ZAMAWIAJĄCY: URZĄD PATENTOWY RZECZYPOSPOLITEJ POLSKIEJ

00-950 Warszawa, al. Niepodległości 188/192

SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA (SOPZ)

Załącznik nr 1 do

SPECYFIKACJI ISTOTNYCH WARUNKÓW ZAMÓWIENIA

Postępowanie prowadzone w trybie przetargu nieograniczonego na dostawę sprzętu i oprogramowania wraz z wdrożeniem do rozbudowy Platformy Usług Elektronicznych Urzędu Patentowego RP

Warszawa, dnia 30 września 2019 r.

Spis treści

I. Wymagania do architektury rozwiązania w domenie infrastrukturalnej

1. Zamawiający wymaga od Wykonawcy, aby dostarczył technologie wirtualizacyjne zgodne z posiadanym przez Zamawiającego środowiskiem VMware vSphere wraz z funkcjonalnościami służącym do przenoszenia aktywności poszczególnych logicznych komponentów systemów między obiektami fizycznymi, które będą zarządzane za pomocą centralnej konsoli Zamawiającego VMware vCenter Server.
2. Zamawiający wymaga od Wykonawcy, aby dostarczył technologie backupu zgodne z posiadanym przez Zamawiającego środowiskiem Veeam Backup & Replication, zarządzanym za pomocą centralnej konsoli Zamawiającego dla systemu backupu.
3. Zamawiający wymaga od Wykonawcy, aby realizując przedmiot zamówienia dostarczył serwery kasetowe, tak by osiągnąć wysoki współczynnik konsolidacji i optymalizacji wykorzystania zasobów IT.
4. Wykonawca zobowiązany jest do instalacji i integracji dostarczonych komponentów z istniejącą infrastrukturą Zamawiającego w sposób niezakłócający działania systemów i sieci teleinformatycznej Zamawiającego.
5. Wszystkie oferowane urządzenia muszą działać pod kontrolą oprogramowania, które jest publiczną wersją, udostępnianą na rynku przez producenta oferowanych urządzeń. Zamawiający nie dopuszcza stosowania oprogramowania stworzonego na potrzeby niniejszego zamówienia, dla zaoferowanych urządzeń.
6. Zamawiający, w celach poglądowych, w **Załączniku 1A do SOPZ** zamieścił wykaz licencji oprogramowania wykorzystywanego obecnie przez Zamawiającego.
7. W przypadku konieczności zakupienia dodatkowych licencji dla sprzętu i programowania dostarczanego w ramach tego postępowania Wykonawca jest zobowiązany do ich dostarczenia na własny koszt.
8. Dla licencji oprogramowania standardowego, dostarczonych przez Wykonawcę, Wykonawca zobowiązany jest do utrzymywania aktualnego wsparcia producenta (w tym prawa do aktualizacji do nowych wersji) przez cały okres obowiązywania Gwarancji na Sprzęt, w sposób opisany w rozdziale III.

II. Gwarancja i wsparcie technicznego dla dostarczanego sprzętu

1. Dostarczony Sprzęt musi być objęty 5 letnią (60 miesięcy) gwarancją producenta (która może być realizowana także przez podmioty autoryzowane przez producenta), liczoną od dnia podpisania przez obie Strony protokołu odbioru bez zastrzeżeń.
2. Do obowiązków Wykonawcy należy zapewnienie 5 letniego (60 miesięcy) wsparcia technicznego dla dostarczonego sprzętu.

3. Wykonawca dostarczy Zamawiającemu drogą elektroniczną na wskazany adresy e-mail niezbędne dane dostępowe umożliwiające skorzystanie z usług serwisu i wsparcia technicznego dla dostarczonego sprzętu.
4. Zasady świadczenia wsparcia technicznego Sprzętu:
   1) Wykonawca jest zobowiązany w trakcie trwania gwarancji do wykonywania gwarancyjnych usług serwisowych polegających w szczególności na diagnozowaniu i usuwaniu wszystkich Awarii i innych nieprawidłowości Sprzętu, a także w razie konieczności wymiany, udostępnienia, dostarczenia i uruchomienia Sprzętu zastępczego lub nowego, wolnego od wad, jak również do zapewnienia sprawnego działania Oprogramowania umożliwiającego jego wykorzystanie w zakresie funkcji opisanych w Dokumentacji, w tym w szczególności do zapewnienia dostarczania aktualizacji Oprogramowania.
   2) Wykonawca zobowiązuje się do poniesienia wszelkich kosztów napraw gwarancyjnych, w szczególności kosztów odinstalowania, transportu, instalacji i uruchomienia Sprzętu i Oprogramowania.
   3) W ramach gwarancji Wykonawca jest zobowiązany do świadczenia usługi wsparcia technicznego, w ramach którego Wykonawca zapewni:
      a. dostęp do najnowszych wersji oprogramowania, bez konieczności wnoszenia dodatkowych opłat,
      b. dostęp do poprawek i łatek do oprogramowania po ich opublikowaniu przez producenta,
      c. dostęp do aktualizacji plików sygnatur, baz danych opisujących ataki, baz kategorii URL itp.,
      d. możliwość bezpośredniego zgłaszania do producenta problemów serwisowych przez Zamawiającego.
   4) Zgłoszenia Awarii Sprzętu przyjmowane będą przez serwis gwarancyjny 24 godziny na dobę drogą telefoniczną, pocztą elektroniczną lub pisemnie. Protokół zgłoszenia Awarii stanowi **Załącznik Nr 4** do Umowy.
   5) Wykonawca zobowiązany jest w ciągu 8 godzin od momentu przesłania zgłoszenia rozpocząć naprawę Sprzętu.
   6) W przypadku, gdy Awarii nie można usunąć w ciągu 1 Dnia roboczego Wykonawca dostarczy sprawny sprzęt zastępczy o nie gorszych parametrach użytkowych, spełniający te same funkcje co urządzenie będące przedmiotem naprawy, na następny Dzień roboczy po przyjęciu zgłoszenia Awarii.
   7) Przy trzeciej Awarii danego Sprzętu w okresie gwarancyjnym Zamawiającemu przysługuje prawo bezpłatnej wymiany Sprzętu na nowy.

8) Naprawy i wymiany Sprzętu muszą być realizowane w miejscu instalacji Sprzętu w siedzibie Zamawiającego.

9) Zamawiający zapewni upoważnionym przedstawicielom Wykonawcy dostęp do Sprzętu objętego zgłoszeniem w celu dokonania naprawy lub wymiany w obecności upoważnionego przedstawiciela Zamawiającego. Dostęp będzie zapewniony po uprzednim powiadomieniu Zamawiającego.

10) W przypadku dokonania naprawy polegającej na wymianie elementów, Wykonawca zobowiązuje się do zastosowania oryginalnych, nieregenerowanych, nierefabrykowanych, fabrycznie nowych części zamiennych o identycznych lub lepszych parametrach niż elementy wymieniane.

11) Wykonawca gwarantuje sprawność i niezawodność wymienionego Sprzętu lub jego wymienionych części przez okres 5 lat od dnia podpisania protokołu z naprawy.

12) Wykonawca oświadcza, że udzielona gwarancja nie ogranicza w szczególności praw Zamawiającego do:

   a. powierzania Sprzętu wraz z Oprogramowaniem, stanowiących Przedmiot Umowy, osobom trzecim, celem ich instalacji i konserwacji w miejscu eksploatacji,

   b. przenoszenia dostarczanego Sprzętu wraz z Oprogramowaniem do innych lokalizacji,

   c. instalowania i wymiany, w zakupionym Sprzęcie standardowych kart i urządzeń (np. sterowników sieci, dysków), zgodnie z zasadami sztuki informatycznej i przez wykwalifikowany personel.

13) Serwis gwarancyjny będący przedmiotem zamówienia, musi być świadczony w taki sposób, aby nie zostały utracone gwarancje producenta na dostarczone rozwiązane.

III. Gwarancja i wsparcie dla dostarczanego oprogramowania standardowego

1. Dostarczone Oprogramowanie standardowe musi być objęte 5 letnim (60 miesięcy) wsparciem technicznym producenta, liczonych od dnia podpisania przez obie Strony protokołu odbioru bez zastrzeżeń.
2. Usługa wsparcia technicznego producenta oferowanego oprogramowania zapewniająca minimum:

   1) nieograniczoną ilość zgłoszeń serwisowych;

2) dostęp do materiałów producenta takich jak: dokumentacja techniczna (jeśli producent udostępnia dokumentację techniczną), internetowa baza wiedzy (jeśli producent oprogramowania udostępnia bazę wiedzy), forum internetowe producenta oprogramowania (jeśli producent oprogramowania udostępnia takie forum);

3) dostęp do poprawek i uaktualnień oprogramowania objętego usługą wsparcia;

4) dostęp do portalu internetowego producenta oprogramowania umożliwiającego: zarządzanie posiadanymi licencjami, założenie biletu serwisowego/zgłoszenie awarii u producenta, pobieranie poprzednich wersji oprogramowania (jeśli producent oficjalnie wspiera poprzednie wersje), pobieranie nowych wersji oprogramowania (jeśli producent opublikuje nowe wersje w czasie trwającej usługi wsparcia);

5) dostęp do rejestru licencji (dostępnego przez portal internetowy producenta oprogramowania);

6) oferowana usługa wsparcia producenta musi zapewniać ciągłość i poufność komunikacji na poszczególnych etapach procesowania zgłoszenia;

7) wsparcie techniczne producenta musi być świadczone minimum w trybie 5x8: poniedziałek - piątek (5 dni w tygodniu) przez co najmniej 8 godzin dziennie.

IV. Dokumentacja

1. Wykonawca zobowiązany jest do wytworzenia i dostarczenia dokumentacji powykonawczej, która będzie podlegała odbiorom. Dostarczona dokumentacja musi być dostępna w wersji papierowej i elektronicznej w języku polskim. Dopuszcza się język angielski w dokumentacji technicznej elementów, które nie są dziełem Wykonawcy, a dokumentacja producenta w języku polskim nie jest dostępna.
2. Dokumentacja powykonawcza musi zawierać co najmniej:
   1) instrukcje i procedury eksploatacyjne, tj. procedury postępowania podczas bieżącej eksploatacji, administracji i konserwacji systemu (np. backup, odtworzenie, zarządzanie logami, zarządzanie użytkownikami i uprawnieniami, monitorowanie parametrów środowiska) niezbędne do zapewnienia prawidłowego działania dostarczonego sprzętu i poprawnej jego aktualizacji,
   2) opis instalacji i konfigurowania wszystkich dostarczonych komponentów,
   3) opis integracji z innymi systemami,
   4) numery części (part number), numery seryjne, etc. wszystkich urządzeń dostarczonych przez Wykonawcę,

5) hasła administratorskie dające maksymalne uprawnienia do wszystkich urządzeń i oprogramowania (hasła muszą być przekazane w bezpieczny sposób, w uzgodnieniu z Zamawiającym),

6) opis wraz ze schematami umiejscowienia oferowanego rozwiązania w topologii sieci zamawiającego w warstwie fizycznej i logicznej zawierający przynajmniej informacje o użytej adresacji, chronionych aplikacjach webowych, użytych mechanizmach ochrony,

7) opis konfiguracji Web Application Firewall (WAF): konfiguracja (postać papierowa i elektroniczna gotowa do importu na urządzenia),

8) opis konfiguracji serwerów: dokładne parametry sprzętowe, opis konfiguracji systemu, wersje, układ dysków, partycjonowanie, konfiguracja interface'ów sieciowych, spis usług działających na serwerze i ich konfiguracja oraz przydzielone im zasoby, etc.

9) opis konfiguracji obudowy dysków dodatkowych do macierzy: dokładne parametry sprzętowe, opis konfiguracji oprogramowania, wersje, układ dysków, partycjonowanie, konfiguracja interface'ów sieciowych, etc.,

10) opis licencji, numery i kucze aktywacyjne i numery licencji, okres wsparcia producenta,

11) opis konfiguracji (postać papierowa i elektroniczna gotowa do importu na serwery i inne urządzenia),

3. Wykonawca zobowiązany jest do wytworzenia planów awaryjnych, sporządzonych dla zapór sieciowych WAF, uwzględniających szczegółowy opis czynności, poleceń i sekwencji działań, które są niezbędne do wykonania w celu odtworzenia całego systemu po katastrofie. Plany awaryjne muszą być zdekomponowane na poszczególne komponenty systemu, które można będzie wykonywać „w górę" od początku odtwarzania zapór sieciowych WAF lub też od określonego poziomu awarii.

V. Warunki równoważności

1. Jeżeli Zamawiający określił w SIWZ wymagania z użyciem nazw własnych produktów lub marek producentów, w szczególności w obszarze specyfikacji przedmiotu zamówienia, to należy traktować wskazane produkty jako rozwiązania wzorcowe. W każdym takim przypadku Zamawiający oczekuje dostarczenia produktów wzorcowych lub równoważnych, spełniających poniższe warunki równoważności.
2. W przypadku dostarczania sprzętu, oprogramowania, szkoleń lub innych produktów równoważnych względem wyspecyfikowanych przez Zamawiającego w SIWZ, Wykonawca musi na swoją odpowiedzialność i swój koszt udowodnić, że dostarczane

produkty spełniają wszystkie wymagania i warunki określone SIWZ, w szczególności w zakresie:

1) warunków licencji / sublicencji w każdym aspekcie licencjonowania / sublicencjonowania, które nie mogą być gorsze niż dla produktu wymienionego w SIWZ,
2) funkcjonalności równoważnej produktu, która nie może być gorsza od funkcjonalności produktu wymienionego w SIWZ,
3) sprzętu i oprogramowania, które muszą być kompatybilne i w sposób niezakłócony współdziałać ze sprzętem i oprogramowaniem funkcjonującym u Zamawiającego,
4) sprzętu i oprogramowania, które nie mogą zakłócić pracy środowiska systemowo-programowego Zamawiającego,
5) sprzętu i oprogramowania, które muszą w pełni współpracować z systemami Zamawiającego, opartymi o dotychczas użytkowane oprogramowanie,
6) sprzętu i oprogramowania, które muszą zapewniać pełną, równoległą współpracę w czasie rzeczywistym i pełną funkcjonalną zamienność produktu równoważnego z produktem określonym w SIWZ,
7) warunków i zakresu usług gwarancji, serwisu pogwarancyjnego, asysty technicznej i konserwacji produktu równoważnego, muszą być nie gorsze niż dla produktu wymienionego w SIWZ.

3. W przypadku zaoferowania przez Wykonawcę produktu równoważnego Wykonawca dokona wspólnie z Zamawiającym instalacji i testowania produktu równoważnego w środowisku sprzętowo-programowym Zamawiającego.
4. W przypadku zaoferowania przez Wykonawcę oprogramowania równoważnego Wykonawca dokona transferu wiedzy w zakresie utrzymania i rozwoju rozwiązania opartego o zaproponowane produkty.
5. W przypadku, gdy zaoferowany przez Wykonawcę produkt równoważny nie będzie właściwie współdziałać ze sprzętem i oprogramowaniem funkcjonującym u Zamawiającego lub spowoduje zakłócenia w funkcjonowaniu pracy środowiska sprzętowo-programowego u Zamawiającego, Wykonawca pokryje wszystkie koszty związane z przywróceniem i sprawnym działaniem infrastruktury sprzętowo-programowej Zamawiającego oraz na własny koszt dokona niezbędnych modyfikacji przywracających właściwe działanie środowiska sprzętowo-programowego Zamawiającego również po usunięciu produktu równoważnego.
6. Wraz z produktem równoważnym Wykonawca jest zobowiązany do dostarczenia niżej wymienionego oświadczenia i następujących dokumentów:

1) oświadczenia dotyczącego zastosowania produktu równoważnego,
2) pełnego postanowienia licencji / sublicencji produktu równoważnego,
3) pełnego wykazu funkcjonalności produktu równoważnego,
4) pełnych warunków i zasad świadczenia usług gwarancji, serwisu pogwarancyjnego, asysty technicznej i konserwacji dla produktu równoważnego,
5) wykazu miejsc użycia produktu równoważnego.

7. Oprogramowanie równoważne dostarczane przez Wykonawcę nie może powodować utraty kompatybilności oraz wsparcia producentów innego używanego i współpracującego z nim oprogramowania.
8. Oprogramowanie równoważne zastosowane przez Wykonawcę nie może w momencie składania przez niego oferty mieć statusu zakończenia wsparcia technicznego producenta. Niedopuszczalne jest zastosowanie oprogramowania równoważnego, dla którego producent ogłosił zakończenie jego rozwoju w terminie 3 lat licząc od momentu złożenia oferty. Niedopuszczalne jest użycie oprogramowania równoważnego, dla którego producent oprogramowania współpracującego ogłosił zaprzestanie wsparcia w jego nowszych wersjach.

VI. Wskaźniki produktów

Lp.	Minimalna moc obliczeniowa dostarczanych komponentów serwerowych	Minimalna przestrzeń dyskowa dostarczanych komponentów
1.	**1,4 Tflops**	**16 TB**

VII. Infrastruktura sprzętowa

W ramach realizacji projektu Wykonawca zobowiązany jest dostarczyć następujące elementy infrastruktury sprzętowej wraz z oprogramowaniem narzędziowym:

Lp.	Produkt	Ilość [szt.]
1.	Serwery kasetowe	2
2.	Obudowa dysków dodatkowych do macierzy wraz z dyskami i niezbędnymi licencjami	2

3.	Zapora sieciowa Web Application Firewall (WAF)	2

VIII. Oprogramowanie standardowe

W ramach realizacji projektu Wykonawca zobowiązany jest dostarczyć następujące licencje i oprogramowanie standardowe:

Lp.	Produkt
1.	Oprogramowanie do tworzenia kopii zapasowych
2.	Oprogramowanie platformy wirtualizacji
3.	Serwerowe systemy operacyjne 1
4.	Serwerowe systemy operacyjne 2

IX. Parametry techniczne dostarczanego sprzętu

1. Serwery kasetowe

1) Przedmiotem zamówienia jest dostawa i wdrożenie serwerów kasetowych – **2 sztuki**.
2) Specyfikacja techniczna serwerów kasetowych:

Lp.	Element/cecha	Wymagania minimalne
1.	Obudowa	Serwer musi być zgodny z posiadaną przez Zamawiającego obudową kasetową Dell PowerEdge M1000e. Obecnie Zamawiający posiada 6 serwerów kasetowych PowerEdge M640, 2 x Intel(R) Xeon(R) Gold 6130 CPU @ 2.10GHz zainstalowanych w obudowie kasetowej. Serwer musi spełniać wymóg migracji bez przerywania pracy działających systemów i aplikacji.

2.	Płyta główna	Płyta główna z możliwością zainstalowania minimum dwóch procesorów.
3.	Procesor	Minimum dwa procesory szesnastordzeniowe, trzydzieści dwa wątki każdy, posiadający min. 22MB pamięci podręcznej Cache z zastosowaną technologią Hyper-Threading, osiągające w testach *CPU2017 Integer Rates,* w polu *„SPECrate2017_int_base”* wynik nie gorszy niż określony przez atrybuty „158” (dla konfiguracji serwera z dwoma procesorami szesnastordzeniowymi). **Wynik testu musi być potwierdzony przez organizację SPEC (www.spec.org) na dzień składania oferty.** Całkowita moc obliczeniowa dostarczonych serwerów kasetowych musi wynosić **minimum 1,4 Tflops** (szacowana realna moc obliczeniowa, przy założeniu wydajności na poziomie 65%, liczona przy pomocy narzędzia Cluster Performance Calculator https://cads.iiap.res.in/tools/flopsCalc).
4.	Pamięć RAM	Zainstalowane 512GB pamięci RAM DDR4 Memory PC4 RDIMM ECC. Na płycie głównej powinno się znajdować minimum 16 slotów na pamięć RAM.
5.	Interfejsy Ethernet	Karta minimum 4-port 10Gb, zgodna z oferowanym serwerem.
6.	Interfejsy FC	Karta minimum 2-port 16Gb FC, zgodna z oferowanym serwerem.
7.	Kieszenie na dyski	Przedni dla min. 2 x 2.5” SAS/SATA/SSD, max 12.8 TB.
8.	Dyski twarde	Dwa dyski twarde o pojemności co najmniej 300GB 15K RPM SAS 12Gbps 512n 2.5in Hot-plug Hard Drive.
9.	Kontroler RAID	Poziomy RAID 0, 1, 5. Obsługiwany Protokół NVMe (Non-Volatile Memory). Wybieralny dysk logiczny jako dysk rozruchowy. Obsługa poleceń TRIM/UNMAP dla dysków SSD, SAS/SATA. Obsługa hot-plug wymiany na gorąco dysków. Obsługa dysków logicznych większych niż 2 TB. Globalna obsługa hot-spare. Obsługa odzyskiwania po błędach.

10.	Wsparcie dla Systemów Operacyjnych/ Systemów wirtualizacji	Wymagane jest wsparcie dla następujących systemów: - Windows Server - Red Hat Linux - SuSE Linux - VMWare vSphere
11.	Warunki gwarancji	Zgodnie z zapisami zawartymi w Rozdziale II i III.
12.	Usługa montażu i uruchomienia	Podłączenie oraz konfiguracja serwerów kasetowych w istniejącym środowisku Zamawiającego. Instalacja i konfiguracja systemu wirtualizacji zgodnie z użytkowanym środowiskiem Zamawiającego. Konfiguracja dostępu zainstalowanego systemu wirtualizacji do udostępnianych zasobów na macierzach dyskowych zgodnie z użytkowanym środowiskiem Zamawiającego, w tym niezbędna konfiguracja połączeń, przełączników FC, macierzy. Konfiguracja i podłączenie serwerów z zainstalowanym systemem wirtualizacji do centralnej konsoli zarządzającej serwerami w środowisku wirtualnym Zamawiającego. Utworzenie i konfiguracja klastra wysokiej dostępności.
13.	Zarządzanie serwerami	Dostarczenie licencji na oprogramowanie do zarządzania konfiguracją serwerów dla każdego z dostarczanych serwerów wraz z 5 letnim wsparciem.

2. Obudowa dysków dodatkowych do macierzy wraz z dyskami i niezbędnymi licencjami

1) Zamawiający wymaga od Wykonawcy dostarczenia nowych obudów dysków dodatkowych do macierzy wraz z dyskami, niezbędnym okablowaniem, gwarancją producenta oraz licencjonowanym oprogramowaniem, w liczbie **2 sztuk**. Przestrzeń użytkowa w każdej obudowie musi wynosić **minimum 8 TB w konfiguracji RAID 5 (łącznie 16 TB)**.

2) Specyfikacja techniczna pamięci masowej:

Lp.	Element/cecha	Wymagania minimalne
1.	Obudowa rozszerzająca / półka dyskowa	Obudowa dysków dodatkowych (moduł rozszerzający) ze wszystkimi komponentami umożliwiająca montaż w standardowej szafie typu Rack 19”. Wysokość każdej obudowy nie może przekraczać rozmiaru 2U. Obudowa i interfejsy muszą być kompatybilne z posiadaną przez Zamawiającego macierzą Dell EMC SC7020 wraz z modułem rozszerzającym SC420 Expansion Enclosure. Obudowa musi mieć możliwość wymiany dysków na gorąco (ang. Hot-swap) w trakcie pracy urządzenia, bez potrzeby wyłączania obudowy czy macierzy. Obudowa powinna posiadać na przednim panelu diody informujące o stanie zasilania oraz o stanie systemu.
2.	Połączenie między kontrolerem macierzy i obudową	Każda z obudów musi posiadać dwa redundantne 4 portowe kontrolery SAS 12 Gb/s, wymienialne bez przerywania pracy z niezbędnym okablowaniem do podłączenia w istniejącym systemie Dell EMC SC7020 jako rozszerzenie o kolejne dyski.
3.	Dyski	Każda z obudów musi być wyposażona w dedykowane przez producenta lub znajdujące się na liście kompatybilności serwerowe dyski 2,5" SSD. Obudowy dysków dodatkowych macierzy muszą posiadać możliwość instalacji minimum 24 dysków 2,5-calowych. Każda z obudów dysków dodatkowych musi obsługiwać dyski 2,5". Każda z obudów dysków dodatkowych musi umożliwiać stosowanie w niej dysków SAS, SSD, HDD 15k, HDD 10k i HDD 7,2k rpm wyposażonych w interfejsy SAS minimum 6 Gbps (SAS, NL-SAS).
4.	Pojemność	Każda z obudów dysków dodatkowych musi zawierać dyski SSD udostępniając użytkownikowi łączną powierzchnię użytkową minimum 8TB w konfiguracji RAID 5 (łącznie 16 TB). Zamawiający wymaga dostarczenia macierzy dyskowych składających się

		z obszaru zapewniającego wysoką wydajność zawierającą dyski SSD dla każdej z obu macierzy.
5.	Interfejsy	Każda z oferowanych obudów musi posiadać minimum 2 kontrolery 4 portowe typu SAS 12 Gb/s które umożliwią redundantne połączenie z obecnie działającą macierzą, dadzą możliwość rozbudowy o kolejne półki dyskowe i mogą być wymieniane na gorąco w trakcie pracy macierzy dyskowej.
6.	RAID	Oferowane urządzenia muszą obsługiwać poziomy RAID minimum: 1, 5, 6 i 10.
7.	Niezawodność półki dyskowej	Każda z obudów powinna być niezawodna - wyposażona w redundantne zasilanie, chłodzenie, kontrolery, dwie ścieżki dostępu do każdego dysku.
8.	Interfejs użytkownika	Każda z obudów musi być kompatybilna oraz obsługiwana przez posiadane przez Zamawiającego oprogramowanie do zarządzania macierzami wyposażone w graficzny interfejs dostępny przez przeglądarkę oraz interfejs tekstowy przez szyfrowane połączenie. Musi istnieć możliwość bezpośredniego monitoringu stanu, w jakim w danym momencie znajduje się obudowa. Dane o parametrach wydajnościowych muszą być dostępne w postaci wykresów w interfejsie GUI. Każda z obudów musi posiadać funkcjonalność zarządzania całością dostępnych zasobów dyskowych, z jednej konsoli administracyjnej macierzy dyskowej, będącej w posiadaniu Zamawiającego.
9.	Oprogramowanie	Wymagane jest, aby każda z dostarczonych obudów rozszerzających była kompatybilna i w pełni zarządzana przez użytkowane przez Zamawiającego oprogramowanie Dell Storage Manager.
10.	Wentylatory i zasilacze	Wentylatory i zasilacze każdej obudowy w pełni nadmiarowe, z możliwością wymiany podczas pracy.
11.	Aktualizacje mikro kodu	Każda z obudów musi umożliwiać wykonywanie aktualizacji mikro kodu w trybie online bez przerywania dostępu do zasobów dyskowych macierzy i przerywania pracy aplikacji.
12.	Konfiguracja przestrzeni	Każda obudowa podłączona do macierzy musi zapewniać funkcjonalność udostępniania przestrzeni bez konieczności fizycznego alokowania wolnego miejsca na dyskach (thin provisioning). Jeżeli funkcjonalność

	dyskowej	wymaga licencji, Wykonawca musi taką licencję dostarczyć dla obu obudów w dostarczonej konfiguracji. Każda obudowa musi współpracować funkcjonalnością tieringu macierzy polegającą na automatycznej migracji bloków danych dysków logicznych pomiędzy różnymi typami dysków fizycznych (SSD, SAS/FC, NLSAS/SATA), w zależności od stopnia wykorzystania danego obszaru przez aplikację. Migracje muszą być wykonywane automatycznie bez udziału administratora. Migracja danych musi odbywać się bez przerywania dostępu do danych od strony hostów i aplikacji. Jeżeli jest niezbędna licencja na obsługę tej funkcjonalności na całą dostarczoną pojemność obu półek macierzy należy ją dostarczyć wraz z urządzeniem. Każda z półek musi współpracować z posiadaną macierzą tak by umożliwiać zwrot zwolnionej przestrzeni dyskowej do puli (space reclamation). Każda z półek do macierzy musi umożliwiać automatyczne rozkładanie bloków dysków logicznych pomiędzy wszystkie dostępne dyski fizyczne funkcjonujące w ramach tej samej puli/grupy dyskowej w przypadku rozszerzania dysku logicznego i dokładania dysków fizycznych. Każda z półek musi umożliwić macierzy użycie funkcjonalności zwiększania rozmiaru wolumenów.
13.	Warunki gwarancji	Zgodnie z zapisami zawartymi w Rozdziale II i III.

3. Zapory sieciowe Web Application Firewall (WAF)

1) Zamawiający wymaga od Wykonawcy dostarczenia Zapór sieciowych Web Application Firewall (WAF) - 2 sztuki wraz z licencjami na oprogramowanie zainstalowane na zaporach sieciowych WAF z 5-letnim wsparciem technicznym producenta, wdrożenie zaoferowanego rozwiązania i przeszkolenia administratorów Zamawiającego.
2) Specyfikacja techniczna Zapory sieciowej Web Application Firewall (WAF) – wymagania minimalne

Lp.	Wymagania minimalne
1.	Oferowane rozwiązanie musi być zrealizowane w postaci dedykowanej platformy sprzętowej (appliance) i oprogramowania, dla którego wsparcie świadczone jest przez jednego producenta.
2.	Oferowane rozwiązanie ma spełniać następujące parametry wydajnościowe: - Przepustowość filtrowania ruchu http/https minimum 200Mbps - Zapewniać ochronę przed atakami z list OWASP Top 10 dla min. 10 aplikacji
3.	Oferowane rozwiązanie musi być dostarczone w postaci dwóch urządzeń pracujących w klastrze niezawodnościowym. Musi istnieć możliwość zbudowania klastra w układzie active-passive / standby oraz active-active. Klaster musi być zarządzany jak jedno urządzenie i tak też widoczny z punktu widzenia podłączonych do niego sieci.
4.	Oferowane urządzenie musi spełniać następujące parametry: - Możliwość instalacji w szafie montażowej 19” - Minimum 4 interfejsy 1GE - Minimum 2 gniazda SFP - Urządzenie musi umożliwiać rozbudowę o minimum 2 interfejsy 10GE
5.	Oferowane rozwiązanie musi mieć możliwość implementacji systemu inline w trybach Reverse Proxy lub Transparentnym.
6.	Oferowane rozwiązanie musi mieć możliwość samodzielnego "uczenia się" publikowanej aplikacji - tryb auto-uczenia.
7.	Oferowane rozwiązanie musi realizować ochronę dla aplikacji webowych co najmniej przed zagrożeniami: - SQL and OS Command Injection - Cross Site Scripting (XSS) - Cross Site Request Forgery - Outbound Data Leakage - HTTP Request Smuggling - Buffer Overflow - Encoding Attacks

	- Cookie Tampering / Poisoning - Session Hijacking - Broken Access Control - Forceful Browsing /Directory Traversal - Oraz innymi podatnościami specyfikowanymi przez listę OWASP Top 10
8.	Oferowane rozwiązanie musi realizować ochronę dla aplikacji webowych przed atakami typu DoS/DDoS. WAF musi posiadać mechanizmy ochrony przed atakami DoS ukierunkowanymi na warstwę aplikacyjną (zalewanie aplikacji web dużą ilością zapytań http).
9.	Oferowane rozwiązanie powinno umożliwiać proaktywne wykrywanie i blokowanie botów, zanim wywołają atak DDoS, web scraping lub brute force.
10.	Oferowane rozwiązanie musi działać w oparciu o pozytywny model bezpieczeństwa (tylko to, co znane i prawidłowe jest dozwolone), model ten tworzony jest na bazie automatycznie budowanego przez WAF profilu aplikacji Web. Pozytywny model bezpieczeństwa powinien kontrolować co najmniej: - wystąpienie URL-i, długość URL-i, zabezpieczenie przed clickjackiem dla danego URLa. - typ servleta występujący pod danym url-em – format komunikacji (http form, JSON, XML, GWT), - przejścia pomiędzy URL-ami (servletami), - dopuszczalne metody http, - dopuszczalne cookie, - parametry dynamiczne, - typ/format parametrów (alfanumeryczny, integer, dynamiczny, statyczny, JSON, XML, e-mail, telefon, plik uploadowany), - dopuszczalne parametry w danym servlecie, - długość zapytań, - nazwy hosta, - wystąpień i długość parametrów (per każdy parametr), - wystąpień i długości nagłówków, - wystąpień i długości cookies, - oczekiwanych typów znaków per każdy parametr, - typów rozszerzeń plików; w tym długości URLa, requestu, query stringu, post data dla danego typu pliku, - URL-i podatnych na CSRF.
11.	Oferowane rozwiązanie musi posiadać funkcje identyfikacji incydentów poprzez

	sygnatury (negatywny model zabezpieczeń).
12.	Oferowane rozwiązanie musi posiadać funkcjonalność automatycznego wykrywania stron logowania użytkowników oraz automatycznie włączać dla tych stron ochronę przed atakami brute force.
13.	Oferowane rozwiązanie musi umożliwiać zablokowanie lub przepuszczanie połączeń na podstawie nazwy kraju, w którym zarejestrowane są adresy IP źródła lub celu połączenia. Weryfikacja przynależności adresu IP do kraju musi się odbywać na bieżąco z Web Application Firewall (WAF) przez Internet. Wykorzystanie nazw krajów do blokowania lub przepuszczania połączeń musi być możliwe w poszczególnych regułach Web Application Firewall (WAF).
14.	Oferowane rozwiązanie musi posiadać serwisy reputacyjne dzięki którym rozwiązanie będzie rozpoznawać i blokować komunikacje co najmniej dla: - Anonimowych proxy, - Sieci Botnet, - Aktywnych źródeł usług oferujących lub dystrybuujących malware, rootkity, robaki oraz wirusy, - Źródeł ataków DDoS/DoS, - Adresów IP zainfekowanych przez malware, - Adresów IP świadczących usługi hostingowe dla phishingu lub fraudów, - Źródeł ataków cross-site scripting, iFrame injection, SQL injection, cross domain injection czy domain password brute force, - Źródłowych adresów IP skanerów służących do rekonesansu poprzez skanowanie hostów oraz domen.
15.	Oferowane rozwiązanie musi posiadać moduł analizy ruchu http. Moduł powinien zbierać co najmniej następujące metryki: - Czas odpowiedzi per serwer, - Czas odpowiedzi per URI, - Ilość sesji użytkownika, - Przepustowość, - Adres źródła, - Kraj, - User Agent (wykorzystywana przez klienta aplikacja), - Metoda dostępu.

16.	Oferowane rozwiązanie musi posiadać funkcję definiowania maksymalnej ilości obsługiwanych przez dany serwer połączeń, w przypadku przekroczenia zdefiniowanej wartości musi istnieć możliwość wysłania klientowi strony błędu lub przekierowania klienta na inny serwer.
17.	Dostęp administracyjny i konfiguracyjny poprzez CLI za pośrednictwem protokołu SSH oraz GUI przy wykorzystaniu protokołu https.
18.	Oferowane rozwiązanie musi posiadać możliwość pełnego odtworzenia konfiguracji oprogramowania i systemu operacyjnego z nośnika USB.
19.	W czasie i po wykonaniu upgrade'u wersji oprogramowania lub po instalacji łatki (patcha), oferowane rozwiązanie musi umożliwiać cofnięcie jego wersji oprogramowania do poprzedniej bez konieczności reinstalacji oprogramowania z nośników zewnętrznych o ile producent umożliwia taką operację dla konkretnej poprawki.
20.	Oferowane rozwiązanie musi obsługiwać protokół SNMP w wersjach 1, 2c i 3 w celach administracyjnych.
21.	Oferowane rozwiązanie musi umożliwiać zapisywanie logów na zewnętrzy serwer Syslog.
22.	Oferowane rozwiązanie powinien pozwalać na przeglądanie, wizualizacji logów generowanych przez WAF. WAF musi obrazować rodzaj wykrywanych ataków. WAF ma przedstawiać informację o statusie portów, ilość przesyłanych danych na portach, ilości przesyłanych danych przez poszczególne rodzaje aplikacji, informację do/z jakich krajów nawiązywane jest połączenie.

3) Licencja na oprogramowanie zainstalowane na zaporach sieciowych Web Application Firewall (WAF) wraz z wsparciem technicznym – wymagania minimalne

Lp.	Wymagania minimalne
1.	Dostęp do najnowszych wersji oprogramowania dla Web Application Firewall (WAF) w okresie 60 miesięcy.

2.	Wsparcie techniczne ze strony autoryzowanego serwisu producenta Web Application Firewall (WAF) ważne na okres 60 miesięcy.
3.	Gwarancja na Web Application Firewall (WAF) ważna na okres 60 miesięcy.
4.	Dostęp do aktualizacji plików sygnatur, silnika wykrywania zagrożeń, itp. dla Web Application Firewall (WAF) w okresie 60 miesięcy.
5.	Pozostałe warunki gwarancji zgodnie z zapisami zawartymi w Rozdziale II i III.

4) Wdrożenie oferowanego rozwiązania – wymagania minimalne

Lp.	Wymagania minimalne
1.	Instalacja, konfiguracja oraz uruchomienie oferowanego rozwiązania musi nastąpić zgodnie z projektem technicznym wdrożenia.
2.	Wykonawca zobowiązany jest do integracji wdrażanego rozwiązania z systemem do zarządzania informacją i zdarzeniami bezpieczeństwa (SIEM) NetIQ Sentinel, będącego w posiadaniu Zamawiającego.
3.	Wykonawca zobowiązany jest do skonfigurowania mechanizmów bezpieczeństwa wdrażanego rozwiązania dla min. 10 aplikacji webowych wskazanych przez Zamawiającego.

5) Szkolenia administratorów – wymagania minimalne

a. Wykonawca zobowiązany będzie do zapewnienia pracownikom Zamawiającego autoryzowanego szkolenia produktowego (certyfikowanego przez producenta rozwiązania) niezbędnego do obsługi i utrzymania dostarczanego sprzętu, który Wykonawca wyspecyfikuje w swojej Ofercie. W przypadku gdy producent sprzętu nie oferuje autoryzowanych szkoleń w języku polskim Wykonawca zobowiązany będzie do ich przeprowadzenia we własnym zakresie.

b. Szkolenie będzie obejmowało co najmniej zagadnienia z zakresu administracji, konfiguracji oraz zarządzania zaoferowanego sprzętu i oprogramowania zgodnie z zakresem wskazanym w pkt k.
c. W szkoleniu weźmie udział 2 administratorów w grupie szkoleniowej nie większej niż 15 osób.
d. Czas szkolenia nie może być krótszy niż liczba dni wskazana w pkt l. Każdy dzień szkolenia musi trwać 8 godzin zegarowych.
e. Wykonawca w ramach wynagrodzenia zapewni wykładowcę posiadającego odpowiednie kwalifikacje do przeprowadzania autoryzowanych szkoleń.
f. Wykonawca zobowiązuje się do zapewnienia miejsca szkolenia wraz ze stanowiskiem komputerowym dla każdego uczestnika szkolenia oraz wszelkie niezbędne oprogramowanie.
g. Każdy z uczestników szkolenia otrzyma komplet materiałów w języku polskim w formie elektronicznej lub papierowej. Zamawiający dopuszcza przekazanie materiałów szkoleniowych w języku angielskim jedynie w przypadku, gdy producent nie udostępnia materiałów w języku polskim.
h. Wykonawca w trakcie szkolenia zapewni salę szkoleniową na terenie Warszawy oraz wyżywienie (jeden gorący posiłek oraz kawa, herbata i zimne napoje każdego dnia podczas trwania szkolenia).
i. Każdy z uczestników otrzyma imienny certyfikat producenta rozwiązania, którego dotyczyło szkolenie.
j. Wszelkie koszty związane ze wszystkimi aspektami szkoleń ponosi Wykonawca.
k. Zakres szkolenia będzie obejmował co najmniej:
    - Sposoby działania systemów WAF i typowych filtrów chroniących przed atakami,
    - Podłączanie urządzenia i tryby pracy,

- Sposoby tworzenia i wdrażania reguł bezpieczeństwa,
- Ochrona przed atakami,
- Raportowanie i rejestrowanie,
- Tryby uczenia,
- Śledzenie sesji,
- Ochrona przed atakami DoS oraz ochrona przed Botami,
- Zarządzanie urządzeniem.

l. Szkolenie będzie trwało minimum 3 dni.

X. Parametry techniczne dostarczanego oprogramowania

1. Oprogramowanie do tworzenia kopii zapasowych

Lp.	Wymagania minimalne
1.	Oprogramowanie do tworzenia kopii zapasowych/archiwizacji musi współpracować z infrastrukturą wirtualizacji opartą o użytkowane przez Zamawiającego oprogramowanie VMware vSphere w wersji co najmniej 6.7 oraz systemem do tworzenia kopii zapasowych Veeam Backup & Replication w wersji 9.5.
2.	Oprogramowanie do tworzenia kopii zapasowych/archiwizacji musi współpracować z infrastrukturą wirtualizacji opartą o oprogramowanie VMware oraz Hyper-V.
3.	Rozwiązanie musi współpracować z hostami ESXi zarządzanymi przez VMware vCenter, zgodnie z posiadanymi przez Zamawiającego licencjami.
4.	Rozwiązanie musi współpracować z hostami Hyper-V zarządzanymi przez System Center Virtual Machine Manager, zgrupowanymi w klastry jak i niezarządzanymi (standalone).
5.	Rozwiązanie musi wspierać backup wszystkich systemów operacyjnych w wirtualnych maszynach, które są wspierane przez VMware (Windows 32/64 bit, Linux 32/64 bit), zgodnie z posiadanymi przez Zamawiającego licencjami.
6.	Rozwiązanie musi mieć możliwość instalacji na systemach operacyjnych, zgodnie

	z posiadanymi przez Zamawiającego, w wersjach 64 bitowych: - Microsoft Windows Server 2019 - Microsoft Windows Server 2016 - Microsoft Windows Server 2012 R2 - Microsoft Windows Server 2012 - Microsoft Windows Server 2008 R2 SP1
7.	Rozwiązanie nie może instalować żadnych swoich komponentów (agent) w backup'owanych maszynach wirtualnych. Zamawiający jednocześnie dopuszcza instalację agenta w przypadku backupu maszyn fizycznych.
8.	Rozwiązanie musi posiadać możliwość odzyskiwania całych obrazów maszyn wirtualnych z obrazów, pojedynczych plików z systemu plików znajdujących się wewnątrz wirtualnej maszyny. Rozwiązanie, musi umożliwiać odzyskiwanie danych z następujących systemów plików: - Linux - Ext2, ext3, ext4, ReiserFS, JFS, XFS - Windows - ReFS, NTFS, FAT, FAT32
9.	Rozwiązanie musi posiadać wbudowane mechanizmy deduplikacji i kompresji archiwum w celu redukcji zajmowanej przez archiwa przestrzeni dyskowej.
10.	Rozwiązanie musi posiadać możliwość podłączenia do centralnej konsoli użytkowanej przez Zamawiającego, do zarządzania większą ilością serwerów kopii zapasowych/archiwizujących oraz jednoczesnego zarządzania backupami środowisk VMware/Hyper-V.
11.	Rozwiązanie musi posiadać możliwość rozbudowy procesu wykonywania kopii zapasowych/archiwizacji o dowolne skrypty tworzone przez administratora i dołączane do zadań archiwizacyjnych.
12.	Dostarczona licencja musi umożliwić obsługę nielimitowanej ilości maszyn wirtualnych i nielimitowanej ilości danych podlegających wykonywaniu kopii zapasowej/archiwizacji
13.	Rozwiązanie musi mieć możliwość bez agentowego tworzenia kopii zapasowych, odzyskiwania i replikacji.

14.	Oprogramowanie musi mieć możliwość tworzenia kopii zapasowych i odzyskiwanie z migawek.
15.	Dostęp do konsoli zarządzającej musi mieć możliwość połączenia realizowany za pomocą przeglądarki WWW.
16.	Rozwiązanie musi wspierać backup maszyn fizycznych.
17.	Rozwiązanie musi posiadać możliwość podłączenia do mechanizmu bibliotek taśmowych LTO6, LTO7, nagrywania danych oraz kopii danych bezpośrednio na taśmy backupowe.
18.	Licencja na oprogramowanie musi być przypisana do każdego procesora fizycznego znajdującego się w dostarczanych serwerach kasetowych.
19.	Licencja musi zostać dostarczona w modelu wieczystym.
20.	Usługa wsparcia technicznego producenta ma być świadczona zgodnie z zapisami zawartymi w Rozdziale III.
21.	Rozwiązanie musi posiadać wbudowaną możliwość automatycznej i manualnej weryfikacji, przywracalności maszyn wirtualnych z wykonanych kopii zapasowych.
22.	Rozwiązanie musi posiadać możliwość utworzenia wyizolowanego środowiska sieciowego na potrzeby testowe.

2. Oprogramowanie platformy wirtualizacji

Lp.	Wymagania minimalne
1.	Licencja na oprogramowanie musi być przypisana do każdego procesora fizycznego znajdującego się w dostarczanych serwerach kasetowych.
2.	Oprogramowanie do tworzenia kopii zapasowych/archiwizacji musi współpracować z infrastrukturą wirtualizacji opartą o użytkowane przez Zamawiającego oprogramowanie VMware vSphere w wersji co najmniej 6.7 oraz systemem do tworzenia kopii zapasowych Veeam Backup & Replication w wersji 9.5.

3.	Dostarczone licencje muszą umożliwiać uruchomienie oprogramowania do wirtualizacji na każdym fizycznym serwerze kasetowym dostarczanym w ramach zamówienia.
4.	Oferowane oprogramowanie musi umożliwiać zarządzanie za pomocą centralnej konsoli zarządzającej (VMware vCenter – licencja posiadana przez Zamawiającego).
5.	Oferowane oprogramowanie musi pozwalać na tworzenie wirtualnych przełączników (ang. virtual switch) LAN, obsługę sieci VLAN. Zarządzanie przełącznikami wirtualnymi powinno odbywać się z centralnego punktu, a konfiguracja powinna być automatycznie dystrybuowana na serwery wirtualne.
6.	Jest rozwiązaniem systemowym tzn. jest instalowane bezpośrednio na sprzęcie fizycznym (serwerze kasetowym).
7.	Posiada możliwość alokacji dla maszyn wirtualnych większej ilości pamięci RAM niż jest fizycznie zainstalowana w serwerze fizycznym w celu osiągnięcia maksymalnego możliwego stopnia konsolidacji oraz zapewnienia wysokiej dostępności w momencie utraty części zasobów maszyn fizycznych.
8.	Umożliwia pracę maszyn wirtualnych w konfiguracji jedno- jak i wieloprocesorowej.
9.	Musi posiadać wsparcie producenta dla maszyn wirtualnych pracujących pod kontrolą systemów operacyjnych z rodziny Windows w wersjach 32 i 64 bitowych, oraz Linux w wersjach 32 i 64 bitowych.
10.	Posiada centralną konsolę graficzną do zarządzania maszynami wirtualnymi oraz centralne zarządzanie infrastrukturą wirtualną, które w trybie ciągłym monitoruje wszystkie komponenty infrastruktury i umożliwia wykonywanie automatycznych bądź manualnych zadań w celu jej optymalizacji na jednej z maszyn wirtualnych.
11.	Posiada wielopoziomowy schemat uprawnień do zarządzania platformą wirtualną oraz dostępu do wirtualnych serwerów.
12.	Zapewnia możliwość monitorowania wykorzystania zasobów fizycznych infrastruktury wirtualnej.
13.	Posiada możliwość przenoszenia maszyn wirtualnych w czasie ich pracy pomiędzy serwerami fizycznymi oraz danych maszyn wirtualnych pomiędzy wolumenami dyskowymi bez konieczności wyłączania maszyn wirtualnych (wykorzystanie

	mechanizmów HA; DRS).
14.	Zapewnia ciągłą pracę usług - powinna 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.
15.	Umożliwia łatwe i szybkie ponowne uruchomienie systemów/usług w przypadku awarii poszczególnych elementów infrastruktury.
16.	Zapewnia bezpieczeństwo danych pomimo poważnego uszkodzenia lub utraty sprzętu lub oprogramowania.
17.	Zapewnia mechanizm bezpiecznego uaktualniania warstwy do wirtualizacji, dla utrzymywanych (ang. hosting) systemów operacyjnych (np. instalowania poprawek) i aplikacji tak, aby zminimalizować ryzyko awarii systemu na skutek wprowadzenia zamiany.
18.	Zapewnia mechanizm wykonywania i przywracania „migawek" systemów operacyjnych wraz z ich pełną konfiguracją i danymi bez przerwy w działaniu systemów.
19.	Zapewnia możliwość tworzenia kopii zapasowych, tzw. klonów całych maszyn wirtualnych w czasie ich pracy.
20.	Posiada możliwość dodawania do maszyn wirtualnych w czasie pracy – procesorów, dodatkowej pamięci RAM oraz zasobów dyskowych.
21.	Umożliwia automatyczne równoważenie obciążenia serwerów fizycznych pracujących jako platforma dla infrastruktury wirtualnej.
22.	Oprogramowanie do wirtualizacji musi obsługiwać przełączenie ścieżek SAN (bez utraty komunikacji) w przypadku awarii jednej z dwóch ścieżek.
23.	Usługa wsparcia technicznego producenta ma być świadczona zgodnie z zapisami zawartymi w Rozdziale III.

3. Serwerowe systemy operacyjne 1

Licencje na serwerowy system operacyjny muszą umożliwiać uruchamianie użytkowanych przez Zamawiającego aplikacji obecnie działających w środowisku systemów operacyjnych Red Hat Enterprise Linux for Virtual Datacenters x86_64.

Lp.	Wymagania minimalne
1.	Serwerowy system operacyjny musi wspierać architekturę x86_64.
2.	Pełny kod źródłowy systemu musi być dostępny na warunkach licencyjnych oprogramowania typu open source.
3.	Oprogramowanie jest standardowo wyposażone w mechanizm bezpieczeństwa Security Enhanced Linux (SELinux) wraz z przygotowanymi i uaktualnionymi politykami bezpieczeństwa. System zapewnia narzędzia tekstowe i graficzne pozwalające w prosty sposób analizować alarmy bezpieczeństwa.
4.	System operacyjny posiada wbudowaną obsługę wirtualizacji oraz narzędzia służące do zarządzania maszynami wirtualnymi.
5.	Instalator systemu operacyjnego umożliwia utworzenie szyfrowanych partycji jeszcze przed instalacją systemu operacyjnego.
6.	System operacyjny posiada certyfikat bezpieczeństwa zgodny z EAL4+.
7.	Licencje na serwerowy system operacyjny muszą być przypisane do każdego rdzenia procesora fizycznego znajdującego się w dostarczanych serwerach kasetowych lub do każdego procesora fizycznego znajdującego się w dostarczanych serwerach kasetowych lub do każdej pary procesorów znajdujących się w dostarczanych serwerach kasetowych (zgodnie z modelem licencjonowania producenta)
8.	Oprogramowanie wraz z niezbędnymi licencjami musi uprawniać do użytkowania serwerowego systemu operacyjnego na każdym dostarczanym fizycznym serwerze kasetowym jednocześnie, przy pełnym wykorzystaniu dostępnych zasobów procesorów/rdzeni.
9.	Oprogramowanie wraz z niezbędnymi licencjami musi uprawniać do uruchamiania serwerowego systemu operacyjnego w środowisku fizycznym i nielimitowanej liczbie

	wirtualnych środowisk serwerowego systemu operacyjnego.
10.	Oprogramowanie musi mieć możliwość uruchamiania na maszynach fizycznych lub w środowiskach wirtualnych.
11.	Oprogramowanie musi posiadać wsparcie producenta dostarczanej platformy wirtualizacji.
12.	Oprogramowanie musi poprawnie współdziałać z dostarczaną platformą sprzętową.
13.	Oprogramowanie musi umożliwiać uwierzytelnianie i autoryzację w usłudze katalogowej Active Directory użytkowanej przez Zamawiającego. Aktualny poziom funkcjonalności domeny to 2016.
14.	Oprogramowanie musi posiadać możliwość centralnego uwierzytelniania użytkowników.
15.	Oprogramowanie musi posiadać możliwość lokalnego autoryzowania dostępu użytkowników.
16.	Oprogramowanie musi posiadać możliwość centralnego autoryzowania dostępu użytkowników.
17.	Oprogramowanie musi wspierać granularny przydział uprawnień.
18.	Oprogramowanie musi umożliwiać budowanie klastrów wysokiej dostępności.
19.	Oprogramowanie musi posiadać możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.
20.	Oprogramowanie musi stosować mechanizmy kryptograficzne do transmisji danych przesyłanych w sieciach publicznych.
21.	Oprogramowanie wraz z niezbędnymi licencjami musi posiadać aktywne wsparcie Producenta zgodnie z zapisami zawartymi w Rozdziale III.
22.	Serwerowy system operacyjny musi znajdować się na liście wspieranej przez producenta konfiguracji dla użytkowanej przez Zamawiającego aplikacji Red Hat Jboss Web Server

4. Serwerowe systemy operacyjne 2

Licencje na serwerowy system operacyjny muszą umożliwiać uruchamianie użytkowanych przez Zamawiającego aplikacji obecnie działających w środowisku Microsoft Windows w architekturze x86_64. Licencje muszą być przypisane do każdego rdzenia procesora fizycznego znajdującego się w dostarczanych serwerach kasetowych. Licencja musi uprawniać do uruchamiania serwerowego systemu operacyjnego w środowisku fizycznym i **nielimitowanej liczbie wirtualnych środowisk** serwerowego systemu operacyjnego. Oprogramowanie wraz z niezbędnymi licencjami musi uprawniać do użytkowania serwerowego systemu operacyjnego na każdym dostarczanym fizycznym serwerze kasetowym jednocześnie, przy pełnym wykorzystaniu dostępnych zasobów procesorów/rdzeni.

Dodatkowo serwerowy system operacyjny musi posiadać następujące wbudowane cechy:

Lp.	Wymagania minimalne
1.	Możliwość wykorzystania do 512 logicznych procesorów oraz co najmniej 24 TB pamięci RAM w środowisku fizycznym.
2.	Możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności do 64TB przez każdy wirtualny serwerowy system operacyjny.
3.	Możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania 7000 maszyn wirtualnych.
4.	Możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci.
5.	Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy.
6.	Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy.
7.	Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.
8.	Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading.
9.	Wbudowane wsparcie instalacji i pracy na wolumenach, które: - pozwalają na zmianę rozmiaru w czasie pracy systemu, - umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów, - umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów, - umożliwiają zdefiniowanie list kontroli dostępu (ACL).

10.	Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.
11.	Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.
12.	Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET.
13.	Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.
14.	Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.
15.	Dostępne dwa rodzaje graficznego interfejsu użytkownika: - Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy, - Dotykowy umożliwiający sterowanie dotykiem na monitorach dotykowych.
16.	Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe.
17.	Możliwość zmiany języka interfejsu po zainstalowaniu systemu, poprzez wybór z listy dostępnych lokalizacji.
18.	Mechanizmy logowania w oparciu o: - Login i hasło, - Karty z certyfikatami (smartcard), - Wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM),
19.	Możliwość wymuszania wieloelementowej dynamicznej kontroli dostępu dla: określonych grup użytkowników, zastosowanej klasyfikacji danych, centralnych polityk dostępu w sieci, centralnych polityk audytowych oraz narzuconych dla grup użytkowników praw do wykorzystywania szyfrowanych danych.
20.	Wsparcie dla powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).

21.	Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.
22.	Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa.
23.	Pochodzący od producenta systemu serwis zarządzania polityką dostępu do informacji w dokumentach (Digital Rights Management).
24.	Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach.
25.	Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji: - Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC. - Usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji: o Podłączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną, o Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania, o Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza. - Bezpieczny mechanizm dołączania do domeny uprawnionych użytkowników prywatnych urządzeń mobilnych opartych o iOS i Windows 8.1. - 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: o Dystrybucję certyfikatów poprzez http o Konsolidację CA dla wielu lasów domeny, o Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen, o Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509.

	- 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). - Wsparcie dla algorytmów Suite B (RFC 4869). - 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 do 1000 aktywnych środowisk wirtualnych systemów operacyjnych. Wirtualne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności. Mechanizmy wirtualizacji mają zapewnić wsparcie dla: o Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych, o Obsługi ramek typu jumbo frames dla maszyn wirtualnych, o Obsługi 4-KB sektorów dysków, o Nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra, o Możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API, o Możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk mode).
26.	Możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta serwerowego systemu operacyjnego umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet.
27.	Wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath).
28.	Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego.

29.	Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.
30.	Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF
31.	Oprogramowanie wraz z niezbędnymi licencjami musi posiadać aktywne wsparcie Producenta zgodnie z zapisami zawartymi w Rozdziale III.
32.	Licencja musi zapewniać możliwość korzystania z wcześniejszych wersji zamawianego oprogramowania.
33.	Licencje muszą być przeznaczone do użytku w jednostkach rządowych na terenie Rzeczpospolitej Polskiej.