, Wykonawca przyjedzie na miejsce eksploatacji urządzeń w celu wykonania naprawy, wymiany poszczególnych komponentów lub całego urządzenia w zależności od stopnia złożoności usterki.
13. Inżynier lub pracownik serwisu Wykonawcy przybywa na miejsce i kontynuuje czynności serwisowe, aż do momentu usunięcia awarii urządzenia lub do momentu opracowania rozwiązania zastępczego (obejścia problemu). Podczas usuwania awarii lub stosowania rozwiązania zastępczego Zamawiający wymaga stosowania jedynie komponentów o parametrach równoważnych lub lepszych niż komponenty wymienione.
14. W przypadku wystąpienia problemów z urządzeniem i oprogramowaniem do tego urządzenia objętym serwisem wynikających z przeprowadzonej aktualizacji, Wykonawca niezwłocznie wykona powrót do poprzednich wersji i zapewni rozwiązanie problemów przed ponownym przystąpieniem do wykonania aktualizacji.
15. W okresie gwarancji na urządzenia objęte świadczeniem usług serwisowych Zamawiający ma prawo do powierzania urządzeń, stanowiących przedmiot zamówienia, osobom trzecim, celem ich rozbudowy oraz ma prawo do relokacji urządzeń, przez podmioty trzecie, posiadające stosowne uprawnienia producenta bez utraty gwarancji.
16. Zamawiający zastrzega prawo do planowanego wyłączania oraz włączania dostarczonej przez Wykonawcę infrastruktury bez utraty gwarancji.
17. Zamawiający zastrzega prawo do nieplanowanego wyłączenia i włączenia dostarczonej przez Wykonawcę infrastruktury bez utraty gwarancji. Nieplanowane wyłączenie i włączenie dostarczonej przez Wykonawcę infrastruktury może nastąpić w wyniku zdarzeń losowych będących zagrożeniem dla przetwarzanych danych, np. zagrożenie zalaniem, pożar, awaria infrastruktury budynku, itp.
18. Podczas realizacji zgłoszenia Wykonawca, jeżeli będzie to według jego uznania konieczne, po konsultacjach z Zamawiającym dokona instalacji dostępnych i zalecanych w danym czasie ulepszeń technicznych w celu zapewnienia poprawnego działania urządzeń oraz podwyższenia jego wydajności (zgodnie z zainstalowanymi częściami zamiennymi). Wykonawca zainstaluje uaktualnienia oprogramowania wewnętrznego danego urządzenia wspierającego sprawne przeprowadzanie procesu usuwania usterek. Dotyczy to tych uaktualnień, które nie są dostępne do samodzielnej instalacji przez użytkownika.
19. Wykonawca w okresie trwania gwarancji dokona na prośbę Zamawiającego aktualizację mikrokodów dostarczanych urządzeń i oprogramowania oraz urządzeń Zamawiającego objętych serwisem pogwarancyjnym, nie rzadziej niż raz na 180 dni kalendarzowych za pomocą aktualnych narzędzi aktualizujących do wersji uzgodnionej z Zamawiającym.
20. Wykonawca w okresie gwarancji będzie wykonywał przeglądy okresowe zgodnie z zaleceniami producentów sprzętu.

# **Szkolenia**

* + - 1. Wykonawca przeprowadzi w siedzibie Zamawiającego warsztaty dla 4 osób z zakresu administracji i utrzymania dostarczanego sprzętu i oprogramowania w ilości 24 godzin.
			2. Wykonawca dostarczy po 4 vouchery na wskazane poniżej autoryzowane szkolenia:
1. VMware vSphere: Install, Configure, Manage [V6.7]
2. VMware vSphere: Fast Track [v6.7]
3. VMware vSphere: Optimize and Scale plus Troubleshooting Fast Track [V6.7]